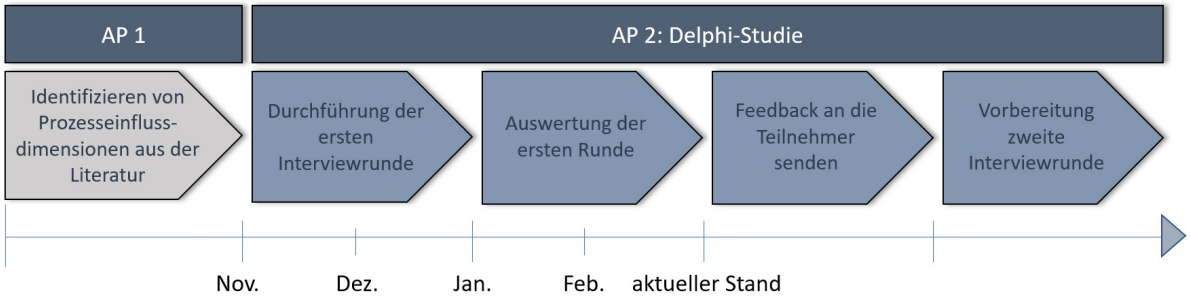
Newsletter 01 - 2022

Projektfortschritt & Aktuelles

Delphi Studie gestartet:



Im ProBITS Projektgeschehen freuen wir uns mitteilen zu können weitere Fortschritte zu machen. Die expertenbasierte Identifikation von Prozesseinflussgrößen und Bewertungsdimensionen von IT-Sicherheitsmaßnahmen ist mit den assoziierten Partnern und weiteren Akteueren aus Wissenschaft und Praxis in Form der Delphi-Methodik gestartet worden. Die Delphi-Methode zielt darauf ab, in iterativen Interviews einen Gesamtkonsens zu erreichen, um Ergebnisse konsolidieren und validieren zu können. Die erste Runde der Exptertеninterviews ist erfolgreich mit allen Projektpartnern durchgeführt und evaluiert worden. Im nächsten Schritt werden die Prozesseinflussdimensionen mit den in der Literatur identifizierten Einflussgrößen abgeglichen. Finaler Abschluss bildet ein Ergebniskatalog, der als Grundlage dient, ein multikriterielles Entscheidungsmodell aufzustellen.

Kommunikation in vollem Gang:

Um unsere Forschungsergebnisse mit anderen teilen zu können und wertvolles Feedback sammeln zu dürfen, haben wir in den vergangenen Monate mehrere internationale Konferenzen und Workshops besucht und organisiert:

International Workshop on Current Compliance Issues in Information Systems Research (CIISR'22) @ WI2022

Am 20.02.2022 fand zum zweiten Mal der internationale Workshop über „Current Compliance Issues in Information Systems Research“ im Rahmen der 17. Internationalen Tagung Wirtschaftsinformatik statt. Wir freuen uns darüber diesen spannenden Workshop abhalten zu dürfen und bedanken uns beim Organisation-Team, bestehend aus Prof. Dr. Stefan Sackmann, Prof. Dr. Simon Trang, Dr. Ilja Nastjuk und Dr. Stephan Kühnel für die wundervolle Vorbereitung.

Im Workshop Opening sprachen die Organisatoren mit den Teilnehmer:innen über Chancen und Risiken der Bewertung von Informations- und IT-Sicherheit im Kontext aktueller Regularien und Data Breaches, gefolgt von einen Kick-off-Vortrag mit dem Titel: *„Lets Help Make Compliance More Effective!“* von Prof. Dr. Simon Trang. Anschließend wurden die folgenden ausgewählten Beiträge präsentiert und diskutiert:

- Tizian Matschak, Theresa Pfaff: *„The Role of Situational Risk Propensity in Technology Threat Avoidance Behavior“*
- Laura Niedzela, Leonard Nake: *„Categories of Approaches for IT Security Investment Decisions: A Systematic Literature Review“*
- Emin Mehmet Yazici: *„Security Issues in Data Analytical Environments“*

Wir danken allen Teilnehmer:innen für die rege Diskussionsbereitschaft! Weitere Informationen über den Workshop finden sie auf unserer offiziellen CIISR-Webseite.

