Serious Games für KMU im produzierenden Gewerbe: Social Engineering und Security Risk Management

Für das Projekt
»Mittelstand 4.0-Kompetenzzentrum Stuttgart«



Mittelstand 4.0
Kompetenzzentrum
Stuttgart

#digitalinBW

Im Auftrag des FZI Forschungszentrum Informatik
entwickelt von

Technische
Hochschule
Wildau
Technical University
of Applied Sciences

Margit Scholl (Hrsg.)

Serious Games für KMU im produzierenden Gewerbe: Social Engineering und Security Risk Management

Für das Projekt
„Mittelstand 4.0-Kompetenzzentrum Stuttgart“

Bibliografische Informationen der Deutschen Nationalbibliothek

Die Deutsche Nationalbibliothek verzeichnet diese Publikation in der Deutschen Nationalbibliografie; detaillierte bibliografische Daten sind im Internet über http://dnb.d-nb.de abrufbar.

Lektorat: Hubertus von Tippelskirch

Copyright © Margit Scholl 2021

Alle Rechte, auch das des auszugsweisen Nachdruckes, der auszugsweisen oder vollständigen Wiedergabe, der Speicherung in Datenverarbeitungsanlagen und der Übersetzung, vorbehalten. Dies gilt auch für die Spielematerialien.

März 2021

Printed in Germany.

ISBN 978-3-9819225-2-3

Projektdokumentation

Serious Games für KMU im produzierenden Gewerbe: Social Engineering und Security Risk Management

Für das Projekt
Mittelstand 4.0-Kompetenzzentrum Stuttgart

Projektlaufzeit 01.04.2020 - 31.03.2021

Gube, Stefanie

Scholl, Margit (Prof. Dr.)

Walch, Marie Christin

Koppatz, Peter

Pokoyski, Dietmar

Ein Projekt der Technischen Hochschule Wildau
im Auftrag des FZI Forschungszentrum Informatik

Technische Hochschule Wildau
Technical University of Applied Sciences
WILDAU

FZI

Mittelstand 4.0
Kompetenzzentrum
Stuttgart

#digitalinBW

Mittelstand-Digital

Das Mittelstand 4.0-Kompetenzzentrum Stuttgart gehört zu Mittelstand-Digital. Mittelstand-Digital informiert kleine und mittlere Unternehmen über die Chancen und Herausforderungen der Digitalisierung. Die geförderten Kompetenzzentren helfen mit Expertenwissen, Demonstrationszentren, Best-Practice-Beispielen sowie Netzwerken, die dem Erfahrungsaustausch dienen. Das Bundesministerium für Wirtschaft und Energie ermöglicht die kostenfreie Nutzung aller Angebote von Mittelstand-Digital. Weitere Informationen finden Sie unter www.mittelstand-digital.de

Gefördert durch:

Bundesministerium für Wirtschaft und Energie

aufgrund eines Beschlusses des Deutschen Bundestages

Inhalt

Abkürzungsverzeichnis ..... **III**

Abbildungsverzeichnis ..... **V**

Kurzdarstellung **1**

1 Ausgangssituation **3**

1.1 Social Engineering 5

1.2 Security Risk Management 6

2 Zielstellung des Projektes **7**

3 Methodische Grundlagen **8**

3.1 Sensibilisierung & Awareness 8

3.2 Analog & Digital 9

3.3 Lernmethoden 9

4 Spielebasierte Lernszenarien **11**

4.1 Social Engineering Theater (SET) 13

4.1.1 SET | Prolog und Epilog 14

4.1.2 SET | Sketch 15

4.1.3 SET | Regie 17

4.1.4 SET | Backstage 21

4.2 Security Risk Roulette 23

5 Tests und Online-Workshops **29**

5.1 Tests 29

5.2 Online-Workshops 32

5.2.1 Technische Einführung Webex 34

5.2.2 Social Engineering Theater 34

5.2.3 Security Risk Roulette 36

6 Bekanntmachung des Projektes und der Projektergebnisse 38

6.1 Öffentlichkeitsarbeit 38

6.2 Wissenschaftliche Konferenzen und Publikationen 39

7 Ausblick 40

Literatur VI

Projektmitarbeitende VII

Anhang VIII

Abkürzungsverzeichnis

ALARM	Awareness Labor KMU
BAköV	Bundesakademie für öffentliche Verwaltung
BMWi	Bundesministerium für Wirtschaft und Energie
BSI	Bundesamt für Sicherheit in der Informationstechnik
CICE	Canada International Conference on Education
ECIE	European Conference on Innovation and Entrepreneurship
ExL	Experiential Learning
FGS	Forschungsgruppe Scholl
FZI	Forschungszentrum Informatik
GBL	Game-based Learning
IEC	International Electrotechnical Commission
IMCIC	Complexity, Informatics and Cybernetics
IS	Informationssicherheit/Information Security
ISA	Information Security Awareness
ISAT	Information Security Awareness-Training
ISO	International Organization for Standardization
IT	Informationstechnik
KMU	Kleinstunternehmen, kleine und mittlere Unternehmen
LS	Lernszenario/Lernszenarien
MAZ	Märkische Allgemeine
RM	Risk Management
SE	Social Engineering

SecAware4job	Informationssicherheit für den Berufseinstieg
SET	Social Engineering Theater
SME	Small and medium-sized enterprise
SRM	Security Risk Management
SRR	Security Risk Roulette
TH Wildau	Technische Hohschule Wildau
TN	Teilnehmende
USA	United States of America
ZIT-BB	Brandenburgischer IT-Dienstleister

Abbildungsverzeichnis

Abbildung 1: Definition KMU 5

Abbildung 2: Projektphasen 11

Abbildung 3: SET | Lernstationen 14

Abbildung 4: SET | Prolog 15

Abbildung 5: SET | Sketch Beispiel 16

Abbildung 6: SET | Regie – Maximale Vertiefung der Handlungsstränge 17

Abbildung 7: SET | Regie – Zeitleiste mit Sprungmarken 18

Abbildung 8: SET | Regie – Verfremdung ASCII Art 19

Abbildung 9: SET | Regie – Verfremdung mit Zeichentrickfilter ohne Farbe 19

Abbildung 10: SET | Regie – Ausschnitt Story Board 20

Abbildung 11: SET | Regie – Finalversion 20

Abbildung 12: SET | Backstage – Zuordnungsprozess in der ersten Version 21

Abbildung 13: SET | Backstage – Beispiel Banküberfall 22

Abbildung 14: SRR | Aufbau 25

Abbildung 15: SRR | Cybermoney 27

Abbildung 16: SET | Backstage – Sequenzdiagramm mit Akteuren/Objekten 30

Abbildung 17: SET | Backstage – vollständiges Sequenzdiagramm 31

Abbildung 18: SET | Sketch – Aufbau Online-Workshop 35

Abbildung 19: SRR | Online-Workshop Beispielfolie 37

Kurzdarstellung

Mit fortschreitender Digitalisierung steigt automatisch das Risiko, Opfer von Cyberattacken zu werden. Nicht zuletzt sind kleine und mittlere Unternehmen (KMU) aufgrund begrenzter Ressourcen besonders gefährdet. Umso präsenter zeigt sich die Problematik in der COVID-19-Pandemie. Dies betont die Bedeutsamkeit von Informationssicherheit (IS). Damit der Faktor Mensch als Stärke und nicht als Schwäche angesehen wird, sind entsprechende Sensibilisierungsmaßnahmen erforderlich.

Unsere Erfahrungen aus anderen Projekten und die psychologisch-basierte Forschung zur betrieblichen Information Security Awareness (ISA) zeigen, dass Sensibilisierungsmaßnahmen eine emotionale Identifikation und interaktive Einbindung der Teilnehmenden erfordert. Eine Möglichkeit Mitarbeitende zu motivieren, sich emotional mit dem Thema IS auseinanderzusetzen und ihr Verhalten entsprechend zu verändern, bietet die Sensibilisierung mittels Learning (GBL). Um Themen der IS spielbar zu gestalten, müssen diese in ihrer Komplexität reduziert werden. Um den Nutzen für Mitarbeitende zu verdeutlichen, sollten sich die Themen dabei in ihren Alltagssituationen widerspiegeln und so zum diskursiven Erfahrungsaustausch anregen.

Im Rahmen des Projektes „Mittelstand 4.0-Kompetenzzentrum Stuttgart“, das vom Bundesministerium für Wirtschaft und Energie (BMWi) gefördert wird, wurde die Technische Hochschule Wildau (TH Wildau) vom FZI Forschungszentrum Informatik (FZI) beauftragt zwei analoge erlebnisorientierte Lernszenarien zu konzipieren und zu entwickeln. Im Zeitraum April 2020 bis März 2021 wurde die Konzeption und Entwicklung der beiden Szenarien zu den Themen Social Engineering und Security Risk Management für KMU des produzierenden Gewerbes umgesetzt.

Der gesamte Prozess der Entwicklung, von der ersten Idee, über das Konzept, zu den Prototypen bis hin zum Testen und Anpassen, wurde von den COVID-19-Maßnahmen maßgeblich beeinflusst und stellte eine besondere Herausforderung dar. Diese Entwicklung war zum Zeitpunkt des Projektauftrages nicht absehbar. Statt der geplanten Kreativworkshops dienten zwei Umfragen mit dem FZI und der Arbeitsgruppe IT-Sicherheit Grundlage für die Entwicklung der Szenarien (siehe Anhang VII-2 bis VII-24). Dies bedeutete einen nicht eingeplanten Mehraufwand.

Das Lernszenario zum Thema Social Engineering basiert auf der Idee eines im Projekt „Informationssicherheit für den Berufseinstieg (SecAware4job)“ entwickelten Rollenspiels. Daraus entstanden drei Lernstationen, die den Perspektivwechsel zwischen Betroffenen und Social Engineers ermöglichen. Das komplette Szenario nennt sich »Social Engineering Theater (SET)«.

»Security Risk Roulette (SRR)« wurde in Kooperation mit dem Projektpartner known_sense entwickelt und greift Elemente des populären Glücksspiels Roulette auf. Der Fokus liegt auf der Risikoeinschätzung und -bewertung mithilfe einer Risikomatrix sowie den Risikobehandlungsoptionen Akzeptanz, Reduktion, Vermeidung und Transfer.

Zur Ergänzung und Vervollständigung der analogen Lernszenarien wurden zwei digitale Ergänzungen konzipiert und programmiert, die über die URL https://diz.wildau.biz/set/regie/index.html und https://diz.wildau.biz/roulette/index.html abgerufen und kostenfrei genutzt werden können.

Kleinere Vor-Ort-Tests wurden mit Auszubildenden und Studierenden unter Einhaltung der COVID-19-Richtlinien durchgeführt. Die geplanten Vor-Ort-Workshops zur Erprobung der Lernszenarien konnten jedoch nicht stattfinden. Um Feedback für die Finalisierung beider Lernszenarien zu erhalten, wurde die Durchführung beider Lernszenarien online-kompatibel umgestaltet, indem inhaltliche Teile modifiziert wurden. Der Workshop zu dem Szenario SET wurde als Hybrid-Variante gestaltet, indem die vor Ort befindlichen Moderatoren von den online zugeschalteten Teilnehmenden angewiesen wurden, Aktionen auszuführen. Der Workshop zu SRR fand dagegen als reines Online-Format statt. Die erfolgreiche Durchführung beider zeigt die Möglichkeit, dass die Spielemechanik von analogen Lernszenarien durchaus digital vermittelt und getestet werden kann. Für das Projektteam entstand dadurch ein nicht einkalkulierter Mehraufwand.

Die Erfahrungen aus diesem Projekt fließen in das neue dreijährige Projekt „Awareness Labor KMU (ALARM) Informationssicherheit“ der FGS der TH Wildau ein, das vom BMWi gefördert wird und seit dem 1. Oktober 2020 läuft.

1 Ausgangssituation

Es besteht kein Zweifel, dass IS für alle Organisationen von zentraler Bedeutung ist und damit ein wichtiges Thema für alle Mitarbeitenden sein sollte. In einer Studie aus dem Jahr 2017 halten zwei Drittel der befragten KMU IT-Sicherheit für sehr wichtig (Hillebrand et al. 2017). Das Risiko, selbst Opfer von Cyberangriffen oder Datenklau zu werden, wird jedoch laut einer von Ernst & Young 2019 durchgeführten Umfrage (Meseke & Kuhlee 2019:7) häufig noch für das eigene Unternehmen unterschätzt. Dies gilt insbesondere für kleine Unternehmen und könnte erklären, warum nur 20 Prozent der KMU bereits IT-Sicherheitsanalysen durchgeführt haben (Hillebrand et al. 2017), obwohl sie mit zum Teil dramatischen Konsequenzen rechnen müssen (Dreißigacker, von Skarczinsik & Wollinger 2020:141). Eine weitere Problematik ist, dass sich Mitarbeitenden in Bezug auf IS nicht immer so verhalten, wie sie es sollen (Aytes & Terry 2004).

Die bestehenden gesetzlichen und regulatorischen Vorgaben zum Sicherheitsbewusstsein sind oft nur für große Unternehmen verbindlich oder, wie im Fall des IT-Sicherheitsgesetzes, abhängig von der jeweiligen Branche (Schmidt, Gondolf & Haufs-Brusberg 2018). Gerade für kleine Unternehmen übersteigen Managementsysteme wie die ISO/IEC-Famile 2700x oder die angepassten deutschen BSI-Standards 200-x ihre vorhandenen Ressourcen (Marmulla 2020). Des Weiteren wird vorwiegend in IT-Technik investiert und gleichzeitig der Faktor Mensch nicht ausreichend beachtet (Luo et al. 2011:1). Dies ist besonders in Hinblick auf den Umstand bedenklich, dass Menschen IT-Technik entwickeln, nutzen und bedienen. Hinzukommend steigen die Anforderungen im Arbeitsalltag und damit die Wahrscheinlichkeit, dass Sicherheitsrichtlinien und -regeln von Mitarbeitenden bewusst oder unbewusst umgangen werden (Fan, Lwakatare & Rong 2017:5).

Im produzierenden Gewerbe führen lediglich 36,8 Prozent der KMU regelmäßig Awareness-Trainings für ihre Mitarbeitenden durch (Hillebrand et al. 2017). In vielen Organisationen beschränken sich Information Security Awareness-Trainings (ISAT) oft auf Maßnahmen zur Wissensvermittlung, die jedoch keine nachhaltige Wirkung zu haben scheinen. Dies wird auch durch Tsohou et al. (2012) aus globalen Sicherheitsumfragen geschlussfolgert. Darüber hinaus reicht eine einmalige Schulung, die darauf abzielt, Lücken im Sicherheitsbewusstsein zu schließen, nicht aus, um die notwendige Einhaltung

der Sicherheitskultur zu gewährleisten (Fagade & Tryfonas 2016). Jährliche Schulungen sind zudem häufig der einzige Anlass, bei denen Mitarbeitende sich mit Richtlinien aktiv auseinandersetzen, was keine nachhaltige Verhaltensänderung bewirkt (Kirlappos, Beautement & Sasse 2013).

Die psychologische Forschung zeigt, dass wir neben dem klassischen theoretischen Ansatz zur Wissensvermittlung einen marketingorientierten Ansatz zur Förderung der emotionalen Identifikation und einen systemischen Ansatz zur teambasierten Kommunikation benötigen (Helisch & Pokoyski 2009). Da es bei IS um mehr als um Technik geht (Albrechtsen 2007) (Kruger, Drevin & Steyn 2007), scheint die soziale Teilhabe an einem kommunikativen Teamprozess eine Schlüsselkomponente bei der Entwicklung von ISATs und entsprechendem Trainingsmaterial zu sein.

Hier kommen Serious Games und die Methodik des GBL ins Spiel. GBL hat großes Potenzial, wertvolle Beiträge zu gesellschaftlich relevanten Bereichen wie Bildung und Gesundheit zu leisten (Göbel 2017) (Institute Of Play 2015). Aus diesem Grund hat es im letzten Jahrzehnt zunehmend Anerkennung als effektive Lehr- und Lernmethode erhalten, die die Motivation verbessert und Verhaltensänderungen auslöst (Bösche & Kattner 2011). Das Erzeugen von emotionaler Resonanz beinhaltet das Ansprechen spezifischer individueller Anliegen. Menschen müssen durch emotionales Engagement „verstehen“, dass sie selbst von einem Mangel an IS betroffen sind. Analoges GBL ist als Mittel zur Motivationsförderung besonders effektiv und sollte explizit für ISAT eingesetzt werden, da die Lernenden die Konsequenzen ihres Handelns direkt sehen und im Dialog ein Gefühl für ihren Wissensstand bekommen können.

Was sind KMU?

Kleinstunternehmen, kleine und mittlere Unternehmen (KMU) werden nach der Empfehlung der EU-Kommission 2003/361 wie folgt definiert (Europäische Kommission 2003):

Unternehmensgröße	Zahl der Beschäftigten	und	Umsatz €/Jahr	oder	Bilanzsumme €/Jahr
kleinst	< 10		≤ 2 Millionen		≤ 2 Millionen
klein	< 50		≤ 10 Millionen		≤ 10 Millionen
mittel	< 250		≤ 50 Millionen		≤ 43 Millionen

Abbildung 1: Definition KMU

1.1 Social Engineering

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) versteht Social Engineering (SE) als Methode, welche menschliche Eigenschaften wie z. B. Hilfsbereitschaft, Vertrauen, Angst oder Respekt vor Autorität ausnutzt, um unberechtigten Zugang zu Informationen oder IT-Systemen zu erlangen (BSI 2020:42). Der Begriff Social Engineering wird laut der Studie „Bluff me if U can“ häufig mit positiven Assoziationen verbunden (known_sense 2015:36). Entgegen dieser Fehlinterpretation stellen Social Engineering Attacken die größte Bedrohung der IS dar (Salahdine & Kaabouch 2019:2).

In einer aktuellen Studie der Bitkom (2020:10) gaben 37 Prozent der mehr als 1.000 befragten Unternehmen an, von analogem und digitalem Social Engineering betroffen gewesen zu sein, wobei die Dunkelziffer auf fast die Hälfte geschätzt wird. Damit ist Social Engineering im Hinblick auf Spionage, Sabotage und Datendiebstahl eines der häufigsten Verbrechen. Dies zeigt deutlich die Notwendigkeit, das Bewusstsein der Mitarbeitenden zu schärfen.

Je nach Art des Angriffs kann nach technik- und menschlich-basierten Social-Engineering-Angriffen unterschieden werden (Albladi & Weir 2018:3). Zu den technik-basierten Angriffsarten zählen z. B. Phishing und der Einsatz von Malware. Zu den menschlich-basierten Angriffen gehören z. B. Identitätswechsel, Identitätsdiebstahl und Shoulder Surfing (= über die Schulter schauen).

1.2 Security Risk Management

Das BSI beschreibt Risikomanagement (RM) als die Gesamtheit aller Aktivitäten mit Bezug auf die strategische und operative Behandlung von Risiken, welche die Identifikation, die Einschätzung und Bewertung, Behandlung und Überwachung von Risiken sowie Risikokommunikation für Organisationen umfasst (BSI 2017a:90). Bei Security Risk Management (SRM) werden entsprechend Informationssicherheitsrisiken berücksichtigt. Mit dem BSI-Standard 200-3 liefert das BSI unter anderem eine Anleitung zur Ermittlung von Gefährdungen, zur Risikoeinstufung und Behandlung von Risiken, um die Ergebnisse im bestehenden Sicherheitskonzept zu integrieren (BSI 2017b).

Einige der häufigen Probleme, die bei der Implementierung eines SRM auftreten können, sind lt. Fenz et al. (2014) die Inventarisierung der Vermögenswerte und Gegenmaßnahmen, die Wertzuweisung der Vermögenswerte, die Risikobewertung und der Kompromiss zwischen Risiko und Kosten.

Die COVID-19-Pandemie zeigt, wie wichtig ein funktionierendes Risikomanagement ist. Interviews von über 1.000 Führungskräften in vier verschiedenen Ländern, darunter Deutschland, ergaben, dass 90 Prozent der Befragten eine Zunahme der Cyberangriffe feststellten (Tanium 2020). Teilweise reagieren Unternehmen bereits auf die Veränderung der Risikolage. In einer Befragung von PwC gaben 112 Risikomanager an, dass in ihrem Bereich die Ressource Cyber Risk Mangement um 73 Prozent für das Jahr 2021 erhöht wird (PwC n.a.).

2 Zielstellung des Projektes

Das FZI hat innerhalb des Projekts „Mittelstand 4.0- Kompetenzzentrum Stuttgart“ einen Unterauftrag betreffend des Arbeitspaketes 1.3 „Konzeption und Entwicklung der Schulungs- und Veranstaltungsinhalte“ und des Arbeitspaktes 1.4 „Durchführung von Schulungen und Veranstaltungen“ an die Forschungsgruppe Scholl (FGS) der Technischen Hochschule Wildau (TH Wildau) vergeben.

Vom 01. April 2020 bis 31. März 2021 sollten zwei analoge, erlebnisorientierte Lernszenarien mit kleinen digitalen Ergänzungen zu den Themen Social Engineering und Security Risk Management für KMU des produzierenden Gewerbes konzipiert und entwickelt werden. Während als Zielgruppe für das Lernszenario zum Thema Social Engineering alle Mitarbeitenden definiert wurden, sollte sich das Lernszenario zu Security Risk Management an das mittlere Management richten.

Die Konzeption und Entwicklung sollte unter Anwendung eines partizipativen Vorgehens und Einbezug technisch-organisatorischer Maßnahmen nach neuen didaktischen und psychologischen Erkenntnissen erfolgen. Anschließend sollten die Lernszenarien im Rahmen zweier Workshops von Mitgliedern der Arbeitsgruppe IT-Sicherheit getestet, diskutiert und reflektiert werden.

Die Lernszenarien zielen darauf ab, Mitarbeitende von KMU erlebnisorientiert für das Thema IS zu sensibilisieren. Beide erlebnisorientierte Lernszenarien stehen nach Projektende den Kooperationspartnern des Projektes „Mittelstand 4.0-Kompetenzzentrum Stuttgart“ und damit auch den Teilnehmenden der Arbeitsgruppe IT-Sicherheit für eigene Veranstaltungen zur Verfügung.

3 Methodische Grundlagen

3.1 Sensibilisierung & Awareness

Nach Wilson und Hash (2003:7) ist Lernen ein kontinuierlicher Prozess, wobei Schulungen auf Sensibilisierung aufbauen. Sensibilisierung im Sinne des Wortes bedeutet „empfindsam machen“ (Wehner et al. 2002:58). Sensibilisierungsmaßnahmen im Kontext der IS sollen ein Bewusstsein für die Wichtigkeit der Thematik schaffen und die Teilnehmenden motivieren, ihr eigenes Verhalten zu reflektieren und entsprechend zu reagieren (Wilson et al. 1998). Schulungen und Awareness-Programme sind in allen Organisationen immens wichtig, wobei die Halbwertszeit des Vergessens oder das Verdrängens der Themen zu beachten ist - regelmäßiges Wiederholen ist unabdingbar und noch viel wichtiger ist ihr alltägliches beispielhaftes Vorleben durch die Verantwortlichen (Darms et al. 2019:19). Die Sensibilisierung der internen und der externen Mitarbeiter ist unerlässlich (Darms et al. 2019:175).

