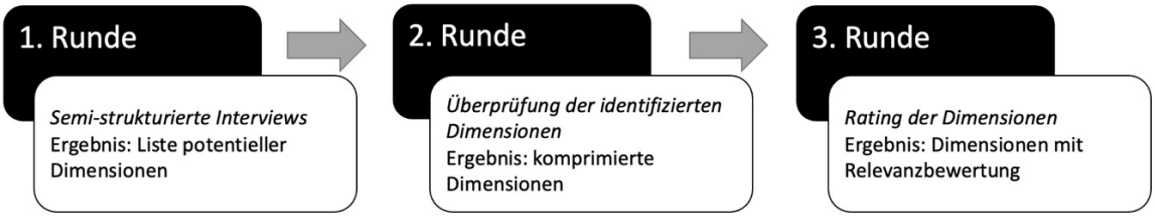
# Newsletter 12/2022

# Projektfortschritt & Aktuelles

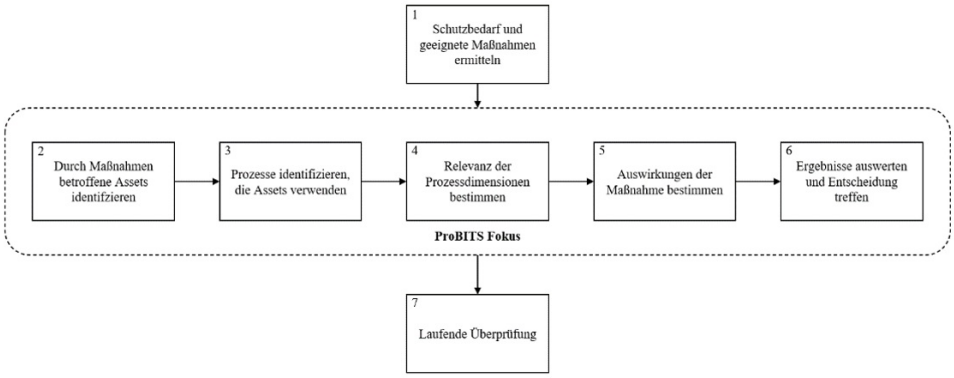
## Abschluss der Delphi Studie

Im vergangenen Newsletter haben wir angekündigt, mit der Durchführung der Delphi-Studie zu beginnen. Heute können wir Ihnen mitteilen, dass die dritte und letzte Iteration kurz vor der Fertigstellung steht. Insgesamt wurden in der Delphi Studie mehr als 25 Unternehmen hinsichtlich potentieller Einflussdimensionen von IT-Sicherheitsmaßnahmen (ITSM) auf Geschäftsprozesse befragt. Dabei wurden in der ersten Interviewrunde zunächst potentielle Prozessdimensionen identifiziert. Anschließend wurden die identifizierten Dimensionen validiert und konsolidiert. Zum aktuellen Zeitpunkt konnten auf diese Weise 29 distinkte Dimension mit mehr als 240 Praxisbeispielen erhoben und definiert werden. Die finale Liste an Dimensionen wird in Kürze an die Projektpartner gesendet, um im Rahmen einer letzten Validierungsrunde die Relevanz der Dimensionen zu bestimmen. Der Ablauf der einzelnen Iterationsrunden verlief wie folgt:




