Newsletter 12/2023

Projektfortschritt & Aktuelles

Umzug der Projektwebsite

Mit dem Wechsel von Prof. Dr. Simon Trang von der Universität Göttingen an den Lehrstuhl für Wirtschaftsinformatik, insb. Nachhaltigkeit der Universität Paderborn, ist auch die Projektwebsite des ehemaligen Lehrstuhls für Informationssicherheit und Compliance an die Universität Paderborn gewechselt. Die Website der Universität Paderborn präsentiert sich dabei in einem neuen, einheitlichen Design. Wie gewohnt finden sich dort neben allgemeinen Informationen, außerdem die beteiligten Verbund- und assoziierten Partner, News über ProBITS und Veröffentlichungen über das Forschungsprojekt.

Die ProBITS Website kann nun unter folgendem Link abgerufen werden:
https://probits.uni-paderborn.de/

Abschluss und Ergebnisse der Delphi-Studie

Für die Durchführung der vierten und abschließenden Runde der ProBITS Delphi-Studie wurden die ProBITS Praxispartner gebeten, alle 26 Prozesseinflussdimensionen anhand ihrer persönlichen Relevanz für den jeweiligen Unternehmenskontext zu bewerten. Das Hauptziel der Umfrage bestand darin, eine Rangfolge der Dimensionen abzuleiten. Die Umfrage wurde von insgesamt 18 Praxispartnern durchgeführt. Unter diesen befanden sich 10 Praxispartner mit einer Firmengröße von mehr als 250 Mitarbeitern und 8 Praxispartner, deren Unternehmen weniger als 250 Mitarbeiter beschäftigen. Somit waren kleine und mittelgroße Unternehmen etwa gleich stark vertreten. Die meisten Teilnehmer stammten aus den Branchen IT & Telekommunikation sowie Bildung & Forschung. Aus dem Feedback der gesamten Teilnehmer ergibt sich die Rangfolge der Dimensionen, sortiert nach absteigender Relevanz. Die Sortierung erfolgt nach dem Prinzip des höchsten Mittelwerts und geringster Standardabweichung.

Ranking (Gewichtung der Relevanz nach Mittelwert und Varianz) - absteigende Sortierung
1. Datenverfügbarkeit
2. Prozesswiederherstellbarkeit (business continuity)
3. Prozessergebnis
4. Prozesstreue
5. Prozesskomplexität
6. Prozessverfügbarkeit
7. Prozessdurchlaufzeit
8. Prozessstabilität
9. IT-Sicherheitsbewusstsein (Awareness)
10. Kundenzufriedenheit
11. Prozessautomatisierung
12. Prozesskompatibilität
13. Mitarbeiteraufwand
14. Abstimmungs- und Planungsaufwand
15. Strategische Wettbewerbsposition
16. Prozessflexibilität/-Anpassungsfähigkeit
17. Prozessverständnis
18. Reputation
19. Mitarbeiterzufriedenheit
20. Dokumentationsaufwand
21. Innovationsfähigkeit
22. Prozessstandardisierung
23. Schulungsaufwand
24. Kooperationsmöglichkeit
25. Technologieaufwand
26. Zuliefererzufriedenheit

Zur Überprüfung der Erkenntnisse auf Generalisierbarkeit wurde die Stichprobe in einer weiteren Umfragerunde vergrößert. Die Stichprobe wurde über die Plattform Prolific erhoben. Durch den Vergleich beider Studien lassen sich (unter anderem) folgende Gemeinsamkeiten und Unterschiede in der Gewichtung der Dimensionen finden:

Gemeinsamkeiten (Beispiele):

- *Business Continuity* und *Datenverfügbarkeit* sind die wichtigsten Einflussfaktoren in beiden Studien
- *Zulieferer-* und *Mitarbeiterzufriedenheit* werden als eine der am wenigsten wichtigen Einflussfaktoren betrachtet und befinden sich auf den untersten Plätzen.