Schulungen zielen auf die Vermittlung von relevanten Sicherheitsfähigkeiten und -kompetenzen ab (Wilson & Hash 2003:9) und sollen diese tiefergehend aufbauen. Information Security Awareness (ISA), kurz Awareness, wird unterschiedlich definiert. Aus dem Englischen übersetzt bedeutet der Begriff „Informationssicherheitsbewusstsein“. Weber et al. (2019:9) unterscheiden zwischen „Sensibilisierung“ als Prozess und „Awareness“ als Zustand. Sie schließen sich der Definition von Richter et al. (2018:9) an, die ISA als den „bewussten Umgang mit Informationen, unabhängig vom Medium“ beschreiben. Awareness-Maßnahmen sollten nach König und Wolf (2018:81) die Aufmerksamkeit der Teilnehmenden wecken und die Inhalte effizient in einer definierten Zeitspanne vermitteln, ohne sie durch zu viele Themen zu überfordern.

Bei der Entwicklung unserer Lernszenarien stehen die Sensibilisierung der Teilnehmenden und die Steigerung ihrer Awareness im Vordergrund. Diese sollen für die Themen Social Engineering und Security Risk Management emotionalisiert und motiviert werden, worauf eine kontinuierliche Fortbildung aufbaut.

3.2 Analog & Digital

Während analoge Formate auf die vollständige Wahrnehmungsbreite abzielen, sind die Wahrnehmungskanäle der Teilnehmenden bei Online-Formaten generell eingeschränkt auf visuelle und akustische Reize. Online-Formate überbrücken zwar Entfernungen, kreieren letztlich aber eine zwischenmenschliche Distanz. Analoge Formate hingegen fördern die Interaktion zwischen den Teilnehmenden, indem mehr Raum für Diskussionen sowie direkten Erfahrungs- und Meinungsaustausch geschaffen wird (Taspinar et al. 2016:114). Die soziale Interaktion hat einen positiven Effekt auf die Leistung und Aufnahmefähigkeit der Teilnehmenden (Hurst, Wallace & Nixon 2013:390). Die intuitive Kommunikation untereinander bewirkt, dass die Teilnehmenden dem Ablauf eines analogen Formates besser folgen können (Rachmah 2020:23). Die anleitende Person kann leichter aktiv Einfluss auf den Ablauf eines analog durchgeführten Lernszenarios nehmen, indem diese interveniert und aktiviert. In vergangenen Forschungsprojekten hat sich die Kombination aus analogen und digitalen Lernszenarien als vorteilhaft erwiesen (Scholl et al. 2017).

3.3 Lernmethoden

Spiele können Modelle unserer Wirklichkeit in einem sanktionsfreien Raum abbilden, die komplexe Prozesse verständlicher gestalten (von Ameln & Kramer 2015b:152). Spielen ist das neue Lernen – aus Mitarbeitenden werden „Spielende“. Bereits 2011 wurde Gamification von der Trend- und Beratungsagentur Gartner als Wegbereiter von Veränderungsprozessen in Organisationen betrachtet (LeHong & Fenn 2011). Der Widerstand gegen Gamifikation und GBL war zu dieser Zeit allerdings noch recht hoch, da das Spielen bis zur vorletzten Dekade kaum als Konzept in der klassisch akzeptierten Weiterbildungsmethodik betrachtet wurde (von Ameln & Kramer 2015a:44). Diese Voreingenommenheit hat sich in den letzten Jahren nach unseren Erfahrungen stetig relativiert, sei es durch das zunehmende Verständnis für die Vorteile gamifizierter Prinzipien oder etwa wegen des Perspektivwandels einhergehend mit dem generationsbedingten Wechsel auf Führungsebenen.

Im Folgenden werden die methodischen Grundlagen für die Entwicklung der Lernszenarien erläutert und voneinander abgegrenzt.

Beim **spielebasierten Lernen** bzw. **Game-based Learning** (GBL) sollen Spiele den Lernprozess unterstützen, indem sie den Lernenden eine Herausforderung zum Erreichen der Lernziele bieten (Romero et al. 2012:5). Diese liegen zum Beispiel in der Bewältigung realitätsnaher Situationen, die sich durch die Anpassung an die Lebenswelt der Zielgruppen ergeben und so den Lernerfolg erhöhen (Lombardi 2007). Die so erschaffene sichere Umgebung bietet die Möglichkeit, Fehler zu machen sowie zu experimentieren (Brougere 1999:138). Gleichzeitig motiviert GBL durch eine unterhaltsame Gestaltung zum Lernen (Dewantara et al. 2020:2) und fördert so Verhaltensänderungen (Buffum et al. 2015:64). Regelwerke bilden ein elementares Element in GBL (Wu et al. 2011:269).

Im Unterschied zu GBL greift **Gamifizierung** bzw. **Gamification** lediglich spieltypische Elemente wie Badgets, Levels oder Ranglisten in einem nichtspielerischen Kontext auf, und fördert so die Bereitschaft, sich einer spezifischen Aufgabe zu widmen oder Lerninhalte anzueignen (Basten 2017:76f.).

Grundlage für das **erlebnisorientierte Lernen** bzw. **Experiential Learning** (ExL) ist das Lernen auf verschiedenen Ebenen in Kontakt mit der eigenen Umwelt und der Auseinandersetzung mit Prozessen, die eine Struktur und einen Feedback-Prozess benötigen (Gentry 1990:20).

Accelerated Learning kann mit „**beschleunigtem Lernen**“ übersetzt werden. Ein gesteigertes Lerntempo wird erreicht, indem positive Umgebungen geschaffen, Menschen in ihrer Gesamtheit betrachtet und gedächtnisfördernde Techniken verwendet werden (Serdyukov 2008:41). Es ist gekennzeichnet durch einen aktiven Prozess und bedient sich vielseitiger Kreativtechniken (Schornack 1996:63).

Mit der Kombination der genannten Methoden zielen wir darauf ab, ein Bewusstsein für das eigene Verhalten in Bezug auf IS zu schaffen und Impulse für eine mögliche Verhaltensänderung zu setzen. Dies soll über die Vereinfachung komplexer zu vermittelnder Inhalte sowie der Emotionalisierung, Interaktion, Motivation und Beteiligung der Teilnehmenden erreicht werden. Die hierfür initiierten Diskussionen intensivieren den Erfahrungsaustausch.

4 Spielebasierte Lernszenarien

Die Abbildung 2 zeigt eine zeitliche Übersicht des Projektes in drei Phasen.

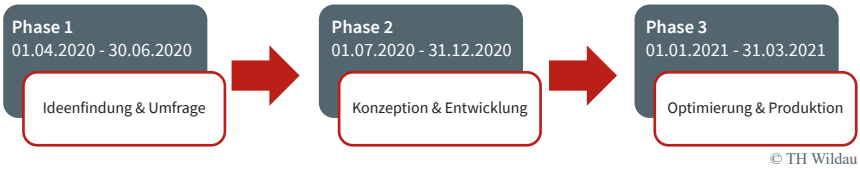


Abbildung 2: Projektphasen

Phase 1

In der ersten Phase vom 01. April 2020 bis 30. Juni 2020 stand die Ideenfindung im Mittelpunkt. Ursprünglich waren hierfür Vor-Ort-Kreativ-Workshops mit Mitgliedern der Arbeitsgruppe IT-Sicherheit geplant, die aufgrund von COVID-19-Maßnahmen nicht stattfinden konnten. Stattdessen wurden zwei Online-Befragungen als Grundlage für die Entwicklung der Szenarien vorbereitet, durchgeführt und ausgewertet. Die erste Umfrage richtete sich direkt an das FZI als Auftraggeber und sollte den Auftrag präzisieren. Die zweite Umfrage wendete sich an die Mitglieder der Arbeitsgruppe IT-Sicherheit und diente der inhaltlichen Schwerpunktsetzung.

Die zweite Umfrage ergab, dass für 60 Prozent der Umfrageteilnehmenden analoge erlebnisorientierte Lernszenarien in der Aus- und Weiterbildung bisher **nicht** verwendet wurden. In den wenigen Fällen, in denen analoge Lernszenarien eingesetzt wurden, waren die Erfahrungen sehr positiv. Um einen Überblick über die bisherigen Sensibilisierungs- und Trainingskonzepte zu erhalten, wurden spezifische Fragen gestellt. Es zeigte sich, dass die Auswahl der Methoden der gängigen Praxis der passiven Wissensvermittlung entspricht. Vorträge, Printmedien (z. B. Poster, Broschüren) und Webinare wurden als Schwerpunkte genannt.

Für die 36 Prozent der KMU, bei denen der Lernerfolg gemessen wird, sind Evaluations- und Feedback- Fragebögen die Methode der Wahl. In der Umfrage bestand die Möglichkeit, konkrete Wünsche zu den Schwerpunkten zu äußern. Die Lernszenarien zum Thema

Social Engineering sollten die Teilnehmenden befähigen, Angriffe zu erkennen und sich davor zu schützen. Das komplexe Lernszenario zum Thema Security Risk Management sollte die Führungskräfte motivieren, sich Risiken bewusst zu werden, statt sie zu ignorieren.

Ergänzend zu der Umfrage wurde für die Generierung von Ideen zu möglichen thematischen Schwerpunkten und Spielemechaniken Brainstorming als Methode verwendet. Diese wurden anschließend mithilfe von Mindmapping organisiert. Entsprechend der Ausführungen von Mandal (2020:336) wurden beide Methoden individuell und im Team durchgeführt, um die Quantität und Qualität der Ergebnisse zu steigern.

Während verschiedene wissenschaftliche Arbeiten (Albladi & Weir 2018) (Mouton et al. 2014) (Schumacher 2011) und das Buch „Die Kunst der Täuschung: Risikofaktor Mensch“ von Mitnick & Simon (2011) als Inspiration für das Thema Social Engineering genutzt wurden, diente der BSI-Standard 200-3 (BSI 2017b) als Basis für die Entwicklung des Spiels zum Risikomanagement.

Phase 2

In der zweiten Phase vom 01. Juli 2020 bis 31. Dezember 2020 standen die Konzeption und Entwicklung im Fokus. Die konzipierten und entwickelten Prototypen wurden nicht wie ursprünglich vorgesehen vor Ort dem FZI vorgestellt, sondern aufgrund der Corona-Maßnahmen postalisch mit dem zugehörigen Konzept zugestellt. Somit fehlte ein direkter Austausch zu den Lernszenarien, wodurch der Umfang des Feedbacks gering ausfiel. Die Selbstanleitung mit Hilfe des Konzeptes ist nur bedingt möglich. Dies verdeutlicht die Wichtigkeit einer Moderationsanleitung. In dem Zeitraum wurde zu den Themen Security Risk Management und Social Engineering jeweils ein Konzept für die digitale Ergänzung erstellt. Während die digitale Ergänzung zu SRR bereits in dieser Phase wie geplant umgesetzt wurde, ist die Entwicklung der digitalen Ergänzung zu »Social Engineering Theater (SET)« in Phase 2 aufgrund von verschärften COVID-19 Maßnahmen nicht über die Vorbereitungen hinaus erfolgt. Die geplanten Vor-Ort-Workshops zum Testen der Lernszenarien mit Mitgliedern der Arbeitsgruppe IT-Sicherheit wurden in Online-Workshops umgewandelt und in Phase 3 durchgeführt.

Phase 3

Die Finalisierung der Lernszenarien erfolgte in der letzten Phase vom 01. Januar 2021 bis 31. März 2021. Nach Durchführung und Auswertung der Online-Workshops sowie der Zusammenfassung der gewonnenen Erkenntnisse erfolgte die Optimierung der beiden analogen Lernszenarien sowie der digitalen Ergänzungen. Mit der Produktion der finalen Versionen erfolgte auch der Druck der überarbeiteten Moderationsanleitung. Die zehn papiergebundenen Exemplare je Lernszenario werden dem FZI nach Projektende übergeben.

4.1 Social Engineering Theater (SET)

Das zu entwickelnde erlebnisorientierte Lernszenario sollte unter Berücksichtigung psychologischer Grundlagen die verschiedenen Aspekte und Facetten des Social Engineerings aufgreifen und die Bedürfnisse und Besonderheiten des produzierenden Gewerbes einbeziehen.

Ausgangsidee für das Lernszenario basierte auf einer Entwicklung eines Rollenspiels im Projekt „SecAware4job“, das sich jedoch als zu komplex für dieses erwies.

Um die Komplexität zu reduzieren und verschiedene Perspektiven in Bezug auf Social Engineering zu realisieren, wurde das Lernszenario in drei Teilen konzipiert, in Anlehnung an bereits in vorherigen Projekten erprobten Lernstationen (siehe Abbildung 3):

- Sketch | Social Engineering als Rollenspiel
- Regie | Handlungsstränge zu Angriffsvektoren
- Backstage | Der Blick hinter die Kulissen von Social Engineering

Die verwendeten Metaphern aus der Theater- und Filmwelt verknüpfen die Teile zu einem Dreiakter und verdeutlichen den Perspektivwechsel. Die Verknüpfung wurde auch deshalb ausgewählt, da Begriffe zu Aktivitäten vor und hinter einer Bühne weitestgehend als bekannt vorausgesetzt werden können. Während in »Sketch« das Rollenspiel aus der Sicht eines Mitarbeitenden ausgewertet wird, nehmen die Teilnehmenden in »Backstage« die Rolle des Social Engineers ein.

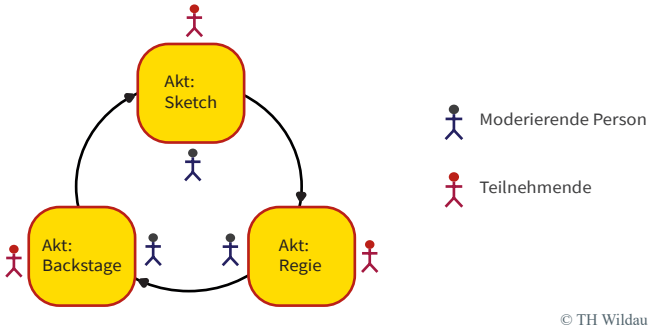


Abbildung 3: SET | Lernstationen

Ausgelegt ist das Lernszenario für zirka neun Teilnehmende (TN) und skalierbar auf max. 30 TN in bis zu drei Teams á zehn TN. Pro Team sollte eine moderierende Person die Regeln erklären, durch den jeweiligen Akt des Lernszenarios führen, Fragen beantworten, den Diskurs unter den Teilnehmenden leiten und wichtige Grundlagen zum Social Engineering anhand der Moderationsanleitung vermitteln.

4.1.1 SET | Prolog und Epilog

Zusätzlich zu den drei Teilen »Sketch«, »Regie« und »Backstage« gibt es den »Prolog« und »Epilog«, die diese einrahmen. Der »Prolog« leitet das Lernszenario ein und stimmt die Teilnehmenden in Form einer Vorstellungsrunde auf das folgende Spiel ein. Dies geschieht mit Hilfe von Zahnrädern, welche die Teilnehmenden mit ihren Eckdaten beschriften (siehe Abbildung 4). Das Motiv der ineinandergreifenden Zahnräder symbolisiert die Zielgruppe produzierendes Gewerbe. Der »Epilog« bietet Raum für eine abschließende Diskussion und Feedback. Eine Anregung innerhalb des Online-Workshops wurde in die Moderationsanleitung aufgenommen: Die in »Sketch« vorhandenen Schutzkarten sollen eine Diskussion darüber initiieren, wie eine effektive Abwehr im dritten Akt gestaltet werden könnte.



© TH Wildau

Abbildung 4: SET | Prolog

4.1.2 SET | Sketch

Nach Nagler (2009:126f.) fördert das Rollenspiel die Reflexion der Teilnehmenden und trägt dazu bei, diese mit den im Rollenspiel erlebten Erfahrungen zu verknüpfen. Des Weiteren hilft das Konzept des Rollenspiels, die erlebten Inhalte besser im Gedächtnis zu behalten (Günther 2019:13).

Die kreative Grundlage von Sketch basiert auf dem Konzept des in SecAware4job entwickelten Rollenspiels. Ziel jedoch war es, den zeitlichen und inhaltlichen Umfang zu reduzieren. Mit zehn unterschiedlichen Charakteren und verschiedenen Situationen war es in seiner Ursprungsform zu komplex. Ähnlich eines Krimidinners mussten sich TN in ihren jeweiligen Charakter hineinversetzen und nur mit wenig textlicher Unterstützung agieren. In einer Sensibilisierungsmaßnahme, die Mitarbeitende unterschiedlicher Bereiche und Unternehmen zusammenführt, ist es in der Kürze der Zeit eher unwahrscheinlich, ein Gemeinschaftsgefühl und die notwendige atmosphärische Stimmung zu erzeugen. Des Weiteren erfordert diese Version zu viel Vorbereitungsaufwand und ist zeitlich für das Lernszenario nicht umsetzbar. Um TN nicht zu überfordern, wurden lediglich einzelne Aspekte herausgegriffen und die Zahl der Charaktere sowie der Situationen eingegrenzt.

Im Ergebnis umfasst Sketch drei konkrete Situationen zu Angriffsvektoren, die nie mehr als zwei Rollen und einen Sprecher/eine Sprecherin erfordern. Die Dialoge sind als Unterstützung vorgegeben und kurz gehalten. Sie setzen kein schauspielerisches Talent vor-

aus und könnten als Sprechtheater einfach abgelesen werden. Die visuelle Beschreibung durch den Sprecher/die Sprecherin hilft den roten Faden zu erhalten.

Der sich anschließende Spielschritt der Kartenzuordnung ist aufgrund der einfachen Spielemechanik intuitiv. Dieser soll hinsichtlich der vorab präsentierten Szene zur Diskussion mit Erfahrungsaustausch über verwendete Angriffsvektoren, Social Engineering-Techniken und Kommunikationskanäle sowie potenzieller Schutz- bzw. Gegenmaßnahmen anregen. Exemplarisch ist dies in Abbildung 5 dargestellt



© TH Wildau

Abbildung 5: SET | Sketch Beispiel

4.1.3 SET | Regie

Der Entwicklungsansatz beruht darauf, dass in der Realität eine Vielzahl von Faktoren einen Social Engineering Angriff beeinflusst und es je nach Verhalten der Betroffenen zu Wendungen durch einen Angriff kommen kann. Ziel war es, diese Dynamik auf ein interaktives Videoquiz zu übertragen. Das heißt, TN sollen selbst über Handlungsstränge eines komplexen Angriffs entscheiden und ihre Auswahl in der Gruppe diskutieren. Aus didaktischer Sicht sind Videos hervorragend geeignet, Diskussionen anzuregen und zu reflektieren (Stadler 2005:174). Vorbild war zum Beispiel der interaktive Film „Black Mirror: Bandersnatch“ von Netflix. Aufgrund der Budgethöhe wurde die Verzweigung auf maximal drei Ebenen beschränkt (siehe Abbildung 6). Im Vordergrund der Videos sollten vor allem die Inhalte zum Thema Social Engineering stehen. Daher erfolgte die Umsetzung mit Laiendarstellern. Um die Anonymität der Darstellenden zu gewährleisten, wurde mit unterschiedlichen Verfremdungstechniken experimentiert. Dabei sollte jedoch der Sensibilisierungseffekt nicht verlorengehen.

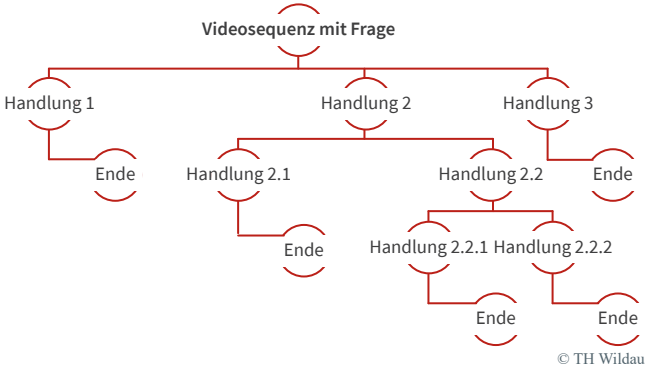
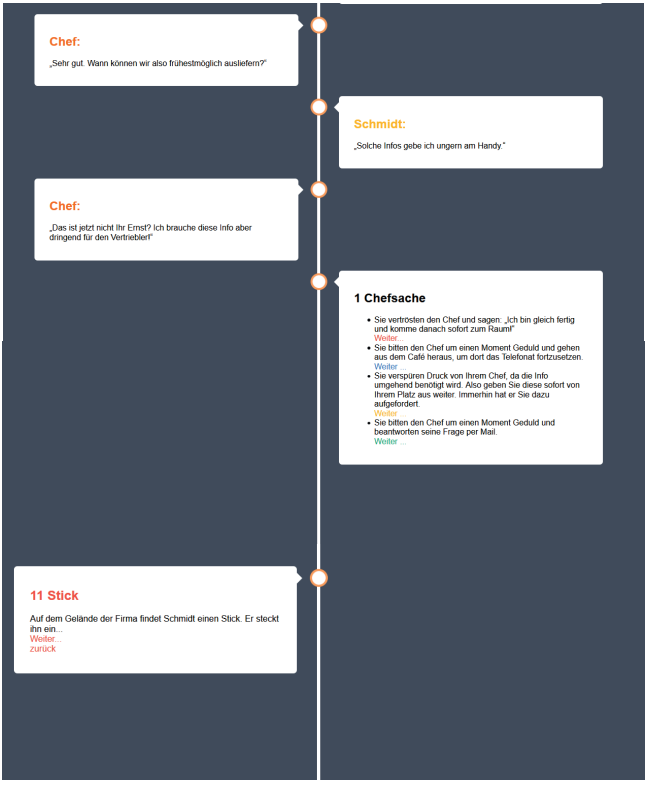


Abbildung 6: SET | Regie – Maximale Vertiefung der Handlungsstränge

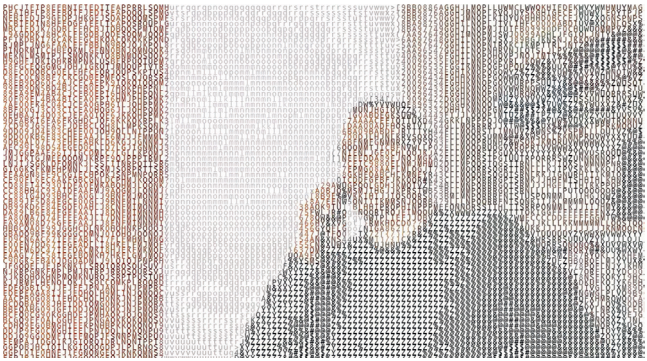
Zu der ersten Storyidee wurde versucht, mithilfe einer Zeitachse einen Ereignisbaum zu realisieren. Entscheidungen an Wendepunkten führen anhand einer Sprungmarke je nach Entscheidung zu unterschiedlichen Positionen auf der Zeitachse (siehe Abbildung 7). Die einzelnen Teile bestanden aus reinem Text und wurden teilweise durch kleine vorab gedrehte Filmsequenzen unterstützt. Diese Probeaufnahmen wurden zur Verfrem-

dung experimentell umgewandelt in ASCII Art (siehe Abbildung 8). Trotz der Kreativität dieses Lösungsansatzes wurde auf eine andere Verfremdungsart zurückgegriffen, da das Ergebnis visuell überfordert und vom Inhalt ablenkt. Neben seiner Ästhetik erwies sich der Zeichentrickstil aufgrund seiner Popularität für unsere Zwecke als besser geeignet. Die Entscheidung bei der Umsetzung fiel zunächst auf den Zeichentrickfilter von Adobe AfterEffects, mit dem einzelne Konfigurationen zum Beispiel hinsichtlich Farbe und Konturen möglich sind (siehe Abbildung 9).



