Moderationsanleitung zu **Social Engineering Theater** und **Security Risk Roulette**

Erlebnisorientierte Lernszenarien 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
WILDAU

Margit Scholl (Hrsg.)

Moderationsanleitung zu **Social Engineering Theater** und **Security Risk Roulette**

Erlebnisorientierte Lernszenarien 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

März 2021

Printed in Germany.

ISBN 978-3-9819225-3-0

Moderationsanleitung zu
Social Engineering Theater und **Security Risk Roulette**

Erlebnisorientierte Lernszenarien für das Projekt

»Mittelstand 4.0-Kompetenzzentrum Stuttgart«

Projektlaufzeit 01.04.2020 - 31.03.2021

Gube, Stefanie

Scholl, Margit (Prof. Dr.)

Koppatz, Peter

Walch, Marie Christin

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

Vorwort & Danksagung

In einer digitalen Welt darf nicht auf analoge Interaktion im Rahmen der Bewusstseinsbildung für mehr Informationssicherheit verzichtet werden.

Die beiden erlebnisorientierten Lernszenarien Social Engineering Theater (SET) und Security Risk Roulette (SRR) sind im Rahmen des Projektes »Mittelstand 4.0 – Kompetenzzentrum Stuttgart« von uns im Auftrag des FZI Forschungszentrum Informatik (FZI) entwickelt und erprobt worden. Ziel ist es, die Mitarbeitenden von kleinen und mittleren Unternehmen (KMU) erlebnisorientiert für das Thema Informationssicherheit zu sensibilisieren. Dieses Buch soll dabei unterstützen, die Lernszenarien erfolgreich einzusetzen. Für einen guten Einstieg in die Moderation finden sich im Teil 3 Zusatzmaterialien wie zum Beispiel ein Glossar.

Das Projektteam dankt der Forschungsgruppe Scholl (FGS) der Technischen Hochschule Wildau (TH Wildau) in der Konstellation 2020/2021 für das konstruktive Feedback und die praktische Unterstützung, insbesondere Ernst-Peter Ehrlich, Hubertus von Tippelskirch, Josephine Gerlach, Julian Bechthold und Regina Schuktomow.

Ein besonderer Dank gilt dem Grafikdesigner Stefan Gensler für die 3D-Animationen sowie Philipp und Valentin für die Hintergrundmusik in SET | Regie.

An dieser Stelle möchten wir dem FZI insbesondere David Ruge, Patrick Seidel, Kerim Zunic und Sabine Schneider für die Zusammenarbeit danken.

Wir danken den Mitgliedern der Arbeitsgruppe IT-Sicherheit, die an unseren Workshops teilgenommen und die Lernszenarien getestet haben. Ihre Anregungen trugen zur Finalisierung der Lernszenarien bei.

Darüber hinaus danken wir unserem Unterauftragnehmer Dietmar Pokoyski (known_sense) für die ideenreiche Unterstützung und die stets gute Zusammenarbeit.

Das Projektteam

Inhalt

Abkürzungsverzeichnis

BSI	Bundesamt für Sicherheit in der Informationstechnik
FGS	Forschungsgruppe Scholl
FZI	Forschungszentrum Informatik
IT	Informationstechnik
ISO	International Organization for Standardization
KMU	Kleinstunternehmen, kleine und mittlere Unternehmen
SET	Social Engineering Theater
SRR	Security Risk Roulette
TN	Teilnehmende

Abbildungsverzeichnis

Social Engineering Theater

Sensibilisierungsmaßnahmen in 3 Akten

TEIL 1:
SOCIAL ENGINEERING THEATER
Sensibilisierungsmaßnahmen in 3 Akten

01

Hintergrund

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) versteht Social Engineering als Methode, welche grundlegende Charaktereigenschaften und Verhaltensmuster wie z. B. Hilfsbereitschaft, Vertrauen, Angst oder Respekt vor Autorität ausnutzt, um unberechtigten Zugang zu Informationen oder IT-Systemen zu erlangen [1]. Der Begriff Social Engineering wird laut der Studie „Bluff me if U can“ häufig mit positiven Assoziationen verbunden [2]. 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 [3].

Je nach Art des Angriffs kann nach technik- und menschlich-basierten Social-Engineering-Angriffen unterschieden werden [4]. Zu den technik-basierten Angriffsarten zählen z. B. Phishing und der Einsatz von Malware. Davon zu differenzieren sind menschlich-basierte Angriffe wie z. B. Identitätswechsel, Identitätsdiebstahl und Shoulder Surfing (= über die Schulter schauen).

Das erlebnisorientierte Lernszenario greift unter Berücksichtigung psychologischer Grundlagen die verschiedenen Aspekte und Facetten des Social Engineerings auf und bezieht die Bedürfnisse und Besonderheiten des produzierenden Gewerbes ein.

Das Lernszenario Social Engineering Theater (SET) ist als Stationenlernen konzipiert. Für die Betrachtung des Themas aus verschiedenen Perspektiven wird das Theater als Metapher verwendet. So wird in den drei Akten (siehe Abbildung 1), die hintereinander durchlaufen werden, sowohl vor als auch hinter die Kulissen geschaut:

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

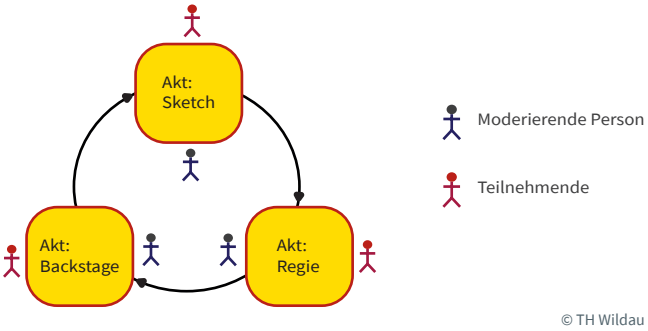


Abbildung 1: SET | Stationenkonzept

Ausgelegt ist das Lernszenario für ca. neun Teilnehmende (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. Es ist zu empfehlen, dass die moderierende Person Kenntnisse zum Thema Social Engineering mitbringt.

Bei bis zu 30 Teilnehmenden ist es möglich, die Gruppe entsprechend in Teams aufzuteilen. Entweder ist das Lernszenario in diesem Fall mehrfach vorhanden oder die Teams durchlaufen das Lernszenario wie ein Zirkeltraining.

TEIL 1:
SOCIAL ENGINEERING THEATER
Sensibilisierungsmaßnahmen in 3 Akten

02

Vorbereitung

Ziel und Zielgruppe

Ziel ist es, die Mitarbeitenden von klein und mittleren Unternehmen (KMU) spielerisch für das Thema Informationssicherheit zu sensibilisieren.

Zeitplanung

Vorbereitung je nach örtlichen Gegebenheiten:	ca. 30 Minuten
Prolog (für alle Teilnehmenden):	ca. 5-15 Minuten
Lernszenario:	**ca. 60-90 Minuten**
pro Szene:	ca. 20-30 Minuten
→ Durchführung:	ca. 15-20 Minuten
→ Auswertung und Nachbereitung:	ca. 5-10 Minuten
Epilog:	ca. 5-15 Minuten

Material

- Material Prolog (siehe Kapitel 3)
- Material Sketch (siehe Kapitel 4)
- Material Regie (siehe Kapitel 5)
- Material Backstage (siehe Kapitel 6)
- Miniglossar (siehe Kapitel 13)

Vom Veranstalter bereitzustellendes Material


Ausreichend großer Raum
(entsprechend der Anzahl der Teilnehmenden)


3 große Tische


Ausreichend Stühle für die Teilnehmenden

Namensetiketten


Große Pinnwand oder Whiteboard


Pinnnadeln oder Magnete


Laptop


Stoppuhr (Smartphone)


Notizzettel und Stifte


Stifte mit wasserlöslicher Farbe wie Whiteboardmarker inklusive Tücher oder Ähnlichem zum Korrigieren und Entfernen von Einträgen

TEIL 1:
SOCIAL ENGINEERING THEATER
Sensibilisierungsmaßnahmen in 3 Akten

03

Prolog

Ziel

Vor Beginn des Lernszenarios sollen die Teilnehmenden die Gelegenheit bekommen, sich mit Hilfe einer Zahnrad-Getriebe-Metapher kurz vorzustellen. Ziel ist es, den Begriff Social Engineering in einer lockeren Atmosphäre zu erörtern.

Material

Der Prolog enthält zehn unterschiedlich farbige Zahnräder, neun für die Teilnehmenden und eins für die Moderation (Beispiel siehe Abbildung 2).

Abbildung 2: SET | Prolog – Zahnrad-Getriebe-Metapher zur Vorstellung

Durchführung

Alle Zahnräder sind an einer großen tragbaren Pinnwand oder einem Whiteboard angebracht. Die Teilnehmenden erhalten die Aufgabe, sich ein passendes Zahnrad im Getriebe auszuwählen und darauf ihren Namen, ihre Funktion im Unternehmen und die Branche des produzierenden Gewerbes (dies entfällt, wenn alle Teilnehmenden dem gleichen Unternehmen angehören) mit einem Whiteboardmarker zu notieren. Im Anschluss stellt sich jeder/jede Teilnehmende den anderen Teilnehmenden kurz vor.

Sie fragen als moderierende Personen in die Runde, was die Teilnehmenden unter Social Engineering verstehen. Nachträglich geben Sie eine kurze Definition:

„Was verstehen Sie unter Social Engineering?“

„Social Engineering ist eine Methode, welche grundlegende Charaktereigenschaften und Verhaltensmuster wie z. B. Hilfsbereitschaft, Vertrauen, Angst oder Respekt vor Autorität ausnutzt, um unberechtigten Zugang zu Informationen oder IT-Systemen zu erlangen [1].“

Anschließend teilen Sie die Gruppe in drei gleich große Teams A, B und C auf. Sie geben nach der Vorstellungsrunde und der Einteilung in Teams einen Ausblick auf die aktive Auseinandersetzung mit unterschiedlichen Aspekten des Social Engineerings in drei Akten.

04

Erster Akt: Sketch
Social Engineering als Rollenspiel

Ziel

Durch anschauliche Darstellung in einem Sketch sollen konkrete Social Engineering Angriffsvektoren nachvollzogen und Fachbegriffe vermittelt werden. Die anschließende Diskussion mit Erfahrungsaustausch fördert die Auseinandersetzung mit der Thematik.

Material

- 1 Spielplan in DIN A0-Format (siehe Abbildung 3)
- 3 x 3 Sketchkarten in DIN A4-Format (Bsp. siehe Abbildung 4)
- 34 Zuordnungskarten in DIN A6-Format + 10 abwischbare Leerkarten (Bsp. siehe Abbildung 5 und 6)
    - 9 + 3 Karten Social Engineering-Techniken
    - 9 + 3 Karten Angriffsvektoren
    - 10 + 2 Karten Schutz- bzw. Gegenmaßnahmen
    - 6 + 2 Karten Kommunikationskanäle

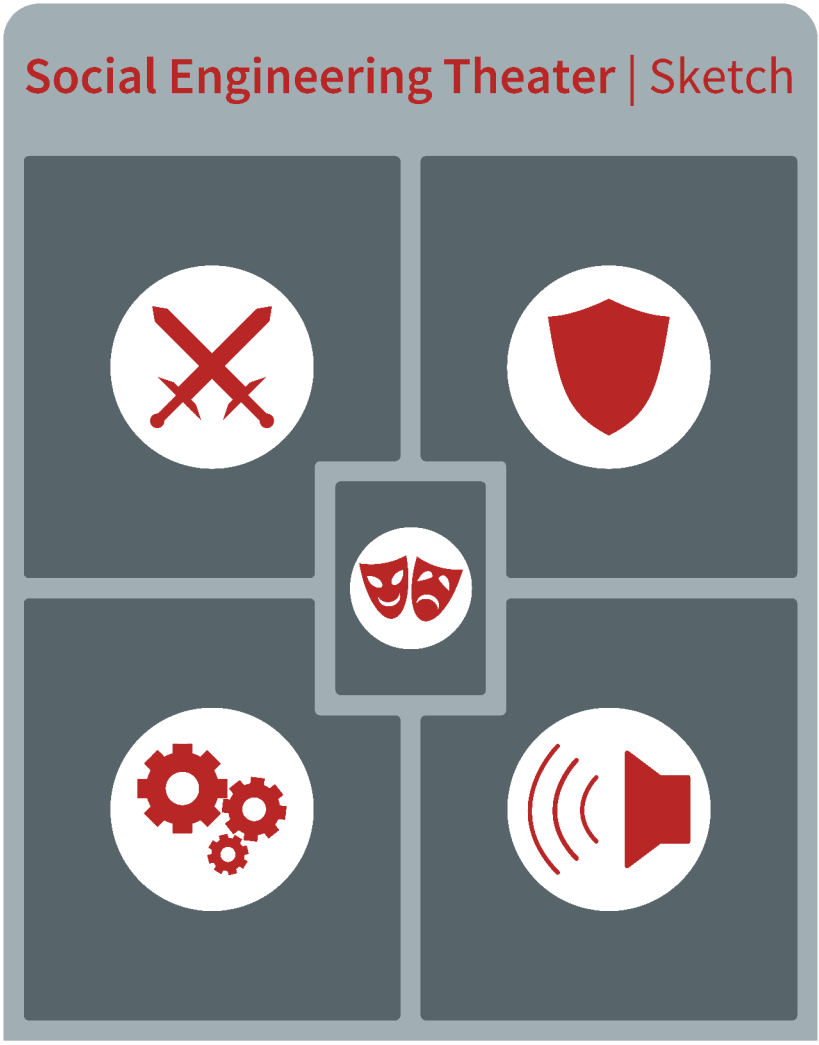


Abbildung 3: SET | Sketch – Spielplan

© TH Wildau

Abbildung 4: SET | Sketch – Beispiel Sketchkarten

© TH Wildau

Abbildung 5: SET | Sketch – Beispiel Zuordnungskarten Vorderseite

Abbildung 6: SET | Sketch – Beispiel Zuordnungskarten Rückseite

Spielvorbereitung

- Der Spielplan wird auf dem Tisch ausgebreitet.
- Die Sketchkarten liegen sortiert auf einem Stapel.
- Alle Zuordnungskarten der jeweiligen Kategorie Angriffsvektoren, Schutzmaßnahmen, Social Engineering-Techniken und Kommunikationskanäle liegen offen auf dem Tisch.

