Hochschule Wismar
Fakultät für Ingenieurwissenschaften
Bereich Elektrotechnik und Informatik

Master-Thesis

Einsatz von Gamification zur Sensibilisierung für Informationssicherheit im Kontext deutscher Hochschulen

eingereicht am: 13. September 2022
von: Susanne Nitschke
in: ...
Studiengang: IT-Sicherheit und Forensik
Erstbetreuerin: Prof. Dr.-Ing. Antje Raab-Düsterhöft
Zweitbetreuer: Prof. Dr. Stefan Schlechtweg

Copyright

Aufgabenstellung

In der Durchführung der Master-Thesis ist ein Schulungskonzept für Informationssicherheit an deutschen Hochschulen unter Verwendung von Gamification zu entwickeln. Ziel ist es dabei, das Konzept adaptionsfähig und erweiterbar zu gestalten, so dass andere Hochschulen dieses an ihre Bedürfnisse anpassen, die Themen aktuell halten und die Motivation der Zielgruppen auf hohem Niveau garantieren können.
Außerdem sind folgende zentrale Fragestellungen mittels einer ausführlichen Literaturrecherche in den Bereichen Didaktik, Kommunikation, Psychologie, Motivation und Change-Management im Kontext der Informationssicherheit zu klären:

1. Wie muss ein auf eine bestimmte Zielgruppe ausgerichtetes Schulungskonzept für Informationssicherheit für deutsche Hochschulen aussehen, welches durch den Einsatz von Gamification zur Wissensbildung und damit zur Sensibilisierung in verschiedenen Zielgruppen beitragen kann?
2. Wie kann die Effektivität und Nachhaltigkeit von Schulungen zur Sensibilisierung für Informationssicherheit, die Gamification beinhalten, gemessen und somit einer möglichen Schadensentstehung vorgebeugt werden?
3. Welche negativen Aspekte und Grenzen hat Gamification beim Einsatz an deutschen Hochschulen und wie können diese vermieden werden?

Für einen ausgesuchten Kommunikationskanal sind Lerninhalte und Spielelemente bezüglich des Konzeptes auszuwählen und kritisch zu bewerten.

Copyright

Kurzreferat

Deutscher Titel:

Einsatz von Gamification zur Sensibilisierung für Informationssicherheit im Kontext deutscher Hochschulen

Das Ziel der Informationssicherheit ist der Schutz aller Informationen, unabhängig davon, ob sie sich auf Papier, in IT-Systemen oder in den Köpfen von Menschen befinden. Sie umfasst demnach nicht nur die technische Sicherheit, sondern auch die nicht-technische Sicherheit von Informationen, für welche die drei Schutzziele der Informationssicherheit gelten. Die Schutzziele umfassen die Vertraulichkeit, Integrität und Verfügbarkeit. Menschen, die nicht ausreichend für die Notwendigkeit der Einhaltung der Schutzziele sensibilisiert sind, können das gesamte Unternehmen gefährden. Da dieses Thema sehr abstrakt und für die Menschen schwer greifbar ist, bietet sich der Einsatz von Instrumenten an, die auf eine unterhaltsame Weise, die wichtigsten Informationen an die Mitarbeitenden eines Unternehmens kommunizieren. Gamification ist in diesem Zusammenhang ein solches Instrument, welches mit spielähnlichen Elementen diesen Prozess unterstützen kann. In dieser Master-Thesis wird das Thema Gamification und dessen Einsatz zur Sensibilisierung für Informationssicherheit aufgegriffen. Das Augenmerk wird dabei auf die Verwendung im Hochschulumfeld gelegt, von dem man annimmt, dass durch die Digitalisierung der Lehre Gamification auch in der eigenen Organisation zum Training der Mitarbeitenden eingesetzt wird. Dazu wurde im Rahmen dieser Thesis eine Umfrage beim Verein der „Zentren für Kommunikationsverarbeitung in Forschung und Lehre“ durchgeführt, dem eine Vielzahl deutscher Hochschulen angehören. Eine weitere Befragung in kleinerem Rahmen bei Herstellern für Serious Games und gamifizierten online-Lernplattformen beschreibt die Erfahrungen, die diese Hersteller in Bezug auf den Einsatz von Gamification an Hochschulen bis heute gemacht haben.

Copyright

Abstract

Title in English:

Use of Gamification to raise Awareness of Information Security in the Context of German Universities.

The goal of information security is to protect all information, regardless of whether it is on paper, in IT systems or in people's heads. Accordingly, it encompasses not only technical security, but also the non-technical security of information, to which the three protection goals of information security apply. The protection goals include confidentiality, integrity and availability. People who are not sufficiently sensitized to the need to comply with the protection goals can endanger the entire company. As this topic is very abstract and difficult for people to grasp, it makes sense to use tools that communicate the most important information to the employees of a company in an entertaining way. Gamification is such an instrument in this context, which can support this process with game-like elements. In this master thesis, the topic of gamification and its use to raise awareness for information security is addressed. The focus is on its use in the higher education environment, where it is assumed that through the digitalization of teaching, gamification will also be used in one's own organization to train employees. For this purpose, a survey was conducted as part of this thesis at the association of "Centers for Communication Processing in Research and Teaching", to which a large number of German universities belong. Another small-scale survey of manufacturers of serious games and gamified online learning platforms describes the experiences these manufacturers have had to date with regard to the use of gamification at universities.

Copyright

Inhaltsverzeichnis

1. Einleitung ... 7
1.1 Motivation.. ... 7
1.2 Problemstellung ... 8
1.3 Herausforderungen ... 11
1.4 Zielsetzung und zentrale Fragestellungen ... 11
1.5 Struktur der Arbeit ... 12
2. Aktueller Überblick über Informationssicherheit und Awareness ... 14
2.1 Faktenlage.. ... 14
2.2 Begriffsbestimmung und Abgrenzung ... 15
2.3 Allgemeine Bemerkungen ... 17
2.4 Empirischer Forschungsstand ... 17
2.5 Cyber-Security Untersuchungen der ENISA ... 21
3. IT-Sicherheit ... 23
3.1 Angriffswege ... 24
3.1.1 Technische Angriffswege ... 24
3.1.2 Menschliche Angriffswege ... 29
3.2 Technische Sicherheitslösungen und ihre Grenzen ... 33
3.3 Lösungsmöglichkeiten ... 34
4. Psychologie ... 36
4.1 Verhaltensänderung ... 37
4.2 Verhaltensänderungsmodelle in der Cybersecurity ... 38
4.3 Studie von Foster ... 41
4.4 Studie von Landers und Landers ... 42
4.5 Persönlichkeitstypen ... 43
5. Motivationsforschung ... 47
5.1 Motive und Motivationsfaktoren ... 47
5.2 Selbstbestimmungstheorie ... 49
5.3 Anwendung in der Informationssicherheit ... 53
6. Kommunikation und Marketing ... 56
6.1 Sensibilisierung ... 56
6.2 Marketingmix ... 59
6.3 Storytelling.. ... 61
6.4 Verfassungsmarketing ... 62
6.5 Verfassungsmarketing in der Informationssicherheit für deutsche Hochschulen ... 64
7. Didaktik ... 73
7.1 Lerntypen… ... 73
7.2 Lernumgebung ... 76
7.3 Lerntheorien ... 79
7.3.1 Behaviorismus ... 79
7.3.2 Kognitivismus ... 79
7.3.3 Konstruktivismus ... 85
7.4 Spielebasiertes Lernen ... 86
7.5 Gamifiziertes Lernen ... 89
7.6 Frameworks ... 90
7.6.1 MDA-Framework ... 90
7.6.2 COFELET-Framework ... 91
7.6.3 OCTALYSIS-Framework ... 93
7.6.4 Kombination von OCTALYSIS- und MDA-Framework ... 100
7.7 Game-Design ... 104
7.8 Spielertypen ... 107
7.9 Spiel-Genres ... 108
8. Konzepterarbeitung ... 111
8.1 Experten-Interviews ... 111
8.2 Umfrage zum Einsatz von Gamification an deutschen Hochschulen ... 114

copyright

8.3 Entwicklung einer Anwendung mit Spielelementen ... 115
8.3.1 Zielgruppenstruktur an der Hochschule Anhalt ... 116
8.3.2 Kompetenzen der ausgewählten Zielgruppe ... 120
8.3.3 Lernziele der ausgewählten Zielgruppe ... 122
8.3.4 Rahmenbedingungen, Methoden, Medien und Organisation ... 124
8.3.5 Einsatz der Spielelemente für die ausgewählte Zielgruppe ... 125
8.3.6 Story-Entwicklung ... 129
8.3.7 Spielregeln, Spieldynamiken, Spiel-Genre und Spielziele ... 130
8.3.8 Storyboard ... 133
8.4 Messung von Effektivität und Nachhaltigkeit eines Schulungskonzepts ... 134
8.5 Negative Aspekte und Grenzen von Gamification ... 138
9. Zusammenfassung und Ausblick ... 141
10. Literaturverzeichnis ... 143
11. Bilderverzeichnis ... 149
12. Tabellenverzeichnis ... 150
13. Anhang ... 151
Anlage 1: Fragebogen zur Ermittlung der Spielertypen ... 151
Anlage 2: Interviews ... 154
Anlage 3: Auszüge aus der Umfrage im ZKI-Arbeitskreis ... 167
Anlage 4: Zielgruppenbildung der Hochschulangehörigen der Hochschule Anhalt ... 176
Anlage 5: Beispiele für Level-Abzeichen und Abschluss-Zertifikat ... 178
Anlage 6: Storyboard beispielhafter Szenen im entwickelten Bound ... 180
Anlage 7: gesamter erstellter Bound ... 182
Anlage 8: Flow-Kurzskala ... 200
Anlage 9: Beispiele der Einhaltung der Design-Empfehlungen ... 202
Anlage 10: Beispiel für Leitfragen zur Selbsteinschätzung von Kompetenzen ... 209
Anlage 11: Negativaspekte von Gamification ... 214
14. Abkürzungsverzeichnis ... 217
15. Glossar ... 218
16. Thesen ... 222
17. Selbständigkeitserklärung ... 223

Copyright

1. Einleitung

„Glück entsteht oft durch Aufmerksamkeit in kleinen Dingen, Unglück oft durch Vernachlässigung kleiner Dinge.“ (Wilhelm Busch, deutscher Dichter, Zeichner und Maler 15.04.1832 - 09.01.1908)

Es sind oft die kleinen vernachlässigten oder nicht wahrgenommenen Dinge, die in der Informationssicherheit zu einem großen Schaden führen. Beispielhaft seien hier die für Laien unscheinbaren, aber für Kriminelle bekannten Software-Sicherheitslücken genannt, die im Angriffsverlauf schamlos ausgenutzt werden.

1.1 Motivation

Angriffe auf IT-Systeme können heutzutage durch das Treffen entsprechender Vorkehrungen oft bereits im Entstehen verhindert werden. Diese Entwicklung beobachten auch die Angreifenden von IT-Systemen und spezialisieren sich zunehmend auf die psychologischen Komponenten, um einen Zugriff auf IT-Systeme zu erlangen und nachgelagert Angriffe durchzuführen. Durch Social Engineering-Methoden, die menschliche Schwächen wie Angst, Neugier, Druck, Leichtgläubigkeit, Vertrauen, Hilfsbereitschaft, Lob, Anerkennung sowie Reziprozität ausnutzen, werden die Benutzenden zu Aktionen wie der Eingabe von Benutzerinformationen in gefälschten Webseiten verleitet. Unter anderen Umständen wären sie aufmerksamer, sich der Gefahr bewusst gewesen und hätten somit das Unglück, Opfer eines Angriffes zu werden, vermieden. Im BSI-IT-Grundschutz[1], in der ISO 27001[2] und auch in der EU-DSGVO[3] stellt deshalb die Sensibilisierung von Mitarbeitenden für Informationssicherheit einen organisatorischen Punkt dar, der zusammen mit den wichtigsten technischen Maßnahmen als erstes umzusetzen ist. Die Absicherung der IT-Infrastruktur gegen ungewollten Datendiebstahl, ungewollte Datenoffenlegung und -veränderung ist das Zusammenspiel aus den beiden großen Komponenten „Technik“ und „Mensch“.

Die Master-Thesis beschäftigt sich mit der Verwendung von spieltypischen Elementen und Vorgängen in einem spielfremden Kontext – genannt Gamification[4] – zur

Copyright

Sensibilisierung für Informationssicherheit an Hochschulen in Deutschland. Denn auch die deutschen Hochschulen sind von Cyberangriffen betroffen – beispielhaft sei die Justus-Liebig-Universität in Gießen genannt[5] – und müssen entsprechend in der Informationssicherheit geschult werden. Mit der Implementierung von spielerischen Elementen in eine Sensibilisierungskampagne für Informationssicherheit wird sich vor dem Hintergrund der zunehmenden Digitalisierung der Hochschullehre eine motivations- und partizipationsfördernde Lernumgebung[6] versprochen, die nicht nur die Studierenden an der Hochschule anspricht, sondern möglichst alle relevanten Zielgruppen. Denn eine Sensibilisierungskampagne soll alle Benutzenden der Hochschulinfrastruktur adressieren und die Sachverhalte an der Stelle aufklären, wo sie von der jeweiligen Zielgruppe als interessant bewertet werden. Die generierten Schulungs- und Aufklärungsangebote müssen aus diesem Grund zielgruppenspezifisch ausgearbeitet werden. Dass dieser Weg im Bereich der Informationssicherheit auch zielführend mit Gamification beschritten werden kann, beweisen die in diesem Markt erfolgreich etablierten Dienstleister wie known_sense aus Köln, die Hidden Awareness UG aus Braunschweig, Fabula Games GmbH aus Dortmund, die mybreev GmbH aus Viersen oder die SoSafe GmbH aus Köln.

1.2 Problemstellung

Wichtig für eine gute Sensibilität der Benutzenden gegenüber möglichen Angriffen auf die Sicherheit der Informationen, ist der Aufbau eines Problembewusstseins und die Förderung der Erkennung von Angriffssituationen. Dazu ist eine ständige Schulung der Benutzenden notwendig, weil sich auch die Angriffsvektoren in einer stetigen Veränderung und auch „Verbesserung“ befinden. Beispielsweise unterscheiden sich E-Mail-Phishing-Angriffe (Angriffe zum „Passwort-Fishing“) heute stark von früheren Angriffen, in denen es durch überwiegend schlechte deutsche Grammatik noch einfacher war, ein Phishing zu erkennen. Die Angreifenden und die Werkzeuge, die von ihnen verwendet werden, haben sich entwickelt und machen es ungeschulten Personen zunehmend schwerer, Angriffe zu enttarnen.

Um Menschen in der Informationssicherheit zu schulen, müssen verschiedene Themenfelder beachtet werden, die dabei ineinandergreifen. Bei den Benutzenden von

Copyright

IT-Systemen treffen verschiedene Typen von Menschen auf unterschiedliche IT-Systeme mit differenzierten Ausstattungen, Anforderungen und mannigfaltigen Einfallstoren für Angreifende. Wie sich ein gewisser Typus Mensch auf einen bestimmten Trigger verhält, ist beispielsweise mit dem Fachgebiet der Psychologie erklärbar. Die Änderung eines Verhaltens ist ein tiefenpsychologischer Aspekt, welcher beachtet werden muss, wenn man eine Verbesserung oder auch die Gewährleistung eines bereits vorhandenen Informationssicherheitsniveaus innerhalb einer Organisation erreichen möchte. Das Ansprechen eines bestimmten Typs erfolgt in der Kommunikationstheorie ebenfalls über unterschiedliche Medien. Beispielsweise sprechen E-Learning-Formate Lerntypen an, die zumeist etwas stiller sind und während eines Präsenzseminars ungern öffentlich Fragen stellen.[7] Somit kommt zur psychologischen Komponente die kommunikative Komponente hinzu. Kommunikation ist bei Veränderungsprozessen wichtig, weil Veränderungen Stress und Emotionen erzeugen. Durch die richtige Kommunikation, die auch eventuell auftretende Emotionen berücksichtigt, ist eine Reduktion des Stressfaktors möglich.[8] Bei der Erstellung einer Kampagne für Informationssicherheit zum Zweck der Sensibilisierung spielt neben der Wahl der Kommunikationskanäle auch die Art und Weise, wie das Wissen vermittelt und von der Zielgruppe im Gedächtnis gespeichert wird, eine Rolle. Es ist somit das Sachgebiet der Didaktik als ein weiterer Baustein zu beachten.[8] Im engen Zusammenhang mit der Form des Lehrens und Lernens steht die Motivation des Menschen, etwas lernen zu wollen. Den Lehrenden muss es gelingen, die Motivation der Teilnehmenden über den benötigten Zeitraum zur Gedächtnisaufnahme aufrecht zu erhalten. Gamification ist dafür ein hilfreiches Mittel.[6]

Dass Gamification allerdings nicht alle Zielgruppen gleichermaßen anspricht, beweist eine Befragung im April 2018 von 1.516 aus Österreich und Deutschland. Dort gaben nur 27 % der Führungskräfte an, dass Gamification eine sinnvolle Ergänzung zur Motivation und Bindung von Mitarbeitenden ist. Dabei ist ein deutlicher Unterschied zu finden, betrachtet man die Altersstruktur näher. Denn bei unter 40-jährigem Führungspersonal liegt die Quote mit 41 % höher als bei über 40-jährigem Führungspersonal mit nur 21 %. Es scheint eine Frage des Alters zu sein, ob und vor allem was gespielt wird.[9] Auch an deutschen Hochschulen könnte das entscheidend für die Durchführung der Sensibilisierungskampagne sein. Denn auch dort ist die Altersstruktur ähnlich verteilt

Copyright

(19 % mit höherem Alter, 41 % in relativ jungem Alter gem. Bild 1).[10] Berücksichtigt man das Kriterium „Führungsebene“ gibt es erste Hinweise, dass die Vermutung stimmen könnte, dass das Alter in der Führungsebene besonders hoch ist. Eine im Jahr 2018 durchgeführte Auswertung von 81 Biografien von Personen in hochschulleitender Funktion an deutschen Universitäten liefert das Durchschnittsalter von 59 Jahren (gem. Bild 2).[11] Die Führungsebene ist aber diejenige Ebene, die die Informationssicherheit in Organisationen fördern muss. Über die Führungsebene werden Prozesse etabliert, die dann auch vorgelebt und gelebt werden müssen.

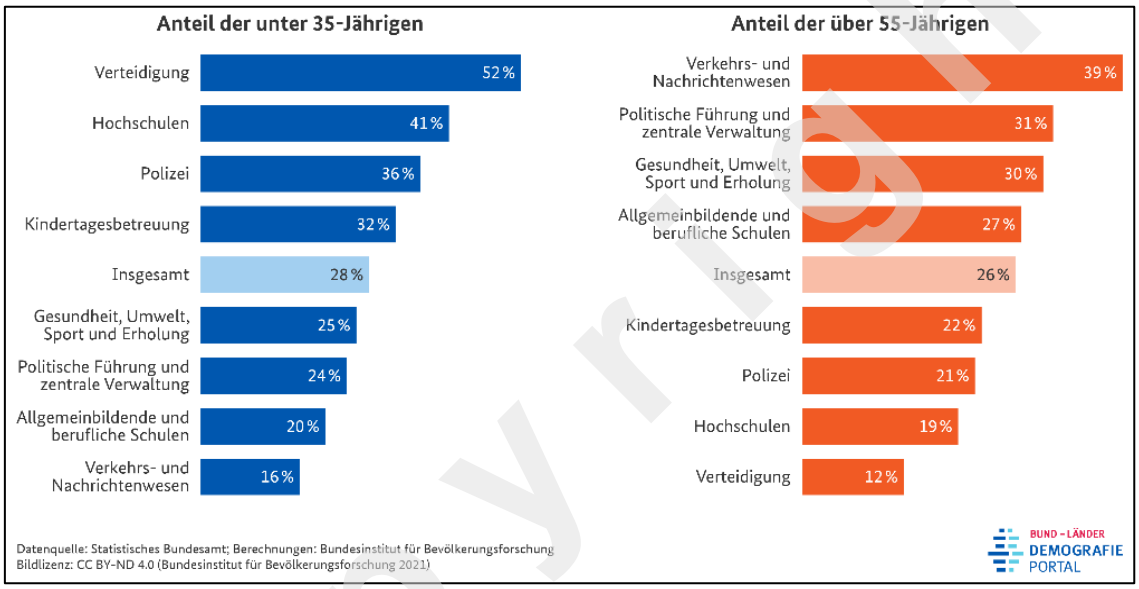


Bild 1: Altersstruktur der Beschäftigten im öffentlichen Dienst, 2020; Quelle: [10]

Bild 2: Ergebnisse der Auswertung von 81 Biografien an 81 deutschen Universitäten; Quelle: [11]

Copyright

Ein Spiel hat die Fähigkeit, Teams zusammen zu schweißen und somit das Arbeitsklima zu verbessern.[12] Eine Hochschule ist oft in festen Strukturen organisiert und Veränderungsprozesse deshalb nur schwer zu vollziehen. Wenn man die Führungsebene von der Sinnhaftigkeit und Nützlichkeit des Einsatzes von spieltypischen Elementen auch in Bezug auf das ernsthafte Thema Informationssicherheit überzeugt, ist der Weg für die verschiedenen Formen von Gamification zur Sensibilisierung und Schaffung von Security Awareness geebnet.

Jedoch ist die Führungsebene – unter der hier ausschließlich die Hochschulleitung zu verstehen ist – nur eine der Zielgruppen an einer Hochschule und auch eine relativ kleine. Um einen Großteil des Zielpublikums zu erreichen, muss sich eine Sensibilisierungskampagne in verschiedenen Medienformaten an alle Hochschulangehörige richten. Unter Hochschulangehörigen werden in diesem Zusammenhang die Professorenschaft, das mittlere Management, wissenschaftlich Beschäftigte, das Verwaltungspersonal und das IT-Personal verstanden.

1.3 Herausforderungen

Gamification wird in vielen Bereichen bereits eingesetzt und betrifft auch genauso viele. Kommunikation, Psychologie, Didaktik und Motivation sind Felder, die untersucht werden müssen. Im Rahmen der Didaktik wird es auch notwendig sein, Nachforschungen zur Spieleentwicklung, zum Spiele-Design und den notwendigen Merkmalen von Spielen anzustellen. Da diese Themengebiete insgesamt sehr groß sind, ist eine genaue Abgrenzung des Themenbereichs der Master-Thesis vorzunehmen.

1.4 Zielsetzung und zentrale Fragestellungen

In der Aufgabenstellung ist bereits das Ziel dieser Thesis ausführlich beschrieben. Neben der zentralen Frage nach einem Schulungskonzept für Hochschulen ist die Messbarkeit von Effektivität und Nachhaltigkeit dieses Konzepts zu untersuchen. Eine Analyse der ENISA (European Network and Information Security Agency) besagt, dass die Selbstwirksamkeitserwartung das einzige psychologische Konstrukt ist, das in einem messbaren Zusammenhang mit sicherem Verhalten steht.[13] Wie kann jedoch Selbstwirksamkeit gemessen werden? Welchen Einfluss haben die negativen Aspekte

Copyright

von Gamification wie Ablenkung, Attraktivitätsverlust, Verletzung der Privatsphäre, Manipulation, Spielsucht, Inakzeptanz, Gleichgültigkeit, Entmutigung, falsche Verstärkung, kommerzieller Zweck?[14] Treten die negativen Aspekte an deutschen Hochschulen überhaupt auf und wenn ja, wie können sie vermieden werden? Im dargestellten Kontext ergeben sich zahlreiche weitere Detailfragen, wie beispielsweise nach den verfügbaren Anreizsystemen im Bereich der Motivationsforschung und der Einordnung und Bewertung von Gamification. Die Sensibilität für Informationssicherheit in Unternehmen, auch Awareness genannt, soll durch Gamification gesteigert werden. Ist dieser Fakt empirisch belegt? Was macht die auf dem Markt befindlichen Sensibilisierungskonzepte so erfolgreich?

1.5 Struktur der Arbeit

Für die Erreichung der gestellten Ziele der Master-Thesis werden Befragungen mit Herstellern von Lernspielen und Awareness-Plattformen durchgeführt. Um den notwendigen Hochschulaspekt zu berücksichtigen, erfolgt mittels eines elektronischen Fragebogens eine online-Umfrage bei den Zentren für Kommunikationsverarbeitung in Forschung und Lehre als zentrale Vertretung für alle Hochschulen in Deutschland. Die Umfrage soll einen Einblick zum Einsatz von Gamification im Rahmen der Benutzendensensibilisierung für die Gewährleistung der Informationssicherheit an diesen Institutionen geben und die Möglichkeit zur Entwicklung eines universell einsetzbaren Systems eröffnen.

Aus der Literatur werden Typisierungen im Persönlichkeits-, Lern- und Spielendenbereich vorgestellt, Motivations- und Lerntheorien beleuchtet sowie Frameworks zur Umsetzung von Lernspielen und spielähnlichen Lernanwendungen beschrieben. Darauf aufbauend erfolgt die Entwicklung eines zielgruppengerechten Schulungskonzepts, in dem die zuvor genannten Theorien berücksichtigt und die passenden Spielelemente ausgewählt werden.

Im Zuge der Entwicklung des Schulungskonzepts werden Lerninhalte und spezifische Spielelemente auf verschiedenen Plattformen eingearbeitet, um neben der Darstellung der individuell zu schulenden Sicherheitsthemen auch den Gamification-Ansatz zu

Copyright

berücksichtigen. Es folgt eine Vorstellung einer Methode zur Beurteilung der Wirksamkeit des erstellten Schulungskonzepts. Mit der Zusammenführung aller Ergebnisse erfolgt ein Ausblick auf eine mögliche Weiterentwicklung des Konzepts.

Copyright

2. Aktueller Überblick über Informationssicherheit und Awareness

Bei Gamification wird das Ziel verfolgt, ein bestehendes Erlebnis zu verbessern, ein Verhalten zu motivieren oder auch zu verändern. In der Games-Branche steht Gamification nach wie vor hoch im Kurs, weshalb sich ein Blick auf die Entwicklungen in diesem Marktsektor lohnt.

2.1 Faktenlage

Die Games-Branche ist sehr erfolgreich. Während es im Jahr 2020 noch 8.325 Millionen Euro waren, die in Deutschland umgesetzt wurden, sind es im Jahr 2021 schon 9.756 Millionen Euro[15]. Auch das Alter der deutschen Spieler steigt von 35 Jahren im Schnitt im Jahr 2016 auf 37,5 Jahre im Jahr 2020. Die Anzahl der Deutschen, die Computer- und Videospiele mindestens gelegentlich spielen, steigt auf 58 %. Spiele werden überwiegend auf Smartphones gespielt, gefolgt von Spielekonsolen, PCs und Tablets. Es spielen mehr Männer als Frauen. 64 % der Gamerinnen und Gamer mögen an Games die Geschichten, die sie darin erleben können.[16] Dass die Simulation von Gefahrensituationen in Games durchaus sinnvoll sein kann oder auch die Beeinflussung von Verhalten mit Games funktionieren kann, zeigt eine repräsentative Umfrage mit 2.052 Beteiligten im Alter von über 16 Jahren, die das Potenzial an dieser Stelle noch nicht ausgeschöpft sehen (siehe Bild 3). Wenn man davon ausgeht, dass auch im Bereich der Informationssicherheit Gefahrensituationen vorherrschen, die ungeschulte Nutzer zu Opfern machen können und dass Simulationen dabei helfen können, diese Situationen im Vorhinein zu trainieren und damit auch ein sicheres Verhalten zu entwickeln, dann ist auch das ein Beispiel, in dem das Potenzial noch nicht vollständig ausgeschöpft ist.

Copyright

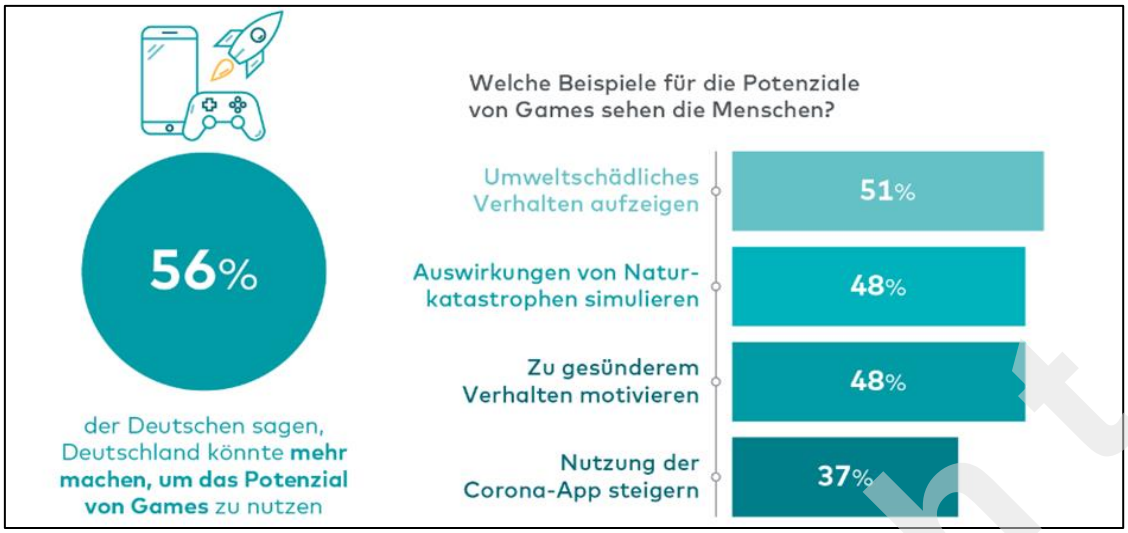


Bild 3: nicht ausgenutzte Potenziale von Games; Quelle: [16]

2.2 Begriffsbestimmung und Abgrenzung

Ein Spiel ist durch seine Gestaltung und seinen Inhalt nicht nur ein Medium zur Unterhaltung, sondern kann auch auf sozialer Ebene verbinden und auf kognitiver Ebene Wissen zur Problembewältigung aufbauen. Serious Games ist der Fachbegriff für solche Spiele, die auf spielerische Art ernsthaftes Wissen vermitteln.[17]

Trotz des eigentlichen Zwecks der Wissensvermittlung folgen sie den in der Definition eines Spiels festgelegten Elementen eines Spiels. Zu den Eigenschaften eines Spiels gehören Regeln, variable messbare Ergebnisse, den Ergebnissen verschieden zugeordnete Wertigkeiten, Herausforderungen, emotionale Kopplungen an das Ergebnis und möglicherweise reale Konsequenzen im Leben.[18]

Gamification ist ähnlich wie Serious Games auch eine Art regelbasiertes, zielorientiertes Spiel und somit nicht einfach nur „Playing“, was freies und regelloses Spielen mit Spielzeugen wäre. Dabei sind die Spielelemente immer in ein Produkt, eine Dienstleistung, Aktivität oder einen Prozess eingebunden. Die Bild 4 stellt die Unterscheidung zwischen beiden Spielarten noch einmal grafisch dar.[19]

Copyright

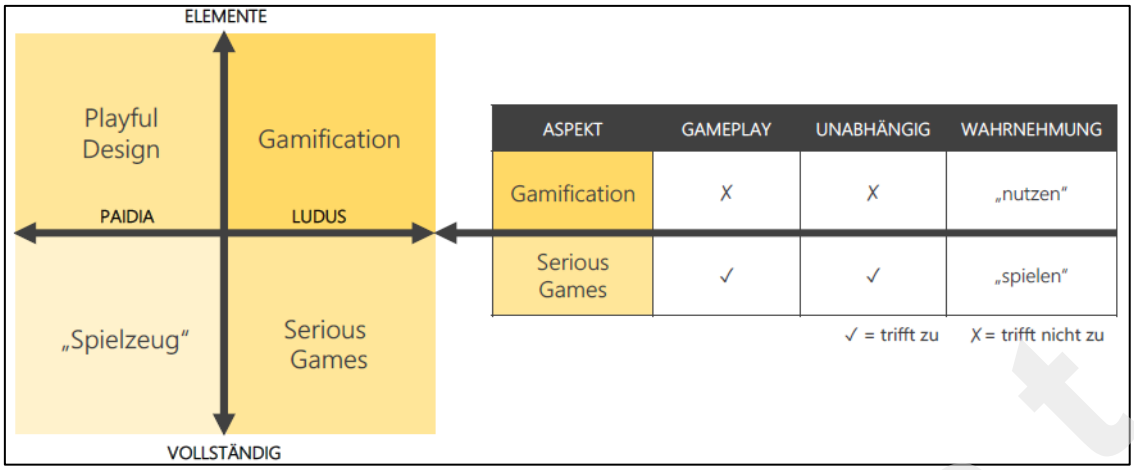


Bild 4: Unterscheidung Serious Game und Gamification; Quelle: [19]

Die Absicht, die hinter Gamification steckt, ist wie bei Serious Games, die Erhöhung der intrinsischen Motivation, ein ernsthaftes Thema freiwillig und mit Begeisterung inhaltlich möglichst umfassend zu begreifen und über diverse Übungseinheiten zu bearbeiten. Extrinsische Motivationsfaktoren in Form von Spiel-Elementen können dazu den ersten Impuls liefern (Wettbewerb). Gamification ist deutlich flexibler einsetzbar als Serious Games, welche immer eine Story benötigen und auch immer einen Abschluss. Auch die Anzahl der Spiel-Elemente ist groß sowie die Art des Spiels. Es ist möglich, die verschiedenen Genres eines Spiels zu integrieren, während dieses bei einem Serious Game von Anfang an festgelegt werden muss.

Schulungen, die einen ernsten Hintergrund haben, versuchen über diesen Ansatz im ersten Schritt die notwendige initiale Aufmerksamkeit für das Thema zu erzeugen. Informationssicherheit gehört zu dem Thema, mit denen man sich nur ungern auseinandersetzt, weil es als trocken, langweilig und komplex empfunden wird.[20] Durch die Darstellung der inhaltlichen Relevanz des Themas für die Zielgruppe soll das Interesse geweckt und mit Hilfe der Vermittlung und Abfrage von Wissen auf individueller Ebene die Motivation zur aktiven Teilnahme an der Schulung aufrechterhalten werden. Abgeschlossen werden die Schulungen dann mit einer für den Spielenden transparenten Bewertung der Lernleistungen, wozu auch wiederum der Einsatz von Spielelementen wie beispielsweise bestimmte Level-Auszeichnungen gehören.

Copyright

2.3 Allgemeine Bemerkungen

Gekaufte standardisierte Awareness-Produkte und vorgefertigte Phishing-Simulationen können kein über einen langen Zeitraum erlerntes Verhalten verändern, nur weil gerade eine Sensibilisierungskampagne notwendig geworden ist und das alte Verhalten von nun an als informations**un**sicher gilt. Was der Arbeitgeber lange Zeit toleriert hat, muss seinen Weg über die aktive Veränderung der angeeigneten Verhaltensweisen und Arbeitsabläufe in einem Veränderungsprozess finden, um zu mehr Informationssicherheit zu gelangen. Dabei ist es notwendig, die Schwachstellen in den Arbeitsroutinen zu analysieren und sukzessive durch die Vermittlung von Wissen und Methoden zur Risikoerkennung, -beseitigung und damit selbständigen Problembewältigung zu entfernen. Es geht um die Stärkung der Selbstwirksamkeit der Mitarbeitenden, die mit den ihnen zur Verfügung stehenden bzw. zur Verfügung gestellten Mitteln die Situation beeinflussen können und um die Machbarkeit in ihrem konkreten Arbeitsumfeld, die nur zusammen zu einer Veränderung führen. Selbstwirksamkeit gilt als eine Lerntheorie, die durch das Vertrauen in die eigenen Fähigkeiten und Möglichkeiten der Problembewältigung zu mehr Selbstvertrauen führt und damit eine bestimmte Lernmotivation begründet. Sie ist aber nach aktuellen Motivationstheorien wie beispielsweise der Selbstbestimmungstheorie nicht ausreichend, um die Lernmotivation in ihrer Gänze zu beschreiben.[21] Wichtig ist aber, dass überhaupt eine Motivation zum Handeln besteht. Wenn diese nicht schon bereits vorhanden ist, muss sie durch externe Trigger erzeugt werden. Das Verständnis für die Vorgehensweisen von Angreifenden, die gewohnte und unsichere Routinen für ihre kriminellen Zwecke ausnutzen können, lässt geschultes Personal die aktuelle Lage genauer einschätzen und ein der Situation angebrachtes Verhalten wählen. Um eine Erhöhung der Selbstwirksamkeit zu erreichen, ist es von zentraler Bedeutung, dass die Trainingsunterlagen Hinweise zur objektiven Beurteilung der Situation sowie eine möglichst standardisierte Vorgehensweise für eine einfache Umsetzung in der Realität enthalten.[13]

2.4 Empirischer Forschungsstand

Es gibt insgesamt 56 empirische Studien über Gamification in insgesamt acht verschiedenen Anwendungsgebieten, wobei der Bildungsbereich mit 17 Studien im Schul- und Hochschulkontext der am meisten erforschte Bereich ist. Wie aus

Copyright

Bild 5 ersichtlich, beschäftigen sich nur fünf Studien mit Gamification in Einführungsphasen und Trainings. Die Ergebnisse in diesen fünf Studien waren durchweg positiv. Die Studien zeigten, dass durch Gamification sichere Verhaltensweisen, Argumentationsfähigkeiten, die Selbstwirksamkeit und intrinsische Motivation sowie die Partizipation und das Engagement in Bezug auf den Lernprozess gefördert werden. Somit hat Gamification einen Anteil am Lernerfolg und an der Leistung der Teilnehmenden.[22]

Einführung und Training im Hochschulkontext

Quelle	Ziel	Spiel-Design-Elemente	Studientyp (N)	Befunde
Fitz-Walter et al. (2011, 2012)	Unterstützung des Einstiegs neuer Studenten an Universitäten	Levels, Abzeichen, Zielsetzung, Herausforderung	quantitativ (26; 121; 13)	Erleichterung des Einstiegs und der Orientierung, teilweise aber auch Verbesserungsbedarf (Pilotstudie, Usability-Studie, Fragebogen) *Ergebnistendenz: positiv*
Smith und Baker (2011)	Unterstützung der Orientierung in Bibliotheken und Training von Fähigkeiten	Rätsel, Level	quantitativ (388;52)	Förderung der Orientierung und der Fähigkeiten zur Nutzung des Bibliothekservices *Ergebnistendenz: positiv*
Foster et al. (2012)	Unterstützung von Lernaktivitäten im Ingenieurstudium	Abzeichen	quantitativ (300)	Förderung sicherer Verhaltensweisen und Argumentationsfähigkeit *Ergebnistendenz: positiv*
Snyder und Hartig (2013)	Förderung der Partizipation an Lernaktivitäten in der Facharztausbildung	Rätsel, Belohnung	quantitativ (181)	Förderung des Engagements und der Partizipation *Ergebnistendenz: positiv*
Banfield und Wilkerson (2014)	Förderung der Motivation und Selbstwirksamkeit bei Hochschulseminaren	Bestenliste	gemischt (96)	Förderung der intrinsischen Motivation und der Selbstwirksamkeit *Ergebnistendenz: positiv*

Bild 5: Studien zu Trainings mit Gamification-Kontext; Quelle: [22]

Es gibt jedoch bis heute keine empirischen Belege für die Wirksamkeit einzelner Spielelemente.[23] Die Kombination verschiedener Spielelemente und die Ableitung von Wirkung und Sinnhaftigkeit der einzelnen Kombination ist ebenfalls bis heute nicht ausreichend erforscht.[23] Auch die Theorie des gamifizierten Lernens liefert keine Informationen über wirksame Lernmechanismen, die durch die Elemente der Spielgestaltung ausgelöst werden. Diese Mechanismen befinden sich in anerkannten psychologischen Theorien, wie beispielsweise der Selbstbestimmungstheorie.[24] Diese beleuchtet die Motivation, den Willen etwas zu lernen, aus mehreren Perspektiven und interessiert sich dafür, ob die Motivation autonom oder kontrolliert und wie stark die Ausprägung ist.[25] Die Selbstbestimmungstheorie gehört somit zu den Motivationstheorien, womit Verhalten erklärt werden kann, welches durch bestimmte eingesetzte Spielelemente ausgelöst wird oder über bestimmte Wege erlernt wurde. Zu

Copyright

den wichtigsten Lerntheorien gehören Verhaltenslernen (Behaviorismus), Kognitivismus und Konstruktivismus. Diverse Ausführungen zu den Verhaltens-, Motivations- und Lerntheorien sind in den Abschnitten 4, 6 und 8 zu finden.

Die Untersuchung von Foster[22] (siehe Markierung in Bild 5) wird im Abschnitt 4 näher betrachtet, da in dieser Studie die Förderung sicherer Verhaltensweisen im Vordergrund standen und sie deshalb auch interessant für den Bereich der Informationssicherheit ist. Auch hier ist es wichtig, sichere Verhaltensweisen zu trainieren bzw. vorhandenes informationssicheres Verhalten zu fördern.

Für den Bereich E-Learning an Hochschulen gibt es elf Studien, die sich in diesem Zusammenhang mit Gamification beschäftigen. Interessant aus diesen Studien ist die Untersuchung von Landers und Landers[22] (rote Umrandung in Bild 6), da sie sich der Theorie des gamifizierten Verhaltens widmet. Vor dem Hintergrund der Entwicklung eines Schulungskonzepts für Informationssicherheit wird auch diese Studie im Abschnitt 4 mit in die nähere Betrachtung einbezogen.

Quelle	Ziel	Spiel-Design-Elemente	Studientyp (N)	Befunde
Cheong et al. (2013)	Steigerung des Lernerfolgs, Engagements und der Freude bei E-Learning	Punkte, Bestenliste, Feedback, Zeit(druck), Herausforderung, Rätsel	quantitativ (76)	Förderung des Engagements, der Freude und des Lernens *Ergebnistendenz: positiv*
Denny (2013)	Förderung der Aktivität bei E-Learning	Abzeichen	quantitativ (1031)	Förderung der Anzahl an beantworteten Fragen und Aktivität innerhalb der Lernplattform; kein Einfluss auf gestellte Fragen *Ergebnistendenz: positiv*
Domínguez et al. (2013)	Steigerung des Lernerfolgs bei E-Learning	Abzeichen, Bestenliste, Levels, Herausforderung	quantitativ (211)	Förderung der Leistung bei praktischen Aufgaben; allerdings ist Leistung bei schriftlichen Tests schlechter und Aktivität niedriger *Ergebnistendenz: gemischt*
Hakulinen et al. (2013)	Positive Beeinflussung von Verhalten und Förderung der Motivation	Abzeichen	quantitativ (281)	Verhaltensänderungen bei manchen Studenten, teilweise Förderung von Motivation *Ergebnistendenz: gemischt*
Landers und Landers (2014)	Förderung des Lernerfolgs (über Time on Task) bei E-Learning	Bestenliste	quantitativ (86)	Förderung von Time on Task und Mediation auf Leistung *Ergebnistendenz: positiv*
Shi et al. (2014)	Förderung der Motivation bei E-Learning	Herausforderung, Zielsetzung, Feedback, Narrativ	gemischt (15)	Förderung des Kompetenz- und Autonomieerlebens und des Erlebens sozialer Eingebundenheit *Ergebnistendenz: positiv*

Bild 6: Studien im E-Learning mit Gamification-Kontext; Quelle: [22]

Bei der Analyse der in den Studien verwendeten Spiel-Design-Elemente trifft man in der Regel auf Punkte (points), Abzeichen (badges) und Bestenlisten (leaderboards), den sogenannten PBL-Dreiklang. Meistens werden mehrere Spiel-Design-Elemente

Copyright

kombiniert.[22] Die meisten Forschungen gibt es zum PBL-Dreiklang. Weitere Design-Elemente wie beispielsweise Geschichten, Herausforderungen oder kontinuierliches Feedback werden nur selten verwendet. Jedoch enthalten wirklich effektive Gamification-Anwendungen gerade diese Elemente.[26] Die umfangreiche Verwendung des Dreiklangs in Studien hat mit dem notwendigen Ausschluss von Faktoren zu tun, die in wechselseitiger Beziehung mit den Spielenden stehen wie bspw. Elemente, die direkt Nutzererlebnisse ausdrücken oder Nutzerreaktionen zeigen und deshalb nicht für empirische Untersuchungen genutzt werden können. Bei der Durchführung von Studien müssen möglichst unabhängige Faktoren untersucht werden, um klare und eindeutige Ergebnisse zu erzielen. Für eine objektive Darstellung eignen sich für Analysezwecke daher Elemente der oberflächlichen Form. Dazu gehören Punkte, Abzeichen, Bestenlisten, Team-Bestenlisten, Leistungsgraphen, Narrativ und Avatar.[22]

Kritisch beurteilt wird die theoretische Fundierung der Studien, die zum großen Teil nur oberflächlich erfolgt oder gar nicht vorhanden ist. Die Studien, die auch theoretisch fundiert sind, beziehen sich zumeist auf die Selbstbestimmungstheorie der Motivation und deren Subtheorien. Vereinzelt werden die Theorie des geplanten Verhaltens oder des gamifizierten Verhaltens zur Bewertung herangezogen.[22]

Einen aktuellen Stand von Gamification in der Ingenieursausbildung in Kanada liefert eine systematische Literaturstudie von 15 veröffentlichten Arbeiten im Zeitraum von 2010 bis 2019. Sie dokumentiert den pädagogischen Einsatz von Spielelementen und kommt zu dem Schluss, dass die Lehrenden eine Vielzahl von Elementen einsetzen, um eine möglichst umfassende Gamification-Erfahrung zu schaffen. Neben Personalisierung und Level-Up verwenden sie für die Lernfortschrittsdarstellung häufig Punkte, Fortschrittsbalken, Freischaltungen und Abzeichen. Ebenso wichtig ist der Einsatz einer Möglichkeit, Fehler machen zu können. Der Lernende hat somit mehrere Versuche, eine Aufgabe zu lösen. Auch ein schnelles Feedback, ob ein Problem erfolgreich bearbeitet wurde, gehört zu den Spielelementen. Zur Verwendung der Wettbewerbsfunktion bemerkt die Studie, dass man sich der Gefahr bewusst sein sollte, dass sich nicht alle über den Wettbewerbsgedanken motivieren lassen. In engem Zusammenhang mit der Verwendung von Wettbewerb steht die Kooperation. In den meisten Fällen tritt dann ein

Copyright

Team gegen ein anderes Team an und muss kooperieren, um sein Ziel zu erreichen. Insgesamt liefert Gamification positive Ergebnisse in Form einer positiven Einstellung der Lernenden gegenüber Gamification, in Form der Leistungsverbesserung und Motivation oder in Form einer steigenden Teilnahmequote an solchen Veranstaltungen.[27]

2.5 Cyber-Security Untersuchungen der ENISA

Die ENISA führte eine Untersuchung von 688 Veröffentlichungen durch[28], wobei der Schwerpunkt auf der Analyse der verhaltenswissenschaftlichen Konstrukte für Cybersicherheit innerhalb von Organisationen liegt. Gemeint sind damit die Variablen, von denen man annimmt, dass sie das Verhalten der Menschen in Bezug auf die Cybersicherheit beeinflussen und somit zur Einhaltung oder Nichteinhaltung von Sicherheitsrichtlinien führen. Für die Ermittlung der Faktoren, die ein Sicherheitsverhalten zuverlässig vorhersagen, sichtete die ENISA die vorhandene Literatur in vier verschiedenen Datenbanken mit Zeitschriften- und Konferenzbeiträgen, von denen 47 Studien in die nähere Auswahl kamen sowie eine relativ aktuelle Übersichtsarbeit zu einem verwandten Thema. Gemäß der Analyse der ENISA behaupten die meisten Studien, eine Verbindung zwischen Konstrukten und Sicherheitsverhalten gefunden zu haben. Konstrukte sind in diesem Zusammenhang:

- Wissensaustausch über Informationssicherheit
- Zusammenarbeit
- Intervention und Erfahrung
- Verbundenheit
- Engagement
- persönliche Normen
- Einstellung zur Einhaltung von Informationssicherheitsrichtlinien
- Absicht zur Einhaltung von Informationssicherheitsrichtlinien[28]

Die Studien kamen zu dem Schluss, dass fehlendes Bewusstsein für Informationssicherheit, Unwissenheit, Nachlässigkeit, Apathie, Unfug und Widerstand Gründe für unsicheres Verhalten sind. Jedoch ist dies aufgrund fehlender Messungen wissenschaftlich nicht belegt. In der analysierten Literatur werden überwiegend drei

Copyright

Modelle für das Verständnis menschlicher Aspekte in Bezug auf die Cybersicherheit genannt:

- Theorie der Schutzmotivation
- Theorie des geplanten Verhaltens
- allgemeine Abschreckungstheorie[28]

Diese Theorien werden mit den bereits zuvor genannten Theorien im Abschnitt 4.2 Verhaltensänderungsmodelle in der Cybersecurity dieser Master-Thesis näher behandelt.