© TH Wildau

Abbildung 7: SET | Regie – Zeitleiste mit Sprungmarken



© TH Wildau

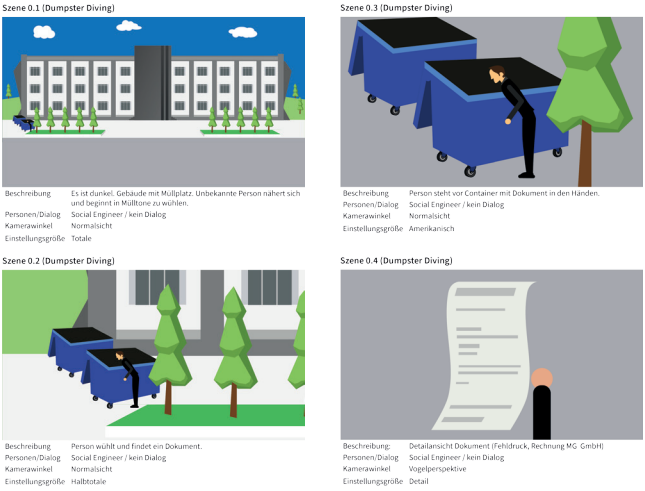
Abbildung 8: SET | Regie – Verfremdung ASCII Art



© TH Wildau

Abbildung 9: SET | Regie – Verfremdung mit Zeichentrickfilter ohne Farbe

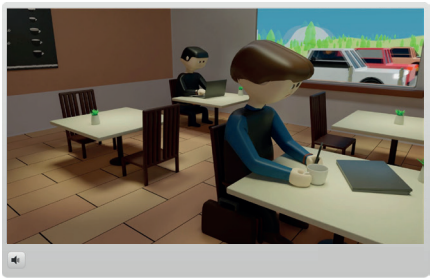
Im Anschluss an die Experimente wurde die Story ausgebaut. In Vorbereitung auf die Dreharbeiten wurde ein Storyboard erstellt, das Informationen zu Kamerawinkeln und -einstellungen enthält (siehe Abbildung 10). Aufgrund der Corona-Maßnahmen verzögerte sich jedoch der eigentliche Videodreh erheblich und konnte letztlich durch die fortlaufenden Verlängerungen dieser nicht durchgeführt werden. Alternativ wurden die für das Storyboard erstellten Grafiken als Videosequenzen aufbereitet. Programmiert wurde das Videoquiz mit der Software Articulate Storyline 3.



© TH Wildau

Abbildung 10: SET | Regie – Ausschnitt Story Board

Die endgültige Version mit in Blender erstellten 3D-Animationen entstand durch die Unterstützung des Grafikdesigners Stefan Gensler. Valentin und Philipp steuerten die musikalische Untermalung bei. Ein Bildausschnitt der Finalversion ist in Abbildung 11 dargestellt.



© TH Wildau

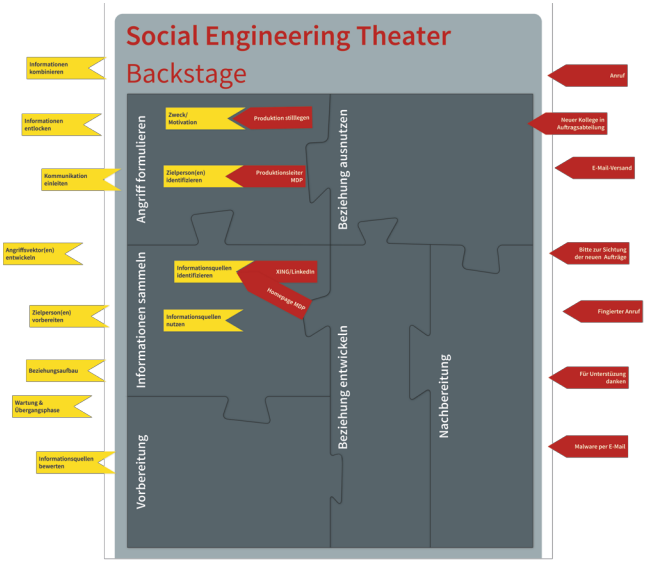
Abbildung 11: SET | Regie – Finalversion

Die finale Version steht unter der folgenden URL zur Verfügung:
https://diz.wildau.biz/set/regie/index.html

4.1.4 SET | Backstage

Die Ausgangsidee für Backstage war der Perspektivwechsel vom Betroffenen hin zum Social Engineer. Hierfür wurde ein fiktiver Zeitungsartikel in loser Anlehnung an wahre Vorkommnisse verfasst, mit dessen Hilfe sich die Teilnehmenden in Social Engineers versetzen und deren Herangehensweise nachvollziehen sollen.

Die Grundlage für die erste Version bildet das Social Engineering Attack Framework von Mouton et al. (2014). In der ersten Phase dieser Version sollten die Teilnehmenden den Angriffsrahmen als Puzzle zusammensetzen. Anschließend sollten die einzelnen Prozessschritte den Phasen zugeordnet werden. Anhand des Zeitungsartikels sollte das Vorgehen der Social Engineers rekonstruiert werden, indem die Fallkarten entsprechend des Artikels mit den Prozessschritten zusammengefügt werden. In Abbildung 12 wird ein Spielmoment exemplarisch gezeigt.



© TH Wildau

Abbildung 12: SET | Backstage – Zuordnungsprozess in der ersten Version

Da sich die Vorgaben für die Teilnehmenden zu umfangreich erwiesen, wurde die erste Version modifiziert. Die Grundlage für die Modifizierung bildet ein Sequenzdiagramm. Diese Diagrammtypen kommen im Rahmen von UML (Unified Modeling Language) für die Modellierung von Interaktion zum Einsatz, insbesondere in der Softwareplanung, (Rumpe 2011). Das Prinzip eines solchen Sequenzdiagramms wurde während der Tests anhand eines Beispiels erläutert. Die gewählte Darstellung erwies sich im Verlauf als zu komplex und unübersichtlich. Um diese zu vereinfachen, wurde auf das Motiv Banküberfall zurückgegriffen, das vielen Teilnehmenden aus dem Filmgenre Heist-Movie bekannt sein sollte, in dem die Planung, Vorbereitung und Durchführung von Raubüberfällen aus der Perspektive der Täter spektakulär inszeniert wird (Venus 2007:301). Zu den allgemein bekannten Filmen des Genres zählen zum Beispiel die Reihen Olsenbande und Ocean's. Das Sequenzdiagramm „Banküberfall" ist in Abbildung 13 dargestellt.

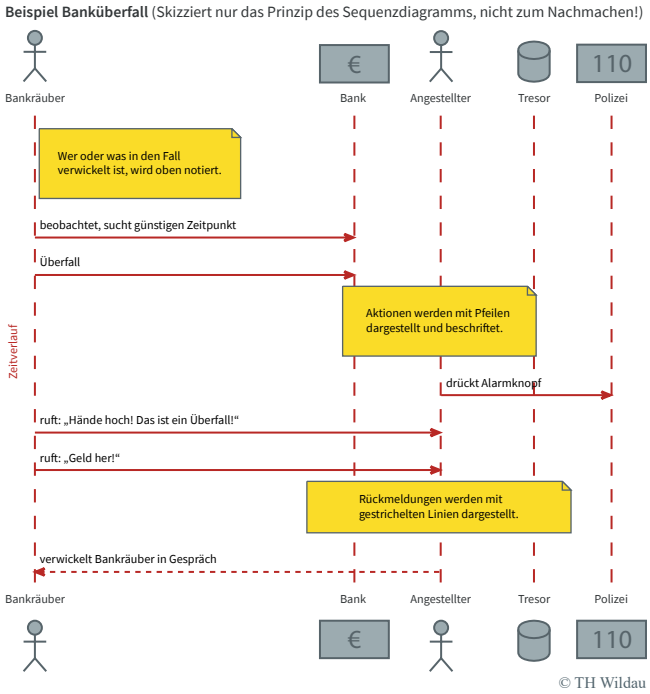


Abbildung 13: SET | Backstage – Beispiel Banküberfall

4.2 Security Risk Roulette

Ziel war es, ein komplexes analoges erlebnisorientiertes Lernszenario zum Thema SRM für Führungskräfte von KMU des produzierenden Gewerbes zu konzipieren und zu entwickeln. An der Entwicklung des Lernszenarios SRR war known_sense als Projektpartner federführend beteiligt. Der Zielgruppe sollte das Thema Risikomanagement als notwendiger Baustein der Unternehmensführung nahegebracht, die komplexen Grundprinzipien vereinfacht demonstriert und die Vorteile für die jeweils eigene Branche und das eigene Unternehmen kommuniziert werden.

Als eine Art Einführung zum Risikomanagementprozess wird durch das Lernszenario von einer moderierenden Person in einer geplanten Länge von zirka 90 bis 120 Minuten geführt. Es eignet sich für Events mit einer Gruppengröße von 4 bis 16 Teilnehmenden. Die Teilnehmenden können dabei entweder aus unterschiedlichen Organisationen kommen oder der gleichen angehören. Innerhalb eines Unternehmens kann das Lernszenario als eine Art Mediation zwischen Sicherheitsfachleuten und Führungskräften fungieren.

Als Awareness-Agentur, Planspielproduzent und Trainer hatte known_sense bereits 2015 gemeinsam mit Dr. Christoph Schog von T-Systems International das Risk Assessment-Planspiel „Security Spot“ auf Basis sogenannter „Painpoint-Karten“ (bis zu 70 Karten, die diverse Sicherheitsrisiken bzw. mögliche Security-Themen für Awareness-Kampagnen umfassen) aus dem Kampagnen-Planungs-Tool „askitMeta“ entwickelt (Schog & Pokoyski 2017). Das Kartenset „askitMeta“ wird bereits seit 2008 nach einer gemeinsamen Entwicklung von known_sense mit dem Awareness-Experten Marcus Beyer vor allem im Rahmen von Kickoff-Workshops zur Priorisierung und Visualisierung von Awareness-Kampagnen eingesetzt. Es umfasst je nach Konfektionierung etwa 100 bis 140 Karten in den vier Kategorien Security-Images (Bildkarten), Security-Painpoints, Zielgruppen sowie Awareness-Kanäle und -Medien. Die Versionen der Bundesakademie für öffentliche Verwaltung (BAköV) werden von der FGS seit 2010 in der Aus-, Fort- und Weiterbildung für Informationssicherheitsbeauftragte und Studierende eingesetzt.

In den Kunden-Workshops werden durch das Legen und Zuordnen bzw. Kommentieren von Kampagnen-Lernkarten die Fragen wiederholt abgearbeitet, die im Rahmen von Awareness-Workshops auftauchen:

- Welches Image wird Informationssicherheit zugeschrieben und was resultiert aus dieser Zuschreibung?
- Welche Risiken stehen im Fokus?
- Welche Zielgruppen sollen in Kampagnen angesprochen werden?
- Welche Kanäle müssen mithilfe welcher Medien gewählt werden?

Die Karten dienen also als typische Kommunikationsbeschleuniger, die das Diskursive im Sinne des Slogans „Talking Security" vorantreiben.

Da der Einsatz des Risk Management-Workshops, „Security Spot", als Kommunikationsbeschleuniger so überzeugend gelang, wurde in einem ersten Konzeptionsschritt geprüft, ob dieser in modifizierter Form auch im Rahmen des neuen Auftrags Einsatz finden könnte. Dazu hätten die Ziele des Planspiels von der Konzernebene auf KMU verschoben werden müssen. Dieser Ansatz wurde schnell verworfen, da die Zielgruppe KMU einen detaillierteren Einstieg in das Risikomanagement benötigt als die Vorstandsebene eines Konzerns. Hieraus wurde abgeleitet, dass eine transparente Simulation der Risikomanagementprozesse für das KMU-Management zu erstellen war.

Im Rahmen des Kickoffs analysierte known_sense innerhalb eines Design Thinking Workshops typische Risikomanagement-Szenarien. Die Methode Design Thinking läuft in der Regel nach einem iterativen Prozess ab, der sich im Wesentlichen durch sechs Schritte auszeichnet: Verstehen – Beobachten – Standpunkte klären – Kreationsprozess einleiten – Prototypen erstellen – Ergebnisse testen. Die Transparenz des Konzeptes Design Thinking fördert eine schnelle Entwicklung, bei der mögliche Hindernisse erkannt und eliminiert werden können. Dies half, die Kernaufgabe bei aller Komplexität des Risikomanagements nicht aus den Augen zu verlieren: Die Modifikation des Risikomanagementprozesses musste gleichsam plakativ wie auch nachvollziehbar gestaltet sowie realistisch und verständlich kommuniziert werden. Im Workshop wurde auch deutlich, dass bei der Wahl der im Spiel simulierten Ereignisse und Budgets verschiedene Aspekte

berücksichtigt werden müssen. Im Fokus sollte für die Teilnehmenden nicht nur der Sieg stehen, sondern vor allem das Nachvollziehen der realitätsnahen Spielschritte und die gewonnenen Einblicke durch eine intensive Diskussion. Dies würde eine Win-Win-Situation schaffen, aus der alle Teilnehmenden Vorteile ziehen, unabhängig von Sieg oder Niederlage.

Bei der Suche nach einem Spielkonzept fiel die Wahl auf das popkulturelle Glücksspiel Roulette, das aufgrund seiner hohen Emotionalität für Spielende als besonders geeignet erschien. Es dient nicht nur als attraktiver Aufhänger für den visuellen und haptischen Einstieg in das Lernszenario, sondern schafft zudem eine Brücke zwischen zufällig und regelmäßig eintretenden Ereignissen. Einer möglichen Reaktanz der Zielgruppe durch die Metapher eines kontextbefreiten „Zockens im Casino“ sollte mithilfe realistischer Szenarien entgegengewirkt werden. Die folgende Abbildung 14 zeigt einen exemplarischen Aufbau des gesamten Lernszenarios für vier Teams.



© TH Wildau

Abbildung 14: SRR | Aufbau

Die Herstellung eines realitätsnahen Bezugs unterliegt verschiedenen Ansprüchen, um die Simulation überzeugend wirken zu lassen. So sollten die Beispiele zu KMU im Allgemeinen und ihren Herausforderungen passen. Dies gelingt über die Unternehmens- und Risikokarten. Die Unternehmenskarten zeigen pro Karte ein fiktives KMU. Die angegebenen Metadaten (Name, Branchenzugehörigkeit, Anzahl der Mitarbeitenden, Standorte und Umsatz) liefern die notwendige Menge an Informationen, um als Mitspielende Entscheidungen im Sinne eines komplexen Risikomanagements fällen zu können. Die Risikokarten beschreiben typische KMU-Risikoszenarien, die sich im Wesentlichen an den IT-Grundschutz-Kompendium orientieren (BSI 2020). Außerdem wurden diese mit einem Risikofaktor von 1 bis 5 beziffert, angepasst an ihre vermeintliche Auswirkung.

Im visuellen Zentrum des klassischen Roulettes steht der Roulette-Kessel, der das Element des Zufalls repräsentiert. In SRR dient der nicht modifizierte Roulette-Kessel als erweiterter Würfel, der die Wahl der Risikokarten bedingt sowie das Ausmaß eines verwirklichten Risikos bestimmt. Dieser wurde nicht als Bestandteil der Finalversion übergeben und steht stattdessen als digitale Ergänzung unter der URL https://diz.wildau.biz/roulette/index.html zur Verfügung. Auf die Entwicklung der Spieledynamik hat der Roulette-Kessel einen untergeordneten Einfluss. Zu Beginn des Lernszenarios erhalten die Mitspielenden ein festgesetztes Budget in Form von Cybermoney. Um eine Alternative zu den Jetons zu liefern, wurde die Währung „Cybermoney“ entsprechend den Jetonwerten entworfen. Angelehnt an echte Währungen wie Dollar oder Deutsche Mark, zeigt das Spielgeld die Portraits verschiedener Persönlichkeiten, die unter dem Aspekt des größten Erfolges im digitalen Bereich basierend auf der Forbes-Liste 2021 ausgewählt wurden (Handelsblatt 2021)[1]. Dies ist in Abbildung 15 dargestellt. Bei der Spieloption mit „Einspruchskarten“ besteht für die Mitspielenden die Möglichkeit, ihr Cybermoney zu setzen und dieses im Spielverlauf zu verdoppeln.

1 Der bereits verstorbene Apple-Gründer Steve Jobs wurde aufgrund seines Status als Ikone in diesem Bereich der Reihe hinzugefügt.



© TH Wildau

Abbildung 15: SRR | Cybermoney

Bei der Spieloption mit „Einspruchskarten“ besteht für die Mitspielenden die Möglichkeit, ihr Cybermoney zu setzen und dieses im Spielverlauf zu verdoppeln. Das Lernszenario SRR beruht jedoch nicht nur auf reinem Glück. Mit dem Erwerb von „Schutzkarten“ können sich Spielende präventiv auf Risiken vorbereiten und auf diese reagieren. Bei Ereigniseintritt vermindern sie entstehende Kosten erheblich. Ihre Nutzung erfordert Strategie und die Analyse der eigenen Situation. Bereits zu einem recht frühen Zeitpunkt der Planung wurde entschieden, dass der Einsatz einer Risiko-Matrix einen zentralen Aspekt im Lernszenario einnehmen soll. Auf dieser sollen die Spielenden das auf der Risikokarte beschriebene Ereignis nach Eintrittswahrscheinlichkeit und Schadensausmaß einordnen. Am Ende des Lernszenarios sollen mindestens 8 Risiken durchgespielt sein.

Basierend auf einem Design Thinking-Workshop wurde ein erstes Konzept von known_sense erstellt. Dieses wurde zu Testzwecken in Zusammenarbeit mit der FGS in sieben iterativen Phasen angepasst und optimiert. Eine hohe Anzahl von Änderungsphasen ist bei komplexen Planspielentwicklungen keine Seltenheit, da Auftraggeber mit wenig oder keiner Erfahrung in der Planspielentwicklung in der Regel deutlich langsamer antizipieren als bei klassischen Medien. Einwände und produktives Feedback seitens der Auftraggeber werden oft erst spät nach der zweiten oder dritten iterativen Phase formuliert.

Aufgrund der COVID-19-Maßnahmen waren während der Entwicklung keine Face-to-Face-Meetings zwischen den beteiligten Parteien möglich. Die erste Pilotversion konnte von der FGS unter Einhaltung der COVID-19-Richtlinien in den Räumlichkeiten der TH Wildau getestet werden, während known_sense an diesem Test via Videoübertragung teilnahm. Dies war ein entscheidender Schritt für die weitere Entwicklung.

Nach zahlreichen Tests und Online-Meetings über einen Gesamtzeitraum von zirka 6 Monaten wurden die Ergebnisse, inklusive vier Optionen hinsichtlich des Ablaufs, den Mitgliedern der Arbeitsgruppe IT-Sicherheit im Rahmen eines Online-Workshops Mitte Januar 2021 vorgestellt. In drei Breakout-Sessions[2] wurden die vier optionalen Spielabläufe präsentiert und entschieden, diese weitestgehend als optional zu belassen. So steht es der moderierenden Person frei, basierend auf konkreten Zielen und dem jeweiligen Einsatzfeld zu entscheiden, welche Zweige der offenen Regelpfade beschritten werden. Idealerweise würde dieser Ansatz im Rahmen eines der Moderationsanleitung ergänzenden Train-the-Trainer-Konzepts erläutert und entsprechend kommentiert werden, welches allerdings nicht Bestandteil des Projektes war.

Die Entwicklung analoger Lernszenarien erfordert grundsätzlich die Interpretation der non- und paraverbalen Kommunikation der Testenden und berücksichtigt deren Intuition, Emotionalität sowie Spontanität. Sowohl für known_sense als auch der FGS war dies die erste Planspielentwicklung ohne die Möglichkeiten von Face-to-face-Begegnungen und stellte ein schwieriges Unterfangen dar, weil neue Wege zum Austausch zwischen allen Beteiligten gefunden werden mussten. Es ist der langjährigen Zusammenarbeit und Erfahrung der Kooperationspartner, der TH Wildau und known_sense, in Bezug auf Spielentwicklung mit begleitender Forschung zu verdanken, dass es trotz aller Einschränkungen gelang, ein attraktives, stimmiges und passendes Planspiel zum Thema zu entwickeln, das hoffentlich über FZI und deren Mitglieder und Partner häufig erfolgreich eingesetzt werden kann.

2 In Online Konferenz-Tools besteht die Möglichkeit, eine Sitzung in Teilsitzungen aufzuteilen. Die Teilnehmenden werden dann automatisch oder manuell diesen sogenannten Breakout-Rooms oder Breakout-Sessions zugewiesen.

5 Tests und Online-Workshops

5.1 Tests

Das Testen der Lernszenarien war beschränkt auf interne Tests mit der FGS, Auszubildenden des Brandenburgischen IT-Dienstleisters (ZIT-BB) und Studierenden des Studiengangs Verwaltungsinformatik jeweils unter den vorgegebenen Abstands- und Hygieneregeln. Die Tests mit den Auszubildenden und Studierenden enthielt bereits vorgenommene Anpassungen nach dem Feedback des FZI.

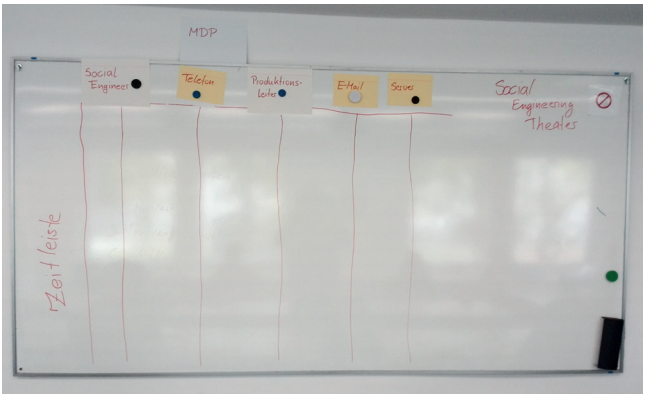
Da das Lernszenario SRR auf das mittlere Management abzielt, wurden mit den vier Auszubildenden des ZIT-BB am 16. Oktober 2020 lediglich die überarbeiteten SET-Bestandteile Sketch und Backstage getestet. Ein anschließend beantworteter kurzer Fragebogen diente im Nachfolgeprojekt „Awareness Labor KMU Informationssicherheit (ALARM Informationssicherheit)“ als erste Datenbasis für die Entwicklung eines Matching-Modells. In einem weiteren Test am 21. Oktober 2020 konnten beide Lernszenarien mit den Studierenden getestet werden.