Einleitung

„In dieser Szene geht es um das Kennenlernen verschiedener Social Engineering Angriffsvektoren und Techniken, die von Social Engineers ausgenutzt werden können. Des Weiteren sollen Schutz- bzw. Gegenmaßnahmen erörtert werden. Nachfolgend werden kurze Sketche gespielt oder wahlweise gesprochen.“

Durchführung

Abbildung 7 zeigt schematisch die Durchführung.

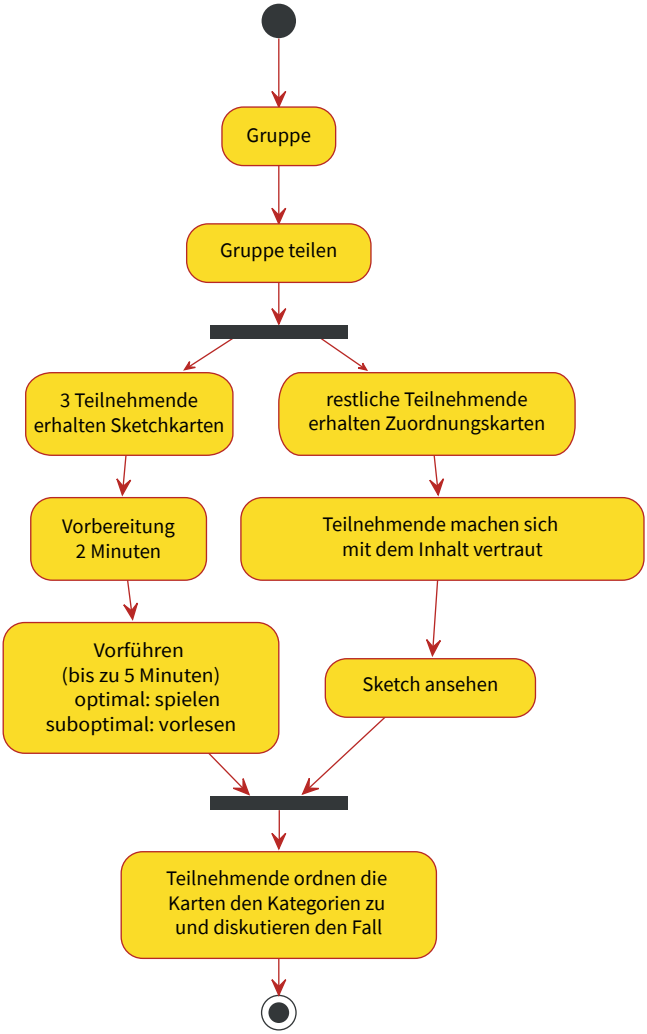


Abbildung 7: SET | Sketch – schematischer Ablauf

- Ein Teammitglied von Team A zieht die zusammengehörigen Sketch-Karten vom Stapel.
- Innerhalb von zwei Minuten berät sich das Team A zur Rollenverteilung und Durchführung.
- Die restlichen Teilnehmenden erhalten die Aufgabenstellung, die offen liegenden Zuordnungskarten zu betrachten und über deren Bedeutung zu diskutieren. Bei Unklarheiten können entsprechende Karten umgedreht werden.
- Nach den zwei Minuten wird der Sketch den restlichen Teilnehmenden vorgestellt (Dauer 2-5 Minuten), welche die entsprechenden Karten zuordnen.
- Im Anschluss können die Teilnehmenden sich über das Gesehene austauschen und diskutieren. Die Zuordnungskarten werden passend zum Sketch auf dem Spielplan platziert. Folgende Fragen sind Teil der Diskussion:
    - Was wurde in der Szene dargestellt?
    - Welche Angriffsvektoren wurden in dem Sketch benutzt?
    - Welche Social Engineering Techniken wurden verwendet?
    - Welche Kommunikationskanäle wurden genutzt?
    - Wie kann man sich dagegen schützen?/
      Wie kann man solche Situationen im Vorfeld vermeiden?
    - Was ist zu tun, wenn eine solche Situation eingetreten ist?
- Im Anschluss wird das Ergebnis fotografisch dokumentiert und der gesamte Vorgang mit Team B und C wiederholt, entweder für weitere zwei Sketche oder bis die verfügbare Zeit vorüber ist.

Auswertung und Nachbereitung

- Im Anschluss werden die Ergebnisse ausgewertet.
- Für jede richtige Zuordnung wird ein Punkt vergeben, für jede falsche Zuordnung abgezogen. Ein Team erhält fünf Zusatzpunkte, wenn sie den Sketch vorspielen statt vorlesen. Die Gesamtpunktzahl wird auf einem Notizzettel für das jeweilige Team notiert.
- Fragen der Teilnehmenden, die noch nicht im Laufe der Szene beantwortet wurden, sollten von Ihnen als moderierende Person (mit Hilfe der Moderationsanleitung) bzw. in der Gruppe beantwortet werden, spätestens jedoch zum Abschluss in großer Runde.

Musterlösung

Die Musterlösung dient der Aufklärung, schließt aber andere mögliche Zuordnungen nicht aus, wenn diese nachvollziehbar begründet werden.

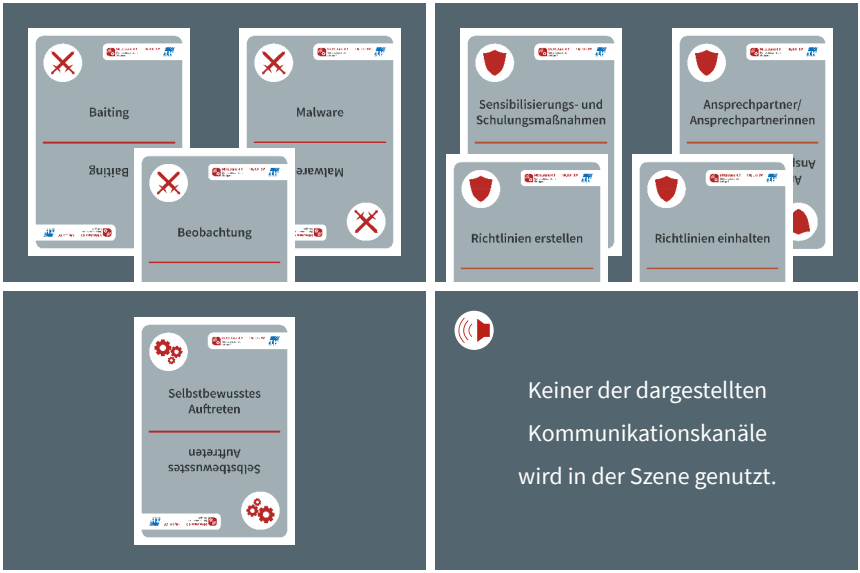
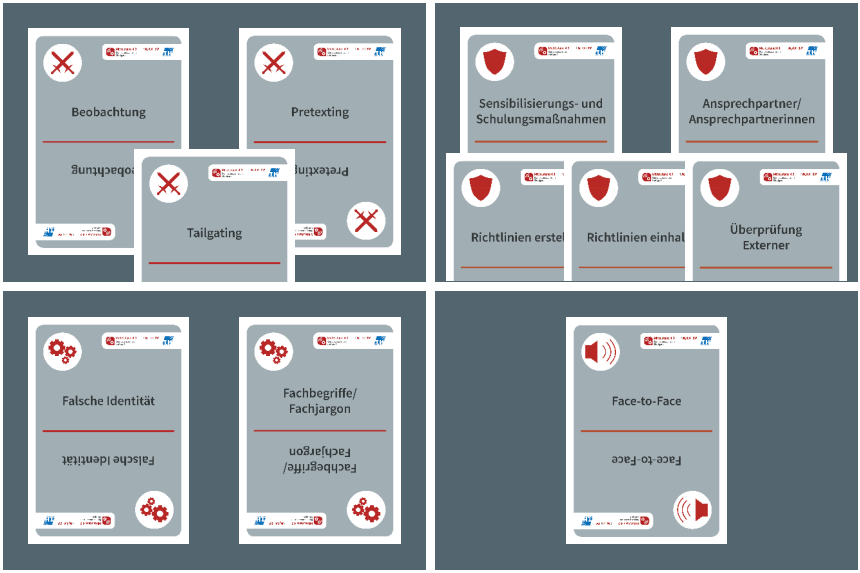


Abbildung 8: SET | Sketch – Musterlösung „Die Parkbank“



© TH Wildau

Abbildung 9: SET | Sketch – Musterlösung „Die Tür“

© TH Wildau

Abbildung 10: SET | Sketch – Musterlösung „Der Anruf“

05

Zweiter Akt: Regie
Handlungsstränge zu Angriffsvektoren

Ziel

Ziel dieses Aktes ist es, dass sich die Teilnehmenden in Situationen gemeinsam entscheiden müssen und zu verschiedenen Angriffsvektoren sensibilisiert werden.

Material

https://diz.wildau.biz/set/regie/index.html

Spielvorbereitung

Dieser Teil des Lernszenarios stellt eine digitale Ergänzung in Form eines Videoquiz dar, für das ein vom Veranstalter bereitzustellender Laptop benötigt wird. Die Gruppe verbleibt in den zu Beginn festgelegten Teams. Als moderierende Person rufen Sie den unter „Material“ angegebenen Link auf.

Durchführung

- Das Videoquiz besteht aus 4 Szenen mit insgesamt 25 kurzen Videosequenzen und einem Abspann.
- Klicken Sie auf den Play Button, um das Videoquiz zu starten und lassen Sie die Teilnehmenden die Sequenzen anschauen.
- Lassen Sie die Teilnehmenden an den jeweiligen Entscheidungspunkten zu einer gemeinsamen Entscheidung kommen. Die Mehrheit entscheidet. Bei einer Pattsituation entscheiden Sie als moderierende Person.
- Am Ende einer Szene folgt jeweils eine Reflexion. Hierfür nutzen Sie entweder den „Reflexionsbutton“ oder diese Moderationsanleitung. Wird die digitale Ergänzung ohne moderierende Person gespielt, ist der Einsatz des „Reflexionsbuttons“ dringend zu empfehlen. Die Fragen sollen die Teilnehmenden zur Diskussion anregen.

Intro

- Die erste Szene ist das Intro zum Videoquiz und enthält keine Entscheidungspunkte.
- Es wird gezeigt, wie eine verdächtige Person in der Papiermülltonne eines Unternehmens wühlt und ein Dokument herauszieht (siehe Abbildung 11).
- Diese Aktion stellt den Angriffsvektor *Dumpster Diving* dar.

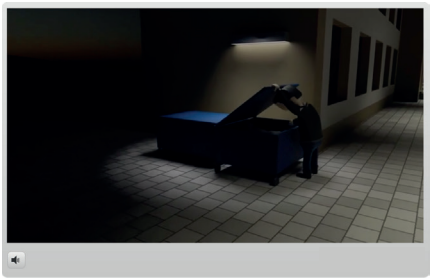


Abbildung 11: SET | Regie – Intro Dumpster Diving

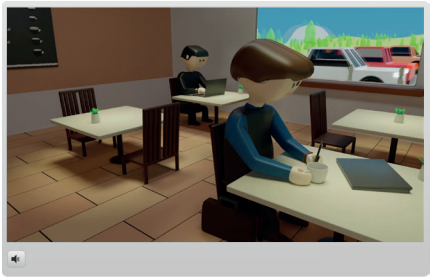
Intro | Reflexion

Folgende Reflexionsfragen sollen zur Diskussion beitragen:

- Wer könnte die Person sein, die im Papiermüll wühlt?
  Ein Mitarbeiter oder eine betriebsfremde Person?
- Wie sollte ich mich gegenüber einer betriebsfremden Person verhalten?
- Was könnte Interessantes im Papiermüll zu finden sein?
- Was darf ich nicht in den Papiermüll werfen?
- Wie kann ich verhindern, dass betriebsfremde Personen Zugriff auf Dokumente erhalten können?
- Wie nennt man diesen Angriffsvektor?