## Entwicklung des Vorgehensmodells

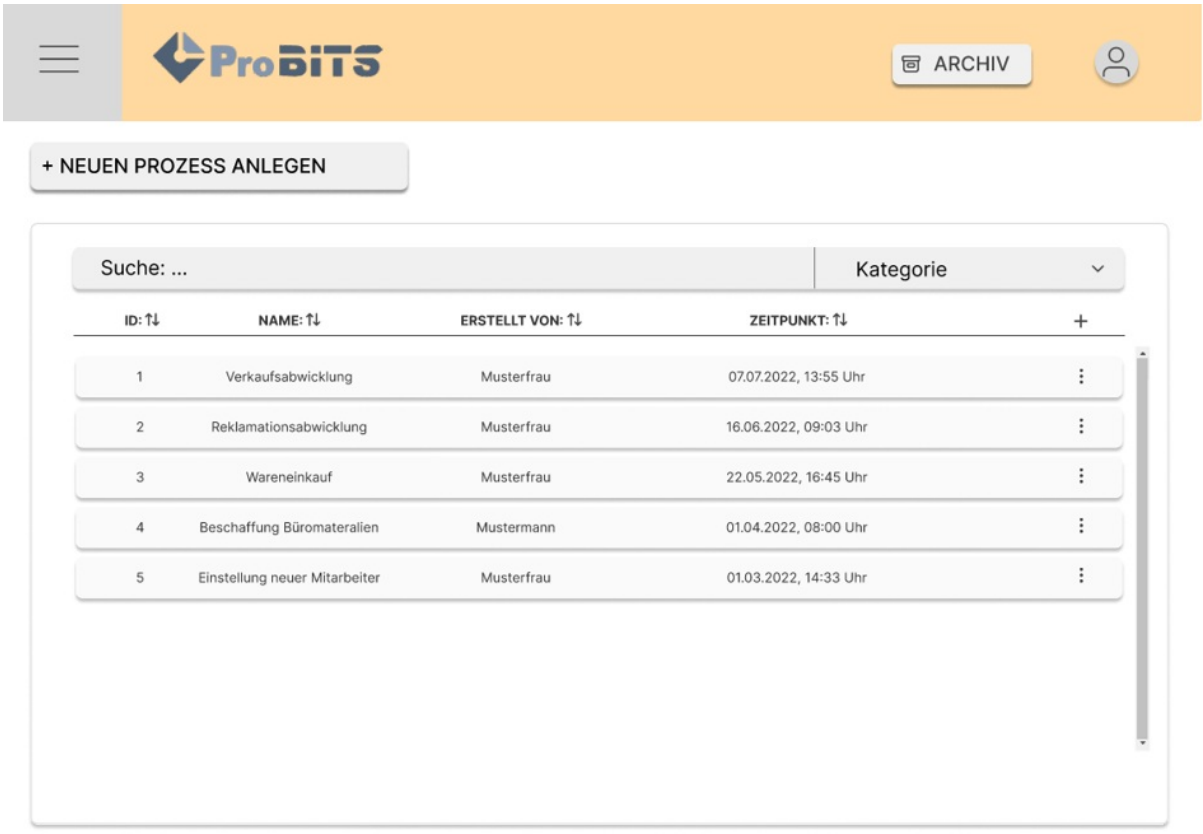
Zusätzlich zur fast vollständigen Delphi-Studie können wir vom fertiggestellten Vorgehensmodell berichten. Das Vorgehensmodell dient als Schablone zur Durchführung einer Bewertung mithilfe der ProBITS-Methode. Es umfasst insgesamt sieben Schritte, wobei Schritt zwei bis sechs die Kernelemente der Methode sind. Das Vorgehensmodell wurde in drei Iterationen entwickelt und anschließend zusammen mit zwei Projektpartnern in zwei Fallstudien validiert.



Um die ProBits-Methode anwenden zu können, müssen im ersten Schritt einige Voraussetzungen erfüllt werden. Zum einen muss zunächst der Schutzbedarf des Unternehmens ermittelt werden und zum anderen müssen potentielle Maßnahmenbündel vorliegen, welche anschließend bewertet werden sollen. Im zweiten Schritt werden dann die von den zuvor ermittelten Maßnahmenbündel betroffenen Assets des Unternehmens identifiziert. Hierzu können sowohl Experten mit IT-Sicherheitserfahrung als auch mit Expertise bzgl. des zugrundeliegenden Prozesses hinzugezogen werden. Im vierten Schritt wird anschließend die Relevanz der einzelnen Prozessdimensionen festgelegt. Hierbei sollte der Fokus auf den individuellen Anforderungen des jeweiligen Unternehmens liegen. Die Methode ist somit auch an das jeweilige Marktumfeld des Unternehmens anpassbar. Im 5. Schritt wird dann der Einfluss der Maßnahmen oder Maßnahmenbündel auf die jeweiligen Prozessdimensionen bewertet. Die Bewertung erfolgt anhand einer Bewertungsskala mit entsprechenden Ausprägungen der Dimensionen. Im letzten Schritt erfolgt dann eine automatische Auswertung der Bewertung. Diese ermöglicht den prozessorientierten Vergleich unterschiedlicher Maßnahmen(-bündel) und soll eine optimale Entscheidung bezüglich der Implementierung von IT-Sicherheitsmaßnahmen unterstützen. Da Sicherheitsmaßnahmen in einem dynmaischen Umfeld implementiert werden und die Anforderungen und Prozesse nicht stets gleichbleiben, muss eine laufende Überprüfung ermöglicht werden, welche sicherstellt, dass die gewählten Maßnahmen auch weiterhin den optimalen Schutz bieten.