Unterschiede (Beispiele):

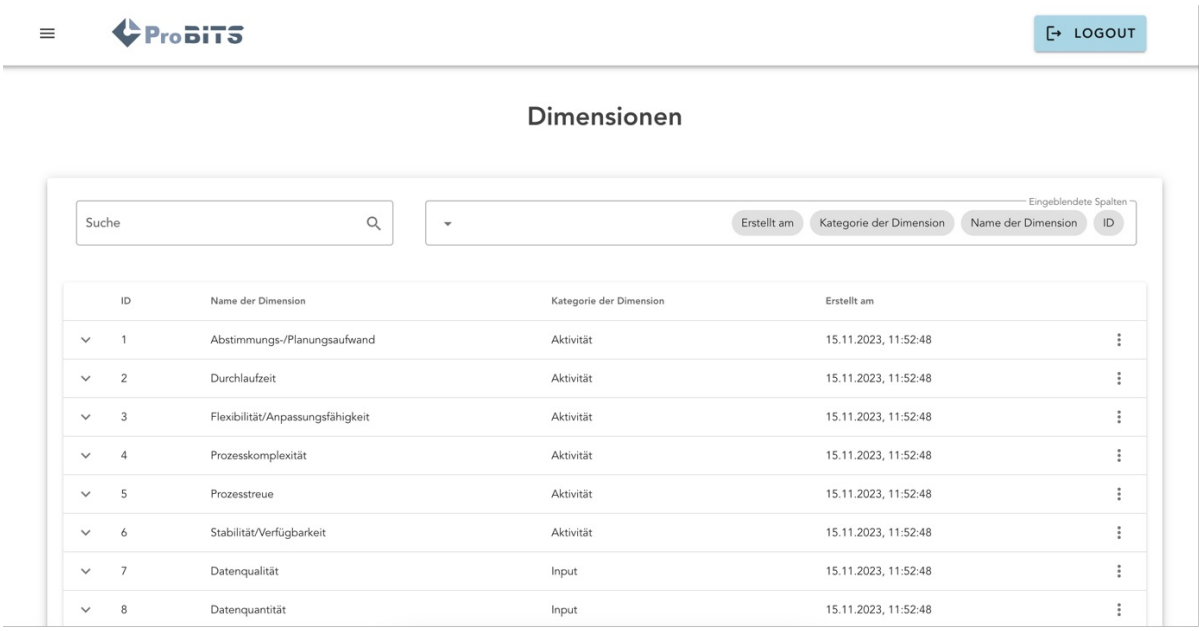
- *Prozesstreue* und *Prozessergebnis* werden in der Praxispartner-Studie als sehr wichtig eingestuft, während diese in der Prolific-Studie im unteren Drittel zu finden sind
- *Reputation* und *Schulungsaufwand* werden in der Prolific-Studie als sehr wichtig eingestuft, während diese in der Praxispartner-Studie im unteren Drittel zu finden sind

Zum besseren Verständnis sind hier ein paar ausgewählte Dimensions-Definitionen aufgelistet:

- *IT-Sicherheitsbewusstsein (Awareness)*: Beschreibt das Bewusstsein und die Achtsamkeit der Mitarbeiter des Unternehmens gegenüber IT-Sicherheitsbedrohungen, -Maßnahmen und Konsequenzen.
- *Mitarbeiterzufriedenheit*: Beschreibt, zu welchem Grad Bedürfnisse und Erwartungen der Mitarbeiter erfüllt werden.
- *Prozesswiederherstellbarkeit (Business Continuity)*: Beschreibt die Fähigkeit, im Ernstfall/nach Ausfall den Prozess schnellstmöglich und kostengünstig wiederherstellen zu können.
- *Prozesstreue*: Beschreibt, inwiefern Mitarbeiter oder IT-Systeme bei der Ausführung des Prozesses von dem vorgesehenen Prozessablauf abweichen.