Szene Café

- Die zweite Szene spielt in einem Café gegenüber des im Intro gezeigten und nicht näher bezeichneten Unternehmens (siehe Abbildung 12).



© TH Wildau

Abbildung 12: SET | Regie – Szene Café (Anfang)

- Schmidt ist der Protagonist dieser Szene.
- Er wird von seinem Vorgesetzten angerufen, der ihn bittet, bis 13 Uhr eine Rechnung per E-Mail an die ELMO GmbH zu senden. Dies ist der erste Entscheidungspunkt dieser Szene.
- Die Teilnehmenden müssen entscheiden, ob Schmidt sich die E-Mail-Adresse der ELMO GmbH per E-Mail senden, ansagen oder im Sekretariat geben lässt.

- Entscheiden sich die Teilnehmenden für die ersten beiden Varianten, steht die Frage im Raum, ob Schmidt die E-Mail im Café oder seinem Büro schreibt. Sollten sich die Teilnehmenden für das Café entscheiden, folgt eine Sequenz, in der diese interaktiv agieren müssen, mit dem Ziel die Rechnung per E-Mail zu versenden.
- Hierfür können sie vorab Einstellungen bezüglich *WLAN* und *VPN* vornehmen (siehe Abbildung 13).

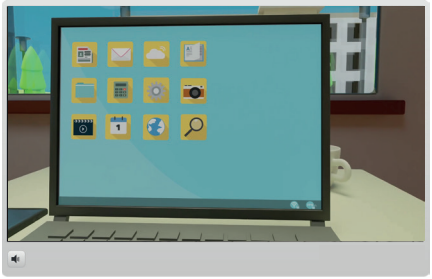


Abbildung 13: SET | Regie – Szene Café (E-Mailversand)

- Daraus ergeben sich folgende Möglichkeiten:
  - *WLAN* an, *VPN* aus (Voreinstellung):
    Social Engineer greift Schmidts E-Mail ab.
  - *WLAN* an, *VPN* an:
    E-Mail kann vom Social Engineer nicht abgefangen werden. (Der Social Engineer muss nun andere Wege nutzen, um an sein Ziel zu gelangen).
  - *WLAN* aus, *VPN* aus:
    E-Mail kann nicht versendet werden. Ein Weiterkommen ist nicht möglich.
  - *WLAN* aus, *VPN* an:
    Diese Kombination ist nicht möglich, da *VPN* eine Internetverbindung voraussetzt.

Merken Sie als moderierende Person, dass die Teilnehmenden nicht weiterkommen, verhelfen Sie ihnen mit gezielten Fragen zur eigenen Antwort.

Szene Café | Reflexion

Folgende Reflexionsfragen sollen zur Diskussion beitragen:

- Wie gehe ich mit eingehenden privaten und/oder beruflichen Anrufen um, wenn ich mich in der Öffentlichkeit befinde?
- Welche Sicherheitsvorkehrungen kann ich ergreifen, wenn ich mobil arbeite (z. B. in einem Café, im Hotel, in der Bahn, auf dem Flughafen)?
- Welche Angriffsvektoren und/oder Social Engineering Techniken wurden in der Szene verwendet?

Szene USB-Stick

- In dieser Szene findet Schmidt auf dem Rückweg zum Büro einen USB-Stick (siehe Abbildung 14).

© TH Wildau

Abbildung 14: SET | Regie – Szene USB-Stick

- Die Teilnehmenden müssen sich entscheiden, ob Schmidt diesen im Sekretariat abgibt oder behält.
- Fällt die Entscheidung auf die Abgabe im Sekretariat, können die Teilnehmenden die Sekretärin eine IT-Mitarbeiterin anrufen oder den USB-Stick von ihr selbst ausprobieren lassen.

- Wird der USB-Stick entweder von Schmidt oder der Sekretärin selbst getestet, installiert sich im Hintergrund Spyware.
- Wird dagegen der USB-Stick von der IT-Mitarbeiterin in einer Quarantäneumgebung getestet, wird die Spyware entdeckt.

Szene USB-Stick | Reflexion

Folgende Reflexionsfragen sollen zur Diskussion beitragen:

- Welche Angriffsvektoren kamen in der Szene zum Einsatz?
- Wie gehe ich mit einem geschenkten oder gefundenen USB-Stick um?
- Sind mir solche Methoden bereits im digitalen Raum begegnet?

Szene Rechnungseingang

- In der letzten Szene erhält der Buchhalter entsprechend der vorhergetroffen Entscheidungen der Teilnehmenden entweder zwei E-Mails mit Rechnungsanhang oder nur eine (siehe Abbildung 15).
- Erhält er zwei E-Mails, können sich die Teilnehmenden entscheiden zwischen:
    - E-Mail-Anhang öffnen und Betrag überweisen
    - E-Mail prüfen, Anhang öffnen und Betrag überweisen
    - Schmidt anrufen
- Erhält er nur eine E-Mail, was bedeutet, dass der Social Engineer Schmidts E-Mail abgefangen hat, können sich die Teilnehmenden nur zwischen den ersten beiden Optionen entscheiden.
- Die Szene endet entweder mit dem Erfolg oder Misserfolg des Social Engineers.

Szene Rechnungseingang | Reflexion

- Welche Angriffsvektoren wurden in der Szene verwendet?
- Woran kann ich verdächtige E-Mails erkennen?
- Wie gehe ich mit verdächtigen E-Mails um?

© TH Wildau

Abbildung 15: SET | Regie – Szene Rechnungseingang

Auswertung und Nachbereitung

- Für die Wahl bestimmter Handlungsstränge erhalten die Teilnehmenden Punkte, die auf Notizzetteln notiert werden.
- Es können maximal 9 Punkte erreicht werden.
- Einen Zusatzpunkt gibt es für das Team, welchem aufgefallen ist, dass der Social Engineer zwei Uhren trägt.
- Je nach zeitlicher Kapazität besteht die Möglichkeit, sich verschiedene alternative Handlungsstränge anzuschauen, auszuwerten und zu diskutieren.

Szene Café

Entscheidung	Option	Punkte
Entscheidung 1	Er bittet um das Zusenden der E-Mail-Adresse	1
	Er bittet um das Ansagen der E-Mail-Adresse	0
	Er lässt sich die E-Mail-Adresse im Sekretariat geben	2
Entscheidung 2	Pause abbrechen	1
	E-Mail im Café schreiben	0
Entscheidung 3	WLAN an und VPN an	1
	WLAN an, aber VPN aus	0

Szene USB-Stick

Entscheidung	Option	Punkte
Entscheidung 4	USB-Stick im Sekretariat abgeben	1
	USB-Stick behalten	0
Entscheidung 5	IT-Mitarbeiterin anrufen	1
	USB-Stick testen	0

Szene Rechnungseingang

Entscheidung	Option	Punkte
Entscheidung 6	E-Mail-Anhang öffnen und Betrag überweisen	0
	E-Mail prüfen, Anhang öffnen und Betrag überweisen	1
	Schmidt anrufen	2

Musterlösung

Aus den Reflexionsfragen ergibt sich folgende Musterlösung:

Intro | Reflexion

- *Wer könnte die Person sein, die im Papiermüll wühlt?*
  - → Es handelt sich sehr wahrscheinlich um eine betriebsfremde Person. In jedem Fall ist diese jedoch sehr suspekt.
- *Wie sollte ich mich gegenüber einer (betriebsfremden) Person verhalten?*
  - → Freundlich, aber bestimmt ansprechen und nach einem Mitarbeiter- oder Besucherausweis fragen.
  - → Kann sich die Person nicht ausweisen, unbekannte Person zur Zielperson oder Empfang geleiten.
- *Was könnte Interessantes im Papiermüll zu finden sein?*
  - → Dokumente, die Details preisgeben zu:
    - der eigenen Person,
    - dem Unternehmen,
    - Kunden,
    - Lieferanten etc.
- *Was darf ich nicht in den Papiermüll werfen?*
  - → Alle Dokumente, die personenbezogene Daten enthalten oder unternehmensinterne Informationen preisgeben.
- *Wie kann ich verhindern, dass betriebsfremde Personen Zugriff auf Dokumente erhalten können?*
  - → Dokumente nicht offen liegen lassen und wegschließen.
  - → Dokumente nicht in den Papierkorb werfen, sondern direkt schreddern oder in Datentonne werfen.
- *Wie nennt man diesen Angriffsvektor?*
  - → *Dumpster Diving*

Szene Café | Reflexion

- *Wie gehe ich mit eingehenden privaten und/oder beruflichen Anrufen um, wenn ich mich in der Öffentlichkeit befinde?*
  - → Keine persönlichen oder beruflichen Details preisgeben.
  - → Anrufenden ggf. auf späteren Zeitpunkt vertrösten.
- *Welche Sicherheitsvorkehrungen kann ich ergreifen, wenn ich mobil arbeite (z. B. in einem Café, im Hotel, in der Bahn, auf dem Flughafen)?*
  - → Sicht auf Laptop vor anderen Personen schützen (z. B. mit Hilfe einer Sichtschutzfolie).
  - → Kein öffentliches WLAN nutzen, sondern immer das firmeneigene VPN.
  - → USB-Ladestationen vermeiden, da diese manipuliert sein und Geräte daran vergessen werden können. Stattdessen Induktionsladung bzw. eigenes Ladegerät oder Powerbanks nutzen.
- Welche Angriffsvektoren wurden in der Szene verwendet?
  - → Beobachtung, Belauschen
  - → *Pretexting* (Anruf Sekretärin)
  - → *Spear-Phishing*

Szene USB-Stick | Reflexion

- *Welche Angriffsvektoren kamen in der Szene zum Einsatz?*
  - → *Baiting*
- *Wie gehe ich mit einem geschenkten oder gefundenen USB-Stick um?*
  - → In einer Quarantäneumgebung von dem/der IT-Mitarbeitenden testen lassen oder sachgerecht entsorgen.

Szene Rechnungseingang | Reflexion

- *Welche Angriffsvektoren wurden in der Szene verwendet?*
  - → *Spear-Phishing*
- *Woran kann ich verdächtige E-Mails erkennen?*
  - → Rechtschreibung, Grammatik
  - → Verdächtiger Absender
  - → Dringlichkeit, Drohung
  - → Verdächtiger Anhang
  - → Unpersönliche Anrede
  - → Aufforderung, einem Link zu folgen
  - → Aber Achtung: Gerade bei Spear-Phishing investieren die Angreifer viel Zeit, weshalb diese E-Mails besonders schwer zu entlarven sind.
- *Wie gehe ich mit verdächtigen E-Mails um?*
  - → Sender mit Hilfe einer Suchmaschine überprüfen.
    Ggf. weitere Überprüfung der Suche mittels Anruf
    (Achtung: Nicht direkt die Kontaktdaten in der E-Mail nutzen!)
  - → Bei eindeutigen Fällen von Phishing-Mails E-Mails gleich löschen und IT-Administration über Vorfall informieren.

06

Dritter Akt: Backstage
Der Blick hinter die Kulissen von Social Engineering

Ziel

In diesem Akt sollen sich die Teilnehmenden anhand einer fiktiven Story in Social Engineers versetzen und deren Herangehensweise nachvollziehen. Die Grundlage bildet das Social Engineering Attack Framework von Mouton et. al. [5].