## Entwicklung des Prototyps hat begonnen

Ziel des Projektes ist es, die entwickelte ProBITS-Methode zur Bewertung von ITSM durch ein geeignetes IT-Tool zu unterstützen. Nachdem nun das Vorgehensmodell vollständig entwickelt und die Delphi Studie fast abgeschlossen ist, wurden die ersten Schritte hin zur Entwicklung eines Prototyps erfolgreich durchlaufen. Zunächst ist dabei mit der Erhebung technischer und funktionaler Anforderung an das IT-Tool begonnen worden, um anschließend mit dem Entwurf einiger Mockups der Benutzeroberfläche fortzufahren. Eines dieser Mockups ist hier zur Veranschaulichung abgebildet.




Darüber hinaus wurde mit dem Aufbau eines geeigneten Toolstacks sowie mit der Implementierung des Prototyps begonnen. Es ist geplant, eine initiale Version des Prototyps bis Ende dieses Jahres fertig zu stellen. Bis dieser seine finale Version erreicht, wird er kontinuierlich mit unseren Projektpartnern evaluiert.

An diese Stelle möchten wir unseren Projektpartnern der Rezeptprüfstelle Duderstadt GmbH und der msu Solutions GmbH herzlich für Ihre tatkräftige Unterstützung bei der Entwicklung danken.

## „ProBITS in Aktion“ mit Smart Metering

Gemeinsam mit der msu Solutions GmbH (MSU) wurde für das Arbeitspaket „ProBITS in Aktion“ ein aktueller Anwendungsfall aus der Energiewirtschaft im Bereich des Smart Metering entwickelt. Der Ausbau intelligenter Messsysteme (Rollout) ermöglicht eine effiziente Datenübertragung von Energieverbrauch und -erzeugung. Damit stellt das „Smart Metering System“ als Teil der kritischen Infrastruktur einen einmaligen Anwendungsfall für die Bewertung und Einführung von IT-Sicherheitsmaßnahmen dar.
Im Projekt ProBITS werden dabei auch die aktuellen Gesetzesentwicklungen hinsichtlich diesem Anwendungsfalles genau beobachtet. Zum Hintergrund: Im Mai dieses Jahres wurde die Allgemeinverfügung und damit die Grundlage zum verpflichtenden flächendeckenden Rollout der intelligenten Messsysteme gestoppt. Etwa 50 Messtellenbetreiber hatten gegen die technische Möglichkeit zur Umsetzung des flächendeckenden Ausbaus Widerspruch erhoben, woraufhin die Allgemeinverfügung zurückgenommen und der verpflichtende Rollout vorerst gestoppt ist (BSI - Marktanalyse (bund.de)).
Da Smart Metering in der energiewirtschaftlichen Praxis dennoch eingesetzt und intelligente Messysteme bereits vielfach verbaut sind und weiterhin werden, werden gemeinsam mit der MSU anhand des Smart-Metering-Prozesses das ProBITS-Entscheidungsmodell, Vorgehensmodell und IT-Tool entwickelt und getestet.

## Mittelstand-Digital Kongress 2022

Am 19. Oktober 2022 war Tizian Matschak im Rahmen des Projektes ProBITS zu Besuch auf dem Mittelstand-Digital Kongress 2022 in Berlin. Unter dem Motto *„Unternehmen nachhaltig und sicher ausrichten“* standen zentrale Themen des deutschen Mittelstands auf der Tagesordnung. Neben einer Keynote zum Thema *„Unternehmerische Verantwortung auf dem Transformationspfad“* von Karin Hübner mit anschließender Diskussionsrunde und einigen anderen Vorträgen war ausreichend Zeit zur Vernetzung mit anderen Kolleg:innen geboten und es konnten einige Schnitt- und Anknüpfungspunkte bezüglich der ProBITS-Idee besprochen werden.