Copyright

3. IT-Sicherheit

Auch wenn sich immer mehr Menschen der Gefahren bewusst sind, die der Cyberraum für sie bereithält, so wissen doch nur wenige Menschen, dass sich dahinter ein richtiges Geschäftsmodell befindet. Die kriminellen Vereinigungen sind gut organisiert, haben ähnliche Strukturen wie legal am Markt befindliche Unternehmen und bieten ihre Dienstleistungen und Produkte häufig auch als „Crime-as-a-Service“ an.

Dass das Geschäftsmodell der Cyberkriminellen äußerst flexibel ist und über verschiedene Arten von Taktiken, Techniken und Verfahren verfügt, zeigen auch die verschiedenen auf dem Markt befindlichen Modelle zur Darstellung von Angriffsverläufen. Mit dem MITRE ATT&CK-Framework als ein Vertreter dieser Modelle können Mitarbeitende einer IT-Abteilung einen möglichen Angriffsverlauf skizzieren, einen erfolgten Angriff nachvollziehen oder selbst auch einen Angriff auf die eigene Infrastruktur durchführen, um mögliche Schwachstellen in einem Unternehmen aufzudecken und Maßnahmen daraus abzuleiten. “ATT&CK” steht dabei für Adversarial Tactics, Techniques und Common Knowledge. Mit dem sogenannten MITRE ATT&CK-Navigator kann der Verlauf von Cyberangriffen farblich markiert, mit Kommentaren und Verlinkungen versehen und als Tabelle exportiert werden. In Bild 7 wurde mit dem Navigator ein mögliches Angriffsszenario ausgewählt. Es beginnt mit der Erkundung und endet nach 13 weiteren Phasen mit der Verschlüsselung sämtlicher Benutzer- und Systemdateien und Festplattenpartitionen.

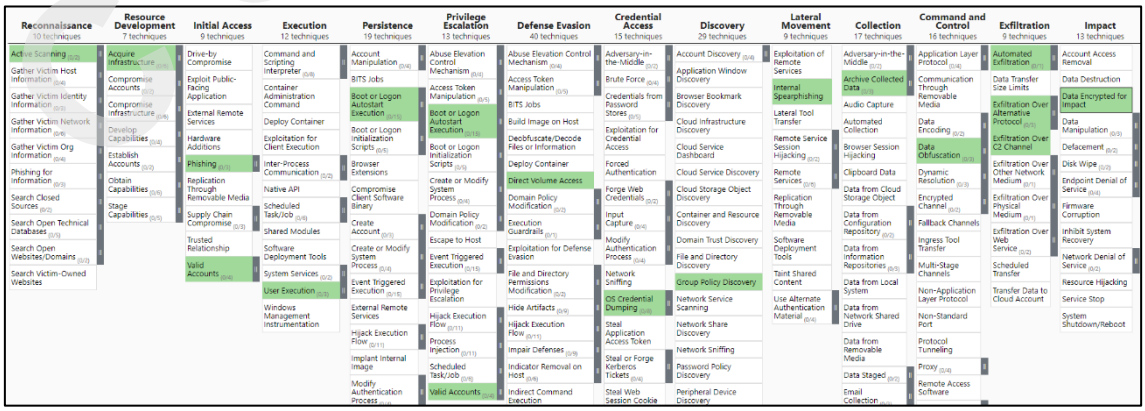


Bild 7: Darstellung eines Angriffsverlaufs im Mitre Att&ck Navigator; Quelle: https://mitre-attack.github.io/attack-navigator/

Copyright

Neben dem möglichen Vorgehen von Angreifenden beschriebt das Framework auch Verfahren, dieses Verhalten frühzeitig zu entdecken. So sind beispielsweise die Beobachtung des Netzwerkverkehrs, der an der Unternehmensgrenze in großem Umfang stattfindet und von einer einzelnen Quelle stammt, oder der Einsatz von Lösungen mit verhaltens- oder signaturbasierter Erkennung von Schadsoftware in Phishing-E-Mails, die Verwendung von Anwendungen zum Schutz des Netzwerkes und der Endpunkte vor der Ausführung schädlicher Dateien, die Durchsetzung von strengen Passwortrichtlinien für die Bildung starker Passwörter, die Überwachung der Benutzerkontenverwendung auf ungewöhnliche Zeiten, Mehrfachanmeldungen oder das Monitoring der Konfigurationseinstellungen für den Autostart von Programmen und auffällige Prozesse oder Skripte, die auf die Ausführung von Programmen für Credential Dumping hindeuten, als Maßnahmen zu nennen.[29]

3.1 Angriffswege

Anhand der im vorherigen Abschnitt beschriebenen Maßnahmen wird deutlich, dass Unternehmen einen enormen Aufwand für die Absicherung gegen Cyberbedrohungen betreiben müssen. Die Angreifenden dagegen müssen zunächst nur einen Angriffsweg wählen und können diesen, wenn er funktioniert, stringent weiterverfolgen. Bei der Wahl der Angriffsmethoden können sie aus einem großen Portfolio schöpfen. Die verwendeten Methoden basieren dabei auf der Ausnutzung von Schwachstellen in Protokollen, von „eingebauten“ Programmierfehlern in Software, von unsicheren Systemkonfigurationen oder auch von menschlichen Schwächen.

3.1.1 Technische Angriffswege

Zu den häufigsten Arten von Cyberangriffen gehören Angriffe auf Systeme mittels Schadsoftware, auf Protokolle, Webserver bzw. Webseiten, Hardware, Kennwörter, Programmschwachstellen, Lieferketten und auf IoT-Geräte.[30] Die Tabelle 1 zeigt einen Auszug der Methoden, die für die Angriffe verwendet werden. Im seit 2008 erscheinenden „Data Breach Investigations Report“ des US-amerikanischen Telekommunikationskonzerns Verizon[31] über die weltweite Entwicklung der Cyberangriffe wird festgestellt, dass vor allem die Verwendung von Ransomware und die Störung von Lieferketten in den letzten Jahren stark zugenommen haben. Bild 8 zeigt,

Copyright

dass die Verschlüsselung von Daten und die Erpressung von Lösegeld demnach eine sehr einträgliche Methode für die Angreifenden ist.

Tabelle 1: häufigste Arten von Cyberangriffen; Quelle: eigene Darstellung in Anlehnung an [30]

Schadsoftware-Angriffe	Protokoll-Angriffe	Webseiten-/Webserver-Angriffe	Hardware-Angriffe
Ransomware	TCP-SYN-Flooding	SQL Injection	infizierte Datenträger
dateilose Malware	Teardrop	Buffer Overflow	Hacking-Hardware
Malware-as-a-Service	Smurf	Denial of Service durch Botnetze	Sabotage
Viren	Ping of Death	Browserspeicher	
Keylogger (Spyware)	IP-Spoofing	Cross-Site-Scripting mittels VB Script, ActiveX, Flash, Java-script	
Trojaner	DNS-Spoofing		
Bots	ARP-Spoofing		
Rootkits	Replay-Angriff		
Backdoors	DNS-Tunneling		
Dropper			
Würmer			
Crypto-Malware			
Drive-by-Malware			
Kennwort-Angriffe	**Schwachstellen-Angriffe**	**IoT-basierte Angriffe**	**Lieferketten-Angriffe**
Brute-Force	Programmierfehler in Hard- oder in Software ausnutzen	zu Bots umfunktionierte IoT-Geräte	Angriff durch Schädigung eines Teilnehmers einer Lieferkette
Wörterbuch	Zero-Day-Exploits		
Geburtstagsparadoxon			
Rainbow-Table			
Pass-the-Hash			

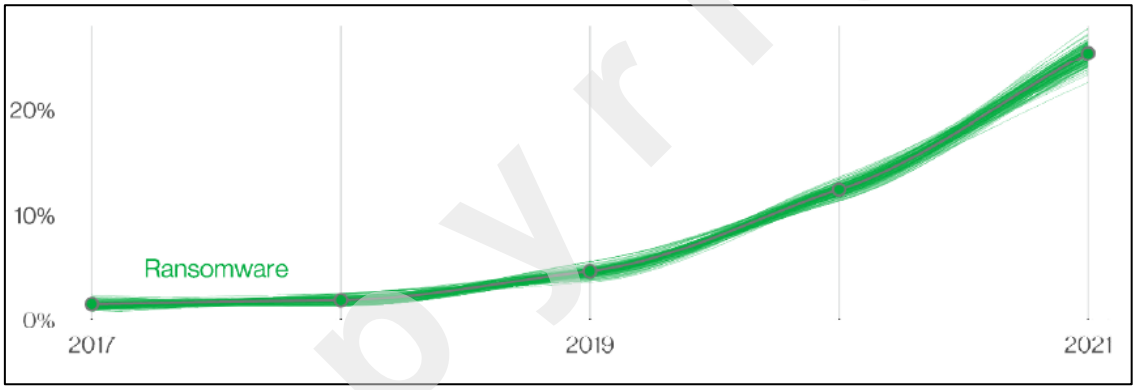


Bild 8: Entwicklung der Verwendung von Ransomware für Cyberangriffe; Quelle: [31]

Verizon[31] klassifiziert in seinem Bericht die verschiedenen Cyberangriffe ebenfalls in acht Cluster, die aber nicht allein technischen Angriffswegen zugeordnet werden:

- Technisch:
  - Angriffe auf Webanwendungen
  - DoS-Angriffe
  - Missbrauch legitimer Privilegien
  - Eindringen in Systeme im Sinne von komplexen Angriffen
- Nicht-technisch:
  - verlorene oder gestohlene Geräte
  - verschiedene Fehler durch unbeabsichtigte Handlungen

Copyright

- Social Engineering
- Technisch und nicht-technisch:
  - alles andere

In allen untersuchten Bereichen zeigt der Bericht hauptsächlich die vier in Bild 9 dargestellten Wege, die Angreifende nutzen, um einen Zugang zu fremden Systemen zu erlangen. An erster Stelle steht die illegale Nutzung von Anmeldedaten, gefolgt von Phishing und der Ausnutzung von Software-Schwachstellen. Auf der vierten Position rangiert die Verwendung von Botnetzen für Angriffszwecke, also die illegale Vernetzung von ferngesteuerten Computern zu einem großen Netz. Durch den Zusammenschluss zu einem großen Netz verfügen die Angreifenden über eine enorme Rechenleistung und damit Schlagkraft beim Angriff auf ein ausgewähltes Opfersystem.

Bild 9: Hauptangriffswege zum Eindringen in fremde Systeme; Quelle: [31]

Technische Maßnahmen, welche die Wege der Angreifenden stören, sind z. B. die Verwendung eines zweiten Faktors bei der Anmeldung an IT-Systemen, die Deaktivierung von verdächtigen Links und die Quarantäne-Verschiebung von verdächtigen Dateianhängen in Phishing-E-Mails sowie die zeitnahe Durchführung von Programm-Updates oder die sofortige Umsetzung von angebotenen „Workarounds“ zur Schließung von Sicherheitslücken bei noch nicht verfügbaren Softwareaktualisierungen.

Das Bild 10 zeigt die Top drei der Angriffsszenarien im Zeitraum von 2017 bis 2019 im Bildungssektor. Darunter befinden sich die Cluster „Eindringen in Systeme“, „Angriffe auf Webanwendungen“ und „unbeabsichtigte Handlungen“. Unter dem Cluster

Copyright

„unbeabsichtigte Handlungen“ ist eine Sicherheitsverletzung mindestens eines der drei Schutzziele Vertraulichkeit, Verfügbarkeit oder Integrität zu verstehen. Die genannten drei Cluster machen 80 % aller Vorfälle aus. Die Akteure sind zu 75 % externe Angreifende, die zu 95 % finanzielle Beweggründe haben.[31]

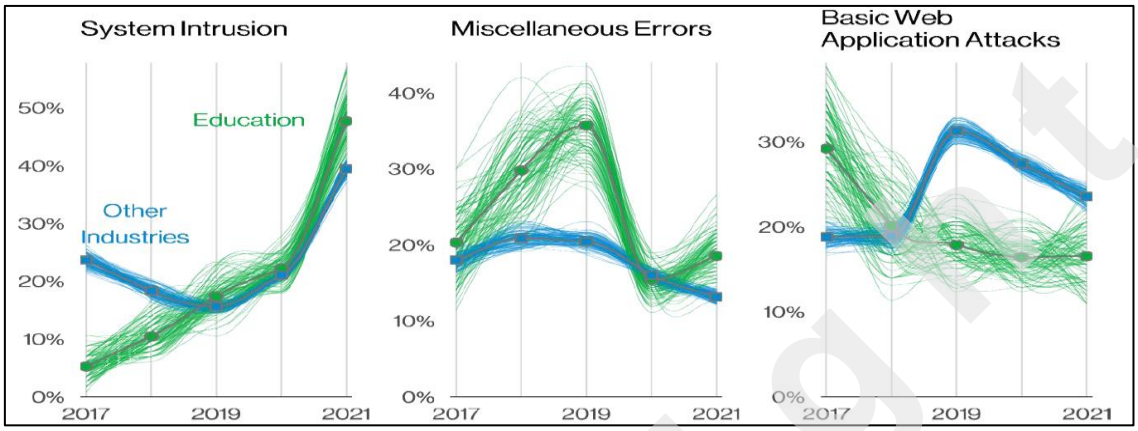


Bild 10: Top 3 Angriffscluster im Bildungssektor; Quelle: [31]

Webserver-Attacken, die unter das Cluster „Angriffe auf Webanwendungen“ (Basic Web Application Attacks) fallen, werden zu 80 % mit gestohlenen Anmeldeinformationen durchgeführt. Bild 11 zeigt, dass für den Zugriff auf Webserver zunehmend auch von der Methode des Ausnutzens einer spezifischen Schwachstelle mittels eines zur Verfügung gestellten Exploits Gebrauch gemacht wird.

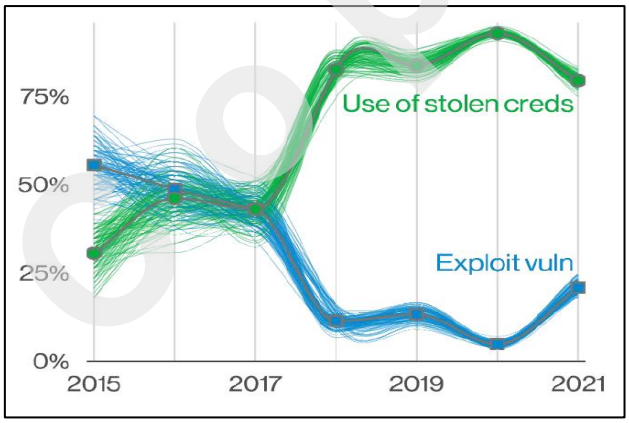


Bild 11: Verlauf der Angriffsmethoden im Cluster „Angriffe auf Webanwendungen“; Quelle: [31]

Das bedeutet im Umkehrschluss, dass z. B. mit einer Multifaktor-Authentifizierung und einem Tool zum sicheren Verwahren von Passwörtern in Form von Passwortmanagern

copyright

80 % der Angriffe auf Webserver und Webanwendungen erfolgreich verhindert werden können.

Im Cluster des „Eindringens in Systeme“ (System Intrusion) registrierte Verizon[31] im Jahr 2021 7.013 Vorfälle, von denen bei 1.999 Vorfällen Daten offengelegt wurden. Das bedeutet, dass bei mehr als einem Viertel der Fälle wissentlich Daten abgeflossen sind. Gestohlene Anmeldeinformationen, Ransomware und Backdoors oder Command- und Control-Infrastrukturen führen die Liste der verwendeten Angriffswerkzeuge an. Erschreckend ist die Erkenntnis, dass in diesem Zusammenhang diese Werkzeuge überwiegend aus der Installation von Software Updates, von Partnern oder auch aus der Verwendung von Bildschirmfreigabe-Software stammen, gefolgt von Email-Phishing und Exploit-Nutzung in Web-Anwendungen.

Beim „Eindringen in Systeme“ werden laut Verizon[31] komplexere Angriffe durchgeführt, die oft mehrere Maßnahmen aus dem sozialen und technischen Bereich kombinieren. Hier sind professionelles Hacking, der umfangreiche Einsatz von Malware und Angriffe auf Teilnehmende von Lieferketten zu finden. Wie aus Bild 12 ersichtlich, vermeiden Angreifende im Allgemeinen, mehr als drei Schritte für einen Angriff auszuführen. Je mehr Schritte ein Angriff umfasst, desto länger dauert dieser und desto größer ist die Chance für die Opfer, den Angriff zu entdecken und zu stoppen.

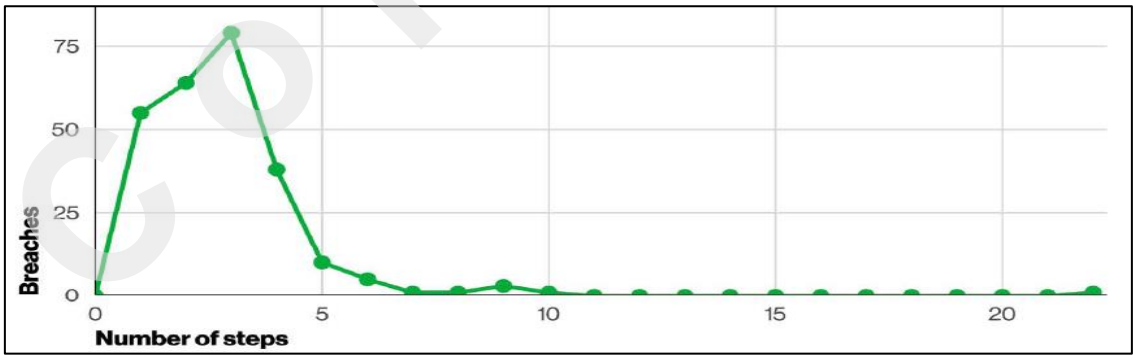


Bild 12: Durchschnittliche Anzahl an Angriffsschritten; Quelle: [31]

Dass gerade im Bildungssektor eine Vielzahl der Vorfälle in dieses Cluster eingeordnet werden, lässt den Schluss zu, dass die Angreifenden in diesem Bereich lange Zeit unentdeckt bleiben und genügend Zeit für die Fortführung des Angriffs haben.

Copyright

Zur Erkennung und Blockierung dieser Eindringversuche in Systeme stehen zahlreiche technische Lösungen wie Intrusion Detection- und Intrusion Prevention-Systeme (IDS und IPS), Next-Generation-Firewalls, zentrale Protokollierungsserver und Monitoring-Tools zur Verfügung. Sogenannte Security Information and Event Management (SIEM) -Systeme (wie z. B. das Produkt „Graylog“ (https://www.graylog.org)) können die Alarme und Logfiles dieser verschiedenen Systeme an zentraler Stelle sammeln, auswerten und dem Systembetreuer anzeigen, der diese entsprechend einschätzen muss.

Im Cluster der „Verschiedenen Fehler“ (Miscellaneous Error) befinden sich laut Verizon[31] hauptsächlich Vorfälle, die durch schlechte Systemkonfigurationen hervorgerufen wurden. Die Hauptverursachenden sind demzufolge nicht externe Angreifende, sondern zu 100 % interne Mitarbeitende, die offensichtlich nicht ausreichend in der sicheren Konfiguration von Systemen geschult sind.

Als technische Maßnahmen zur Entdeckung unsicher eingerichteter IT-Systeme stehen bspw. Tools zur Schwachstellenanalyse wie die Open Source Software „OpenVAS“ (Open Vulnerability Assessment System) der Firma Greenbone zur Verfügung. Über Scan-Berichte zu existierenden Sicherheitslücken und durch Visualisierung fehlerbehafteter Geschäftsprozesse zeigt dieses Tool den Systembetreuenden z. B. Fehler in Konfigurationseinstellungen an oder veraltete Betriebssysteme, abgelaufene Zertifikate, voreingestellte Standard-Benutzeranmeldungen und geöffnete Ports.[32]

3.1.2 Menschliche Angriffswege

Menschen werden angegriffen, weil auch sie Schwächen haben. Menschliche Schwächen, die von Angreifenden ausgenutzt werden, sind beispielsweise Hilfsbereitschaft, Vertrauen, Angst, Respekt vor Autorität, Neugierde, Faulheit, Überraschungseffekt, Scham, Schuldgefühl, Zorn, Stolz, Neid, Narzissmus und Mitleid.[33] Ergänzen kann man diese Aufstellung noch durch viele weitere menschliche Schwächen wie Druck, Leichtgläubigkeit, Lob, Anerkennung sowie Reziprozität. Dabei wird bei dieser Art des Angriffs – dem Social Engineering – die soziale Seite des Menschen ausgenutzt (social), um eine Beziehung aufzubauen (engineering). Stattfinden kann der Angriff auf einem analogen oder auch auf einem digitalen Weg.

Copyright

Analoges Social Engineering ist beispielsweise „Dumpster Diving“, „Tailgating“, „Media Dropping“, „Sextortion“, „Quid pro Quo“, Aushorchen von Personal, Ablesen von Informationen auf Flipcharts in Besprechungszimmern, am Arbeitsplatz der Mitarbeitenden oder in sozialen Netzwerken.[34][35][36] Die Beispiele zeigen, wie Faulheit, Hilfsbereitschaft, Neugierde, Druck und Reziprozität als Schwachstellen bei den Menschen ausgenutzt werden. Weitere Methoden des analogen Social Engineering zeigt die Tabelle 2.

Tabelle 2: Weitere Social Engineering-Methoden; Quelle: eigene Darstellung aus [36], [37]

Social-Engineering-Angriffe	Beschreibung der Methode
Pretexting	Nutzung eines frei erfundenen Vorwands, um an Informationen zu gelangen
Shoulder Surfing	Datendiebstahl durch Beobachtung über die Schulter z. B. bei der Eingabe von Passwörtern oder Geheimzahlen
Honeypots	Personen, die eine persönliche Beziehung aufbauen wollen, um sensible Daten zu sammeln

Wie aus dem Bild 13 ersichtlich, führt das analoge Social Engineering laut einer Bitkom-Studie[38] als Angriffsform neben dem Diebstahl von IT- oder Telekommunikationsgeräten die Liste der Ursachen von Angriffen auf Unternehmen und Informationen im Jahr 2019 an. Mehr als jedes fünfte Unternehmen war von dieser Angriffsform betroffen. Aber auch das digitale Social Engineering ist mit 15 % in den Top 9 der Ursachen für Angriffe aufgeführt, wozu auch E-Mail-Phishing gehört.

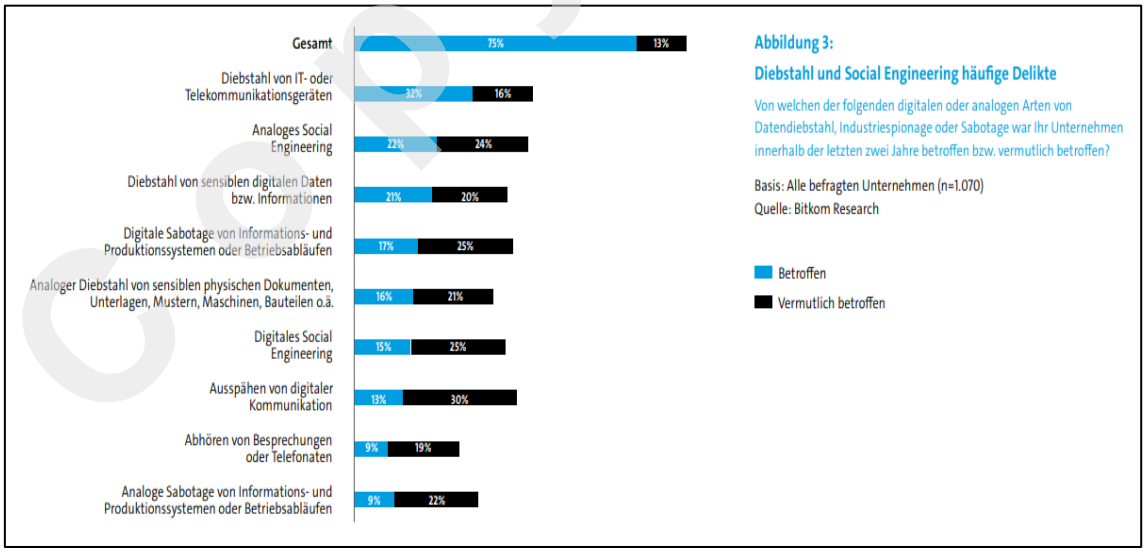


Bild 13: Ursachen von Informationssicherheitsvorfällen; Quelle: [38]

Die häufigste Angriffsart ist gemäß einer Umfrage des BSI[39] aus dem Jahre 2018 das Phishing. Bei über der Hälfte der gemeldeten Cyber-Sicherheits-Vorfälle ist Malware

Copyright

verwendet wurden, die in 90 % der Fälle in E-Mails verlinkt oder angehängt war. Die Hälfte dieser Angriffe konnte durch technische Schutzeinrichtungen eine Infektion verhindern. Die andere Hälfte wurde durch die Mitarbeitenden erkannt und blockiert. Genau diese Art der Interpretation und Erkennung sozialer Beziehungen und Inhalte können Computer nicht leisten.[40] Das bedeutet, dass der initiale Angriff auf die menschlichen Schwachstellen, um in ein IT-System einzudringen, mindestens genauso erfolgreich, wenn nicht sogar noch einfacher ist. Je authentischer, vertrauenswürdiger und plausibler eine elektronische Nachricht ist, desto eher erreichen die Angreifenden ihr Ziel. Die Vertrauenswürdigkeit von Nachrichten kann man z. B. mit Informationen erhöhen, die sehr privat sind und von denen das Opfer annimmt, dass keine fremde Person diese Informationen kennen kann. Mit sogenannten OSINT-Werkzeugen (open source intelligence) namens „Shodan“, „Maltego“ oder „theHarvester“, die sämtliche Daten über Personen und Unternehmen sammeln, finden auch die Angreifenden individuelle Informationen, um ihren Angriffserfolg im Rahmen vom Social Engineering-Attacken zu erhöhen.[40]

Tabelle 3 zeigt neben dem Phishing weitere Formen des digitalen Social Engineerings. Mit der Social Engineering-Angriffstechnik wird das menschliche Verhalten auf psychologischer Ebene manipuliert.[40]

Tabelle 3: weitere Formen des digitalen Social Engineering; Quelle: eigene Darstellung aus [35; 36; 41]

Social-Engineering-Angriffe	Beschreibung der Methode
Spear-Phishing	auf ein bestimmtes Ziel optimierte Phishing-Mails
Baiting	z. B. Angebot eines kostenlosen Downloads über ein Formular oder Link (Malware)
CEO-Fraud	Anweisung zur Überweisung hoher Geldbeträge durch angebliche Führungspersönlichkeiten
Tech-Support Scams	falscher Support, der per Remote auf den Rechner gelangen möchte, um die Daten zu stehlen
Watering-Hole	Malwareplatzierung auf oft besuchten Webseiten
Scareware	Software, die Ängste schürt und dann eine Malware als "Säuberungsprogramm" anbietet
Vishing	betrügerische Anrufe
Smishing	betrügerische SMS, die meist auf gefälschte Webseiten lockt
Impersonation	Diebstahl der digitalen Identität für missbräuchliche Zwecke

Beim menschlichen Verhalten ist zwischen automatischem und kontrolliertem Verhalten zu unterscheiden. Das automatische Verhalten erfolgt aufgrund festgelegter Handlungsmuster bzw. erlernter Standardreaktionen auf bestimmte Auslösemerkmale. Damit erspart sich der Mensch den Prozess der gründlichen Abwägung und damit Zeit bei der Entscheidungsfindung. Diese Verhaltensmuster sind fest verankert, führen

Copyright

meistens zum Erfolg und werden deshalb ohne weitere Überlegung angewendet. Je bedeutender aber ein Sachverhalt für einen Menschen ist, desto gründlicher analysiert er die Vor- und Nachteile und wägt ab, was seiner Ansicht nach, die richtige Entscheidung wäre. Dieses Verhalten wird als kontrolliertes Verhalten bezeichnet. Für die Abwehr von Social Engineering-Angriffen ist ein kontrolliertes Verhalten notwendig. Die Auslösemerkmale für automatische Verhaltensweisen sind Reziprozität, Konsequenz und Commitment, soziale Bewährtheit, Sympathie, Autorität und Knappheit.[40]

Sie werden von Social Engineers benutzt, weil die damit verbundenen Eigenschaften und Verhaltensweisen in der Natur des Menschen liegen. Der Mensch ist ein soziales Wesen und auf das Zusammenleben mit anderen Menschen angewiesen. Und um in einem sozialen Miteinander zu existieren, bedarf es bestimmter Regeln und Verhaltensmuster. Aristoteles bezeichnet das als Grundbestimmung des Menschen, der nur so seine Natur verwirklichen kann.[42]

Reziprozität bedeutet, dass derjenige, der gibt, eine Gegenleistung erwartet bzw. der andere sich dazu verpflichtet fühlt.[43] Konsequenz führt automatisch zur Erhaltung alter Verhaltensmuster, um nicht früher getroffene Entscheidungen revidieren zu müssen.[40] Wenn sich ein Verhalten in bestimmten Situationen im Miteinander mit Menschen bewährt hat und deshalb von anderen kopiert und automatisch ausgeführt wird, spricht man von sozialer Bewährtheit.[40] Der sogenannte „Halo-Effekt“ beschreibt die Überstrahlung negativer Eigenschaften von Menschen, wenn diese von ihrem Gegenüber als besonders attraktiv empfunden werden und deshalb automatisch sympathisch sind.[40] Mit autoritärem Auftreten kann ein bestimmtes automatisches Verhalten provoziert werden, wenn Menschen dafür besonders empfänglich sind.[40] Auch knappe Informationen, können für Menschen attraktiv sein und automatisches Verhalten auslösen, wenn deren Besitz als besonders wertvoll empfunden werden.[40]

Wenn die Mitarbeitenden eines Unternehmens diese Auslösemerkmale und die Methoden der Social Engineers kennen und gleichzeitig das automatische Verhalten in ein kontrolliertes Verhalten umwandeln können, dann besteht die Chance, diese Art der Angriffe zu identifizieren und abzuwehren. Schulungen und Trainings erhöhen die

Copyright

Chancen der Erkennung und sollten in Unternehmen stets präsent sein. Die Belegschaft darf sich auch zu keiner Zeit zu sicher vor Angriffen und Informationssicherheitsvorfällen fühlen, weil sie sonst auf reale Situationen nicht korrekt oder zu langsam reagieren.

3.2 Technische Sicherheitslösungen und ihre Grenzen

Wie bei jedem System haben auch die technischen Sicherheitseinrichtungen ihre Grenzen. Es kann zu sogenannten False-Positives oder False-Negatives kommen. Dabei handelt es sich um Falscherkennungen oder Nichterkennungen von Sicherheitslücken. Komplexe Angriffsverläufe können auch nicht in einem einzelnen System erkannt werden. Einzelne Sicherheitssysteme müssten gekoppelt werden, um diese sichtbar zu machen. Handelt es sich bei den technischen Sicherheitseinrichtungen um selbst programmierte Anwendungen, können diese auch nicht auf eine öffentlich bekannte Sicherheitsschwachstelle getestet werden, weil sie nicht unter öffentlicher Aufsicht stehen.[44] Oftmals ist die Konfiguration der IT-Systeme nicht trivial und sollte nur von gut geschultem IT-Personal vorgenommen werden. Die hohe Komplexität der Konfigurationsmöglichkeiten kann auch zu Fehleinstellungen und damit Sicherheitslücken führen, die trotz des Vorhandenseins z. B. einer Firewall eine Umgehung durch die Angreifenden ermöglichen. Ohne die Funktion der Anwendungserkennung in einer Firewall können bspw. ungewollte Anwendungsprotokolle über das http-Protokoll getunnelt werden und über einen anderen Port in das Netzwerk gelangen. Für die korrekte Funktionsweise der technischen Sicherheitslösungen ist neben der richtigen Konfiguration, auch die Aktualität der Systeme entscheidend, die ebenfalls vom Menschen gewährleistet werden muss. Der Abgleich von ankommenden Datenpaketen auf schadhafte Signaturen oder von Nutzendenverhalten auf anormale Muster mit in den Systemdatenbanken gespeicherten aktuellsten Informationen ist für die Erkennung und Blockierung der neuesten Angriffsmethoden essentiell.

Obwohl auch die Lernprozesse zur Verhaltensmustererkennung durch Angreifende manipuliert und die Systeme nicht vor Innentätern geschützt werden können, so leisten sie trotz allem eine Hilfestellung zur Entdeckung und Entfernung vorhandener Sicherheitslücken und Richtlinienverstöße in kompletten Netzwerken, Anwendungen

Copyright

und Diensten. Sie tragen zur Härtung der gesamten IT-Infrastruktur bei und erschweren maliziöse Angriffe. Wobei die Systeme jedoch keine Hilfe leisten können, ist nicht korrektes Verhalten aufgrund von Unsicherheiten des Personals in bestimmten Unternehmensprozessen, weil klare Vorgaben zum informationssicheren Verhalten fehlen. An dieser Stelle müssen organisatorische und personelle Maßnahmen eingesetzt werden, um diese Unsicherheiten zu entfernen.

3.3 Lösungsmöglichkeiten

Organisatorische Maßnahmen können Nutzungs- und Verhaltensrichtlinien sein, Verfahrens- und Arbeitsanweisungen sowie explizite Regelungen zur Festlegung von Verantwortlichkeiten und Zuständigkeiten. Zu den personellen Maßnahmen gehören Schulungen zur Erkennung von Phishing-Mails oder zur sicheren Konfiguration von IT-Systemen. Angriffe auf sozialer, analoger Ebene (siehe Abschnitt 3.1.2 Menschliche Angriffswege) können durch technische Maßnahmen allein nicht verhindert werden. Das bedeutet, dass das Personal befähigt werden muss, alle Angriffsversuche zu identifizieren und zu blockieren, auch solche, die auf menschlicher Ebene ablaufen. Diese sogenannte Information Security Awareness kann ausschließlich über die Kombination von Wissen, Wollen und Können geschaffen werden.[45] Die Anwendenden müssen in Schulungen die notwendige Motivation (Wollen) erhalten, das Wissen über die möglichen Bedrohungen erlangen sowie Techniken zur Erkennung und Behandlung dieser Bedrohungen gelehrt und trainiert bekommen (Wissen) und auch mit entsprechenden Werkzeugen ausgestattet werden (Können), um dieses Wissen später in ihrem Verhalten in einer bedrohlichen Situation zeitnah abzurufen.[45] Dieser Dreiklang wird von den vielen Einflussfaktoren auf das menschliche Verhalten determiniert. Ein einfacher Security-Workshop oder eine digitale online-Schulung ohne eine psychologisch aufbereitete, didaktisch wertvolle, kommunikative und werbende Hintergrundkampagne sind nicht ausreichend, um den geforderten Dreiklang herzustellen. Um Menschen und ihre Handlungen zu verstehen, um sie zu erreichen, zu überzeugen und vielleicht auch zu verändern, ist eine ganzheitliche Security Awareness notwendig, welche die Determinanten Didaktik, Marketing, Kommunikation und Psychologie berücksichtigt.[46]

Copyright

Die Literatur nennt folgende Empfehlungen, um eine gute Security Awareness mit seinen Determinanten in einer Organisation umzusetzen:

- *Training:* Einsatz von zur Organisationskultur passenden und strategischen Awareness-Maßnahmen
- *Didaktik:* interaktives und dialoggeführtes Veränderungsmanagement
- *Marketing:* Verwendung erprobter und fundierter Methoden
- *Kommunikation:* Kombination von klassischen und neuen, modernen Kommunikationsmedien
- *Psychologie:* Aufforderung zur Identifikation und zur Loyalität der Belegschaft mit und gegenüber dem Unternehmen.[46]

Das bedeutet, dass die einzelnen Fachdisziplinen die Gestaltung einer Awareness-Kampagne begleiten sollten. Das Gleiche gilt für den Aufbau einer Awareness-Schulung. Denn auch hier spielen Didaktik, Marketing, Kommunikation, Psychologie und Training eine große Rolle. Die herausgearbeiteten Informationen liefern wichtige Impulse für das Schulungskonzept und können den Grundstein für die Bewusstseinsbildung legen. Denn die Ausführungen in diesem Kapitel haben gezeigt, dass es technische und nicht-technische Bedrohungen gibt, die nicht ausschließlich durch technische und organisatorische Maßnahmen zu bekämpfen sind. Auch personelle Maßnahmen in Form von Schulungen müssen den Aufbau einer organisationsweiten Security Awareness unterstützen.

Copyright

4. Psychologie

Eine der Empfehlung für eine gute Security Awareness ist die Aufforderung zur Identifikation und zur Loyalität der Belegschaft mit und gegenüber dem Unternehmen.[46] Identifikation und Loyalität drücken die Bereitschaft von Individuen aus, sich in eine Gruppe zu integrieren und nach den gleichen Zielen zu streben. Identifikation ist dabei ein spezifisches psychisches Merkmal, das auf dem Gefühl des „Einssein“ mit der und eine Entscheidung für die Organisation beruht.[47] Bei 20.000 Entscheidungen pro Tag ist der Entscheidungsprozess für eine Sache äußerst wichtig.[48] Die Bedeutung und damit Entscheidung kann bei jedem Menschen unterschiedlich ausfallen, je nach individuellen und kulturellen Erfahrungen.[49]

Die Konsequenzen bei überwiegend subjektiv getroffenen Entscheidungen können sich auch als Fehlentscheidungen äußern, begründet durch eine Wahrnehmungsverzerrung oder einen Denkfehler des Menschen. Gerade bei der Bewertung von Risiken für die Informationssicherheit kann es zu Fehleinschätzungen kommen mit zum Teil ernsthaften Folgen. Es gibt verschiedene kognitive Verzerrungen, die ursächlich für diese Fehleinschätzungen sein können. Dazu gehören der sogenannte ökologische Fehlschluss, der Ankereffekt, die Verfügbarkeitsheuristik, der Bestätigungsfehler, der Framing-Effekt und der Attributionsfehler.[48]

Beim ökologischen Fehlschluss schließt man irrtümlicherweise von einem Gruppenverhalten auf das Verhalten einzelner Personen. Der Ankereffekt bedeutet, dass man nur die Gefahren wahrnimmt, auf welche man trainiert wurde. Die Verfügbarkeitsheuristik schätzt die Eintrittswahrscheinlichkeit eines Ereignisses höher ein, wenn scheinbar in allen verfügbaren Medien darüber berichtet wird. Wenn Informationen von einer Person so ausgewählt werden, dass sie der eigenen Erwartung oder Überzeugung entsprechen und andere Informationen ignoriert, vergessen oder unterbewertet werden, dann spricht man vom Bestätigungsfehler. Der Framing-Effekt ist die in einen sprachlichen Rahmen eingebettete Nachricht, welche vom Adressaten der Nachricht falsch empfangen wird. Ein Attributionsfehler liegt vor, wenn ein beobachtetes falsches Verhalten auf der Annahme von Eigenschaften einer bestimmten Gruppe von

Copyright

Menschen beruht und nicht auf einen möglichen Fehler bei einem selbst zurückgeführt wird.[48]

4.1 Verhaltensänderung

Eine unzureichende oder nicht durchgeführte Schulung sind zwei Begründungen für ein Verhalten, dessen Ursache in der Unternehmensorganisation liegen kann. Im Bild 14 wird das als Einschränkungen aus dem Umfeld betitelt. Das menschliche Verhalten wird aber noch von weiteren überwiegend persönlichen Faktoren beeinflusst (Wissen und Fähigkeiten, Salienz, Verhaltensabsicht und Gewohnheit).[45]

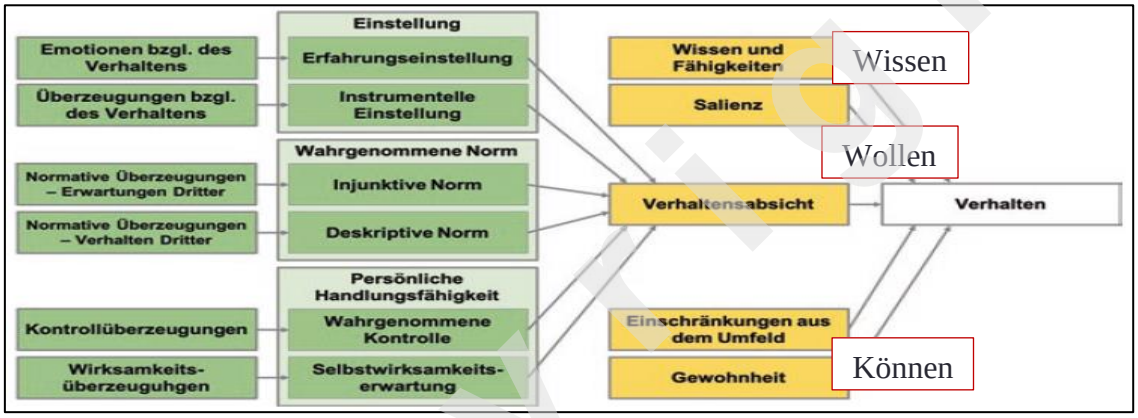


Bild 14: Prozess der Verhaltensbildung; Quelle: [45] (leicht verändert)

Salienz ist dabei die Bedeutsamkeit eines Verhaltens für einen Menschen. Wenn dieses Verhalten zur Gewohnheit wird, dann braucht es nur einen kleinen Anstupser (auch „Nudging“ genannt), um von der Person automatisch ohne weiteres Nachdenken ausgeführt zu werden. Es handelt sich um ein automatisches Verhalten. Den größten Einfluss auf das Verhalten hat aber der Punkt Verhaltensabsicht, die sich aus den drei Bereichen Einstellung, wahrgenommene Norm oder persönliche Handlungsfähigkeit ergibt. Die Einstellung einer Person kann aus eigenen Erfahrungen oder aus der persönlichen Einschätzung von Auswirkungen eines bestimmten Verhaltens resultieren. Die wahrgenommene Norm kann eine Empfindung sein, wie andere Personen das eigene Verhalten beurteilen oder wie die Person das Verhalten der anderen im sozialen Umfeld wahrnimmt. Mit Handlungsfähigkeit ist die persönliche Überzeugung einer Person zur Lösung einer schwierigen Aufgabe mit den eigenen vorhandenen Fähigkeiten (Selbstwirksamkeitserwartung) und die Einschätzung einer hohen Wahrscheinlichkeit

Copyright

über einen kontrollierten Einsatz der eigenen Ressourcen (vorhandenes Wissen zum Zeitpunkt) gemeint.[45]

Das Verhalten eines Menschen direkt verändern zu wollen, geht nur über Zwang, führt aber nicht zu einer höheren Awareness. Maßnahmen in der Sensibilisierung müssen also auf die Beeinflussung der genannten Faktoren Wissen und Fähigkeiten, Salienz, Gewohnheit und Verhaltensabsicht abzielen.[45]

4.2 Verhaltensänderungsmodelle in der Cybersecurity

„COM-B“- und „Fogg“-Verhaltensmodell

Das „COM-B“-Modell besagt, dass das Verhalten eines Menschen von der Fähigkeit (englisch: capability), der Gelegenheit (englisch: opportunity) zur Durchführung der Handlung und von der Motivation (englisch: motivation) abhängt.[50] Ein ähnliches Modell ist das vom Psychologen B. J. Fogg entwickelte Modell[51]. Es wird dort, wie im Bild 15 dargestellt, anstatt der Gelegenheit von Triggern (Prompts) gesprochen, die ab einer bestimmten Aktivierungsschwelle in Abhängigkeit von der Motivation und der Fähigkeit zum Handeln ein Verhalten mit einer gewissen Wahrscheinlichkeit auslöst.

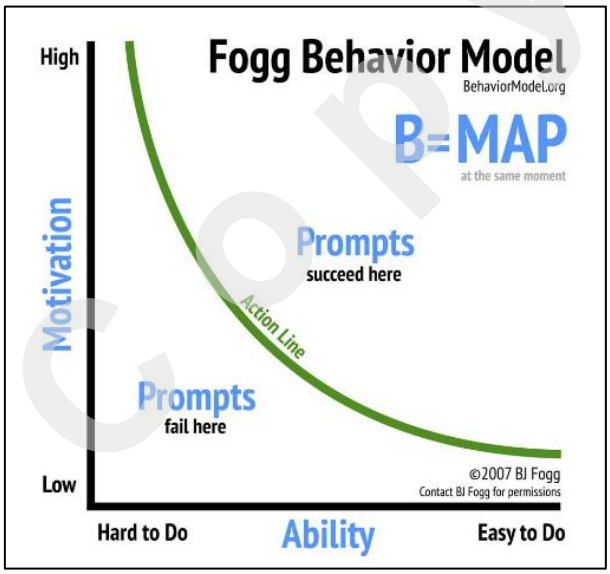


Bild 15: Darstellung des Fogg-Verhaltensmodells; Quelle: [51; 52]

Ist ein Mensch fähig, eine spezifische Aufgabe zu erledigen (z. B. die Bedienung einer Software zum Erstellen und Aufbewahren sicherer Passwörter (Passwortmanager)), wird ihm dazu auch die Gelegenheit gegeben (z. B. die Zurverfügungstellung der Software auf

Copyright

dem dienstlichen IT-Gerät) und ist er dann auch gewillt, zukünftig seine Passwörter mit dieser Software zu verwalten, weil sie sich sehr einfach und komfortabel bedienen lässt, dann ist er hochmotiviert, dies auch zu tun und dann kann es zu wirklich sicherem Verhalten kommen. Hinweisreize und Trigger auf das alte und unsichere Verhalten müssen dabei entfernt (z. B. selbstklebende Erinnerungszettel, auf denen gern das Passwort notiert und unter der Tastatur versteckt wurde) oder geschickt ersetzt werden. Die Erleichterung eines Prozesses durch eine komfortable Lösung ist ein Trigger, der zu einem bestimmten Verhalten führen kann. Bei einem Passwortmanager muss man sich nur noch ein einziges sicheres Passwort merken und die anderen sicheren Passwörter liegen geschützt vor dem Zugriff Dritter in einer Datenbank. Eine andere Variante wäre ein erscheinendes Warnsignal, wenn z. B. ein zu schwach gewähltes Passwort für eine Anwendung gewählt wurde. Ein weiterer Trigger kann auch nur ein Hinweis auf die Möglichkeit der Installation eines Passwortmanagers aus dem unternehmenseigenen Software-Kiosk sein. Wenn der Adressatenkreis dazu fähig und motiviert ist, eine Verbesserung und Arbeitserleichterung vorzunehmen, dann wird er die Installation höchstwahrscheinlich vornehmen.