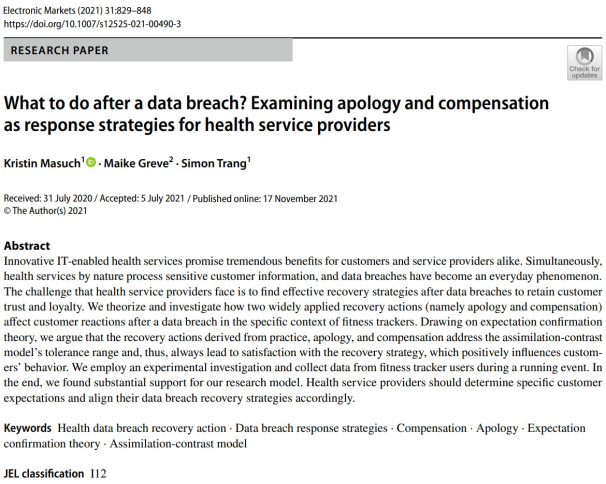
Workshop on Information Security and Privacy (WISP, Austin Texas)

Mitte Dezember 2021 konnten Kristin Masuch, Florian Rampold und Tizian Matschak erfolgreich am Workshop für Informationssicherheit und Privatsphäre in Austin (Texas) teilnehmen. Hierbei bot sich nicht nur die Möglichkeit aktuelle Themen aus den Bereichen IS und Privatsphäre mit internationalen Forscher:innen zu besprechen, sondern auch wertvolles Feedback für die eigenen Forschungsbeiträge im ProBITS-Projektkontext zu erhalten. Zur Tagesordnung gehörten unter anderem die Themen „Sozio-technische Analyse von Informationssicherheit/ Privatsphäre“, „Kulturelle Probleme der Informationssicherheit/ Privatsphäre“, „Analyse von System-Schwachstellen und Risikoexposition“, „Cyber Threat Intelligence“ und „Analyse sicherer Plattformen im Internet, Freiheit der Meinungsäußerung, Schutz der Privatsphäre“ und viele weitere. Wir freuen uns über die gewonnenen Eindrücke und die Möglichkeit, die ProBITS-Idee international vorzustellen.

Aktuelle ProBITS News

Aktuelles aus der Forschung

Masuch, K.; Greve, M.; Trang, S. (2021): What to do after a data breach? Examining apology and compensation as response strategies for health service providers, Electronic Markets, 31



Electronic Markets (2021) 31:829–848
https://doi.org/10.1007/s12525-021-00490-3

RESEARCH PAPER

What to do after a data breach? Examining apology and compensation as response strategies for health service providers

Kristin Masuch[1] · Maike Greve[2] · Simon Trang[1]

Received: 31 July 2020 / Accepted: 5 July 2021 / Published online: 17 November 2021

Abstract
Innovative IT-enabled health services promise tremendous benefits for customers and service providers alike. Simultaneously, health services by nature process sensitive customer information, and data breaches have become an everyday phenomenon. The challenge that health service providers face is to find effective recovery strategies after data breaches to retain customer trust and loyalty. We theorize and investigate how two widely applied recovery actions (namely apology and compensation) affect customer reactions after a data breach in the specific context of fitness trackers. Drawing on expectation confirmation theory, we argue that the recovery actions derived from practice, apology, and compensation address the assimilation-contrast model's tolerance range and, thus, always lead to satisfaction with the recovery strategy, which positively influences customers' behavior. We employ an experimental investigation and collect data from fitness tracker users during a running event. In the end, we found substantial support for our research model. Health service providers should determine specific customer expectations and align their data breach recovery strategies accordingly.

Keywords Health data breach recovery action · Data breach response strategies · Compensation · Apology · Expectation confirmation theory · Assimilation-contrast model

JEL classification I12

Moderne Gesundheitsdienstleister verarbeiten naturgemäß sensible Nutzerdaten. Da Datenleaks immer häufiger auftreten stellt sich die Frage, welche Strategien nach einem solchen angewendet werden können, um effektiv die Langzeitbeziehungen zu Kund:innen zu stabilisieren. Die Autor:innen untersuchten hierzu die Recovery Strategien “Entschuldigung” und “Kompensation” im Kontext von Fitness Trackern. Die Autoren konnten nachweisen, dass die untersuchten Strategien Kundenzufriedenheit und -Verhalten positive beeinflussen können.