Weiter Informationen: www.mittelstand-digital.de

Besonders ist dabei der Sec-O-Mat der Transferstelle IT-Sicherheit im Mittelstand (TISiM) in Erinnerung geblieben. Angelehnt an den bekannten Wahl-O-Mat, hilft der Sec-O-Mat bei der Erstellung eines individuellen Aktionsplans hinsichtlich konkreter Sicherheitsbedarfe und Vorschlägen zur Umsetzung geeigneter Maßnahmen. Der Sec-O-Mat sticht besonders durch seine einfache Handhabung hervor, die auch für ‚Sicherheits-Laien‘ verständlich ist.

Weitere Informationen: www.sec-o-mat.de/

Die TISiM stellte zudem ihr Projekt **mIT Sicherheit ausbilden** vor. Es unterstützt Ausbildungsverantwortliche dabei, IT-Sicherheit von Anfang an mit in die Ausbildungsinhalte einfließen zu lassen. Hierzu wurde eine eigene, fünf-schrittige Transfermethode sowie eine Lernplattform für Ausbildungsverantwortliche entwickelt.

Weiter Informationen: www.tisim.de

Zuletzt soll hier das **BAKGame** vorgestellt werden. Hierbei handelt es sich um ein Projekt mit dem Ziel Lernspiele, die zielgruppengerecht und realitätsnah Kompetenzen und Fähigkeiten für die Thematik IT-Sicherheit vermitteln zu erforschen, entwickeln und evaluieren. Bisher wurden drei vielversprechend wirkende Spiele zu den Themen Phishing, Passwörterwahl und Security

Entscheidungen entwickelt, welche auf der Projekt-Webseite auch schon getestet werden können.

Weitere Informationen: www.bakgame.de/

## International Conference on Information Systems

Vom 09. bis zum 14.12.2022 fand die jährliche International Conference on Information Systems in Kopenhagen statt, auf welcher ausgewählte Projektergebnisse vorgestellt wurden. Wir danken allen Anwesenden für ihr wertvolles Feedback und die interessante Konferenz.

Aktuelle ProBITS News

---

# Aktuelles aus der Forschung

**Matschak, T; Nastjuk, I; Kühnel, S; Trang, S (2022): Exploring the Dark Side of IT Security: Delphi Study on Business Processes' Influencing Factors (WISP 2022), Copenhagen, Denmark**

In der bestehenden wissenschaftlichen Literatur wurden vor allem die primären Ziele von IT-Sicherheitsmaßnahmen (ITSM) untersucht. Diese sind vornehmlich die Gewährleistung der Schutzziele Vertraulichkeit, Integrität und Verfügbarkeit, um so das Risiko eine IT-Sicherheitsvorfalls zu reduzieren. Aktuelle Forschung wie auch unsere Beobachtungen lassen jedoch den Schluss zu, dass ITSM auch sekundäre (unbeabsichtigte) Auswirkungen haben können, die bisher nicht ausreichend untersucht wurden. So können beiepilsweise ITSM Geschäftsprozesse verlangsamen oder deren Komplexität steigern. Durch die Anwendung der Delphi-Methode und Interviews mit 28 Praktiker*innen, wurden 30 Dimensionen identifiziert, die abbilden, wie ITSM Geschäftsprozesse beeinflussen können. Die Definition und das Verständnis dieser Mechanismen hat das Potenzial, die Kosten-Nutzen-Bewertung von IT-Sicherheitsinvestitionen zu verbessern und somit IT-Sicherheitsbeauftragten sowie Managern bei der Entscheidungsfindung zu unterstützen.

**Rampold, F.; Schütz, F.; Masuch, K.; Köpfer, P.; Warwas, J. (2022): Are you aware of your competencies? The potentials of competence research to design effective SETA programs (ECIS 2022), Timisoara, Romania [VHB 3: B]**

# ARE YOU AWARE OF YOUR COMPETENCIES? – THE POTENTIALS OF COMPETENCE RESEARCH TO DESIGN EFFECTIVE SETA PROGRAMS

*Research Paper*

Rampold, Florian, University of Goettingen, Goettingen, Germany, florian.rampold@uni-goettingen.de

Schütz, Florian, University of Goettingen, Goettingen, Germany, florian.schuetz@uni-goettingen.de