Für die Motivation definiert Fogg die drei Elemente Empfindung, Antizipation und Zugehörigkeit.[53] Der Mensch handelt, wenn er dabei eine positive Empfindung hat oder eine mögliche negative vermeidet. Die positive Empfindung kann man durch Belohnung oder Freude an der Sache, weil z. B. etwas einfach zu verstehen und durchzuführen ist, hervorrufen. Er handelt außerdem, weil er damit einen positiven Zustand in der Zukunft anstrebt oder einen negativen verhindert (Antizipation). Wenn der Mensch z. B. durch die Aktivierung eines Newsletters immer auf dem aktuellen Wissensstand ist, dann vermeidet er dadurch einen möglichen Informationsverlust. Durch diesen Informationsvorsprung hat er in einer Gruppe möglicherweise mehr Anerkennung zu erwarten und handelt deshalb so. Würde er durch sein Handeln Ablehnung in der Gruppe erfahren, würde er diese unterlassen (Zugehörigkeit).

Kritikpunkt an diesen Verhaltensmodellen ist, dass alle drei Elemente (Motivation, Fähigkeit, Trigger bzw. Gelegenheit) zusammen in einer gewissen Stärke auftreten müssen. Fehlt ein Element oder ist nur unzulänglich vorhanden, dann tritt die Handlung

Copyright

nicht ein.[54] Ist beispielsweise die Motivation zu einem Verhalten nicht vorhanden, dann kann durch Aufklärung, Belohnung oder Bestrafung eine Motivation erreicht werden. Ist die Fähigkeit nicht in ausreichendem Umfang vorhanden, dann wäre eine Schulung ein Weg zur Befähigung.[50]

In beiden Modellen finden sich somit die drei Dimensionen „Wissen“, „Wollen“ und „Können“ wieder, die zu einem Verhalten führen. Die Benutzenden müssen wissen, wie es geht. Sie müssen die Fähigkeiten zur Ausführung haben. Sie müssen in der Lage sein, die Ausführung ohne Behinderung vorzunehmen. Sie müssen also auch die Gelegenheit dazu vom Unternehmensumfeld bekommen. Um das gewünschte Verhalten der Personen zusätzlich zu stärken, muss die Bedeutsamkeit eines sicheren Verhaltens (Salienz) hervorgehoben, die wichtigen Handlungen immer wieder trainiert (Gewohnheit) und Reize gesetzt werden, welche die persönliche Erfahrungen bereichern, die Selbstwirksamkeit und Selbstkontrolle fördern sowie positive Empfindungen bei angemessenem Verhalten auslösen (Verhaltensabsicht).

Weitere Verhaltensmodelle

Bei der *Theorie des geplanten Verhaltens* geht man davon aus, dass sich das Verhalten aus der Kombination von positiver persönlicher Einstellung gegenüber dem Verhalten anderer und subjektiv wahrgenommener Kontrolle über das eigene Verhalten ergibt.[50]

Bei der *Theorie der Schutzmotivation* werden Schutzmaßnahmen dann durchgeführt, wenn man eine Bedrohung oder die Verletzlichkeit als hoch einschätzt, diese jedoch mit vertretbarem Aufwand wirksam bekämpfen kann. Ist der Gewinn, den man durch Unterlassen der Bedrohungsbekämpfung erreichen würde höher und die Verletzbarkeit schätzungsweise niedrig, dann werden keine Schutzmaßnahmen durchgeführt, sondern das unsichere Verhalten weiterhin geduldet.[50]

Die *Selbstbestimmungstheorie der Motivation* besagt, dass ein Verhalten dann ausgeführt wird, wenn man es als von innen herausgewollt empfindet und man zusätzlich die Kontrolle darüber hat. Das subjektiv wahrgenommene Gefühl, über sein Handeln frei zu entscheiden, ist der Kern der Selbstbestimmungstheorie. Dabei kann der erste Anlass zur

Copyright

Handlung intrinsisch (von innen) oder extrinsisch (von außen) motiviert sein. Übertragen auf die Informationssicherheit bedeutet das, dass die informations**un**sicher verhaltende Person der Informationssicherheit einen hohen Wert beimessen muss, um zu einer Verhaltensänderung bereit zu sein. Die aktive positive Beeinflussung der Informationssicherheit wird dann als selbstbestimmt erlebt.[55]

Bei der *allgemeinen Abschreckungstheorie* wird davon ausgegangen, dass man ein ungewünschtes Verhalten beeinflussen kann, wenn man dieses Verhalten mit einer Unannehmlichkeit verbindet. Dabei muss die drohende Strafe mindestens genauso hoch sein wie die Attraktivität der ungewollten bzw. verbotenen Handlung. Es muss außerdem klar sein, dass die Bestrafung auch sofort und mit Sicherheit eintreten würde. Eine verbotene Handlungsoption wird gewählt, wenn deren subjektiv erwarteter Nutzen über dem Nutzen anderer Optionen liegt oder wenn die Sanktionswahrscheinlichkeit als niedrig eingestuft wird. In zahlreichen Untersuchungen wurde bewiesen, dass soziale Missbilligung, Gefühle der Scham und der Verlegenheit gegenüber anderen oft schwerer wiegen als die Bestrafung, die am Ende für das verbotene Verhalten droht.[56] Übertragen auf die Informationssicherheit kann man sich die allgemeine Abschreckungstheorie zunutze machen, indem man Handlungsoptionen anbietet, die attraktiver sind als die unsicheren Optionen und dass nicht mit Bestrafung gedroht, sondern eher die sozialen Faktoren „Teamgeist“ und „gemeinsame Zielerreichung“ in den Vordergrund gestellt werden.

Eine weitere Theorie zur Verhaltensänderung ist die des *gamifizierten Verhaltens*. Im Punkt 4.4 wird mit Bezug auf die Studie von Landers und Landers[22] noch einmal näher auf diese Theorie eingegangen. Im Abschnitt 5 erfolgt die detaillierte Untersuchung des Motivationsbegriffs, da dieser in nahezu allen Verhaltenstheorien von Bedeutung ist.

4.3 Studie von Foster

Die Studie von Foster[22] untersucht vornehmlich die Verwendung von Abzeichen als Spiel-Design-Elemente und ihrem Vermögen, das Verhalten von Lernenden zu beeinflussen bzw. zu ändern. Abzeichen werden in der Regel freiwillig gesammelt. Sie führen dazu, dass die Nutzenden einen bestimmten Wert erreichen wollen und sind somit

Copyright

für das Engagement von Lernenden förderlich. Abzeichen können Verhalten zusätzlich steuern, wenn sie mögliche gewünschte Aktivitäten aufzeigen. Sie laden außerdem zum Entdecken und Ausprobieren ein. Verliehene Abzeichen drücken die Interessen und das Wissen ihrer Besitzenden aus. Sie können auch als eine Art Statussymbol für das bereits Erreichte gegenüber anderen Personen dienen. Außerdem erinnern sie die Besitzenden in einer Art Feedback daran, was sie schon gelernt haben und bestärken sie somit in deren Selbstbewusstsein und fördern ein Kompetenzerleben. In einer Gruppe von Personen, die alle das gleiche Abzeichen besitzen, führen sie zu einer Art Zusammengehörigkeitsgefühl, wodurch erkennbar ist, dass offensichtlich die gleichen Interessen geteilt werden.[22]

4.4 Studie von Landers und Landers

Landers und Landers verwenden in ihrer Studie[22] die Bestenliste als Game-Design-Element und beschäftigen sich überwiegend mit der Theorie des gamifizierten Verhaltens. Landers und Landers bewiesen darin, dass Bestenlisten zu einer längeren Beschäftigung der Lernenden mit den Lerninhalten führen, was sich wiederum positiv auf den Lernerfolg auswirkt. Mit individuellen Bestenlisten ist es für die Teilnehmenden möglich, den eigenen Lernfortschritt zu verfolgen und den eigenen Leistungsstand zu evaluieren. Somit ist ein Kompetenzerleben mit Bestenlisten möglich. Bestenlisten führen aber auch dazu, dass Leistungen einzelner Nutzenden öffentlich einsehbar sind, was für die ein oder andere Person sehr demotivierend sein kann. Denn es wird nicht die Leistung des Individuums dargestellt, dessen Anstrengung für den erreichten Platz in der Rangliste vielleicht enorm gewesen sind. Es wird ein Vergleich zu den anderen Teilnehmenden der Gruppe gezogen, in dessen Folge die hart erbrachte Individualleistung vom Individuum als ein Misserfolg empfunden wird. Die individuelle Aufgaben- und Lernzielorientierung wird vor allem durch die Verwendung individueller Bezugsnormen gefördert und nicht durch soziale Bezugsnormen aus dem Vergleich mit einer Gruppe anderen Leistungsstands. Haben alle Teilnehmenden den gleichen Leistungsstand bzw. die gleichen Voraussetzungen und Fähigkeiten, dann kann eine Bestenliste auch zum Wettbewerb und damit zu einer höheren Anstrengung führen, was für den Lernerfolg förderlich ist. Die erreichte Platzierung muss dabei aber von allen Teilnehmenden klar nachvollziehbar sein, d. h. die zu erreichende Zielsetzung muss zuvor

Copyright

spezifisch, messbar, akzeptiert, realistisch und terminiert (SMART) für alle definiert werden. Ist die Bewertung der individuellen Leistungen von den Personen akzeptiert, dann kann die Bestenliste ebenfalls zu einem Kompetenzerleben beitragen, weil damit eine Reflexion auf die eigene Leistungsfähigkeit erfolgt.[22]

Im Bereich der Lehre kann Gamification als Zusatzinstrument eine Bereicherung für den Lehrinhalt sein. Denn es beeinflusst das Verhalten und die Einstellung von Lernenden, in dem es eine aktive Beteiligung und kontinuierliche Mitarbeit fordert und eine schnelle Rückmeldung erlaubt, allesamt Faktoren, die in der Lehre als wirksam empirisch belegt sind. Der Lernfortschritt wird nicht durch Gamification beeinflusst, sondern hängt ausschließlich vom Lehrinhalt ab. Gamification ist also lediglich eine Unterstützung zum bestehenden Lehrinhalt. Das Gute daran ist, dass durch diese Unterstützungsfunktion die einfache Integration in vorhandene Lehrkonzepte möglich ist.[23]

4.5 Persönlichkeitstypen

Um die Entwicklung von Menschen besser nachvollziehen zu können, klassifiziert man sie anhand ihrer Charakteristika in verschiedene Gruppen. Sie dient keinesfalls der Diskriminierung von Menschen. Im Bild 16 sind einige Klassifizierungsmodelle angegeben, welche die Menschen möglichst wertfrei nach bestimmten Merkmalen unterteilen. Unterscheidungsmerkmale können das Denken, Fühlen, Empfinden und die Intuition eines Menschen sein oder der Antrieb, die Aufmerksamkeit, die Entscheidung und der Lebensstil oder die Ausrichtung der Handlung auf Nähe, Distanz, Wechsel oder Dauer oder die Unterscheidung nach den „Big Five“.[57]

Copyright

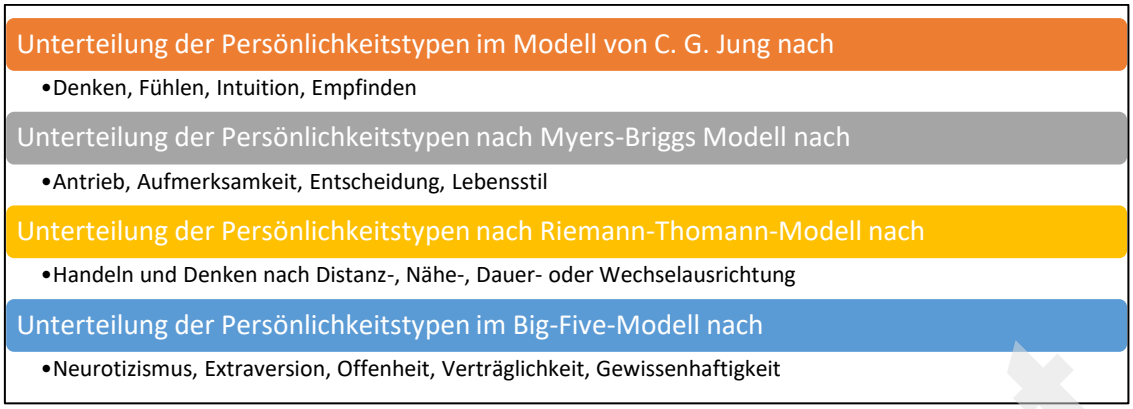


Bild 16: Modelle der Persönlichkeitstypen; Quelle: eigene Darstellung in Anlehnung an [57]

Das universelle Standardmodell der Persönlichkeitsforschung ist das Modell der „Big Five“. Es beschreibt dabei fünf Hauptdimensionen, in welche Menschen mit ihrer Persönlichkeit eingeordnet werden können:

- Offenheit für neue Erfahrungen, Erlebnisse oder Eindrücke
- Gewissenhaftigkeit bei guter Selbstkontrolle, Genauigkeit und Zielstrebigkeit
- Extraversion bzw. Begeisterungsfähigkeit für Aktivitäten und Zwischenmenschliches
- Verträglichkeit im Miteinander aufgrund von Vertrauen, Mitgefühl und Kooperation
- Neurotizismus durch Unzufriedenheit und das häufige Erleben negativer Gefühle

Die Unterschiedlichkeit zwischen den Menschen ist zu ca. 50 % auf die Genetik bzw. Vererbung zurück zu führen. Die andere Hälfte beeinflussen individuelle Umweltfaktoren.[58] Das Bild 17 zeigt die möglichen Ausprägungen der Persönlichkeitstypen mit den Eigenschaften, die sie am besten beschreiben, wobei die Zahl vier die höchste Ausprägung darstellt.

Copyright

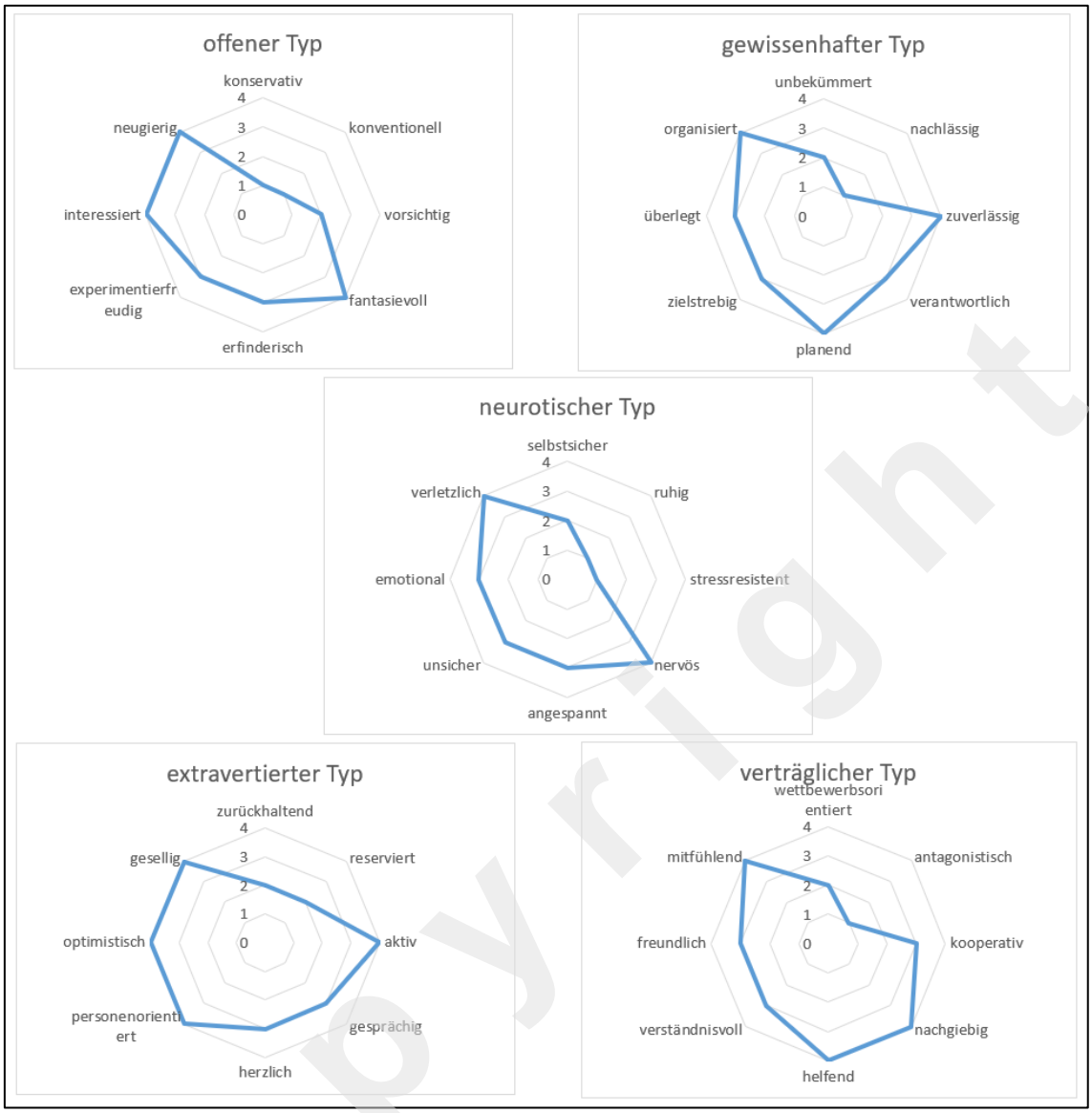


Bild 17: mögliche Ausprägungen der einzelnen Persönlichkeitstypen im „Big Five“-Modell; Quelle: eigene Darstellung in Anlehnung an [58]

Demnach ist der offene Typ vor allem neugierig, interessiert und fantasievoll sowie experimentierfreudig und erfinderisch. Der gewissenhafte Persönlichkeitstyp ist zielstrebig, zuverlässig, organisiert und handelt planerisch, überlegt und eigenverantwortlich. Neurotische Persönlichkeitstypen sind leicht verletzlich, sehr emotional, unsicher, angespannt und nervös sowie wenig stressresistent. Wohingegen extrovertierte Persönlichkeiten gern auf Menschen zugehen, gesellig, gesprächig, herzlich, optimistisch und aktiv sind. Menschen des verträglichen Persönlichkeitstyps helfen gern, sind verständnisvoll und freundlich, können mitfühlen, kooperativ und nachgiebig sein.[58]

Copyright

Die Persönlichkeit ist jedoch nicht nur genetisch- und umweltbedingt, sondern auch vom Alter abhängig. So gibt es verschiedene Entwicklungsphasen, in denen sich die Persönlichkeit herausbildet und auch noch verändern kann.

Im frühen Erwachsenenalter stabilisiert sich die Persönlichkeit, im mittleren und späten Erwachsenenalter kann sie sich noch einmal aufgrund der Lebenserfahrung und der sozialen Umstände verändern. Besonders der gewissenhafte und verträgliche Persönlichkeitstyp nehmen zu, wobei der offene Typ abnimmt.[58]

Das erklärt eventuell auch den recht schwierigen Einsatz von bestimmten Spielvarianten im höheren Alter. Spiele wie Ego-Shooter oder Sportsimulationen werden bei älteren Menschen selten gespielt. Reaktionsschnelligkeit oder schnelle Entscheidungen fallen im Alter 50+ zunehmend schwerer und werden deshalb eher abgewählt. Das heißt aber nicht, dass ältere Menschen gar nicht spielen. Durch die digitale Aufbereitung altbekannter Spielvarianten wie Skat, Puzzle oder Kreuzworträtsel und die Zurverfügungstellung auf mobilen Endgeräten wie Smartphones und Tablets werden ältere Personen auch in der Games-Branche erfolgreich in Deutschland angesprochen.[59]

Copyright

5. Motivationsforschung

Die verschiedenen Persönlichkeiten haben auch verschiedene Motivationen. In der Psychologie werden unter der Motivation emotionale Prozesse zur Setzung und Bewertung von Zielen verstanden, die zu einem Verhalten oder einer Handlung führen, wenn das Motiv stark genug ist.[60]

In der Motivationsforschung werden die Motive in verschiedene Arten unterteilt. Es gibt angeborene oder im Verlauf erworbene primäre bzw. biogene und sekundäre bzw. soziogene Motive sowie implizite und explizite. Primäre Motive oder auch Bedürfnisse sind z. B. angeborene existentielle biologische Grundbedürfnisse nach der Stillung von Hunger und Durst. Ein sekundäres Motiv ist z. B. das Zugehörigkeitsgefühl zu einer Gruppe und eine Folge der Sozialisation. Sekundäre Bedürfnisse werden häufig von den primären Bedürfnissen überlagert. Das bedeutet, dass ein sekundäres Motiv erst in Erscheinung tritt, wenn in diesem Moment die primären Bedürfnisse befriedigt sind. Implizite Motive sind unbewusste Bedürfnisse, die man suggeriert bekommen hat und welche sich über einen längeren Zeitraum zu einem großen Bedürfnis entwickelt haben. Explizite Bedürfnisse können bewusst benannt werden und entstehen auf der Grundlage einer kognitiven Verarbeitung. Persönliche Motive sind meistens explizite, sekundäre Motive.[60]

5.1 Motive und Motivationsfaktoren

Beispiele für persönliche explizite, sekundäre Motive sind das Leistungsmotiv durch Setzung eigener Ziele und Streben nach Anerkennung, das Machtmotiv mit dem Ziel der Beeinflussung anderer Personen, das Anschlussmotiv zur Besetzung einer Rolle in der Gesellschaft und das Selbstverwirklichungsmotiv aufgrund der Suche nach einem tieferen Sinn und persönlicher Entfaltung.[60]

Fehlt ein Motiv, kommt es nicht zu einer Motivation, welche wiederum für ein Handeln unabdingbar ist. Ein Motiv eines unbefriedigten Bedürfnisses muss dabei durch einen Anreiz aktiviert werden, was z. B. eine bestimmte Situation sein kann. Anreize bzw. Motivationsfaktoren können die Aussicht auf Belohnung, auf Anerkennung und Erfolg

Copyright

oder die Unterbeweisstellung der eigenen Fähigkeiten sein.[60] Diese Zusammenhänge verdeutlicht noch einmal das Bild 18.

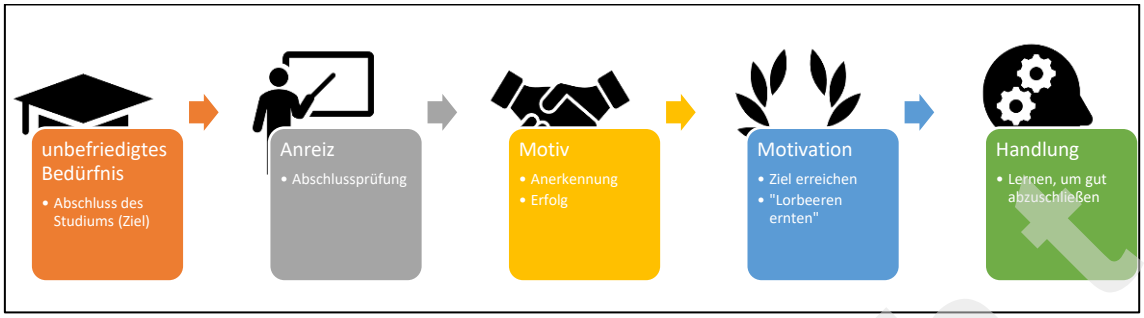


Bild 18: Voraussetzung für das Zustandekommen einer Handlung; Quelle: eigene Darstellung

Neben der Aussicht auf Belohnung in Form materieller Dinge wie Geld oder Sachpreise oder der Aussicht auf Erfüllung immaterieller Bedürfnisse wie Interesse, Selbstbestätigung, Macht, Verantwortung, Selbstentfaltung, Spaß an der Sache selbst, gesellschaftliche Interaktion und Mitgestaltung, Auszeichnung, Lob und Anerkennung der eigenen Leistungen durch andere oder die Repräsentation des Erfolgs gegenüber anderen Personen ist auch die Vermeidung von Strafen ein Motivationsfaktor.

In der Forschung wird oft auch die Bindung des Menschen an die jeweilige Organisation als Kern der Motivation angesehen. Bei Arbeitsorganisationen, bei denen man für seine Leistung eine Gehaltszahlung erhält und eine gewisse Verpflichtung eingeht, tritt die Bindung in Form der Identifikation mit dem Unternehmen auf. Je stärker diese ausgeprägt ist, desto länger wollen die Mitarbeitenden von sich heraus bei dem Unternehmen beschäftigt sein (affektives Commitment). Beim sogenannten normativen Commitment fühlen sich die Personen zum Bleiben und gegenüber den Werten und Zielen der Organisation sowie den einzelnen Mitarbeitenden verpflichtet. Wenn eine Person eine Abwägung zwischen dem Nutzen des Verlassens des Unternehmens und der damit verbundenen Kosten vorgenommen hat und diese Abwägung zugunsten des Verbleibs ausgefallen ist, dann spricht man vom fortsetzungsbezogenen Commitment.[61]

Die Gründe und die Einflussfaktoren, warum Menschen ein bestimmtes Verhalten zeigen, sind vielfältig. In der Freiwilligenarbeit zählen bspw. Werte, Erfahrungen, Schutz, Selbstwert, Karriere und soziale Anpassung zu den Gründen. Innerhalb dieser Funktionen

Copyright

gibt es bestimmte Anreize, die von innen heraus existieren (intrinsisch) oder von außen (extrinsisch) vorgegeben werden. [61]

Als nachhaltiger wird die intrinsische Motivation angesehen, weil sie von innen heraus entsteht und keine äußeren Reize benötigt, die immer wieder gegeben werden müssen. Menschen führen die Tätigkeit aus, weil sie ihnen Vergnügen bereitet. Sie erwarten dafür keine Belohnung. Die Ausführung der Handlung ist die Belohnung.

5.2 Selbstbestimmungstheorie

Ein Mensch, der eine bestimmte Motivation hat, erfüllt sich damit ein bestimmtes psychologisches Grundbedürfnis. Die menschlichen Bedürfnisse werden in verschiedenen Motivationstheorien untersucht. Neben der Theorie von Maslow[62], der Zwei-Faktoren-Theorie von Herzberg[63], der Human-Relation-Theorie[64] und dem Human-Resources-Ansatz[65], ist vor allem die Selbstbestimmungstheorie[66] interessant.

Sie besagt, dass das Verhalten nach dem bestimmt ist, inwieweit die Handlung von einem selbst und nicht durch äußere Zwänge hervorgerufen wird. Sie entstand auf theoretischen Überlegungen und Forschungen, dass der Mensch drei psychologische Grundbedürfnisse hat, die für seine Motivation ausschlaggebend. Zu ihnen zählen die Autonomie in Form eines Kontrollgefühls, die soziale Eingebundenheit durch ein Zugehörigkeitsgefühl und die Kompetenz durch ein Gefühl der Leistungsfähigkeit.[67]

Je nachdem, ob die Motive zur Handlung selbst- oder fremdbestimmt sind, unterscheidet man in die intrinsische und in vier Formen der extrinsischen Motivation, die sich vor allem über das Merkmal der relativen Autonomie und nicht über die Selbstwirksamkeit voneinander differenzieren. Es gibt die Externale, die Introjektion, die Identifikation und die Integration.[21]

Intrinsische Motivation

Die höchste Form der Motivation ist die intrinsische Motivation. Der Selbstbestimmungstheorie liegen mehrere Phasen zugrunde, angefangen bei einer

Copyright

fehlenden Handlungsabsicht (Amotivation), fortgeführt über eine extern oder selbst erzwungene Handlung bis hin zu einer freiwillig ausgeführten Handlung, weil sie interessant ist und Freude bereitet.[67] Die Selbstbestimmtheit ist da am höchsten, wo das Ausmaß einer als frei gewählt erlebten Handlung am größten ist.[68] Intrinsisch motivierte Menschen benötigen keine Anreize. Sie führen ihre Handlungen nicht ergebnisorientiert, sondern der Handlung selbst wegen durch. Die Handlung ist das Motiv.[69] Ein intrinsisch motivierter Mensch wird durch die Handlung und die unmittelbaren Gegebenheiten an sich neugierig gemacht, durch welche sein Entdeckergeist und seine Spontanität angesprochen werden. Das Handeln folgt der eigenen Auffassung von sich selbst.[68]

Eine hohe intrinsische Motivation ergibt sich aus einer hohen Selbstwirksamkeit bei der Aufgabenerledigung. Der Mensch entwickelt bei aktiven Prozessen ein tieferes Verständnis und entwickelt Fähigkeiten für die behandelte Thematik. Die intrinsische Motivation gilt als Schlüsselelement für ein erfolgreiches Lernen. Intrinsisch motivierte Personen sind neugieriger, interessierter und strengen sich mehr an als extrinsisch motivierte Menschen.[70]

Die handlungsleitenden Motive, die als selbstbestimmt wahrgenommen werden, lassen sich durch ein „ich will“ ausdrücken. Handlungen, die der Erfüllung sozialer Normen und Werte dienen, die aber persönlich nicht als wertvoll und wichtig erachtet werden, lassen sich durch ein „ich soll“ ausdrücken. Handlungen, die aufgrund einer externen Regulation durchgeführt werden, können durch ein „ich muss“ beschrieben werden. Der Grad der Selbstbestimmung sinkt von der höchsten Form der Motivation (intrinsische Motivation) bis zur Amotivation kontinuierlich ab.[69]

Extrinsische Motivation

Extrinsisch motiviertes Verhalten verfolgt ein bestimmtes Ziel, hat eine eindeutige Absicht und tritt klar getrennt von der eigentlichen Handlung auf. Spontanes Verhalten aus persönlichem Interesse gibt es bei einer extrinsischen Motivation nicht. Es handelt sich um instrumentelle, zuvor kalkulierte Verhaltensweisen.[68] Extrinsisch motiviert ist ein Mensch, wenn er nicht aus eigenem Antrieb ein Ziel anstrebt, sondern von außen zur

Copyright

Leistungserbringung gezwungen wird, etwa durch das Versprechen einer Belohnung oder durch die Androhung einer Strafe.[67]

Werden ausschließlich Belohnungen oder Strafen zur Motivation eingesetzt, handelt es sich um den Typ der externalen extrinsischen Motivation. Die Motivation zum gewünschten Verhalten ist fremdbestimmt und wird nur durch externe Faktoren aufrechterhalten. Fallen diese Faktoren weg, ist auch die Motivation für die Person, sich wie gefordert zu verhalten, nicht mehr vorhanden. Über kontinuierliche Kontrollen kann ein sich veränderndes Verhalten erkannt werden. Das ist sehr aufwendig und in Bezug auf die Erhaltung einer permanenten Aufmerksamkeit, die für die Gewährleistung eines bestimmten Informationssicherheitsniveaus notwendig ist, kein effektiver Weg für ein Unternehmen. Für die Aufgabenbearbeitung werden nur oberflächlich erlernte Strategien angewendet, die auch nur von geringer Qualität und Kreativität sind. Es werden keine ernsthaften Anstrengungen unternommen, die Thematik besonders gut zu verstehen und Wissen anzuwenden, sondern es wird sich eher vom Thema entfernt, da die Ziele fremdgesetzt sind. Die Selbstsicherheit, die in der Bewältigung einer realen Situation wichtig wäre, ist nicht vorhanden, sondern eher von negativen Gefühlen wie Angst oder Stress geprägt, weil man sich der Anforderung nicht gewachsen fühlt.[21]

Wenn eine Person handelt, um den sich selbst auferlegten Pflichten, die sie aus ihrem sozialen Umfeld kennt, gerecht zu werden und um dafür Zustimmung und Anerkennung von außen zu erhalten, dann spricht man vom Typ der introjizierten extrinsischen Motivation. Schuld, Scham oder Angst vor Nichtakzeptanz und Nichtzugehörigkeit sollen durch die persönliche Übernahme der allgemein akzeptierten Anstrengungen für eine gute Leistung vermieden werden.[21] Die Person setzt sich durch die sie umgebene Umwelt unter Druck, empfindet es aber nicht als fremdbestimmt. Die Umwelt ist an diesem Prozess nicht aktiv beteiligt, beeinflusst jedoch indirekt die Motivation der Person.

Identifiziert ein Mensch eine Handlung als wichtig und für die Zielerreichung notwendig, dann ist die Tat identifiziert extrinsisch motiviert. Er erachtet die Angelegenheit als besonders wertvoll und handelt aus innerlicher Überzeugung. Die Umsetzung erfolgt auf

Copyright

Basis eines bereits persönlich entwickelten Interesses an der Sache und wird als weitestgehend selbstbestimmt und freiwillig empfunden bei positiver Selbsteinschätzung der dafür erforderlichen und vorhandenen Kompetenzen.[21]

Wenn die Tätigkeit mehrmals aufgrund ihrer eingeschätzten Notwendig- und Wichtigkeit zur Gewohnheit und in den Tagesablauf integriert wird, dann spricht man vom Typ der integrierten extrinsischen Motivation. Genauso wie der identifizierte Typ der extrinsischen Motivation als selbstbestimmt erlebt wird, wird auch die integrierte extrinsische Motivation als selbstbestimmt empfunden.[71]

Das Bild 19 verdeutlicht die vier Typen der extrinsischen Motivation und die Zunahme des Empfindens der Selbstbestimmtheit.

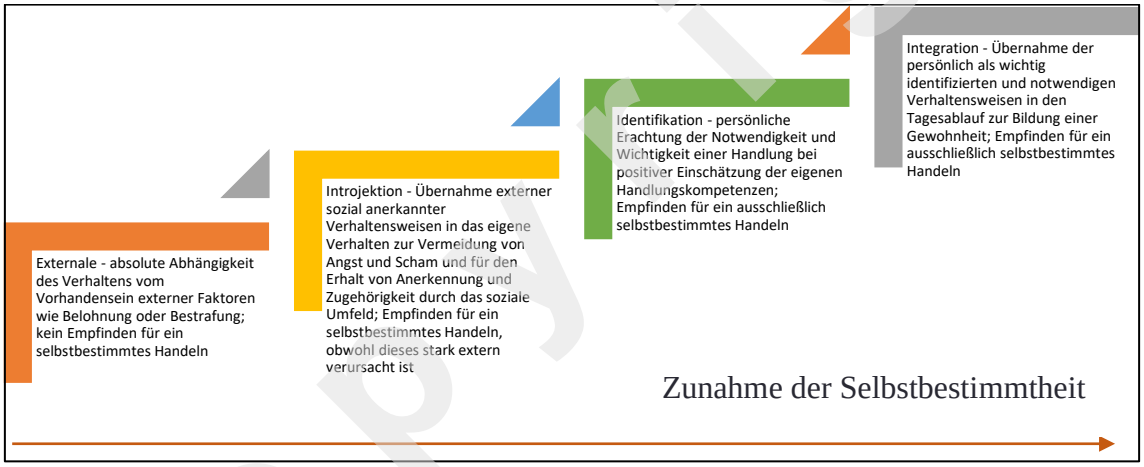


Bild 19: Darstellung der vier Typen der extrinsischen Motivation; Quelle: eigene Darstellung

Die beiden letztgenannten Typen der extrinsischen Motivation können ähnliche Merkmale wie die intrinsische Motivation aufweisen, wenn der Grad des Empfindens für die Selbstbestimmtheit hoch ist und die Zielsetzung verinnerlicht wurde. Anderenfalls verändern sich die anfänglich positive Stimmung, die gute Leistung, das Wohlbefinden und der Umgang mit Misserfolgen in negativer Weise.[67] Der Prozess, durch welchen externe Werte in die internen Regulationsprozesse eines Menschen übernommen werden, wird Internalisation genannt. Werte, die aus dem sozialen Umfeld des Menschen stammen, werden oft aus dem Grund des Zugehörigkeitsgefühls internalisiert und

Copyright

integriert, so dass der Mensch ein extern dargestelltes Verhalten dann trotzdem als selbstbestimmt erlebt.[68]

Die spezifischen Merkmale der Motivationen stellt Tabelle 4 noch einmal gegenüber. Bis sich die der intrinsischen Motivation ähnliche integrierte Motivation entwickelt hat, sind extrinsische Motivationsfaktoren, wie etwa spezifische Ziele in Wettbewerben (Gamification), ein wirksames Mittel. Die Durchführung von Wettbewerben beeinflusst die Beteiligten in der Weise, dass sie durch mehr Lernen auch über mehr Wissen verfügen und somit dem sozialen Leistungsdruck durch die Gruppe besser standhalten, wodurch sich auch deren Selbstwirksamkeitsüberzeugung verbessert.[70]

Tabelle 4: Merkmale der Motivationen; Quelle: eigene Darstellung

Merkmale	Art der Motivation				
	extrinsische Motivation →				intrinsische Motivation
Phasen	Externale	Introjektion	Identifikation	Integration	-
Motiv	fremdbestimmt	übernommen	Handlung als wichtig erkannt	weitgehend selbstbestimmt	selbstbestimmt
Handlungsabsicht	fehlend (Amotivation)	extern erzwungen	selbst erzwungen	freiwillig	aus Eigeninteresse
Anreize	Belohnung Bestrafung	Zustimmung Anerkennung	persönliches Interesse an der Sache Angelegenheit wertvoll	Notwendigkeit und Wichtigkeit Zugehörigkeit	nicht nötig -
Selbstwirksamkeit	niedrig	unsicher	positiv eingeschätzt	am höchsten	am höchsten
Leitsatz	ich muss	ich soll	ich will	ich bin es gewöhnt	ich handle einfach
Selbstbestimmung	am niedrigsten	höher	hoch	am höchsten	am höchsten
Ziel	definiert	übernommen	als notwendig identifiziert	integriert	die Handlung selbst
Verhalten	ergebnisorientiert instrumentell kalkuliert direkt von der Umwelt beeinflusst ohne besondere Anstrengungen oberflächlich	setzt sich selbst unter Druck indirekt von der Umwelt beeinflusst hohe persönliche Anstrengungen von der Umwelt übernommen getrieben -	aus entwickelter Überzeugung hohe persönliche Anstrengungen bewusst - - -	gewohnheitsmäßig Erfüllung ohne Anstrengung ohne Einfluss aus der Umwelt routiniert - -	spontan aus persönlichem Interesse ohne Einfluss aus der Umwelt Erfüllung ohne Anstrengung automatisch - -

5.3 Anwendung in der Informationssicherheit

Die Personen, die sich wenig für das Thema Informationssicherheit interessieren, muss man mit äußeren Reizen extrinsisch zur Anwendung der empfohlenen Verhaltensweisen motivieren und Schritt für Schritt zur Verinnerlichung des Verhaltens bringen, welches dann immer mehr einer intrinsischen Motivation ähnelt. Die Menschen ohne intrinsische Motivation führen keine informationssichere Handlung ihrer selbst wegen aus, sie benötigen ein Ziel, weshalb sie eine Handlung informationssicher ausführen sollen. Über die Darstellung der Schwachstellen ihrer derzeitigen unsicheren Verhaltensweisen und die Vorstellung einer alternativen informationssicheren und stets attraktiven, mit einer in ihren Augen lohnenswerten Anreizen ausgestatteten Handlungsanweisung ist es möglich, zu dieser Verinnerlichung zu kommen.

Copyright

Das sogenannte Nudging ist eine Anwendung, den Kontext eines Verhaltens zu verändern, indem man den gewünschten Weg durch eine kleine Beigabe attraktiver gestaltet. Damit wird nicht das Individuum an sich verändert, sondern die Umwelt, in der sich das Individuum befindet. Es ist vergleichbar mit dem Trigger-Faktor im Verhaltensmodell von B. J. Fogg. Die Prozessbeteiligten sollen durch kleine Beigaben den informationssicheren Weg geebnet bekommen. Wird an der gleichen Stelle noch Gamification eingesetzt, macht das Verhalten zusätzlich noch Spaß.[72] Ein Beispiel für Nudging wäre ein voreingestellter abgesicherter Standardinternet-Browser wie Firefox mit einer voreingestellten sicheren Suchmaschine wie Startpage.com. Es handelt sich bei diesem Nudge um die Kategorie der manipulierten Auswahl, bei der das Verhalten einer Person gesteuert, von dieser aber nicht wahrgenommen wird. Das Bild 20 zeigt weitere Kategorien von Nugdes. Verfügt der eingestellte Browser noch über eingebaute Spielelemente z. B. zur Individualisierung des Erscheinungsbildes (dark mode) erzeugt seine Verwendung zusätzlich noch ein gewisses Wohlgefühl.

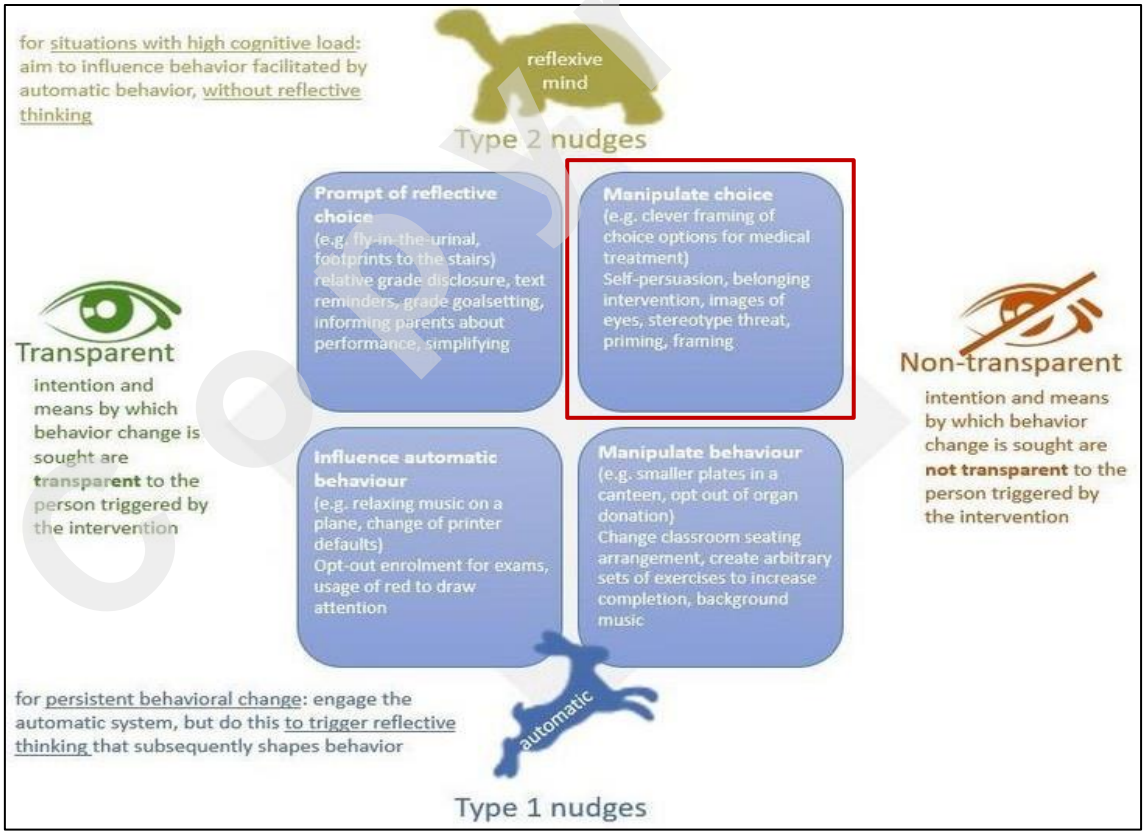


Bild 20: Kategorien von Nudges; Quelle: [73]

Copyright

Für die Formulierung von Zielen ist es aus Wirkungssicht wichtig, einen positiven Zustand in der Zukunft zu beschreiben und einen Zeitpunkt, an dem dieser Zustand erreicht ist. Der Transfer vom erlernten Wissen aus dem Training heraus in den Alltag ist dabei die besondere Herausforderung. Dort herrschen andere Umgebungsbedingungen und Aufgaben und die Laborbedingungen, unter denen gelernt wurde, sind nicht mehr vorhanden. Es ist zu klären, wie die unterschiedlichen und real existierenden Bedrohungen zielgruppenspezifisch dargestellt werden können, so dass sie auch von der Zielgruppe als für ihren Bereich risikobehaftet und somit verbesserungswürdig wahrgenommen werden. Außerdem muss die Realisierbarkeit von geforderten Verhaltensweisen im Arbeitsalltag geprüft werden. Die Bezeichnung ganz konkreter Instrumente zum informationssicheren Umgang helfen der Zielgruppe, das gesteckte Ziel zu erreichen.[72]

Mit der Hilfe eines Gamification-Frameworks kann man überprüfen, wie Beteiligte durch Spielelemente motiviert werden. Ein starker Motivationsfaktor ist beispielsweise das Feedback. Es wird vermutet, dass die Art des Feedbacks das Motivationspotenzial des Spielelements bestimmt. Auch eine individuelle Bezugsnorm, welche die persönliche Leistungssteigerung zeigt, ist für manche motivierender als ein Vergleich zu einer Gruppe.[23] Nähere Ausführungen zu Frameworks und Spielelementen erfolgen in Kapitel 7.

Copyright

6. Kommunikation und Marketing

Wenn Feedback ein starker Motivationsfaktor ist, dann hat auch die Kommunikation einen starken Einfluss auf die Motivation. Denn Feedback ist die Rückübermittlung von Informationen durch die empfangende Person.[74] Es kommt sehr genau darauf an, wie die sendende Person ihre Nachricht gestaltet, wenn sie möchte, dass sie wie gewollt verstanden wird. Ob die Übermittlung ohne Fehler funktioniert hat, erfährt sie erst durch ein Feedback der empfangenen Person.

6.1 Sensibilisierung

AIDA-Modell

Möchte man Personen für ein Thema sensibilisieren, muss man zunächst ihre Aufmerksamkeit und ihr Interesse gewinnen. Über auf die Zielgruppe abgestimmte Kommunikationsmethoden, -werkzeuge und -wege erreicht man das gewünschte Publikum.

Eine in der Werbung erfolgreich eingesetzte und bewährte Methode ist die sogenannte AIDA-Formel. Zunächst wird die Aufmerksamkeit erregt (A = Attention / Aufmerksamkeit). Danach folgen Maßnahmen, die ein echtes Interesse bei der angesprochenen Zielgruppe erzeugen (I = Interest / Interesse). Der nächste Schritt ist die Darstellung des Produkts, welches einen Bedarf zur Erlangung des Produkts erzeugen soll (D = Desire / Verlangen). In der letzten Phase des Modells führt die Zielgruppe die gewünschte Handlung (A = Action / Aktion) aus.[75]

Auch zur Sensibilisierung für Informationssicherheit ist das AIDA-Modell anwendbar. Durch ein Ereignis auf emotionaler Ebene bspw. mit einem auffälligen Plakat und einer emotionalen Nachricht (Bild 21) wird Aufmerksamkeit erzeugt und bleibt aufgrund der Emotionalität länger im Gedächtnis verankert.[76] Das Interesse erweckt man dann z. B. mit der Darstellung von realen E-Mail-Phishing-Angriffen, die im Arbeitsbereich der Zielgruppe immer passieren können (Bild 22). Zur Erzeugung eines Bedarfs für den Aufbau von Wissen und Fähigkeiten können Schulungen in Form von online-Kursen mit Themen (Bild 23) angeboten werden, welche die Zielgruppen betreffen und deshalb

Copyright

relevant für diese sind. Damit wird der Übergang von einer extrinsischen in eine intrinsische Motivation unterstützt. Zur Vorbereitung auf die reale Situation und zur Entwicklung einer Problemlösungskompetenz erfolgt in der letzten Phase die aktive Testung des erlernten Wissens in bspw. Phishing-Simulationen (Bild 24).