Material

- 1 Spielplan (siehe Abbildung 16)
- 1 Beispiel Sequenzdiagramm (siehe Abbildung 17)
- 3 x 1 abwischbarer, fiktiver Zeitungsartikel (siehe Abbildung 18)
- 16 abwischbare Akteurs-/Objektkarten
- 20 abwischbare, vorwärtsgerichtete Aktionskarten
- 20 abwischbare, rückwärtsgerichtete Aktionsarten
- 4 abwischbare, selbstgerichtete Aktionskarten

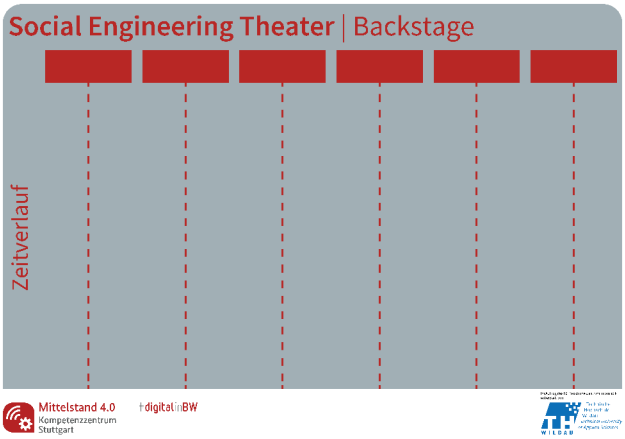


Abbildung 16: SET | Backstage – Spielplan

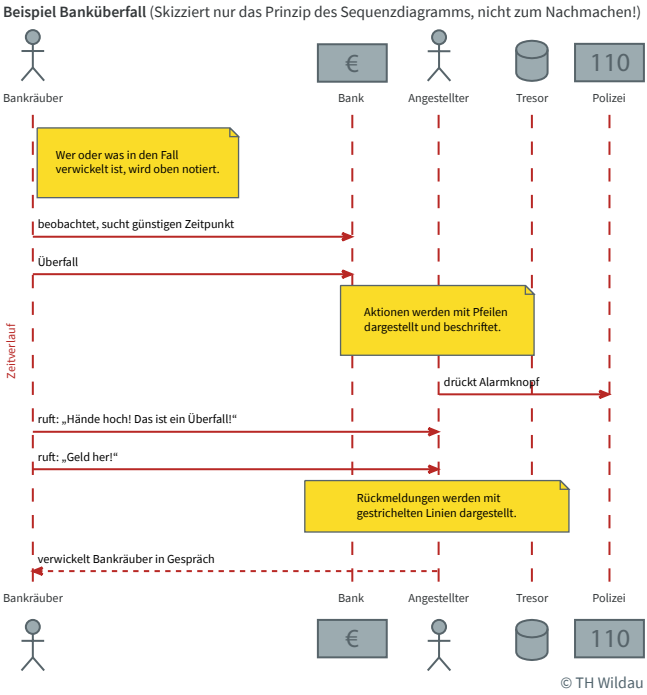
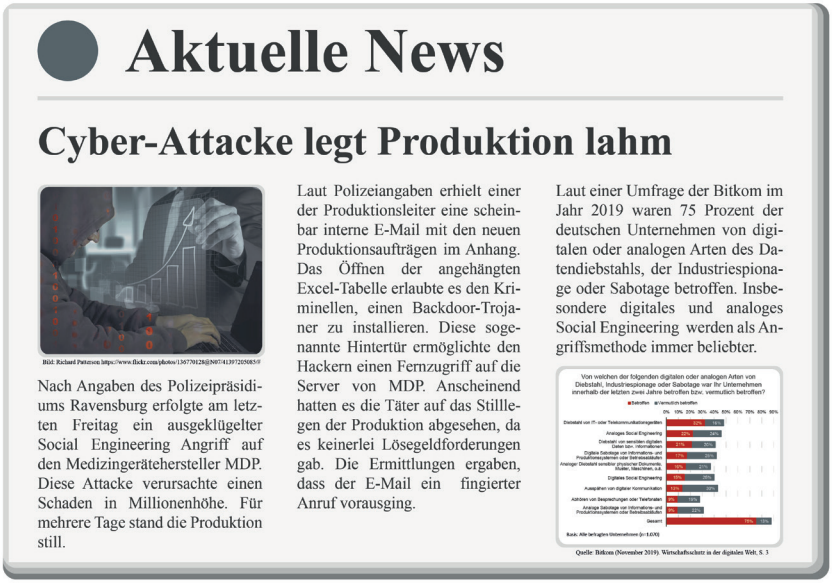


Abbildung 17: SET | Backstage – Beispiel Sequenzdiagramm



Aktuelle News

Cyber-Attacke legt Produktion lahm

Nach Angaben des Polizeipräsidiums Ravensburg erfolgte am letzten Freitag ein ausgeklügelter Social Engineering Angriff auf den Medizingerätehersteller MDP. Diese Attacke verursachte einen Schaden in Millionenhöhe. Für mehrere Tage stand die Produktion still.

Laut Polizeiangaben erhielt einer der Produktionsleiter eine scheinbar interne E-Mail mit den neuen Produktionsaufträgen im Anhang. Das Öffnen der angehängten Excel-Tabelle erlaubte es den Kriminellen, einen Backdoor-Trojaner zu installieren. Diese sogenannte Hintertür ermöglichte den Hackern einen Fernzugriff auf die Server von MDP. Anscheinend hatten es die Täter auf das Stilllegen der Produktion abgesehen, da es keinerlei Lösegeldforderungen gab. Die Ermittlungen ergaben, dass der E-Mail ein fingierter Anruf vorausging.

Laut einer Umfrage der Bitkom im Jahr 2019 waren 75 Prozent der deutschen Unternehmen von digitalen oder analogen Arten des Datendiebstahls, der Industriespionage oder Sabotage betroffen. Insbesondere digitales und analoges Social Engineering werden als Angriffsmethode immer beliebter.

Quelle: Bitkom (November 2019). Wirtschaftsschutz in der digitalen Welt. S. 3

Abbildung 18: SET | Backstage – fiktiver Zeitungsartikel

Spielvorbereitung

- Der Spielplan wird auf dem Tisch ausgebreitet.
- Die Zeitungsartikel und das Beispiel eines Sequenzdiagramms liegen daneben.
- Alle Akteurs-/Objektkarten und Aktionskarten liegen stapelweise ebenfalls neben dem Spielplan.

Je nach Gruppengröße können die Teilnehmenden wie beim Sketch in kleinere Teams aufgeteilt werden. Als zusätzliche Spielpläne kann ein Whiteboard oder eine Tafel dienen.

Durchführung

- Als moderierende Person erläutern Sie kurz die wichtigsten Schritte und erklären das Prinzip eines Sequenzdiagramms anhand des Beispiels „Banküberfall“.
- Die Teilnehmenden erhalten den Zeitungsartikel und lesen sich diesen durch oder laut vor.
- Dabei sollen sie mit abwischbaren (Whiteboard-)Markern die im Zeitungsartikel erwähnten Akteure und Objekte sowie alle ablaufenden Aktionen markieren.
- Im nächsten Schritt sollen die Teilnehmenden die für sie relevanten Akteure und Objekte auf den roten Platzhaltern des Spielplans platzieren. Für Akteure und/oder Objekte, die ihrer Meinung nach fehlen, können die Teilnehmenden die Leerkarten nutzen.
- Anschließend sollen die Aktionskarten beschriftet und zeitlich geordnet auf dem Spielplan platziert werden.
- Weisen Sie ggf. darauf hin, dass der Zeitungsartikel nur einen Ausschnitt zeigt.
- Alle unklaren Dinge können von den Teilnehmenden selbst definiert werden.

Der Schwierigkeitsgrad kann erhöht werden, wenn die vorgegebenen Akteurs-/Objektkarten nicht verwendet werden. Stattdessen ist die Rückseite offen auszulegen.

Auswertung und Nachbereitung

- Für die Auswertung stellen sich die Teams das Vorgehen gegenseitig vor und diskutieren die Nachvollziehbarkeit.
- Hierfür gibt es jeweils Punkte:
    - 1 Punkt für nachvollziehbare Akteure und Objekte
    - 1 Punkt für nachvollziehbare Aktionen
    - 1 Punkt für nachvollziehbare Verbindung zwischen Akteuren/Objekten und Aktionen im zeitlichen Verlauf

- Die Punkte werden von den anderen Teams vergeben. Bei Uneinigkeit entscheiden Sie als moderierende Person.
- Abschließend sollen die Teilnehmenden erörtern, durch welche Schutz- bzw. Gegenmaßnahmen die Vorgehensweise der Social Engineers verhindert werden können (siehe auch Kapitel 7).

Musterlösung

Eine mögliche Lösung zeigt Abbildung 19:

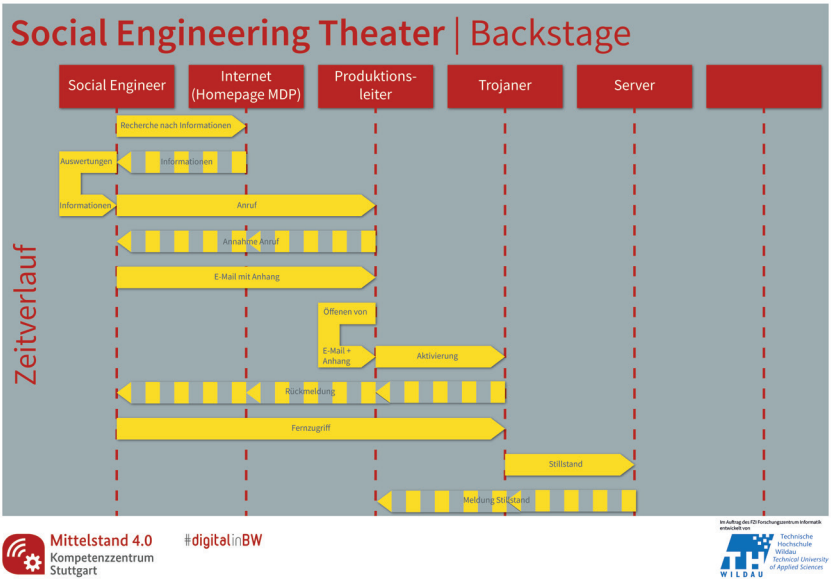


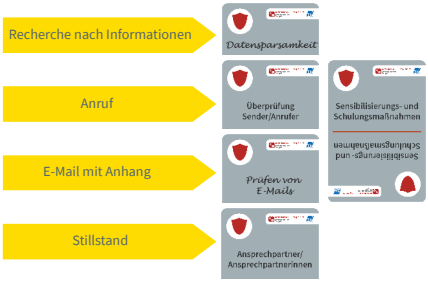
Abbildung 19: SET | Backstage – Musterlösung

07

Epilog

Der Epilog kann dazu genutzt werden, den dritten Akt Backstage hinsichtlich möglicher Schutz- bzw. Gegenmaßnahmen mit Hilfe der Zuordnungskarten aus Sketch zu erörtern.

Anhand der Musterlösung aus dem Akt Backstage könnte sich dann folgendes Bild ergeben:

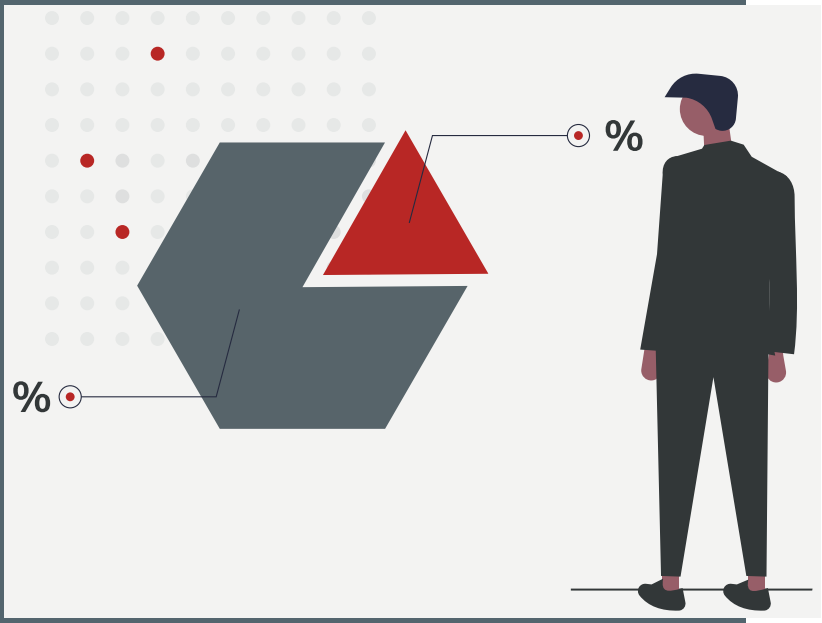


© TH Wildau

Abbildung 20: SET | Epilog – Kombination Sketch mit Backstage

Der Abschluss der Sensibilisierungsveranstaltung sollte von Ihnen genutzt werden, um das Erlebte kurz Revue passieren zu lassen und ein Feedback der Teilnehmenden zumindest mündlich einzuholen, um spätere Veranstaltungen optimieren zu können.

Security Risk Roulette
Ein Planspiel für Risikomanagement in der Informationssicherheit



TEIL 2:
SECURITY RISK ROULETTE
Ein Planspiel für Risikomanagement in der Informationssicherheit

08

Hintergrund

Allgemein wird Risikomanagement im ISO Guide 73 als „koordinierte Aktivitäten zur Steuerung und Kontrolle einer Organisation unter Berücksichtigung von Risiken“ definiert [6]. 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 [7].

Security Risk Roulette (SRR) ist ein erlebnisorientiertes Lernszenario zum Thema Risikomanagement in der Informationssicherheit mit Zielgruppen-Schwerpunkt KMU des produzierenden Gewerbes. Das Planspiel stellt einen Kommunikationsbeschleuniger dar, der Sie in der Moderation darin unterstützt, die Grundidee des Risikomanagements spezifisch für Unternehmen zu kommunizieren. Das Planspiel als Werkzeug bedarf daher einer Einbettung in ein Gesamt-Workshop-Konzept, das Sie als moderierende Person mitgestalten. Ihr persönlicher Anteil benötigt eine eingehende Vorbereitung – vor allem in Bezug auf Einleitung und Nachbereitung. Regeln und Material sind so gestaltet, dass diese Ihnen den entsprechenden Freiraum verschaffen, offene und implizite Inhalte zu integrieren.