Masuch, Kristin, University of Goettingen, Goettingen, Germany, kristin.masuch@wiwi.uni-goettingen.de

Köpfer, Patricia, University of Hohenheim, Stuttgart, Germany, patricia.koepfer@uni-hohenheim.de

Warwas, Julia, University of Hohenheim, Stuttgart, Germany, julia.warwas@uni-hohenheim.de

## Abstract

*Since the late 1990s, security education training and awareness (SETA) programs have become commonplace. Despite extensive research into the effective design of such programs and factors influencing compliance behavior, SETA programs tend not to be as effective as they should be. In order to tailor learning content as closely as possible to individual needs, vocational education relies on the modeling and measurement of competencies. We argue that this existing knowledge can be transferred to the information security domain. Therefore, we introduce a competence model from vocational education and consider it in the context of the information security domain. Subsequently, we conduct a structured literature review on conceptualization and effective SETA design and investigate to what extent the competence dimensions from vocational education are already considered in the SETA literature. Our results indicate that competence research can make an important contribution to adapting SETA programs to individual situational actions.*

*Keywords: SETA, Security Education Training and Awareness, Competence Model, Vocational Education*

Seit den späten 1990er Jahren sind Programme zur Schulung und Sensibilisierung für Sicherheitsfragen (SETA) alltäglich geworden. Trotz umfangreicher Forschungsarbeiten zur effektiven Gestaltung solcher Programme und zu den Faktoren, die das Compliance-Verhalten beeinflussen, sind SETA-Programme in der Regel nicht so effektiv, wie sie sein sollten.
Um die Lerninhalte so genau wie möglich auf die individuellen Bedürfnisse zuzuschneiden, stützt sich die Domäne der beruflichen Bildung auf die Modellierung und Messung von Kompetenzen. Das Paper argumentiert, dass dieses vorhandene Wissen auf den Bereich der Informationssicherheit übertragen werden kann. Daher wird ein Kompetenzmodell aus der beruflichen Bildung vorgestellt und im Kontext der Informationssicherheitsdomäne betrachtet. Eine anschließende, strukturierte Literaturrecherche zur Konzeptualisierung und effektiven Gestaltung von SETA Programmen untersucht, inwieweit die Kompetenzdimensionen aus der beruflichen Bildung in der SETA-Literatur bereits berücksichtigt werden. Die Ergebnisse zeigen, dass die Kompetenzforschung einen wichtigen Beitrag zur Anpassung von SETA-Programmen an individuelles situatives Handeln leisten kann.

Weitere Informationen unter:

[Are you aware of your competencies? The potentials of competence research to design effective SETA programs (ECIS 2022)]

**Kuehnel, Stephan; Sackmann, Stefan; Damarosky, Johannes; Boehmer, Martin (2022): EconBPC: A Tool for Activity-based Monetary Assessment and Visualization of Security and Compliance Measures in Business Processes, 20th International Conference on Business Process Management (BPM 2022), Proceedings of the Best**

**Dissertation Award, Doctoral Consortium, and demonstration & Resources Track, CEUR-WS Vol. 3216, Münster, Germany, pp. 127-131.**

# EconBPC: A Tool for Activity-based Monetary Assessment and Visualization of Security and Compliance Measures in Business Processes

Stephan Kuehnel [1], Stefan Sackmann [1], Johannes Damarowsky [1], and Martin Boehmer [1]

[1] *Martin Luther University Halle-Wittenberg, Universitaetsring 3, 06108 Halle (Saale), Germany*

**Abstract**

In this paper, we present the four-stage concept, implementation, application, and 2-stage evaluation of the tool EconBPC. EconBPC is a software artifact that emerged from a design science research initiative on the use of extensible event streams (XES). It was created to take a first step towards an automated activity-based monetary assessment of security and compliance measures in business processes and their addressee-oriented representation in a compliance view. For this purpose, EconBPC provides users with annotation features for XES and compliance processes, enables the storage of annotated log files, and the comparison of expenses for security and compliance activities with costs from associated regulatory breaches.

