Newsletter 05/2023

Projektfortschritt & Aktuelles

Delphi Studie

Nachdem im letzten Newsletter des Jahres 2022 davon berichtet wurde, dass die Delphi-Studie kurz vor der Fertigstellung steht, können wir heute bekannt geben, dass die dritte Iteration erfolgreich abgeschlossen wurde. Nach der finalen Aggregation haben wir insgesamt 26 individuelle Prozesseinflussdimensionen von IT-Sicherheitsmaßnahmen definiert. Hierzu gehören unter anderem Dimensionen wie *Abstimmungs- und Planungsaufwände*, *Mitarbeiterzufriedenheit* oder aber auch *Prozessdurchlaufzeit* sowie viele weitere. Momentan werden diese Prozesseinflussdimensionen nach ihrer Praxisrelevanz priorisiert. Eine detaillierte Übersicht aller Prozessdimensionen werden wir Ihnen in Kürze zur Verfügung stellen.

Kategorisierung

Zusätzlich zur Finalisierung der Delphi-Studie, und damit auch der Prozessdimensionen, wurde damit begonnen, die Prozessdimensionen zu kategorisieren. Hierfür wurden im Rahmen von mehreren Interviews mit den Projektpartnern (nochmals ein großes Danke and die Rezeptprüfstelle Duderstadt GmbH und die msu solutions GmbH) die Prozessdimensionen zu anwenderorientierten Meta-Kategorien zugeordnet. Die Kategorisierung soll die Bewertung von Investitionen in IT-Sicherheitsmaßnahmen mit Hilfe der ProBITS-Methode erleichtern, indem die potenziellen Prozesseinflussdimensionen strukturiert dargestellt werden. Die Kategorisierung ist in zwei Ebenen unterteilt, wobei sich die obere Ebene auf das generische Prozessmodell *(Inputs, Prozesseigenschaften, Outputs* und *Outcomes*) bezieht. Darüber hinaus wurden auf der zweiten Ebene Inputs und Outcomes in insgesamt sieben Unterkategorien untergliedert (*Personeller Aufwand, Ressourcenaufwand, Compliance/Regulatorik, Zufriedenheit, Kompetenzen, Wettbewerbsvor/ -nachteile, Prozessqualität*).

„ProBITS in Aktion“ Entscheidungsmodell

In den vergangenen Newslettern wurde bereits über den Einsatz des multikriteriellen Entscheidungsmodells mit den Projektpartnern der Rezeptprüfstelle Duderstadt GmbH und der msu solutions GmbH berichtet. Im Verlauf der vergangenen Monate wurde das Modell weiterhin iterativ angepasst und im Kontext unterschiedlicher Fallstudien getestet. Darüber hinaus wurde das Entscheidungsmodell auch bei der Volkswagen Financial Services AG – assoziierter Partner von ProBITS – erfolgreich angewendet. Wir bedanken uns vielmals für die Unterstützung bei der Entwicklung des Entscheidungsmodells bei den involvierten Projektpartnern.

Nationale Konferenz IT-Sicherheitsforschung 2023

Im Rahmen der Projekt-Kommunikation war das ProBITS-Team auf der Nationalen Konferenz IT-Sicherheitsforschung des Bundesministeriums für Bildung und Forschung vertreten, um über den aktuellen Stand des Projektes zu berichten und um sich mit weiteren Mitgliedern der IT-

Sicherheitsforschungsgemeinde über aktuelle Thematiken und Probleme auszutauschen. Die Konferenz stand unter dem Motto „*Die digital vernetzte Gesellschaft stärken*“ zu dem anregende Vorträge gehalten und Diskussionen geführt wurden.

Community Days (summit) bei den Leipziger Softwareforen

Im Mai 2023 fanden die Community Days zu „Governance, Risk und Compliance in der IT“ und „IT- Security-Management“ der Softwareforen Leipzig statt. Das ProBITS-Team nahm an der Tagung teil und referierte über das Thema: „*IT- Sicherheit: (K)eine Frage des Geldes? Wie Sie Prozesse nutzen können, um wirtschaftliche Entscheidungen zu IT- Sicherheitsmaßnahmen zu treffen*“. Der inhaltliche Fokus lag zum einen auf der Vorstellung einer realen Fallstudie, im Rahmen derer das multikriterielle Entscheidungsmodell der ProBITS-Methode bei unserem assoziierten Partner Volkswagen Financial Services AG angewendet wurde, sowie zum anderen auf allgemeinen Adoptionsbarrieren von Bewertungsverfahren für IT-Sicherheitsinvestitionen.