SET | Sketch

Das Feedback der Auszubildenden und Studierenden führte zu einer erneuten Überarbeitung der Dialoge mit Hinweisen, wie Szenen gespielt und dargestellt werden können. Fragen der Testenden zur Realitätsnähe, zur Strategiewahl des Social Engineers und zu Handlungsmöglichkeiten Betroffener, offenbarten das erhoffte Reflexions- und Diskussionspotenzial sowohl der Sketche als auch der Kartenzuordnungen.

SET | Backstage

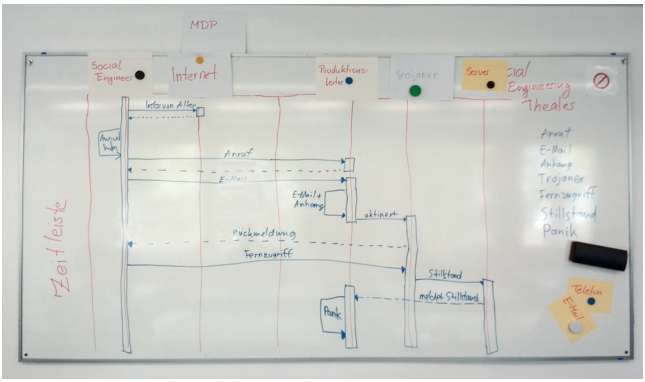
Nachdem der erste Entwurf vom FIZ verworfen wurde, wurde die Spielmechanik auf Basis eines Sequenzdiagrammes komplett überarbeitet und mit den Auszubildenden und Studierenden in einer vorerst rudimentären Version getestet. Der fiktive Zeitungsartikel wurde für diese Testreihe unverändert übernommen. Aber statt des in der Finalversion befindlichen Spielplans und der beschreibbaren Pfeile, stand jeweils zum Testen nur ein Whiteboard zur Verfügung. Dies war ausreichend, um die Spielmechanik und die Idee zu transportieren. Auf einem Whiteboard wurde das Grundgerüst eines Sequenzdiagramms gezeichnet und vorbereitete Karten bereitgelegt, die den Findungsprozess von den im Zeitungsartikel involvierten Akteuren bzw. Objekten erleichterten (siehe Abbildung 16). Die wichtigste Frage zu diesem Zeitpunkt lautete: Wie viele Vorgaben sind notwendig, um mit und in der Gruppe in die Diskussion zu kommen?



© TH Wildau

Abbildung 16: SET | Backstage – Sequenzdiagramm mit Akteuren/Objekten

Die Prinzipien der Darstellung wurden kurz erläutert und nach der Diskussion ergab sich die in Abbildung 17 dargestellte Erweiterung mit den Aktionen.



© TH Wildau

Abbildung 17: SET | Backstage – vollständiges Sequenzdiagramm

Nachdem die Testenden den Zeitungsartikel gelesen hatten, wurde ihnen ein Muster eines klassischen Sequenzdiagramms zur Erläuterung der Aufgabe gezeigt, auf dem alle wichtigen Elemente eines solchen abgebildet waren. Die Grafik wurde von den Testenden als zu komplex eingestuft, was vermutlich daran lag, dass der Diagrammtyp vorher unbekannt war. Nach anfänglich stockender Diskussion und Auswahl einer Person, die das Schreiben bzw. Zeichnen am Whiteboard übernahm, beschleunigte und intensivierte sich der Austausch nach vertiefender Analyse des Zeitungsartikels. Trotz anfänglicher Schwierigkeiten war das Feedback positiv und gab Anlass, diese Idee weiterzuentwickeln.

Security Risk Roulette

Das Lernszenario SRR wurde in einigen Punkten vom FZI als zu komplex empfunden. Die ursprünglichen und alternativen Optionen wurden in drei verschiedenen Studentengruppen getestet, aus denen sich jedoch keine spezifische Präferenz von Optionen ergab. Diese Problematik wurde daher für die Konzeption eines Online-Workshops aufgegriffen.

5.2 Online-Workshops

Konzeption und Durchführung

Ziel der Workshops war das Testen der erlebnisorientierten Lernszenarien und damit einhergehend der notwendige Erhalt von Feedback für die Finalisierung beider erlebnisorientierter Lernszenarien. Durch die Bedingungen der COVID-19-Pandemie konnten die Workshops nicht analog stattfinden. Die Veränderungen bedeuteten einen enormen Mehraufwand für die FGS.

Beide Workshops wurden als Hybridverfahren geplant. Hybrid bedeutet in diesem Fall, dass sich die Workshop-Moderatoren vor Ort mit dem jeweiligen aufgebauten Lernszenario befinden, die Teilnehmenden sich jedoch alle über ein Videokonferenzsystem einloggen. Tatsächlich musste der Online-Workshop zu SRR aufgrund der Verschärfung der COVID-19-Maßnahmen und damit einhergehender Planungsunsicherheiten komplett online durchgeführt werden. Das Ziel beider Workshops war es, die Prototypen der Lernszenarien zu testen und die Teilnehmenden aktiv und emotional zu involvieren. Das digitale Testen von analogen Lernszenarien stellte eine Herausforderung dar und soll die Elemente Interaktivität, Erlebbarkeit und Erfahrungsaustausch vereinen.

Um die verschiedenen Einschränkungen zum Beispiel hinsichtlich der Wahrnehmungskanäle zu berücksichtigen, kam eine 1:1 Übertragung des analogen auf ein digitales Format nicht in Betracht. Diese Vorgehensweise wird auch von Kerres (2020:14) empfohlen. Zur Gewährleistung der aktiven Teilnahme am Workshop wurde die Anzahl auf zehn Personen begrenzt. Voraussetzung für ein gutes Gelingen, war eine gute technische Ausrüstung und eine störungsfreie Übertragung. Wie im analogen Workshop wurde auf ein ausgewogenes Verhältnis zwischen aktiven Phasen und Pausen geachtet. Für beide Workshops wurden 2 Stunden zuzüglich 30 Minuten Puffer angesetzt mit je einer viertel Stunde Pause nach den ersten 45 Minuten.

Evaluation

Als Methoden zur Evaluierung der Online-Workshops wurden eine offene Feedbackrunde am Ende der Workshops sowie ein Online-Fragebogen gewählt.

Der Online-Fragebogen bestand aus 10 Fragen gegliedert in Einleitung, Technisches und Allgemeines, Online-Workshop sowie Lernszenario (siehe Anhang VII-25 bis VII-28). Der Fragebogen enthielt keinerlei Erhebungen von personenbezogenen bzw. personenbeziehbaren Daten. Als Fragetypen wurden vorwiegend geschlossene Fragen gestellt, die entweder Single-Choice oder eine Matrix als Antwortoption enthielten. Die zwei offenen Fragen enthielten entsprechend ein Textfeld zur Beantwortung.

Zu Beginn der Befragung wurden die Teilnehmenden aufgefordert, den jeweiligen besuchten Workshop anzugeben. Es war die einzige Pflichtfrage der Umfrage, die aufgrund der theoretischen Zuordnung anhand des Datums lediglich als Kontrollfrage diente. Im Part Technisches und Allgemeines wurde nach dem genutzten Gerätetyp, nach der Headsetnutzung, der Qualität, technischen Problemen sowie der optimalen Dauer eines Workshops gefragt. Im Part „Online-Workshop“ gaben die Teilnehmenden Feedback zur Durchführung und konkrete Änderungswünsche zu dieser an. Abschließend sollten die Teilnehmenden im Part „Lernszenario“ bewerten, inwieweit der Online-Workshop das Prinzip und die Spielemechanik adäquat vermitteln konnte und welche konkreten Änderungswünsche für das Lernszenario bestehen.

Die beiden Online-Workshops konnten wie geplant und ohne größere technische Probleme durchgeführt werden. An der Online-Umfrage haben sich 12 von insgesamt 20 Teilnehmenden beteiligt und diese beendet, 7 für SRR und 5 für SET. Aufgrund der limitierten Teilnehmerzahl sind die dokumentierten Ergebnisse als Tendenz zu bewerten.

75 Prozent der Teilnehmenden haben mit einem Laptop und 25 Prozent mit einem Desktop-PC an den Online-Workshops teilgenommen. Ein Headset wurde von über 80 Prozent verwendet. In Sachen Qualitätsfragen reichte die Bewertung von sehr gut bis neutral. Die Qualität der Akustik wurde mit gut (ca. 58 %) bis sehr gut (ca. 42 %) bewertet. Knapp 60 Prozent bewerteten die technische Einführung zum genutzten Tool als sehr gut, ein Drittel als gut. Für die Hälfte war die Einbeziehung des Etherpads[3] als externes Tool sehr gut und für ein Drittel gut.

3 Als webbasierter Texteditor erlaubt die Open-Source-Software Etherpad, Texte kollaborativ zu bearbeiten (https://etherpad.org/).

Der Fakt, dass sich teilweise andere Teilnehmende nicht stummschalteten führte bei einer Person zu einer erschwerten Teilnahme durch Störgeräusche. Ansonsten gab es keine technischen Probleme auf Seiten der Teilnehmenden. Für knapp jeweils 45 Prozent sollte ein digitaler Workshop eine Mindestdauer von entweder 30 bis 60 oder 60 bis 90 Minuten betragen. Für zwei Drittel der Teilnehmenden sollte ein Online-Workshop nicht länger als drei Stunden dauern.

Trotz des guten bis sehr guten Feedbacks der Teilnehmenden, spiegelten einige, dass sie Präsenzveranstaltungen präferieren.

5.2.1 Technische Einführung Webex

Die Online-Konferenztools Zoom, Jitsi, BigBlueButton und Cisco Webex wurden eingehend auf Funktionalität und Eignung hinsichtlich datenschutzrechtlicher Aspekte geprüft. Letztlich wurde aus Gründen der Aufwandsminimierung und der Reduzierung bei der Datenerhebung das auf den Servern der Hochschule laufende Cisco Webex ausgewählt.

Jeweils ein Tag vor Workshop Beginn wurden alle Teilnehmenden zum technischen Einführung zu Webex eingeladen. Dies sollte Schwierigkeiten und Unsicherheiten im Umgang mit dem Tool an den eigentlichen Workshop-Tagen verhindern oder zumindest reduzieren. In diesem Zuge wurden die für den Workshop notwendigen Funktionen getestet. Dies umfasst Möglichkeiten der Stummschaltung, An- und Ausschalten des Videosignals, Nutzen des Chats, Beantwortung von Umfragen, das Betreten und Verlassen einer Breakout-Session, Bedienen externer Tools (Etherpad), gemeinsame Bearbeitung von Bildern.

5.2.2 Social Engineering Theater

Konzeption und Durchführung

Für das Online-Format kam keine ausschließlich digitale Version in Betracht, weil hierdurch der analoge Charakter komplett verloren gehen und ein neues Spiel entstehen würde. Da die Teilnehmenden digital nicht selbst agieren können, wurde auf eine Avatarlösung zurückgegriffen. Die moderierenden Personen wurden als Avatare durch die Teilnehmenden angeleitet und führten deren Anweisungen aus, z. B. Karten beschriften und an bestimmte Positionen legen.

Der Aufbau des Lernszenarios erfolgte sowohl an Whiteboards, als auch auf einem Tisch. Für den Online-Workshop zu SET waren hochauflösende Webkameras sowie Kamerastative erforderlich. Beim Aufbau auf einem Tisch wurde ein Stativ mit Schwenkarm und Gegengewichten verwendet (siehe Abbildung 18). Um eventuelle Defizite der Kamerasysteme auszugleichen, sind die Materialien möglichst groß gestaltet. Für drei Breakout-Rooms wurden entsprechend drei Räume vor Ort vorbereitet, um eine gute Audioqualität zu gewährleisten und Geräuschüberlagerungen zu vermeiden.

Der Online-Workshop zu SET wurde in drei Teilen konzipiert: Während im ersten Teil »Prolog« sich die Teilnehmenden vorstellten, notierte einer der moderierenden Personen die Angaben auf den Zahnrädern und legte diese dann ins Kamerabild. Im zweiten Teil »Sketch« wurde ein Sketch von den Moderatoren anstelle der Teilnehmenden vorgeführt. Die Gruppe wird anschließend in drei Breakout-Rooms mit jeweils einer moderierenden Person aufgeteilt. In diesen wurden die Sketche besprochen und diskutiert. Der dritte Teil »Backstage« verläuft nach einem ähnlichen Prinzip.



© TH Wildau

Abbildung 18: SET | Sketch – Aufbau Online-Workshop

Evaluation

Alle Teilnehmenden, die sich auch an der Umfrage beteiligten, fühlten sich in den Workshop einbezogen. Die Pause war für eine Person nicht ausreichend. Dementsprechend wurde der Wunsch geäußert, feste Pausenzeiten einzurichten. Der Inhalt war aus Sicht der Teilnehmenden zeitlich gut bis sehr gut abgestimmt, das Ziel verständlich kommuniziert und die Aufgabenstellung gut verständlich und nachvollziehbar. Die Qualität der geteilten Inhalte wurde als gut (60%) bis sehr gut (40%) bewertet. Der Workshop wurde zudem als abwechslungsreich empfunden. Fast alle nehmen wichtige Informationen für den Berufsalltag mit.

Für vier der fünf Teilnehmenden konnte der Workshop gut das Prinzip und die Spielmechanik des analogen Lernszenarios vermitteln, für eine Person sogar sehr gut. Änderungswünsche für das Lernszenario wurden bereits im Vorfeld in der offenen Feedbackrunde geäußert. Hierzu gehören zum Beispiel der Wunsch nach vorheriger Erläuterung der Begriffe „Angriffsvektor“ und „Social Engineering Technik“. Eine Anregung, die tatsächlich den Ablauf leicht verändern würde, ist der Vorschlag, im »Epilog« mit den im »Sketch« vorhandenen Schutzkarten eine Diskussion zu initiieren, wie eine effektive Abwehr im dritten Akt gestaltet werden könnte.

5.2.3 Security Risk Roulette

Konzeption

Die erhöhte Komplexität des Lernszenarios »Security Risk Roulettes« erfordert eine andere Herangehensweise in der Konzeption des Workshops. Daher wurden Stills erstellt (Beispiel siehe Abbildung 19), anhand derer in einer Präsentation die Spielemechanik step by step visualisiert wird. Die darin erläuterten offenen Regelpfade wurden auf drei Breakout-Sessions aufgeteilt und in kleinen Gruppen diskutiert, um die Ergebnisse anschließend in der großen Runde vorzustellen.



1 Company-Karte pro Team pro Runde ziehen und vorlesen.

© TH Wildau

Abbildung 19: SRR | Online-Workshop Beispielfolie

Evaluation

Die Qualität der geteilten Inhalte wurde als überwiegend sehr gut (ca. 71 %), vereinzelt als gut oder neutral (je ca. 14 %) bewertet. Die Mehrheit der Teilnehmenden (ca.85 %) stimmt den Aussagen teilweise oder ganz zu, dass der Inhalt zeitlich optimal abgestimmt und die Pause ausreichend war. Fast alle Teilnehmenden (85,17 %) fühlten sich gut in den Workshop eingebunden. Der Workshop wurde von allen als abwechslungsreich empfunden. Fast 30 Prozent der Teilnehmenden nehmen eine neutrale Position beim Punkt Verständlichkeit und Nachvollziehbarkeit der Aufgabenstellung ein, beim Punkt klare Zielkommunikation sind es zirka 14 Prozent. Dies deutet auf leichten Nachbesserungsbedarf in diesen Punkten hin. Nur ein Teil der Teilnehmenden gab an, Informationen aus dem Workshop für den Berufsalltag mitzunehmen. Für den Workshop wurde mehrfach der Wunsch geäußert, das Spiel konkret zu spielen.

Für vier der sieben Teilnehmenden konnte der Workshop gut das Prinzip und die Spielmechanik des analogen Lernszenarios vermitteln, für zwei Personen sogar sehr gut und für eine Person nur mäßig. Als konkrete Änderungswünsche des Lernszenarios wurden z. B. Blankokarten für eine Personalisierung und operative Erweiterung sowie die Beibehaltung der verschieden Spielvarianten genannt.

6 Bekanntmachung des Projektes und der Projektergebnisse

6.1 Öffentlichkeitsarbeit

Die Präsentation der Projektergebnisse erfolgt auf unterschiedlichen Kanälen. Online steht eine Projektwebsite zur Verfügung, erreichbar unter https://diz.wildau.biz/. Dort können Interessierte Informationen in Deutsch und Englisch abgerufen. Für einen ersten Eindruck finden sich Screenshots im Anhang VII-29 bis VII-31.

In Deutsch und Englisch entworfene Plakate stellen die Lernszenarien vor und sollen zu verschiedenen Anlässen Interessierte sowie zukünftige Projektpartner auf das Projekt aufmerksam machen. Diese finden sich ebenfalls im Anhang unter VII-32 bis VII-35. Das Projekt wird zudem im Bericht Forschung und Transfer 2020 der TH Wildau beschrieben, der im Frühjahr 2021 erscheinen wird. Eine Kurzdarstellung des Projektes ist im Bericht Forschung und Transfer 2021 der TH Wildau geplant.

Ein Artikel zum Online-Workshop SET erschien am 4. März 2021 in der Märkischen Allgemeinen Zeitung (siehe Anhang VII-36). Zum Abschluss des Projektes ist eine Berichterstattung auf der Campusseite der Märkischen Allgemeinen Zeitung geplant.

Die Moderationsanleitungen werden als gebundene Ausgabe unter der ISBN 978-3-9819225-3-0 herausgebracht.

6.2 Wissenschaftliche Konferenzen und Publikationen

Im Rahmen der Konferenz „Complexity, Informatics and Cybernetics: IMCIC 2021“ vom 9. bis 12. März 2021 in Orlando, Florida USA wurde ein Paper unter dem Titel „Development of Learning Scenarios for Social Engineering and Security Risk Management for SMEs in the Manufacturing Industry” eingereicht, welches virtuell am 12. März 2021 präsentiert wurde. Die IMCIC 2021 ist ein internationales Forum für Wissenschaftler und Ingenieure, Forscher und Berater, Theoretiker und Praktiker auf den Gebieten der Komplexität, Informatik und Kybernetik.

Ein weiteres Paper wurde unter dem Titel „Workshops in a COVID-19 pandemic situation: Testing analogue experiential learning scenarios” verfasst, dessen Abstract bei der “European Conference on Innovation and Entrepreneurship: ECIE 2021” eingereicht wurde. Diese wird als hybride Veranstaltung am 16. und 17. September 2021 ausgetragen.

Unter dem Titel „Awareness Raising in SMEs by Using the Analog Serious Games *Social Engineering Theater* and *Security Risk Roulette*“ wird ein drittes Paper bei der „Canada International Conference on Education (CICE)“ eringereicht, die vom 22. bis 24. Juni 2021 virtuell stattfinden wird. Diese Konferenz widmet sich der Weiterentwicklung von Theorie und Praxis im Bildungswesen.

Ein viertes Paper für ist für die e-Government Konferenz 2021, die unter dem Motto „Vom e-Government zur Digitalisierung“ stattfindet, in Arbeit.

7 Ausblick

Nach den Tests und nachfolgenden Optimierungen müsste üblicherweise eine weitere Entwicklungsiteration beider Lernszenarien mit den jeweiligen Zielgruppen stattfinden. Dies könnte in weiteren Projekten erfolgen, da in der Projektlaufzeit von einem Jahr keine weiteren Iterationen und vertiefende Forschung eingeplant waren. Unter den verwendeten Spielmethoden hat sich insbesondere das Rollenspiel als vielversprechender Ansatz erwiesen, das durch seine variable Modifizierbarkeit bezüglich seines Inhalts für den Transfer auf andere Lernszenarien geeignet ist.

Der gesamte Projektverlauf war geprägt von der COVID-19-Pandemie. Solche außergewöhnlichen Ereignisse lassen sich in kleinen Projekten nur schwer voraussehen und einplanen. Diese Ausnahmesituation stellte das Forschungsteam und den Projektpartner known_sense vor große Herausforderungen, erforderte eine flexible Herangehensweise und hatte einen erhöhten Aufwand zur Folge. So waren durch die COVID-19-Maßnahmen Face-to-Face-Begegnungen nicht bzw. sehr eingeschränkt zwischen den Beteiligten möglich. Daher musste bei der Entwicklung und den Tests der analogen Lernszenarien auf digitale Lösungen zurückgegriffen werden. Die Workshops haben gezeigt, dass es generell möglich ist, die Spielemechanik von analogen Lernszenarien digital zu vermitteln und zu testen. Als Forschungsgruppe nahmen wir die Herausforderung an und bewältigten diese souverän.

In weiteren Forschungsprojekten muss überprüft werden, inwieweit unterschiedliche hybride Formate, in denen analoge Lernszenarien digital übertragen werden, greifbar gestaltet und von der Zielgruppe akzeptiert werden können. Die derzeitigen Nachteile digitaler Lösungsansätze gilt es in Zukunft z. B. durch neue Konzepte oder Nutzung neuer Technologien wie Virtual oder Augmented Reality auszugleichen und neue Möglichkeiten für das Lernen zu erschließen.

Kapitel 3 zeigt deutlich, dass analoge Vermittlungsformate nicht gänzlich durch digitale ersetzbar sind und diesen gegenüber signifikante Vorteile mitbringen. Dies schließt auch analoge Lernszenarien selbst ein. Wir vertreten den Standpunkt, dass besonders analoge erlebnisorientierte Lernszenarien sich dazu eignen, das Bewusstsein der Mitarbeitenden für komplexe Themen der IS zu schärfen.

Um dies empirisch zu belegen, ist die Entwicklung von derzeit unzureichenden Methoden zur expliziten Messung von ISA erforderlich.

Innerhalb des seit dem 1. Oktober 2020 angelaufenen Nachfolgeprojektes „Awareness Labor KMU (ALARM) Informationssicherheit“, in das die Erfahrungen aus diesem Projekt einfließen, sollen solche Messmethoden entwickelt werden. In dem interdisziplinären Forschungsprojekt „ALARM Informationssicherheit“ soll eine Kombination aus sieben analogen und digitalen Lernszenarien sowie „Vor-Ort-Angriffen“ iterativ in drei Phasen, agil und partizipatorisch entwickelt und durchgeführt werden. Sie sollen vor allem der Sensibilisierung von Mitarbeitenden kleiner und mittlerer Unternehmen für IS dienen.