**Keywords**

Business Processes Compliance, Process Mining, Annotation, Cost, XES, event log, log file

Vor dem Hintergrund des zunehmenden Umfangs an Regulatorik dem sich Unternehmen ausgesetzt sehen, ist Prozess-Compliance ein zunehmend komplexes wie auch kostenintensives Thema. Die ökonomische Analyse zur Gewährleistung einer möglichst effizienten Sicherstellung von Prozess-Compliance ist dabei aufgrund von häufig großen Datenmengen, die analysiert werden müssen, keine leichte Aufgabe. EconBPC ist ein Software-Artefakt, welches zur Lösung dieses Problems entwickelt wurde und einen ersten Schritt in Richtung einer automatisierten aktivitätsbasierten monetären Bewertung von Sicherheits- und Compliance-Maßnahmen in Geschäftsprozessen bietet. Zusätzlich ermöglicht es eine Adressaten orientierte Darstellung dieser Maßnahmen und Prozesse in einer speziellen Compliance-Sicht. Diese Sicht ermöglicht den effektiven Vergleich von Kosten, die durch Sicherheits- und Compliance-Aktivitäten entstehen mit solchen Kosten, die durch Verstöße gegen die Regulatorik entstehen.

# EconBPC: A Tool for Activity-based Monetary Assessment and Visualization of Security and Compliance Measures in Business Processes

Kuehnel, Stephan[1]; Sackmann, Stefan[1]; Damarowsky, Johannes[1]; and Boehmer, Martin[1]

[1] Martin Luther University Halle-Wittenberg, Universitaetsring 3, 06108 Halle (Saale), Germany

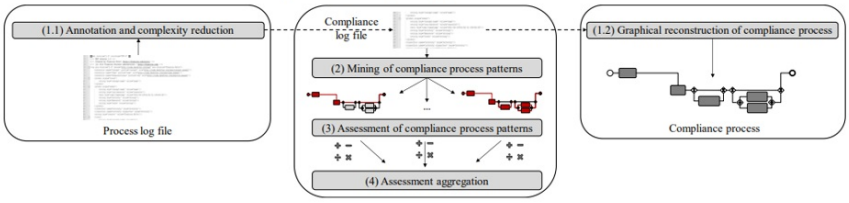
## Motivation, Problem Description, and Goal

- Current legislation on the protection of personal data requires the consideration of economic criteria when introducing compliance and security measures in business processes (see, e.g., Article 32 (1) of the European Union's General Data Protection Regulation (EU GDPR)).
- The economic assessment of business process compliance (BPC) is a complex task for process owners, especially when data from large log files have to be analyzed. Studies from the field of decision making theory suggest the use of software artifacts to support such complex tasks in order to enable a reduction of the cognitive effort for the end user [1, 2], e.g., by enabling special security and compliance views on business processes or by increasingly automating necessary calculations in large process models [3, 4].

- **Goal:** Demonstrate EconBPC, a tool based on Extensible Event Streams (XES) that (1) visualizes security and compliance measures of business processes in a separate view and (2) represents a first step towards an automated economic assessment of BPC, accounting for monetary cost and benefit aspects.

## Concept and Software Architecture

**Figure 1**: Conceptual approach of EconBPC




(1.1) Data can be stored in log files that further specify the activities performed (so-called events) [5]. If the available log file does not yet contain data about the event type (business/compliance event), costs, or reliabilities of compliance events, these must be annotated.
This is followed by a complexity reduction. All events that are not of the "compliance" type are removed from the log file. The resulting so-called compliance log file only contains data required for the monetary assessment of BPC, which increases the efficiency of subsequent calculations.

(1.2) A compliance process can be visualized based on the compliance log file. Such a visualization provides an overview of security/compliance activities and can be used as a basis for presenting calculation results graphically in a way appropriate to the target audience.

(2) Each executed instance of a business process consists of a finite set of events and is referred to as a trace according to the XES standard [6]. A compliance log file contains only compliance traces, i.e. the executed instances of a compliance process. First, the event sequences of all compliance traces are analyzed and a list of all those sequences differing in their order is created. Each entry in this list is a unique tuple that represents one of a finite number of pathways through a compliance process and is referred to as a compliance process pattern. Second, the relative frequency of occurrence is determined for each pattern.

(3) Using our computational approach originating from prior work [7], we determine the costs and reliabilities of the compliance process patterns.