Als moderierende Person sind Sie verantwortlich für:

- die Organisation des Workshops,
- die Organisation der nicht im Planspiel-Set enthaltenen Materialien (siehe Kapitel 9),
- die Überprüfung der Materialien auf Vollständigkeit vor dem Workshop,
- die Durchführung bzw. Moderation des Workshops sowie
- die Nachbereitung des Workshops.

Diese Version der Spielanleitung enthält zusätzliche Spielregeln, die als Alternativen zum „klassischen" Verlauf jeweils unter dem Schlagwort „Option" angeboten werden und über deren Einsatz Sie entscheiden können. Die dem Spielmaterial beiliegenden Regelblätter enthalten eine verkürzte Form des Spielablaufs.

Das Lernszenario ist ausgelegt für zwei bis acht Spielende/Teams (bei 16 TN z. B. 8 Paare) und beginnt mit der Vorstellungsrunde. Die Aufgaben der moderierenden Person bestehen darin:

- die Regeln zu erklären,
- das Spiel zu leiten,
- als „Croupier" bzw. „Bank" zu fungieren,
- Fragen zu beantworten,
- den Diskurs unter den Teilnehmenden zu beschleunigen,
- Entscheidungen bei unklaren oder unentschiedenen Auseinandersetzungen bzw. Bewertungen hinsichtlich einer Fortsetzung des Spielprozesses zu fällen sowie
- wichtige Grundlagen des Risikomanagements in der Informationssicherheit zu vermitteln.

Als Lokation eignen sich daher vor allem Besprechungsräume mit einem großen Tisch und ausreichenden Plätzen für die o. g. Anzahl an Teilnehmenden (siehe Kapitel 9).

Hinweise & Empfehlungen

Wir empfehlen neben der intensiven Auseinandersetzung mit dem Planspielmaterial, dass Sie sich vorab selbstständig mit den Grundprinzipien des Risikomanagements befassen und vertraut machen, da hierauf in dieser Spielanleitung nicht weiter eingegangen wird. Unter Kapitel 12 finden Sie weiterführende Links.

Da Sie je nach Rahmen, Lokation und Teilnehmenden auch Unterstützung bei der Organisation vor Ort benötigen, empfehlen wir die Anfertigung eines gesonderten Train-the-Trainer-Konzeptes. Bestandteil eines solchen Konzeptes sind alle nicht in dieser Spielanleitung benannten Details. Das Konzept sollte z. B. Fragen rund um die Organisation wie Teilnehmenden-Management klären. Ein weiterer wichtiger Aspekt betrifft die Moderation. Wie gehen Sie mit Widerständen um? Welche der zahlreichen Optionen als Abweichung vom „klassischen“ Spielverlauf passt am besten zu den Zielen Ihres Workshops? Welche Vor- und Nachteile bieten diese? Wie sieht ein detailliertes Zeitmanagement mit genügend Pausen aus? Das Konzept sollte aber auch Informationen zum Risikomanagement enthalten.

Sollten Sie Hilfe bei der Erstellung eines individuellen Train-the-Trainer-Konzeptes benötigen, wenden Sie sich an:

Technische Hochschule Wildau
Fachbereich:
Wirtschaft, Informatik, Recht (WIR)
Prof. Dr. Margit Scholl
margit.scholl@th-wildau.de

known_sense
Dietmar Pokoyski
pokoyski@known-sense.de

TEIL 2:
SECURITY RISK ROULETTE
Ein Planspiel für Risikomanagement in der Informationssicherheit

09

Vorbereitung

Ziel und Zielgruppe

Wesentliche Intention beim Einsatz des erlebnisorientierten Lernszenarios ist die Konfrontation der Teilnehmenden mit typischen Elementen des Risikomanagements. Die Mitspielenden bewerten dazu verschiedene auf sogenannten Risikokarten beschriebene, potenzielle Szenarien hinsichtlich der möglichen Auswirkungen auf ein via Rollenbeschreibung definiertes, fiktives Unternehmen (optional auf das eigene), wobei zusätzliche Ereignisse mit Wirkungspotenzial zu berücksichtigen sind. Dabei ist der qualitative Prozess, der sich aus dem diskursiven Anteil der Auseinandersetzung mit dem Thema und der Bewertungen der Mitspielenden zusammensetzt, relevanter als der quantitative Aspekt des „Gewinnens". Dennoch wird es am Ende eine „Siegerin"/einen „Sieger" bzw. ein „Siegerteam" geben. Der Punktestand entscheidet über den Sieg: Dieser lässt sich ermitteln aus dem wirtschaftlichen Erfolg (Jetons bzw. Cybermoney) abzüglich des Wertes, der sich aus der bewussten Akzeptanz von Risiken, abgebildet durch die Positionierung in der Risikomatrix, ergibt. Im Gesamtbild bewerten die Teilnehmenden also die Wirtschaftlichkeit vor dem Hintergrund größtmöglicher Stabilität. Zielgruppe sind Führungskräfte der ersten und zweiten Ebene.

Zeitplanung

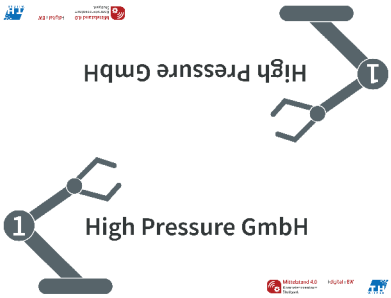
Vorbereitung je nach örtlichen Gegebenheiten:	ca. 15-30 Minuten
Erlebnisorientiertes Lernszenario:	ca. 90-120 Minuten
Einleitung (Briefing):	ca. 30 Minuten gesamt
→ Vorstellungsrunde	ca. 15 Minuten
→ Erläuterung der Regeln mit evtl. Fragen	ca. 15 Minuten
Durchführung (Ein Spiel mit 8 Risikobewertungen sollte nach Möglichkeit beendet werden. Die Spielzeit muss potenziell entsprechend angepasst werden.)	ca. 40-70 Minuten
Nachbereitung (Debriefing)	ca. 20 Minuten

Material

Vor Beginn eines jeden Workshops ist das Material auf Vollständigkeit zu prüfen:

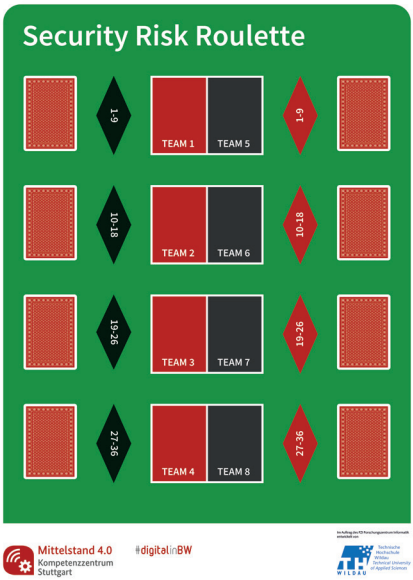
- **8 Faltkarten** mit Team-Nummern und Namen der fiktiven Unternehmen, 7 Faltkarten ohne Nummern und Unternehmensbezeichnungen und 1 Faltkarte Mittelstands GmbH[1] (Bsp. siehe Abbildung 21)
- **1 Spielplan** in DIN A0-Format (siehe Abbildung 22)
  Die 8 äußeren vorgezeichneten Felder dienen der Platzierung der Risikokarten. Die 8 inneren vorgezeichneten Felder sind für den Einsatz der Mitspielenden bzw. Teams vorgesehen.
- **8 Regelblätter** (siehe Abbildung 23)
  Die DIN A4 großen Regelblätter geben den Teilnehmenden eine Zusammenfassung der wichtigsten Schritte sowie einen Überblick über die wichtigsten Infos der Unternehmenskarten, sodass jeder/jede Mitspielende die Rolle der anderen kennt.

[1] https://www.mittelstand-gmbh.de/



© TH Wildau

Abbildung 21: SRR | Material – Beispiel Faltkarte



© TH Wildau

Abbildung 22: SRR | Material – Spielplan

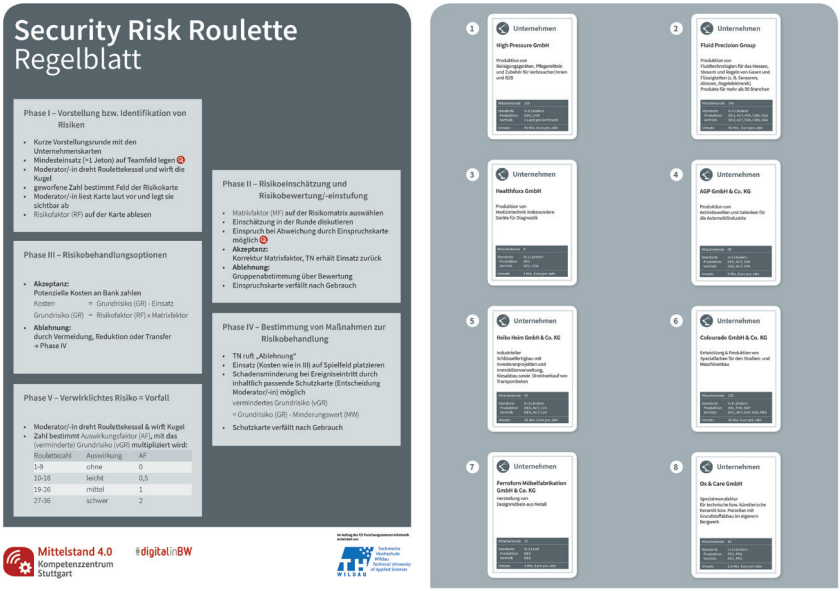


Abbildung 23: SRR | Material – Regelblatt

- **1 digitaler Roulettekessel** (siehe Abbildung 24)
  Sie finden diesen unter https://diz.wildau.biz/roulette/index.html.
- **8 Risikomatrix-Karten** (siehe Abbildung 25)
  Die DIN A4 großen abwischbaren Karten mit den Dimensionen Eintrittswahrscheinlichkeit und Schadensausmaß sind nach der 4x4-Risikomatrix des BSI-Standards 200-3 gestaltet [7]. Je höher Eintrittswahrscheinlichkeit und Schadensausmaß sind, desto größer ist das Grundrisiko (grün = geringer Wert, rot = hoher Wert).
- **8 Berechnungsschema-Karten** (siehe Abbildung 26)
  Die DIN A4 großen abwischbaren Karten zeigen das Berechnungsschema.
- **8 Unternehmenskarten** (Bsp. siehe Abbildung 27)
  7 abwischbare Leerkarten
  1 Unternehmenskarte Mittelstands GmbH
  Die Karten enthalten die Rollenbeschreibungen von verschiedenen KMU mit diversen Informationen bzw. Werten.