Literatur

Albladi, S. M. & Weir, G. R. S. (2018).

User characteristics that influence judgment of social engineering attacks in social networks, Human-centric Computing and Information Sciences, Vol. 8, No. 1, 2018. DOI: https://doi.org/10.1186/s13673-018-0128-7

Albrechtsen, E. (2017).

A qualitative study of users' view on information security, Computers & Security, Vol. 26, 2007, S. 276-289.

Aytes, K. und Terry, C. (2014).

Computer security and risky computing practices: A rational choice perspective. In: Journal of Organizational and End User Computing, Vol. 16, 2004, S. 22-40.

Basten, D. (2017).

Gamification. IEEE Software. Vol. 34, No. 5, S. 76-81.
DOI: https://doi.org/10.1109/MS.2017.3571581

Bitkom (2020).

Spionage, Sabotage und Datendiebstahl – Wirtschaftsschutz in der vernetzten Welt: Studienbericht 2020, Berlin. Abgerufen am 15. Februar 2021 von: https://www.bitkom.org/sites/default/files/2020-02/200211_bitkom_studie_wirtschaftsschutz_2020_final.pdf

Bösche, W. und Kattner, F. (2011).

Fear of (serious) digital games and learning? Causes, Consequences and a possible countermeasure. In: International Journal of Learning, Vol. 1, No. 3, 2011, S. 1-15.

Brougere, G. (1999).

Some Elements Relating to Children's Play and Adult Simulation/Gaming. Simulation & Gaming, Vol. 30, No. 2, 1999, S. 134-146.
DOI: https://doi.org/10.1177/104687819903000204

BSI (2017a).

Leitfaden zur Basis-Absicherung nach IT-Grundschutz. In drei Schritten zur Informationssicherheit, Bonn. Abgerufen am 15. Februar 2021 von: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Broschueren/Leitfaden_zur_Basis-Absicherung.pdf?__blob=publicationFile&v=3

BSI (2017b).

BSI-Standard 200-3: Risikoanalyse auf der Basis IT-Grundschutz. Bonn. Abgerufen am 15. Februar 2021 von: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/BSI_Standards/standard_200_3.pdf?__blob=publicationFile&v=2

BSI (2020).

IT-Grundschutz-Kompendium. Köln, Bonn: Reguvis Bundesanzeiger Verlag, Bundesanzeiger Verlag. Abgerufen am 15. Februar 2021 von: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Kompendium/IT_Grundschutz_Kompendium_Edition2020.pdf?__blob=publicationFile&v=6

Buffum, P. S., Boyer, K. E., Wiebe, E. N., Mott, B. W. & Lester, J. C. (2015).

Mind the Gap: Improving Gender Equity in Learning Environments with Learning Companions. In: C. Conati, N. Heffernan, A. Mitrovic, & M. F. Verdejo (Hrsg.), Artificial Intelligence in Education: 17th International Conference, AIED 2015, Madrid, Spain, June 22-26, 2015, S. 64-73. Schweiz: Springer International Publishing. DOI: https://doi.org/10.1007/978-3-319-19773-9_7

Darms, M., Haßfeld, S., & Fedtke, S. (2019).

Krankenhäuser und Kliniken – groß, anonym und damit ideal für Angreifer. In: IT-Sicherheit und Datenschutz im Gesundheitswesen, S. 175-195. Springer Vieweg, Wiesbaden.

Dewantara, D., Wati, M., Misbah, M., Mahtari, S. and Haryandi, S. (2020).
The Effectiveness of Game Based Learning on The Logic Gate Topics. In: Journal of Physics: Conference Series. Vol. 1491, 012045.
DOI: https://doi.org/10.1088/1742-6596/1491/1/012045

Dreißigacker, A., von Skarczinsik, B. and Wollinger, G. R. (2020).
Cyberangriffe gegen Unternehmen in Deutschland, Druck Team Druckgesellschaft mbH, Hannover.

Europäische Kommission (2003).
Amtsblatt der Europäischen Union: Empfehlung der Kommission vom 6. Mai 2003 betreffend die Definition der Kleinstunternehmen sowie der kleinen und mittleren Unternehmen (Bekannt gegeben unter Aktenzeichen K(2003) 1422) (2003/361/EG). Abgerufen am 15. Februar 2021 von:
https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:32003H0361&from=EN

Fagade, T. und Tryfonas, T. (2016).
Security by compliance? A study of insider threat implications for Nigerian banks. In: Tryfonas, T. (Hrsg.), Human Aspects of Information Security, Privacy, and Trust, HAS 2016, Lecture Notes in Computer Science, Cham: Springer, Vol. 9750, 2016, S. 128-139.

Fan, W., Lwakatare, K., & Rong, R. (2017).
Social Engineering: I-E based Model of Human Weakness for Attack and Defense Investigations. In: International Journal of Computer Network & Information Security, Vol. 9, No. 1, 2017, S. 1-11.
DOI: https://doi.org/10.5815/ijcnis.2017.01.01

Fenz, S.; Heurix, J.; Neubauer, T. und Pechstein, F. (2014).
Current challenges in information security risk management. In: Information Management & Computer Security, Vol. 22, No. 5, 2014, S. 410-430.
DOI: https://doi.org/10.1108/IMCS-07-2013-0053

Gentry, J. W. (1990).

Guide to business gaming and experiential learning. East Brunswick, Nichols/ GP Pub.

Göbel S. (2017).

Autorenumgebung für Serious Games- StoryTec: Eine Autorenumgebung und narrative Objekte für personalisierte Serious Games, TU Darmstadt, Dissertation.

Günther, M. (2019).

Pädagogisches Rollenspiel. Wissensbaustein und Leitfaden für die psychosoziale Praxis. Wiesbaden: Springer Fachmedien Wiesbaden.

DOI: https://doi.org/10.1007/978-3-658-22793-7

Handelsblatt (2021).

Forbes-Liste 2021. Das sind die reichsten Menschen der Welt.

Abgerufen am 28. Februar 2021 von:

https://www.handelsblatt.com/unternehmen/management/forbes-liste-2021-das-sind-die-reichsten-menschen-der-welt/25725996.html?ticket=ST-7341052-AbboWym4pmUFc0abuPv7-ap1, zitiert von:

https://www.forbes.com/real-time-billionaires/#69290e393d78

Helisch and D. Pokoyski (Hrsg.) (2009).

Security Awareness. Neue Wege zur erfolgreichen Mitarbeiter-Sensibilisierung, Wiesbaden: Vieweg + Teubner, 2009.

Hillebrand, A.; Niederprüm, A.; Schäfer, S.; Thiele, S. und Henseler-Unger, I. (2017).

WIK Report. Aktuelle Lage der IT-Sicherheit in KMU, WIKI Wissenschaftliches Institut für Infrastruktur und Kommunikationsdienste, Bad Honnef, 2017.

Hurst, B., Wallace, R. and Nixon, S. B. (2013).

The Impact of Social Interaction on Student Learning. In: Reading Horizons: A Journal of Literacy and Language Arts, Vol. 52, No. 4, 2013.

Abgerufen am 15. Februar 2021 von:

https://scholarworks.wmich.edu/reading_horizons/vol52/iss4/5

Institute Of Play (2015).

Q Design Pack School. Abgerufen am 15. Februar 2021 von: https://clalliance.org/wp-content/uploads/2020/02/Design-Pack-School.pdf

Kerres, K. (2020).

Frustration in Videokonferenzen vermeiden: Limitation einer Technik und Folgerung für videobasierte Lehren“. In: K. Wilbers (Hrsg.), Handbuch Learning, Köln: Wolters Kluwer, preprint.

Khan, B.; Alghathbar, K. S.; Nabi, S. I. und Khan, M. K. (2011).

Effectiveness of information security – awareness methods based on psychological theories. In: African Journal of Business Management, Vol. 5, No. 26, 2011, S. 10.862-10.868.

Kirlappos, I.; Beautement, A. und Sasse, M. A. (2013).

Comply or die‘ is dead: Long live security-aware principal agents. In: Adams, A. A., Brenner, M. and Smith, M. (Hrsg), Financial Cryptography and Data Security, Lecture Notes in Computer Science, Heidelberg: Springer, Vol. 7.862, 2013, S. 70-82.

known_sense (2015).

Studie: Bluff me if U can - Gefährliche Freundschaften am Arbeitsplatz, Tiefenpsychologische Wirkungsanalyse Social Engineering und seine Abwehr. (known_sense, Hrsg.) Köln. Abgerufen am 10. Januar 2021 von: https://www.known-sense.de/security-studien

König, J., & Wolf, M.R. (2018).

Cyber Security Awareness Training Provided by the Competence Developing Game GHOST. In: ACHI 2018: The Eleventh International Conference on Advances in Computer-Human Interactions, S. 81-87.

Kruger, H.; Drevin, L. und Steyn, T. (2007).

Email security awareness: A practical assessment of employee behaviour". In: Futcher, L. and Dodge, R. (Hrsg.), Fifth World Conference on Information Security Education, IFIP – International Federation for Information Processing. Boston, MA: Springer, Vol. 237, 2007, S. 33-40.

LeHong, H. & Fenn, J. (2011).

Hype Cycle for Emerging Technologies, 2011.
Abgerufen am 28. Februar 2021 von:
https://www.gartner.com/en/documents/1754719/hype-cycle-for-emerging-technologies-2011

Lombardi, M. (2007).

Authentic Learning for the 21st Century: An Overview. (D. G. Oblinger, Hrsg.)
Abgerufen am 30. April 2020 von
https://www.researchgate.net/publication/220040581_Authentic_Learning_for_the_21st_Century_An_Overview

Luo, R., Brody, R., Seazzu, A. und Burd, S. (2011).

Social Engineering: The Neglected Human Factor for Information Security Management. IRMJ. Vol. 24, No. 3.
DOI: https://doi.org/10.4018/irmj.2011070101

Mandal, H. K. (2020).

Brainstorming Approach And Mind Mapping. In: Synergy Creating Activity, Global Journal of Finance and Management, Vol. 6, No. 4, 2014, S. 333-338.
Abgerufen am 15. Februar 2021 von:
https://www.ripublication.com/gjfm-spl/gjfmv6n4_07.pdf

Marmulla, C. (2020).

Security für KMU – In 12 Schritten zur Informationssicherheit. In: computerwoche online, 2020, Abgerufen am 15. Februar 2021 von: https://www.computerwoche.de/a/in-12-schritten-zur-informationssicherheit,3547543

Meseke, B. und Kuhlee, L. (2019).

Datenklau: virtuelle Gefahr – reale Schäden. Eine Befragung von über 450 deutschen Unternehmen. Abgerufen am 15. Februar 2021 von: https://www.ey.com/de_de/forensic-integrity-services/datenklau-warum-eine-kehrtwende-der-verteidigungsstrategie-gefragt-ist

Mitnick, K. D. und Simon, W. L. (2011).

Die Kunst der Täuschung: Risikofaktor Mensch. Heidelberg: mitp.

Mouton, F.; Malan, M. M.; Leenen, L. und Venter, H. S. (2014).

Social engineering attack framework, Information Security for South Africa (ISSA), Johannesburg, South Africa, IEEE, 2014, S. 1–9.

Nagler, B. (2009).

Rollenspiel. In: Kühl S., Strodtholz P., Taffertshofer A. (Hrsg.) Handbuch Methoden der Organisationsforschung. VS Verlag für Sozialwissenschaften. DOI: https://doi.org/10.1007/978-3-531-91570-8_7

PwC (n.a.).

Risk management leader insights. Latest findings from PwC's Pulse Survey. Abgerufen am 15. Februar 2021 von: https://www.pwc.com/us/en/library/risk-management-leader.html

Rachmah, N. (2020).

Effectiveness of Online vs Offline classes for EFL Classroom: a study case in a higher education. In: Journal of English Teaching, Applied Linguistics and Literatures (JETALL). Vol. 3, No. 1, 2020. DOI: https://doi.org/10.20527/jetall.v3i1.7703

Richter, S., Straub, T. & Lucke, C. (2018).
Information Security Awareness – eine konzeptionelle Neubetrachtung.
Abgerufen am 15. Februar 2021 von:
https://www.researchgate.net/publication/323827248_Information_Security_Awareness_-_eine_konzeptionelle_Neubetrachtung

Romero, M., Usart, M., Ott M., Earp J., De Freitas, S. & Arnab, S. (2012).
Learning Through Playing For Or Against Each Other? Promoting Collaborative Learning. In: Digital Game Based Learning Proceedings of the 20th European Conference on Information Systems (ECIS) (Barcelona: ECIS).

Rumpe, B. (2011).
Sequenzdiagramme. In: Modellierung mit UML. Xpert.press. Berlin, Heidelberg: Springer Berlin Heidelberg, S. 209-228.

Salahdine, F. & Kaabouch, N. (2019).
Social Engineering Attacks: A Survey. Future Internet, 11(4), S.89.
DOI: http://dx.doi.org/10.3390/fi11040089

Schmidt, H.; Gondolf, J und Haufs-Brusberg, P. (2018).
Studie zur Information Security Awareness in kleinen und mittleren Unternehmen (KMU), Hochschule Düsseldorf, Medien, Düsseldorf, 2018.
DOI: https://doi.org/10.20385/2625-3690/2018.1

Schog, C und Pokoyski, D. (2017).
Security Spot – Awareness- und Risk-Management-Assessment für Manager. Anwenderbericht. In: <kes>, Vol. 5, 2017, S. 14-17.
Abgerufen am 15. Februar 2021 von:
http://s522854922.online.de/TSystems.pdf

Scholl, M., Fuhrmann, F., Edich, D., Ehrlich, P., Leiner, B., Scholl, R., & Koppatz, P. (2017).

Das Projekt SecAware4job: Auf spielerischem Weg zu erhöhtem Informationssicherheitsbewusstsein für den Berufseinstieg. In: TH Wildau (Hrsg.), Wissenschaftliche Beiträge 2017, S. 23-30. Wildau.

DOI: https://doi.org/10.15771/0949-8214_2017_3

Schornack, R. G. (1996).

Accelerated learning techniques for adults: An instructional design concept for the next decade. Fourth Annual College of Career Education Faculty Symposium on Teaching Effectiveness: Embry-Riddle Aeronautical University.

Schumacher, S. (2011).

Die psychologischen Grundlagen des Social Engineerings. In: Magdeburger Journal zur Sicherheitsforschung, Vol. 1, 2011, S. 1-26.

Serdyukov, P. (2008).

Accelerated Learning: What is it? In: Journal of Research in Innovative Teaching. Vol. 1, No. 1, 2008, S. 35-59. Abgerufen am 15. Februar 2021 von: http://www.jrit-nu.org/

Stadler, H. (2005).

Intervention durch Forschung. Wege zur Unterstützung der Professionalisierung von Lehrkräften mittels Video. In: Welzel, M., Stadler, H. (Hrsg.), „Nimm doch mal die Kamera!“ Zur Nutzung von Videos in der Lehrerbildung – Beispiele und Empfehlungen aus den Naturwissenschaften. Münster, New York, München, Berlin: Waxmann. 2005, S 171-190.

Tanium (2020).

When the World Stayed Home Cyberattacks increased as Global IT leaders transitioned to a distributed workforce. Abgerufen am 15. Februar 2021 von: https://world-at-home.tanium.com/

Taspinar, B., Schmidt, W. & Schuhbauer, H. (2016).
Gamification in Education: A Board Game Approach to Knowledge Acquisition. In: Procedia Computer Science. Vol. 99, 2016, S. 101-116. DOI: https://doi.org/10.1016/j.procs.2016.09.104

Tsohou, A.; Karyda, M; Kokalakis, S. und Kiountouzi, E. (2012).
Analyzing trajectories of information security awareness, Information Technology & People, Vol. 25, 2012, S. 327-352.

Venus, J. (2007).
Teamspirit. Zur Morphologie der Gruppenfigur. In: Leschke, R., Venus, J. (Hrsg.), Spielformen im Spielfilm. Zur Medienmorphologie des Kinos nach der Postmoderne. Bielefeld: Transcript-Verl. (Medienumbrüche, 22).
Abgerufen am 15. Februar 2021 von:
http://dokumentix.ub.uni-siegen.de/opus/volltexte/2008/361/pdf/spielformen.pdf

von Ameln, F. & Kramer, J. (2015a).
Wie wirken handlungsorientierte Methoden? In: Organisationen in Bewegung bringen. Berlin, Heidelberg: Springer Berlin Heidelberg, S. 15-50.

von Ameln, F. & Kramer, J. (2015b).
Planspiel. In: Organisationen in Bewegung bringen. Berlin, Heidelberg: Springer Berlin Heidelberg, S. 149-179.

Weber, K.; Schütz, A. E. & Fertig, T. (2019).
Grundlagen und Anwendungen von Information Security Awareness: Mitarbeiter zielgerichtet für Informationssicherheit sensibilisieren. Wiesbaden: Springer Viehweg. DOI: https://doi.org/10.1007/978-3-658-26258-7

Wehner, T., Derboven, W. & Dick, M. (2002).
Sensibilisierung - ein zentrales Handlungsfeld im Wissensmanagement. In: Lüthy, W., Wissensma-nagement-Praxis : Einführung, Handlungsfelder und Fallbeispiele, Zürich.

Wilson, M., de Zafra, D., Pitcher, S., Tressler, J., & Ippolito, J. (1998).
Information Technology Security Training Requirements: A Role and Performance-Based Model. NIST Special Publication 800-16 (National Institut of Standards and Technology, Hrsg.) Gaithersburg.
Abgerufen am 15. Februar 2021 von:
https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-16.pdf

Wilson, M. & Hash, J. (2003).
Building an Information Technology Security Awareness and Training Program. NIST Special Publication 800-50. (National Institut of Standards and Technology, Hrsg.) Gaithersburg, Computer Security.
Abgerufen am 15. Februar 2021 von:
http://citadel-information.com/wp-content/uploads/2012/08/nist-sp800-50-building-information-security-awareness-program-2003.pdf

Wu, W. H., Hsiao, H. S., Wu, P. L., Lin, C. H. & Huang, S. H. (2011).
Investigating the learning-theory foundations of learning: A meta-analysis. In: Journal of Computer Assisted Learning. Vol. 28, No. 3, 2011, S. 265-279.
DOI: https://doi.org/10.1111/j.1365-2729.2011.00437.x

Projektmitarbeitende



Margit C. Scholl (Prof. Dr. rer. nat.)

Professorin für Wirtschafts- und Verwaltungsinformatik an der Technischen Hochschule Wildau, Fachbereich Wirtschaft, Informatik, Recht. Sie ist Projektleiterin in diesem Projekt.



Stefanie Gube

Wissenschaftliche Mitarbeiterin und operative Projektleiterin in diesem Projekt.



Peter Koppatz

Wissenschaftlicher Mitarbeiter und zuständig für digitale Anwendungen, Webentwicklung.



Marie Christin Walch

Studentische Mitarbeiterin mit Schwerpunkt Lektorat und digitale Anwendungen.



Denis Edich

Zeitweiliger wissenschaftlicher Mitarbeiter und zuständig für Webentwicklung.

Projektpartner



Dietmar Pokoyski (known_sense)

Im Projekt war known_sense zuständig für die Konzeption und Entwicklung eines analogen spielebasierten Lernszenarios zum Thema Security Risk Management.

Anhang

Umfrage 1 ..... VII-2

Ergebnisse Umfrage 1 ..... VII-11

Umfrage 2 ..... VII-14

Ergebnisse Umfrage 2 ..... VII-21

Feedbackbogen VII-25

Webseite VII-29

Poster zu Social Engineering Theater in Deutsch VII-32

Poster zu Social Engineering Theater in Englisch VII-33

Poster zu Security Risk Roulette in Deutsch VII-34

Poster zu Security Risk Roulette in Englisch VII-35

Zeitungsartikel Märkische Allgemeine (MAZ) VII-36

Impressionen Entwicklung Social Engineering Theater VII-37

Impressionen Entwicklung Security Risk Roulette VII-38

Umfrage 1

Technische Hochschule Wildau
Technical University of Applied Sciences

20% (1/5)

Konzeption und Entwicklung von zwei analogen spielebasierten Lernzenarien für KMU im Projekt "Mittelstand 4.0 - Kompetenzzentrum Stuttgart"

Herzlich Willkommen!

Die TH Wildau entwickelt für das Projekt "Mittelstand 4.0 - Kompetenzzentrum Stuttgart" zwei analoge Lernszenarien. Wir nutzen im Folgenden den Begriff "Lernszenarien" und meinen damit spielebasierte, interaktive Erfahrungen bzw. "Serious Games".
Die Lernszenarien sind inhaltlich ausgerichtet auf:

- Social Engineering für die Zielgruppe produzierendes Gewerbe
- Security Risk Management für die Zielgruppe mittleres Management im produzierenden Gewerbe

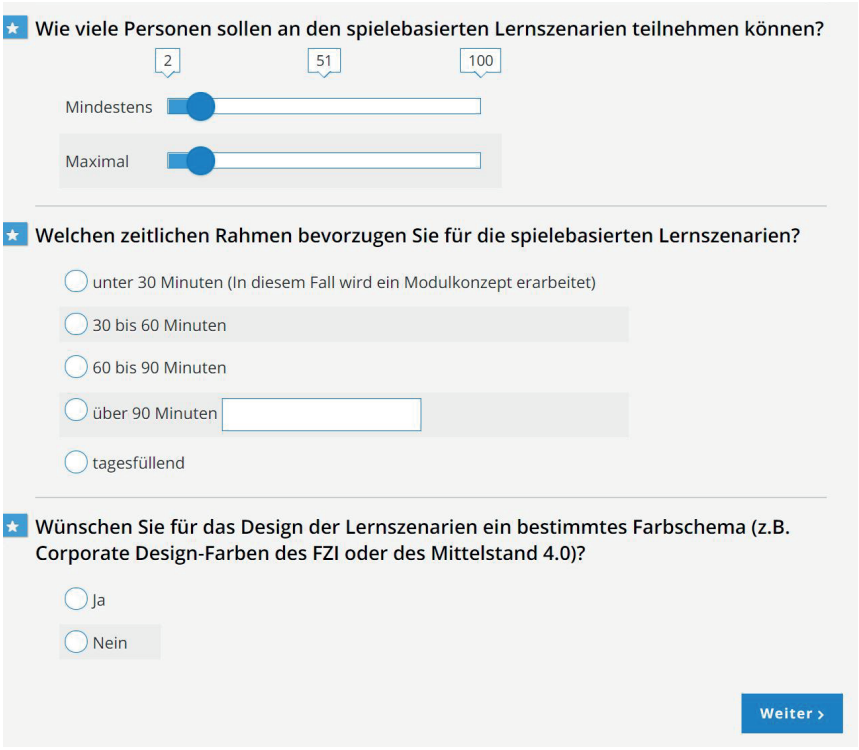
Als Auftakt zur Konzeption und Entwicklung war am 15.04.2020 ein Kreativworkshop zu Social Engineering in Berlin geplant. Wie so oft in diesen Tagen, musste auch diese Veranstaltung abgesagt bzw. auf unbestimmte Zeit verschoben werden. Diese Umfrage soll den ausgefallenen Kreativworkshop ein wenig kompensieren und uns einen Überblick zu Ihren Erwartungen liefern, um den Auftrag weiter konkretisieren zu können.