Bild 21: emotionales Plakat; Quelle: https://security.to.com/themen/mitarbeiter-sensibilisieren/

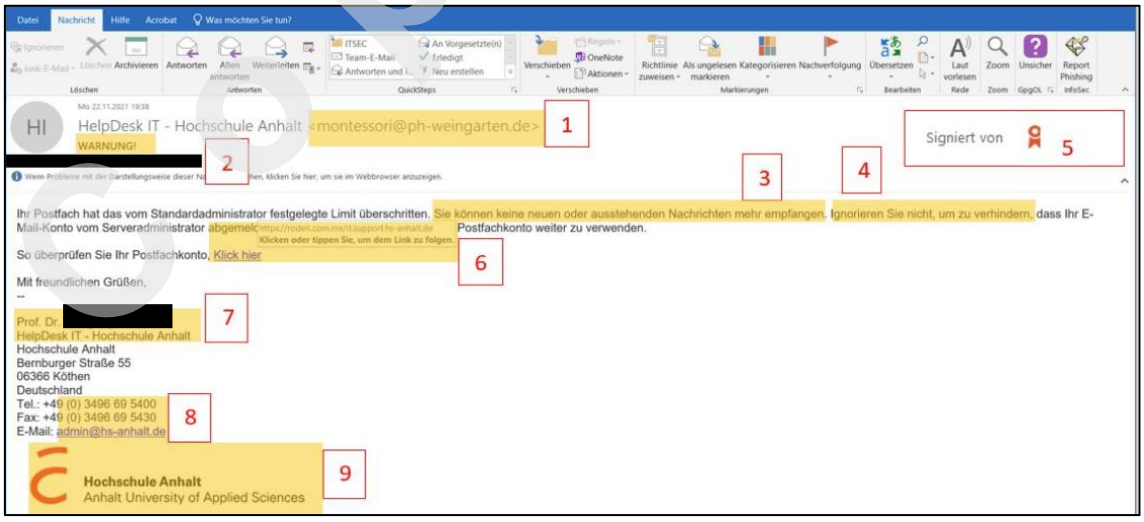


Bild 22: Phishing-Mail an der HSA mit Erläuterungen zu Identifikationsmerkmalen; Quelle: eigene Darstellung (hochschulintern)

Copyright

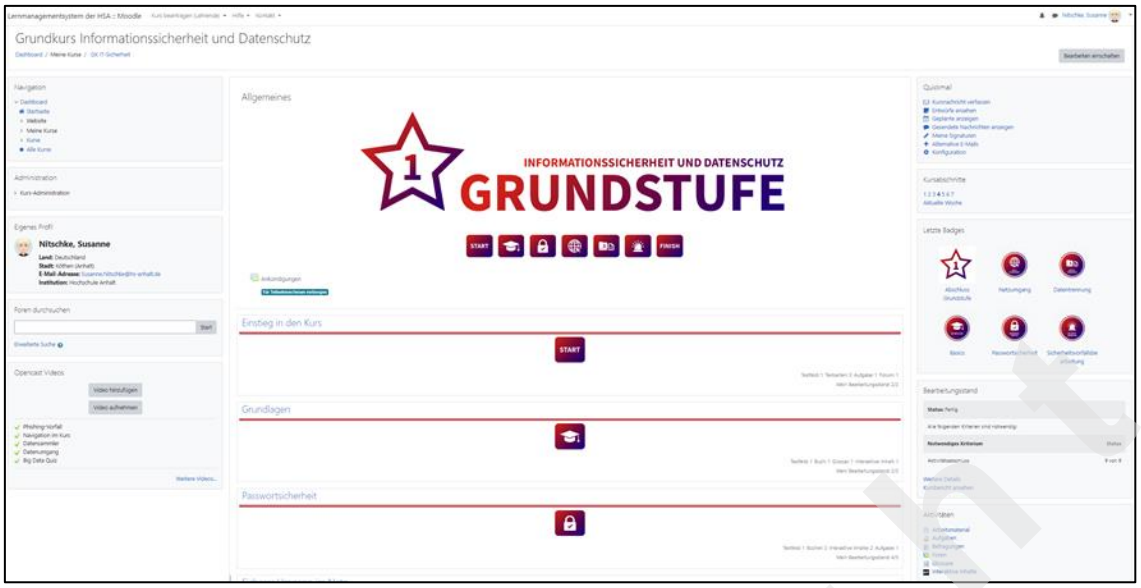


Bild 23: Bereitstellung eines online-Kurses in der moodle-Lernumgebung; Quelle: eigene Darstellung (hochschulintern)

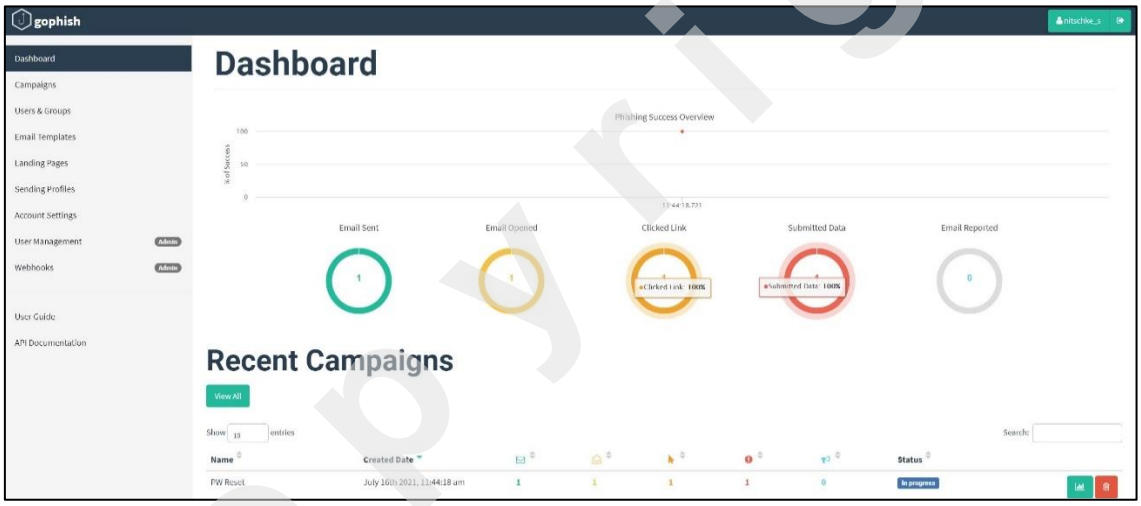


Bild 24: Dashboard-Ansicht der kostenfreien Phishing-Simulation „gophish"; Quelle: eigene Darstellung (hochschulintern)

Nimmt die Zielgruppe an den angebotenen Schulungen teil und damit aktiv Wissen auf, muss die vorhandene Motivation immer wieder durch ein interessantes Lern- und Trainingsangebot auf hohem Niveau gehalten werden. Dieses Vorgehen verspricht eine ebenfalls hohe Aufmerksamkeit im Tagesgeschäft. Zur Aufrechterhaltung der Security Awareness, auch Persistenz genannt, wird eine gut gestaltete Marketingkampagne mit verschiedenen Werbemitteln als Botschafts- und Informationsträgern empfohlen und der Einsatz von Gamification.

Copyright

Die Kampagne muss zur Unternehmenskultur passen, informationssichere Verhaltensweisen vermitteln und überprüfen sowie über verschiedene Kanäle und Medien gestreut werden, um alle Lerntypen zu erreichen.[77]

6.2 Marketingmix

Betrachtet man den klassischen Marketing-Mix[78], wie im Bild 25 dargestellt, ist besonders der Bereich der Kommunikationspolitik interessant. Hier sind Werbung und verkaufsfördernde Maßnahmen verankert.[79]

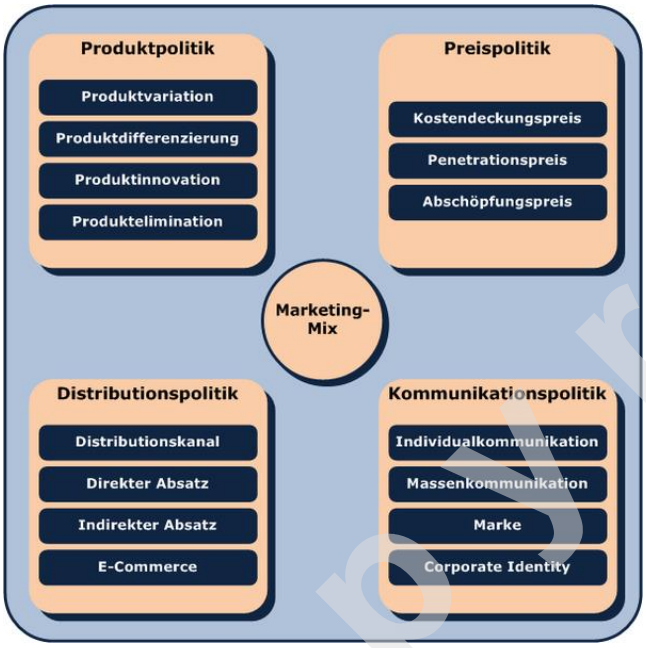


Bild 25: Marketing-Mix; Quelle: https://de.wikipedia.org/wiki/Marketing-Mix

Beispiele für verkaufsfördernde Maßnahmen sind Gewinnspiele, Verlosungen, Rabatte, Preisdifferenzierungen für ausgesuchte Gruppen, Gutscheine, Promotion-Codes, und Aufsteller.[80] Wenn die verkaufsfördernden Maßnahmen nicht selbst schon eine Art Spiel in Form digitaler Quizze und Rätsel mit Gewinnoptionen und Verlosungen sind, dann können diese gamifiziert werden, um auf noch einfachere Weise eine Erhöhung der Sensibilität der Mitarbeitenden für das Thema Informationssicherheit zu erreichen. Es können Gutscheine für besonders hochwertige oder interessante Schulungen (z. B. Hacking-Labor), Promotion-Codes für den Zugang zu online-Spielen der Informationssicherheit (z. B. Escape-Game) eingesetzt oder Eintrittskarten für ein besonderes Event (z. B. Live-Hacking) verlost werden. Aufsteller mit QR-Codes können

Copyright

auf einen Security-Awareness-Tag hinweisen. Von Teilnehmenden gewonnene Promotion-Codes gelangen automatisch in einen Lostopf für nächste Veranstaltungen. Mit diesen verschiedenen Medien werden gleichzeitig auch verschiedene Persönlichkeits- und Lerntypen in den Zielgruppen angesprochen.

Die Vorteile der Verwendung mehrerer Kommunikationskanäle für die gleiche Botschaft liegen in der besseren Verankerung im Gedächtnis und in der passenden Ansprache des jeweiligen Lerntyps (siehe auch 7.1 Lerntypen).[77]

Jedoch gibt es ein Problem, das auch die Werbebranche betrifft. Die wachsende Reizüberflutung mit Informationen durch Massenmedien macht es Menschen zunehmend schwerer, Reize aus ihrer Umwelt wahrzunehmen. Das Gehirn kann diese nicht mehr aufnehmen und verarbeiten und schottet sich deshalb gegen diese ab. Die Menschen sind nicht mehr fähig, die für sie relevanten und wichtigen Informationen zu erkennen. Wie aus dem Bild 26 ersichtlich, fühlen sich von 1.000 deutschen Befragten besonders Personen ab einem Alter über 50 Jahren von der heutigen Informationsmenge überfordert.[81]

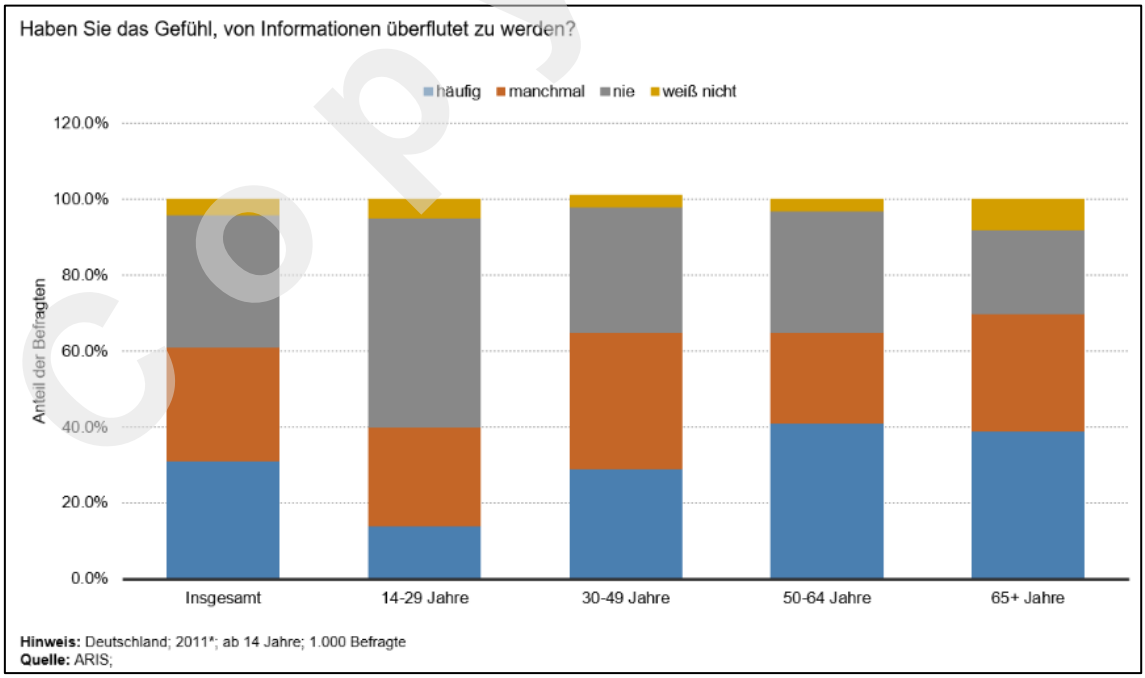


Bild 26: Informationsreizüberflutung in den verschiedenen Altersklassen; Quelle: [81]

Copyright

Um den Untergang des Themas Informationssicherheit in den Massenmedien zu vermeiden, ist eine Überschreitung der Wahrnehmungsschwelle wichtig. Dazu müssen entsprechend intensive Reize gesetzt werden, die bestenfalls eine Empfindung auslösen. Vor allem emotional behaftete Reize werden vom menschlichen Gehirn als relevant registriert, verarbeitet und länger gespeichert.[81]

6.3 Storytelling

Eine Möglichkeit, einen intensiven emotionalen Reiz auszulösen, ist der Einsatz von Storytelling – einem dynamischen Spielelement im Bereich von Gamification. Dort werden Begebenheiten von Figuren erzählt, die etwas Spannendes, Dramatisches oder Emotionales erlebt haben und dadurch die Zuhörer an ihre Story binden.

In Erzählungen wird das ausgedrückt, was Menschen gegenüber bestimmten Dingen empfinden und wie sie diese interpretieren. Mit ihnen ist es möglich, Werte in eine Motivation zum Handeln zu übertragen. Welche Wirkung die Geschichte erzielt, hängt davon ab, von wem sie erzählt wird, an welchem Ort dies stattfindet, wer ihr zuhört und warum. Handelt es sich um eine sehr persönliche Erzählung, können sich die Zuhörenden besser damit identifizieren und in die Geschichte hineinversetzen. Sie werden eher emotional bewegt.[82]

Gute Geschichten haben die Kraft, komplexe oder unbequeme Botschaften spannend zu vermitteln. Innerhalb einer Security Awareness-Kampagne kann Storytelling langfristig die Aufmerksamkeit der Zielgruppe gewinnen und maximieren. Die emotionale Kommunikation über eine persönliche Erzählung kann als „Türöffner“ für die rationale Kommunikation dienen, in der nachgelagert das Wissen vermittelt werden muss. Man baut mit der Story eine emotionale Basis zur Zielgruppe auf und gewinnt so deren Aufmerksamkeit. Damit den Zuhörenden der Einstieg in die Geschichte leichtfällt, bedient man sich der Erzeugung eines Spannungsbogens über Anfang, Höhepunkt und Ende der Erzählung mit verschiedenen Beteiligten und einem interessanten Konflikt. Im Mittelpunkt steht eine Hauptfigur, mit der sich die Zuhörenden identifizieren können. Die Hauptdarsteller müssen keine Heldenfiguren sein, sondern eher Sympathieträger. Die Gegenfigur verursacht den Konflikt, den es allein oder zusammen mit einem Team zu

Copyright

bewältigen gilt. Dabei benötigt die Hauptfigur immer die Hilfe anderer Personen. Am Ende der Geschichte gibt es immer eine Moral, die dann für alle Beteiligten nachvollziehbar ist.[83]

Mit Bezug auf das Thema Informationssicherheit lassen sich auch in Unternehmen Stories entwickeln und an die Zielgruppe herantragen. Wenn man diverse Sicherheitsvorfälle im Unternehmen sammelt, die bereits aufgetreten sind und daraus interessante Geschichten mit einer sympathischen Hauptfigur und einem zentralen Konflikt konstruiert, welcher dann in der Zusammenarbeit mit anderen Mitarbeitenden gelöst werden muss, dann erregt das Aufmerksamkeit und überzeugt die Zuhörenden, welche die Geschichte dann auch weitererzählen.

Dem Trend des partizipatorischen Storytellings sollte man auch in der Informationssicherheit folgen, indem die Personen, die früher nur die Zuhörenden waren, heute selbst mit in die Geschichte eintauchen und miterzählen. Eine Möglichkeit ist die Erstellung und Durchführung von Security Escape Rooms oder die Verwendung der Möglichkeiten im Bereich der gemischten und erweiterten Realität.[83]

6.4 Verfassungsmarketing

Eine Sensibilisierung, die auf alten Methoden aufsetzt, aber die neuen Trends gleichermaßen beachtet und dabei den Menschen und seine Verhaltensweisen auf individueller und gesamtsystemischer Ebene in den Mittelpunkt stellt, gilt als Schlüssel für die Sensibilisierung zur Informationssicherheit. Dieses angepasste Verständnis von Awareness definiert auch die Zielgruppen neu, indem es neben den traditionellen Modellen auf das Marketing der Verfassungen von Menschen setzt, die je nach Stimmungslage ihr Verhalten ändern. Die vom Marketing eingesetzten Medien orientieren sich an diesen Verfassungen als psychologische Trigger, die Bezugspunkte im Rahmen von Awareness-Kampagnen darstellen und die eine informationssichere Verhaltensweise in der Arbeitswelt herbeiführen. Die traditionellen Top-Down- und Bottom-Up-Ansätze werden wie im Bild 27 dargestellt durch eine breitere Aufstellung in den relevanten Unternehmensbereichen und eine Beurteilung der

Copyright

Sensibilisierungsmaßnahmen von außen durch Experten verschiedener Fachrichtungen erweitert.[84]

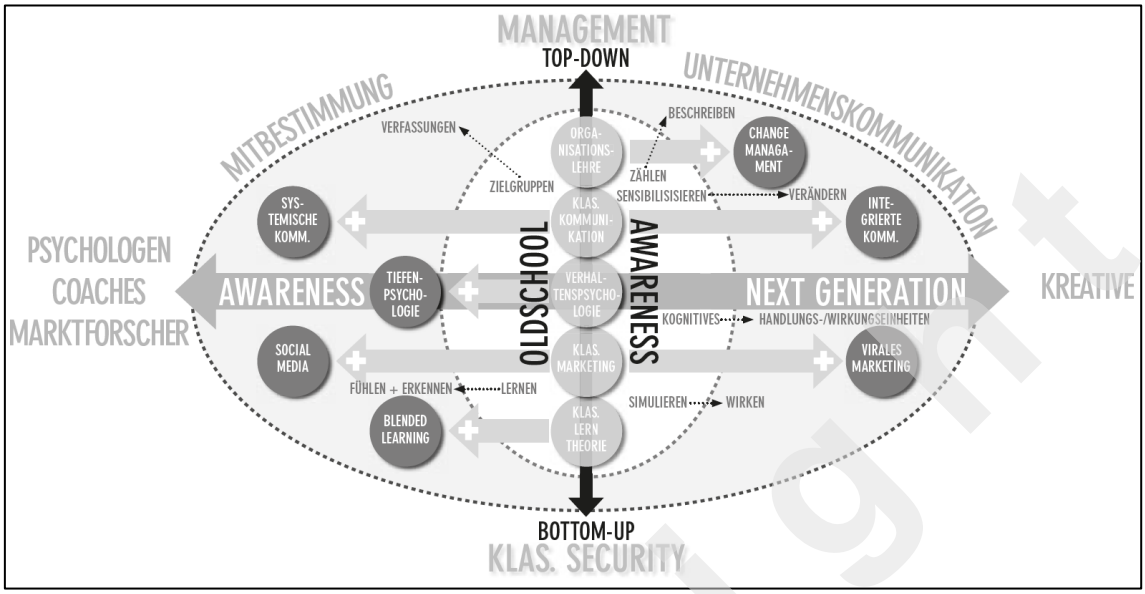


Bild 27: verändertes Awareness-Konzept; Quelle: [84]

Heutige Verhaltensmuster sind weniger gruppenkonform als noch vor einigen Jahren. Wo früher noch Ableitungen des Kauf- und Konsumverhaltens allein aus der Zuordnung anhand eines soziodemografischen Merkmals (z. B. der Zugehörigkeit zu einer bestimmten Berufsgruppe, Alter, Geschlecht, Bildung, Einkommen) möglich waren, entspricht das heute nicht mehr der Realität. Marketingmaßnahmen wirken nicht mehr wie erhofft, da die subjektiv definierten Zielgruppen mit den angenommenen Verhaltensmustern nicht mehr existieren.[85]

Die heutigen Konsumenten wollen vieles zugleich sein und keine Option missen müssen. Sie wollen sich jederzeit verwandeln können. Man spricht auch von multiplen Persönlichkeiten, deren Verhalten weniger einer Gruppe entspricht, sondern eher an bestimmte Kontexte gebunden ist. Traditionelle Zielgruppenmodelle, die überwiegend nach gruppen- und personengebundenen Verhaltensmustern suchen, sind deshalb heutzutage nur noch schwer anwendbar. Sie sind heute maximal als grobe, erste Definitionskriterien noch nützlich. Gleiches gilt für die Einbeziehung psychologischer Merkmale (z. B. anhand der Bedürfnis-Pyramide). Um Märkte generell zu betrachten und

Copyright

eine Ausgangsbasis für Gruppenbildungen zu schaffen, werden diese jedoch noch angewendet.[86]

Das Modell des Verfassungsmarketings betrachtet das Konsumverhalten aus einer neuen, anderen Sicht. Bei der heutigen Gesellschaft existieren unterschiedliche psychologische Verfassungen in verschiedenen Lebenssituationen, verschiedene Lebensgefühle, Bilder und damit verbundene Verwendungsmotive für Produkte. Marketing und Kommunikation sind zielführender, wenn sie sich an diesen Verfassungen und Stimmungen orientieren.[85]

Um das Verfassungsmarketing auch auf den Bereich der Informationssicherheit zu übertragen, muss ermittelt werden, welche Verfassungen das zu erreichende Publikum beim Kontakt mit dem Thema hat. Außerdem sollte man überlegen, wie die Kontaktaufnahme erfolgreich beeinflusst werden kann. Verfassungen verändern sich im Tagesablauf. Abhängig davon, wann am Tag, aus welchem Grund oder zu welchem Anlass man sich an einem bestimmten Ort befindet und mit wem man dort zusammen ist, ist auch die Verfassung und das Verhalten anders. Die Informationssicherheit kann als ein psychisches Kräftefeld beschrieben werden, in dem bestimmte Bedingungen vorherrschen, welchen die Menschen ausgesetzt sind, die dieses Feld betreten. Anhand der Stimmung, dem Zustand oder den Bedingungen lassen sich innerhalb des Spannungs- bzw. Kräftefeldes verschiedene Verfassungen hervorheben.

6.5 Verfassungsmarketing in der Informationssicherheit für deutsche Hochschulen

Das Bild 28 zeigt das Spannungsfeld der Informationssicherheit für deutsche Hochschulen mit folgenden Dimensionen:

- Awareness vs. Offenheit von Kultur und Lehre
- Sicherheitsmaßnahmen vs. Freiheit und Autonomie[87] bzw. Bürokratie durch Autonomie[88]

Die Awareness könnte man auch mit Vorbereitung und Training beschreiben. Offenheit hängt eng mit Sorglosigkeit zusammen. Zur Sicherheit zählt auch die Standardisierung von Prozessen und zur Freiheit und Autonomie von Forschung Lehre der Komfort. Der

Copyright

Preis für die Sicherheit des zu schützenden Gutes beeinflusst die Ausgaben, die z. B. für die Forschung Lehre zur Verfügung stehen und damit deren Autonomie. Eine entscheidungsfähige Organisation ist für die Durchsetzung der Sicherheitsmaßnahmen notwendig, steht aber einer starken Bürokratie und Abstimmungsstruktur aufgrund einer traditionellen Autonomie in vielen Hochschulbereichen gegenüber.

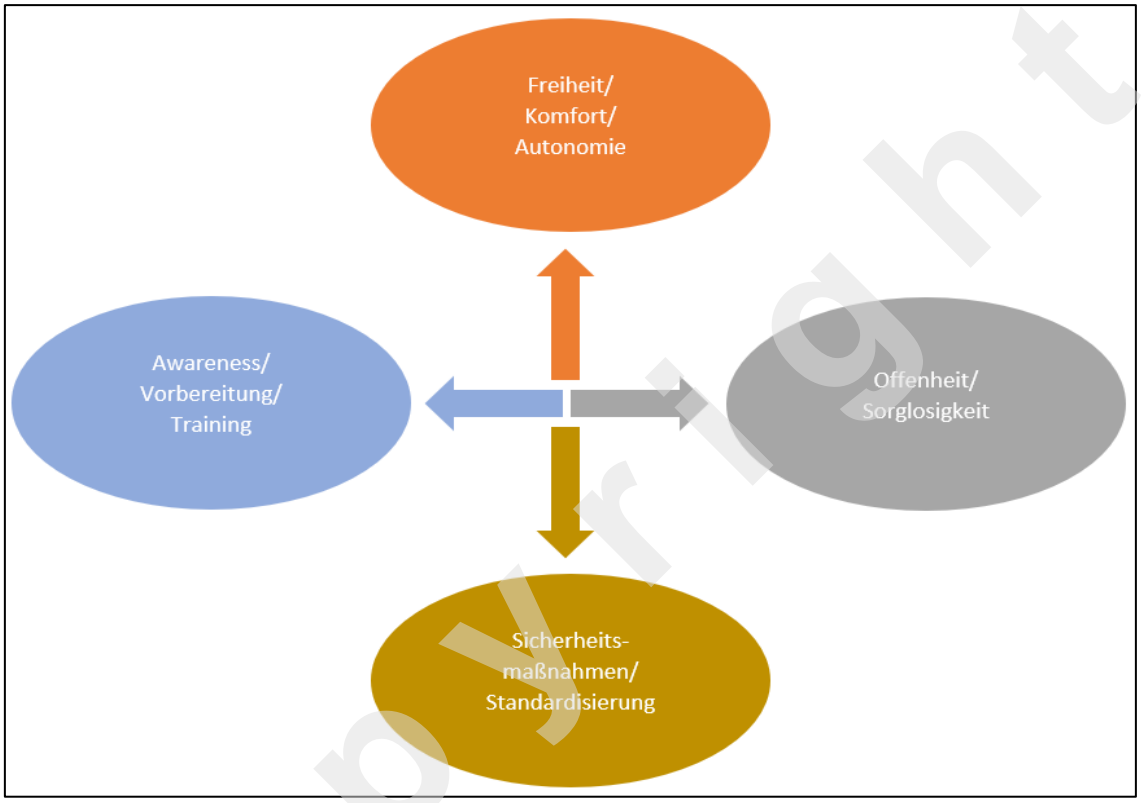


Bild 28: Spannungsfeld der Informationssicherheit; Quelle: eigene Darstellung

Für die Erarbeitung der unterschiedlichen Verfassungen erfolgt eine erste grobe Untergliederung anhand der bereits erwähnten Zielgruppen an deutschen Hochschulen, wobei die Studierenden von der Betrachtung ausgeschlossen werden, weil sich das zu entwickelnde Konzept ausschließlich auf die Mitarbeitenden beziehen soll. Für die weitere Unterscheidung bietet es sich an, die möglichen Verfassungen und relevanten Themen anhand des jeweiligen Einsatzortes und Arbeitsumfeldes abzuleiten. So gibt es bspw. Mitarbeitende, die überwiegend handwerkend, sachbearbeitend, fachpraktisch, prozessübergreifend, forschend, leitend und/oder lehrend und IT-systemverändernd tätig sind. In der Anlage 4 dieser Master-Thesis wurde solch eine Einteilung beispielhaft für die Mitarbeitenden der Hochschule Anhalt vorgenommen. Bei der Durchführung der

Copyright

Arbeiten treten bestimmte Verfassungen auf, die mit einem bestimmten Motiv, Bedürfnis oder Zweck verbunden sind. Die individuellen Bedürfnisse, die beispielhaft im Bild 29 dargestellt sind, variieren je nach aktuellem Umfeld (öffentlich/privat) und Perspektive (ich/wir) und führen zu einer unterschiedlichen Bewertung der Relevanz des Themas. Eine zielgruppengerechte Sensibilisierung ist dann möglich, wenn diese Bedürfnisse und deren Bedeutungen für die jeweilige Zielgruppe erkannt und anlassbezogen befriedigt werden können.

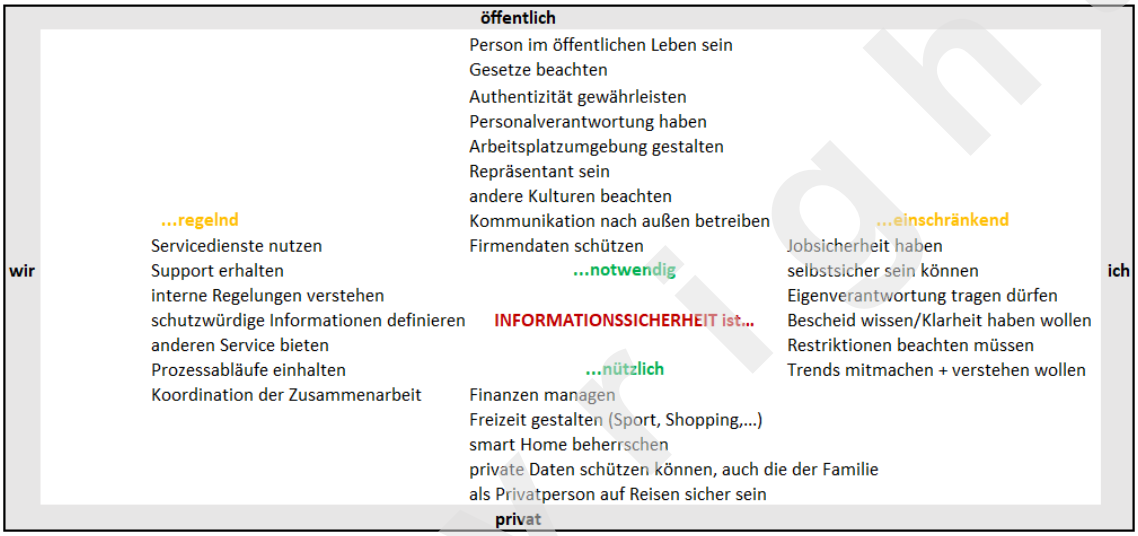


Bild 29: Facetten der Informationssicherheit; Quelle: eigene Darstellung

Folgende Bedürfnisse können in der Hochschullandschaft, aber auch in anderen Unternehmen so auftreten:

- private Daten und wichtige Firmendaten schützen
- Informationssicherheitsrisiken kennen und vermeiden
- Support in Bezug auf sichere Verhaltensweisen erhalten
- bereitgestellte Sicherheitswerkzeuge und Servicedienste bedienen
- Kompetenz und Verantwortung trotz neuer Restriktionen behalten
- wichtiger Teil einer Gemeinschaft sein
- möglichst uneingeschränkt, aber auch verantwortungsbewusst arbeiten, forschen
- zu sicheren Verwaltungsprozessen zur Sicherstellung der Beschäftigung beitragen
- auf dem neuesten technischen Stand und Wissensstand sein
- Unkenntnisse abbauen, Kenntnisse aufbauen
- sein Gesicht, seinen guten Ruf wahren

Copyright

- bei der Veränderung mitreden, mitgestalten

Durch die Einbindung in konkrete Anlässe erfolgt oftmals eine emotionale Aufladung und der Begriff wird Teil einer größeren Story.[89] Hier kommt jetzt das Arbeitsumfeld Hochschule ins Spiel. Dieses unterscheidet sich durch seine nicht gewinnorientierte Organisation von anderen produzierenden Unternehmen. Das Bild 30 zeigt beispielhaft einige dienstliche Anlässe bzw. Situationen an Hochschulen, in denen Informationssicherheit eine Rolle spielt. Viele dieser Anlässe gibt es auch in gewinnorientierten Unternehmen, so dass es dort Parallelen gibt.

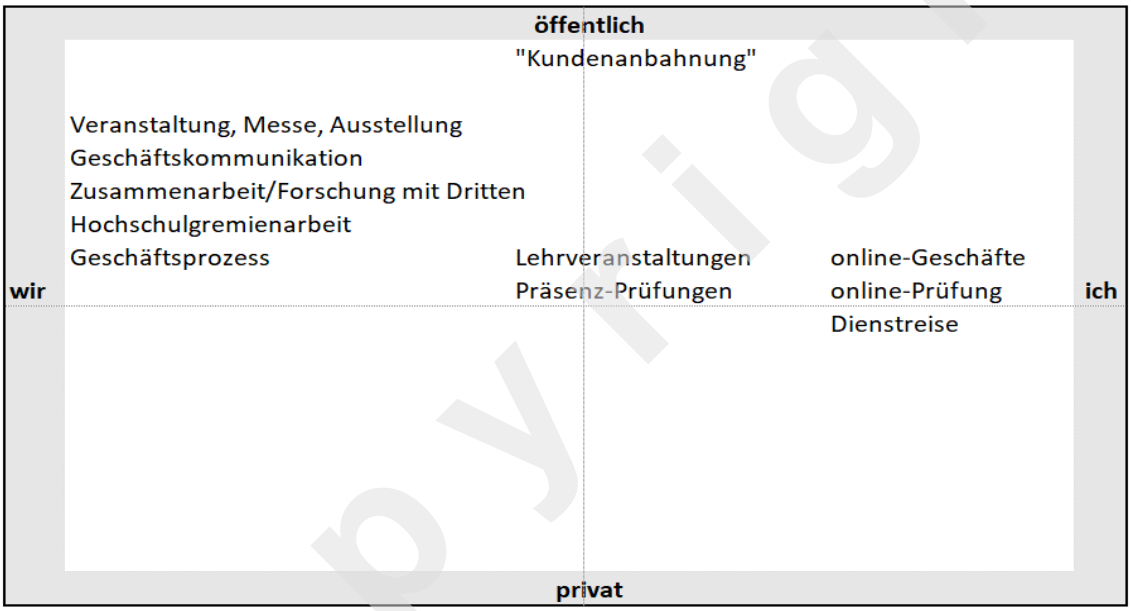


Bild 30: mögliche Anlässe für Informationssicherheit; Quelle: eigene Darstellung

Unter Kundenanbahnung ist die Anwerbung von Studierenden, Personal und Drittmittelgebern gemeint. Im Bereich der online-Geschäfte geht es z. B. um Transaktionen und mögliche Gefahren bei Einkaufsprozessen, die im öffentlichen Sektor durch die Verpflichtungen zur Ausschreibung von Aufträgen und zur Einhaltung der Wirtschaftlichkeit gekennzeichnet sind. Der Einkauf bei online-Shops ist bei zumeist ausschreibungspflichtigen Beträgen nicht die Regel, aber auch viele Kleinbestellungen unter 500 € netto können in Summe zu einem größeren Schaden führen, wenn man nicht ausreichend z. B. in der Erkennung von betrügerischen online-Shops geschult ist. Unter Geschäftskommunikation ist der sichere Einsatz von verschiedenen Kommunikationsmedien wie Telefon und E-Mail gemeint sowie die Inhalte, die darüber

kommuniziert werden dürfen. Diese Problematik betrifft jedoch nicht nur explizit Hochschulen, sondern auch andere Unternehmen. Bei der Organisation von Veranstaltungen, Messen und Ausstellungen mit vielen Beteiligten ist auch immer die Sicherheit der Informationen zu beachten. Nicht jeder Besucher muss jede Information zur Verfügung haben. Eine Hochschule ist jedoch durch einen offenen Charakter gekennzeichnet, weshalb die Einhaltung dieser Regel in der Praxis schwerfallen könnte. In der Situation der Hochschulgremienarbeit vertreten Beteiligte möglicherweise andere Sichtweisen in Bezug auf die Informationssicherheit als in einer privaten Umgebung, wo der Fokus noch mehr auf dem Schutz der Privatsphäre liegt. Als Beteiligte an einem Geschäftsprozess wie beispielsweise in der Personal- oder Finanzabteilung, in der Gebäudeverwaltung und -pflege oder auch beim Qualitätsmanagement gerät man durch die Anpassung von Arbeitsabläufen und Verantwortlichkeiten aufgrund einer Neuausrichtung und Fokussierung auf das Thema Informationssicherheit in eine Situation, diese Änderungen nicht immer sofort nachvollziehen und verstehen zu können. Änderungsprozesse an Hochschulen sind aufgrund der starken Bürokratie und Abstimmungsstruktur besonders schwer umsetzbar. Beim Anlass Lehrveranstaltungen füllen die Lehrbeauftragten eine bestimmte Rolle aus, die auch an die Rahmenbedingungen der Informationssicherheit gebunden ist. Man muss wissen, welche Möglichkeiten zur Lehre den Studierenden zur Verfügung gestellt werden dürfen. Nicht jede Software, die kostenlos und frei verfügbar im Internet zur Verfügung steht, ist auch sicher in der Anwendung. Bestimmte Situationen sind auch immer Präsenz- und online-Prüfungen, in denen viele Prüflinge zusammen sind und jeder einzelne Prüfling für sich eine bestimmte Verfassung hat. Die Prüflinge erwarten einen reibungslosen Prüfungsablauf und die gerechte sowie sichere Verwahrung der Prüfungsergebnisse. Auch auf Dienstreisen begibt man sich in eine Situation, welche die Sicherheit von Informationen gefährden kann. Werden dienstliche Geräte z. B. auf einer Auslandsreise mitgenommen, die von den dortigen Behörden technisch untersucht werden, kann es zur Offenlegung von Geschäftsgeheimnissen kommen, die nicht gewollt ist. Dieser Punkt ist gerade auch für die Zusammenarbeit von Hochschulen mit der Wirtschaft und deren große Abhängigkeit von den Finanzmitteln dieser externen Unternehmen zur Absicherung ihrer Existenz extrem wichtig.

Copyright

Diese Anlässe können nun für die Einschätzung der verschiedenen Verfassungen der genannten Zielgruppen an Hochschulen verwendet werden. Aus den Verfassungen lassen sich die Triggerpunkte ableiten, über welche das Thema Informationssicherheit für die Zielgruppe seine Relevanz erhält.

Aus persönlichen Befragungen, Beobachtungen und Literatur-Recherchen ist die Skizzierung nachfolgender Verfassungen der Zielgruppen im Kontext des Arbeitsumfeldes möglich und die Bestimmung der spezifischen Medien zur Awareness-Schaffung:

- Die Zielgruppe der überwiegend handwerkend und vor Ort tätigen Personen benötigt konkrete Leitfäden in einer Art „Do-it-Yourself"-Problemlösung. Die verwendeten Kommunikationsmedien müssen über die Gefahren für die Informationssicherheit im Arbeitsbereich dieser Zielgruppe (wie bspw. Tailgating) aufklären, übersichtlich, einfach, kurz und gut strukturiert sein ohne zu viele Details.

- Die Zielgruppe der überwiegend sachbearbeitend tätigen Personen will über persönliche Konsequenzen bei Fehlverhalten informiert werden, aber auch möglichst keine Fehler machen. Sie suchen nach dem persönlichen Nutzen, welchen die Informationssicherheit sowohl beruflich als auch privat für sie bereithalten kann. Das erlangte Wissen teilen sie privat auch anderen Personen in ihrem Umkreis mit. Sie wollen einen strukturierten, klar definierten und informationssicheren Arbeitsablauf und machen auch gern auf Schwachstellen aufmerksam. Sie müssen die Möglichkeit erhalten, aktiv an der Informationssicherheit mit zu arbeiten z. B. durch die Meldung von Phishing-Mails an eine vom Unternehmen bereitgestellte Service-Mail-Adresse.

- Die Zielgruppe der fachpraktisch tätigen Personen befindet sich in einer Phase der Vorbereitung auf ihren späteren Beruf. In der Betreuung von Studierenden in z. B. Übungen, Projekt- und Bachelorarbeiten lernen sie in der jeweiligen Lehreinrichtung die zukünftigen Gegebenheiten in der Lern- und Arbeitswelt

Copyright

kennen sowie den Umgang mit unterschiedlichen Persönlichkeits- und Lerntypen. Sie unterstützen die Organisation in Instituts- und Studienangelegenheiten. Es ist davon auszugehen, dass diese Personen offen für Neues, engagiert in der Arbeit und interessiert an Informationen zu existierenden Arbeitsabläufen sind. Aufgrund ihrer Kontakte zur Professorenschaft und zu den Studierenden sollten sie mit ausreichend Informationen und Handreichungen zum Thema ausgestattet werden. Sie können ihren persönlichen Beziehungen nutzen, um für die Informationssicherheit in der Einrichtung zu werben und Überzeugungsarbeit zu leisten.

- Die Projektmitarbeitenden an einer Hochschule müssen prozessübergreifend denken und in Teams die optimale Lösung für die Problemstellungen innerhalb ihres Projekts finden. Sie kommunizieren, diskutieren, organisieren, bearbeiten spezifische Themen, hinterfragen bestehende Lösungen und kontrollieren ihren Projektfortschritt. Sie wissen, dass es bei der Abarbeitung ihrer Projekte auch Risiken gibt, die sie behandeln müssen. Sie wissen, dass es wichtig ist, alle Stakeholder mit einzubeziehen. Als Teamplayer sind Team-Events die richtige Form, um die Projektmitarbeitenden mit dem Thema Informationssicherheit zu konfrontieren. Besonders auch der Fokus der Risikovermeidung dürfte für diese Zielgruppe interessant sein.

- Die Zielgruppe der überwiegend forschend tätigen Personen ist an neuesten Technologien und Trends interessiert und möchte sich beständig fortbilden. Da die Forschung stark abhängig von den knappen Gütern Personal und Finanzen ist, fühlen sie sich oft in ihrer Forschungsfreiheit eingeschränkt. Für diese Zielgruppe ist im Rahmen der Informationssicherheit wichtig, dass ihre Forschung weiterhin möglich ist. Ein offener Austausch zu den Gefahren und Maßnahmen zur Abwehr und Sicherstellung der Informationssicherheit z. B. in Form von unabhängigen Forschungsinseln im Netzwerk der Hochschule dürfte für diese Zielgruppe die Lösung darstellen.

Copyright

- Lehrend tätige Personen beschäftigen sich mit unterschiedlichsten Themen, die sie für ihre Lehre didaktisch aufbereiten. Sie sind vielseitig interessiert, aber auch frustriert, wenn die Freiheit von Forschung und Lehre beschnitten wird. Jegliche weitere Einschränkung z. B. durch Maßnahmen der Informationssicherheit bringt weiteren Frust, der sich im Engagement für die Lehre auswirken kann.[98] Transparenz, Kommunikation und die aktive Einbeziehung in die kommenden Veränderungen sowie die Darstellung von Fakten zum Thema Cybercrime tragen zur Überzeugung der Notwendigkeit der Sicherheitsmaßnahmen bei. Eine mediale Form, die sich hierfür anbietet, ist die Durchführung von kleineren Workshops mit dieser Zielgruppe. Oft nimmt die Professorenschaft auch leitende Funktionen wahr, so dass sie zusammen mit den wenigen leitenden Personen der Hochschuleinrichtung eine Zielgruppe bilden. Die überwiegend leitend tätigen Personen interessieren sich insbesondere für die Darstellung der möglichen Risiken und Konsequenzen aus z. B. Gesetzesverstößen für die Organisation. Sie benötigen konkrete Lösungsmöglichkeiten und Präventionsmaßnahmen, um das Risiko zu minimieren, um damit auch die Last der Verantwortung, die sie tragen zu vermindern. Die Verankerung der Informationssicherheit im Risikomanagement sowie die Bildung von objektiven Kennzahlen zur Informationssicherheit im Controlling können hier die notwendige Klarheit schaffen.

- Die Zielgruppe der Personen, die überwiegend systemverändernd tätig sind, arbeiten oft als IT-Administratoren in verschiedenen Themengebieten. Zur Abarbeitung ihrer Aufgaben benötigen sie stets genaue Angaben. Sie sind es gewöhnt, einerseits sehr detaillierte Beschreibungen von komplexen Vorgängen in Handbüchern zu lesen und andererseits sehr lückenhafte Schilderungen von IT-Benutzenden zu erhalten. Die zentrale und sichere Bedienung und Überwachung mehrerer IT-Systeme sowie ein organisierter Troubleshooting- und Benutzenden-Support-Prozess unterstützen diese Zielgruppe bei der Gewährleistung der Informationssicherheit durch die bessere Einordnung von auftretenden Störungen und System-Sicherheitshinweisen. Informationssicherheit ist für diese Zielgruppe selbstverständlich und auch gewünscht, nur steckt die Umsetzung von

Copyright

Sicherheitsmaßnahmen oft in organisatorischen Sackgassen fest, die sie nicht beeinflussen können. Sie benötigen vor allem die Unterstützung aus der Leitungsebene, um die Maßnahmen zur Sicherstellung der Informationssicherheit nicht jedes Mal begründen zu müssen. Klare organisatorische Regelungen und die Festlegung von Verantwortlichkeiten im Rahmen eines Informationssicherheitsmanagementsystems helfen dieser Personengruppe bei der Wahrnehmung ihrer Aufgaben.

Copyright

7. Didaktik

Die Aufnahme und Verarbeitung von Informationen wie es auch beim Lernprozess der Fall ist, hängt ebenfalls von der jeweiligen psychischen Verfassung ab. Es ist davon auszugehen, dass eine gute psychische Verfassung auch zu guten Ergebnissen führt.