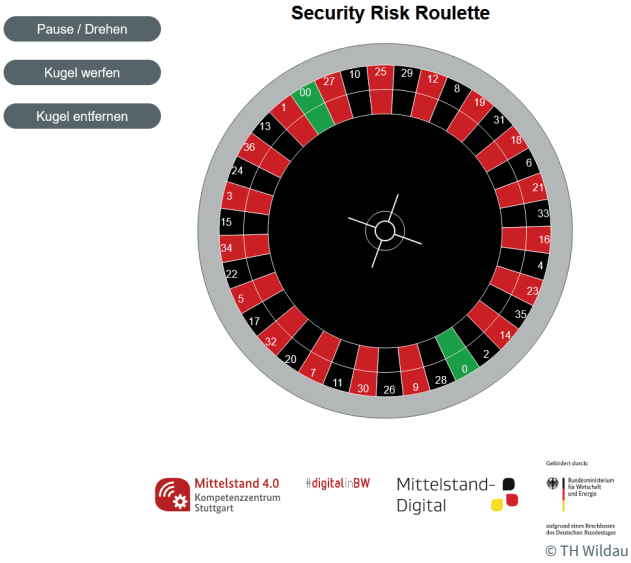


Abbildung 24: SRR | Material – digitaler Roulettekessel

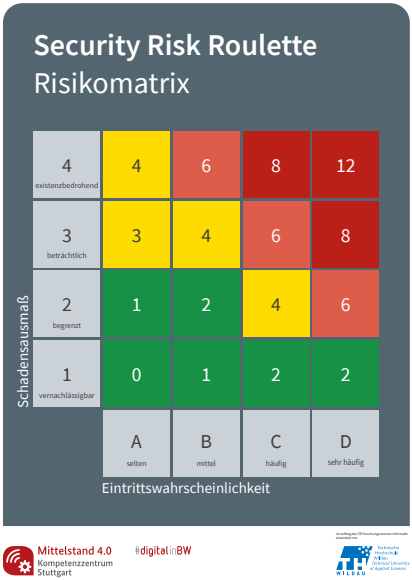


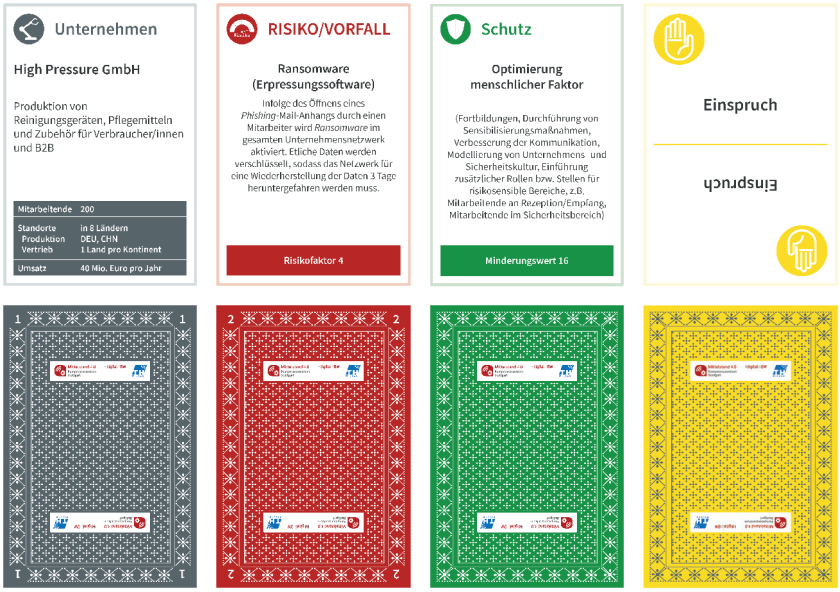
Abbildung 25: SRR | Material – Risikomatrix-Karte

Abbildung 26: SRR | Material – Berechnungsschema-Karte

- **24 Risikokarten** (Bsp. siehe Abbildung 27)
  4 abwischbare Leerkarten
  Auf den Risikokarten ist pro Karte ein (Sicherheits-)Risikofaktor von 1 bis 5 beschrieben, der sich aus dem generellen Schadensausmaß einer der 24 Gefährdungen ableitet. Abhängig von Branche, Produkt bzw. Service, Größe und Umsatz (siehe Beschreibung Unternehmenskarten) wird der Sicherheitsrisikofaktor mit einem entsprechend ausgewählten Faktor der Risikomatrix multipliziert, um das Grundrisiko zu bestimmen.

- **24 Schutzkarten** (Bsp. siehe Abbildung 27)
  4 abwischbare Leerkarten
  Jede Maßnahme ist viermal im Kartensatz vorhanden. Die Teilnehmenden verfügen damit über Abwehrmaßnahmen, die entweder der Vermeidung, der Reduktion oder dem Transfer des Risikos dienen. Auf den Karten ist ein Minderungswert angegeben, um den die Gesamtrisikopunkte gemindert werden.

- **16 Einspruchskarten** (siehe Abbildung 27)
  Diese Karten sind im identischen Layout gestaltet und mit der Aufschrift „Einspruch“ versehen.



© TH Wildau

Abbildung 27: SRR | Material – Beispiel Karten Vorder- und Rückseite

- **Cybermoney** in verschiedenen Stückelungen (siehe Abbildung 28)
  Der Wert des Cybermoneys korrespondiert mit den sogenannten Vorfallwerten (Grundrisiko, ggf. vermindert, multipliziert mit dem Auswirkungsfaktor, siehe Kapitel 10 Phase V).

Anzahl		Wert	Abgebildetes Portrait (siehe Infobox)
200	x	1er	Steve Jobs
100	x	5er	Mark Zuckerberg
100	x	10er	Bill Gates
50	x	25er	Elon Musk
20	x	50er	Jeff Bezos

Abbildung 28: SRR | Material – Cybermoney

Angelehnt an echte Währungen wie Dollar oder Deutsche Mark, zeigt das Spielgeld die Porträts verschiedener Persönlichkeiten, die unter dem Aspekt des größten Erfolges im digitalen Bereich basierend auf der Forbes-Liste 2021 ausgewählt wurden [8]. Der bereits verstorbene Apple-Gründer Steve Jobs wurde aufgrund seines Status als Ikone in diesem Bereich der Reihe hinzugefügt.

Nicht inbegriffenes Material

- **8 transparente Tischaufsteller/Displays**
  Die Aufsteller dienen zum Schutz der Faltkarten und sollen die Lebensdauer erhöhen. Sie sind nicht zwingend erforderlich.
- **1 Roulettekessel mit Kugel** (siehe Abbildung 29)
  Der Roulettekessel dient vor allem dem Erlebnisfaktor.
- **1 Rateau (Rakel)**
  Der Rateau wird zum Einziehen der Jetons benutzt und dient wie der Roulettekessel dem Erlebnisfaktor. Dieser ist jedoch nicht zwingend erforderlich.
- **Jetons** in verschiedenen Stückelungen (siehe Abbildung 30)
  Der Wert der Jetons korrespondiert mit den sogenannten Vorfallwerten (Grundrisiko, ggf. das vermindert, multipliziert mit dem Auswirkungsfaktor, siehe Kapitel 10 Phase V).

Anzahl		Wert	Farbe
200	x	1er	grün
100	x	5er	gelb
100	x	10er	rot
50	x	25er	schwarz
20	x	50er	lila

© TH Wildau

Abbildung 29: SRR | Nicht inbegriffenes Material – Roulettekessel

© TH Wildau

Abbildung 30: SRR | Nicht inbegriffenes Material – Jetons

Vom Veranstalter bereitzustellendes Material

Ausreichend großer Raum
(entsprechend der Anzahl der Teilnehmenden)

1 ausreichend großer Tisch
mit der entsprechend benötigten Anzahl an Plätzen

Ausreichend Stühle für die Teilnehmenden

Namensetiketten

Große Pinnwand, Whiteboard oder Flipchart für die Nachbereitung

Pinnnadeln oder Magnete

Laptop (für digitale Ergänzung)

Stoppuhr (Smartphone)

Taschenrechner (Smartphone)

Notizzettel und Stifte

Stifte mit wasserlöslicher Farbe wie Whiteboardmarker inklusive Tücher oder Ähnlichem zum Korrigieren und Entfernen von Einträgen

Aufbau

Als moderierende Person richten Sie das Lernszenario ein, d. h. das Spielfeld wird auf dem Tisch und der Roulettekessel am oberen Rand des Spielfeldes platziert. Die 24 Risikokarten werden gemischt und zu gleichen Anteilen auf den dafür vorgesehenen Tableau-Feldern des äußeren Spielfeldbereiches angeordnet. Die acht Unternehmenskarten sowie je vier Schutzkarten werden verdeckt gemeinsam mit den acht Risikomatrix-Karten, je 2 Einspruchskarten, der Währung (Cybermoney bzw. Jetons) sowie den Faltkarten zusammen mit Stiften und Notizzetteln je nach Anzahl der Teams auf den einzelnen Plätzen als Individualmaterial verteilt. Der komplette Aufbau ist in Abbildung 31 zu sehen.

Budget für jeden Mitspielenden bzw. jedes Team (Wert = insgesamt 400):

Anzahl		Wert	Farbe	Porträt
20	x	1er	grün	Steve Jobs
12	x	5er	gelb	Mark Zuckerberg
12	x	10er	rot	Bill Gates
4	x	25er	schwarz/grau	Elon Musk
2	x	50er	lila	Jeff Bezos

Es erhalten nicht alle Teilnehmenden individuelle Unternehmenskarten; vielmehr wird in jeder Runde von Ihnen eine Unternehmenskarte gezogen, die in der jeweiligen Spielrunde für die Bewertung aller Teilnehmenden bindend ist. Mit dieser Option sind die Einspruchskarten nicht zwingend erforderlich. Je nach Einigung mit den Mitspielenden kann auch das eigene Unternehmen einbezogen werden. Hierfür werden die Leerkarten entsprechend ausgefüllt. Das eigene Unternehmen ins Spiel zu bringen, eignet sich besonders dann, wenn alle Mitspielenden aus einem Unternehmen stammen.

Die Schutzkarten werden nicht mitverteilt, sondern müssen von jedem Teilnehmenden – je nach Strategie – zu einem festzulegenden Preis (z. B. 50% des Minderungswertes) vor Spielphase IV erworben werden.

Bei bis zu 8 Teilnehmenden kann einzeln gespielt werden. Bei mehr als 8 Teilnehmenden werden Zweier- bzw. Dreierteams gebildet (z. B. bei neun Teilnehmenden drei Paare und ein Dreierteam etc.).

© TH Wildau

Abbildung 31: SRR | Aufbau

10

Ablauf

Überblick

- Einleitung (Briefing)
- Phase I Vorstellung bzw. Identifikation von Risiken
- Phase II Risikoeinschätzung und Risikobewertung/-einstufung
- Phase III Risikobehandlungsoptionen
- Phase IV Bestimmung von Maßnahmen zur Risikobehandlung
- Phase V Verwirklichtes Risiko = Vorfall (Incident)
- Auswertung und Nachbereitung (Debriefing)

Einleitung (Briefing)

- Sie begrüßen nach Start der Veranstaltung die Teilnehmenden und erklären, dass dieses Planspiel das Thema Risikomanagement in der Informationssicherheit behandelt und den Teilnehmenden Prozesse, Zusammenhänge und Wissenswertes aus diesem Bereich erlebnisorientiert vermittelt.
- Dabei soll den Teilnehmenden ihre individuelle Haltung zum Thema Risikomanagement im Kontext ihrer jeweils eigenen Organisation bewusst werden.
- Die Teilnehmenden stellen sich kurz mit Namen, Organisation und Aufgaben in ihrem realen Unternehmen vor.
- Vor Beginn des Lernszenarios kann von Ihnen abgefragt werden, ob und inwiefern Erfahrungen mit Risikomanagement von einzelnen Teilnehmenden gesammelt worden sind. Von Interesse wären hier auch Inhalt und Grundlage dieser Erfahrungen.
- Hierbei kann die Situation in den jeweiligen Unternehmen der Teilnehmenden angesprochen werden, ohne vertiefend auf Details einzugehen.
- Das Individualmaterial der einzelnen Mitspielenden/Teams wird auf Vollständigkeit geprüft und von der moderierenden Person erklärt.
- Die Teilnehmenden nehmen spätestens zu diesem Zeitpunkt ihre Plätze um den Spielplan ein.
- Die Reihenfolge und Auswahl der fiktiven Unternehmen ist mit der Wahl des Sitzplatzes festgelegt.

Alternativ wird eine zentrale Unternehmenskarte pro Spielrunde von Ihnen gezogen und vorgestellt.

Sind die auf den Unternehmenskarten verwendeten Ländercodes unbekannt, werfen Sie einen Blick ins Kapitel 14.

Phase I – Vorstellung bzw. Identifikation von Risiken

- Die Teilnehmenden stellen kurz die wichtigsten Informationen der Unternehmenskarte vor.
- Jeder/jede Mitspielende bzw. jedes Team setzt einen Risikowert-Mindestbeitrag von 1 als Jeton (Wert = 1) auf die Teamnummer des Spielfeldes (siehe Abbildung 32). Jede Person/jedes Team kann auch „Zocken“ und einen höheren Betrag setzen, der nach erfolgreichem Einspruch von der Bank (Moderation) verdoppelt wird.

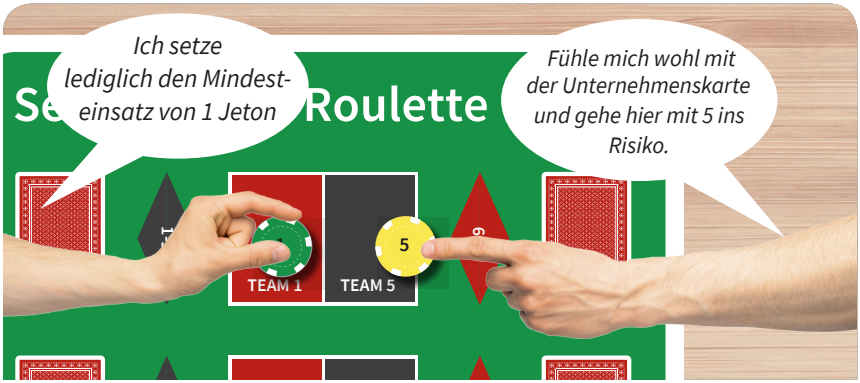


Abbildung 32: SRR | Phase I – Einsatz

Ein erhöhter Einsatz dient also entweder einer potenziellen Gewinnoption bei erfolgreichem Einspruch oder erweitert das eigene Sicherheitsbudget zum Erwerb von Schutzkarten. Hierauf kann im Sinne einer Spielvereinfachung verzichtet werden. Dann wird allerdings ein möglicher Einspruch nicht mehr belohnt (siehe Kapitel 10 Phase 2).