Sie benötigen für diese Umfrage ca. 20 bis 30 Minuten.
Wir danken Ihnen schon jetzt für die aktive Teilnahme.

Ihr Forschungsteam der TH-Wildau

Werden bereits analoge spielebasierte Lernszenarien (Serious Games) in den vorhandenen "Labs", bei Schulungen oder bei Trainings genutzt?

- ◯ Ja
- ◯ Nein
- ◯ Unbekannt


Wie viele Personen sollen an den spielebasierten Lernszenarien teilnehmen können?
2
51
100
Mindestens
Maximal
Welchen zeitlichen Rahmen bevorzugen Sie für die spielebasierten Lernszenarien?
unter 30 Minuten (In diesem Fall wird ein Modulkonzept erarbeitet)
30 bis 60 Minuten
60 bis 90 Minuten
über 90 Minuten
tagesfüllend
Wünschen Sie für das Design der Lernszenarien ein bestimmtes Farbschema (z.B. Corporate Design-Farben des FZI oder des Mittelstand 4.0)?
Ja
Nein
Weiter ›
Technische Hochschule Wildau
Technical University of Applied Sciences
WILDAU
40% (2/5)
Zielgruppe KMU im produzierenden Gewerbe

Für welche Teilbereiche des produzierenden Gewerbes sehen Sie eine besondere Relevanz der beiden zu entwickelnden Lernszenarien?

- [ ] Automobil
- [ ] Maschinenbau
- [ ] Chemie- und Pharma
- [ ] Stahl
- [ ] Textil- und Bekleidung
- [ ] Sonstige
- [ ] Relevanz für alle Teilbereiche

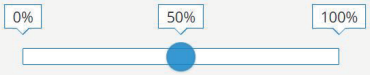
Die nachfolgenden Fragen beziehen sich auf die im Projekt "Mittelstand 4.0 - Kompetenzzentrum Stuttgart" beteiligten KMU.
Wie viele KMU sind im Projekt beteiligt?

- ( ) 0
- ( ) Unbekannt

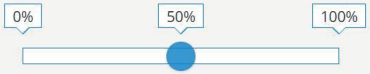
Verwenden KMU im produzierenden Gewerbe mobile Endgeräte?

- ( ) Ja, nur dienstlich
- ( ) Ja, auch privat
- ( ) Nein
- ( ) Unbekannt

Schätzen Sie den Anteil der KMU, die ihren Mitarbeitenden mobile Endgeräte zum Dienstgebrauch zur Verfügung stellen.



Schätzen Sie den Anteil der KMU, in denen Mitarbeitende ihre privaten mobilen Endgeräte für den dienstlichen Gebrauch verwenden (Bring your own device).



Bitte schätzen Sie den Anteil der KMU, ...

	0%	50%	100%
... die Sensibilisierungs- und Schulungskonzepte für Risk Management einsetzen?			
... die Sensibilisierungs- und Schulungskonzepte für Social Engineering einsetzen?			
... die Sensibilisierungs- und Schulungskonzepte in eine Strategie der Geschäftsführung einbinden?			
... in denen Strategien für die Nachhaltigkeit von Sensibilisierungs- und Schulungsmaßnahmen existieren?			

Wird in KMU zwischen Sensibilisierung und Schulung unterschieden?

- ◯ Ja
- ◯ Nein
- ◯ Unbekannt

Wer führt Sensibilisierungen/Schulungen zu Themen der Informationssicherheit in KMU durch?

	Sensibilisierung	Schulung
Externe Berater	☐	☐
Externe Sicherheitsexperten	☐	☐
Interne Sicherheitsbeauftragte	☐	☐
Interne Mitarbeitende (z.B. Admin)	☐	☐
Sonstige	☐	☐

Welche Werkzeuge werden für die Sensibilisierung und Schulung von Mitarbeitenden in KMU eingesetzt?

	wird bereits durchgeführt	Durchführung geplant	wird nicht durchgeführt	unbekannt
Webinar	☐	☐	☐	☐
Lehrvideo	☐	☐	☐	☐
Online-Quiz	☐	☐	☐	☐
Anleitung (z.B. Wiki)	☐	☐	☐	☐
Workshop	☐	☐	☐	☐
Vortrag/Präsentation	☐	☐	☐	☐
Game-based Learning (analog)	☐	☐	☐	☐
Game-based Learning (digital)	☐	☐	☐	☐
Sonstiges	☐	☐	☐	☐

★ **Wird der Lernfortschritt/-erfolg in KMU gemessen?**

- ○ Ja
- ○ Nein
- ○ Unbekannt

★ **Wie informieren KMU ihre Mitarbeiter über notwendige Änderungen (Changemanagement)?**

- ☐ Schulungen
- ☐ Newsletter
- ☐ unterschriftspflichtige Belehrungen
- ☐ Sonstiges

‹ Zurück Weiter ›

Technische Hochschule Wildau
Technical University of Applied Sciences

60% (3/5)

Social Engineering

Der Schwerpunkt für das Lernszenario soll gesetzt werden auf ...

- ◯ Human-based Social Engineering
- ◯ Technical-based Social Engineering
- ◯ Human-based und technical-based Social Engineering

Social Engineering beinhaltet eine Vielzahl von Angriffsvektoren.
Bitte bewerten Sie die Relevanz dieser Angriffsvektoren für die KMU im produzierenden Gewerbe.

Diese Bewertung dient der Schwerpunktsetzung für das Lernszenario Social Engineering.

	sehr relevant	relevant	neutral	wenig relevant	nicht relevant
Pretexting (fingierter Vorwand)	◯	◯	◯	◯	◯
Tailgaiting (Durchschlüpfen)	◯	◯	◯	◯	◯
Soziale Netzwerke	◯	◯	◯	◯	◯
Lauschangriff	◯	◯	◯	◯	◯
Telefon	◯	◯	◯	◯	◯
Innentäter/-in	◯	◯	◯	◯	◯
Baiting (digitaler oder physischer Köder wie z.B. USB-Sticks)	◯	◯	◯	◯	◯
Dumpster Diving (Durchsuchen von Papiertonnen)	◯	◯	◯	◯	◯
Shoulder Surfing	◯	◯	◯	◯	◯
Phishing (Spear-Phishing, Vishing, Clone Phishing, Whaling, Evil Twins)	◯	◯	◯	◯	◯
Malware, Scareware, Spyware	◯	◯	◯	◯	◯
Sonstiges	◯	◯	◯	◯	◯

Welche Social Engineering Angriffe werden als aktive Test-, Simulations- bzw. Schulungsmaßnahme durchgeführt?

- [ ] gezielter Spam-Versand
- [ ] abgelegte USB-Sticks
- [ ] unbefugtes Betreten des Firmengeländes durch Firmenfremde (Tailgaiting = Hindurchschlüpfen)
- [ ] CEO-Fraud-Angriffe
- [ ] Telefonanrufe
- [ ] unbekannt
- [ ] sonstiges

‹ Zurück Weiter ›

Technische Hochschule Wildau
Technical University of Applied Sciences

80% (4/5)

Security Risk Management

Nicht berücksichtige und bewertete elementare Gefährdungen können zu Schäden für ein Unternehmen führen.
Bewerten Sie aus Sicht eines KMU im produzierenden Gewerbe die folgenden elementaren Gefährdungen nach Schadenshöhe bei Eintritt und Eintrittswahrscheinlichkeit.

	Schadenshöhe/ Schadensauswirkung				Eintrittswahrscheinlichkeit			
	vernach-lässigbar	begrenzt	beträcht-lich	existenz-bedrohend	selten	mittel	häufig	sehr häufig
Missbrauch von Berechtigungen	○	○	○	○	○	○	○	○
Identitätsdiebstahl	○	○	○	○	○	○	○	○
Abstreiten von Handlungen	○	○	○	○	○	○	○	○
Missbrauch personenbezogener Daten	○	○	○	○	○	○	○	○
Social Engineering	○	○	○	○	○	○	○	○
Datenverlust	○	○	○	○	○	○	○	○
Integritätsverlust schützenswerter Informationen	○	○	○	○	○	○	○	○

	Schadenshöhe/ Schadensauswirkung				Eintrittswahrscheinlichkeit			
	vernach-lässigbar	begrenzt	beträcht-lich	existenz-bedrohend	selten	mittel	häufig	sehr häufig
Ausspähen von Informationen (Spionage)	○	○	○	○	○	○	○	○
Abhören	○	○	○	○	○	○	○	○
Offenlegung schützenswerter Informationen	○	○	○	○	○	○	○	○
Zerstörung von Geräten oder Datenträgern	○	○	○	○	○	○	○	○
Verstoß gegen Gesetze oder Regelungen	○	○	○	○	○	○	○	○
Unberechtigte Nutzung oder Administration von Geräten und Systemen	○	○	○	○	○	○	○	○
Fehlerhafte Nutzung oder Administration von Geräten und Systemen	○	○	○	○	○	○	○	○

‹ Zurück

Weiter ›


Technische Hochschule Wildau Technical University of Applied Sciences
WILDAU
100% (5/5)
Kleine digitale Ergänzungen
Welche Art der aufgeführten digitalen Ergänzungen bevorzugen Sie für die KMU im produzierenden Gewerbe?
Mehrfachauswahl möglich.
Quiz (Wissensabfrage)
Test mit Zertifikat (Wissensnachweis)
Selbsttest mit weiteren Hinweisen
zusätzliche Informationen zu den Themen Social Engineering und Security Risk Management
Anleitungen
Checklisten
Wiki
digitale Ergänzung als Teil des analogen Lernszenarios
‹ Zurück
Beenden ›

Ergebnisse Umfrage 1

Laufzeit Umfrage	1 Woche 10 h
Besucher	4
Teilnehmeranzahl	1
Datum der Teilnahme	21.04.2020
Beantwortungsdauer	2633s
Laufzeit	43 Minuten 53 Sekunden
Bearbeitungszeit	2h
Beantwortungsquote	85.19% (23 von 27)
Ist Anonymisiert?	Ja
Rücklauf vollständig?	Ja
Endseite gesehen (beendet)	Ja

Nr.	Frage	Antwort
01	Werden bereits analoge spielebasierte Lernszenarien (Serious Games) in den vorhandenen „Labs“, bei Schulungen oder bei Trainings genutzt?	Ja
02	Um welche Art von spielebasierten Lernszenarien handelt es sich?	Brettspiele Kartenspiele
03	Werden diese spielebasierten Lernszenarien vom FZI für Ihre Kunden angepasst?	Ja
04	Wie sind Ihre bisherigen Erfahrungen mit analogen Lernszenarien?	„sehr gut, wird positiv aufgenommen, bringt einen ins Gespräch“
05	Wie viele Personen sollen an den spielebasierten Lernszenarien teilnehmen können?	Mind.: 3 Max.: 30
06	Welchen zeitlichen Rahmen bevorzugen Sie für die spielebasierten Lernszenarien?	60 bis 90 Minuten
07	Wünschen Sie für das Design der Lernszenarien ein bestimmtes Farbschema (z.B. Corporate Design-Farben des FZI oder des Mittelstand 4.0)?	Ja
08	Bitten geben Sie Details zum gewünschten Farbschema an.	„Corporate Design Farben, mindestens neutrales Farbschema mit Logos“
09	Für welche Teilbereiche des produzierenden Gewerbes sehen Sie eine besondere Relevanz der beiden zu entwickelnden Lernszenarien?	Automobil Maschinenbau Chemie- und Pharma
10	Die nachfolgenden Fragen beziehen sich auf die im Projekt „Mittelstand 4.0-Kompetenzzentrum Stuttgart“ beteiligten KMU. Wie viele KMU sind im Projekt beteiligt?	unbekannt
11	Verwenden KMU im produzierenden Gewerbe mobile Endgeräte?	Ja, auch privat
12	Schätzen Sie den Anteil der KMU, die ihren Mitarbeitenden mobile Endgeräte zum Dienstgebrauch zur Verfügung stellen.	-
13	Schätzen Sie den Anteil der KMU, in denen Mitarbeitende ihre privaten mobilen Endgeräte für den dienstlichen Gebrauch verwenden (Bring your own device).	-
14	Bitte schätzen Sie den Anteil der KMU, die Sensibilisierungs- und Schulungskonzepte für Risk Management einsetzen?	-
	Bitte schätzen Sie den Anteil der KMU, die Sensibilisierungs- und Schulungskonzepte für Social Engineering einsetzen?	-

Nr.	Frage	Antwort		
	Bitte schätzen Sie den Anteil der KMU, die Sensibilisierungs- und Schulungskonzepte in eine Strategie der Geschäftsführung einbinden?	-		
	Bitte schätzen Sie den Anteil der KMU, in denen Strategien für die Nachhaltigkeit von Sensibilisierungs- und Schulungsmaßnahmen existieren?	-		
15	Wird in KMU zwischen Sensibilisierung und Schulung unterschieden?	Ja		
16	Wer führt Sensibilisierungen/Schulungen zu Themen der Informationssicherheit in KMU durch?		Sensibilisierung	Schulung
		Externe Berater	X	X
		Externe Sicherheitsexperten	X	X
		Interne Sicherheitsbeauftragte	-	-
		Interne Mitarbeitende (z.B. Admin)	X	-
		Sonstige	-	-
17	Welche Werkzeuge werden für die Sensibilisierung und Schulung von Mitarbeitenden in KMU eingesetzt?	Webinar	unbekannt	
		Lehrvideo	unbekannt	
		Online-Quiz	unbekannt	
		Anleitung (z.B. Wiki)	wird bereits durchgeführt	
		Workshop	wird bereits durchgeführt	
		Vortrag/Präsentation	wird bereits durchgeführt	
		Learning (analog)	unbekannt	
		Learning (digital)	unbekannt	
		Sonstiges	-	
18	Wird der Lernfortschritt/-erfolg in KMU gemessen?	Unbekannt		
19	Wie wird der Lernfortschritt/-erfolg in KMU gemessen?	-		
20	Wie informieren KMU ihre Mitarbeiter über notwendige Änderungen (Changemanagement)?	Schulungen Newsletter		
21	Der Schwerpunkt für das Lernszenario soll gesetzt werden auf ...	Human-based und technical-based Social Engineering		

Nr.	Frage	Antwort		
22	Social Engineering beinhaltet eine Vielzahl von Angriffsvektoren. Bitte bewerten Sie die Relevanz dieser Angriffsvektoren für die KMU im produzierenden Gewerbe.	Pretexting (fingierter Vorwand)	sehr relevant	
		Tailgaiting (Durchschlüpfen)	relevant	
		Soziale Netzwerke	sehr relevant	
		Lauschangriff	neutral	
		Telefon	relevant	
		Innentäter/-in	neutral	
		Baiting (digitaler oder physischer Köder wie z.B. USB-Sticks)	relevant	
		Dumpster Diving (Durchsuchen von Papiertonnen)	relevant	
		Shoulder Surfing	relevant	
		Phishing (Spear-Phishing, Vishing, Clone Phishing, Whaling, Evil Twins)	sehr relevant	
		Malware, Scareware, Spyware	sehr relevant	
		Sonstiges	-	
24	Welche Social Engineering Angriffe werden als aktive Test-, Simulation- bzw. Schulungsmaßnahme durchgeführt?	unbekannt		
25	Nicht berücksichtige und bewertete elementare Gefährdungen können zu Schäden für ein Unternehmen führen. Bewerten Sie aus Sicht eines KMU im produzierenden Gewerbe die folgenden elementaren Gefährdungen nach Schadenshöhe bei Eintritt und Eintrittswahrscheinlichkeit.		Schadenshöhe	Eintrittswahrscheinlichkeit
		Missbrauch von Berechtigungen	beträchtlich	mittel
		Identitätsdiebstahl	beträchtlich	selten
		Abstreiten von Handlungen	begrenzt	mittel
		Missbrauch personenbezogener Daten	begrenzt	sehr häufig
		Social Engineering	beträchtlich	häufig
		Datenverlust	existenzbedrohend	häufig
		Integritätsverlust schützenswerter Informationen	existenzbedrohend	selten
		Ausspähen von Informationen (Spionage)	existenzbedrohend	selten
		Abhören	begrenzt	selten
		Offenlegung schützenswerter Informationen	existenzbedrohend	mittel
		Zerstörung von Geräten oder Datenträgern	existenzbedrohend	selten
		Verstoß gegen Gesetze oder Regelungen	begrenzt	häufig
		Unberechtigte Nutzung oder Administration von Geräten und Systemen	begrenzt	häufig
		Fehlerhafte Nutzung oder Administration von Geräten und Systemen	begrenzt	häufig
27	Welche Art der aufgeführten digitalen Ergänzungen bevorzugen Sie für die KMU im produzierenden Gewerbe?	Quiz (Wissensabfrage) Test mit Zertifikat (Wissensnachweis) Selbsttest mit weiteren Hinweisen		

Umfrage 2

Technische Hochschule Wildau
Technical University of Applied Sciences

25% (1/4)

Konzeption und Entwicklung von zwei analogen spielebasierten Lernzenarien für KMU im Projekt "Mittelstand 4.0 - Kompetenzzentrum Stuttgart"

Herzlich Willkommen!

Die TH Wildau entwickelt für das Projekt "Mittelstand 4.0 - Kompetenzzentrum Stuttgart" zwei analoge Lernszenarien. Wir nutzen im Folgenden den Begriff "Lernszenarien" und meinen damit spielebasierte, interaktive Erfahrungen bzw. "Serious Games".
Die Lernszenarien sind inhaltlich ausgerichtet auf:

- Social Engineering für die Zielgruppe produzierendes Gewerbe
- Security Risk Management für die Zielgruppe mittleres Management im produzierenden Gewerbe

Als Auftakt zur Konzeption und Entwicklung war am 15.04.2020 ein Kreativworkshop zu Social Engineering in Berlin geplant. Wie so oft in diesen Tagen, musste auch diese Veranstaltung abgesagt bzw. auf unbestimmte Zeit verschoben werden. Diese Umfrage soll den ausgefallenen Kreativworkshop ein wenig kompensieren und uns einen Überblick verschaffen.

Sie benötigen für diese Umfrage ca. 30 bis 45 Minuten.
Wir danken Ihnen schon jetzt für die aktive Teilnahme.

Ihr Forschungsteam der TH-Wildau

Werden bereits analoge spielebasierte Lernszenarien (Serious Games) in den vorhandenen "Labs", bei Schulungen oder bei Trainings genutzt?

- ◯ Ja
- ◯ Nein
- ◯ Unbekannt

Weiter ›

Technische Hochschule Wildau
Technical University of Applied Sciences

50% (2/4)

Zielgruppe KMU im produzierenden Gewerbe

Welchen Teilbereich des produzierenden Gewerbes repräsentieren Sie in der AG IT-Sicherheit?

Für welche Teilbereiche des produzierenden Gewerbes sehen Sie eine besondere Relevanz der beiden zu entwickelnden Lernszenarien?

- [ ] Automobil
- [ ] Maschinenbau
- [ ] Chemie- und Pharma
- [ ] Stahl
- [ ] Textil- und Bekleidung
- [ ] Sonstige
- [ ] Relevanz für alle Teilbereiche

Welche Werkzeuge werden für die Sensibilisierung und Schulung von Mitarbeitenden in KMU eingesetzt?

	wird bereits durchgeführt	Durchführung geplant	wird nicht durchgeführt	unbekannt
Print (Poster, Quickguide, Aufkleber, Aufsteller etc.)	☐	☐	☐	☐
Webinar	☐	☐	☐	☐
(Lehr-)Video	☐	☐	☐	☐
Anleitung (z.B. Wiki)	☐	☐	☐	☐
Workshop	☐	☐	☐	☐
Vortrag/Präsentation	☐	☐	☐	☐
Mitarbeiter-Event	☐	☐	☐	☐
Comic/Cartoon	☐	☐	☐	☐
Game-based Learning (analog)	☐	☐	☐	☐
Game-based Learning (digital)	☐	☐	☐	☐
Sonstiges	☐	☐	☐	☐

★ **Wird der Lernfortschritt/-erfolg in KMU gemessen?**

- ◯ Ja
- ◯ Nein
- ◯ Unbekannt

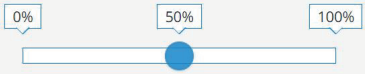
‹ Zurück Weiter ›

Technische Hochschule Wildau
Technical University of Applied Sciences

75% (3/4)

Social Engineering

Bitte schätzen Sie, zu wie viel Prozent die Mitarbeitenden in KMU des produzierenden Gewerbes den Begriff "Social Engineering" kennen.



Welche konkreten Angriffsvektoren verbinden Sie mit der folgenden Definition von Social Engineering?

Definition:
Social Engineering ist eine Form der Manipulation von Menschen, bei der ein Angreifer unter Verwendung gesammelter Informationen und/oder Vortäuschung falscher Tatsachen versucht, unberechtigten Zugang zu vertraulichen Informationen oder IT-Systemen zu erlangen.

Hinweis: Die stichpunktartige Beantwortung ist ausreichend.

Welche konkreten Vorfälle zu Social Engineering, die KMU betreffen, sind Ihnen bekannt?

Mit welchen der von Ihnen in der vorherigen Frage genannten Angriffsvektoren haben Sie persönlich bereits negative Erfahrungen gesammelt?

Social Engineering beinhaltet eine Vielzahl von Angriffsvektoren.
Bitte bewerten Sie die Relevanz dieser Angriffsvektoren für die KMU im produzierenden Gewerbe.

Diese Bewertung dient der Schwerpunktsetzung für das Lernszenario Social Engineering.

	sehr relevant	relevant	neutral	wenig relevant	nicht relevant
Pretexting (= fingierter Vorwand)	◯	◯	◯	◯	◯
Quid pro Quo (= Gegenleistung)	◯	◯	◯	◯	◯
Shoulder Surfing (= "Über die Schulter schauen")	◯	◯	◯	◯	◯
Beobachtung	◯	◯	◯	◯	◯
Belauschen	◯	◯	◯	◯	◯
Tailgaiting (= Durchschlüpfen)	◯	◯	◯	◯	◯
Dumpster Diving (= Durchsuchen von Papiertonnen)	◯	◯	◯	◯	◯
Phishing (Spear-Phishing, Vishing, Clone Phishing, Whaling, Evil Twins)	◯	◯	◯	◯	◯
Malware, Scareware, Spyware	◯	◯	◯	◯	◯
Baiting (digitaler oder physischer Köder wie z.B. USB-Sticks)	◯	◯	◯	◯	◯
Sonstiges	◯	◯	◯	◯	◯

★ **Welche Social Engineering Angriffe werden als aktive Test-, Simulations- bzw. Schulungsmaßnahme für/in KMU durchgeführt?**

- ☐ Phishingsimulation
- ☐ abgelegte USB-Sticks
- ☐ unbefugtes Betreten des Firmengeländes durch Firmenfremde (Tailgaiting = Hindurchschlüpfen)
- ☐ CEO-Fraud-Angriffe
- ☐ Telefonanrufe
- ☐ unbekannt
- ☐ sonstiges

Wozu soll das Lernszenario Social Engineering die Teilnehmenden motivieren?