Aktueller Stand des IT-Tools

Der Prototyp wird laufend getestet und weiterentwickelt. In diesem iterativen Verfahren, hat sich das Design der Applikation seit der ersten Version merklich verändert. Auf Basis des Feedbacks der ProBITS Praxispartner arbeiten wir beispielsweise aktuell an der Weiterentwicklung des Usermanagements und Anpassung des ProBITS-Bewertungsprozesses innerhalb des Tools. Insgesamt sind wir überzeugt, dass der Prototyp der zweiten Version einen deutlichen Fortschritt in Bezug auf Benutzerfreundlichkeit gemacht hat. Gleichzeitig ist zu beachten, dass wir uns noch nicht am Ende des Entwicklungsprozesses befinden. Der Prototyp unterliegt einer fortlaufenden Bewertung von Akzeptanzfaktoren und wird kontinuierlich optimiert. Im Folgenden sehen Sie einen beispielhaften Screenshot der überarbeiteten Designs für die Dimensionsübersicht.



Das Frontend wird mit dem Vue.js Framework umgesetzt und mithilfe des HTTP-Clients Axios werden die Anfragen an das Django Backend gesendet und sicher verarbeitet. Selbst wenn die App später keinen Internetzugang hat, werden die Sicherheitsaspekte beachtet, wie etwa das Hashen von Passwörtern in der Datenbank oder die Berechtigungen für bestimmte Bereiche der Anwendung.

An dieser Stelle möchten wir unseren Projektpartnern der Rezeptprüfstelle Duderstadt GmbH und der msu Solutions GmbH herzlich für Ihre tatkräftige Unterstützung bei der Entwicklung und Evaluation des ProBITS IT-Tools danken.

Erfolgreiche Durchführung des 3rd International Workshop on Current Information Security and Compliance Issues in Information Systems Research (CIISR'23) @ WI 2023

Am 18.09.2023 fand bereits zum dritten Mal der Internationale Workshop zum Thema 'Current Information Security and Compliance Issues in Information Systems Research' statt. Dieser wurde von Dr. Stephan Kühnel, Dr. Ilja Nastjuk, Prof. Dr. Stefan Sackmann und Prof. Dr. Simon Trang im Rahmen der 18. Internationalen Tagung Wirtschaftsinformatik (WI 2023) organisiert.

Da in diesem Jahr viele Forschungspapiere eingereicht wurden und letztendlich acht nach einem rigorosen Peer-Review-Prozess akzeptiert werden konnten, wurde der Workshop in zwei Sessions aufgeteilt. Eine Session für Full Research Papers, die vor dem Auditorium präsentiert und mit den Teilnehmern intensiv diskutiert wurden, und eine Poster-Session für Short Papers. Wir danken allen Vortragenden, Poster-Präsentatoren und Teilnehmern für den gelungenen Workshop!

Weitere Informationen und die final akzeptierten Beiträge finden Sie auf https://ciisr.wiwi.uni-halle.de/ oder auf der Website der WI-Konferenz unter https://wi2023.de/ws02/

Liste der akzeptierten Beiträge:

- **Sellami, Mahdi; Bueno Momčilović, Tomas; Kuhn, Peter; Balta, Dian**: *Interaction Patterns for Regulatory Compliance in Federated Learning*
- **Hillmann, Felix; Klauenberg, Tim; Schroeder, Lennart; Diesterhöft, Till Ole**: *A User-centric View on Data Breach Response Expectations*
- **Nake, Leonard**: *Integrating IT Security Aspects into Business Process Models: A Taxonomy of BPMN Extensions*
- **Böhmer, Martin**: *From Pixels to Generalization: Ensuring Information Security and Model Performance with Design Principles for Synthetic Image Data in Deep Learning*
- **Klymenko, Alexandra; Meisenbacher, Stephen; Messmer, Florian; Matthes, Florian**: *Privacy- Enhancing Technologies in the Process of Data Privacy Compliance: An Educational Perspective*
- **Pfaff, Theresa**: *Nudging Towards Compliance? Assessing the Impact of Nudging Strategies on Information Security Policy Adherence*
- **Hövel, Gilbert Georg; Matschak, Tizian**: *How to Foster Compliance in Non-Integrated IT-Landscapes? The Case of Manual Medical Data Transfers*
- **Klymenko, Alexandra; Meisenbacher, Stephen; Matthes, Florian**: *The Structure of Data Privacy Compliance*