(4) As part of assessment aggregation, expected costs and expected reliabilities of the entire compliance process are calculated. For this purpose, we use the costs and reliabilities of the compliance process patterns and weight them with the frequencies of occurrence determined in step (2). At the highest level of aggregation, the expected costs of the compliance process can be compared with its benefits, which can be represented in terms of the monetary damage prevented, e.g., by avoiding regulatory breaches [7].

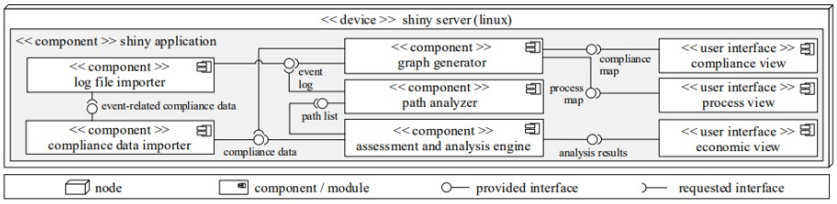



**Figure 2**: Software architecture of EconBPC, represented as UML component diagram

## Maturity

- The tool was tested with an XES dataset containing 105 synthetic instances of a credit application process.
- The tool was tested by 12 experts from the field of IT governance, risk, and compliance in think-aloud sessions on case studies (see [8]).
- The design principles of EconBPC were evaluated by means of questionnaires in terms of perceived usefulness, comprehensibility, traceability, and practicability (see [8]).

## References

[1] W. Wang, I. Benbasat, Interactive Decision Aids for Consumer Decision Making in E-Commerce: The Influence of Perceived Strategy Restrictiveness, MIS Quarterly 33 (2009), pp. 293-320.
[2] H. Meth, B. Mueller, A. Maedche, Designing a Requirement Mining System, JAIS 16(9), 2015, pp. 799–837, DOI: 10.17705/1jais.00408
[3] N. Adams, A. Augusto, M.J. Davern, M. La Rosa, On the Role of Process Mining in Business Process Compliance, SSRN Journal (2022). DOI: 10.2139/ssrn.4081558.
[4] A.J. Varela-Vaca, L. Parody, R.M. Gasca, M.T. Gomez-Lopez, Automatic Verification and Diagnosis of Security Risk Assessments in Business Process Models, IEEE Access 7, 2019, pp. 26448–26465, DOI: 10.1109/ACCESS.2019.2901408.
[5] M.T. Wynn, W.Z. Low, t. A.H.M. Hofstede, W.E. Nauta, A framework for cost-aware process management: Journal of Universal Computer Science 20, 2014, pp. 406–430.
[6] C.W. Günther, E. Verbeek, XES Standard Definition 2.0, second ed., Eindhoven, 2014.
[7] S. Kuehnel, A. Zasada, An Approach Toward the Economic Assessment of Business Process Compliance, in: Advances in Conceptual Modeling, ER 2018, Proceedings, Springer Cham, 2018, LNCS vol 11158. pp. 228–238, DOI: 10.1007/978-3-030-01391-2_28
[8] S. Kuehnel, S. Trang, S. Lindner, Conceptualization, Design, and Implementation of EconBPC – A Software Artifact for the Economic Analysis of Business Process Compliance, in: Conceptual Modeling, ER 2019, Proceedings, Springer Cham, 2019, LNCS vol 11788., pp. 378–386, DOI: 10.1007/978-3-030-33223-5_31

20th International Conference on Business Process Management (BPM 2022)
Demo Track, Muenster, Germany, September 11th to 16th, 2022

MARTIN LUTHER UNIVERSITY
HALLE-WITTENBERG

Weiter Informationen unter:

[EconBPC: A Tool for Activity-based Monetary Assessment and Visualization of Security and Compliance Measures in Business Processes, 20th International Conference on Business Process Management (BPM 2022)]

[Webseite des Lehrstuhls]

**Hengstler, Sebastian; Pryazhnykova, Natalya; and Kühnel, Stephan, "How Employees Learn Information Security Policy Compliance Behavior: Toward a Social Learning Perspective" (2022). ECIS 2022 Research Papers. 85.**

# HOW EMPLOYEES LEARN INFORMATION SECURITY POLICY COMPLIANCE BEHAVIOR: TOWARD A SOCIAL LEARNING PERSPECTIVE

*Research Paper*

Sebastian Hengstler, University of Goettingen, Goettingen, Germany, s.hengstler@stud.uni-goettingen.de