Mit welchem Verständnis, Wissen, Verhaltensweisen und Fähigkeiten sollen die Teilnehmenden aus dem Lernszenario Social Engineering herausgehen?

‹ Zurück Weiter ›

Technische Hochschule Wildau Technical University of Applied Sciences

100% (4/4)

Security Risk Management

★ Trifft die folgende Definition von Risikomanagement auf die KMU im produzierenden Gewerbe zu?

Definition:
Risikomanagement umfasst alle koodinierten Aktivitäten zur Steuerung und Kontrolle einer Organisation unter Berücksichtigung von Risiken.

- ◯ Ja
- ◯ Nein
- ◯ Uneins

Wie würden Sie diese Definition ergänzen?

Definition:
Risikomanagement umfasst alle koodinierten Aktivitäten zur Steuerung und Kontrolle einer Organisation unter Berücksichtigung von Risiken.

Worauf soll der Fokus beim Lernszenario Security Risk Management gelegt werden?

Worauf soll der Fokus bei der Entwicklung des Lernszenarios hinsichtlich Gefährdungungen durch menschliche Fehlhandlung gesetzt werden?

	Fahrlässigkeit	Vorsatz
Mitarbeitende	☐	☐
Management	☐	☐
Externe Dienstleister (DL)	☐	☐

Wozu soll das Lernszenario Security Risk Management die Teilnehmenden motivieren?

Mit welchem Verständnis, Wissen, Verhaltensweisen und Fähigkeiten sollen die Teilnehmenden aus dem Lernszenario Security Risk Management herausgehen?

‹ Zurück

Beenden ›

Ergebnisse Umfrage 2

Allgemeine Statistik

Die zweite Online-Umfrage richtete sich an die insgesamt 99 Mitglieder der AG IT-Sicherheit. Die Umfrage war 1 Woche und 2 Tage online, beginnend vom 11.05.2020 bis 19.05.2020. Insgesamt besuchten 24 Personen die Umfrageseite, von denen 15 Personen tatsächlich daran teilnahmen und 10 Personen sie auch beendeten. Von den potenziellen 99 Teilnehmern (TN) nahmen dementsprechend knapp 15 Prozent der Mitglieder der AG IT-Sicherheit teil.

Die Teilnahmen konzentrierten sich dabei vor allem auf die ersten beiden Tage sowie den letzten Tag. Am ersten Tag war eine besonders hohe Abbruchquote zu verzeichnen. Als Drop-Out-Ursachen sind die Fragebogenlänge sowie missverständliche Fragestellungen wahrscheinlich. Darüber hinaus gab es keinerlei Möglichkeiten des Motivationseinflusses, weshalb auch mangelnde Motivation als Ursache in Betracht kommt. Der Median der Bearbeitungszeit liegt bei 12 Minuten und 47 Sekunden. Die längste Bearbeitungszeit lag bei 50 Minuten 42 Sekunden und die kürzeste bei 5 Minuten 41. Da die Umfrage viele freie Antwortmöglichkeiten vorsah (insgesamt 12 von 22 Fragen), wurden alle Ergebnisse inklusive der Abbrechenden ausgewertet.

Einstieg (Fragen 1-3)

Die ersten drei Fragen dienten als Einstieg in die Thematik und für das Projektteam als Orientierung bezüglich der Erfahrung/Akzeptanz von spielebasierten Lernszenarien (LS). Von den 15 Teilnehmenden gaben 9 TN (60,00%) an, dass solche nicht bei Schulungen oder Trainings eingesetzt werden. 4 TN (13,33%) ist eine solche Nutzung unbekannt. Bei den 2 übrigen TN, handelte es sich um Brettspiele und ein erlebnisorientiertes, an realen Situationen ausgerichtetes LS, bei dem jeweils sehr positive Erfahrungen gesammelt wurden. Besonders hervorgehoben wurde die bessere Einbindung der TN sowie die Möglichkeit interaktiv Wissen zu erlangen. Aufgrund der geringen Anzahl derer, die Erfahrungen gesammelt haben, lässt sich zwar das Ergebnis nicht pauschalisieren, es deckt sich jedoch mit den Erfahrungen der Forschungsgruppe.

Produzierendes Gewerbe (Fragen 4 - 8)

Für die Umsetzung der geplanten Lernszenarien ist die Adressierung der Zielgruppen ein entscheidendes Kriterium für den Erfolg des Projektes, um effektive Sensibilisierungsmaßnahmen anbieten zu können. Die Umfrage zeigt, dass besonders die Teilbereiche Automobil und Maschinenbau relevant sind, was sehr wahrscheinlich an der in und um Stuttgart angesiedelten Industrien geschuldet ist. Daher ist bei der Entwicklung der Lernszenarien ein besonderer Schwerpunkt auf diese Teilbereiche zu setzen. Unabhängig von dieser zentralen Zielstellung sollten die Maßnahmen einen allgemeinen Einsatz in anderen Branchen nicht ausschließen, denn auch 45,5 % der TN sehen eine Relevanz für alle Teilbereiche des produzierenden Gewerbes.

Um die Einordnung in bereits bekannte Schulungsmethoden vornehmen zu können, wurde auch nach bekannten Schulungskonzepten gefragt. Die Wahl der Methoden entspricht der gängigen Praxis der passiven Wissensvermittlung. Als Schwerpunkte wurden genannt:

- Vorträge, Präsentationen
- Printmedien (Poster, Quickguide, Aufkleber, Aufsteller etc.)
- Webinare

Des Weiteren werden TN auch aktiv in Workshops sensibilisiert bzw. geschult. GBL wird dagegen bisher selten genutzt. Hier würde der Einsatz interaktiver Sensibilisierungsmaßnahmen einen Mehrwert und neue Aspekte für die bekannten Schulungskonzepte ergänzen. Der Lernerfolg der verschiedenen Maßnahmen wird in knapp 64 Prozent der KMU nicht gemessen. Bei den 36 Prozent der KMU, bei denen der Lernerfolg gemessen wird, sind Evaluations- und Feedbackfragebögen das Mittel der Wahl.

Social Engineering (Fragen 5 - 16)

Die Befragten schätzen, dass lediglich 25 Prozent der Mitarbeitenden von KMU den Begriff Social Engineering kennen. Dies ist in der Entwicklung des LS zu berücksichtigen.

Zur Begriffsbestimmung „Social Engineering“ und den dazugehörigen Angriffsarten wurde bei den Mitgliedern der AG-IT-Sicherheit allgemein von einer Kenntnis der Definition und der vollen Bandbreite der Angriffsmöglichkeiten ausgegangen. In Bezug auf die Angriffsvektoren trifft dies jedoch nur teilweise zu, was sich aus den Antworten auf andere Fragen schließen lässt. Am bekanntesten sind wohl Phishing-Attacken und CEO-Fraud. Die Frage nach persönlichen Erfahrungen der Befragten, reduziert sich ebenfalls auf den bekannten Kommunikationskanal E-Mail.

Nach relevanten SE-Angriffsvektoren gefragt, ergeben sich folgende mögliche Schwerpunkte für die Sensibilisierung:

1. Malware, Scareware, Spyware
2. Phishing (bereits in Arena von known_sense enthalten)
3. Baiting (digitaler oder physischer Köder wie z.B. USB-Sticks)
4. Pretexting (= fingierter Vorwand)
5. Beobachtung
6. Belauschen

Als aktive Test-, Simulation-bzw. Schulungsmaßnahmen kamen bereits Baiting-, Phishing- und CEO-Fraud-Simulationen zum Einsatz. 64 Prozent der TN ist jedoch unbekannt, ob solche Maßnahmen in dieser Weise durchgeführt werden.

Die TN sollen vor allem motiviert werden ihr Verhalten zu prüfen und ggf. zu überdenken. Besonders hinsichtlich E-Mail, Webseiten, Telefonanrufen sollen die TN motiviert werden, achtsam und kritisch vorzugehen. Die Frage „Mit welchem Verständnis, Wissen, Verhaltensweisen und Fähigkeiten sollen die Teilnehmenden aus dem Lernszenario Social Engineering herausgehen“ wurde sehr umfangreich geantwortet. Besonders hervorzuheben sind das Erkennen möglicher Social-Engineering-Versuche, Möglichkeiten Social-Engineering-Gefahren einzuschätzen und sie abzuwehren.

Security Risk Management (Fragen 17 - 22)

Die Definition zum Risikomanagement:

»Risikomanagement umfasst alle koordinierten Aktivitäten zur Steuerung und Kontrolle einer Organisation unter Berücksichtigung von Risiken« wurde von 30 Prozent der TN als zu allgemein und generisch eingestuft.

Der Fokus des Lernszenarios zu SRM soll liegen auf:

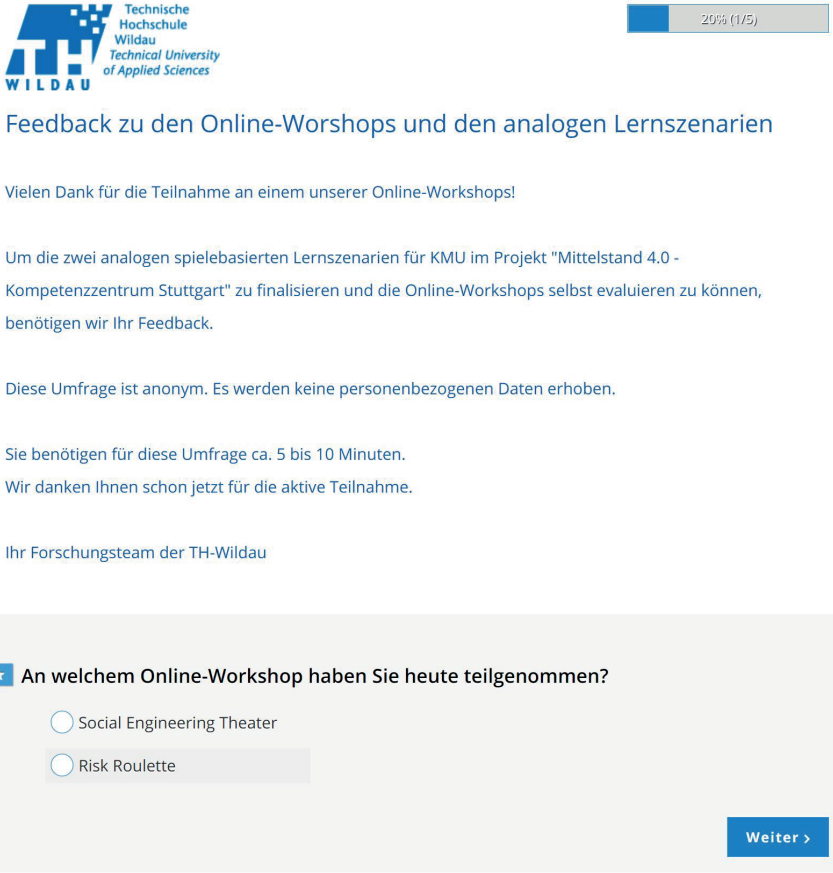
- KMU-spezifische Belange, d. h. vor allem verständlicher Inhalt, ggf. Einsteiger- und Fortsetzungsmodul (nicht so theoretisch wie BSI Standard); wenn Fachbegriffe, dann möglichst deutsch
- resultierenden Vorteile von RM, inklusive der Notwendigkeit finanzielle Mittel dafür einzuplanen
- Risiken beurteilen lernen und Maßnahmen für den Eintrittsfall abzuleiten

Die Umfrage ergibt, dass bei der Gefährdung durch menschliches Fehlverhalten der Fokus auf dem fahrlässigen Fehlverhalten von Mitarbeitern, Führungskräften und Dienstleistern liegen sollte.

Das zu entwickelnde Lernszenario sollte soll die TN vor allem motivieren, sich Risiken anzunehmen und nicht zu ignorieren.

An Verständnis, Wissen, Verhaltensweisen und Fähigkeiten sollen die Teilnehmenden vor allem ein Bewusstsein, ein Abschätzungsvermögen und Bewältigungs-/ Präventionsstrategien für Risiken sowie Handwerkszeug zur Durchführung einer Risikoanalyse mitnehmen. Des Weiteren werden gesetzliche Vorgaben aufgezeigt. In diesem Zusammenhang ist auch das KonTra-Gesetz genannt worden, das in dem Konzept berücksichtigt werden sollte.

Feedbackbogen



Technische Hochschule Wildau
Technical University of Applied Sciences

40% (2/5)

Technisches & Allgemeines

Mit welchem Gerätetyp haben Sie an dem Online- Workshop teilgenommen?

- ◯ Desktop PC
- ◯ Laptop
- ◯ Tablet
- ◯ Smartphone

Haben Sie mit einem Headset an dem Online-Workshop teilgenommen?

- ◯ Ja
- ◯ Nein

Bitte bewerten Sie die folgenden Punkte

	Sehr gut	Gut	Neutral	Schlecht	Sehr schlecht
Qualität der Akustik	◯	◯	◯	◯	◯
Qualiät der geteilten Inhalte	◯	◯	◯	◯	◯
Einbeziehung des Etherpads für die Gruppenarbeit	◯	◯	◯	◯	◯
Technische Einführung zu Webex	◯	◯	◯	◯	◯

Gab es technische Probleme vor oder während des Online-Workshops, die Ihre Teilnahme erschwerten?

- ◯ Ja
- ◯ Nein

Gab es technische Probleme vor oder während des Online-Workshops, die Ihre Teilnahme erschwerten?

- ◯ Ja
- ◯ Nein

Wie lange sollte Ihrer Meinung nach ein Online-Workshop dauern?

	bis 30 Minuten	30 bis 60 Minuten	60 bis 90 Minuten	1,5 bis 3 Stunden	3 bis 6 Stunden	mehr als 6 Stunden
mindestens	◯	◯	◯	◯	◯	◯
maximal	◯	◯	◯	◯	◯	◯

‹ Zurück Weiter ›

Technische Hochschule Wildau Technical University of Applied Sciences

60% (3/5)

Online-Workshop

Bewerten Sie bitte folgende Punkte zur Durchführung des Online-Workshops.

	stimme voll zu	stimme zu	Neutral	nicht immer	stimme nicht zu
Der Inhalt ist zeitlich optimal abgestimmt.	◯	◯	◯	◯	◯
Die Pause war ausreichend.	◯	◯	◯	◯	◯
Das Ziel des Online-Workshops ist klar kommuniziert worden.	◯	◯	◯	◯	◯
Die Aufgabenstellung für die Gruppenarbeit war verständlich und nachvollziehbar.	◯	◯	◯	◯	◯
Ich wurde in den Online-Workshop gut einbezogen.	◯	◯	◯	◯	◯
Der Online-Workshop wurde abwechslungsreich aufgebaut.	◯	◯	◯	◯	◯
Ich nehme viele wichtige Informationen für meinen Berufsalltag aus dem Online-Workshop mit.	◯	◯	◯	◯	◯

Welche konkreten Änderungen würden Sie sich für einen weiteren Online-Workshop wünschen?

‹ Zurück | Weiter ›



80% (4/5)

Lernszenario

Bewerten Sie bitte, inwieweit der Online-Workshop das Prinzip und die Spielmechanik des analogen Lernszenarios adäquat vermitteln konnte.

Sehr gut	Gut	Mäßig	Schlecht	Sehr schlecht
○	○	○	○	○

Welche konkreten Änderungen würden Sie sich für dieses Lernszenario wünschen?

‹ Zurück | Weiter ›



100% (5/5)

Vielen Dank für Ihr Feedback!

Beenden ›

Webseite


HOME
PROJEKT
METHODIK
LERNSZENARIEN
LINKS
TEAM
KONTAKT
DE | EN
Entwicklung von spielebasierten Lernszenarien zu Social Engineering und Security Risk Management im produzierenden Gewerbe
Für das Projekt
»Mittelstand 4.0 – Kompetenzzentrum Stuttgart«
Über das Projekt
Ziel
Im Rahmen des Projekts „Mittelstand 4.0 – Kompetenzzentrum Stuttgart" sollen zwei komplexe analoge Lernszenarien entwickelt und erprobt werden. Diese Lernszenarien werden anschließend in der Arbeitsgruppe IT-Sicherheit des Projekts »Mittelstand 4.0 – Kompetenzzentrum Stuttgart« getestet. Ziel ist es, die Mitarbeitenden von KMU spielerisch für das Thema Informationssicherheit zu sensibilisieren. Für diese Sensibilisierungsmaßnahmen sollen den Kooperationspartnern des Projektes »Mittelstand 4.0 – Kompetenzzentrum Stuttgart« und damit auch den Teilnehmenden der Arbeitsgruppe IT-Sicherheit die beiden erlebnisorientierten Lernszenarien für eigene Veranstaltungen zur Verfügung gestellt werden.
Leistungsgegenstand
Gegenstand des Projekts ist die Konzeption und Entwicklung von zwei komplexen analogen spielebasierten Lernszenarien für KMU mit kleinen digitalen Ergänzungen. Die Lernszenarien sind inhaltlich ausgerichtet auf Social Engineering für die Zielgruppe produzierendes Gewerbe und Security Risk Management für die Zielgruppe mittleres Management im produzierenden Gewerbe.
Auftraggeber
FZI Forschungszentrum Informatik Karlsruhe
Methodik
Game-Based Learning
Game-based Learning erlaubt eine aktive Auseinandersetzung mit den Lerninhalten statt einer passiven Informationsaufnahme (Vortrag, Video, Lesen). Es bietet die Möglichkeit Fehler zu machen sowie zu experimentieren. Lernspiele sind motivationsfördernd und unterstützen die Verhaltensänderung [1]. Wichtig für die Entwicklung und Konzeption sind die zielgruppenspezifischen Ausrichtungen und Anpassung an die Lebenswelt der Zielgruppen. Diese Verbindung zu realen Situationen und Herausforderungen verbessert den Lernerfolg [2].
Analog & Digital
Analog oder digital, was verspricht den besten Erfolg? Der Mix aus analogen und digitalen Anteilen hat sich in vergangenen Forschungsprojekten als vorteilhaft erwiesen [3]. Eine dritte Komponente sollte bei analogen Lernszenarien nicht unterschätzt werden - die Interaktion zwischen den Teilnehmenden - die eine Diskussion und den direkten Erfahrungs- und Meinungsaustausch fördert. Diese kurz skizzierten Aspekte können unter dem Begriff »Authentic-Learning« [4] zusammengefasst werden und sind Teil der Umsetzungsstrategie für unser Projekt.
Transformation
Die »Spirale der transformativen Wechselwirkung« (siehe Abbild) verdeutlicht, wie ausgehend von den Zielen einer Organisation die erfolgskritischen Informationen durch Fortbildung, Information und Sensibilisierung gesichert werden können. Das Ideal der gelebten Sicherheitskultur, die eine Transparenz der Ziele einer Organisation voraussetzt, sollte alle Beschäftigten an den Entscheidungsprozessen beteiligen. Das fördert die Kultur des Teilens, der Zusammenarbeit und des Wissenstransfers in allen Bereichen eines Unternehmens. Die Pfeile am Rand des Spiralbandes verdeutlichen den sich ständig wiederholenden Prozess [5].
Sensibilisierung
Schulung ist von Sensibilisierung zu unterscheiden. Sensibilisierungsmaßnahmen sollen ein Bewusstsein für Informationssicherheit schaffen und den einzelnen Teilnehmenden ermöglichen, die Wichtigkeit der Thematik zu erkennen, ihr eigenes Verhalten zu reflektieren und entsprechend zu reagieren [6]. Eine Schulung hat dagegen das Ziel, tiefergehendes Wissen und Fähigkeiten aufzubauen. Bei der Entwicklung der Lernszenarien geht es vor allem um die Sensibilisierung. Diese soll die Teilnehmenden für die Themen emotionalisieren und motivieren, womit ein Grundstein für eine kontinuierliche Fortbildung gelegt wird.

Lernszenarien

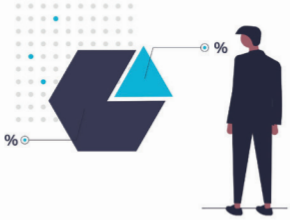


Social Engineering

Das BSI versteht Social Engineering als Methode, welche menschliche Eigenschaften wie z. B. Hilfsbereitschaft, Vertrauen, Angst oder Respekt vor Autorität ausnutzt, um unberechtigten Zugang zu Informationen oder IT-Systemen zu erlangen [7]. Der Begriff Social Engineering wird laut der Studie „Bluff me if U can" häufig mit positiven Assoziationen verbunden [8]. Jedoch ist diese Art der zwischenmenschlichen Manipulation eine der am häufigsten genannten Angriffsarten, von denen Unternehmen in Deutschland in Bezug auf Datendiebstähle, Industriespionage und Sabotage betroffen sind [9].

Je nach Art des Angriffs kann nach technik- und menschlich-basierten Social-Engineering-Angriffen unterschieden werden [10]. Zu den technik-basierten Angriffsarten zählen z.B. Phishing und der Einsatz von Malware, zu den menschlich-basierten Angriffen gehören z.B. Identitätswechsel, Identitätsdiebstahl und Shoulder Surfing (= über die Schulter schauen).

Das zu entwickelnde spielebasierte Lernszenario wird unter Berücksichtigung psychologischer Grundlagen die verschiedenen Aspekte und Facetten des Social Engineering aufgreifen und die Bedürfnisse und Besonderheiten des produzierenden Gewerbes einbeziehen.



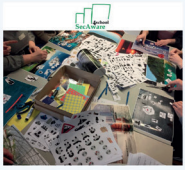
Security Risk Management

Allgemein wird Risikomanagement im ISO Guide 73 als „koordinierte Aktivitäten zur Steuerung und Kontrolle einer Organisation unter Berücksichtigung von Risiken" definiert [11]. Bei Security Risk Management werden entsprechend Informationssicherheitsrisiken berücksichtigt.

Einen Einstieg ins Risikomanagement bietet der BSI Standard 200-3. Dieser Standard gibt unter anderem eine Anleitung zur Ermittlung von Gefährdungen, zur Risikoeinstufung und Behandlung von Risiken, um die Ergebnisse im bestehenden Sicherheitskonzept zu integrieren [12]. Das Thema Management von Informationssicherheitsrisiken wird ebenfalls in der ISO/IEC 27005 behandelt [13].

Das Lernszenario soll das Management von KMU hinsichtlich der grundsätzlichen Wichtigkeit von Risikomanagement und darüber hinaus zu potenziellen Gefährdungen sensibilisieren. Insgesamt soll eine Befähigung erreicht werden, Risikomanagement anzuwenden, Schwachstellen aufzudecken um damit Risiken zu vermeiden, zu reduzieren und gegebenenfalls das Restrisiko zu akzeptieren. Zu Risikomanagement gehört ebenfalls die Kommunikation mit den Sicherheitsbereichen und dem Risk Management. Implizite Intention des Szenarios ist daher auch eine Mediation von Management und Sicherheitsprotagonisten bzw. Risk Management im Sinne eines Kommunikationsbeschleunigers.