7.1 Lerntypen

Will man Gamification einsetzen, muss man es auf Typisierungen beziehen, deren Wirksamkeit im universitären Lernalltag empirisch gesichert ist. Hier gibt es die sogenannte 5-Klassen-Lösung.[23]

Nach der 5-Klassen-Lösung werden fünf verschiedene Lernmotivationen von Lerntypen unterschieden, die im Bild 31 dargestellt sind:

- pragmatische Lernmotivation
- angstbestimmte Lernmotivation
- selbstbestimmte Lernmotivation
- strategische Lernmotivation
- rezessive (vermeidende) Lernmotivation[90]

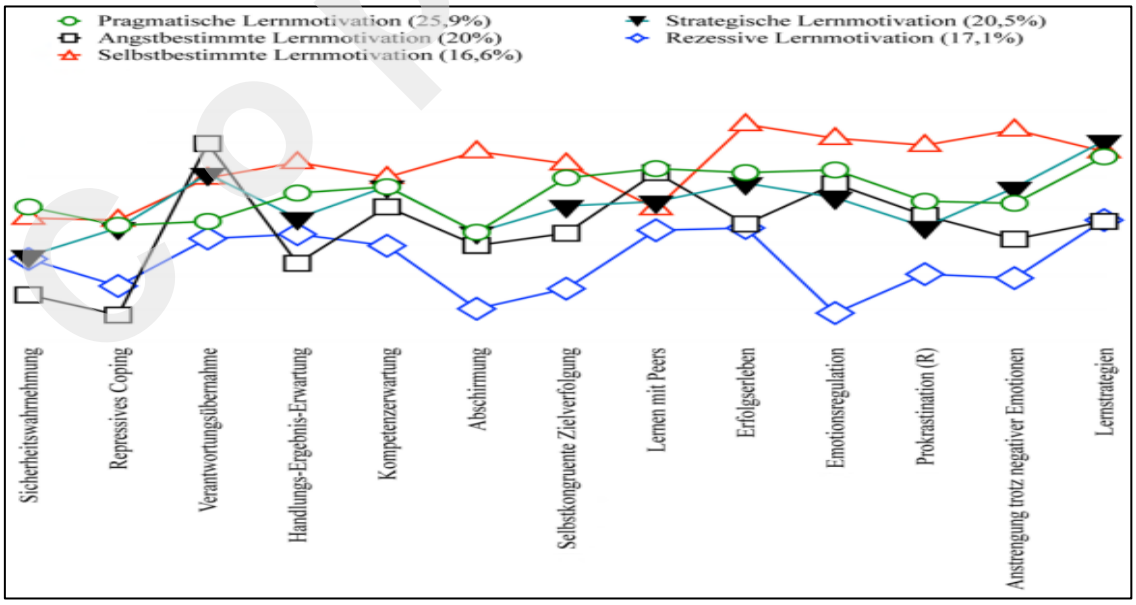


Bild 31: Profile unterschiedlicher Lernmotivation (5-Klassen-Lösung); Quelle: [91]

Copyright

Aus dem Bild 31 wird deutlich, wie verschieden die Lerntypen mit bestimmten Situationen umgehen. Manche lassen sich leicht ablenken und schirmen sich nicht von der Umwelt ab (rezessiv lernmotivierte Personen), andere dagegen verstehen es, sich im Lernprozess voll auf das Thema zu konzentrieren (selbstbestimmt lernmotivierte Personen). Ein ähnlich großer Abstand zeigt sich bei diesen beiden Typen in der Regulation von Emotionen und der Anstrengung trotz negativer Emotionen. Während die überwiegend selbstbestimmt Lernmotivierten relativ gut mit schwierigen Aufgaben und damit einhergehend möglichen negativen Gefühlen umgehen können, lassen sich rezessiv Lernmotivierte schnell ablenken, geben schneller auf und haben nicht die Erwartung an eine eigene hohe Kompetenz bzw. weichen dem Beweis ihrer eigenen Kompetenz gern aus (in den abschließenden Prüfungen). Sie schieben Aufgaben lieber auf. Ihr Durchhaltevermögen ist von allen Lerntypen am niedrigsten. Beim Lernen mit Peers können die rezessiv Lernmotivierten ihre Stärken entwickeln. Für die selbstbestimmt Lernmotivierten ist diese Form des Lernens eher nicht geeignet. Dort fällt die Kurve der Lernmotivation.[90] Sie bestimmen lieber selbst über Erfolg oder Misserfolg und übernehmen dafür allein die Verantwortung. Sie möchten mit ihrer Leistungsfähigkeit nicht abhängig von anderen Lernenden sein.

Bei rezessiv Lernmotivierten wird das Verhalten nicht durch selbstkongruente Ziele gesteuert, sondern muss durch äußeren Druck oder innere Zwänge erfolgen. Sie sind auf diese Art der Handlungserzwingung angewiesen, da sie sich schlecht selbst motivieren können. Im Gegenteil dazu fällt den selbstbestimmt Lernmotivierten die Verfolgung von selbstkongruenten Zielen leicht, da sie sich mit ihnen identifizieren und in ihren Lernvorgang integrieren können sowie ihr Verhalten entsprechend regulieren.[92]

Die schwächeren Lerner müssen frühzeitig gefördert und unterstützt werden, indem die Lernumgebung und die Strukturen angepasst werden und eine Begleitung des Lernprozesses stattfindet. Für sie ist nicht die Benotung am Ende wichtig, sondern der Prozess an sich. Alle Störfaktoren, die den Prozess beeinflussen, müssen beseitigt und die Ziele klar gesteckt und verstanden werden. Es darf weder Angst vor der bevorstehenden Prüfung geschürt werden, noch darf es ablenkende Faktoren und die Duldung von Aufschiebeverhalten geben. Auch dem Aufkommen negativer Gefühle durch Misserfolge

Copyright

muss entgegengewirkt und lange Konzentrationsphasen müssen vermieden werden.[90] Vielmehr muss es mehrere kleine Lernerfolge geben, die ihnen ein Erleben der eigenen Kompetenz ermöglicht und damit die Lernmotivation steigert.[91]

Um allen Lernmotivationstypen erfolgreich Wissen zu vermitteln, wird empfohlen, Lehrveranstaltungen in Blöcken durchzuführen, begleitende Selbstlernphasen anzubieten, schaffbare Aufgaben zu stellen, zeitnahe Rückmeldungen zu geben, selbst erarbeitetes Wissen zu testen, abwechselnde Lern- und Übungsformen zu wählen und eine offene Lernsituation zu schaffen. Die Wissensvermittlung soll in einem didaktischen Zirkel aus Aufgabe, Anwendungsorientierung, Selbststudium und Rückmeldung bestehen[90] und den Lernenden mehr Orientierung und Sicherheit über den eigenen Lernprozess geben.[91]

Die Lehrorganisation hat einen Einfluss darauf, wie intensiv und anhaltend sich mit einem Thema beschäftigt wird. Aber um ein Verhalten zu erlernen, welches ein schnelles Handeln unter Druck in bedrohlichen Situationen ermöglicht, muss über einen langen Zeitraum trainiert werden. Die Durchführung von einfachen praktischen Übungen ist nicht ausreichend, um dieses Verhalten zu erlernen. Es muss in einem mehrstufigen Prozess den Lernenden bewusst gemacht werden. Dieser Prozess wird von einer externen Beurteilung durch Experten und einer möglichen Neuausrichtung zur Wirksamkeitserhöhung begleitet. Die subjektiven Theorien, die das Interaktionshandeln beim Menschen unbewusst steuern, haben sich über die Kindheit, Jugend und das Erwachsenenalter entwickelt und sind deshalb nur schwer veränderbar. Sie sind enger mit der Person verbunden als didaktisch-methodische Theorien. Die Änderung kann nur über einen längeren Zeitraum erfolgen und hat zum Ziel, die abgespeicherten Standardabläufe bewusst und damit bearbeitbar, d. h. veränderbar zu machen.[93]

Die größte aktive Wirkung auf die Lernenden hat aber der Rückmeldeprozess. Dieser wird jedoch vom jeweiligen Lerntyp unterschiedlich wahrgenommen. Bei schwächer Lernenden kann sich dieser auch negativ auswirken, wenn diese dadurch für sie negative „Lernerfolge“ sehen und damit nicht umgehen können.

Copyright

7.2 Lernumgebung

Die Ergebnisse, die die Lernenden erzielen, stehen im unmittelbaren Zusammenhang mit dem Lehrprozess und einer geeigneten Lernumgebung. Das Handeln selbst ist ein Ergebnis aus Emotionen, physiologischen und psychologischen Bedürfnissen. Erkunden, Spielen und andere spontane Aktionen beruhen auf psychologischen Regulierungsprozessen.[24]

Die Selbstbestimmungstheorie nennt die Bedürfnisse Motive. Motive führen zu Handlungen und diese werden lieber durchgeführt, wenn sie zu persönlichem Wohlbefinden beitragen. Wohlbefinden empfindet jemand, wenn er seine eigene Kompetenz erlebt und damit aktiv die gesetzten Ziele erreichen kann. Stehen die Anforderungen der Aktivität im Gleichgewicht mit den Fähigkeiten zur Bewältigung der Aktivität, spricht man auch vom sogenannten Flow.[94] Der Flow bewirkt die vollkommene Konzentration und Begeisterung für die aktuelle Aufgabe, bei der ein bestimmtes Wohlbefinden und eine bestimmte Qualität des Engagements und der Leistung erreicht werden.[25] Die drei psychologischen Grundbedürfnisse Kompetenzerleben, Autonomie und soziale Zugehörigkeit sind von zentraler Bedeutung, wenn es darum geht, ein hochwertiges Lernen in einer Lernumgebung zu ermöglichen, in der diese Bedürfnisse befriedigt werden.[24]

Je nachdem wie stark das Interesse an einem Thema ausgeprägt ist, bedarf es mehr oder weniger Anreize zum Lernen. Bei schwachem Interesse ist die Lernumgebung wichtig für die Steigerung des Interesses. Dort müssen entsprechende Anreize gesetzt werden (siehe extrinsische Motivation in Kapitel 5). Ist das Interesse hoch, sind nur wenige oder sogar gar keine situativen Anreize notwendig. Hochinteressierte Personen wollen zusätzlich noch die Umweltbedingungen verändern. Das Bild 32 zeigt, dass ein nicht vorhandenes oder schwaches Interesse verschiedene Gründe haben kann, die im kognitiven oder im emotionalen Bereich, im Wertebereich, im Verhalten oder in einer erneuten Auseinandersetzung der Person mit dem Gegenstand liegen können.[95]

Copyright

Merkmale	Desinteresse	Abneigung
kognitiver Bereich	punktuelles Wissen und fremdbestimmte Handlungsfähigkeit gegenüber dem von außen vorgebenen Gegenstand	selektiv erworbenes Wissen, weitere Informationsaufnahme wird selektiert oder vermieden
emotionaler Bereich	leicht negative Gefühle gegenüber dem Gegenstand	ausgeprägt negative Gefühle gegenüber dem Gegenstand
Wertebereich	keine besondere Wertschätzung des Gegenstandes	negative Wertschätzung des Gegenstandes
erneute Person-Gegenstands-Auseinandersetzung	keine oder wenn, nur fremdbestimmte Auseinandersetzung mit dem Gegenstand	selbstintentionale, aktive Vermeidung von Auseinandersetzungen mit dem Gegenstand
Verhalten	passive Ablehnung	aktive Ablehnung

Bild 32: Gründe für Nicht-Interesse; Quelle: [95]

Der Gestaltung der Lernumgebung kommt somit eine enorme Bedeutung zu, um die schwach interessierten Personen für die Thematik zu begeistern. Um die verschiedenen Gründe des Desinteresses zu beeinflussen, empfiehlt es sich, den Personen das Thema nicht von außen aufzudrängen, sondern sie in die Verantwortung zu nehmen, die Wichtigkeit des Themas auch für ihren Arbeitsbereich zu verdeutlichen. Mit dem Einsatz moderner Medien ist es zudem möglich, das Thema modern und interessant darzustellen, um sie damit zu einer erneuten Auseinandersetzung mit dem Thema zu bringen.

ARCS-Modell

Die Beschreibungen zur Beschaffenheit von multimedialen Lernumgebungen basieren zum großen Teil auf dem sogenannten ARCS-Modell, wobei „A“ für „Attention/Aufmerksamkeit“, „R“ für „Relevance/Relevanz“, „C“ für „Confidence/Vertrauen/Erfolgszuversicht“ und „S“ für „Satisfaction/Zufriedenheit“ stehen.[96]

Um die nötige Aufmerksamkeit (Attention) zu bekommen oder zu erhalten, muss versucht werden, die Lernenden durch den Einsatz von provokativen und widersprüchlichen Aussagen, besonderen Tönen und animierten Grafiken so zu fesseln, dass sie gezwungen sind, sich mit dem Thema auseinander zu setzen. Mit der Möglichkeit, sich selbst Fragen stellen zu können oder Fragen und Problemlösungen gestellt zu bekommen, kann man die Neugier wecken. Wechseln sich die Elemente dann noch zwischen Darstellung und Interaktion ab, sollte die Aufmerksamkeit der Lernenden vorhanden sein.[96]

Copyright

Um für das Thema eine individuelle Relevanz (Relevance) zu erhalten, müssen Vertrautheit geschaffen sowie vom Wissensstand abhängige individuelle Lernziele angeboten und die Anpassung an unterschiedliche Motivationen ermöglicht werden. Vertrautheit erzielt man beispielsweise durch eine personalisierte Ansprache, durch Beispiele aus der Lebenswelt des Zielpublikums oder durch die Verwendung einer Leitfigur. Individuell auswählbare Lernziele erreicht man durch ein breites Angebotsspektrum in Form verschiedener Spiele oder Simulationen. Für die Befriedigung der im Zielpublikum unterschiedlich vorhandenen Motivationsprofile eignen sich wiederum unterschiedliche Schwierigkeitsgrade und transparente Bewertungssysteme, die etwas über die individuelle Leistung aussagen sowie kooperative Lernformate zur Unterstützung der sozialen Motivbefriedigung und Verantwortungsübertragung durch Leitungsaufgaben für Lernende, die machtmotiviert sind.[96]

Die Stärkung der Zuversicht (Confidence) des Lernenden, das geforderte Lernziel mit eigenen Mitteln zu erreichen, erfordert, dass er über die Lernanforderungen, die Bewertungen, die Voraussetzungen und den Umfang in der Gesamtübersicht informiert ist. Sie sollten genügend Möglichkeiten haben, Erfolge im Lernen durch das Angebot von Herausforderungen, die je nach Wissensstand variieren zu generieren. Um zu erzielen, dass sich die Lernenden den Erfolg selbst zuschreiben können, ist es wichtig, dass sie eine gewisse Selbstkontrolle über den Lehrstoff und das Lerntempo haben.[96]

Es gibt einige Empfehlungen, um dem Zielpublikum ein Gefühl von Zufriedenheit (Satisfaction) zu vermitteln. Allem voran steht die Prüfung des gerade erworbenen Wissens. Für diesen Zweck bieten sich ebenfalls Lernspiele oder Simulationen an. In den Lernangeboten sollte anfangs noch häufig positives Feedback gegeben werden, wenn Aufgaben richtig gelöst wurden. Um sich auch selbst z. B. in Form von besonderen Spielangeboten belohnen zu können, wird angeraten, wenn die Lernenden diese vorab selbst wählen können. Für das notwendige Gerechtigkeitsgefühl bei der Bewertung von abschließenden Tests ist darauf zu achten, dass wirklich nur das Gelehrte abgefragt wird und dass die Maßstäbe der Bewertung auch nachvollziehbar sind.[96]

Copyright

7.3 Lerntheorien

Mit der Selbstbestimmungstheorie versucht man die Motive und das daraus resultierende Verhalten von Lebewesen zu untersuchen und zu erklären. Dass dieses Verhalten nicht nur Auslöser (wie beispielsweise bestimmte Spielelemente) hat, sondern auch über bestimmte Wege und eine gewisse Zeit erlernt ist, postulieren die Lerntheorien. Zu den wichtigsten Lerntheorien gehören Verhaltenslernen bzw. Behaviorismus, Kognitivismus und Konstruktivismus.

7.3.1 Behaviorismus

Grundlage des Behaviorismus ist das Reiz-Reaktions-Modell. Das Lebewesen reagiert dabei auf einen Reiz mit einer angeborenen oder erlernten Verhaltensweise. Konsequenzen aus dem Verhalten werden als neue Reize gespeichert und dadurch das Verhalten beeinflusst. Wenn spontanes Verhalten mit einem Reiz gekoppelt wird oder ein neutraler Reiz mit einem anderen Reiz zeitlich gekoppelt wird, spricht man von operanter bzw. klassischer Verhaltenskonditionierung. Aber nicht nur durch eigenes Handeln oder Verstärkung eines Reizes in diesem assoziativen Verhaltenslernen kann sich ein Lebewesen Verhalten und Wissen aneignen, sondern auch durch Beobachtung und Nachahmung von Verhalten.[97] Beobachtungslernen von einem Modell und assoziatives Lernen sind nicht vollständig voneinander trennbar. Denn das beobachtete Verhalten, das eine Person ausführt, kann durch eine anschließende klassische oder operante Konditionierung gefördert oder verhindert werden. Auch die Folgen einer Handlung, die andere durch die Beobachtung der ausführenden Person sehen, können Handlungen ermutigen oder davon abhalten. Im Bereich der (frühkindlichen) Bildung hat Verhaltenslernen einen großen Stellenwert zur Disziplinierung und Förderung des sozialen Umgangs durch positive und negative Verstärkung.[98]

7.3.2 Kognitivismus

Kognitivismus untersucht die Verarbeitung von Informationen durch den Menschen zum Zwecke der Problemlösung. Man geht davon aus, dass der Mensch nicht nur auf bestimmte Situationen reagiert, sondern durch die Anwendung von berechenbaren Beziehungen und Regeln auch zielgerichtet und problemorientiert handelt. Die Informationen werden aufgenommen, zu Wissen verarbeitet und im Gehirn gespeichert.

Copyright

Die Lernenden sind aktiv am Lernprozess beteiligt, können diesen aber nicht selbsttätig steuern, weil das die Lehrenden durch die didaktische Aufbereitung des Lehrstoffs übernehmen. Die Konsequenz daraus ist, dass den Lernenden die Entscheidungsfreiheit genommen wird und sie deshalb extern gesteuert sind. Es hängt stark von einer guten Informationsübertragung vom Sender (Lehrende) zum Empfänger (Lernende) ab und einer verständlichen Informationskommunikation, was und in welcher Weise die Lernenden die Informationen aufnehmen und verarbeiten.[97]

Eine kognitive Lerntheorie ist die Selbstwirksamkeit. Sie wird durch vier Faktoren der direkten und stellvertretenden Erfahrung, der verbalen Überzeugung sowie der emotionalen und physiologischen Zustände und deren Zusammenspiel beeinflusst.[13]

Wenn Lernende direkt selbst eine positive Erfahrung machen, dann wird das Gefühl der positiven Selbstwirksamkeit verstärkt bzw. das Gefühl, die richtige Entscheidung getroffen und eigene Fähigkeiten zur Lösung genutzt zu haben. Ist die Erfahrung eine negative, dann müssen entweder andere Personen aus dem Arbeitsumfeld in Stellvertretung den besseren, sicheren und richtigen Weg aufzeigen, so dass dieser beobachtet, nachgeahmt und verinnerlicht werden kann oder die Vorgesetzten müssen mit Vertrauenszuspruch in die Kompetenzen der Person und Unterstützung bei stark emotionsgetriebenen Verhaltensweisen auf die Mitarbeiter eingehen und Regelverstöße nicht sanktionieren, sondern die Gründe für die mitunter stressbedingten, panischen Handlungen für unsicheres Verhalten ermitteln und somit die Angst vor Fehlverhalten abbauen.[13]

Die Einschätzung der Handlungsfähigkeiten fällt pro Person unterschiedlich aus und ist abhängig von der subjektiv wahrgenommenen Schwierigkeit einer Aufgabe und denen zur Lösung zur Verfügung stehenden persönlichen Mitteln. Im Bewertungsprozess der Aufgabe muss die Person vor allem die verschiedenen psychischen Zustände für sich evaluieren. Dazu gehören die Analyse des aktuellen emotionalen, kognitiven und motivationalen Zustandes bei der Überlegung zur Aufgabenbewältigung sowie die Entscheidung für eine der Handlungsoptionen. Ist eine Person nicht angstgetrieben oder gestresst und zuversichtlich, was die Lösung der gestellten Aufgabe betrifft und zudem

Copyright

bereit, entsprechend Aufwand in die Problembehandlung zu investieren, hat sie die notwendige Motivation und trifft die Entscheidung, die Aufgabe auch zu lösen. Personen mit einer höheren individuellen Selbstwirksamkeitserwartung verstehen schwierige Aufgaben deshalb auch eher als Herausforderung und nicht als eine Belastung. Sie verwenden auch höhere Anstrengungen an die Lösungsbewältigung und gehen mit Rückschlägen und Misserfolgen gelassener um als Personen mit einer niedrigen Selbstwirksamkeitserwartung.[99] Hier gibt es eine eindeutige Überschneidung mit selbstbestimmt Lernmotivierten (siehe auch 7.1 Lerntypen).

Das Bild 33 zeigt die Möglichkeiten zur Förderung des Selbstwirksamkeitserlebens bei den Wirksamkeitsfaktoren Erfahrung und Überzeugung. Durch die gemeinsame Festlegung von Zielen sowie die Überwachung der schrittweisen Realisierung wird der Zielerreichungsprozess der Lernenden unterstützt. Werden Lernende mit unterschiedlichem Lerntempo in gemeinsamen Lerngemeinschaften mit einem Gesamtgruppenziel zusammengestellt, zeigen Personen mit einer höheren Selbstwirksamkeit Lösungswege auf, die von den Schwächeren aufgrund des Identifikationsfaktors mit der Gruppe und den Mitgliedern bereitwillig adaptiert werden. Die schwächer Lernenden sammeln somit stellvertretend ihre Erfahrungen. Ein weiteres Instrument zur Steigerung der Selbstwirksamkeitserwartung ist das Aufzeigen der individuell bereits vorhandenen Kompetenzen in einem Reflexionsgespräch zwischen Lehrenden und Lernenden. Die Lehrenden leisten damit verbale Überzeugungsarbeit und stärken das Vertrauen der Lernenden in ihre eigenen Fähigkeiten.[99]

	eigene Erfolgserfahrung	***stellvertretende Erfolgserfahrung***	***sprachliche Überzeugung***
Wirkfaktor	*erfolgreiche Aufgabenbewältigung*	*Beobachtung von Erfolgserfahrungen*	*Ziel- / Ergebnisabgleich*
Förderung des individuellen SelbstWirksamkeits-erlebens	*Förderplanung: Systematische Zielsetzung (SMARTe-Ziele) und Evaluation der Zielerreichung Visualisierung der Zielerreichung*	*Darstellung der Bewältigung von herausfordernden Situationen durch ein Modell (MitschülerInnen) Peer-Tutoring*	*Reflexionsgespräche zwischen Lehrkraft / SchülerIn / Eltern Wertschätzung der Meinung der Schülerin / des Schülers*

Bild 33: Strategien zur Förderung des Selbstwirksamkeitserlebens; Quelle: [99]

Copyright

Bei einer sehr gemischten Gruppe von Lernenden kann die Konzentration auf die Personen mit niedriger Selbstwirksamkeitserwartung zur Vernachlässigung derer führen, die eine hohe haben. Jedoch ist auch deren Motivation recht hoch, die Aufgabe selbständig zu lösen und erwarten oder wollen deshalb auch keine externe Unterstützung. Ob die Selbstwirksamkeitserwartung hoch oder niedrig ist, lässt sich über die Messung von z. B. Herzrasen aufgrund von Stress oder Anspannung bei der Präsentation der Aufgabe auch körperlich messen. Awareness und damit sicheres Verhalten ist also über verschiedene Faktoren ermittelbar.[13] Es ist zu vermuten, dass je sicherer sich ein Mensch fühlt, desto niedriger sind auch die stressauslösenden Faktoren. Das heißt, dass Symptome wie Herzrasen dort nicht auftreten. Für die Beurteilung des Awareness-Levels und damit für die Bewertung von Stresssituationen in einem Unternehmen ist das psychologische Modell für die Bewältigung von Stress interessant. Eine schlechte Stressbewältigung kann nämlich die Informationssicherheit gefährden.

Psychologische Modelle konzentrieren sich auf die kognitiven Reize, die als Stressor wahrgenommen werden und wie diese Informationen verarbeitet werden.[100] Die kognitiven Reize sind durch gedankliche Konflikte, Widersprüche und Überraschungen hervorgerufen.[101] Aber nicht jede Situation oder jeder Reiz ist für jeden Menschen ein Stressauslöser und wird demzufolge anders verarbeitet. Erst wenn diejenige Person nach einem Bewertungsprozess von Relevanz und Konsequenz und Abschätzung der Bewältigungsmöglichkeiten bzw. Fähigkeiten (sogenannter Coping-Prozess) nicht weiß, wie sie mit einer sie herausfordernden Situation umgehen soll, entsteht Stress.[100] Der Person fehlt die nötige Handlungsoption, was bei ihr Stress verursacht.

Für die Bewältigung von Stress ist es dabei nicht ausschlaggebend, welche Methode – entweder die bewusste Vermeidung oder die instrumentelle Ausschaltung – verwendet wird, sondern dass die das Coping anwendende Person über ein breites Wissen von Strategien verfügt und es auch der Situation entsprechend und flexibel einsetzt. Die Flexibilität des Einsatzes hängt stark davon ab, welche sozialen, finanziellen und externen Ressourcen und welche Handlungskompetenzen der Person zum aktuellen Zeitpunkt zur Verfügung stehen, um die Ressourcen zu nutzen.[100]

Copyright

Es ist wie bei der Vorbereitung auf eine Prüfung. Man kann den Stress auf relativ einfache Art vermeiden, indem man die Prüfung nicht antritt oder man bereitet sich intensiv auf den zu prüfenden Sachverhalt vor, wendet dazu bewährte Lernstrategien an und reduziert somit den Stressor „Prüfung“.

Ausgewählte Stressoren für die Bedrohung der Gewährleistung der Informationssicherheit können Berufseinstieg oder -ausstieg, Zeitdruck, Überforderung und Unterforderung, Konkurrenz, zwischenmenschliche Konflikte und Reizüberflutung sein.[100]

Diese Stressoren sind bei jedem Menschen anders ausgeprägt. Eine Person, die neu in einem Unternehmen beschäftigt ist, muss sich erst einmal mit den Gewohnheiten und seiner Arbeitsumgebung auseinandersetzen und ist damit auch einer gewissen Reizüberflutung ausgesetzt. Eine Person, die ein Unternehmen in naher Zukunft verlässt, ist möglicherweise auch gedanklich schon nicht mehr mit dem Unternehmen verbunden oder hat eine Vielzahl von Tätigkeiten an eine nachfolgende Person unter einem gewissen Zeitdruck zu übergeben, was sich in der oberflächlichen und nicht mehr gründlichen Abarbeitung seiner täglichen Arbeitsaufgaben äußern kann. Was für einen Menschen eine Überforderung darstellt, kann für den anderen gut geschulten Menschen eine Unterforderung sein. Beides ist gefährlich, da bei einer Überforderung die Angst vorherrscht, etwas falsch zu machen und man nicht weiß, wie die Situation zu handhaben ist und man dann möglichst gar nichts unternimmt. Bei einer Unterforderung besteht die Gefahr, dass man Fehler macht, weil man annimmt, alles schon zu kennen, die Sache „abzutun“ und nicht das Richtige der Situation Angemessene zu unternehmen. Auch ein vorherrschendes Konkurrenzdenken und damit verbundene zwischenmenschliche Konflikte beeinflussen die Wahrnehmung für sicherheitsgefährdende Situationen, weil man aus Angst, sich vor der Konkurrenz aufgrund einer falschen Reaktion zu blamieren, Fehler gar nicht erst eingesteht und kommuniziert und somit keine Reaktionen im Rahmen eines Incident Response Prozesses zur Bearbeitung des Vorfalls und Wiederherstellung der Informationssicherheit möglich sind.

Copyright

Durch eine detaillierte Analyse der Prozessabläufe z. B. mit Hilfe der Durchführung von Interviews können die Stressoren aufgedeckt werden, die zu unsicherem Verhalten führen. Mitunter versuchen Prozessbeteiligte auch unbewusst den Stressor zu vermeiden oder auszuschalten, indem sie eine andere und für sie weniger psychisch belastende Handlungsoption wählen. Im Interview können zusammen mit den Beteiligten die offensichtlichen Gründe für die Handlungswahl erörtert werden.

Zur Steigerung der Informationssicherheit in der Institution müssen diese Gründe entfernt und die alten, falschen Handlungsweisen durch neue, richtige ersetzt werden. Die neuen Verhaltensweisen müssen den Mitarbeitern einleuchten und sie müssen verstehen, warum es wichtig ist, die neuen Handlungsweisen anzuwenden. Es muss ihnen aber auch gestattet sein, Verbesserungen an neuen Richtlinien vorzuschlagen, wenn das von ihnen verlangte Verhalten in ihrem Arbeitsalltag nicht umsetzbar ist oder nicht vertretbare Auswirkungen hat. Wenn man es geschafft hat, dass der Willen zur Veränderung vorhanden ist, kann man diesen im Training mit einem Hinweisreiz kombinieren, der auch im Arbeitsalltag auftauchen kann. In der realen Situation würde dieser Hinweisreiz dann das sichere Verhalten „abrufen“.[102]

Stressauslösende Faktoren, die auf dem Angriff der menschlichen Schwächen beruhen, werden auch gern im Social Engineering verwendet, so dass es sich empfiehlt, diese im Training ebenfalls zu verwenden. Es sollten z. B. Situationen trainiert werden, in denen man unter Druck gerät, leichtgläubig Aktionen durchführt, neugierig auf eine Sache gemacht wird oder Zorn und Mitleid empfindet.

Für eine nachhaltige Verhaltensänderung ist eine hohe Beteiligung der Prozessbeteiligten notwendig sowie die Beurteilung der Auswirkungen einer verlangten Veränderung aus Sicht der Prozessbeteiligten. So ist es möglich, gemeinsam mit allen Beteiligten die optimale Lösung zu finden.[46]

Die Selbstwirksamkeitstheorie hat nach Ansicht heutiger Analysten jedoch Schwächen, weil sie lediglich die Erwartung einer Person berücksichtigt, nicht aber den Wert bzw. Zweck einer Handlung und somit Aspekte der Lernmotivation nur bedingt beschreiben

Copyright

kann. Heutige Motivationstheorien gehen davon aus, dass nicht nur eine Komponente das Handlungsgeschehen steuert, sondern dass weitere Komponenten wie z. B. die Qualität der sozialen Beziehungen und des emotionalen Erlebens während der Handlung Verhalten beeinflussen. Kognitive Theorien sind deshalb nicht ausreichend und wurden durch andere Theorien wie die der Selbstbestimmungstheorie ergänzt, welche auch die Ausrichtung der Motivation – also das Warum – betrachtet. Die Ausrichtung der Motivation hat nämlich erhebliche Auswirkungen auf die Persistenz, die Erlebensqualität und die Art der Handlungsergebnisse (vgl. Abschnitt 5).[21]

7.3.3 Konstruktivismus

Im Konstruktivismus gestaltet der Mensch seine Umwelt nach seinen individuellen Vorstellungen aus der Beobachtung, der Wahrnehmung, dem Denken und den individuell bereits vorhandenen Erkenntnissen. Um erfolgreich zu lernen, muss dieser Prozess der Konstruktion der eigenen Welt durch Störungen unterbrochen werden. Dies kann durch komplexe Lernumgebungen mit realitätsnahen Inhalten und Aufgaben erfolgen, welche die Selbstorganisation und den sozialen Austausch des Menschen mit der Umwelt erfordern. Auch das können die Lehrenden durch einen ausgewogenen Dialog mit den Lernenden aktiv beeinflussen.[97]

Weil in der Online-Lerntechnologie die Einflussnahme der Lehrenden begrenzt ist, kann hier hauptsächlich nur die Theorie des Verhaltenslernens in das Trainingsprogramm integriert werden. Im Nachgang an die Online-Schulung können dann die Motive für das Verhalten im Rahmen der Selbstbestimmungstheorie untersucht werden. In der Lerntechnologie muss dabei sichergestellt sein, dass auch die richtigen Verhaltensweisen verstärkt und die anderen (z. B. das Vermeiden des Lernens) geschwächt werden. Dazu kann Gamification in Form von positiven Verstärkern bzw. Anreizen als Reiz-Reaktions-Modell eingesetzt werden. Aber auch bei der Realisierung dieser Lernmethode haben die Lehrenden ein enormes Maß an Kontrolle, indem sie die Lernpfade und das Lernen überwachen sowie Feedback geben. Der Lerngemeinschaft wird damit die Entscheidungsfreiheit entzogen, also die Autonomie. In Bezug auf die Selbstbestimmungstheorie würde somit ein wichtiger Aspekt verlorengehen. Jedes Mitglied der Lerngemeinschaft könnte sein Lernen nicht mehr selbst bewerten und würde

Copyright

damit das psychologische Bedürfnis der Kontrolle über das eigene Leben nicht befriedigen können und in der Folge demotiviert sein.[103] Um das zu vermeiden, müssen in die Lernumgebung Spielelemente eingebaut sein, die neben der sozialen Zugehörigkeit zu einer Gruppe, dem Erleben der eigenen Kompetenz, auch eine Autonomie ermöglichen. Individuell festlegbare Ziele und flexible Lösungswege sollten deshalb den Vorzug vor einer zu stringenten Zielvorgabe und geradlinigen Führung erhalten.

7.4 Spielebasiertes Lernen

Gamification im Kontext des Lernens kann in den Varianten spielebasiertes Lernen und gamifiziertes Lernen vorkommen. Spielebasiertes Lernen (game based learning) erfolgt in einem vollwertigen interaktiven Spiel wie bspw. in sogenannten Serious oder Educational Games. Gamifiziertes Lernen konzentriert sich auf die Veränderung und Anpassung bestehender Lernprozesse mit Spielelementen, um das Lernen für den Benutzenden spielähnlich zu gestalten.[24]

Gegenüber klassischen Lernmethoden haben Serious Games den Vorteil, dass sie sich auch unabhängig von Alter und Games-Affinität der Nutzenden einsetzen lassen.[17]

Typisch für Serious Games beim spielebasierten Lernen ist die Absolvierung einer spezifischen Spielsituation unter Konfrontation der Spielenden mit Lerninhalten. Die Spielenden werden durch das Spiel in ihrer Motivation unterstützt, das Lernmaterial durchzuarbeiten. Für die Produktion der Spiele kann auf Drittanbieter für individuell gestaltete Spiele, auf vorgefertigte Spiele oder Spielvorlagen sowie auf kommerziell angebotene Videospiele zurückgegriffen und an die Lernziele angepasst werden. Die Entscheidung für die jeweilige Variante ist dabei davon abhängig, welcher Zeit- und Kostenrahmen zur Verfügung steht. Individuell angefertigte Spiele sind kostspieliger und zeitaufwendiger als vorgefertigte Spielvorlagen oder am Markt befindliche kommerzielle Spiele. Ein Nachteil der preiswerten Varianten kann jedoch durch die Unzulänglichkeit der Moderatoren oder Lehrenden bezüglich der Qualität ihrer Aufgabenerfüllung entstehen. Denn diese müssen in der Lage sein, die Lerngemeinschaft richtig zu lenken, so dass sowohl die Lehrenden als auch die Lernenden das Bildungsziel erreichen.[103]

Copyright

Ein Beispiel für ein kommerzielles Spiel ist „Minecraft“, welches heute schon in verschiedenen Themenfeldern im Bildungsbereich Anwendung findet (siehe https://education.minecraft.net/de-de/resources/computer-science-subject-kit).

Ein Beispiel für ein individuell zugeschnittenes Spiel ist das Spiel „The SECRET of Photonorvin“. Es ist ein speziell für die Bayer AG entwickeltes Serious Game der Firma Fabula Games GmbH mit dem Ziel, die Mitarbeitenden des Unternehmens weltweit wieder für das Thema Informationssicherheit zu interessieren und zu einer Änderung des Verhaltens zu führen, das sicherer ist als bisher.[104]

Ein Beispiel für ein vorgefertigtes und sofort einsatzbereites Serious Game im Bereich Informationssicherheit ist „myRo P7“ der Firma Fabula Games GmbH. Das Bild 34 zeigt eine Szene aus diesem Spiel, welches insgesamt 13 Themen der Informationssicherheit behandelt. Es müssen aktiv Entscheidungen getroffen und die folgenden Konsequenzen von den Spielenden getragen werden. Mehrfach werden die gewünschten sicheren Verhaltensweisen trainiert. Bei Bedarf steht während des Spiels ein Mentor zur Verfügung. Alle Episoden schließen mit einem Test ab. Erst wenn der Test bestanden wurde, kann die nächste Episode gespielt werden. Neben der Freischaltung der nächsten Episoden werden weitere Spielelemente genutzt. Dazu gehören z. B. Rätsel, die gelöst werden müssen, Security Sterne, die gesammelt und Handlungsoptionen, die gewählt werden können.[105]

Bild 34: Szene aus dem Serious Game „myRo P7“; Quelle: [105]

Um das Spiel lebendig zu gestalten, muss der spielende Part dazu gebracht werden, eine Art Investition in das Spiel zu tätigen. Er wendet z. B. sein Wissen an oder gibt

Informationen über sich preis und sammelt dafür Belohnungen, die vorher nicht bekannt sind. Es entsteht ein kontinuierlicher Kreislauf aus Investition und Belohnung, wenn die Belohnungen stark genug waren, ihn neugierig zu machen und er weitere Investitionen in das Spiel vornimmt, um weitere Belohnungen zu erhalten. Dieser Zyklus, dargestellt im Bild 35, beginnt mit einem externen Auslöser, dem eine Aktion folgt und eine stets variable unvorhersehbare Belohnung, auf welche wiederum eine Investition folgt. Im späteren Verlauf wird aus dem externen Auslöser ein interner Trigger, das Spiel fortzusetzen, weil eine intrinsische Motivation entstanden ist bzw. eine Konditionierung über das Belohnungssystem stattgefunden hat.

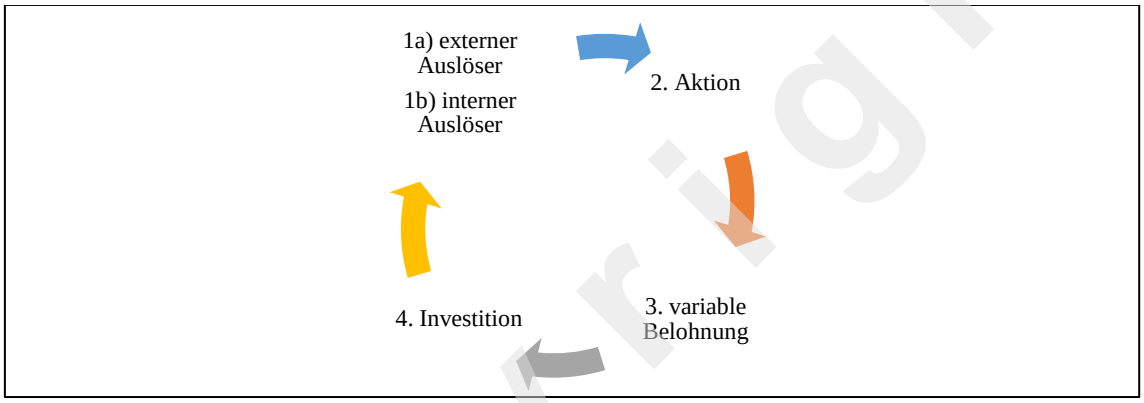


Bild 35: Kreislauf eines erfolgreichen Produkts; Quelle: in Anlehnung an [106]

Dieses System folgt somit dem Modell von Nir Eyal namens „Hooked“[54] und kennzeichnet nach seinem Dafürhalten ein erfolgreiches Produkt. Er spricht von alten Gewohnheiten, die Menschen haben und von der Schwierigkeit, neue Gewohnheiten bei Menschen zu etablieren. Nur über die häufige Anwendung eines Produktes bzw. einer Verhaltensweise oder über die wahrgenommene Nützlichkeit dessen zur Vermeidung oder Erleichterung von einer Art Schmerz oder zur Erhöhung des Wohlbefindens werden alte Gewohnheiten abgelöst und die neuen verfestigt. Ist der Gebrauch zur Gewohnheit geworden, dann wird es als Automatismus im Gehirn abgespeichert und nur noch abgerufen. Es wird zu einer automatischen Verhaltensweise. Um die Wahrscheinlichkeit einer gewünschten Handlung zu erhöhen, muss der gedankliche Aufwand für die Entscheidung zur Durchführung der Aktion so gering wie möglich gehalten werden. Das können beispielsweise auf ein Minimum reduzierte Auswahlmöglichkeiten sein.[54]

Copyright

7.5 Gamifiziertes Lernen

Spielmechaniken wie z. B. Punkte, Level und Abzeichen werden auch in Lernmanagementsystemen angewendet. Im Wesentlichen gibt es ein traditionell strukturiertes Trainingsprogramm, welchem mit diesen Elementen zusätzlicher Schwung verliehen wird. Die Spielmechaniken wie das Sammeln von Punkten, Prämien oder der Erhalt zusätzlicher Spielzeit oder die Löschung von falschen Antworten werden auch während des Spiels integriert und nicht wie bei z. B. Serious Games nach Abschluss einer bestimmten Spielszene.[103] Man spricht in diesem Zusammenhang auch vom gamifizierten Lernen.

In der Theorie des gamifizierten Lernens werden vier Komponenten genannt, die einen direkten Zusammenhang zwischen Gamification und Lernen erklären sollen. Es handelt sich dabei um Lehrinhalte, Verhaltensweisen und Einstellungen, Spieleigenschaften und Lernergebnisse. Der Lernprozess wird dabei durch einen spielähnlichen Kontext unterstützt. Ein Kritikpunkt an dieser Theorie ist jedoch, dass nicht klar erkennbar ist, welchen Beitrag die Spielgestaltung bzw. einzelne Spielelemente zu einem wirksamen Lernmechanismus leisten.[24]

Gamification hat erwiesenermaßen positive Effekte auf kognitive, motivationale und verhaltensbezogene Lernergebnisse. Lernrelevante, d.h. vor allem interaktive und konstruktive Aktivitäten führen zu einer tieferen kognitiven Verarbeitung beim Lernen. Der Einsatz von Gamification beim Lernen fördert den Enthusiasmus, ermöglicht ein sofortiges Feedback auf die eigene Leistung, kann das Bedürfnis nach Anerkennung befriedigen und unterstützt die Zielerreichung. Durch die Verwendung von Begriffen und Konzepten, die aus dem Alltag bekannt sind und mit positiven Assoziationen verbunden werden, kann das Engagement durch Game-Design-Elemente wie beispielsweise der Fortschrittsanzeige erhöht und Vertrauen aufgebaut werden.[107]

Gamification ist eine Art Pädagogik, welche die Zuversicht der Lernenden auf Erfolg steigern soll, ohne dabei die Glaubwürdigkeit der Bildung zu beeinträchtigen. Der treibende Faktor bei Gamification ist der Wettbewerb – entweder gegen sich selbst oder gegen eine Gruppe.[70]

Copyright

7.6 Frameworks

In diesem Abschnitt werden drei bekannte Vorgehensweisen zur Modellierung von Spielen vorgestellt, wovon eine vertieft behandelt wird.

7.6.1 MDA-Framework

Im sogenannten MDA-Modell[108] wird zwischen der Mechanik, Dynamik und Ästhetik eines Spiels unterschieden, wobei die Mechanik vom Designer direkt beeinflusst werden kann, die Ästhetik ist die direkt bei den Spielenden ausgelöste emotionale Antwort bzw. das Nutzendenerlebnis (vgl. Bild 36). Die Dynamik stellt damit das Bindeglied zwischen Mechanik und Ästhetik dar. Je nachdem wie gut die Mechanik eines Spiels gestaltet ist, ist auch die Dynamik des Spiels und damit das Erlebnis. Beispielhaft sei hier die Bestenliste als Mechanik genannt, der damit ausgelöste Wettbewerb als Dynamik und die entsprechende Herausforderung bei den Spielenden als Ästhetik. Ein anderes Modell verwendet Komponenten als Verkörperung der Mechaniken und Dynamiken eines Spiels. Sie sind die Ausgangsbasis für die Mechaniken, denen wiederum die Dynamiken folgen. Beispiele für diese Spiel-Elemente-Hierarchie sind Levels als eine Form von Komponenten, Feedback als eine Art der Spiel-Mechanik und Fortschritt als Form der Dynamik. In anderen Betrachtungen gelten die Spiel-Mechaniken als Grundbausteine für Gamification. Die Spiel-Dynamiken spiegeln sich in den Erlebnissen wieder, welche die Nutzenden haben. Diese folgen wiederum einer bestimmten Motivation. Als Motive werden Neugierde, Leistung, soziale Anerkennung, sozialer Austausch, kognitive Stimulierung und Selbstbestimmung genannt.[22] Ob Nutzende ein bestimmtes Motiv im Spiel verfolgen, ist individuell unterschiedlich und vom subjektiven Empfinden der Spielenden abhängig.[22]

In diesem Zusammenhang sei auf die verschiedenen Persönlichkeitstypen aus der Wissenschaft der Psychologie (Abschnitt 4.5 Persönlichkeitstypen), auf die verschiedenen Lerntypen im Rahmen der Didaktik (Abschnitt 7.1 Lerntypen) und auf die verschiedenen Spielertypen hingewiesen, auf welche in diesem Kapitel noch näher eingegangen wird.

Copyright

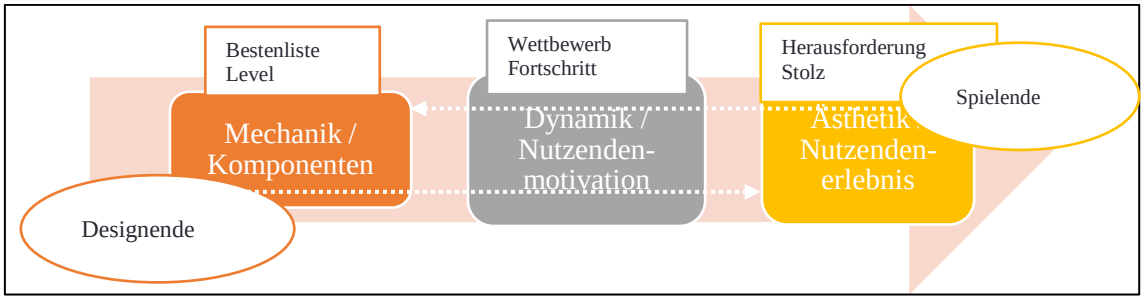


Bild 36: abgewandeltes MDA-Framework; Quelle: eigene Darstellung in Anlehnung an [22]

Das erwähnte Game-Design-Modell kann auch für Gamification verwendet werden. Weitere Einsatzorte von Gamification sind aus dem Bild 37 ersichtlich. So kommt Gamification auch in weiteren Methoden, Mechanismen und Game-Design-Grundsätzen zum Einsatz. Um gamifizierte Anwendungen spezifisch nach den Nutzenden zu entwerfen, wird empfohlen, Schritt für Schritt von den Game-Design-Methoden über die Modelle, Grundsätze und Mechanismen zu den Elementen zu gelangen und entsprechend den Nutzerbedürfnissen bzw. Anwendungszielen anzupassen.[19]

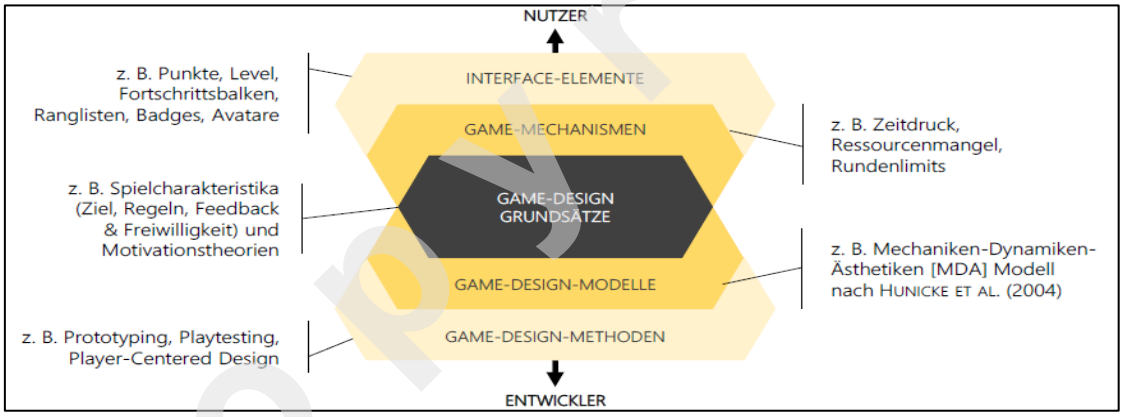


Bild 37: Einsatz von Gamification; Quelle: [19]

7.6.2 COFELET-Framework

Das COFELET-Framework (Conceptual Framework for eLearning and Training) ist ein konzeptioneller Rahmen für die Gestaltung und Umsetzung von pädagogisch wirksamen Serious Games zur Cybersicherheit.[109] Mit diesem Rahmen werden die Hauptelemente für die Gewährleistung der Wirksamkeit des Serious Games festgelegt.[110] Das Rahmenwerk ist eine Erweiterung des Learning Mechanic – Game Mechanic-Modells (LM-GM-Modell)[111] und basiert als ATMSG-Modell (Activity Theory Model for Serious Games)[112] auf der Aktivitätstheorie.[109] Die Aktivitätstheorie ist eine sozial-

Copyright

konstruktivistische Lerntheorie, die Lernspiele als interaktive, zusammengesetzte und dynamische Systeme betrachtet, die unter Spiel-, Lern- und Lehrperspektiven analysiert werden.[109] Das zentrale Element im COFELET-Rahmen ist die Aufgabe (siehe Markierung im Bild 38), welche die Handlungen darstellt, die von den Lernenden oder anderen Charakteren (z. B. Mentoren, Mitspielern, Gegnern) ausgeführt werden. Der „Scenario Execution Flow“ beschreibt die notwendige Reihenfolge der Aufgabenabarbeitung durch die Lernenden und die Verknüpfung der verschiedenen Aufgaben untereinander. Der Spielkontext („Gaming“) beschreibt den Zustand des Spiels mit seinen Eigenschaften in Bezug auf Spielstände, Spieldauer, Koordinaten der Avatare etc. und der bestehenden Bedingungen. Die Komplexität des Szenarios („Scenario Complexity“) ergibt sich aus der Anzahl der Aufgaben, die erfüllt werden müssen. Die verschiedenen Stresslevel („Stress Level“) im Spiel werden z. B. durch Zeitbeschränkungen zur Aufgabenlösung oder durch das Punktevergabe- und Punkteabzugssystem erzeugt.[109] Eine Empfehlung für Serious Games, die für die Zwecke der Sensibilisierung für Informationssicherheit eingesetzt werden, ist die Orientierung bei der Reihenfolge der Aufgaben an realen Angriffsverläufen aus den bekannten Cybersicherheitsmodellen wie dem MITRE ATT&CK-Framework.[109]

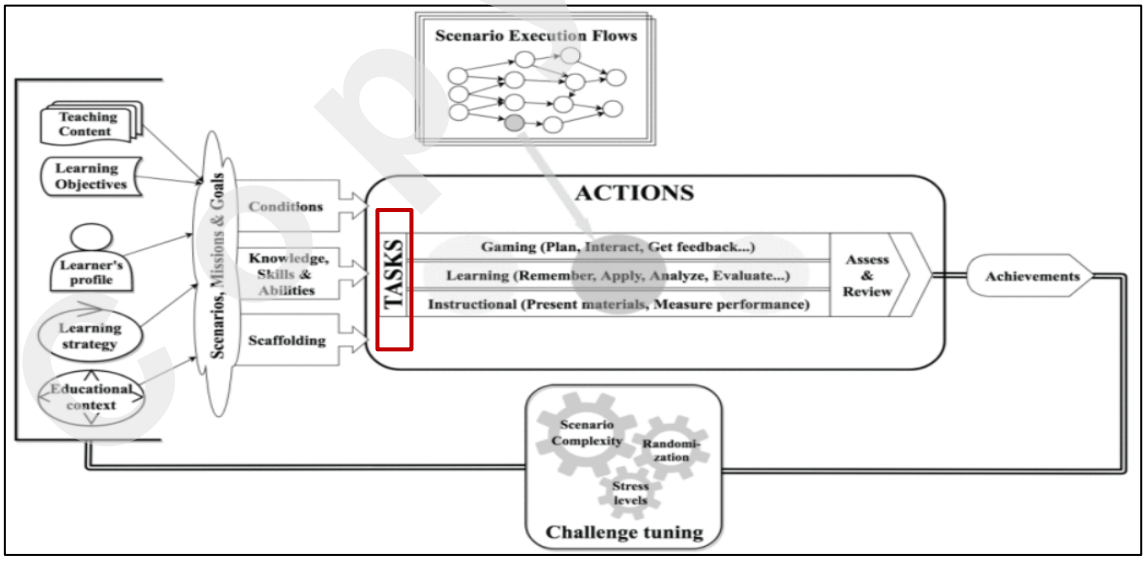


Bild 38: COFELET-Framework; Quelle: [109]

Copyright

7.6.3 OCTALYSIS-Framework

Ein anderes Framework ist OCTALYSIS von Yu-kai Chou[113]. Dabei ist das Design eines Spiels auf den Menschen mit seinen Gefühlen, Motivationen und seinem Engagement ausgerichtet und nicht auf die Funktionen eines Spiels. Punkte, Abzeichen und Bestenlisten sind für das Spieledesign wichtig, aber die wirkliche Motivation der Spielenden liegt z. B. in der Strategie eines Spiels oder in der Möglichkeit, sich gegen andere Spielende zu behaupten oder sich selbst herauszufordern. Es sind die intrinsischen Faktoren, welche die Benutzenden zur Fortführung eines Spiels motivieren und nicht allein die extrinsischen Motivationsfaktoren wie Punkte, Abzeichen oder Level.