- Sie drehen den Roulettekessel im Uhrzeigersinn und werfen die Kugel entgegen des Uhrzeigersinns ein.
- Sobald die Kugel in einem Nummernfach liegen bleibt, wird von Ihnen die entsprechende Zahl angesagt.
- Bei einer 0 oder 00 wird erneut gedreht.
- Von dem der Zahl zugehörigen Risikokarten-Feld auf dem Spielfeld wird die oben liegende Risikokarte gezogen (z. B. bei der Nummer 5 rot aus dem Stapel 1-9 neben der roten Raute) und vorgestellt (vorlesen und sichtbar ablegen) (siehe Abbildung 33). Der Faktor auf der Karte entspricht dem sogenannten Risikofaktor.

Abbildung 33: SRR | Phase I – Risikokarte

Phase II – Risikoeinschätzung (Ermittlung von Eintrittshäufigkeit und Schadenshöhe) und Risikobewertung/ -einstufung (Ermittlung der Risikokategorie)

- Sie fordern die Teilnehmenden auf: *„Schätzen Sie das Risiko für Ihr Unternehmen entsprechend der Unternehmenskarte zum aufgedeckten Risikofall ein!“*
- Jeder/jede Mitspielende bzw. jedes Team trägt die Nummer der Risikokarte auf dem für das Unternehmen zutreffende Feld der eigenen Risikomatrix-Karte ein. Dabei wird erwartet, dass jede Einschätzung so „fair“ vorgenommen wird wie möglich. Je nach Art des Unternehmens können Positionierungen sehr unterschiedlich ausfallen (siehe Abbildung 34).
- Die Teilnehmenden stellen durch Vorzeigen der Karte innerhalb der Runde ihre Risiko-Einschätzung kurz vor. Der/die Mitspielende/das Team links von Ihnen beginnt. In den folgenden Teilspielrunden geht es im Uhrzeigersinn weiter.

© TH Wildau

Abbildung 34: SRR | Phase II – Risikomatrix

- Entsprechend der Risikomatrix wird nun das entsprechende Risiko wie folgt eingestuft:
    - geringes Risiko (grün)
    - mittleres Risiko (gelb)
    - hohes Risiko (hellrot)
    - sehr hohes Risiko (rot)
- Einspruch (siehe Abbildung 35):
  Falls jemand zu einer abweichenden Einschätzung kommt, kann die Einspruchskarte gezogen und vor demjenigen platziert werden, dessen Einschätzung widersprochen wird (Einspruch im eigenen Team ist unzulässig).
    - Der/die Widersprechende muss dann benennen, wo das Risiko stattdessen zu positionieren wäre (max. 60 Sekunden Zeit).
    - Sie fragen dann, ob der Einspruch mit der neu vorgeschlagenen Positionierung akzeptiert wird oder nicht.
    - Bei Annahme des Einspruchs wird der ursprüngliche Eintrag in der Risikomatrix-Karte gelöscht und durch den neuen ersetzt.
    - Wird diese nicht akzeptiert (d. h. der Vorschlag des Widersprechenden wird abgelehnt), rufen Sie zur Abstimmung unter allen Teilnehmenden auf. Bei einem Unentschieden entscheiden Sie.
    - Falls die Mehrheit der Meinung ist, die Positionierung sei richtig, bleibt es bei diesem Eintrag.
    - Falls dem Einspruch stattgegeben wird, erhält der/die Einspruchserhebende den durch die Bank (diese Rolle übernehmen Sie) verdoppelten Mindesteinsatz vom eigenen Teamfeld.
    - Eine einmal gezogene Einspruchskarte verfällt und kann damit kein weiteres Mal eingesetzt werden.

Abbildung 35: SRR | Phase II – Einspruch

Der Einspruch kann insofern vereinfacht oder sogar komplett eliminiert werden, als dass durch Sie eine Abfrage- bzw. Diskussionsrunde bzgl. der Risiko-Positionierung für die jeweils in der Spielrunde ausgewählte Unternehmenskarte gestartet wird. In diesem Fall entscheidet die mehrheitliche Bewertung und der Mindesteinsatz wird unter denjenigen aufgeteilt, die das Risiko im Cluster der Mehrheit positioniert hat. Im Zweifelsfall entscheiden Sie.

Phase III – Risikobehandlungsoptionen

An die Risikoeinstufung schließt die Wahl der folgenden Behandlungsoptionen. Jeder/jede bzw. jedes Team begründet, warum ein Risiko vermieden, reduziert, transferiert oder akzeptiert werden soll.

- Akzeptanz des Risikos
  Die potenziellen Kosten des Risikos müssen auf dem jeweils eigenen Teamfeld als Rückstellungsbudget verwahrt werden. Sie ergeben sich aus der Multiplikation des auf der Risikokarte ausgewiesenen Wertes (Faktor 1 bis 5) mit dem auf der Risikomatrix gewählten Wertes. Von den Kosten wird der bereits zu Beginn der Runde gesetzte Einsatz abgezogen.
- Ablehnung des Risikos
  Wird das Risiko nicht akzeptiert, liegt eine der folgenden Behandlungsoptionen vor und es geht in Phase IV weiter mit den Risikomanagement-Optionen:
    - Vermeidung
    - Reduktion
    - Transfer

Phase IV – Bestimmung von Maßnahmen zur Risikobehandlung

- Die im Risikomanagement etablierten Strategien Vermeidung, Reduktion und Transfer werden in dem Planspiel unter der Bezeichnung und dem Schritt „Ablehnung“ zusammengefasst.
- Der/die Mitspielende/das Team sagt laut „Ablehnung“, falls das Risiko nicht akzeptiert wird.
- Die Mitspielenden/Teams legen ihren Einsatz, der sich aus den wie oben beschriebenen Faktoren zusammensetzt (Faktor von der jeweiligen Risikokarte mal Faktor aus der zugehörigen Positionierung innerhalb der Risikomatrix), auf das zugehörige Teamfeld des Spielfeldes.
- Das Ausmaß eines verwirklichten Risikovorfalls kann durch das Setzen einer passenden Schutzkarte gemindert werden.
- Die auf der Schutzkarte beschriebene Reduktionsmaßnahme muss inhaltlich zum beschriebenen Vorfall passen (siehe Abbildung 36). Im Zweifelsfall entscheiden Sie über die Anerkennung.
- Die eingesetzte Schutzkarte verliert nach einmaligem Einsatz ihre Gültigkeit.

Abbildung 36: SRR | Phase IV – Schutzkarte

Phase V – Verwirklichtes Risiko = Vorfall (Incident)

- Es wird per Zufall (Roulettekessel) bestimmt, ob die in der jeweiligen Teilspielrunde behandelte Gefährdung sich realisiert und mit welcher Intensität sie eintritt.
- Sie drehen dafür erneut den Roulettekessel.
- Die erzielte Zahl (Auswirkungsfaktor) gibt die Auswirkung des Risikos vor (Bsp. siehe Abbildung 37):
    - Zahlen 1 bis 9:
      Ereignis tritt nicht ein
      (Auswirkungs- bzw. Multiplikations-Faktor = 0)
      D. h. das Geld darf wieder vom Spielfeld genommen und behalten werden.
    - Zahlen 10 bis 18:
      Ereignis hat leichte Auswirkungen
      (Auswirkungs- bzw. Multiplikations-Faktor = 0,5).
      D. h. die mit dem Risiko verbundenen Kosten dürfen halbiert werden.
    - Zahlen 19 bis 27:
      Ereignis hat mittlere Auswirkungen (Auswirkungs- bzw. Multiplikations-Faktor = 1).
      D. h. der Einsatz bleibt, wie er ist.
    - Zahlen 28 bis 36:
      Ereignis hat schwere Auswirkungen (Auswirkungs- bzw. Multiplikations-Faktor = 2).
      D. h. die mit dem Risiko verbundenen Kosten müssen verdoppelt werden.
    - Zahlen 0 und 00:
      Es wird erneut gedreht.

Abbildung 37: SRR | Phase V – Vorfall (Incident)

Übersicht der Berechnungsformel:

	Risikofaktor (RF)
x	Matrixfaktor (MF)
=	Grundrisiko (GR) 18
-	Minderungswert 15
=	vermindertes Grundrisiko (vGR)
x	Auswirkungsfaktor (AF)
=	Vorfall-/Inzidentwert (IW)

Beispiel

Es wird die Risikokarte 9 *Dumpster Diving* gezogen mit dem Risikofaktor 3. Das Team 3 (Healthfoxx GmbH) stuft innerhalb der Risikomatrix mithilfe der Eintrittswahrscheinlichkeit (mittel) und dem Schadensausmaß (existenzbedrohend) die potenzielle Gefährdung bei 12 ein. 3 x 12 = Grundrisiko von 36. Wenn die Healthfoxx GmbH das Risiko akzeptiert, müssen 36 Risikopunkte in Form von Jetons oder Cybermoney auf das jeweils eigene Teamfeld abgelegt werden. Falls nicht, müssen 36 Risikopunkte abzüglich des Minderungswertes einer passenden Schutzkarte auf dem Spielfeld platziert werden. Wird zur Minderung in Form einer Schutzkarte „Sensibilisierung bzw. Optimierung menschlicher Faktor" eine ggf. laufende Awareness-Maßnahme vorgebracht, die ein potenzielles Schadensausmaß reduzieren würde (Minderungswert = 16), wären lediglich 20 Risikopunkte zu platzieren. Wenn nach dem anschließenden Drehen des Roulettekessels über die Roulettezahlen 1-9 der Auswirkungsfaktor 0 hinsichtlich eines realen Eintritts ermittelt wird, wäre Healthfoxx GmbH mit einem blauen Auge davon gekommen. Das Gefährdungsereignis (Vorfall) tritt also nicht ein und die Healthfoxx GmbH erhält die Jetons vom Teamfeld komplett zurück.

Weitere Teilspielrunden

- Die neu im Kessel ermittelte Ziffer gibt gleichzeitig den Zifferncode für die neue, zweite Teilspielrunde vor und damit das Ziehen der zweiten Risikokarte.
- Es sollte (bei maximaler Auslastung von 8 Mitspielenden/Teams) mindestens 1 komplette Spielrunde (mit demnach 8 Teilspielrunden) durchgeführt werden.
- Optional: Da 8 Teilspielrunden als Mindestdauer bedeuten würden, dass sämtliche Unternehmenskarten im Spiel wären, muss die Teilrundenzahl auf 4-6 verkürzt werden oder die Anzahl der Unternehmenskarten muss erhöht werden, um bei ggf. schnelleren Spielrunden weitere Unternehmen ins Spiel zu bringen.
- Bei 90 Minuten Gesamtdauer inkl. Einleitung und Nachbereitung sollte eine Teilspielrunde demnach maximal 5 Minuten in Anspruch nehmen.
- Sollte die Spielzeit mehr Runden als 8 vorsehen, kommen entweder bereits verwendete Unternehmenskarten ein zweites Mal ins Spiel oder es werden Leerkarten neu beschrieben.

Auswertung und Nachbereitung (Debriefing)

- Es gewinnt der/die Teilnehmende bzw. das Team mit dem höchsten Punktestand bzw. meisten Jetons.
- Sie helfen bei der quantitativen Auswertung (Jetons bzw. Punktestand zählen) und rufen den Gewinner aus.
- Sie bieten eine Nachbereitung an, bei der die Teilnehmenden Spielablauf bzw. das Erlebte reflektieren (bitte vorbereiten, s. o.).
- Diese Reflexion wird in eine offene Diskussion überführt.

Zusatzmaterial
Ein Einstieg in die Moderation

TEIL 3:
ZUSATZMATERIAL

11

Glossar

Begriff	Bedeutung
(Information Security) Awareness	engl. „(Informationssicherheits-)Bewusstsein“ Awareness-Maßnahmen konzentrieren sich darauf, das Bewusstsein für potenzielle Risiken und Bedrohungen für Informationssicherheit zu schärfen, die auf menschliches Verhalten abzielen.
Angriffsvektor	Ein Angriffsvektor ist ein Angriffsweg oder eine Angriffstechnik, mittels derer Cyberkriminelle eine Attacke auf ein IT-System durchführen. Dies kann mehrstufig erfolgen.
Backdoor	engl. „Hintertür“ Eine Backdoor oder Trapdoor (engl. „Falltür“) ist eine unbefugte, heimliche und bewusst eingebaute Möglichkeit, mit der die normale Zugriffssicherung umgangen und ein Zugang zum Computer oder einer geschützten Funktion eines Computerprogramms erlangt werden kann.