Die Softwareforen vereinen im Rahmen der Community Days (bzw. unter dem neuen Namen „summit“) Unternehmen unterschiedlicher Branchen aus dem deutschsprachigen Raum. Dadurch ermöglicht die Tagung den Austausch zu aktuellen Entwicklungen aus dem IT-Bereich über verschiedenste Wirtschaftssektoren hinweg. Während, sowie im Anschluss an den Vortrag, wurde sich lebendig über das Vortragsthema sowie das Projekt ProBITS ausgetauscht. Insgesamt konnte das ProBITS-Team viele neue Erkenntnisse gewinnen, die zur Weiterentwicklung der ProBITS-Methode beitragen.

Aktuelle ProBITS News

Aktuelle Entwicklungen im Bereich Informationssicherheit

Artificial Intelligence Act

Bereits im April 2021 hat die EU-Kommission den Artificial Intelligence Act (AI Act), also das Gesetz über künstliche Intelligenz vorgeschlagen, um eine europäische Regulierung von KI zu etablieren und somit den Endnutzer zu schützen. In den vergangen zwei Jahren wurden unterschiedliche Aspekte kontrovers diskutiert. Vor allem die Größe und Komplexität des Vorhabens gestaltet die Verhandlungen schwierig. Anfang Mai 2023 haben der Binnenmarktausschuss und der Ausschuss für bürgerliche Freiheiten in Straßburg den Entwurf eines Verhandlungsmandats angenommen. Die Abgeordneten wollen in dem Änderungsantrag zum Kommissionsvorschlag sicherstellen, dass KI-Systeme von Menschen überwacht werden und eine Reihe von Eigenschaften, wie Transparenz und Sicherheit, nachweisen. Zudem wird eine einheitliche und technologieneutrale Definition, welche für alle bestehenden und zukünftigen KI-Systeme gilt, gefordert.

Der aktuelle Vorschlag wird aber nicht nur vom Gesetzgeber diskutiert, auch Wirtschaftsverbände sehen einige Probleme. Im März 2023 veröffentlichte der deutsche Digitalverband „Bitkom e.V.“ ein Positionspapier, in welchem drei Hauptprobleme aufgezeigt werden. So wird aufgeführt, dass eine Hoch-Risiko Klassifikationsebene für KI-Systeme fehlt, welche dazu führen könnte, dass KI-Systeme zu restriktiv klassifiziert werden. Weiterhin wird kritisiert, das eine Grundrechtsprüfung, wie sie im aktuellen Vorschlag gefordert wird, bereits durch andere Risikomanagement-Maßnahmen abgedeckt ist und der Vorschlag somit unnötig komplex ist. Zuletzt wird gefordert, dass sogenannte General-Purpose-KIs, also KI-Systeme ohne spezifischen Zweck, nicht durch den AI-Act betroffen sein sollten. Es wird argumentiert, dass ein Risiko durch eine KI erst durch einen spezifischen Einsatz oder Zweck entsteht und nicht durch ihre allgemeine Funktionsweise. Nichtsdestotrotz sollten aber auch für Entwickler solcher KI-Systeme Regeln gelten.

Bevor die Verhandlungen über die endgültige Form des Gesetzes beginnen können, muss der Entwurf vom gesamten Parlament gebilligt werden. Diese Abstimmung wird voraussichtlich in der Sitzung vom 12. bis 15. Juni 2023 erfolgen.

Quellen: www.europarl.europa.eu; www.bitkom.org

Deezer Datenleck

Im Februar 2023 ist bekannt geworden, dass es bei einem Partnerunternehmen des Musikstreaming Dienstes Deezer bereits Mitte 2019 zu einem Hacker Angriff mit anschließendem Datendiebstahl kam. Insgesamt wurden rund 230 Millionen Nutzerdatensätze gestohlen, darunter sind ca. 14 Millionen Datensätze von deutschen Nutzern. Deezer gibt an, dass das Unternehmen erst im November 2022 von dem Datenleck erfahren hat.

Eine besondere Problemstellung ergibt sich aus der Kooperation des Mobilfunkanbieters Vodafone mit Deezer. Durch die Kooperation konnten Vodafone Nutzer das Angebot von Deezer kostenlos nutzen. Dies führt aber auch dazu, dass viele Vodafone Kunden ein Deezer-Konto besitzen, ohne davon zu wissen, da das entsprechende Konto automatisch bei Vertragsabschluss mit Vodafone erstellt wurde.

Unterdessen könnte der Vorfall dem Unternehmen teuer zu stehen kommen. Medienanwälte gehen aufgrund einer ähnlichen Rechtsprechung bei einem Facebook-Datenleck davon aus, dass betroffenen Nutzern aus der EU eine Entschädigung von bis zu 1000€ zusteht.