Aktuelles aus der Forschung

Neue Publikation in der Zeitschrift Computers & Security erschienen (Impact Factor: 5,6)

Computers & Security 133 (2023) 103370

Contents lists available at ScienceDirect

Computers & Security

journal homepage: www.elsevier.com/locate/cose

Should i really do that? Using quantile regression to examine the impact of sanctions on information security policy compliance behavior

Sebastian Hengstler[a,#,*], Stephan Kuehnel[b], Kristin Masuch[a], Ilja Nastjuk[a], Simon Trang[c]

[a] Georg-August-Universität Göttingen – Research Group on Information Security and Compliance, Platz der Göttinger Sieben 5, Göttingen 37073, Germany
[b] Martin Luther University Halle-Wittenberg, Chair for Information Systems, esp. Business Information Management, Universitaetsring 3, Halle (Saale) 06108, Germany
[c] University of Paderborn – Chair of Information Systems and Sustainability, Warburger Str. 100, Paderborn 33098, Germany

ARTICLE INFO

Article history:
Received 1 January 2023
Revised 30 May 2023
Accepted 25 June 2023
Available online 29 June 2023

Keywords:
Information security policy compliance
International information security management
Deterrence theory
Quantile regression
Compliance behavior

ABSTRACT

Deterrence theory is one of the most commonly used theories to study information security policy non-compliance behavior. However, the results of studies in the information security field are ambiguous. To further address this heterogeneity, various influencing factors have been considered in the context of deterrence theory. However, a current challenge with these findings is that recent studies that quantitatively assess the effectiveness of deterrence have relied predominantly on methods that analyze the underlying data, starting from a regression-based approach. By applying quantile regression, we estimate the overall effect of deterrents, and uncover how their effect differs among employees with different inclinations toward ISP compliance behavior – a critical insight for determining security measures for specific employee groups. Based on longitudinal data gathered in the U.S., our findings show significantly different effects in the analyzed quantiles for both aspects of sanctions, namely certainty and severity.

Der Zeitschriftenartikel *Should I Really do That? Using Quantile Regression to Examine the Impact of Sanctions on Information Security Policy Compliance Behavior*, verfasst von Sebastian

Hengstler, Dr. Stephan Kühnel, Dr. Kristin Masuch, Dr. Ilja Nastjuk und Prof. Dr. Simon Trang geht der Frage nach, wie sich die Wirkung von Abschreckungsmechanismen bei Mitarbeiter:innen mit unterschiedlichem Informationssicherheitsbewusstsein unterscheidet. Zu diesem Zweck wurden Längsschnittdaten auf Basis einer Quantilregression analysiert. Die Ergebnisse zeigen signifikant unterschiedliche Effekte in den untersuchten Quantilen für Sanktionssicherheit und schwere, was eine wichtige Erkenntnis für die Festlegung von Informationssicherheitsmaßnahmen für bestimmte Mitarbeitergruppen ist.

Die Publikation ist frei verfügbar und kann über https://doi.org/10.1016/j.cose.2023.103370 abgerufen werden.

Beitrag auf der Informatik 2023

Leonard Nake, Dr. Stephan Kühnel, Laura Bauer und Prof. Dr. Stefan Sackmann konnten einen Beitrag auf der 53. Jahrestagung der Gesellschaft für Informatik platzieren und im Rahmen des 8. Workshop zum Stand und den Herausforderungen des Geschäftsprozessmanagements (ZuGPM 2023), organisiert von Prof. Dr. Ralf Laue und Prof. Dr. Michael Fellmann, präsentieren. So stellte unser Kollege Leonard Nake die folgende Publikation vor:

- **Leonard Nake, Stephan Kuehnel, Laura Bauer und Stefan Sackmann**: *Towards Identifying GDPR-Critical Tasks in Textual Business Process Descriptions, in: M. Klein, D. Krupka, C. Winter., V. Wohlgemuth (Hrsg.): INFORMATIK 2023, Lecture Notes in Informatics (LNI), Gesellschaft für Informatik, Bonn 2023 (forthcoming)*