Kernantriebe

Es gibt laut Yu-kai Chou[113] acht Kernantriebe, die uns zum Handeln motivieren.

- 1) Berufung: Spielende müssen glauben, dass sie zu etwas ganz Besonderem berufen sind, was größer als sie selbst ist.
- 2) Leistung: Spielende müssen sich Herausforderungen stellen, für welche sie in den meisten Fällen eine Belohnung erhalten.
- 3) Kreativität: Spielende müssen ihre kreativen Fähigkeiten benutzen und erhalten dafür Feedback.
- 4) Besitz: Menschen möchten gern etwas besitzen, es vergrößern und die Kontrolle darüber haben. Das gilt auch im Spiel.
- 5) Umfeld: Für Menschen sind (auch in Spielen) soziale Akzeptanz, soziales Feedback, Kameradschaft, Wettbewerb und Neid starke Motivationsfaktoren für die Ausführung einer Handlung.
- 6) Knappheit: Knapp vorhandene, seltene, nicht sofort verfügbare oder exklusive Dinge motivieren Personen, immer wieder nach Gelegenheiten zu suchen, diese Dinge zu besitzen.
- 7) Neugierde: Menschen werden neugierig, wenn etwas Unvorhersehbares passiert bzw. von im Gehirn gespeicherten Standardmustern abweicht.
- 8) Verlust: Menschen wollen Negatives vermeiden. Ein Beispiel ist das Bestreben nach der Erhaltung einer Chance im Spiel, die sich

Copyright

möglicherweise nicht wieder ergibt.

Das Bild 39 zeigt die psychologischen Kernantriebe, die dabei entweder intrinsischer oder extrinsischer Natur sind, welche als positiv oder negativ gelten.[113]

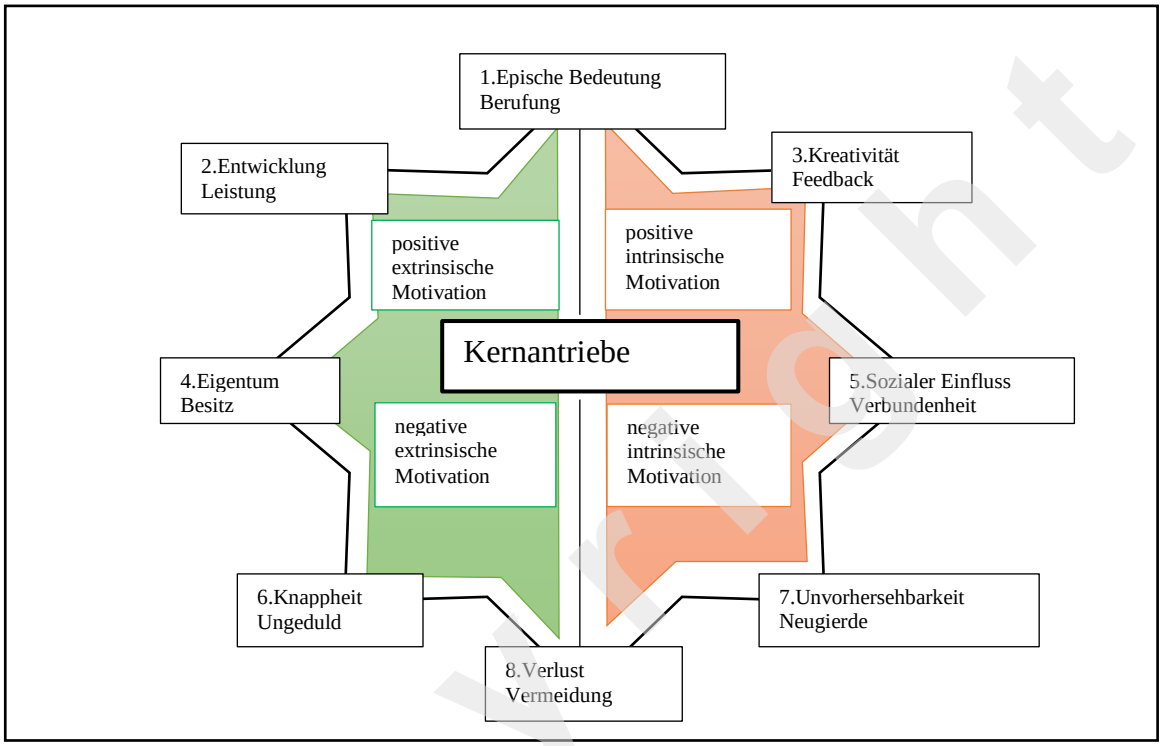


Bild 39: 8 Kernantriebe für Verhalten; Quelle: eigene Darstellung in Anlehnung an [124]

Um dieses Rahmenwerk auf die Informationssicherheit zu übertragen, muss ermittelt werden, wie diese acht Kernantriebe innerhalb der vier Phasen einer Heldenreise[114] in einem Lernprozess unterschiedlicher Spielertypen durch Gamification optimal angesprochen werden können. Das Modell des erfahrungsbasierten Lernens, das häufig in Schulungen verwendet wird, ist dabei eine Anwendung der Heldenreise, die ursprünglich auf den Theorien von Joseph Campbell und Christopher Vogler[115] zum Aufbau guter Geschichten basiert. Sie ist auf jedes Genre übertragbar, in denen Stories erzählt werden sollen, die einen Konflikt und dessen Lösung beschreiben wollen.

Phasen der Heldenreise

Die vier Phasen bestehen aus dem Entdecken von Inhalten und Argumenten für das Spiel, der Einführung zur Erklärung von Regeln und Werkzeugen, dem Kompetenzaufbau

Copyright

durch mehrfaches Wiederholen und Anwenden des Erlernten mit dem Fokus auf das große Ziel und dem Endspiel zur Bindung der Spielenden. Innerhalb der Phasen werden die Kernantriebe unterschiedlich stark genutzt. Unvorhersehbarkeit und Neugierde ist für die Phase der Entdeckung der Antrieb, sich näher mit einem Sachverhalt zu beschäftigen. In der Einführungsphase kann die Leistung der Spielenden der Motivationsfaktor sein, der am stärksten hervortritt. Getrieben von ihrem sozialen Umfeld versuchen die Spielbeteiligten in der Phase des Kompetenzaufbaus, bisher nicht umgesetzte Ziele zu erreichen, die sie in der Endphase des Spiels halten wollen und damit dem Kernantrieb der Vermeidung folgen.[113]

Für den Einsatz der Kernantriebe in den Phasen einer Heldenreise gibt es in der Literatur[113] Empfehlungen. Diese sind in der Tabelle 5 dargestellt.

Tabelle 5: Einordnung der Kernantriebe in die Phasen der Heldenreise; Quelle: eigene Darstellung

Kernantrieb		Phasen der Heldenreise			
		Entdeckung	Einführung	Kompetenzaufbau	Endphase
1	Berufung	x			
2	Leistung		x		
3	Kreativität			x	
4	Besitz			x	
5	Umfeld	x	x		
6	Knappheit			x	x
7	Neugierde			x	x
8	Verlust				x

Spielelemente

In den jeweiligen Kernantrieben beschreibt Yu-kai Chou[113] folgende Spielelemente:

<u>Kernantrieb 1:</u>

- Storytelling (siehe auch Abschnitt 6.3 Storytelling)
- Elitismus zur Schaffung eines Zusammengehörigkeitsgefühls einer gleichgesinnten Gruppe
- Heldentum zur Erfüllung einer bedeutenden Mission
- Anfängerglück zur Vermittlung eines „Auserwählten-Gefühls“
- Gratisgeschenke zur Erhöhung der Wahrscheinlichkeit des Wiederkommens

Copyright

Kernantrieb 2:

- Fortschrittsbalken zur Motivation, etwas zu 100 % zu erfüllen
- Erfolgssymbole wie Abzeichen, Trophäen, Medaillen, Punkte zur Einschätzung des aktuellen Status
- Ranglistenplätze mit Vorgänger- und Nachfolgeranzeige
- Team-Ranglisten
- Rockstar-Effekt für die Schaffung eines Gefühls, dass man etwas Besonderes ist, weil fremde Personen (Follower) sich für einen interessieren

Kernantrieb 3:

- Superkräfte, die nur vorübergehend aktiv sind
- Freischaltungen von Funktionen zu Zeitpunkten, wo man normalerweise das Spiel beenden würde
- Wahlmöglichkeiten

Kernantrieb 4:

- Sammelobjekte
- Punkte für den Tausch gegen einen wahrgenommenen Wert einer Handlung
- Schaffung von Vertrautheit durch ständige Beobachtung, auch Monitor-Attachment genannt
- Anpassung von Inhalten an Nutzergewohnheiten, der sogenannte Alfred-Effekt

Kernantrieb 5:

- Mentoring zur Führung und Begleitung im Spiel sowie zur Förderung von Fähigkeiten
- Trophäen-Regale oder sogenannte Angeber-Knöpfe zur Darstellung der erreichten Leistungen gegenüber anderen Spielenden
- Gruppenaufgaben, die nur zusammen mit anderen gelöst werden können
- Verwendung sogenannter sozialer Anstupser zum Zweck der Interaktion von Personen
- Konformitäts-Anker zur Visualisierung einer zu erreichenden Norm

Kernantrieb 6:

- Verbindung von Spiel und Realität durch Vergleichsangebote, die einen zu zahlenden Preis dem noch notwendigen Spielaufwand zur Erreichung eines Spielziels gegenüberstellen

Copyright

- Festlegung maximaler Obergrenzen als Motivationsfaktor zur Ausreizung dieser Grenzen
- Erzeugung einer Termindynamik, d. h. regelmäßiges Auftauchen ausgewählter Aktionen zu festgelegten Zeiten
- Einsatz sogenannter Folterpausen, eine für die Spielenden meist ungewollte Spielunterbrechung
- eingeschränkter Funktionsumfang am Beginn, der im Verlauf vergrößert wird

Kernantrieb 7:

- überraschende Hervorhebung durchzuführender Aktionen durch visuelle Effekte (Glowing-Choice)
- erwartete, auf eine bestimmte Aktion folgende, sogenannte Mistery Boxes, deren Inhalt unbekannt ist, aber eine Belohnung darstellt
- unerwartete, nicht an bestimmte Aktionen gebundene Belohnungen durch sogenannte Easter Eggs
- Gewinn einer unwahrscheinlichen Belohnung durch eine schrittweise Erarbeitung oder Investition in das Spiel (genannt Lotterie, rollende Belohnung)

Kernantrieb 8:

- Berechtigung auf eine bestimmte Art der Belohnung, welche die Spielenden mit der Durchführung spezifischer Aktionen erlangt haben (sogenanntes rechtmäßiges Erbe)
- zeitgebundenes Verschwinden einer Gelegenheit im Spiel, um eine schnelle Reaktion zu provozieren
- Ausnutzung der bestehenden Trägheit zur Änderung von Verhalten, auch Status Quo Faulheit genannt, d. h. Unterstützung des Verhaltens durch wiederkehrende, interessante Spielschleifen mit dem Ziel eines gewohnheitsmäßigen Verhaltens
- Einsatz des sogenannten FOMO-Punchs (Fear Of Missing Out) für die Erzeugung des Gefühls einer verpassten Chance
- Androhung des Verlustes aller erspielten und investierten Objekte bei Verlassen eines Spiels, auch Gefängnis der versunkenen Kosten genannt

Copyright

Kontext der Motivation

Ein wichtiger Aspekt im OCTALYSIS-Framework ist die Unterscheidung der Kernantriebe in Antriebe, die überwiegend der linken oder überwiegend der rechten Gehirnhälfte zugeordnet werden. Sie sind auch in der Bild 39 jeweils in der linken bzw. rechten Bildhälfte angeordnet. Aktivitäten im Zusammenhang mit Logik, Besitz und Analytik werden eher in der linken Gehirnhälfte verarbeitet. Sie sind von Natur aus ziel- bzw. ergebnisorientiert und meistens extrinsisch motiviert. Die Kernantriebe der rechten Hälfte berühren eher die Erfahrungen und den Prozess, die von der rechten Gehirnhälfte verarbeitet werden. Es ist möglich, dass extrinsische Motivatoren intrinsische Motivatoren überlagern und sich negativ auf die Gesamtleistung einer Aktivität auswirken, weil der Anreiz nicht mehr die reine Neugierde oder Kreativität ausnutzt, sondern die möglichst schnelle und mühelose Zielerreichung. Ein Beispiel für diesen Konflikt sind bezahlte Künstler. Je mehr Geld sie für ihre Kunst erhalten, welche sie selbst nicht als besonders kreativ empfinden, umso weniger kreativ werden sie bei den nächsten Kunstwerken sein. Sie erreichen ihr Ziel auch mit geringerem Aufwand. Der Kernantrieb drei (Kreativität und Feedback) verschiebt sich hin zu Kernantrieb vier (Besitz und Eigentum).[113]

Bezogen auf die Schaffung von Awareness bedeutet dies, dass zwar die Anwendung von informationsrichtigem Verhalten in alltags- und routineähnlichen Situationen mit extrinsischen Motivatoren wie Belohnungen durch Punkte, Fortschrittsbalken und Abzeichen unterstützt werden kann, nicht aber Verhalten in Situationen, die kognitive Fähigkeiten erfordern. Diese Situationen weichen vom Alltag und der Routine ab und können nur im Vorhinein beispielhaft trainiert werden. Diese Abweichung zu erkennen und die Einschaltung der kognitiven Fähigkeiten vorzunehmen, ist besonders bei realen Social Engineering-Angriffen wichtig. Hier werden von den Angreifenden bereits bestehende kognitive Verzerrungen (siehe Abschnitt 4) zusätzlich systematisch manipuliert, um das Opfer zu ungewollten Aktionsausführungen zu motivieren.

Extrinsische Motivatoren sind gerade auch in der Entdeckungsphase dienlich, um Interesse und Lust an einer Handlung zu wecken. Wenn Menschen den Nutzen und den Grund einer Handlung für sich erkennen, beschäftigen sie sich auch näher mit deren

Copyright

Inhalt. Dazu ist es hilfreich, ihnen eine extrinsische Belohnung für das Ausprobieren anzubieten, die im Einklang mit der notwendigen aufzuwendenden Zeit steht. Danach sollte eine intrinsische Belohnung beispielsweise durch Anerkennung, Status oder Zugang zu besonderen Aktionen erfolgen, um diese für die Sicherstellung des langfristigen Engagements zu nutzen. Um die intrinsische Motivation zu steigern, müssen mehr soziale, unvorhersehbare, kuriose Erlebnisse und sinnvolle Wahloptionen, die verschiedene Spielwege eröffnen, ermöglicht werden. Für die Förderung der Kreativität wird der Einsatz von Boostern, also kurzfristigen Superkräften, empfohlen, die verschieden sind und verschiedene Ziele erreichbar lassen machen.[113]

Für Spielanwendungen gibt es Design-Ansätze, die besonders die Benutzerfreundlichkeit in den Fokus stellen. Mit dem OCTALYSIS-Framework ist es zusätzlich möglich, auch die verschiedenen Motivationen zu implementieren und damit die Anwendung noch erfolgreicher zu machen.

Spielelemente und Spielphasen

Mit der Zuordnung der Kernantriebe zu den Phasen einer Heldenreise erfolgt eine Festlegung der zu verwendenden Spielelemente. Es kann aber vorkommen, dass einzelne Spielelemente in einer anderen Phase besser wirken. Der Einsatz von Mentoring ist nicht nur in der Anfangsphase von Spielen sinnvoll, sondern auch explizit in der Endphase, wenn es von erfahrenen Spielenden übernommen wird, um unerfahrene, neue Spielende in das Spiel einzuweisen.[113] Unter Berücksichtigung dieses und des Motivationsaspekts wird im Bild 40 eine spezifischere Einordnung der einzelnen Spielelemente in die Entdeckungs-, Einführungs-, Kompetenzaufbau- und Endphase vorgenommen. Zu den Elementen, die in der Entdeckungsphase eingesetzt werden, gehören hauptsächlich Storytelling, Heldentum, Elitismus, Anfängerglück, Gratisgeschenke, Sammelfiguren, Mentoring, rechtmäßiges Erbe, FOMO-Punch, anfangs schnell zu erhaltene Erfolgssymbole und die Verbindung von Spiel und Realität. Sie dienen dazu, die Spielenden für das Spiel neugierig zu machen, Ausprobieren zu fördern, frühzeitig an das Spiel zu binden oder ihnen einen Grund zu liefern, warum sie das Spiel sollten. Für die soziale Komponente und Überraschungsmomente vom Beginn an, dienen Anstupser und Easter Eggs. In der Einführungsphase wird die Aufmerksamkeit der

Copyright

Spielenden auf das Anhäufen von Punkten und das Gewinnen von Trophäen als Bestätigung der Leistungen gelenkt. Durch Limitierungen, Freischaltungen und schwindende Gelegenheiten werden diese Punktesysteme gleich in der Einführung beeinflusst. Die sozialen Komponenten in dieser Phase sind Angeber-Knöpfe, Gruppenaufgaben und der Rockstar-Effekt. Damit sich die Beteiligten gleich zu Beginn im Spiel zurechtfinden, kann das Spielelement Glowing Choice verwendet werden. In der Phase des Kompetenzaufbaus dienen Belohnungen, die nach erfolgreicher Aufgabenlösung vergeben werden. Das können Freischaltungen besonderer Inhalte, Superkräfte, spezielle Wahlmöglichkeiten und Belohnungen in Form von Geschenken (Mistery Boxes) und Spiel-Lotteriegewinne sein. Zur Darstellung der erworbenen Kompetenzen und zur Ermöglichung der Selbstreflexion und Orientierung werden den Spielenden jeweils Fortschrittsbalken, Ranglistenplätze, Team-Ranglisten, Maximalobergrenzen und der Konformitäts-Anker zur Verfügung gestellt. In der Endphase eines Spiels müssen die Beteiligten so lange wie möglich, im Spiel gehalten werden, um den maximalen Nutzen zu generieren. Dafür können Folterpausen und die Status Quo Faulheit der Spielenden genutzt werden. Hat man im Spielverlauf geschickt die Investition persönlicher Werte integriert, kann man jetzt die Angst vor dem Verlust aller investierten Werte ausnutzen, um die Endphase zu verlängern.

Kernantrieb	Spielelemente					
1	Storytelling	Heldentum	Elitismus	Anfängerglück	Gratisgeschenke	
2	Fortschrittsbalken	Erfolgssymbole	Statuspunkte	Ranglistenplätze	Team-Ranglisten	Rockstar-Effekt
3	Freischaltungen	Superkräfte	Wahlmöglichkeiten			
4	Sammelfiguren	Austauschpunkte	Vertrautheit	angepasste Vorlieben/Inhalte		
5	Mentoring	Trophäen	Angeber-Knöpfe	Gruppenaufgaben	Anstupser	Konformitäts-Anker
6	Spiel und Realität verbinden	Limitierungen	maximale Obergrenze	Termindynamik	Folterpausen	Freischaltungen im Spielverlauf
7	Glowing Choice	Mistery Boxes	Easter Eggs	Lotterie, rollende Belohnung		
8	rechtmäßiges Erbe	schwindende Gelegenheit	Status Quo Faulheit	FOMO-Punch	Gefängnis der versunkenen Kosten	

Phasen:	Entdeckungsphase	Einführungsphase	Kompetenzaufbauphase	Endphase
Motivation:	extrinsisch	intrinsisch		

Bild 40: Einordnung der Spielelemente in die Spielphasen; Quelle: eigene Darstellung

7.6.4 Kombination von OCTALYSIS- und MDA-Framework

Das OCTALYSIS-Framework beschreibt sehr umfassend die verschiedenen Motivationen und Gefühlszustände von Spielenden, aber die konkrete Entwicklung eines Gesamtkonzepts wird damit nicht ausreichend unterstützt. Für die Erstellung eines konkreten Gamification-Konzepts kann das MDA-Framework (siehe dazu Bild 41) besser behilflich sein, in welchem die Spielelemente ihre konkrete Zuordnung im

Copyright

Ästhetik-Teil des Rahmenwerks erhalten. In der Spieldynamik wird die zentrale strategische und zeitliche Gestaltung des Spiels definiert. In der Spielmechanik werden die Einstellungen zum Spielablauf, zu den einzelnen Spielprozessen und zum Management der Wahlmöglichkeiten festgelegt. Zutage treten die in der Spieldynamik und -mechanik festgelegten Phasen und Aktionen in den konkret von den Spielenden wahrnehmbaren Spielelementen.[116]

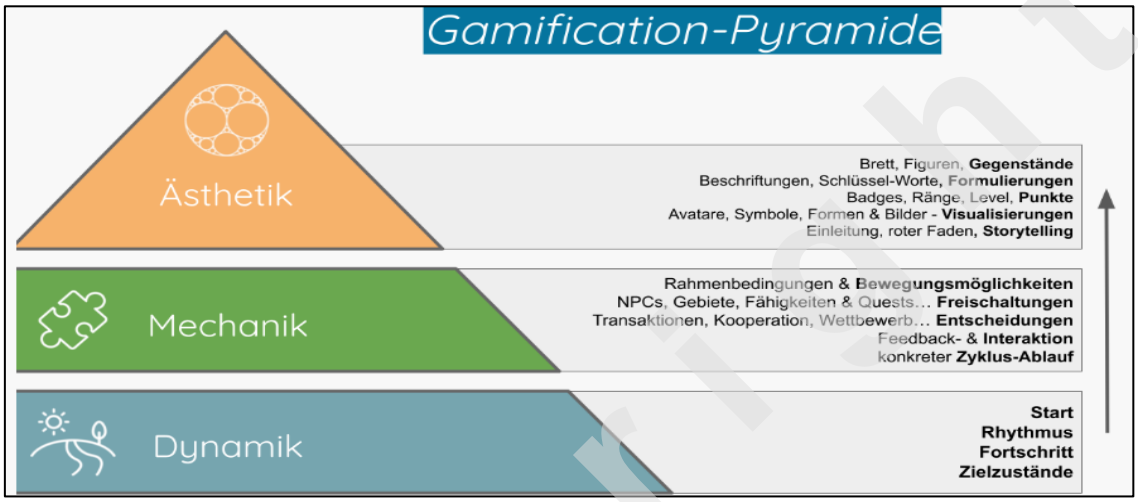


Bild 41: Einordnung der Spielelemente in das MDA-Framework; Quelle: [116]

In der Spieldynamik findet sich das OCTALYSIS-Framework in Form von Emotionen (Neugierde, Glück, Frustration), Limitierungen, Storytelling, Leistungen und sozialem Einfluss (Kameradschaft, Status, Altruismus) wieder. Hervorgerufen wird die Spieldynamik durch die Mechaniken, die ebenfalls im OCTALYSIS-Rahmenwerk in Form der einzelnen Spieltechniken enthalten sind. Sie erzeugen ein gewünschtes Spielverhalten z. B. in mehreren Runden oder führen die Spielenden zu verschiedenen Handlungen durch Chancen, Herausforderungen in Kampfsituationen gegen imaginäre Gegner, Belohnungen aufgrund von Erfolgen, Feedback, Trans-, Tausch- und Sammelaktionen von virtuellen Gütern und Zusammenarbeit mit anderen Beteiligten oder sogar Avataren. Die Resultate der Handlungen drücken sich dann z. B. in Abzeichen, Inhaltsfreischaltungen, Platzierungen auf Ranglisten, erreichten Levels und Punkten aus.[117]

Um möglichst alle psychologischen Grundbedürfnisse der Menschen beim Einsatz von Gamification zu berücksichtigen, wird die Kombination mehrerer Spielelemente

Copyright

empfohlen, auch wenn manche Spielelemente mehrere Grundbedürfnisse gleichzeitig ansprechen (siehe dazu Tabelle 6 auf der nächsten Seite). Beachtet werden muss außerdem, dass sich manche Spielelemente gegenseitig beeinflussen. Beispielsweise können Ranglisten sozialen Druck auf einzelne Spielende ausüben, welche dann bei subjektiv empfundenem schlechtem Wissensstand an Motivation verlieren. Die Bildung von Teams wirkt diesem Empfinden des persönlichen Scheiterns entgegen, indem dieses dann als Gruppenscheitern gewertet wird und oft zur Durchführung eines neuen Versuches motiviert. Game-Design- bzw. Spielelemente sollten angepasst an die jeweilige Situation in der Zielgruppe eingesetzt werden. Es gibt Elemente, die gezielt die Motivation ansprechen (z. B. Kollektionen) und es gibt Elemente, welche zu einer längeren Beschäftigung mit dem Lerninhalt führen (z. B. Freischaltungen von Inhalten). Der Einsatz von Gamification führt zu einer Intensivierung des Lernprozesses, weil die Lernenden aktiviert und zum Experimentieren motiviert werden und der damit verbundene Wissenserwerb bewusst erfolgt. Dieser bildet bei den Lernenden eine Problemlösungskompetenz aus und steigert die Lernmotivation.[107]

Copyright

Tabelle 6: Einordnung der Game-Design-Elemente nach Art und psychologischem Bedürfnis; Quelle: eigene Darstellung in Anlehnung an: https://www.mebis.bayern.de/infoportal/mediendidaktik/methoden/was-ist-gamification/ und [107]

psychologisches Bedürfnis	Game-Design-Element	Art von Gamification
Kompetenzerleben	Punkte	Belohnung
	Bestenliste	Status
	Auszeichnungen (Badges)	Belohnung
	Leistungsanzeige	Status
	Levelsystem	Status
	Quests (Missionen, Aufgaben)	Selbstbestimmung
	Kollektionen	Belohnung
	virtuelle Güter	Belohnung
	Freischaltung von Inhalten	Belohnung
	Rangliste	Status
	Privilegien	Status
	Fortschrittsanzeige	Status
	Feedback	Status
Autonomie	Profilgestaltung	Selbstbestimmung
	Avatare	Status
	freie Gestaltung der Aktivitäten (Wahl)	Selbstbestimmung
	Auszeichnungen (Badges)	Belohnung
	bedeutsame Stories	Identifikation
	Quests	Selbstbestimmung
	Überraschungen	Selbstbestimmung
	Wettkämpfe	Selbstbestimmung
	individuelle Neugierde und Fantasie	Identifikation
	Soundeffekte	Selbstbestimmung
	Visualisierung (Zeigen von...)	Selbstbestimmung
	Hierarchisierung von Aktivitäts-Möglichkeiten	Selbstbestimmung
soziale Zugehörigkeit	Teams, Kooperationen	Identifikation
	Team-Events	Belohnung
	Bestenliste	Status
	Auszeichnungen (Badges)	Belohnung
	Netzwerkfunktionen (Kommentare, Likes)	Selbstbestimmung
	Epic Meaning	Identifikation
	virtuelle Güter	Belohnung
	Freischaltung von Inhalten	Belohnung

Copyright

Gamification ist eine Kombination aus Game Design, Spiele-Dynamiken, Motivationspsychologie, Verhaltensökonomie, UX (User Experience) / UI (User Interface), Neurobiologie, Technologieplattformen und Geschäftssystemen, die einen ROI erzielen. Aus dem Bereich von UX/UI lassen sich für Gamification die Leichtigkeit des Ausführens einer Aktion und die Erzeugung des Flows bei der Benutzung einer Anwendung ableiten.

7.7 Game-Design

Gamification ist vielseitig und wird auch in digitalen Lernanwendungen eingesetzt. Diese Anwendungen beinhalten drei pädagogische Ebenen. Im Präsentationsraum, auch User-Interface genannt, werden die verschiedenen Inhalte angeboten und grafisch repräsentiert. Im Ereignisraum interagieren die Benutzenden mit der Software. Durch die mögliche Vernetzung mit anderen Spielenden hat dieser zunehmend auch eine soziale Komponente. Die dritte Ebene ist der Bedeutungsraum, in welchem die Nutzenden ihre Erfahrungen anwenden können bzw. in welchem Interaktionen ermöglicht oder verhindert werden durch den verwendeten Softwarecode, die gespeicherten Inhalte, die relationalen Verknüpfungen und die Interaktions-Skripte. Um eine individuelle Entwicklung der Nutzenden zu gewährleisten und gleichzeitig eine Überforderung zu vermeiden, ist bei der Gestaltung die Balance zwischen Restriktion und Komplexität wichtig. Für die Bindung und Identifikation der Spielenden mit dem Spiel dienen eine ausgeprägte Interaktivität, strukturelle Gestaltungsmittel im dramaturgischen oder audiovisuellen Bereich sowie die vier Freiheiten des Spiels, der Parodie und die damit verbundene Folgenlosigkeit in der digitalen Welt.[118]

Zu den Freiheiten des Spiels gehören die Freiheit zu Scheitern ohne dafür eine Bestrafung zu erfahren. Das Scheitern ermöglicht das Auffinden neuer Wege und unterstützt damit den Lernprozess. Eine weitere Freiheit ist die des Experimentierens. Die Spielenden können probieren, was funktioniert, was nicht funktioniert oder welche Alternativen existieren. Die Freiheit des Hineinschlüpfens in fremde Rollen im Spiel führt zu Perspektivwechseln, die anfangs nicht vorstellbare Ansichten ermöglichen. Das wiederum bereichert den individuellen Erfahrungsschatz und fördert das Verstehen von Zusammenhängen. Die vierte Freiheit im Spiel ist die Freiheit, selbst entscheiden zu können, welche Anstrengung und welcher Aufwand in die Zielerreichung gesteckt werden. Unterstützt durch Spielelemente ist eine Selbstreflexion zum eigenen Wissensstand möglich und damit eine Einschätzung der Fähigkeiten zur Lösung der Aufgaben. Die Spielenden haben die Chance, das Spiel zu unterbrechen, neue Fähigkeiten zu erlernen und dann die Aufgabe mit einer guten Leistung abzuschließen.[119] Vom Spiel abgeleitet gibt es ebenfalls Grundsätze, die auch beim Einsatz von Gamification beachtet werden sollten. Zu jenen gehören die Informationstransparenz, das Regelwerk,

Copyright

die Entscheidungsfreiheit, die Herausforderung und das Echtzeit-Feedback. Wenn die Anwendung alle für das Spiel relevanten Informationen zur Verfügung stellt, um in diesem voranzukommen, dann spricht man von Informationstransparenz. Das Regelwerk befähigt die Spielenden zum sicheren und selbstbewussten Handeln im vorgegebenen Rahmen. Wenn die Spielenden noch selbst entscheiden können, was sie wann und wie tun, haben sie die Entscheidungsfreiheit, die sie von einem Spiel trotz aller Regeln erwarten. Die stärkste Regel ist dabei oft die Verpflichtung, die sie sich selbst auferlegen. Diese Verpflichtung kann die Bewältigung einer im Spiel gestellten Herausforderung sein. Stimmen dabei die eigenen Fähigkeiten mit den notwendigen Fähigkeiten überein, findet die Herausforderung auf einem angemessenen Niveau statt. Auch das ist ein Grundsatz für einen gelungenen Einsatz von Gamification. Wenn im Spiel ein Feedback in kürzester Zeit gegeben und den Spielenden Chancen eingeräumt werden, sich zu verbessern, ist auch der letzte Grundsatz erfüllt. Feedback ist dabei ein entscheidendes Element, um die Selbstreflexion der Spielenden zu unterstützen.[120]

Weitere Elemente, die eine Selbstreflexion ermöglichen, sind z. B. Lernhilfen, in Spielen implementierte Ironie, verschiedene Informationsebenen auf dem Bildschirm mit parallelen Angaben zum Spiel und zu den Spielenden selbst sowie absichtlich durch bestimmte Aktionen hervorgerufene irrationale Szenen im Spiel. Diese Elemente erzeugen eine gewisse Distanz zum Spiel, unterbrechen es aber nicht.[118]

Der Einsatz der Elemente beeinflusst somit das sogenannte User Interface (UI). Das UI ist die grafische Oberfläche einer Anwendung. Bei ihrem Design werden weitere Festlegungen zum Aussehen und zur Verwendung von Such- oder Scroll-Funktionen getroffen. Ziel ist, die Aufmerksamkeit der Benutzenden möglichst lange an die Szenerie zu binden.

Es geht bei UI nicht nur um die ansprechende visuelle Gestaltung, sondern auch um die Übermittlung einer Botschaft und um die effektive und effiziente Interaktion der Benutzenden mit der Anwendung. Die Handhabung muss vor allem intuitiv sein, ohne dass ihre Benutzenden groß über die Funktionsweise nachdenken. Hinter dem User Interface befindet sich die User Experience (UX), das Erlebnis vor, nach und während

Copyright

der Nutzung. Damit sind z. B. ein bestimmter Ton oder eine bestimmte Länge eines Tons gemeint. Mit der UX soll vorrangig der Nutzungskontext der Menschen befriedigt und ein einheitlicher Auftritt und Kommunikationsstil eines Produkts ermöglicht werden.[121]

Für die unterschiedlichen Gruppen von Nutzenden sind in der Literatur Empfehlungen zu finden, welche die Wahrscheinlichkeit einer nachhaltigen Verwendung des entwickelten Spiels erhöhen. Dazu gehören bspw. unterschiedliche Eingabeoberflächen und -geräte zur Spielsteuerung, Tastenkombinationen zur Abkürzung von Klickfolgen, Möglichkeiten zur Individualisierung des Spiels, verständliche Rückmeldungen, erreichbare Ziele, messbare Ergebnisse, Transparenz, Speicherbarkeit von Zwischenständen sowie Vernetzungsmechanismen. Das Bild 42 zeigt Merkmale guter Spiele mit aktivierenden Spielelementen. Besonders hervorzuheben sind dabei die Merkmale Marktplatz und Echtzeitkommunikation. Durch den Erwerb virtueller Güter und die Möglichkeit des Tausches auf einem virtuellen Marktplatz wird die Vernetzung gefördert sowie die Einschätzung der Wertigkeit der Güter. Die Echtzeitkommunikation erzeugt bei gleichen Bedingungen und eindeutigen klaren Regeln für alle Teilnehmenden eine transparente Bereitstellung von Informationen. Fairness und Transparenz führen zu Vertrauen, welches einen hohen Stellenwert für die Spielenden hat. Besteht das Vertrauen nicht mehr, wenden sich die Spielenden in aller Regel vom Spiel ab.[122]

Bild 42: Merkmale für ein erfolgreiches Spiel; Quelle: [122]

Beim Game-Design muss die Unterschiedlichkeit der Personen innerhalb der Zielgruppe berücksichtigt werden, da aufgrund der verschiedenen Persönlichkeitstypen auch

verschiedene Reaktionen auf Gamification erfolgen. Diese Unterscheidung kann über die Persönlichkeits- oder auch über sogenannte Spielertypen geschehen. Einfacher ist die Einteilung nach den Spielertypen, die im nächsten Abschnitt näher beschrieben werden.[123] Das Spielsystem mit seinen Eigenschaften sollte die Triggerpunkte treffen, die Begeisterung und Engagement bei den Teilnehmenden hervorrufen.

Zwar sind nicht alle Menschen gleichermaßen auch Spielende, aber dennoch sind sie über bestimmte Spielelemente ansprechbar. Je nach Stärke der Ausprägung des individuellen Typs wirken bestimmten Spielelemente besser. Die Persönlichkeitstypen sollten trotz allem aber nicht unbeachtet gelassen und in größtmögliche Übereinstimmung gebracht werden. Mit dem Octalysis-Framework werden speziell die psychologischen Antriebsfaktoren genannt, die ein Handeln hervorrufen und die bei der Klassifizierung der Persönlichkeitstypen eine Rolle spielen. Ordnet man nun noch die Spielertypen zu, erhält man zusätzlich die spielerischen Profile[124].

7.8 Spielertypen

Der bis heute gültige Standard für die Klassifizierung von Spielenden in sogenannte Spielertypen ist die Taxonomie von Bartle[125]. Sie hilft auch heutigen Spieleentwickelnden bei der Abstimmung ihrer Spiele auf die spezifische Zielgruppe. Zwar finden sich die Spielenden in der Regel in allen Spielertypen gemäß dem Bild 43 wieder, jedoch überwiegt ein spezifischer Typ. Wenn Entwickelnde versuchen, ein Spiel für alle gleichermaßen zu gestalten, dann wird es keinem der Spielenden gut gefallen. Genauso verschieden wie die Typen selbst, sind auch die Treiber im Spiel, die sie motivieren und beeinflussen. Für „Killertypen“ zählen der Wettbewerb, das Gewinnen und der Test der eigenen Fähigkeiten – auch gegen andere Spielende. „Achievertypen“ benötigen Punkte, Abzeichen, Level, Trophäen und persönliche Bestleistungen. Sie gelten als perfekte Gamification-Nutzende. Das Suchen, das Erkunden, das Entdecken und das „sich Zeit für das Spiel nehmen“, begeistert vor allem die „Explorertypen“. Sie freuen sich besonders über die Freischaltung kleiner Nischen in Spielen und „Easter Eggs“. Freundschaften, Kommunikation, Kooperation, Miteinander und Gemeinschaft sind für die „Socializertypen“ wichtig. Im Spiel sollte es für sie Freundschaftslisten, Chat-Funktionen und Newsfeeds geben.[126]

Copyright

Bild 43: Spielertypen nach Bartle; Quelle: [124]

In der Tabelle 7 werden die verschiedenen Spielertypen zu den Kernantrieben des Octalysis-Frameworks beispielhaft zugeordnet. Erkennbar ist, dass die Spielelemente abhängig vom primären Spielertyp und Persönlichkeitstyp eingesetzt werden sollten, um die gewünschte Aktivierung der in der Zielgruppe überwiegend vertretenen Spielertypen zu erreichen. Dazu kann zuvor die Zielgruppe mithilfe eines Fragebogens auf ihre Bartle-Spielertypen hin analysiert werden (siehe Anlage 1 im Anhang).

Wenn es gelingt zusätzlich noch die in der Zielgruppe existierenden verschiedenen Lerntypen festzustellen, können das Game-Design und die Wissensvermittlung noch optimiert werden. Zwischen den Spieler-, Persönlichkeits- und Lerntypen gibt es zwar statistisch einige Überdeckungen, aber die Befunde für den effektiven Einsatz von Gamification in einer Lernplattform reichen leider nicht aus.[23] Aus diesem Grund wurde deshalb in der Tabelle 7 auf die Zuordnung der Lerntypen verzichtet.

Tabelle 7: Zuordnung der verschiedenen Typen zum Octalysis-Framework; Quelle: eigene Darstellung

Kernantriebe (Motivationen)	Spielelemente	Persönlichkeitstypen	Spielertypen
1 - epische Bedeutung	Storytelling, Elitismus, Heldentum, Anfängerglück, Gratisgeschenke	alle Persönlichkeitstypen	alle Spielertypen
2 - Entwicklung/Leistung	Fortschritt, Erfolgssymbole, Statuspunkte, Ranglistenplätze, Rockstar	extravertiert, gewissenhaft, neurotisch	Achievers, Killers
3 - Kreativität/Feedback	Superkräfte, Freischaltungen, Wahlmöglichkeiten	extravertiert, gewissenhaft, offen	Killers, Achievers, Explorers
4 - Eigentum/Besitz	Sammelfiguren, Austauschpunkte, Vertrautheit, Vorlieben/Inhalte	gewissenhaft, extravertiert	Achievers, Killers
5 - sozialer Einfluss	Mentoring, Trophäen, Angeber-Knöpfe, Gruppenaufgabe, Anker, Anstupser	extravertiert, verträglich	Killers, Socializers
6 - Knappheit/Ungeduld	Spiel/Realität, Limitierungen, Obergrenze, Termindynamik, Folterpause	extravertiert	Killers
7 - Unvorhersehbarkeit/Neugierde	Freischaltung, Mistery Box, Glowing Choice, Easter Eggs, rollende Belohnung/Lotterie	offen	Explorers
8 - Verlust/Vermeidung	rechtmäßiges Erbe, schwindende Gelegenheit, Status Quo, FOMO, versunkene Kosten	gewissenhaft, extravertiert	Achievers, Killers

7.9 Spiel-Genres

In der Literatur existiert noch keine allgemein gültige Definition des Begriffs Spielgenre. Sie werden unterschiedlich je nach Betrachtungsweise kategorisiert und auch vermischt mit Untergenres. Wenn ein Genre genannt wird, liefert es trotz allem einen Hinweis zur

zu erwartenden Spielmechanik und zu den möglichen Anforderungen an die Spielenden.[123]

Aus der Fokussierung auf die Nutzenden mit ihren persönlichen Eigenschaften und psychologischen Hintergründen werden verschiedene Spiel-Genres gebildet.[124] Möchte man das Erlernen wichtiger Sachverhalte positiv beeinflussen, müssen die zum Lernen und Spielen geeigneten Spielmerkmale identifiziert und das Genre festgelegt werden.[127] Auch die Vermischung verschiedener Elemente von Spiel-Genres in einem Lernpaket, welches dann nicht mehr als Lernspiel in dem Sinne wahrgenommen wird, kann äußerst erfolgreich sein.[128]

Für die Bestimmung des Spielgenre lässt sich ein Computerspiel vereinfacht auf eine der vier Komponenten Strategie, Geschicklichkeit, Simulation und Rolle aufteilen. Damit erhält man bei der Entwicklung im Rahmen eines Serious Game eine Orientierungshilfe für die Genre-Auswahl.[123] Da es sich bei Gamification aber nicht um ein komplettes Spiel handelt und der Fokus auf den Spielelementen liegt, die in das didaktische Konzept eingearbeitet sind, tritt ein Spielgenre höchstens in Teilen auf, um eine spielähnliche Erfahrung zu bieten.

Mit Spielen können verschiedene Kompetenzen geschult werden. Bewegungs- und Sportspiele schulen motorische und sensorische Fähigkeiten. Kognitive Kompetenzen werden mit Denk- und Strategiespielen, Planspielen, Management- und Konstruktionsspielen, Adventure- und Actionspielen gefördert. Rollenspiele dienen zur Schulung sozialer Kompetenzen.[123]

Für Gamification im Bereich der Sensibilisierung für Informationssicherheit bieten sich vor allem Genres an, welche die kognitiven Kompetenzen fördern. In der Tabelle 8 sind die Genres aufgeführt, die das Bundesministerium für Digitales und Verkehr unterscheidet. Farblich gekennzeichnet sind dort die Genres, die kognitive Kompetenzen fördern.

Copyright

Tabelle 8: Spielgenres; Quelle: [129]

Computerspiel-Sachgebiet	
Abenteuer	Quiz
Brettspiel	Rennspiel
Escape-/Fluchtspiel	Rogue-Like
Gedächtnisspiel	Rollenspiel
Geschicklichkeitsspiel	Rätselspiel
Horror	Schleichspiel
Interaktiver Film	Shooter
Kartenspiel	Simulation
Lernspiel	Sportspiel
MOBA (Multiplayer Online Battle Arena)	Strategiespiel
Musikspiel	Überlebensspiel
Plattformer	-

Bei der Auswahl des Spiel-Genres ist zu beachten, dass es Computerspiele gibt, bei denen die Lerninhalte durch das Game-Design schon mit seinen Regeln, Geschichten und Wettbewerben integriert sind wie bei Simulations-, Rollen-, Action- und Abenteuerspielen. Es gibt aber auch Formen wie Puzzle, Quiz und traditionelle Brettspiele, die mit ihren Lerninhalten auf dem Spiel aufsetzen und keinen Effekt auf das Game-Design haben.[127]

Für die Entwicklung eines Verständnisses für Funktionsprinzipien bieten sich Simulationsspiele an. Wenn es um das Treffen von strategischen Entscheidungen geht, können Rollenspiele verwendet werden. Umfassen die Lernaktivitäten das entdeckende Lernen, welches aus dem Beobachten, der Problemidentifikation und dem Üben und Lernen aus Rückmeldungen besteht, dann bieten sich Abenteuerspiele an. Für Fehleranalysen in komplexen Strukturen können Puzzlespiele den Lernprozess unterstützen. Für Entscheidungen, die auf ethischer Ebene getroffen werden müssen wie beim Social Engineering, helfen Lerntechniken, die durch das gezielte Stellen von Fragen spezifische Situationen durchspielen. Für diesen Zweck können Quizze zur Lernförderung verwendet werden. Wenn die Lernaktivität das Auswendiglernen von Fakten wie Sicherheitsrichtlinien umfasst, unterstützen Wettbewerbe durch die Nutzung von Karten und traditionellen Brettspielen das Üben und Feedback-Lernen.[127]

Copyright

8. Konzepterarbeitung

Um einen Überblick über die Kriterien zu bekommen, die bei der Erarbeitung eines Schulungskonzepts zu beachten sind und welche Spielelemente in der Realität bei Spielen mit ernsthaftem Hintergrund besonders gut wirken, wurden Experten-Befragungen durchgeführt. Eine Analyse der vorhandenen Hochschulpersonalstruktur liefert die spezifischen Zielgruppen, welche die Ausgangsbasis für die Entwicklung des Konzepts unter Verwendung von Gamification bilden.