Begriff	Bedeutung
Baiting	engl. „Köder, ködern“ Unter Baiting wird ein digitaler oder physischer Köder verstanden, der als Trojanisches Pferd dient. Social Engineers locken z. B. mit kostenlosen Musik- oder Film-Downloads oder USB-Sticks.
CEO (Chief Executive Officer)	engl. „Geschäftsführer/Geschäftsführerin“
CEO-Fraud	engl. „Geschäftsführerbetrug“ CEO-Fraud ist eine Betrugsmethode, bei der sich der Angreifer als Geschäftsführer, Manager oder Chef ausgibt und Mitarbeitende beispielsweise dazu auffordert, Geld auf ein bestimmtes Konto zu überweisen.
Clean-Desk-Policy	engl. „Richtlinie für Schreibtischordnung“ Ein ordentlicher Schreibtisch ist gelebter Datenschutz. Bei Publikumsverkehr werden offenliegende Dokumente mit personenbezogenen Daten schnell zum Datenschutzproblem.
DoS (Denial of Service)	engl. „Verweigerung des Dienstes“ Die Nichtverfügbarkeit eines Internetdienstes (z. B. Onlineshop) wird durch eine Vielzahl von gezielten Anfragen verursacht.

Begriff	Bedeutung
Dumpster Diving	engl. „Müllcontainertauchen“ Als Dumpster Diving wird die Suche nach verwertbaren Informationen im Müll bezeichnet, um mit diesen eine Cyber-Attacke durchzuführen. Hierfür sind nicht nur Zugangscodes oder Passwörter interessant, sondern auch vermeintlich harmlose Informationen wie Telefonlisten, Kalender oder Organisationsdiagramme.
Face-to-Face	engl. „von Angesicht zu Angesicht“ Mit Face-to-Face-Kommunikation ist persönliche Kommunikation vor Ort gemeint.
Firmware	Bei der Firmware handelt es sich um eine Software, die fest mit der Hardware verbunden ist und als Schnittstelle zwischen den physikalischen Komponenten eines Geräts und der Anwendungssoftware dient. Über die Firmware werden alle Grundfunktionen eines Geräts gelenkt.
Fraud	engl. „Betrug, Fälschung, List, Schwindel“ Fraud ist ein Sammelbegriff für verschiedene Arten von Wirtschaftskriminalität.
Malware	engl. „Schadsoftware“ Malware ist der Oberbegriff für Schadsoftware wie Viren, Würmer und Trojaner.
Patch	engl. „Pflaster“ Mit Patches korrigieren Softwarehersteller Fehler in Programmen, schließen Sicherheitslücken oder rüsten Funktionen nach.

Begriff	Bedeutung
Phishing	engl. „Passwort-Fischen“ (Kunstwort) Das Ziel von Phishing ist es, mit gefälschten E-Mails an persönliche Daten anderer Personen wie Passwörter, Kreditkartennummern o. ä. zu gelangen.
Pretexting	engl. „Vorwand“ Diese Art von Angriff zeichnet sich dadurch aus, dass sich Social Engineers eine Geschichte oder einen Vorwand ausdenken, um die Zielperson zu täuschen und wertvolle Informationen oder den Zugang zu einer Dienstleistung oder einem System zu erhalten.
Quid pro Quo	engl. „Gegenleistung“ (lat. „dies für das“) Quid Pro Quo-Attacken versprechen einen Vorteil (z. B. IT-Unterstützung) gegen Informationen oder die Durchführung einer bestimmten Aktion (z. B. Installation eines Programmes).
Ransomware	engl. „Erpressungssoftware“ Ransomware sind Schadprogramme, die den Computer sperren oder darauf befindliche Daten verschlüsseln. Es erfolgt danach meist eine Erpressung.
Server	Ein Server ist ein Rechner, welcher Funktionalitäten, Dienstprogramme, Daten oder andere Ressourcen bereitstellt, damit andere Rechner („Clients“) darauf zugreifen können.

Begriff	Bedeutung
Social Engineering	engl. „Soziale Manipulation“ Social Engineering ist eine Methode, welche grundlegende Charaktereigenschaften und Verhaltensmuster wie z. B. Hilfsbereitschaft, Vertrauen, Angst oder Respekt vor Autorität ausnutzt, um unberechtigten Zugang zu Informationen oder IT-Systemen zu erlangen [1].
Spear-Phishing	engl. „Passwort-Speerfischen“ (Kunstwort) Spear-Phishing ist eine besondere Form des Phishing, das zielgerichtet auf eine Person oder Organisation ist.
Tailgating	engl. „Hindurchschlüpfen“ Beim Tailgating-Angriff versuchen Social-Engineers, unberechtigten Zugang zum Firmengelände zu erhalten, indem sie einfach eine autorisierte Person austricksen und dieser für den Zutritt hinterherlaufen.
Trojaner	Ein Trojaner ist als nützliche Anwendung getarnt, führt aber im Hintergrund ohne Wissen des Anwenders eine andere Funktion aus.
Update	engl. „Aktualisierung“ Mit einem Update wird der Funktionsumfang des Programms erweitert oder verbessert. Teilweise werden damit aber auch wie bei einem Patch Fehler behoben.

Begriff	Bedeutung
USB Juice Jacking	engl. „manipulierte USB-Ladestation“ Beim USB Juice Jacking wird die Ladestation so manipuliert, dass eine Datenübertragung stattfindet. So können entweder Daten in unbefugte Hände gelangen oder das Endgerät wird mit Malware infiziert.
VPN (Virtual Private Network)	engl. „virtuelles privates Netzwerk“ VPN bezeichnet eine Netzwerkverbindung, die von Unbeteiligten nicht einsehbar ist.
WLAN (Wireless Local Area Network)	engl. „drahtloses lokales Netzwerk“
Zugangskontrolle	Die Zugangskontrolle verhindert die Nutzung der Datenverarbeitungsanlagen durch Unbefugte z. B. mittels Passwort, Chipkarte, Pin-Verfahren.
Zugriffskontrolle	Die Zugriffskontrolle stellt sicher, dass ausschließlich befugte Personen Zugriff auf personenbezogene Daten, Programme, und Dokumente erhalten. Die Berechtigung ergibt sich aus der Aufgabenzuweisung und der Organisation des Unternehmens.
Zutrittskontrolle	Die Zutrittskontrolle verhindert den physikalischen Zutritt unbefugter Personen zu Datenverarbeitungsanlagen z. B. durch verschlossene Türen, Alarmanlage, Videoüberwachung, Schlüssel.

TEIL 3:
ZUSATZMATERIAL

12

Weitere Informationen

Unsere Projekte

Informationssicherheitsbewusstsein für den Berufseinstieg (SecAware4job):
https://secaware4job.wildau.biz/

Informationssicherheitsbewusstsein für den Schulalltag (SecAware4school):
https://secaware4school.wildau.biz/

Gendersensible Studien-und Berufsorientierung für den Beruf Security Spezialistin (Securi♀y):
https://security.wildau.biz/

Social Engineering

Mitnick, K. D. und Simon, W. L. (2011).
Die Kunst der Täuschung: Risikofaktor Mensch. Heidelberg: mitp.

Anderson, R. (2020).
Chapter 3 Psychology and Usability. In: Anderson, R., Security Engineering: A Guide to Building Dependable Distributed Systems, 3rd Edition.

Security Risk Management

BSI-Standard 200-3 – Risikomanagement
https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/IT-Grundschutz/BSI-Standards/BSI-Standard-200-3-Risikomanagement/bsi-standard-200-3-risikomanagement_node.html

Online-Kurs-IT-Grundschutz – Lektion 7
https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/IT-Grundschutz/Zertifizierte-Informationssicherheit/IT-Grundschutzschulung/Online-Kurs-IT-Grundschutz/Lektion_7_Risikoanalyse/Lektion_7_node.html

Klipper, Sebastian (2015).
Information Security Risk Management:
Risikomanagement mit ISO/IEC 27001, 27005 und 31010.
Wiesbaden: Springer Vieweg, 2015. DOI: https://doi.org/10.1007/978-3-658-08774-6

TEIL 3:
ZUSATZMATERIAL

13

Miniglossar

Das Miniglossar dient als Unterstützung im Lernszenarion Social Engineering Theater.

Die folgende Seite können Sie heraustrennen und für Veranstaltungen im Rahmen des Projektes »Mittelstand 4.0-Kompetenzzentrum Stuttgart« für Teilnehmende als Handreichung vervielfältigen.

Social Engineering Theater | Glossar

Begriff	Bedeutung
(Information Security) Awareness	engl. „(Informationssicherheits-) Bewusstsein“
Backdoor	engl. „Hintertür“
Baiting	engl. „Köder, ködern“
CEO (Chief Executive Officer)	engl. „Geschäftsführer/Geschäftsführerin“
CEO-Fraud	engl. „Geschäftsführerbetrug“
Clean-Desk-Policy	engl. „Richtlinie für Schreibtischordnung“
DoS (Denial of Service)	engl. „Verweigerung des Dienstes“
Dumpster Diving	engl. „Müllcontainertauchen“
Face-to-Face	engl. „von Angesicht zu Angesicht“
Fraud	engl. „Betrug, Fälschung, List, Schwindel“
Malware	engl. „Schadsoftware“
Patch	engl. „Pflaster“
Phishing	engl. „Passwort Fischen“
Pretexting	engl. „Vorwand“
Quid pro Quo	engl. „Gegenleistung“ (lat. „dies für das“)
Ransomware	engl. „Erpressungssoftware“
Social Engineering	engl. „Soziale Manipulation“
Tailgating	engl. „Hindurchschlüpfen“

Mittelstand 4.0 Kompetenzzentrum Stuttgart

#digitalinBW

Im Auftrag des FZI Forschungszentrum Informatik entwickelt von

Technische Hochschule Wildau Technical University of Applied Sciences

Social Engineering Theater | Glossar

Begriff	Bedeutung
Trojaner	Ein Trojaner ist als nützliche Anwendung getarnt, führt aber im Hintergrund ohne Wissen des Anwenders eine andere Funktion aus.
Update	engl. „Aktualisierung“
VPN (Virtual Private Network)	engl. „virtuelles privates Netzwerk“
WLAN (Wireless Local Area Network)	engl. „drahtloses lokales Netzwerk“

Mittelstand 4.0 Kompetenzzentrum Stuttgart

#digitalinBW

Im Auftrag des FZI Forschungszentrum Informatik entwickelt von

Technische Hochschule Wildau Technical University of Applied Sciences

TEIL 3:
ZUSATZMATERIAL

14

ISO Ländercodes

Auf den Unternehmenskarten werden die folgenden Ländercodes nach ISO-3166-1 (alpha3 verwendet):

ISO 3166-1 alpha3	Land
AUT	Österreich
CHN	China
DEU	Deutschland
ESP	Spanien
FRA	Frankreich
IND	Indien
LUX	Luxemburg
MEX	Mexiko
POL	Polen
SGP	Singapur
SVK	Slovakei
THA	Thailand
USA	Vereinigte Staaten von Amerika

Referenzen

[1] BSI (Hrsg.). (2020).
IT-Grundschutz-Kompendium. Köln, Bonn: Reguvis Bundesanzeiger Verlag, Bundesanzeiger Verlag, S. 42. Abgerufen am 28. Februar 2021 von: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Kompendium/IT_Grundschutz_Kompendium_Edition2020.pdf?__blob=publicationFile&v=6

[2] known_sense. (2015).
Studie: Bluff me if U can - Gefährliche Freundschaften am Arbeitsplatz, Tiefenpsychologische Wirkungsanalyse Social Engineering und seine Abwehr. (known_sense, Hrsg.) Köln, S. 36. Abgerufen am 30. April 2020: von http://www.known-sense.de/BluffMeIfUCanAuszug.pdf

[3] Berg, A., & Niemeier, M. (6. November 2019).
Wirtschaftsschutz in der digitalen Welt. (bitkom, Hrsg.), S. 3.
Abgerufen am 28. Februar 2021 von https://www.bitkom.org/sites/default/files/2019-11/bitkom_wirtschaftsschutz_2019_0.pdf

[4] 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, S. 3.
DOI: https://doi.org/10.1186/s13673-018-0128-7

[5] Mouton, F., Leenen, L., Malan, M. M., Venter, H. S. (2014).
Social Engineering Attack Framework. Information Security for South Africa, Johannesburg, 2014, S. 1-9. DOI: https://doi.org/10.1109/ISSA.2014.6950510

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

[7] BSI (Hrsg.). (2017).
BSI-Standard 200-3: Risikoanalyse auf der Basis IT-Grundschutz. Bonn.
Abgerufen am 28. Februar 2020 von:
https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/BSI_Standards/standard_200_3.pdf?__blob=publicationFile&v=2

[8] 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

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.

Unterauftragnehmer

Dietmar Pokoyski (known_sense)

Im Projekt hat known_sense das Projektteam unterstützt, insbesondere bei der Konzeption und Entwicklung des analogen erlebnisorientierten Lernszenarios zum Thema Security Risk Management.

Technische Hochschule Wildau
Technical University of Applied Sciences

Projektlaufzeit: 01.03.2020 - 31.03.2021

ISBN: 978-3-9819225-3-0

Gefördert durch:

Bundesministerium für Wirtschaft und Energie

aufgrund eines Beschlusses des Deutschen Bundestages

Mittelstand-Digital