Die Publikation befasst sich mit einem Ansatz, der durch die Verwendung von Maschinellem Lernen automatisch Aktivitäten in Geschäftsprozessbeschreibungen identifiziert, die persönliche Daten verarbeitet (angelehnt an die Definition aus der DSGVO). Weitere Informationen über die Konferenz und die einzelnen Themenbereiche finden Sie unter https://informatik2023.gi.de/

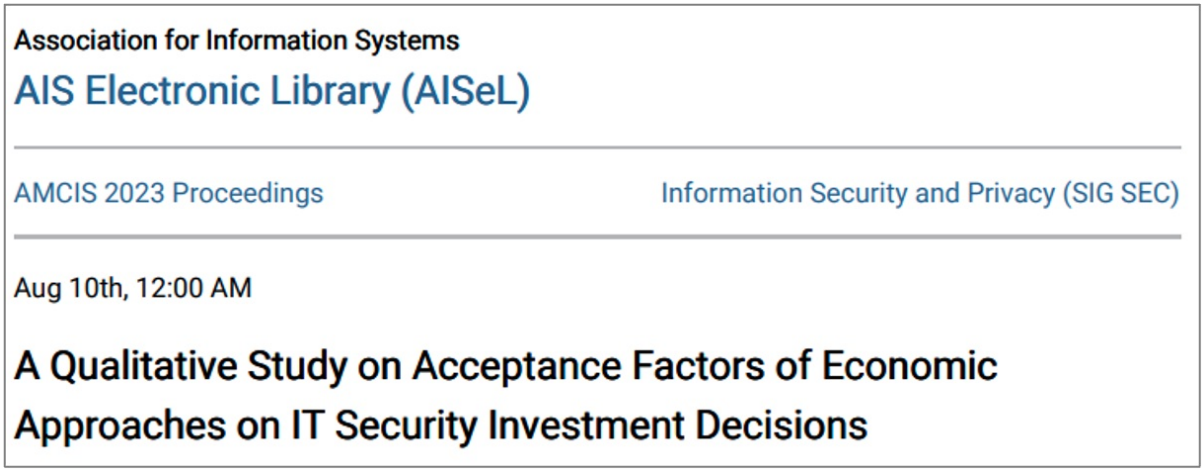
Beitrag auf dem 3rd International Workshop on Current Information Security and Compliance Issues in Information Systems Research auf der WI23

Unser Kollege Leonard Nake stellte auf dem diesjährigen CIISR Workshop eine Publikation vor, die im Rahmen des ProBITS-Projekts entstand. Es trägt den Titel:

- **Nake, Leonard**: *Integrating IT Security Aspects into Business Process Models: A Taxonomy of BPMN Extensions*, in: Kühnel, Stephan, Nastjuk, Ilja, Sackmann, Stefan und Trang, Simon (Hrsg.): Proceedings of the 3rd International Workshop on Current Information Security and Compliance Issues in Information Systems Research (CIISR 2023)

Der Artikel befasst sich mit der Entwicklung einer Taxonomie unterschiedlicher Erweiterungen der Modellierungssprache für Geschäftsprozessmodellierung BPMN, die Aspekte der IT Security in die Geschäftsprozessmodelle von Unternehmen integrieren.

Beiträge auf der Americas' Conference on Information Systems


Association for Information Systems
AIS Electronic Library (AISeL)