Natalya Pryazhnykova, University of Goettingen, Goettingen, Germany, pryazhnykova@gmail.com

Stephan Kuehnel, Martin Luther University Halle-Wittenberg, Halle (Saale), Germany, stephan.kuehnel@wiwi.uni-halle.de

## Abstract

*Information security attacks typically exploit the weakest link in the chain, which is in most cases is the IT end user at the workplace. While great strides have been made in understanding and explaining information security behavior, little is known about how such behavior is acquired by individuals in the first place. This research approaches the phenomenon through the lens of social learning theory. We argue that a new employee's behavior is initially learned through differential associations within the social network, rather than through knowledge of formal policies and associated sanctions. We used a scenario-based experimental approach and collected data from new employees with five years or less of work experience. Our results show that employee's behavior changes over time. Reinforcement through sanctions becomes more important in the maintenance phase, while imitation of others becomes less relevant.*

*Keywords: Social Learning; Information Security; Compliance Behavior, Information Security Policy Compliance.*

Angriffe auf die Informationssicherheit nutzen in der Regel das schwächste Glied in der Sicherheitskette aus, was in den meisten Fällen der IT-Endbenutzer am Arbeitsplatz ist. Obwohl Unternehmen vermehrt in das Verhalten ihrer Mitarbeiter investieren, ist nur wenig darüber bekannt, wie sich Endbenutzer ein solches Verhalten überhaupt aneignen. Die vorliegende Studie nähert sich dem Phänomen durch die Brille der Theorie des sozialen Lernens. Es wird argumentiert, dass das Verhalten eines neuen Mitarbeiters zunächst durch unterschiedliche Assoziationen innerhalb des sozialen Netzwerks erlernt wird, und nicht durch die Kenntnis formaler Richtlinien und damit verbundener Sanktionen. Mit Hilfe eines Szenario-basierten, experimentellen Ansatzes konnte gezeigt werden, dass sich das Verhalten der Mitarbeiter im Laufe der Zeit ändert. Die Verstärkung durch Sanktionen wird in der Erhaltungsphase wichtiger, während die Nachahmung anderer weniger relevant wird.

Weiter Informationen unter:

How Employees Learn Information Security Policy Compliance Behavior: Toward a Social Learning Perspective

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

Kontakt aufnehmen

# Aktuelle Entwicklungen im Bereich Informationssicherheit

## Chefwechsel beim BSI

Am 18. Oktober 2022 hat Innenministerin Nancy Faeser den Präsidenten des Bundesamtes für Sicherheit in der Informationsverarbeitung Arne Schönbohm freigestellt. Schönbohm werden enge Beziehungen zum Verein „Cyber-Sicherheitsrat Deutschland e.V.“ und dessen Präsidenten Hans-Wilhelm Dünn vorgeworfen. Sowohl der Verein als auch Dünn pflegen dabei anscheinend zu kritisierende Beziehungen in die Richtung Russlands.

Quelle: www.spiegel.de

## Fehlerhafte Serverkonfiguration bei Microsoft

Am 19. Oktober 2022 bestätigte Microsoft die fehlerhafte Konfiguration eines Servers. Die Schwachstelle wurde am 24. September 2022 durch Forscher des Unternehmens SOCRadar aufgedeckt. Wie die Computer Bild berichtet, waren Daten von ca. 65.000 Geschäftskunden im Umfang von fast 2,4 Terrabyte frei zugänglich. Zu den Daten gehören E-Mails, Kontaktdaten sowie weitere Dateien.

Quellen: www.computerbild.de; www.microsoft.com

---

# Ausblick und kommende Termine

### Nächste Projektschritte

In den kommenden Wochen ist es unser Hauptziel, die Implementierung des Prototyps abzuschließen und diesen zusammen mit unseren Praxispartnern ausgiebig zu testen. Wir hoffen, Ihnen im nächsten Newsletter 2023 die entsprechenden Ergebnisse vorstellen zu können.

### Kommende Termine

- 13.03. - 15.03.2023 Nationale Konferenz IT-Sicherheitsforschung - Die digital vernetzte Gesellschaft stärken

---

## Das Gesamte Team wünscht eine Frohe Weihnachtszeit!

## 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