8.1 Experten-Interviews

Im Anhang dieser Master-Thesis befinden sich in der Anlage 2 die ausführlichen Ergebnisse dieser Befragung von sechs Experten aus der Security-Awareness-Branche. Sie alle sind leitende Angestellte in Unternehmen, die Produkte bzw. Dienstleistungen im Bereich der Security-Awareness anbieten. Allen gemein ist die Verwendung von Spielelementen in ihren Produkten. Zwei der Befragten bieten online-Plattformen an, worüber Unternehmen ihre Mitarbeiter schulen können. Zwei weitere Befragte sind im Bereich Serious Game tätig und wiederum zwei Befragte bieten Dienstleistungen vor allem in der Erstellung und Schulung von analogen Spielvariationen mit Bezug zur Informationssicherheit an. Die Befragungen fanden vom 21.02.2022 bis zum 06.06.2022 anhand einer vorbereiteten Fragenliste statt, die per E-Mail ausgetauscht wurde. Die wichtigsten Erkenntnisse werden in der nachfolgenden Zusammenfassung dargestellt.

Wichtig für eine gute Awareness ist zusätzlich zu digitalen Formaten das Zwischenmenschliche und Analoge, um eine Verknüpfung zwischen der Theorie, dem Erleben durch die menschlichen Sinne und der kognitiven Verarbeitung im Gehirn herzustellen. Die Verankerung im Gehirn führt zu einer automatisierten und standardisierten Handlungsabfolge, weil sie nur noch aus dem Gedächtnis abgerufen und nicht lange darüber nachgedacht wird. In vielen Führungsebenen wird das Spielen jedoch immer noch als Zeitverschwendung angesehen, befindet sich aber mit zunehmendem Erfolg von Gamification im Wandel. Folgt man wissenschaftlichen Studien, ist das spielerische Lernen seit jeher tief in den Menschen verwurzelt und sehr wirkungsvoll, was auch an Hochschulen im Rahmen ihrer pädagogischen Forschung bekannt ist.

Copyright

Deshalb hat der Einsatz von Gamification oder Serious Games in den letzten Jahren an Hochschulen auch zugenommen. Die Lernenden, auch die Führungskräfte, müssen keine Experten auf dem Gebiet der Informationssicherheit sein, haben aber über Gamification-Anwendungen die Möglichkeit, die Folgen ihrer Handlungen in einer Testumgebung zu erleben, Fehler zu machen, Risiken zu erkennen und sich somit auf mögliche Situationen vorzubereiten. Zwar ist das Interesse an der Darstellung aller denkbaren Szenarien und darauf anzuwendender Sicherheitsregeln und Verhaltensweisen sehr verschieden, aber die Vorbereitung auf solche Situationen ist essentiell für die Umsetzung in der Realität. Genauso wie im Spielen werden auch in der Sicherheit Regeln benötigt, um eine korrekte Funktionsweise zu gewährleisten. Unkreatives und stupides Lehren und Lernen von Regeln ist nicht der richtige Weg, Awareness bei Mitarbeitern zu implementieren. Regelmäßiges Training, die Schaffung einer intrinsischen Motivation zur selbstgesteuerten Vertiefung eines Sachverhalts und damit Bildung von Awareness ist kein bloßer Lerninhalt, sondern eine nachhaltige Verhaltensänderung, bei der das notwendige Fachwissen dafür über konventionelle Lernmethoden kommt. Der Wissensaufbau kann auch über digitale Lernmodule erfolgen, um eine breite Wissensbasis insgesamt zu schaffen. In der gamifizierten oder simulierten Variante kann dann über das Durchspielen bestimmter Alternativen das Wissen auf die Probe gestellt und somit Erfahrung vor dem Ernstfall gesammelt werden. Vorhandene Studien zeigen, dass die Lerneffizienz von Gamification-Anwendungen im Vergleich zu herkömmlichem E-Learning um ein Vielfaches höher ist, weil es motivierender und langfristig einprägsamer (also nachhaltiger) ist. Wichtig dabei ist, dass dabei auch die soziale Ebene des Menschen angesprochen wird. Dies ist mit gutem, authentischem und spannendem Storytelling aus der Arbeits- und Alltagswelt der Lernenden möglich, welches einen emotionalen Anker setzt und für eine intensivere und kontinuierliche Auseinandersetzung jedes einzelnen Menschen mit der Thematik sorgt. Die andauernde Beschäftigung z. B. mit dem Thema Phishing führt zu einer signifikanten Verbesserung der Klickrate, d. h. es klicken nicht mehr so viele Personen auf einen maliziösen Phishing-Link. Eine für den langfristigen Erfolg essentielle Kontinuität im Lernen erreicht man neben der guten Idee für eine Story mit einem durchgängigen Handlungsstrang, dem die Spielenden folgen möchten und mit einem Charakter, mit dem man sich möglichst identifizieren kann – angeboten in einem für die Lernenden zugänglichen Medienformat. Je besser die

Copyright

Lernenden sich in die Spielsituation hineinversetzen können, desto höher ist die Immersion. Dazu müssen die auszubildenden Personen bei der Spielentwicklung im Mittelpunkt stehen. Wird dies beachtet, kann es zu einem vollkommenen Eintauchen in die Spiele- bzw. Lernwelt kommen. Zusammen mit dieser Immersion führt auch die Kollaboration mit anderen Spielenden dazu, dass eine höhere Motivation entsteht. In der Folge wird dadurch ein besseres Lernergebnis bzw. eine optimale Problemlösung aufgrund des Wissensaustauschs untereinander und der Schwarmintelligenz erzielt. Neben Intellekt, Kognition und Rationalität ist die Intuition, die emotionale Intelligenz gefragt. Sie kann in einem erweiterten und auch alternativen Rahmen in Form von Gamification erlernt werden. Wird der Inhalt des Trainings auf kognitive und emotionale Art vermittelt, funktioniert die Immersion und Involvierung in das Spielthema bei jedem Menschen. Die Erfolgsrate von Gamification kann im Steigerungsgrad der Motivation gemessen werden. Wenn Spielelemente verwendet werden, schließen deutlich mehr Menschen ein Training ab und das hat Auswirkungen auf die gesamte Sicherheitskultur in der Organisation. Bei der Produktion von Gamification-Anwendungen ist aber auch darauf zu achten, welche Art von Game-Design überhaupt wirksam ist und was diese kostet. Schnell kann die Entwicklung eines individuellen Spiels, dass möglichst viele Zielgruppen in einer Organisation anspricht, sehr kostspielig werden. Bekanntlich ist der Hochschulsektor stark abhängig von Drittmitteln und in der Vergabe von Aufträgen an das Wirtschaftlichkeitsgebot und Gesetzmäßigkeiten für die öffentliche Ausschreibung von Aufträgen gebunden, so dass oft Zwänge bestehen, die zur Verfügung stehenden Mittel nach Prioritäten und möglicherweise nicht für die Schaffung von Awareness einzusetzen. Aus diesen Gründen wird oft kein ausreichendes Budget für Projekte dieser Art zur Verfügung gestellt. Um ein Projekt dennoch umzusetzen, müssen häufig Abstriche bei Komfort und Qualität gemacht werden. Insgesamt ist Gamification durch ihre systemischen Bezüge ein erweiterter Rahmen der klassischen Lerntheorie, die aber als Lernmethode noch nicht anerkannt ist. Um ein sicheres Verhalten auch in der Praxis zu erzielen, kann Gamification den emotionalen Anker für die Erinnerung an das gewünschte Verhalten setzen. Da das Prinzip des spielerischen Lernens schon seit der Kindheit tief in den Menschen verwurzelt ist, ist auch die Speicherung von solchen spielerischen Ankern im Gehirn einfacher, weil es von Kindesbeinen an praktiziert wird.

Copyright

Insbesondere Hochschulen können Gamification im E-Learning nutzen und für den Ernstfall spielerisch üben.[20]

8.2 Umfrage zum Einsatz von Gamification an deutschen Hochschulen

In der Anlage 3 befinden sich Auszüge aus der Auswertung zu einer im Rahmen dieser Master-Thesis im Zeitraum vom 31.05.-30.06.2022 mit dem Softwaretool „limesurvey“ durchgeführten Umfrage im ZKI-Arbeitskreis. Dieser zählt 217 Mitglieder in Form von Hochschulen und Großforschungseinrichtungen. Die Umfrage enthielt insgesamt 31 Fragen, aufgeteilt in 3 Fragenblöcke (allgemeine Angaben, Fragen zur Informationssicherheit, Schulungen zur Informationssicherheit) und steht bei Bedarf auf Abruf zur Verfügung. An der Umfrage haben 86 Einrichtungen teilgenommen. Das entspricht einer Teilnahmequote von ca. 40 %. Alle Fragen vollständig beantwortet haben jedoch nur 23 Teilnehmende. Von diesen haben knapp 48 % schon einmal einen ernsten Informationssicherheitsvorfall gehabt. Etwa 70 % davon führen Sensibilisierungsmaßnahmen für Informationssicherheit durch. 56,52 % davon verwenden bei ihren Schulungen Gamification-Ansätze. Für die Sensibilisierung werden vor allem Lernmanagementsysteme, gekaufte Selbstlernplattformen oder gekaufte online-Kurse eingesetzt (z. B. moodle, ILIAS, BayLern, ARS Nova, SoSafe). 34,78 % benutzen in ihrem Lernmanagementsystem Spielelemente. Die anderen 65,22 % bedienen sich der klassischen Vergabe von Noten, der Durchführung von Prüfungen und Tests zur Motivationssteigerung. Hauptsächlich werden Quizze (z. B. mit dem Tool „kahoot“), Abzeichen, Feedback, Punkte, Narrative und Herausforderungen verwendet. Individualisierte Avatare werden gar nicht eingesetzt. Etwa 17 % bieten auch Escape Rooms bzw. Escape Games zur Sensibilisierung an. Nur 8,70 % bedienen sich interaktiver Gamification-Apps wie z. B. „Actionbound“. Bei der Frage nach der Reihenfolge der Durchführung der Sensibilisierungsmaßnahmen steht an erster Stelle die Hochschulleitung, gefolgt von der IT, der Verwaltung, den wissenschaftlich Beschäftigten, dem mittleren Management, der Professorenschaft und den Studierenden. Bei der Frage nach der Priorisierung definierter Kompetenzen, die zur Absicherung von Prozessen in schützenswerten Hochschulbereichen notwendig sind, legen die Befragten die in der Tabelle 9 dargestellte Rangfolge fest.[130]

Copyright

Tabelle 9: Wichtigste Kompetenzen für schützenswerte Hochschulbereiche; Quelle: eigene Darstellung

Kompetenzen / Rangfolge	Fachkompetenzen (Top 5)	Sozialkompetenzen (Top 5)	Selbstkompetenzen (Top 5)	Methodenkompetenzen (Top 5)
1	technisches Verständnis für die Anwendungen	Diskretion/Integrität	Lernbereitschaft	analytisches/vernetztes Denken
2	Datenschutz	Zuverlässigkeit/Konsequenz	Eigenverantwortung	Bewertungsvermögen
3	physische Sicherheit (Zugang/Zutritt)	Teamfähigkeit/Kooperation	Verantwortungsbewusstsein	Selbständigkeit
4	Angriffsarten/Bedrohungen	Kunden-/Serviceorientierung	Veränderungsbereitschaft	Projektmanagement
5	Malwareschutz/mobiles Arbeiten/Verhalten in soz.	Schulungskompetenz/ Kommunikation	Genauigkeit	Organisationsgeschick

An oberster Stelle stehen das technische Verständnis, die Diskretion, die Lernbereitschaft und das analytische Denken. Als Fachkompetenzen werden die Kompetenzen verstanden, die eine Person zur sicheren Arbeitsbewältigung in ihrem Fachbereich benötigt. Mit Sozialkompetenz ist die Fähigkeit zur Durchsetzung von Zielen und Plänen unter Berücksichtigung sozialer Aspekte gemeint. Die Selbstkompetenz einer Person spiegelt die Einstellung dieser Person zur Abarbeitung der von ihr verlangten Aufgaben wieder. Die Selbstkompetenz hängt somit stark mit der Motivation und dem Verhalten zusammen, die positiv beeinflusst werden muss, um zu einem sicheren Verhalten zu kommen, das aus dem inneren Antrieb der Person resultiert. Unter der Methodenkompetenz wird die Fähigkeit verstanden, selbständig die erlernten Methoden auch auf andere komplexe Sachverhalte zu übertragen und anzuwenden. Hier kommt es mit Bezug auf die Informationssicherheit auf die Selbstwirksamkeitserwartung der betroffenen Person an, die gestärkt werden muss.[131]

8.3 Entwicklung einer Anwendung mit Spielelementen

Die Frage nach den Kompetenzen ist insofern interessant, als dass man damit erkennt, welche fachlichen Themen die zu entwickelnde Gamification-Anwendung beinhalten muss bzw. welche anderen Kompetenzen außerdem getestet werden sollten. Jetzt fehlen für die Berücksichtigung des didaktischen Designs der Anwendung noch die Lernziele, die Ablauforganisation und die Rahmenbedingungen.[132] Danach erfolgt das Game-Design anhand der im Bild 44 dargestellten Vorgehensweise. Dazu wird das hauptsächliche Spielziel festgelegt, die zu verwendenden Komponenten (Story, Quests etc.), die Spielregeln, die Kerndynamik, weitere Spielmechaniken, die Beschreibung des Problems und des Raumes, in dem das Spiel stattfindet.

Copyright

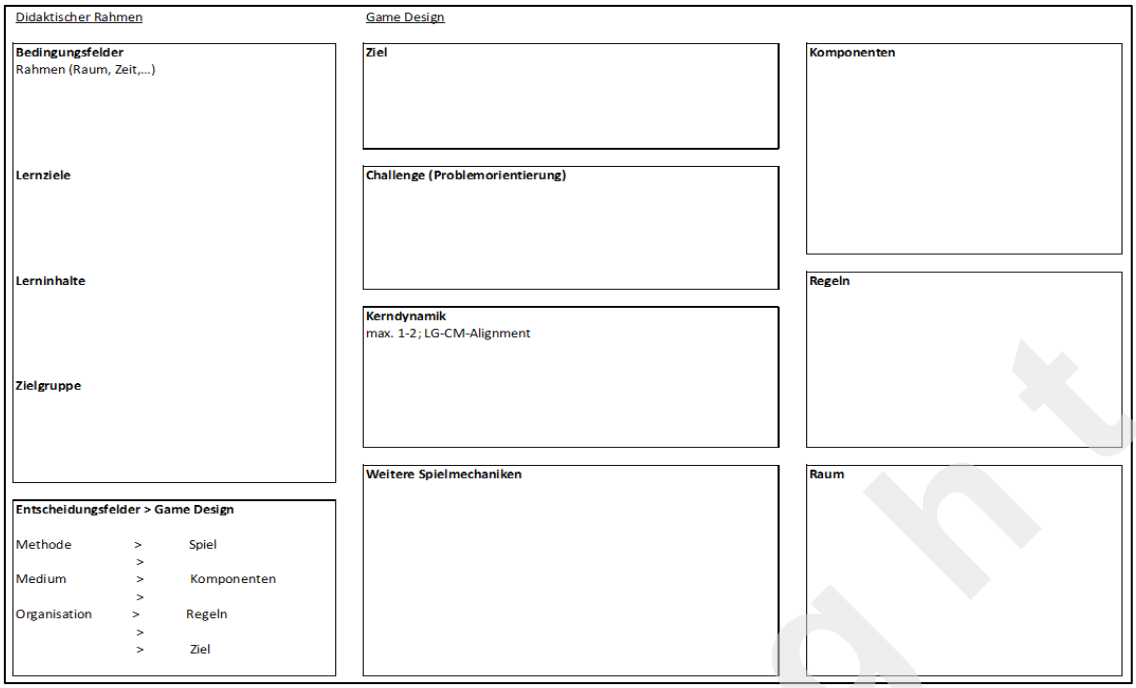


Bild 44: Vorgehensweise zur Entwicklung der Anwendung; Quelle: [133], leicht gekürzt

Dabei ist darauf zu achten, dass die Lernziele der Zielgruppe und Spielelemente zueinander passen und kein „Chocolate-Covered-Broccoli“ daraus wird – ein erfolgloser Versuch, wichtige Lerninhalte (Brokkoli) unter beliebigen Spielelementen (Schokolade) zu verstecken. Die Tätigkeiten während des Spiels sollten etwas mit den Lernzielen zu tun haben, damit das Lehrkonzept von den Lernenden nachvollzogen werden kann.[134]

8.3.1 Zielgruppenstruktur an der Hochschule Anhalt

Das ZKI identifiziert für Hochschulen die Zielgruppen Hochschulleitung, Professorenschaft, mittleres Management, wissenschaftlich Beschäftigte, Verwaltungspersonal, IT-Personal und Studierende. Da sich bei der Entwicklung des Schulungskonzepts ausschließlich auf die Hochschulangehörigen konzentriert werden soll, werden die Studierenden aus den nachfolgenden Betrachtungen ausgeschlossen. Für die Bildung von Zielgruppen wurden die 732 Mitarbeitenden an der Hochschule Anhalt über ein sie voneinander abtrennendes Differenzierungsmerkmal in sieben Gruppen aufgeteilt (siehe Anlage 4). Die Merkmale ergeben sich aus den überwiegenden Tätigkeiten der einzelnen Mitarbeitenden. So gibt es „handwerklich“, „sachbearbeitend“, „fachpraktisch“, „prozessübergreifend“, „forschend“, „leitend und/oder lehrend“ sowie „systemverändernd“ tätige Mitarbeitende. Der größte Anteil der Hochschulangehörigen

Copyright

fällt auf die Gruppe der „leitend/lehrend“ tätigen Personen, die zusammen 28,42 % ausmachen (siehe Bild 45). Die kleinste Gruppe mit nur 2,46 % stellen die IT-Beschäftigten, die Systeme mit weitreichenden Befugnissen administrieren.

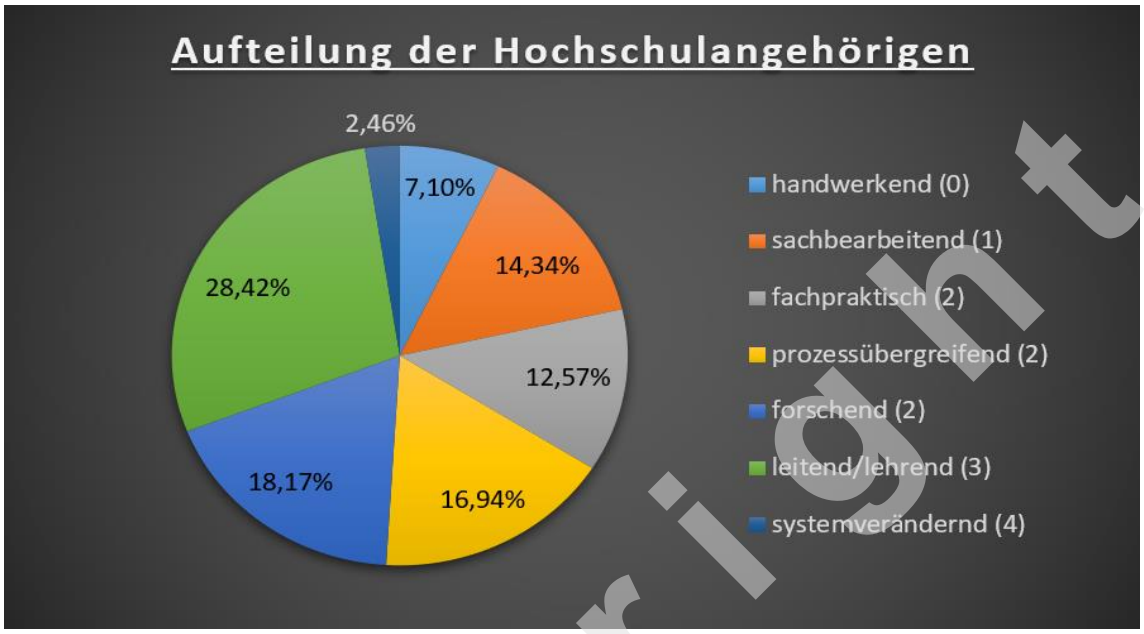


Bild 45: Zielgruppen an der Hochschule Anhalt; Quelle: eigene Darstellung

Festlegung auf eine Zielgruppe

Um eine zielgruppengerechte Gamification-Anwendung zu erarbeiten, erfolgt für die nächsten Ausführungen die Festlegung auf die Zielgruppe der überwiegend sachbearbeitenden Personen. Sie stellt mit 105 Personen die viertgrößte Zielgruppe dar und kann als Vorlage zur Erarbeitung der weiteren Gamification-Anwendungen für das andere an der Hochschule beschäftigte Personal verwendet werden.

Spielertypen in der Zielgruppe

Über einen Bartle-Test, der sich in der Anlage 1 befindet, kann die in der Zielgruppe am stärksten vertretene Spielertypen-Gruppe ermittelt und der Einsatz der Spielelemente und -techniken daran ausgerichtet werden. Aus Zeitgründen muss an dieser Stelle jedoch auf die konkrete Analyse der Zielgruppe verzichtet und durch Annahmen ersetzt werden.

In der Literatur ist dazu aber eine explorative Studie mit 15 Teilnehmenden (Studierende) und eine Vergleichsstudie mit 29 Teilnehmenden zu finden. In beiden Studien treten

Copyright

Explorer und Socializer als die dominanten Spielertypen auf. Danach folgen Achiever und an letzter Stelle die Killer.[23]

Eine andere Studie zu den sogenannten BrainHex-Spielertypen mit 300 Befragten im Alter von 18 bis 60 Jahren und 180 vollständigen Antworten sichert die Annahme ab, dass der Explorer in vielen Studien den dominanten Spielertyp darstellt.[135]

Projiziert man nun die Ergebnisse der Studie anhand der Merkmale der BrainHex-Spielertypen auf die Bartle-Spielertypen erhält man folgende veränderte Statistik:

Tabelle 10: Projektion der BrainHex-Spielertypen auf die Bartle-Spielertypen; Quelle: eigene Darstellung in Anlehnung an [135]

BrainHex-Spielertyp	Merkmale	Auszählung	Bartle-Spielertyp
Seeker	interessiert an Spielmechanismen, neugierig	45,00%	Explorer
Masterminds	strategisch denken, Rätsel lösen		
Survivor	Angstgenuss, Erleichterung nach Anspannung	31,60%	Killer
Daredevil	Jagd, Nervenkitzel		
Conquerer	gegen andere siegen, Herausforderungen lieben		
Achiever	langfristige Leistungen, Fixierung, Herausforderungen	19,40%	Achiever
Socializer	sprechen, helfen, anderen vertrauen	9,40%	Socializer

Aufgrund dieser Festellungen wird sich bei der Auswahl der Spielelemente im Abschnitt 8.3.5 neben der Standard-Triade (Punkte, Badges, Level) auf den Explorer als dominanten Spielertyp fokussiert und durch Elemente ergänzt, die alle Spielertypen anspricht.

Persönlichkeitstypen in der Zielgruppe

In der Zielgruppe der überwiegend sachbearbeitend tätigen Personen sind Auszubildende, Assistentinnen und Assistenten, Dekanassistentinnen und Dekanassistenten, IT-Technikerinnen und IT-Techniker, die keine administrativen Aufgaben haben, Mitarbeitende in der Hochschulbibliothek und im Marketing- und Kommunikationsbereich, Sachbearbeiterinnen und Sachbearbeiter, Studiengangskoordinatorinnen und Studiengangskoordinatoren sowie Verwaltungsmitarbeitende zusammengefasst (siehe Anlage 4). Aufgrund der Vielfältigkeit in der Gruppe wird davon ausgegangen, dass auch alle Big Five-Persönlichkeitstypen in unterschiedlicher Zahl vertreten sind. Um alle

Copyright

Persönlichkeitstypen anzusprechen, muss die zu entwickelnde Gamification-Anwendung Erfahrungen, Erlebnisse, Eindrücke, Aktivitäten und Zwischenmenschliches, Mitgefühl und Kooperation bieten bei notwendiger Genauigkeit, Zielstrebigkeit und Selbstkontrolle. Sie muss eine aufkommende Unzufriedenheit aufgrund von Negativerlebnissen vermeiden und zum Durchhalten motivieren.

Lerntypen in der Zielgruppe

Besondere Aufmerksamkeit beim Lernen und Verstehen neuer Inhalte benötigen rezessiv und angstbestimmt Lernmotivierte. Wie bereits im Abschnitt 7.1 erklärt, haben diese Lerntypen eine niedrige Kompetenzerwartung, ein niedriges Erfolgserleben, keine ausgeprägte Lernstrategie und Schwierigkeiten bei der Verarbeitung negativer Emotionen aufgrund schlechter Lernergebnisse. Da sie sich allein unsicher, aber in der Gruppe motiviert fühlen, sind vor allem Gruppenaufgaben für diese Lerntypen essentiell.

Folgende, weitere Funktionen sollten in der Gamification-Anwendung zur Erhöhung des Selbstvertrauens in die eigenen Kompetenzen und Fähigkeiten und damit zur Erhöhung der Selbstwirksamkeit für diese beiden Lerntypen zunächst in der grundsätzlichen Ausstattung zur Verfügung gestellt werden:

- vordefinierte Lernziele
- schnelle Erfolgserlebnisse
- begrenzter Funktionsumfang
- Quests auf freiwilliger Basis zur Prüfung der Selbstkompetenz
- Gruppenaufgaben
- begleitete Aufgabenlösung

Je nachdem, wie flexibel und anpassbar die Anwendung ist, können diese Funktionen auch in abgewandelter Form für die anderen Lerntypen in einer Erweiterung verwendet werden. Aus vordefinierten Zielen lassen sich evtl. individuelle Lernziele gestalten. Auch eine Funktion zum Wählen des individuellen Schwierigkeitsgrades vor der jeweiligen Aufgabe lässt einen Erfolg als Erfolg empfinden. Eine weitere dynamische Komponente kann die sukzessive Vergrößerung des Funktionsumfangs im Spielverlauf sein. Zum Test der Selbstkompetenz können individuelle Einzel-Quests mit erhöhtem

Copyright

Schwierigkeitsgrad durchgeführt werden. Das Mentoring zu Aufgaben wird nur durch eine bestimmte Funktion aktiviert. Ansonsten ist es ausgeschalten. Da eine hohe Selbstwirksamkeit und damit Selbstvertrauen in die eigenen Fähigkeiten und Kompetenzen zur Schaffung einer Awareness für Informationssicherheit unabdingbar sind, wird sich besonders auf Elemente zur Unterstützung der beiden o. g. Lerntypen konzentriert.

Verfassungen in der Zielgruppe

Die Verfassungen der Zielgruppe der überwiegend sachbearbeitend tätigen Personen wurden bereits in Abschnitt 6.5 ausführlich beschrieben. Insgesamt ist diese Zielgruppe als vorsichtig, lernwillig und hilfsbereit zu beschreiben, die mit konkreten Anweisungen angeleitet und über die selbständige Auswahl einfacher zur Verfügung gestellter Handlungsoptionen eingebunden werden müssen.

8.3.2 Kompetenzen der ausgewählten Zielgruppe

Zur Definition der Schulungsschwerpunkte und Ableitung der sich daraus ergebenden notwendigen Fähigkeiten werden verschiedene Kompetenzstufen gebildet, die gleichzeitig auch zur gegenseitigen Abgrenzung dienen. Insgesamt werden fünf Stufen gebildet, die von Mitarbeitenden, die keine IT-Administrierenden sind, erreicht werden müssen (siehe Tabelle 11). Dabei richtet sich die Einstufung nach dem Arbeitsort, dem Einsatzgebiet und nach der Art der Verrichtung der Arbeit. Die festgelegte Zielgruppe befindet sich in der Kompetenzstufe 1, die bereits Grundkenntnisse im Bereich der Begrifflichkeiten und den Themengebieten Passwort, Datenschutz und Internetsicherheit (inkl. Browsernutzung, E-Mail- und App-Anwendungen) voraussetzt. Zur Abprüfung, ob die notwendigen Kenntnisse auch vorhanden sind, dient ein kleiner Einstiegstest. Um die Grundkenntnisse zu vertiefen und vorhandene Wissenslücken zu schließen, werden häufige Zwischentests durchgeführt. Um ein Mindest-Sicherheitsniveau in einem bestimmten Bereich zu gewährleisten, ist es erforderlich, dass die Mitarbeitenden immer eine Kompetenzstufe höher ausgebildet werden als für ihre Tätigkeit in ihrem Bereich notwendig. Das wäre im Fall der sachbearbeitend tätigen Personen die Stufe 2. In dieser Kompetenzstufe sind keine Wissenslücken in den erweiterten Grundkenntnissen vorhanden. Es werden Inhalte vermittelt, die über dieses Wissen hinausgehen. Durch

Copyright

zyklische Tests wird der erlernte Stoff wiederkehrend abgeprüft und somit im Gedächtnis gespeichert. Analog erfolgt das Vorgehen in den anderen Kompetenzstufen. Die Zielgruppe kann spätestens bei Stufe 1 mit einem Einstiegstest zu den Grundkenntnissen beginnen und muss bis zur Stufe 2 (mittel) die Schulungen absolvieren.

Tabelle 11: Definition der Kompetenzstufen; Quelle: eigene Darstellung

Stufe	Bezeichnung	notwendiger Kenntnisstand	Testung	Niveauabsicherung
0	gering	keine Vorkenntnisse notwendig	erlerntes Wissen in einem begrenzten Kontext beweisen	Mängel durch zusätzliches vermehrtes Üben auch in Form von Workshops beseitigen
1	normal	Grundkenntnisse vorausgesetzt	Wissenslücken in den vertieften Grundkenntnissen durch Schulungstests schließen	üben in häufigen online-Zwischentests
2	mittel	erweiterte Grundkenntnisse	keine Wissenslücken in den Grundkenntnissen; Tests darüber hinaus mit 70 % bestehen	üben in online-Zwischentests
3	hoch	Expertenwissen	keine Wissenslücken in den Grundkenntnissen; Tests darüber hinaus mit 90 % bestehen	Fähigkeit, Wissen in Form der Lehre an andere weiter zu geben, unter Beweis stellen
4	sehr hoch	Spezialwissen	keine Wissenslücken; Tests mit 100 % bestehen und kleineres Spezialwissen abfragen	Training und Mentoring von Hochschulangehörigen, Vorträge vor anderen Admins inkl. detaillierter Schilderung von Sachverhalten der Informationssicherheit

Aus der Umfrage beim ZKI [130] sind bereits die Top 5 der klassischen Kompetenzen für die Prozesse ermittelt wurden, die in besonders schützenswerten Hochschulbereichen notwendig sind (siehe Tabelle 9). Für die gewählte Zielgruppe sind davon folgende für ihre Tätigkeiten unbedingt notwendig (alle mit 4 bewerteten Kompetenzen im Bild 46):

<u>Methodenkompetenzen:</u>

- Selbständigkeit

<u>Fachkompetenzen:</u>

- Datenschutz
- Bedrohungen, Angriffsarten
- IT-Wissen
  (Internetsicherheit inkl. Browser, E-Mail- und App-Nutzung, Malwareschutz, mobiles Arbeiten, Verhalten in sozialen Netzwerken)

<u>Sozialkompetenzen:</u>

- Zuverlässigkeit, Konsequenz
- Diskretion, Integrität

Copyright

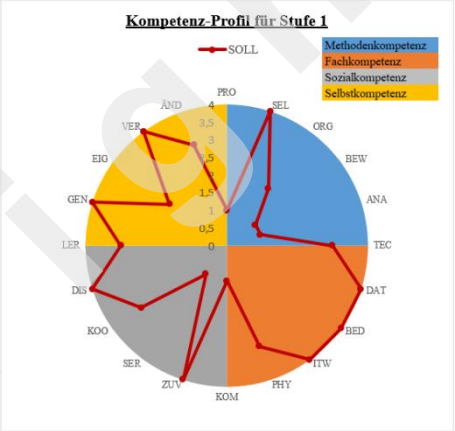
Selbstkompetenzen:

- Genauigkeit
- Verantwortungsbewusstsein

Daraus ergibt sich das im Bild 46 dargestellte Soll-Profil der Kompetenzen für diese Zielgruppe der Hochschule. In der Stufe 2 werden die Fachkompetenzen um zusätzlich relevante Themen oder technische Detailschulungen erweitert. Die anderen Anforderungen bleiben bestehen.

Stufe 1 - sachbearbeitend

Kürzel für die Kompetenz	Bezeichnung für die Kompetenz	SOLL
PRO	Projektmanagement	1
SEL	Selbständigkeit	4
ORG	Organisationsgeschick	2
BEW	Bewertungsvermögen	1
ANA	analytisches/vernetztes Denken	1
TEC	technisches Verständnis, sichere Nutzung digitaler Anwendungen	3
DAT	Datenschutz (DSGVO)	4
BED	Bedrohungen/Angriffsarten	4
ITW	IT-Wissen zum Malwareschutz, mobilen Arbeiten, Verhalten in sozialen Netzwerken, zum Internet (Browser, E-Mail, App)	4
PHY	physische Sicherheit (Zugang/Zutritt)	3
KOM	Schulungskompetenz, kommunikative Fähigkeiten	1
ZUV	Zuverlässigkeit, Konsequenz	4
SER	Kunden-/Serviceorientierung	1
KOO	Teamfähigkeit/Kooperation	3
DIS	Diskretion/Integrität	4
LER	Lernbereitschaft	3
GEN	Genauigkeit	4
EIG	Eigenverantwortung	2
VER	Verantwortungsbewusstsein	4
ÄND	Veränderungsbereitschaft	3



Abstufung:
0 = nicht notwendig
1 = hilfreich für den Job
2 = unterstützt erheblich die Arbeit
3 = notwendig
4 = unbedingt notwendig (Pflicht)

Bild 46: Soll-Profil für die Zielgruppe „sachbearbeitend"; Quelle: eigene Darstellung

8.3.3 Lernziele der ausgewählten Zielgruppe

Besonderer Wert muss auf die Erhöhung der Selbstwirksamkeit gelegt werden, auf die positive Beeinflussung der Motivation und Selbstwahrnehmung der Mitarbeitenden sowie auf die Genauigkeit und das Verantwortungsbewusstsein bei der Abarbeitung der Arbeitsaufgaben. Dies erreicht man vor allem durch die Entwicklung einer für die Zielgruppe bedeutsamen, relevanten Story und durch das Aufzeigen der Konsequenzen bei Entscheidungsvorgängen. Nach der Schulung kann die Zielgruppe verschiedene Gefahren aus den Basisthemen umfassend beschreiben, versteht die Notwendigkeit einzelner Regelungen und Prozessvorgaben, kann risikobehaftete Aktivitäten identifizieren und von risikolosen trennen. Aus Fallbeispielen hat sie gelernt, aufkommende Gefahrensituationen zu diagnostizieren, systematisch zu analysieren,

Copyright

fachmännisch zu bewerten und die erlernten Verhaltensweisen auf reale Situationen angepasst anzuwenden. Die Zielgruppe erkennt die Relevanz des Themas für sich und ihren Beitrag zur Gewährleistung der Informationssicherheit für die gesamte Einrichtung und entwickelt ein Interesse für eine sichere Verhaltensweise. Folgende in Tabelle 12 beispielhaft dargestellten Themen führen zur Erweiterung der bereits vorhandenen fachlichen Grundkenntnisse für die ausgewählte Zielgruppe. Tabelle 13 zeigt das zusätzlich zu erlernende Wissen und den Nutzen, der sich aus dem Erlernten unter Berücksichtigung ihrer Verfassungen ergibt.

Tabelle 12: erweiterte Grundkenntnisse für die ausgewählte Zielgruppe; Quelle: eigene Darstellung

Themenblock	Thema
Passwortsicherheit	einfache Passwörter selbst erraten oder knacken
Internetsicherheit	technische Informationen zur Passwortspeicherung im Browser
	Erkennung professioneller Phishing-URLs
Datenschutz	Datenschutzeinstellungen bei Apps
	Klassifizierung von Daten im Hinblick auf ihre Vertraulichkeit, ihren Personenbezug, ihre Herkunft
	Vorgehensweise zur Verschlüsselung von E-Mails
Sicherheitsvorfallsmanagement	Anlaufstation im Sicherheitsvorfall für Zielgruppe mit Kompetenzstufe 0

Tabelle 13: Darstellung von zu erlernendem Wissen und Nutzen für die ausgewählte Zielgruppe; Quelle: eigene Darstellung

Themenblock	erlerntes Wissen/Verhalten	Nutzen / Relevanz aus den Verfassungen der Zielgruppe
Passwortsicherheit	Passwortsafe benutzen, Zwei-Faktor-Authentisierung aktivieren	Anwendung auch im privaten Bereich möglich
Internetsicherheit	Passwortspeicherung im Browser deaktivieren	Anwendung auch im privaten Bereich möglich
	Analyse des Wer-Bereichs von URLs	mehr Sicherheit in der Erkennung bösartiger Links
Datenschutz	Kriterien zur Prüfung und Herstellung des Datenschutzes kennen	Anwendung auch im privaten Bereich möglich
	Trennung von dienstlichen und privaten Daten verstehen und auch selbst durchführen	aktive Mitarbeit und Beeinflussung des Ergebnisses, das sich aus dem Klassifizierungsprozess ergibt
	Absicherung des Versandes personenbezogener Daten per E-Mail	mehr Sicherheit im Umgang mit personenbezogenen Daten
Sicherheitsvorfallsmanagement	richtiges Verhalten im Notfall	Kompetenzzuspruch und Teilung von Wissen

In der Kompetenzstufe 2 könnten folgende Themen, wie aus Tabelle 14 ersichtlich, für die Zielgruppe hinzukommen:

Tabelle 14: Kenntnisse für die ausgewählte Zielgruppe in der Stufe 2; Quelle: eigene Darstellung

Themenblock	Thema
soziale Netzwerke	Verhalten in sozialen Netzwerken (was darf man posten, was nicht)
Malware	Arten und prinzipielle Funktionsweisen
	technische Schutzeinrichtungen vor Malware-Befall
Mobiles Arbeiten	WLAN-Sicherheit (Hotspots, offenes, geschlossenes WLAN)
	Datenübertragungsarten (Bluetooth, NFC, USB, Cloud etc.)
	Verbindungswege (VPN, VDI, LAN, WLAN etc.)
Social Engineering	Arten von Social Engineering-Angriffen und Abwehrmechanismen
Heimarbeit	Einhaltung der Regelungen zur sicheren Arbeit zu Hause
Sicherheitsvorfallsmanagement	aktive Hilfestellung bei Informationssicherheitsvorfällen

Copyright

Die anderen Kompetenzen (Selbständigkeit, Zuverlässigkeit und Konsequenz, Diskretion und Integrität, Genauigkeit, Verantwortungsbewusstsein) werden durch den Einsatz der Spielelemente und das Game-Design beansprucht.

8.3.4 Rahmenbedingungen, Methoden, Medien und Organisation

Nach der Analyse der Zielgruppe, der Kompetenzen und der Lernziele müssen noch die Rahmenbedingungen festgelegt werden. Zu den Einflussgrößen einer erfolgreichen Awareness-Kampagne gehören die dramaturgische und audiovisuelle Gestaltung, die Ausbaufähigkeit und der langfristige Einsatz der Werkzeuge, die Verwendung erprobter Marketingmethoden, die Kommunikation über klassische und moderne Medien, die Berührung der Menschen auf psychologischer Ebene sowie die Unterstützung und das Verständnis durch die Mitarbeitenden.[46] Analoge Vermittlungsformate können durch digitale Formate nicht gänzlich abgelöst werden, da sich besonders analoge erlebnisorientierte Lernszenarien dazu eignen, das Sicherheitsbewusstsein der Menschen für komplexe Themen zu erhöhen.[136]

Aus diesen genannten Gründen wird der Einsatz von Gamification in zwei Formaten Anwendung finden. Zunächst wird in einer online-Schulung das notwendige theoretische Wissen im Selbststudium erarbeitet und durch Tests abgeprüft. Die Festigung der erlernten Inhalte erfolgt in einem Workshop sowie in einer digital begleiteten modernen offline-Variante, in welcher das Wissen praktisch angewendet wird. Die beiden Applikationen, die dafür verwendet werden, sind das Lernmanagementsystem „Moodle“ und der Internetdienst „Actionbound“. Beide Applikationen wurden in der Umfrage des ZKI als Tools im Rahmen der Sensibilisierung bei Hochschulen benannt.

Der online-Spiel- und Schulungsraum „Moodle“ ist mit Texten, Videos, Bildern, Lückentexten, Drag-and-Drop-Tests, Quizzes und Abschlusstests pro Thema ausgestattet. Dort werden erste Spielelemente verwendet (z. B. Abzeichen, Level, Rangliste, Erfahrungspunkte, Fortschritt, Avatar, Forum, Zuordnungs- und Gruppenaufgaben). Hier findet auch die Einweisung in das Spiel mit seinen Regeln und dem Spielziel statt sowie die Einbettung des Kurses in die Gesamtstory.

Copyright

Den offline-Spielraum stellt der Campus der Hochschule dar, auf dem zu den jeweiligen Schulungsthemen in der begleitenden Actionbound-App, die ebenfalls Spielelemente enthält, passende Aktivitäten durchzuführen und Aufgaben innerhalb einer vorgegebenen Zeit zu lösen sind. Gespielt wird während der Arbeitszeit und es werden auch in der App wieder Spielelemente zur Förderung der Motivation verwendet. Der sogenannte Bound wird über eine URL-Adresse den Teilnehmenden zuvor im online-Spiel- und Schulungsraum bekannt gegeben sowie der Treffpunkt und die Uhrzeit. Das Spiel ist eine Art digitale Schnitzeljagd und muss für die Durchführung nach der Installation der App vorgeladen werden, um offline spielen zu können. Zur Einhaltung des Datenschutzes ist vor der Installation und Verwendung eine Einverständniserklärung zur Verwendung des Mobiltelefons oder Tablets mit Zugriff der App auf den Standort einzuholen. Durch die Verbindung von online- und offline-Spielraum findet eine Überleitung und Öffnung zum realen Arbeitsumfeld statt. Zusammenhänge lassen sich besser erkennen und fördern zusätzlich den Dialog zwischen Schulungsteilnehmenden und Schulenden, die gemeinsam an der Schnitzeljagd teilnehmen.

8.3.5 Einsatz der Spielelemente für die ausgewählte Zielgruppe

Durch den Einsatz der Kompetenzstufen werden von Grund auf schon mindestens zwei Spielelemente verwendet, nämlich Level und Herausforderung. Die Herausforderung besteht in der Absolvierung einer höheren Stufe als prinzipiell für die Tätigkeit im jeweiligen Hochschulbereich notwendig ist. Damit wird gleichzeitig die Motivation der Teilnehmenden gesteigert. Die gewählten Schulungsformate (online-Schulung und digital begleitetes offline-Security-Event) enthalten weitere Elemente, die zum Teil erst durch die Installation bestimmter Plugins (wie z. B. Block Level Up XP Gamification bei Moodle) nutzbar sind. Außerdem bietet das entwickelte Schulungskonzept die Möglichkeit der Selbstreflexion und des Kompetenz- oder auch Nichtkompetenzerlebens in verschiedenen Tests und praktischen Prüfungen, womit zusätzlich eine Feedback-Funktion geschaffen wird. Aufgrund der gesammelten Erfahrungen aus den im Spiel getroffenen Entscheidungen können die Lernenden die so wichtige Selbstwirksamkeit erleben. Bei der Auswahl der weiteren Spielelemente muss darauf geachtet werden, dass diese auch zu den Lernzielen passen. Durch die Verwendung der verschiedenen Quiz- und Aufgabentypen zu den jeweiligen Schulungsthemen wird man dieser Forderung

Copyright

gerecht. Denn die Teilnehmenden werden in Kongruenz zu den definierten Lernzielen darauf trainiert, Gefahren zu erkennen, zu beschreiben und Lösungen zu benennen. Die gemeinsamen Vor-Ort-Aktivitäten im Arbeitsumfeld der Beteiligten stellen den Bezug und die notwendige Relevanz des Themas her. Gleichzeitig wird über wichtige Regeln informiert, die durch die Schulungen zu mehr Verständnis führen. Am Ende entwickeln die Beteiligten ein Interesse für eine sichere Verhaltensweise, um auch aktiv ihren Beitrag zur gesamten Organisationssicherheit zu leisten. Die anderen geforderten Kompetenzen bedient die Kombination aus der online- und offline-Schulung ebenfalls. Denn Genauigkeit beim Lesen der Fragen und Ausführen der Aufgaben ist genauso wichtig wie die Zuverlässigkeit und Kommunikation in der Gruppe im offline-Spiel. Auf die Einhaltung von Diskretion und Integrität wird im Rahmen des Themas Datenschutz eingegangen. Die Selbständigkeit in der Erarbeitung von Themen wurde im Rahmen der online-Schulung bereits berücksichtigt. Durch die gemeinsamen Entscheidungen in der Gruppe beim offline-Spiel lernen die Teilnehmenden mit den Konsequenzen ihrer Handlungen umzugehen. Die Tabelle 15 stellt noch einmal in einer Übersicht dar, welche Spielelemente in den verschiedenen Medien zum Einsatz kommen. Es handelt sich dabei um Elemente, die zur standardmäßigen sogenannten PBL-Triade gehören wie bspw. Abzeichen, Level, Punkte und Fortschrittsbalken. Es kommen auch Elemente zum Einsatz, die besonders den Spielertyp Explorer ansprechen wie z. B. Freischaltungen und Mistery Boxes. Sie sind in der Übersicht als Haupt-Element bezeichnet. Um die anderen Spielertypen auch anzusprechen, werden Zusatz-Elemente wie z. B. Gratisgeschenke, Anfängerglück und Konformitäts-Anker verwendet.