Quellen: www.netzwelt.de; www.heise.de; www.wbs.legal

Russisches „Snake“-Malware-Netzwerk durch FBI lahmgelegt

Eine Einheit des russischen Geheimdienstes namens „Turla“ nutzte seit fast 20 Jahren eine Snake-Malware, um sensible Dokumente von Computersystemen in mindestens 50 Ländern zu stehlen. Dabei wurden Regierungen von NATO-Mitgliedsstaaten, Journalisten und andere für Russland interessante Ziele angergriffen. Turla schleuste die Dokumente dazu durch ein

verdecktes Netzwerk aus mit der Schadsoftware kompromittierten Computern auf der ganzen Welt.

Das FBI hat ein Tool namens Perseus entwickelt, mit dem es nun gelungen ist, das Netzwerk außer Gefecht zu setzen. Dieses hat der Malware Befehle untergeschoben, damit das Programm essenzielle Komponenten selbst überschreibt.

Allerdings wurden keine Schwachstellen gepatcht und auch nicht nach zusätzlicher Malware oder Hackertools gesucht, die möglicherweise auf den Rechnern der Opfer platziert wurden, weshalb Betroffene zusätzliche Maßnahmen ergreifen sollten. Das US-Justizministerium empfiehlt etwa die tiefgehende Analyse der Schadsoftware der US-Cyber-Sicherheitsbehörde CISA zu konsultieren.

Quelle: www.heise.de

Zwei Komponenten des Linux-Kernels von Sicherheitslücken betroffen

Über die Use-After-Free-Lücke im nf_tables-Modul und einem Logikfehler in FUSE (Filesystem in Userspace) können unprivilegierte Nutzer mit Root-Rechten, und damit der Ausweitung der eigenen Rechte, das System übernehmen.

Mit FUSE ist es möglich Linux-fremde Dateisysteme einzubinden, ohne dass der Nutzer zusätzliche Rechte benötigt. Allerdings ist es Sicherheitsforschern gelungen, die Interaktion zwischen Linux-Kernel und FUSE beim Kopieren von Dateien durcheinanderzubringen und auf diesem Weg Root-Rechte zu erlangen. Betroffen sind Systeme mit Kernelversionen zwischen 5.11 und 5.19 sowie installierten FUSE.

Dagegen ist über die Sicherheitslücke im nf_tables bislang relativ wenig bekannt. Sicherheitsforscher haben den Bug veröffentlicht und einen Root-Exploit entwickelt. Dieser wird allerdings noch veröffentlicht werden, um Entwicklern eine Embargofrist einzuräumen, sodass sie die Lücke schließen können. Die Manipulation der nf_tables-Konfiguration soll zu einem fehlerhaften Speicherzugriff führen (use after free), indem direkt aufeinanderfolgende Operationen unter Umständen falsch verarbeitet werden.

In beiden Fällen ist ein Angriff aus der Ferne nicht möglich, der Angreifer benötigt lokalen Zugang zum System.

Quelle: www.heise.de

Ausblick und kommende Termine

Nächste Projektschritte

Im weiteren Verlauf des Projektes steht weiterhin die abschließende Entwicklung und Implementierung des Prototyps des ProBITS-IT-Tools im Mittelpunkt. Hierzu wird demnächst eine ausführliche Erprobung gestartet. Zusätzlich werden aktuell konkrete Beispiele und Ausprägungen der einzelnen Prozessdimensionen gesammelt bzw. evaluiert. Diese sollen dem Anwender als Unterstützung zur Einschätzung dienen.

Kommende Termine

- Präsentation der Forschungsartikel „*A Qualitative Study on Acceptance Factors of Economic Approaches on IT Security Investment Decisions*“ und „*A Process-Based Approach to Information Security Investment Evaluation: Design, Implementation, and Evaluation*“ auf der 2023 Americas Conference on Information Systems, welche vom 9. – 12. August in Panama City stattfindet.
- Veranstaltung des dritten *International Workshop on Current Information Security and Compliance Issues in Information System Research (CIISR 2023)*, welcher im Rahmen der *18th International Conference on Wirtschaftsinformatik (WI2023)* am 18. September 2023 in Paderborn stattfindet.

Impressum

www.probits.uni-goettingen.de

Universität Paderborn

Professur für Wirtschaftsinformatik, insb. Nachhaltigkeit
Warburger Straße 100
33098 Paderborn

Vertreten durch:
Prof. Dr. Simon Trang
Warburger Straße 100
33098 Paderborn
probits@uni-goettingen.de

Universität Paderborn
Warburger Straße 100
33098 Paderborn
T +49 5251 600
presse@zv.upb.de