Weitere Informationen unter:

[What to do after a data breach? Examining apology and compensation as response strategies for health service providers (springer.com)]

Masuch, K.; Greve, M; Trang, S. (2020): Please be Silent? Examining the Impact of Data Breach Response Strategies on the Stock Value, Proceedings of the International Conference on Information Systems (ICIS), Hyderabad, India. [VHB 3: A]

Please be Silent?
Examining the Impact of Data Breach Response Strategies on the Stock Value

Completed Research Paper

Kristin Masuch
University of Goettingen
Kristin.masuch@uni-goettingen.de

Maike Greve
University of Goettingen
maike.greve@uni-goettingen.de

Simon Trang
University of Goettingen
strang@uni-goettingen.de

Abstract

Incidents of security breaches have increased and caused immense damage, affecting the stock price. Data breaches are particularly problematic as they have fatal consequences on customer relations. By applying recovery actions after a data breach, a company is able to mitigate these consequences. However, there is a controversy: The recovery actions offered to customers are perceived differently by the company's investors. While customer loyalty can be maintained, the value of the company's stock is damaged. This study examines this controversy through an event study. Real response strategies to data breaches are coded and their effects on investor behavior are examined on the basis of stock value. The results show that apologizing a data breach has harmful effects on investor behavior. The opposite might occur if the response is whitewashed. Further effects can be determined by the affected group and the year of the data breach.

Keywords: Data Breach Recovery Actions, Apology, Whitewash, Impact on Stock Value, Event Study

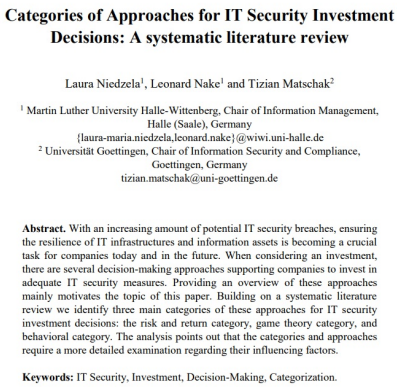
Nach Datenverlusten haben Unternehmen unterschiedlichste Möglichkeiten um die Auswirkungen auf Kundenbeziehungen zu mitigieren. Häufig bietet sich hier allerdings eine Kontroverse, da solche Maßnahmen durch Investoren negativ aufgefasst werden können und somit Aktienpreise und den Marktwert des Unternehmens schmälern können. Die Autor:innen

untersuchen daher den Einfluss möglicher Recovery Strategiem auf Investoren mittels einer Event-Studie. Die Ergebnisse zeigen, dass Entschuldigungen zu negativen Effekten seitens der Investor:innen führen können, während das herunterspielen des Verlusts gegenteilige Effekte hervorrufen kann.

Weitere Informationen unter:

AIS Electronic Library (AISeL) - ICIS 2020 Proceedings: Please be Silent? Examining the Impact of Data Breach Response Strategies on the Stock Value (aisnet.org)

Niedzela, L., Nake, L., Matschak, T. (2022): Categories of Approaches for IT Security Investment Decisions: A systematic literature review, Wirtschaftsinformatik 2022 Proceedings, 4



Categories of Approaches for IT Security Investment Decisions: A systematic literature review

Laura Niedzela[1], Leonard Nake[1] and Tizian Matschak[2]

[1] Martin Luther University Halle-Wittenberg, Chair of Information Management, Halle (Saale), Germany
{laura-maria.niedzela,leonard.nake}@wiwi.uni-halle.de
[2] Universität Goettingen, Chair of Information Security and Compliance, Goettingen, Germany
tizian.matschak@uni-goettingen.de

Abstract. With an increasing amount of potential IT security breaches, ensuring the resilience of IT infrastructures and information assets is becoming a crucial task for companies today and in the future. When considering an investment, there are several decision-making approaches supporting companies to invest in adequate IT security measures. Providing an overview of these approaches mainly motivates the topic of this paper. Building on a systematic literature review we identify three main categories of these approaches for IT security investment decisions: the risk and return category, game theory category, and behavioral category. The analysis points out that the categories and approaches require a more detailed examination regarding their influencing factors.

Keywords: IT Security, Investment, Decision-Making, Categorization.

Im Rahmen zunehmender Relevanz von IT-Sicherheit werden effiziente und sinnvolle Entscheidungen bezüglich der Auswahl von IT-Sicherheitsmaßnahmen immer wichtiger. In der Wissenschaft finden sich unterschiedliche Ansätze aus unterschiedlichen Forschungsbereichen, um diese Entscheidungen zu unterstützen. Mittels einer strukturierten Literaturanalyse konnten die Autoren 3 Kategorien solcher Ansätze untersuchen und somit eine Basis für zukünftige Forschungsvorhaben erstellen. In Zukunft könnten dadurch individuelle Faktoren, die den Entscheidungsfindungsprozess beeinflussen, differenzierter analysiert werden.

Weitere Informationen finden Sie hier.