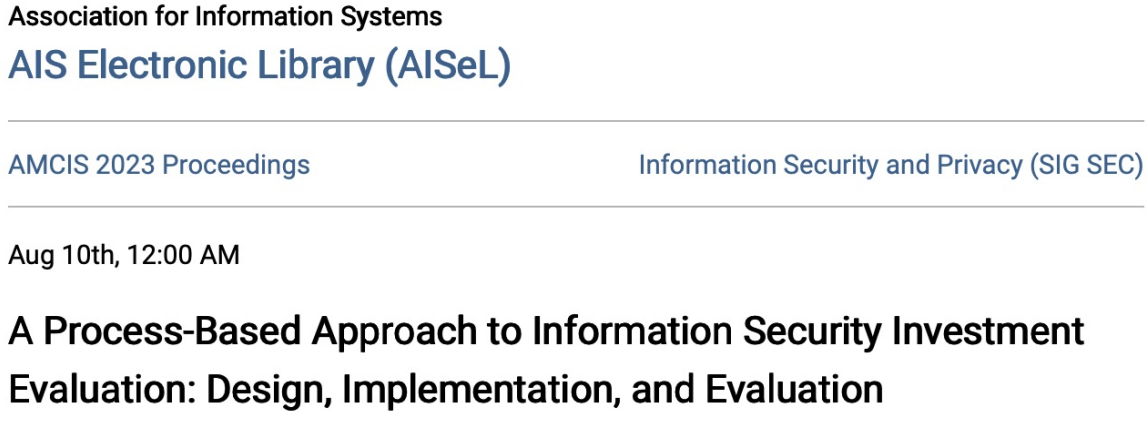
AMCIS 2023 Proceedings | Information Security and Privacy (SIG SEC)

Aug 10th, 12:00 AM

A Qualitative Study on Acceptance Factors of Economic Approaches on IT Security Investment Decisions

Der Konferenzbeitrag *A Qualitative Study on Acceptance Factors of Economic Approaches on IT Security Investment Decisions* von Laura Bauer (geb. Niedzela), Dr. Stephan Kühnel, Dr. Ilja Nastjuk, Tizian Matschak, Prof. Dr. Stefan Sackmann und Prof. Dr. Simon Trang befasst sich mit der Frage, welche Faktoren die Akzeptanz und den Einsatz wirtschaftlicher Ansätze bei der Bewertung von IT-Sicherheitsinvestitionen beeinflussen. Hierfür wurde eine mehrstufige qualitative Analyse auf der Grundlage von Expertenbefragungen durchgeführt, wodurch fünf Kernbereiche mit untergeordneten Akzeptanzfaktoren abgeleitet werden konnten. Die Faktoren liefern dabei einen tiefgehenden Einblick in den Entscheidungsprozess zu IT-Sicherheitsmaßnahmen und gehen differenziert auf unterschiedliche Unternehmensebenen und mögliche Entscheidungsmethoden ein.

Der Forschungsbeitrag ist verfügbar unter [AIS Electronic Library (AISeL) - AMCIS 2023 Proceedings: A Qualitative Study on Acceptance Factors of Economic Approaches on IT Security Investment Decisions (aisnet.org)]


Association for Information Systems
AIS Electronic Library (AISeL)

AMCIS 2023 Proceedings | Information Security and Privacy (SIG SEC)

Aug 10th, 12:00 AM

A Process-Based Approach to Information Security Investment Evaluation: Design, Implementation, and Evaluation

Der Konferenzbeitrag *A Process-Based Approach to Information Security Investment Evaluation: Design, Implementation, and Evaluation* von Tizian Matschak, Dr. Ilja Nastjuk, Laura Bauer (geb. Niedzela), Dr. Stephan Kühnel und Prof. Dr. Simon Trang befasst sich mit der Frage, wie die Auswirkungen von Investitionen in die Informationssicherheit auf Geschäftsprozesse bewertet werden können. Dazu wird in diesem Beitrag eine neuartige prozessbasierte Bewertungsmethode vorgestellt, mit der diese bewertet werden können. Der Beitrag skizziert die praktischen Anforderungen an die Methode und ihre Umsetzung in Form eines Prototyps, der dann anhand eines dreistufigen Ansatzes mit zwei Unternehmen aus dem Gesundheitswesen und dem Energiesektor evaluiert wird. Die Evaluierungsergebnisse belegen die Nützlichkeit der vorgeschlagenen Methode für Investitionsentscheidungen im Bereich der Informationssicherheit. Diese Arbeit leistet einen Beitrag zur Bewertung von Investitionen in die Informationssicherheit, indem sie ein Proof-of-Concept liefert, das den Weg für künftige Forschungen zur Verbesserung der Qualität und Wirtschaftlichkeit von Investitionen in die Informationssicherheit ebnen kann.