Weitere Projekte

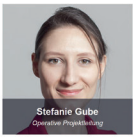




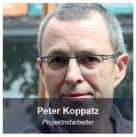


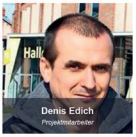
Team













Kontakt

Technische Hochschule Wildau
Fachbereich: Wirtschaft, Informatik, Recht (WIR)
Hochschulring 1
15745 Wildau

Prof. Dr. Margit Scholl
Projektmanagement
+49 3375 508 917
margit.scholl@th-wildau.de
http://www.th-wildau.de/scholl
Haus 100, Raum 106

Stefanie Gube
Operative Projektleitung
+49 3375 508 239
gube@th-wildau.de
Haus 100, Raum U04

Peter Koppatz
Projektmitarbeiter
+49 3375 508 758
koppatz@th-wildau.de
Haus 100, Raum U04

Quellenverzeichnis

[1] Buffum, P. S., Boyer, K. E., Wiebe, E. N., Mott, B. W., & Lester, J. C. (2015).
Mind the Gap: Improving Gender Equity in Game-Based Learning Environments with Learning Companions. In C. Conati, N. Heffernan, A. Mitrovic, & M. F. Verdejo (Hrsg.), Artificial Intelligence in Education: 17th International Conference, AIED 2015, Madrid, Spain, June 22-26, 2015 (S. 64–73). Schweiz: Springer International Publishing. doi:10.1007/978-3-319-19773-9_7

[2] Lombardi, M. (Januar 2007).
Authentic Learning for the 21st Century: An Overview. (D. G. Oblinger, Hrsg.) Abgerufen am 30. April 2020 von https://www.researchgate.net/publication/220040581_Authentic_Learning_for_the_21st_Century_An_Overview

[3] Scholl, M., Fuhrmann, F., Edich, D., Ehrlich, P., Leiner, B., Scholl, R., & Koppatz, P. (2017).
Das Projekt SecAware4job: Auf spielerischem Weg zu erhöhtem Informationssicherheitsbewusstsein für den Berufseinstieg. In TH Wildau (Hrsg.), Wissenschaftliche Beiträge 2017, (S. 23-30). Wildau. doi:https://doi.org/10.15771/0949-8214_2017_3

[4] Great Schools Partnership (Hrsg.). (19. September 2013).
Authentic Learning. Abgerufen am 30. April 2020 von
https://www.edglossary.org/authentic-learning/

[5] Fuhrmann, F., Scholl, M., Edich, D., Koppatz, P., Scholl, L. R., Leiner, K. B., & Ehrlich, E. P. (2017).
Informationssicherheitsbewusstsein für den Berufseinstieg (SecAware4job). Aachen: Shaker Verlag.

[6] de Zafra, D., Pitcher, S., Tressler, J., & Ippolito, J. (1998).
Information Technology Security Training Requirements: A Role and Performance-Based Model.
(National Institut of Standards and Technology, Hrsg.) Gaithersburg.
Abgerufen am 03. Juni 2020 von https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-16.pdf

[7] BSI (Hrsg.). (2020).
IT-Grundschutz-Kompendium. Köln, Bonn: Reguvis Bundesanzeiger Verlag, Bundesanzeiger Verlag. Abgerufen am 30. April 2020 von
IT-Grundschutz-Kompendium, S. 42

[8] known_sense. (2015).
Studie: Bluff me if U can - Gefährliche Freundschaften am Arbeitsplatz, Tiefenpsychologische Wirkungsanalyse Social Engineering und seine Abwehr.
(known_sense, Hrsg.) Köln.
Von http://www.known-sense.de/BluffMeIfUCanAuszug.pdf abgerufen, S. 36

[9] Berg, A., & Niemeier, M. (6. November 2019).
Wirtschaftsschutz in der digitalen Welt. (bitkom, Hrsg.) Abgerufen am 30. April 2020 von
https://www.bitkom.org/sites/default/files/2019-11/bitkom_wirtschaftsschutz_2019_0.pdf, S. 3

[10] Albladi, S. M., & Weir, G. R. (2018).
User characteristics that influence judgment of social engineering attacks in social networkes. (University Strathclyde: Human Centric Computing and Information Science, Hrsg.) Glasgow: SpringerOpen. doi:https://doi.org/10.1186/s13673-018-0128-7, S. 3

[11] Klipper, S. (2015).
Information Security Risk Management: Risikomanagement mit ISO/IEC 27001, 27005 und 31010 (2. Ausg.). Wiesbaden: Springer Fachmedien.
doi:10.1007/978-3-658-08774-6, S.44

[12] BSI (Hrsg.). (2017).
BSI-Standard 200-3: Risikoanalyse auf der Basis IT-Grundschutz. Bonn.
Abgerufen am 05. Mai 2020 von
https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Kompendium/standard_200_3.pdf

[13] Bitkom (Hrsg.). (n.a.).
ISO/IEC 27005. Abgerufen am 05. Mai 2020 von
https://www.kompass-sicherheitsstandards.de/
https://www.kompass-sicherheitsstandards.de/Risikomanagement/ISO-IEC-27005

Mittelstand 4.0 Kompetenzzentrum Stuttgart
digitalLiBW
Mittelstand-Digital
Gefördert durch: Bundesministerium für Wirtschaft und Energie aufgrund eines Beschlusses des Deutschen Bundestages

© Copyright Rapid. All Rights Reserved
Designed by BootstrapMade
Impressum

Poster zu Social Engineering Theater in Deutsch

Mittelstand 4.0 Kompetenzzentrum Stuttgart | #digitalinBW | Mittelstand-Digital | Gefördert durch: Bundesministerium für Wirtschaft und Energie aufgrund eines Beschlusses des Deutschen Bundestages | 30 Jahre 1991 – 2021 | Technische Hochschule Wildau [FH] Technical University of Applied Sciences

» Forschung in Wildau – innovativ und praxisnah «

Lernszenario - Social Engineering Theater

Sensibilisierung für das Thema der zwischenmenschlichen Manipulation





Ziel des Lernszenarios

- Angriffsarten erkennen und für die Abwehr gewappnet sein
- Kommunikationskanäle bewerten und Schutzmaßnahmen ergreifen

Mehrwert

- Lerneffekt durch Praxisbezug und Alltagssituationen
- Unter Berücksichtigung psychologischer Grundlagen die verschiedenen Aspekte und vielfältigen Facetten des Social Engineering aufgreifen
- Einbeziehung der Bedürfnisse und Besonderheiten des produzierenden Gewerbes

https://diz.wildau.biz/

Im Auftrag des FZI Forschungszentrums Informatik
Projektleitung: Prof. Dr. Margit Scholl
Operative Leitung: Stefanie Gube
Technische Leitung: Peter Koppatz
E-Mail: margit.scholl@th-wildau.de
Telefon: +49 (0) 3375 / 508 239

Poster zu Social Engineering Theater in Englisch

Mittelstand 4.0 Kompetenzzentrum Stuttgart | #digitalinBW | Mittelstand-Digital | Gefördert durch: Bundesministerium für Wirtschaft und Energie aufgrund eines Beschlusses des Deutschen Bundestages | 30 Jahre 1991 – 2021 | Technische Hochschule Wildau [FH] Technical University of Applied Sciences

» Research in Wildau – innovative and practical «

Learning Scenario - Social Engineering Theater

Raising awareness of interpersonal manipulation





Aim of the scenario

- Recognize types of attacks and be prepared to defend against them
- Evaluate communication channels and take protective measures

Added value

- Learning is delivered via everyday situations with practical relevance
- Different aspects of social engineering are explored from a psychological perspective
- The needs and characteristics of the manufacturing industry are included

https://diz.wildau.biz/

To act on behalf of FZI Forschungszentrum Informatik
Project management: Prof. Dr. Margit Scholl e-mail: margit.scholl@th-wildau.de
Operational management: Stefanie Gube phone: +49 (0) 3375 / 508 239
Technical management: Peter Koppatz

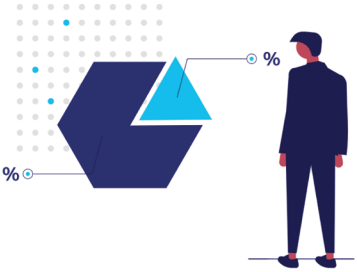
Poster zu Security Risk Roulette in Deutsch

Mittelstand 4.0 Kompetenzzentrum Stuttgart | #digitalinBW | Mittelstand-Digital | Gefördert durch: Bundesministerium für Wirtschaft und Energie aufgrund eines Beschlusses des Deutschen Bundestages | 30 Jahre 1991 – 2021 | Technische Hochschule Wildau [FH] Technical University of Applied Sciences

» Forschung in Wildau – innovativ und praxisnah «

Lernszenario – Security Risk Roulette

Sensibilisierung hinsichtlich der Wichtigkeit von Risikomanagement und potenziellen Gefährdungen





Ziel des Lernszenarios

Befähigung, Risikomanagement anzuwenden, Schwachstellen aufzudecken, um damit Risiken zu vermeiden, zu reduzieren und gegebenenfalls das Restrisiko zu akzeptieren

Mehrwert

- Lerneffekt durch Praxisbezug und Alltagssituationen
- Bedeutung der Notwendigkeit einer umfassenden Kommunikation mit Sicherheitsbereichen und Risikomanagement wird aufgezeigt
- Bedürfnisse und Besonderheiten des produzierenden Gewerbes werden einbezogen

https://diz.wildau.biz/

Im Auftrag des FZI Forschungszentrums Informatik
Projektleitung: Prof. Dr. Margit Scholl
Operative Leitung: Stefanie Gube
Technische Leitung: Peter Koppatz
E-Mail: margit.scholl@th-wildau.de
Telefon: +49 (0) 3375 / 508 239

Poster zu Security Risk Roulette in Englisch

Mittelstand 4.0 Kompetenzzentrum Stuttgart · #digitalinBW · Mittelstand-Digital · Gefördert durch: Bundesministerium für Wirtschaft und Energie aufgrund eines Beschlusses des Deutschen Bundestages · 30 Jahre 1991 – 2021 · Technische Hochschule Wildau [FH] Technical University of Applied Sciences

» Research in Wildau – innovative and practical «

Learning Scenario – Security Risk Roulette

Raising awareness of potential threats and the importance of risk management





Aim of the scenario

Ability to apply risk management and uncover weak points in order to avoid and reduce risks and, if necessary, accept any residual risk.

Added value

- Learning is delivered via everyday situations with practical relevance
- Importance of comprehensive communication with security areas and risk management is shown
- The needs and characteristics of the manufacturing industry are included

https://diz.wildau.biz/

To act on behalf of FZI Forschungszentrum Informatik
Project management: Prof. Dr. Margit Scholl e-mail: margit.scholl@th-wildau.de
Operational management: Stefanie Gube phone: +49 (0) 3375 / 508 239
Technical management: Peter Koppatz

Zeitungsartikel Märkische Allgemeine (MAZ)

Viel gelernt und Spaß dabei

Die MAZ hat bei einem Online-Test eines Projektes der Technischen Hochschule Wildau mitgewirkt

Von Karen Grunow

Wildau. Punkt 10 Uhr wähle ich mich ein in das Online-Meeting, zu dem Stefanie Gube mir bereits vor acht Tagen einen Link nebst Kalendererinnerung per E-Mail zugeschickt hat. Ich darf mitmachen bei einem Online-Workshop der Technischen Hochschule Wildau. Getestet werden soll das „Social Engineering Theater", ein im Auftrag des Forschungszentrums Informatik (FZI) Karlsruhe im Rahmen des Projekts „Mittelstand 4.0 – Kompetenzzentrum Stuttgart" entwickeltes Lernszenario zum Thema Informationssicherheit. Das in dem Bereich sehr versierte Team um TH-Professorin Margit Scholl hat dafür zwei komplexe Lernszenarien entworfen, bei denen nun per Online-Tests der letzte Feinschliff passieren soll.

Stefanie Gube, die operative Projektleiterin, begrüßt alle Teilnehmer, die sich kurz vorstellen. Auch ich sage ein paar Worte, will ja nicht nur stille Beobachterin sein, sondern auf jeden Fall richtig mitwirken. Ich bin gespannt und registriere mit Interesse, von wo die anderen 18 Teilnehmer sich eingewählt haben: von Kompetenzzentren in Saarbrücken, Chemnitz und Stuttgart, außerdem aus Oldenburg, Magdeburg und Berlin. Überdies vom FZI Karlsruhe und vom Fraunhofer Institut für Arbeitswirtschaft und Organisation, bei beiden Institutionen liegt die Leitung des Kompetenzzentrums Stuttgart. Diese bundesweit im Rahmen einer Förderinitiative des Bundesministeriums für Wirtschaft und Energie aufgebauten Zentren stehen mittelständischen Unternehmen und Handwerksbetrieben mit zahlreichen kostenlosen Angeboten bei der Digitalisierung ihrer Prozesse im Betrieb zur Seite.

> Die Lernszenarien sollen dazu anregen, dass man sich austauscht, miteinander diskutiert.
>
> **Stefanie Gube,** TH Wildau

Jene Szenarien entstehen, um auf eine nahezu spielerische Art sämtliche Mitarbeiter einer Firma mit Informationssicherheit vertraut zu machen. „Die Lernszenarien sollen dazu anregen, dass man sich austauscht, miteinander diskutiert", sagt Stefanie Gube. Sie, Peter Koppatz und Julian Bechthold spielen zunächst einen Sketch vor. Geschildert wird eine gar nicht so leicht durchschaubare Situation, wie ein Social Engineer geschickt die Leichtgläubigkeit und Unwissenheit einer Person ausnutzt, um an Firmendaten zu gelangen.

Nun wird die Teilnehmerrunde in drei Gruppen geteilt, Julian Bechthold begrüßt mich und die anderen



Wie ein Social Engineer vorgeht, um an geschützte Informationen zu kommen, vermitteln die Lernszenarien auf spielerische Art. FOTOS: KAREN GRUNOW (2)

unseren kleineren Runde noch einmal herzlich. Ich merke, ich bin etwas unsicher: Was sollen wir jetzt tun? Bechthold wirft Begriffe auf den Bildschirm – Tailgaiting, Baiting, Dumpster Diving. Irgendwas kann ich mir entfernt darunter vorstellen, aber was hat das mit diesem Sketch zu tun? Ich bin etwas ratlos, auch einige der anderen fragen direkt nach. Unser Teamleiter erklärt und zeigt die Begriffskärtchen, auf denen die Worte ebenfalls erläutert werden. Andere Teilnehmer ergänzen, die Diskussion ist also eröffnet, genau so soll es sein, dass alle miteinander ins Gespräch kommen.

Tailgaiting bedeutet, dass jemand versucht, in einen nur für dafür autorisierte Personen zugänglichen Bereich einzudringen; Baiting meint, dass jemand die Neugier anderer auszunutzen versucht, indem er einen Köder – zum Beispiel einen Downloadlink – auswirft. Und beim Dumpster Diving wird gezielt in Papierkörben, aber auch vermeintlich harmlosen Dateien wie Telefonlisten nach verwertbaren Informationen gesucht. Aha. Ich lerne gerade viel über so genannte Social-Engineering-Techniken wie Vortäuschung falscher Identitäten, Manipulation durch Fachjargon, Verunsicherung des Gegenübers, Druck ausüben oder Einschmeichelei. Die im Sketch dargestellte Situation wird entsprechend analysiert und auch, was zum Beispiel unternommen werden sollte, damit so etwas in einem kleinen Betrieb nicht vorfallen kann.

Derweil wir abwägen und diskutieren, passiert in den Gruppen von Stefanie Gube und Peter Koppatz Ähnliches. Nach einer Weile treffen sich alle wieder im großen virtuellen Raum. Die drei TH-Mitarbeiter sind direkt an der Hochschule und agieren dort tatsächlich ganz real in unterschiedlichen Räumen. Technisch klappt das mit den Wechseln, den Präsentationen an realen und virtuellen Tafeln alles erstaunlich gut. Souverän führt Stefanie Gube durch die Veranstaltung.

Nächste Runde, wieder in den kleinen Gruppen. Ein Zeitungsartikel wird eingeblendet: „Aktuelle News: Cyber-Attacke legt Produktion lahm". Als wären wir Kriminalkommissare, versuchen wir nun aufzudröseln, was genau da wie und wann passiert sein muss. Ich merke, ich bin mehr in meinem Metier als beim ersten Lernszenario: Hier gilt es, wichtige Informationen aus einer Meldung zu fischen, auch zwischen den Zeilen zu lesen, den nur sehr knapp geschilderten Zeitablauf zu rekonstruieren, über möglicherweise handelnde Personen nachzudenken. Noch einmal wabert das erschreckende Ergebnis einer Studie des Digitalverbands Bitkom durch den virtuellen Raum: Demnach waren 75 Prozent der Unternehmen in den Jahren 2018 und 2019 von Datendiebstahl, Industriespionage oder Sabotage betroffen. Wir kommen intensiv miteinander ins Gespräch, überlegen gemeinsam, wie jene Cyber-Attacke durchgeführt worden sein kann. Ich merke: Jeder



Stefanie Gube führte als operative Projektleiterin durch den Online-Workshop, bei dem 19 Teilnehmer dabei waren.

von uns geht etwas anders vor, je nach eigenem beruflichen und persönlichen Hintergrund. Mir wird klar: Insbesondere dieses Lernszenario dürfte für Unternehmen spannend sein, da Mitarbeiter beim gemeinsamen Tüfteln die Struktur des eigenen Unternehmens spiegeln. Ich bin begeistert, voll dabei. Adrenalin steigt auch ohne einen Schluck aus dem Kaffeepott, der neben meinem Computer steht.

Nach einigen Minuten schaltet uns Julian Bechthold wieder zurück in die große Runde mit allen Teilnehmern des Online-Workshops. Das Ergebnis: Drei Gruppen, drei völlig verschiedene Wege, die Cyber-Attacke zu rekonstruieren. Und alle sind stimmig. Toll. Mein virtueller Daumen geht hoch.

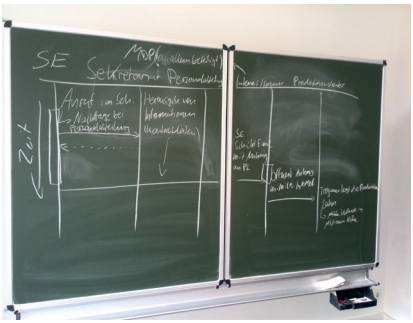
Macht die Reihenfolge Sinn? Wo gibt es Hürden? Sind die Begriffe zu kompliziert? Welche Hilfsmittel sollten Teilnehmer bekommen? Viele Fragen ploppen nun auf, Stefanie Gube und ihre Kollegen sammeln das Feedback, haben noch einen Fragebogen vorbereitet. Bis Ende März soll dann alles abgeschlossen sein.

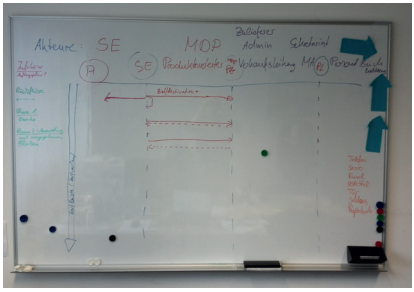
Nach zweieinhalb Stunden, wie vorab geplant, verabschiedet das TH-Team alle. Noch einmal kommt mir in den Sinn, dass die Corona-Situation zwar verhindert, vor Ort an der TH zusammenzusitzen und dort die Tests zu machen. Aber dass durch die Online-Variante Teilnehmer aus allen Teilen Deutschlands dabei waren.

Ich winke in die Kamera und danke und schalte das Webex-Meeting aus. Ich fühle mich euphorisiert, so als hätte ich etwas Tolles erlebt. Dabei saß ich doch „nur" an meinem heimischen Schreibtisch. Es hat eben einfach richtig Spaß gemacht.

Impressionen Entwicklung Social Engineering Theater



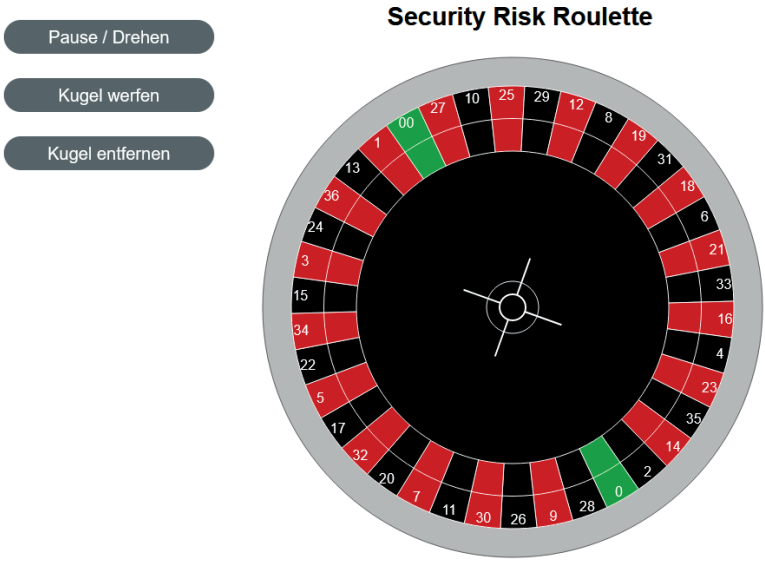








Impressionen Entwicklung Security Risk Roulette

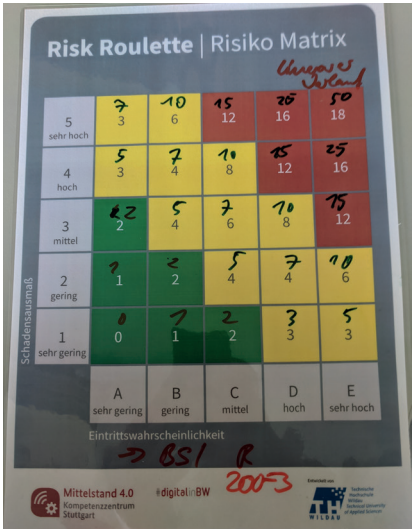


Mittelstand 4.0 Kompetenzzentrum Stuttgart

#digitalinBW

Mittelstand-Digital

Gefördert durch: Bundesministerium für Wirtschaft und Energie aufgrund eines Beschlusses des Deutschen Bundestages





Im Auftrag des FZI Forschungszentrum Informatik entwickelt von

Technische Hochschule Wildau
Technical University of Applied Sciences

https://diz.wildau.biz



Projektlaufzeit: 01.03.2020 - 31.03.2021

ISBN: 978-3-9819225-2-3

Gefördert durch:

Bundesministerium für Wirtschaft und Energie

aufgrund eines Beschlusses des Deutschen Bundestages

Mittelstand-Digital