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

Kontakt aufnehmen

Aktuelle Entwicklungen im Bereich Informationssicherheit

Informationssicherheit auf der Münchener Cyber Sicherheitskonferenz

Auch im Rahmen der Münchener Sicherheitskonferenz (MSC) spielt das Thema Informationssicherheit eine Rolle. Die 8. Münchener Cyber Sicherheitskonferenz (MCSC) fand traditionsgemäß am Tag vor der MSC statt. Internationale Experten diskutierten hier Themen rund um Cybersicherheit und Cyberkrieg. So wurde unteranderem auch über die Gefahren der Versorgungssicherheit der Bürger:innen, welche von Cloud-Systemen ausgehen, diskutiert.

„Die Cloud-Infrastrukturen werden massiv attackiert. Aber diese IT- und die Cyber-Infrastruktur ist wichtig, damit die weltweiten Lieferketten funktionieren, damit wir versorgt werden mit Gütern, sowohl in Deutschland, in Europa, in der ganzen Welt. Da gibt es bereits viele Gefahren.“

Ralf Wintergerst, Vorstandsvorsitzender von Giesecke & Devrient

Aktuelle Angriffe

Log4J

Das BSI hat die IT-Bedrohungslage im Zusammenhang mit den entdeckten Schwachstellen in log4J in einem neusten Update seit dem 17.12.2021 auf Stufe rot gesetzt. Log4j kommt dabei in vielen Java-Anwendungen zum Einsatz und dient der aggregierten Sammlung von Protokolldaten. Bereits in einem früheren Update ist auf GitHub eine Liste von Sicherheitswarnung für Produkte von über 140 Herstellern veröffentlicht worden. Das Aktualisieren der Softwarebibliothek allein reicht dabei als Schwachstellenabdeckung nicht aus. Es wird angenommen, dass durch die Schwachstelle nicht nur weitere Schadsoftware injiziert werden kann, sondern auch vertrauliche Daten offengelegt werden können. Der Hersteller des Schwachstellenscanners GSM hat bereits eine kostenfreie Scan-Konfiguration zur Schwachstellenerkennung bereitgestellt. Das BSI bittet bei Betroffenheit um weitere Informationen aufgrund der sich dynamisch ändernden Informationslage.

Weitere Informationen rund um die Bewertung und Maßnahmen im log4j-Kontext finden Sie unter:

BSI - Log4j

MediamarktSaturn

Im November des vergangenen Jahres wurde der Elektronikhändler MediamarktSaturn Opfer eines Hackerangriffs. Viele Dienstleistungen des Händlers waren daher für ca. eine Woche nicht verfügbar. So konnten Kund:innen unteranderem nicht mittels „Click & Collect“ bestellen oder Finanzierungen im Markt abschließen. Auch die Belegerstellung in den Märkten oder das Bezahlen mittels Gutscheine war vorrübergehend nicht möglich. Die Hacker hatten Berichten Zufolge ein Lösegeld von 50 Millionen Euro gefordert. Vermutet Ursache/Schwachstelle des Angriffs: Phishing.

Hier finden sie weitere Informationen.

Thalia

Am 20. Januar diesen Jahres ist der Onlinebuchhandel Thalia mittels einer Brute-Force-Attacke gehackt worden. Laut Angaben sei über mehrere Stunden hinweg versucht worden, Anmelde- und Passwortkombination von Kundenkonten zu knacken, um gezielt an Kontodaten der Nutzer zu kommen. Dies gelingt mit Erfolg. Laut dem Onlinehändler seien weder Daten der Kunden verändert worden, noch unberechtigte Bestellungen getätigt worden. Der Grund für den erfolgreichen Angriff ist ein fehlendes IPS (Intrusion Prevention System) gewesen. Ein Vorhandensein hätte die Attacke verhindern können. Die Kosten bewegen sich im mittlerem fünfstelligen Bereich.

Für weitere Infos: Trankappe.info, Heise.de

Ausblick und kommende Termine

Nächste Projektschritte

Bis zum nächsten Newsletter sind folgende Ergebnisse zu erwarten:

- Abschluss der Delphi Studie im ProBits Projekt
- Erster Zwischenbericht mit einem Rückblick über das vergangene erste Jahr

Impressum

www.probits.uni-goettingen.de

Georg-August-Universität Göttingen

Lehrstuhl für Informationssicherheit und Compliance
Platz der Göttinger Sieben 5
37073 Göttingen

Vertreten durch:
Prof. Dr. Simon Trang
Platz der Göttinger Sieben 5
37073 Göttingen
probits@uni-goettingen.de

Georg-August-Universität Göttingen
Wilhelmsplatz 1
37073 Göttingen
T 0551 39-0
oeffentlichkeitsarbeit@uni-goettingen.de