Der Forschungsbeitrag ist verfügbar unter A Process-Based Approach to Information Security Investment Evaluation: Design, Implementation, and Evaluation

Bei Fragen und Interesse an unseren Publikationen kontaktieren Sie uns gerne.

Kontakt aufnehmen

Aktuelle Entwicklungen im Bereich Informationssicherheit

Hackerangriff auf die Hotelkette Motel One

Die Hotelkette „Motel One“ hat Ende September erklärt Ziel eines Hackerangriffs geworden zu sein, bei dem laut einem Medienbericht Millionen Namen und Reisedaten von Gästen online zu finden sind. Es soll sich dabei insbesondere um Adress- und Rechnungsdaten handeln und ein Volumen von sechs Terabyte umfassen. Das Unternehmen gibt außerdem an, dass die gestohlenen Daten im Darknet veröffentlicht wurden.

Zu dem Vorfall soll sich die Hackergruppe AlphV bekannt haben, die mutmaßlich Geld erpressen wollte und dem Unternehmen ansonsten mit einem Imageschaden drohte. Es soll sich dabei um eine russische Gruppierung handeln, die in der Vergangenheit bereits für einen Angriff auf ein Gesundheitsnetzwerk in Pennsylvania verantwortlich war.

Die Hotelkette verweist auf ihre umfassenden und hohen Sicherheitsstandards zum Schutz von personenbezogenen Daten. Dass der Hackerangriff dennoch erfolgreich war, spreche für die hohe kriminelle Energie der Täter. Um solche Vorfälle in Zukunft zu vermeiden arbeite „Motel One“ eng mit erfahrenen Experten für Informations- und IT-Sicherheit und den zuständigen Behörden zusammen, um zu jeder Zeit die größtmögliche Datensicherheit zu gewährleisten.

Quellen: www.t3n.de; www.tagesschau.de; www.motel-one.com

CEOs sorgen sich um Cybersicherheit

Aus einer international durchgeführten Umfrage geht hervor, dass der Großteil der befragten CEOs ihre Unternehmen nicht ausreichend gegen Cyberangriffe geschützt sieht. Demnach gaben laut einer Accenture-Umfrage 75 Prozent der insgesamt 1000 Befragten an, dass ihre Unternehmen nicht in der Lage sind Cyberangriffe abzuwehren. Allerdings gab fast die Hälfte an, nicht in präventive Maßnahmen investieren zu wollen. 46 Prozent verfolgen einen reaktiven Ansatz auf Cyberangriffe, anstatt in die Verhinderung dieser zu investieren.

Außerdem gaben 44 Prozent an, dass Cybersicherheit punktuelle, kurzfristige Aktionen anstatt eines kontinuierlichen Engagements erfordere. Begründet wird dies damit, dass die Kosten für die Implementierung eines langfristigen Konzepts höher seien als die Kosten eines potenziellen Cyberangriffs. Untersucht wurden die Sicherheitspraktiken von CEOs aus insgesamt 15 Länder aus unterschiedlichen Branchen.

Quellen: www.t3n.de; www.newsroom.accenture.de

Ausblick und kommende Termine

Nächste Projektschritte

Im weiteren Verlauf des Projektes wird das ProBITS-IT-Tools finalisiert und getestet. Hierzu gehört insbesondere die Evaluation der Version 2 mit den Praxispartnern. Zusätzlich wird die Hauptpublikation der Ergebnisse der Delphi Studie vorbereitet.

Kommende Termine

- Präsentation des Forschungsartikels „How to Avoid Medication Errors – Investigating the Roles of Policies and Nudging from a Stress Perspective” beim Pre-ICIS Workshop on Information Security and Privacy, welcher im Rahmen der International Conference on Information Systems am 10. Dezember in Hyderabad, Indien stattfindet

---

Das gesamte Team wünscht eine frohe Weihnachtszeit!

Impressum
https://probits.uni-paderborn.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