Copyright

Tabelle 15: Übersicht der im online- und offline-Medium verwendeten Spielelemente; Quelle: eigene Darstellung

Element	Art	Bedürfnis	Medium
Abzeichen	Standard-Element	Errungenschaften	online
Level	Standard-Element	Kompetenzerleben	online
Easter Eggs	Haupt-Element für Explorer	Autonomie	offline
Elitismus	Zusatz-Element für alle Spielertypen	soziale Zugehörigkeit	online + offline
Storytelling	Zusatz-Element für alle Spielertypen	Narrativ	online + offline
Heldentum	Zusatz-Element für alle Spielertypen	Narrativ	online + offline
Gratisgeschenke	Zusatz-Element für alle Spielertypen	Errungenschaften	offline
Anfängerglück	Zusatz-Element für alle Spielertypen	Kompetenzerleben	offline
Mentoring	Zusatz-Element für alle Spielertypen	Lernen	online + offline
Punkte/Austauschpunkte	Standard-Element	Errungenschaften	online + offline
virtueller Marktplatz	Standard-Element	Selbstbestimmung	online
Freischaltungen	Haupt-Element für Explorer	Kompetenzerleben	offline
Gruppenaufgabe	Zusatz-Element für alle Spielertypen	soziale Zugehörigkeit	online + offline
Newsfeed / Feedback	Zusatz-Element für alle Spielertypen	kontinuierliches Feedback	online + offline
schwindende Gelegenheit	Zusatz-Element für alle Spielertypen	Herausforderungen	offline
Wahlmöglichkeiten	Zusatz-Element für alle Spielertypen	Selbstbestimmung	online
Konformitätsanker	Zusatz-Element für alle Spielertypen	soziale Zugehörigkeit	online
Rangliste	Zusatz-Element für alle Spielertypen	Konkurrenz	online
Fortschrittsbalken	Standard-Element	Kompetenzerleben	online + offline
Mistery Boxes	Haupt-Element für Explorer	Autonomie	offline
angepasste Inhalte	Zusatz-Element für alle Spielertypen	Selbstbestimmung	online
Sammelfiguren	Zusatz-Element für alle Spielertypen	Errungenschaften	offline

Sollen im Lernmanagementsystem Abzeichen als Belohnung verwendet werden, kann auf passende Vorlagen aus dem Internet zurückgegriffen werden oder es werden selbst Abzeichen entworfen. Das Bild 47 zeigt eigenentwickelte Abzeichen in den Corporate-Farben der Hochschule Anhalt.

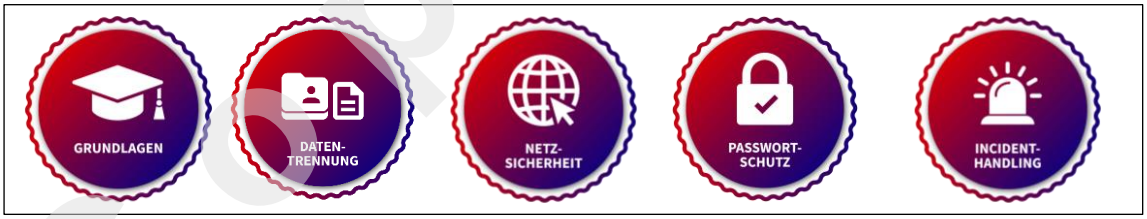


Bild 47: beispielhafte Darstellung für hochschulinterne Abzeichen; Quelle: eigene Darstellung

Gleiches gilt für die Entwicklung der Kompetenzlevel-Symbole und für das Abschluss-Zertifikat (siehe Anlage 5). Auch diese können selbst designt und in den vom Marketing der Hochschule vorgegebenen Farben coloriert werden. Die Verwendung des Corporate-Designs führt zu einer stärkeren Identifikation der Lernenden mit der lehrenden Institution und damit zu einem höheren Verbundenheitsgrad.

copyright

Außerhalb der genannten Spielelemente ordnen die Entwickelnden der Moodle-Lernplattform gemäß dem Bild 48 die verschiedenen Funktionen den Bartle-Spielertypen zu. So passen nach ihrer Meinung die Funktionen Forum, Wiki und Choice besonders zum Explorer-Spielertyp (grün eingefärbte Kästchen beim rot umrandeten Spielertyp Explorer). Die Funktion Glossary passt am besten auf die anderen Spielertypen. Die Funktionen Workshop und Quiz werden ebenfalls als sinnvoll für den Einsatz als Spielelement erachtet. Von diesen Funktionen werden Forum, Glossary und Quiz in der erstellten online-Schulung aktiv verwendet.

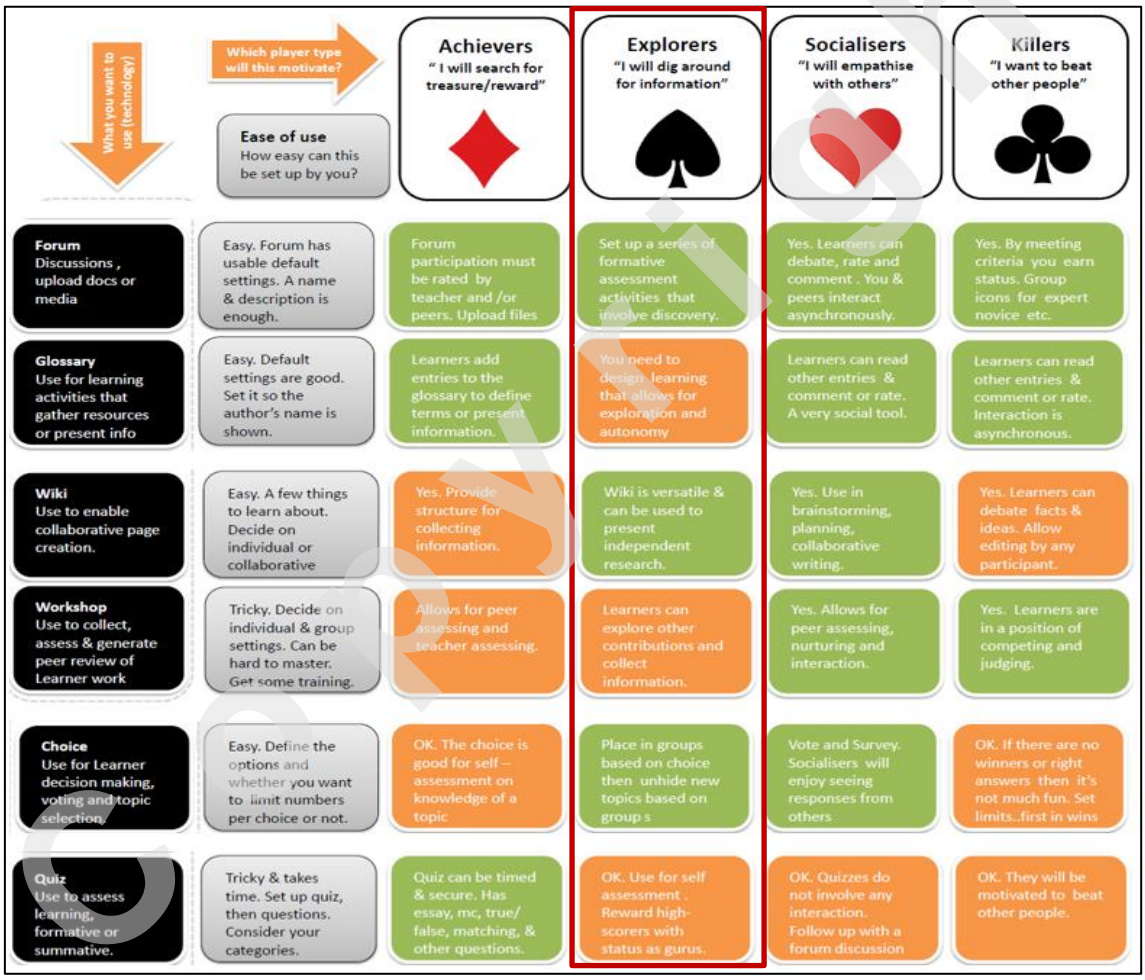


Bild 48: Zuordnung der Funktionen zu den Spielertypen; Quelle: http://mojoo.com.au/downloads/Moodle_For_Motivation_Guide.pdf; abgerufen: 15.08.2022

Copyright

8.3.6 Story-Entwicklung

Möchte man dem ersten Kernantrieb des OCTALYSIS-Frameworks im Schulungskonzept gerecht werden, so muss man es in einen größeren Rahmen einbinden. Die Beteiligten müssen sich berufen fühlen, das Thema intensiv zu bearbeiten. Eine Möglichkeit ist die Entwicklung einer Story, die alle gemeinsam lösen und die aber auch für die verschiedenen Teams in den Kompetenzstufen eine Einzel-Mission darstellt, um die Spieltechnik des Elitismus zu verwenden. Die Einzel-Mission pro Team wird in der online-Schulung vorgestellt. Die jeweilige Zielgruppe stellt die Auserwählten im Rahmen ihrer Einzel-Mission dar. Alle Zielgruppen tragen gemeinsam zur Lösung der Gesamt-Mission bei. Zur Identifizierung mit ihrer Mission erhält die Mission der jeweiligen Gruppe einen besonderen Titel. Wurde die Teil-Mission erfolgreich abgeschlossen und damit der erste Teil erfüllt, erhalten die Teilnehmenden zur Erinnerung an das Spiel und als emotionalen Anker in der realen Arbeitswelt ein Sammelobjekt. Damit wird das Interesse für weitere Kurse und Missionen geweckt, die innerhalb der Awareness-Kampagnen angeboten werden und mit der Sammlung weiterer Objekte verknüpft sind.

Beteiligte Zielgruppen

Es handelt sich somit um ein kooperatives Schulungskonzept, was aber auch mit individuellen Lerneinheiten und kompetitiven Elementen ausgestattet ist. Es geht nicht um einen Konflikt, der zu lösen ist, sondern um die Enthüllung eines bedeutenden Geheimnisses. Insgesamt sind an der Lösung des Geheimnisses die gebildeten sieben Zielgruppen beteiligt.

Story zum Spiel

Die Informationssicherheit ist für viele Personen ein „Buch mit sieben Siegeln“ und das ist der Aufhänger für die Gesamtstory. Nur die Auserwählten können jeweils ein Siegel finden, welches ein Dokument verschließt. Zur Öffnung dieses Siegels müssen sie unterschiedliche Fallstricke im Spiel überwinden, welche die verschiedenen Bedrohungen in der Informationssicherheit darstellen und Aufgaben lösen, was den erlernten Gegenmaßnahmen zur Abwendung dieser Bedrohungen entspricht. Ein geöffnetes Siegel bzw. Dokument allein ergibt noch keinen Sinn. Erst wenn alle sieben Siegel geöffnet und alle Dokumente miteinander richtig kombiniert werden, geben sie das

Copyright

große Geheimnis frei. Für die ausgewählte Zielgruppe der sachbearbeitenden Personen könnte die Teil-Mission den Titel „Das Siegel der SaPé“ tragen, wobei „SaPé“ für „Sachbearbeitende Personen“ steht.

8.3.7 Spielregeln, Spieldynamiken, Spiel-Genre und Spielziele

Spielregeln

Da eine online-Schulung weitestgehend selbsterklärend ist, bedarf es einzig für die digital begleitete Schnitzeljagd einer kleinen Spielanleitung. Folgende Spielanleitung kann vor Ausführung der Teil-Mission für die jeweilige Zielgruppe mit ausgegeben werden:

Gespielt wird in einem Team von 5 – 6 Personen. Das Spiel dauert maximal 60 Minuten. Innerhalb dieser Zeit muss das Ziel erreicht werden. Als Materialien werden ein Smartphone oder Tablet, eine Internetverbindung und eine Applikation namens Actionbound benötigt. Diese sollte vorab aus dem Google Play Store oder aus dem App Store heruntergeladen und installiert werden. Für die richtige Funktionsweise der App und die Ausführung der Aktionen muss der Zugriff auf die Kamera, den Standort und den Speicher des Smartphones berechtigt werden. Nach der Installation kann entweder ein mitgeteilter URL-Link (https://actionbound.com/bound/MissionSaPe) oder QR-Code (siehe Bild 49) des entsprechenden Bounds namens „Mission SaPé“ ausgewählt und auch für den offline-Gebrauch abgespeichert werden. Das Spiel beginnt am im online-Schulungskurs mitgeteilten Treffpunkt um die vereinbarte Uhrzeit. Die Teil-Mission (Bound) darf erst gestartet werden, wenn alle Teilnehmenden vor Ort sind. Mit Start des Spiels läuft die Zeit. Ein Unterbrechen ist zu jederzeit möglich, wird aber aufgrund der relativ kurzen Spielzeit nicht empfohlen. Auch ein Abbrechen ist möglich, führt aber zum Verlust des aktuellen Fortschritts. Ziel des Spiels ist das Finden eines Dokuments, das mit einem Siegel gesichert ist. Das Siegel muss fotografiert, hochgeladen und eingesammelt werden. Danach darf das Siegel gebrochen und das Dokument geöffnet werden. Dieses ist ebenfalls zu fotografieren und im Lernmanagementsystem unter dem zugehörigen online-Kurs nachträglich (wenn alle sieben Teams gespielt haben) im Forum mit dem Betreff „Actionbound-Schnitzeljagd“ als Beitrag einzustellen. Um das Spielziel zu erreichen, müssen die Teilnehmenden im Spielverlauf verschiedene Aufgaben erledigen und Aktivitäten durchführen, die sich alle auf das Thema

Copyright

Informationssicherheit beziehen. Für die richtig gelösten Aufgaben erhalten die Spielenden Punkte. Sind die Antworten falsch, werden Punkte abgezogen. Manche Aufgaben sind mit einer Wiederholungsfunktion ausgestattet, so dass nicht sofort die Gefahr des Punkteabzugs besteht. Über das Actionbound-Menü am oberen rechten Telefon-Bildschirm können die Punkte, der Fortschritt und der jeweilige Spielabschnitt eingeblendet werden. Die Punkte, die das Team am Ende gesammelt hat, werden zu den jeweiligen individuell erreichten Punkten im online-Kurs hinzugezählt und ergeben einen neuen Punktestand, der in einer Rangliste dargestellt wird.

Bild 49: QR-Code des erstellten Bounds; Quelle: erzeugt aus der Actionbound-App

Spieldynamiken

Mit der Dynamik werden Prozesse in einem Spiel in Gang gesetzt. Sie gibt einen Impuls oder eine Aufforderung zur Gestaltung des Spiels. Auch die Reize, die von Grafik, Animation und Sound ausgehen, gehören zur Dynamik.[137]

In der digital begleiteten offline-Variante mit Actionbound sind Spieldynamiken in Form von zeitlich begrenzten Aktionen, Spannungsmomenten durch überraschende Punktvergaben und Soundeffekte sowie durch die Art der Aufgaben vorhanden (Orte per GPS finden, QR-Codes scannen, Interaktionen mit der App). Der online-Kurs besitzt in Form eines aktiven Forums dynamische Effekte. In diesem Forum können die

Copyright

Teilnehmenden miteinander kommunizieren und sich gegenseitig zu Aktionen auffordern.

Die dynamische Komponente im gesamten Schulungskonzept stellen die flexiblen Aufgaben und Prüfungsbausteine in den verschiedenen Schulungsformaten dar. Sie unterstützen damit die Aufrechterhaltung der erarbeiteten Qualifikation der Mitarbeitenden, denn Lerninhalte müssen immer wieder und in unterschiedlichen Formen und Situationen angewendet werden, damit sie nicht in Vergessenheit geraten. Zusätzlich dienen Besprechungen dazu, nach durchgeführten Workshops und Events wie einer digitalen Schnitzeljagd, das erworbene Wissen in einem außerhalb der Schulungen liegenden Kontext anzuwenden.

Spiel-Genre

Die gewählten Schulungsformate stellen eine Mischung unterschiedlicher Spiel-Genre dar. Im Schulungskonzept werden Quizze und Rätsel in den verschiedenen Anwendungen eingesetzt, die insgesamt einem Lernspiel ähneln und die im Part der digital begleiteten offline-Variante durch die Zeitbegrenzung einen Escape-Charakter haben. Hier erkennt man klar den Vorteil des Einsatzes von Gamification im Gegenteil zu Serious Games. Denn hier muss nicht von Anfang an eine Festlegung auf ein bestimmtes Genre erfolgen, sondern es ist möglich, mehrere Genres zu vermischen und damit auch verschiedene Spielertypen zu erreichen und verschiedene Sinnelemente bei Menschen anzusprechen. Vor allem der Erkenntnistrieb, der Forschungsdrang, der Spieltrieb, das Gestaltungsbedürfnis und der Wettkampftrieb werden durch die gewählten Formate befriedigt.

Spielziel der Teil-Mission

Jede Zielgruppe hat in ihrer jeweiligen Kompetenzstufe eine Einzel-Mission zu erfüllen. Sie müssen mit Hilfe der Actionbound-App innerhalb einer bestimmten Zeit ein an der Hochschule verstecktes Dokument finden, welches mit einem Siegel verschlossen ist. Das Dokument stellt einen Teil der Lösung für die Entschlüsselung des Geheimnisses der Gesamt-Mission dar.

Copyright

Spielziel der Gesamt-Mission

Alle sieben Zielgruppen müssen ihr individuelles Siegel und Dokument finden und mit den anderen Zielgruppen teilen. Durch die richtige Kombination aller gefundenen Dokumente wird das große Geheimnis der Gesamt-Mission gelüftet.

8.3.8 Storyboard

Actionbound ist eine weitere Form der Schulung, die durch die interaktiven und aktiven Elemente jedoch intensiver empfunden wird als ein online-Kurs, der überwiegend im Selbststudium durchgeführt wird. Folgende Abschnitte sind im erstellten Bound angelegt und enthalten Quizze, Informationsseiten, Turniere und Aufgaben:

- Einleitung
- Datenschutzeinstellungen bei Apps
- Passwortknacker
- Passwörter aus dem Browserspeicher auslesen bzw. verwenden
- Klassifizierung von Daten (vertraulich, privat, dienstlich)
- verschlüsselte E-Mails
- Reaktion bei Sicherheitsvorfällen
- Abschluss

In der Anlage 6 ist für die einzelnen Abschnitte jeweils eine Beispielszene in einem Storyboard dargestellt. Einen besseren Eindruck zur Interaktion zwischen Spiel und Spielenden vermittelt das Bild 50. Zu sehen sind darauf die verschiedenen Aktionen, die von den Spielenden vor Ort durchgeführt werden müssen, um die Aufgabe 11 des Bounds zu lösen. Die Anlage 7 zeigt den gesamten erstellten Bound.

Copyright

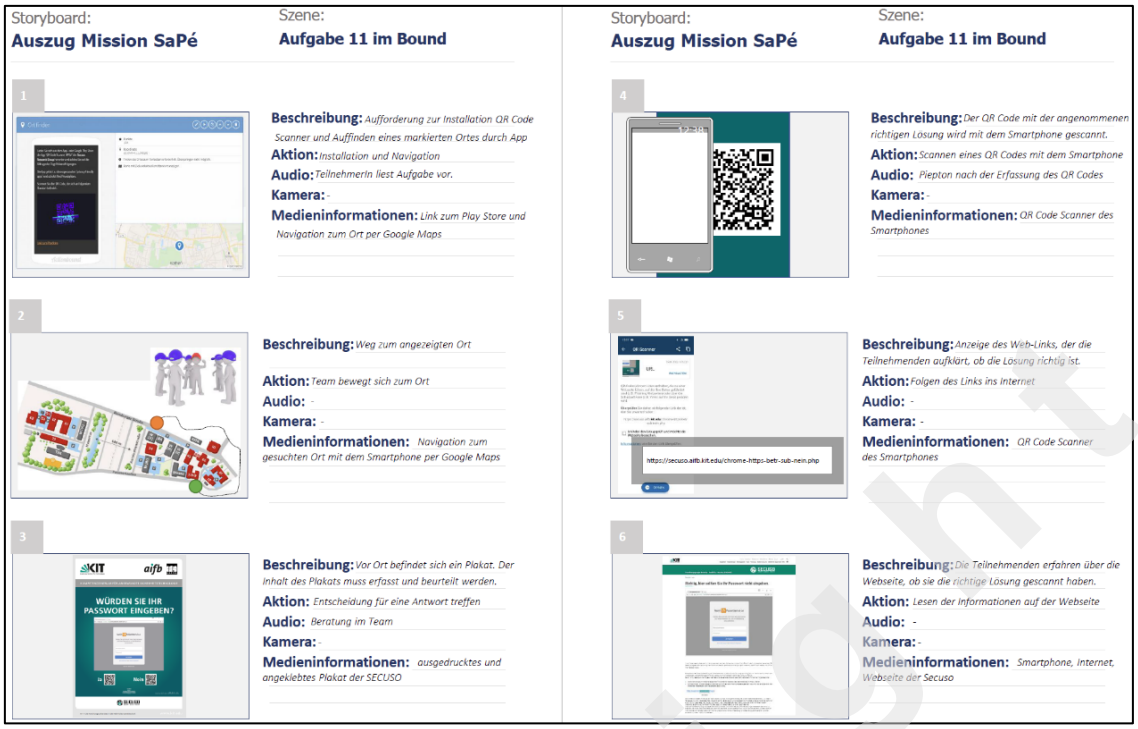


Bild 50: Ablauf der Aufgabe 11 im selbst erstellten Bound; Quelle: eigene Darstellung

8.4 Messung von Effektivität und Nachhaltigkeit eines Schulungskonzepts

Trotz vieler Fallstudien gibt es bis heute keine klaren Erkenntnisse davon, welche Spielelemente oder welche Kombinationen von Spielelementen welche Wirkung zur Folge haben.[23] Das bedeutet aber nicht, dass eine gamifizierte Schulung nicht effektiv und nachhaltig ist. Nach der Durchführung der umfassenden Literaturrecherche scheint für die Bestimmung der Wirksamkeit das Zusammenspiel von drei Komponenten entscheidend zu sein:

- Selbstbestimmtheit
- Motivation
- Selbstwirksamkeit.

Der Grad der Selbstbestimmtheit ist dort am höchsten, wo die durchgeführte Handlung als selbst und frei gewählt empfunden wird.[68] Ist der Grad der Selbstbestimmtheit hoch, ist auch die Motivation zur Handlung hoch. Im Bereich des Lernens beurteilen selbstbestimmt Lernmotivierte ihre Selbstwirksamkeit als hoch. Sie gehen davon aus, dass sie aufgrund ihrer Fähigkeiten, Kenntnisse und psychischen Verfassung die ihnen gestellten Aufgaben meistern werden. Aus diesem Grund verhalten sie sich selbstsicher

Copyright

und nehmen Herausforderungen gern an. Sie sind entsprechend motiviert. Die Motivation ist eine Art Erleben eines Gefühls. Die Selbstwirksamkeit ist ein bewusst gesteuertes Verhalten zum Vorgehen bei der Problemlösung. Der Grad der Selbstwirksamkeit äußert sich im Lernerfolg der Lernenden. Als Lernerfolg gilt, wenn mit einem Problem professionell umgegangen wird und keine Zweifel an der Richtigkeit der Vorgehensweise bestehen. Die Wirksamkeit einer Schulung, die Spielelemente enthält, lässt sich am besten im Vergleich mit einer Schulung, die keine Spielelemente beinhaltet, feststellen. Die Abschlussquote bei einer Schulung mit Spielelementen sollte höher und die Abbruchquote geringer sein. Auch eine professionelle Verhaltensweise bei Stresssituationen in unangekündigten Tests (z. B. Phishing-Simulation mit Erfassung der Klick-Rate) oder die eindeutige Kenntnis von Vorgehensweisen bei Sicherheitsvorfällen, die durch Auditierungen nach bspw. DIN EN 9001:2015 festgestellt wird, sind Hinweise auf die Nachhaltigkeit und Effektivität vorangegangener Trainings. Ein weiteres Mittel, die Qualität von Schulungen festzustellen, ist die sogenannte Flow-Kurzskala[138] (siehe dazu Anlage 8). Sie kann während stattfindender Schulungen das Flow-Erlebnis der Teilnehmenden erfassen. Wenn sich eine Person im Flow befindet, hat sie das Gefühl des tiefen Eintauchens in die Thematik, weil die Anforderungen und Fähigkeiten der Person ausbalanciert sind. Sie verschmilzt ganz mit den Schulungsinhalten und hat dabei eine hohe kognitive Verarbeitung im Gehirn, was wiederum zur nachhaltigen Festsetzung führt. Eine qualitätsunterstützende Maßnahme kann auch die Kontrolle der Einhaltung der Empfehlungen für das Design einer Schulung in Bezug auf die Selbstwirksamkeit und Lernmotivation sein. Dies kann in Form einer Checkliste erfolgen (siehe nachfolgende Tabelle 16). Für das entwickelte Schulungskonzept sind diese Empfehlungen größtenteils umgesetzt worden. In der Anlage 9 befinden sich ein paar anschauliche Beispiele dafür. Auch die im Abschnitt 8.3.1 gestellten Forderungen nach Erfahrungen und Kooperationen in Kombination mit Durchhaltevermögen, Genauigkeit und Selbstkontrolle bei der Aufgabenerledigung zur Berücksichtigung der verschiedenen Persönlichkeitstypen wurden eingearbeitet.

Copyright

Tabelle 16: Checkliste für die Einhaltung einer hohen Selbstwirksamkeit; Quelle: eigene Darstellung

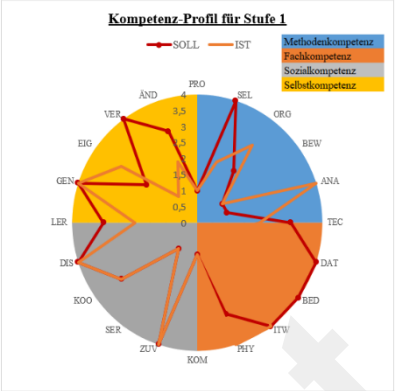
Empfehlungen	**erfüllt ja/nein?**
Identifikation mit den gesetzten Zielen (selbstkongruent)	☐
Erfolgserleben durch schnelle Erfolge	☐
zunächst begrenzter Funktionsumfang, keine Ablenkung	☐
Quests auf freiwilliger Basis zur Prüfung der Selbstkompetenz	☐
Lernen mit und von anderen in Gruppen	☐
Unterstützung der Anstrengungen durch positives Feedback	☐
Übertragung von Verantwortung zur Kompetenzstärkung	☐
Aufzeigen von Lernstrategien	☐
Begleitung in der Aufgabenlösung (unabhängige Kommunikation möglich)	☐

In der Gegenüberstellung des zuvor definierten Soll-Kompetenzprofils (siehe Abschnitt 8.3.2) mit dem nach der Schulung erreichten Ist-Kompetenzprofil ist die Entwicklung der Teilnehmenden erkennbar und lässt ebenfalls einen Rückschluss auf die Wirksamkeit der Schulung zu. Dazu schätzen sich die Schulungsteilnehmenden über einen mit einer Bewertungsskala versehenen Fragebogen mit ausgewählten Leitfragen zu den jeweiligen Kompetenzen selbst ein (siehe Anlage 10)[139]. Neben der Einschätzung der durchlaufenden Entwicklung ist auch eine Aussage zu den noch vorhandenen Lücken in den einzelnen Kompetenzbereichen möglich. Im Bild 51 stellt im Kreisdiagramm der Bereich zwischen Soll- und Ist-Linie diese Fehlstellen dar. Anschließend durchgeführte Schulungen können darauf ausgerichtet werden, diesen Zwischenraum in den Profilen systematisch zu schließen. Im Bild wäre das bspw. die Datenschutzthematik als Fachkompetenz, die noch weiter in Trainings behandelt werden müsste. Dies kann z. B. durch das vermehrte Üben unterschiedlicher Fallbeispiele und Quizze erreicht werden.

Copyright

Stufe 1 - sachbearbeitend

Kürzel für die Kompetenz	Bezeichnung für die Kompetenz	SOLL	IST
PRO	Projektmanagement	1	1
SEL	Selbständigkeit	4	2
ORG	Organisationsgeschick	2	3
BEW	Bewertungsvermögen	1	1
ANA	analytisches/vernetztes Denken	1	4
TEC	technisches Verständnis, sichere Nutzung digitaler Anwendungen	3	2
DAT	Datenschutz (DSGVO)	4	1
BED	Bedrohungen/Angriffsarten	4	2
ITW	IT-Wissen zum Malwareschutz, mobilen Arbeiten, Verhalten in sozialen Netzwerken, zum Internet (Browser, E-Mail, App)	4	4
PHY	physische Sicherheit (Zugang/Zutritt)	3	4
KOM	Schulungskompetenz, kommunikative Fähigkeiten	1	1
ZUV	Zuverlässigkeit, Konsequenz	4	4
SER	Kunden-/Serviceorientierung	1	1
KOO	Teamfähigkeit/Kooperation	3	3
DIS	Diskretion/Integrität	4	4
LER	Lernbereitschaft	3	2
GEN	Genauigkeit	4	4
EIG	Eigenverantwortung	2	3
VER	Verantwortungsbewusstsein	4	1
ÄND	Veränderungsbereitschaft	3	2



Abstufung:
0 = nicht notwendig
1 = hilfreich für den Job
2 = unterstützt erheblich die Arbeit
3 = notwendig
4 = unbedingt notwendig (Pflicht)

Bild 51: beispielhafte Darstellung von Soll- und Ist-Kompetenz-Profil für Stufe 1; Quelle: eigene Darstellung

Es ist nicht ausreichend festzustellen, dass ein gewünschtes Kompetenz-Profil vorhanden ist oder erreicht wurde. Vielmehr müssen die vorhandenen Kompetenzen auf dem notwendigen Soll-Niveau gehalten werden, um nachhaltig verankert zu sein. Das bedeutet, dass eine Schulung die Kompetenzen dauerhaft lehren und prüfen muss, aber auch neue Sichtweisen und andere Instrumente verwenden muss, um die Motivation und das Interesse der Schulungsteilnehmenden aufrecht zu erhalten. In Schulungen eingesetzte Spielelemente erfüllen diesen Zweck auf besondere Weise, indem sie auf die psychologischen Bedürfnisse der Spielenden abgestimmt und eingesetzt werden können. Ein Element, das in der Literatur immer wieder als besonders wichtig hervorgehoben wird, ist das kontinuierliche Feedback. Je nach Art beeinflusst es maßgeblich das Motivationspotenzial der Teilnehmenden.[23] Es unterstützt beim Übergang von der extrinsischen zur intrinsischen Motivation, denn eine individuelle positive Rückmeldung wirkt sich durch ihren Belohnungscharakter auch positiv auf die intrinsische Motivation und damit positiv auf das Empfinden eines Menschen aus. Wenn Feedback jedoch als Überwachungsinstrument empfunden wird, kann es sich auch negativ auf die intrinsische Motivation auswirken. Feedback muss ehrlich, neutral und möglichst individuell sein. Weil Menschen positive Emotionen und Zielzustände lieben, muss man ihnen positives Feedback und richtungsweisende Anreize (Nudges) zukommen lassen oder Gelegenheiten schaffen, in denen die positiven Gefühle durch die Ausführung bestimmter und bekannter Handlungsweisen entstehen. Das alles kann man durch Gamification erreichen, nur immer in einer etwas anderen Form. Durch den variablen Einsatz von

Copyright

Gamification wird auch Informationssicherheit interessant. Es wird darüber geredet und sich untereinander ausgetauscht. Gleichzeitig wird ein Zusammengehörigkeitsgefühl geschaffen und die Einstellung zum Thema als persönlich zu verfolgende Norm in das Bewusstsein aufgenommen.

8.5 Negative Aspekte und Grenzen von Gamification

Auch wenn Gamification in seinem Einsatz sehr variabel ist, so hat es auch negative Aspekte. Diese sind bspw. wie eingangs erwähnt Ablenkung, Attraktivitätsverlust, Verletzung der Privatsphäre, Manipulation, Spielsucht, Inakzeptanz, Gleichgültigkeit, Entmutigung und falsche Verstärkung, um nur einige zu nennen.[14] In der Anlage 11 sind weitere mögliche Risiken oder Nebenwirkungen von Gamification zusammengetragen, die alle losgelöst von ihrem jeweiligen Kontext identifiziert wurden. Besonders Bestenlisten, Abzeichen und Punkte sollen laut einer Übersichtsarbeit mit 17 Studien zur „Dark Side of Gamification“ die meisten negativen Effekte auslösen.[14]

Es ist wie bei so vielen Dingen, zu viel und falsch verwendet, wirken sie nicht wie gewünscht. Das trifft auch auf den Einsatz von Gamification zu. Die Menschen gewöhnen sich schnell an Dinge, vor allem auch an Belohnungen, womit diese mit der Zeit uninteressant werden. Sie stumpfen ab oder wissen, wie man etwas leichter oder auf anderen Wegen erreicht. Um anderen zu imponieren, ändern sie ihr Verhalten, obwohl sie anders denken und fühlen. Sie werden in gewisser Weise abhängig gemacht und sind getrieben von den Spielelementen. Sie handeln nur, weil sie dafür belohnt werden und weil sie anderen zeigen können, was sie schon erreicht haben. Die Aktivitäten führen sie dann nicht aus ihrem inneren Antrieb heraus aus. Man kann sich leicht vorstellen, dass damit auch gute (Team-) Verhältnisse zerstört werden, indem Spielbeteiligte auf die erreichten und präsentierten Erfolge neidisch und eifersüchtig werden. Der soziale Umgang kann negativ beeinflusst werden. Menschen begeben sich in Rollen und täuschen Teamgeist vor, um Belohnungen und damit Zufriedenheit zu erlangen. Doch sind die Formen der Belohnungen irgendwann ausgeschöpft, die Zufriedenheit der Menschen aber nicht. In diesem Fall besteht die Gefahr einer aufkommenden Demotivation. Setzt man dann die falschen Spielelemente zur Verstärkung einer Motivation oder Verhaltensweise ein, ohne einen zusätzlichen positiven Nutzen für die Spielenden zu generieren, kann es

Copyright

zu ungewollten Verhaltensweisen kommen oder auch zu Fehlinterpretationen. Es bedarf eines gesunden Mittelmaßes zum Einsatz der Spielelemente und zusätzlich der Abstimmung und Kontrolle mit den Lernzielen, um diese Auswirkungen zu vermeiden.

Ein anderer negativer Aspekt von Gamification ist die Kategorisierung der Spielenden in Spielertypen. Ziel dabei ist, sie mit Spielelementen zu versorgen, von denen man annimmt, dass sie am besten zu ihnen passen. Aber wenn man davon ausgeht, dass die Menschen heutzutage mehrere Rollen spielen wollen (siehe 6.4 Verfassungsmarketing), dann ist solch eine Klasseneinteilung gar nicht möglich. Auch die Erfassung der Daten von Spielenden im Zusammenhang mit den zunehmenden online-Funktionalitäten von gamifizierten Anwendungen wird in der Literatur kritisiert. Die Information und die Zurverfügungstellung einer Auswahl- bzw. Abwahlfunktion für die Spielenden über die jeweils erfassten Daten und ihre Art der Verarbeitung und Speicherung kann die Hersteller der Anwendungen vom dargestellten Datenschutzproblem entlasten.

Die negativen Aspekte von Gamification können auch an Hochschulen auftreten, aber bei ihrem Einsatz in der Lehre zum Zwecke der Motivation auch zur Überforderung und Ablenkung der Lernenden führen, wenn Lern- und Spielkontext nicht optimal aufeinander abgestimmt sind. Damit entsteht die Gefahr, dass das eigentliche Lernziel nicht erreicht wird.[14] In einigen Untersuchungen im Bildungsbereich haben die Lernenden selbst festgestellt, dass ihnen der konkrete Nutzen nicht klar ist und dass es vereinzelt zu Neid und Unsicherheit kommt.[107] Dabei ist aber auch zu bemerken, dass die Risiken in Bezug auf ihre Auswirkungen bei den Beteiligten unterschiedlich schwer wiegen und Menschen auch verschieden auf Gamification reagieren.[14]

Seine Grenzen hat Gamification auch im Change-Management-Prozess. Der Einsatz von gamifizierten Anwendungen muss vom Top-Management unterstützt werden. Es bedarf eines Paradigmen-Wechsels von „Spielen ist etwas für Kinder“ zu „Spielen ist die neue Art zu lernen und Wissen zu vermitteln“. Diese Veränderung kann nur stattfinden, wenn die Verantwortung für diesen Wechsel von der Führungsebene einer Organisation übernommen wird und die zu schulenden Mitarbeitenden durch ein permanentes Training und durch eigene Erfahrungen die Vorteile des Einsatzes von Gamification erkennen und

Copyright

entsprechend Feedback für Verbesserungen geben, so dass am Ende ein Paket entsteht, dass möglichst viele Mitarbeitende in ihren Arbeitssituationen abholt und von der Sinnhaftigkeit und dem Nutzen der intelligenten Verknüpfung von Ernsthaftigkeit und Spielspaß überzeugt.

Auch ist Gamification allein nicht zur Steigerung der organisationsweiten Awareness verwendbar. Neben dem Wissen, welches in den Schulungen vermittelt wird und dem Willen der Spielenden, sicherheitskonform zu handeln, ist auch das Können zur Anwendung der gewünschten Verhaltensweisen wichtig. Das Können muss das Unternehmen gewährleisten, indem eine Arbeitsumgebung geschaffen wird, die eine Umsetzung der zu Arbeitsabläufen erstellten Sicherheitsrichtlinien ermöglicht (siehe Bild 52). Damit ist das Personal in der Lage, in ihrem Arbeitsalltag entsprechend den vorgegebenen Regularien zu handeln bzw. sich nach den in den Trainings erlernten Mustern zu verhalten.[46] Damit die Belegschaft das Verhalten auch ändern kann, müssen Sicherheitsbarrieren in altbewährten bestehenden Prozessabläufen erkannt und eliminiert werden. Dazu ist eine IST-Analyse der wichtigsten Prozessabläufe durchzuführen unter Ermittlung der bestehenden Schwachstellen. Die Schwachstellen werden nach Eintrittswahrscheinlichkeit und Schadensausmaß bewertet und ergeben ein Risiko für das Unternehmen und die Security Awareness, welches von der Führungsebene entweder getragen oder minimiert werden muss.

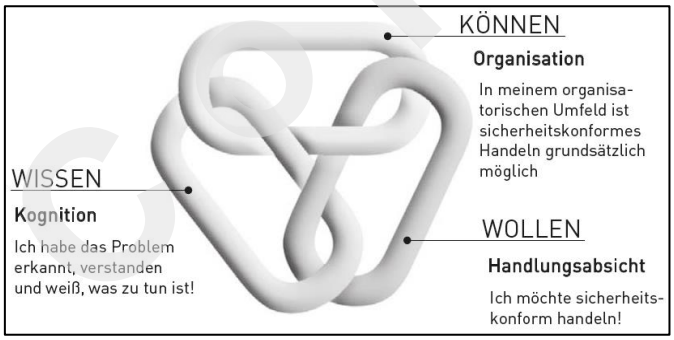


Bild 52: Zusammenspiel der Security Awareness; Quelle: [46]

Copyright

9. Zusammenfassung und Ausblick

Das Ziel der Master-Thesis war die Untersuchung des Einsatzes von Gamification zur Sensibilisierung für Informationssicherheit an deutschen Hochschulen. Es hat sich gezeigt, dass trotz der fortschreitenden Digitalisierung der Hochschullehre für die Mitarbeitenden an Hochschulen diese Formate noch nicht in großem Umfang eingesetzt werden. Das bestätigten die beiden im Rahmen dieser Thesis durchgeführten Umfragen. Ein Grund dafür könnte die Konzentration der Einrichtungen auf die Forschung und Lehre und weniger auf die Ausbildung ihrer eigenen Mitarbeitenden sein. Diese werden zwar für die Notwendigkeit der Einhaltung der Informationssicherheit in Schulungen unterrichtet, aber die Instrumente, die dazu eingesetzt werden, entsprechen oft in ihrer Ausgestaltung nicht dem eigentlichen Ziel von Gamification. Wirkliches Gamification verwendet nicht nur Punkte, Abzeichen und Bestenlisten, sondern erfordert die Entwicklung einer Gesamtstory und die Integration verschiedener Hochschulbereiche zur Erstellung einer ganzheitlichen Awareness-Kampagne, die Gamification auf die unterschiedlichste Weise und in variablen Formen verwendet. Eine solche Kampagne bedeutet internen Aufwand und diesen scheuen viele Hochschulen noch. Die ständige Personal- und Finanzknappheit könnten Gründe dafür sein, jedoch gibt es eine Vielzahl an Möglichkeiten, auch mit geringen Mitteln eine gute Story und Kampagne zu gestalten, die alle Zielgruppen einer Hochschuleinrichtung anspricht. Exemplarisch wurde in dieser Arbeit eine Zielgruppe ausgewählt und anhand dessen gezeigt, wie die Entwicklung eines Schulungskonzepts aussehen kann, das für viele Zielgruppen und Hochschulbereiche adaptier- und erweiterbar ist. Es wurden die verschiedenen Persönlichkeits-, Spieler- und Lerntypen vorgestellt und Spielelemente definiert, die auf diesen Klassifizierungen aufbauen. Zur Absicherung der Wirksamkeit des entwickelten Konzepts wird die Durchführung einer Umfrage mit jeder Zielgruppe nach Abschluss ihrer Ausbildung in der jeweiligen Kompetenzstufe empfohlen. Wichtig bei dieser Befragung ist die Ermittlung des Grades der Harmonie zwischen vorgegebenen Lernzielen und gewählten Spielelementen sowie die Erstellung eines Vorschlages durch die Teilnehmenden zu individuellen Lernzielen für die nächste Schulungseinheit.

Copyright

Gamification kann im Rahmen von Schulungen als Mittel zur Sensibilisierung des abstrakten und komplexen Themas Informationssicherheit eingesetzt werden, muss aber auch durch eine professionelle Unterstützung des Marketing- und Kommunikationsbereichs und durch die Führungsebene einer Hochschuleinrichtung unter Berücksichtigung psychologischer Aspekte und marktüblicher Instrumente begleitet und gefördert werden. Die am Anfang dieser Arbeit genannten Gründe für unsicheres Verhalten, die in fehlendem Bewusstsein für Informationssicherheit, Unwissenheit, Nachlässigkeit, Apathie und Widerstand liegen, treten damit gar nicht erst auf. Es hängt an der Hochschulleitung, dem vorgestellten Konzept zu vertrauen und die zur Verwendung vorgeschlagenen Medien inklusive der beispielhaften Story in ihrer Art und ihrem Umfang und zu diesem Zweck zum Einsatz zu bringen. Denn es bedarf sicherlich etwas Mut, sich vom Gedanken des Spielens als pure Zeitverschwendung zu lösen und offen die Meinung zu vertreten, dass während der Arbeitszeit auch so oft wie nötig gespielt werden darf. Um das Gelernte zu verfestigen, sind permanentes Lernen, Wiederholen und Überprüfen der Leistungen notwendig. Außerdem muss ein Prozess etabliert werden, der einen Abgleich zwischen erstellten Unternehmensrichtlinien und geschulten Inhalten sowie deren Realisierbarkeit in den vorhandenen Arbeitsabläufen vornimmt. Nicht immer unterstützt Gamification die Herstellung des Bezugs zur Realität und den Vollzug des Transfers des Erlernten in die Praxis, aber es ist ein Instrument, das die Motivation, das Interesse und das soziale Miteinander der Lernenden fördern kann. Aufgrund seiner überwiegend positiven Eigenschaften ist Gamification für den Einsatz zur Sensibilisierung für Informationssicherheit auch für Hochschuleinrichtungen in Deutschland geeignet.

Copyright

10. Literaturverzeichnis

[1] Bundesamt für Sicherheit in der Informationstechnik (s.a): IT-Grundschutz-Kompendium. Bundesanzeiger-Verl., Köln.

[2] Deutsches Institut für Normung e. V. (06/2017): DIN EN ISO/IEC 27001:2017-06, Informationstechnik_- Sicherheitsverfahren_- Informationssicherheitsmanagementsysteme_- Anforderungen (ISO/IEC_27001:2013 einschließlich Cor_1:2014 und Cor_2:2015); Deutsche Fassung EN_ISO/IEC_27001:2017, 03.100.70, 35.030(27001:2017-06). Abgerufen am 23.08.2022.

[3] Office, P (2020): Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung) (Freund). In: Schuster, F, Grützmacher, M (Hrsg), *IT-Recht.* Verlag Dr. Otto Schmidt.

[4] Bendel Dr., O (13.07.2021): Gamification. Definition: Was ist "Gamification"? https://wirtschaftslexikon.gabler.de/definition/gamification-53874/version-384606. Abgerufen am 27.04.2022.

[5] Kondruss, B: Cyberangriffe auf Universitäten. https://konbriefing.com/de-topics/cyber-angriffe-universitaeten.html#. Abgerufen am 21.01.2022.

[6] Fischer, H, Heinz, M, Schlenker, L, Münster, S, Follert, F, Köhler, T (2017): Die Gamifizierung der Hochschullehre – Potenziale und Herausforderungen. In: Strahringer, S, Leyh, C (Hrsg), *Gamification und serious games. Grundlagen, Vorgehen und Anwendungen.* Springer Vieweg, Wiesbaden, Heidelberg.

[7] takeawaresecandlifemagazine04.

[8] Aengenheyster, S, Dörr, KM (2019): Praxishandbuch IT-Kommunikation. Springer Berlin Heidelberg, Berlin, Heidelberg.

[9] Langner, A: HMR_3_2018_Gamification-und-Playful-Business.

[10] Demografieportal - 2021: Altersstruktur im öffentlichen Dienst. https://www.demografie-portal.de/DE/Fakten/oeffentlicher-dienst-altersstruktur.html. Abgerufen am 20.01.2022.

[11] Roessler, I (2019): CHECK - Universitätsleitung in Deutschland, Gütersloh.

[12] working@office (2019): Motivationsspiele: Die etwas andere Art der Motivationssteigerung. Abwechslung im Arbeitsalltag. https://www.workingoffice.de/motivationsspiele/. Abgerufen am 22.08.2022.

[13] Sasse, Angela Prof. Dr. M., Hielscher, J, Friedauer, J, Menges, U, Pfeiffer, M (2022): Warum IT-Sicherheit in Organisationen einen Neustart braucht. In: , *Cyber-Sicherheit ist Chefinnen- und Chefsache! Tagungsband zum 18. Deutschen IT-Sicherheitskongress.* SecuMedia, Ingelheim.

[14] Heinz, M, Fischer, H (2020): Ausgespielt? Zu Risiken und Nebenwirkungen von Gamification. In: Köhler, T, Schoop, E, Kahnwald, N (Hrsg), *Gemeinschaften in Neuen Medien. Von hybriden Realitäten zu hybriden Gemeinschaften. 23. Workshop GeNeMe'20 Gemeinschaften in Neuen Medien : Dresden, 07.-09.10.2020 = Communities in new media. From hybrid realities to hybrid communities. : proceedings of 23rd Conference GeNeMe.* TUDpress, Dresden.

[15] game - Verband der deutschen Games-Branche e. V. (2022): Deutscher Games-Markt 2021 mit weiterem Umsatzsprung. https://www.game.de/marktdaten/deutscher-games-markt-2021-mit-weiterem-umsatzsprung/. Abgerufen am 23.08.2022.

[16] game - Verband der deutschen Games-Branche e. V. (2022): Marktdaten. Zahlen und Fakten. https://www.game.de/marktdaten/#Zahlen%20und%20Fakten. Abgerufen am 13.05.2022.

[17] game - Verband der deutschen Games-Branche e. V. (2022): game Fokus Serious Games. https://www.game.de/game-fokus-serious-games/. Abgerufen am 14.07.2022.

[18] Juul, J (2003): The game, the player, the world: looking for a heart of gameness, DiGRA Conference.

[19] Wesseloh, H, Schumann, M (2019): Einsatz von Gamification zum Fördern intrinsischer Motivation. Aktueller Stand der Forschung und Herleitung eines Forschungsmodells, online.

[20] Pokoyski, D, Matas, I, Fischer, M, Flury, E, Moyerer, V, Hellemann, N (21.02.-06.06.2022): Einsatz von Gamification zur Sensibilisierung für Informationssicherheit im Kontext deutscher Hochschulen. Abgerufen am 04.08.2022.

[21] Krapp, Andreas, Ryan, M, R: Selbstwirksamkeit und Lernmotivation. Eine kritische Betrachtung der Theorie von Bandura aus der Sicht der Selbstbestimmungstheorie und der pädagogisch-psychologischen Interessentheorie.

Copyright

[22] Sailer, M (Hrsg) (2016): Die Wirkung von Gamification auf Motivation und Leistung. Empirische Studien im Kontext manueller Arbeitsprozesse. Springer, Wiesbaden.
[23] Igel, C, Ullrich, C, Wessner, M (Hrsg) (2017): DeLFI 2017 - Bildungsräume. Tagung vom 5. bis 8. September 2017 in Chemnitz. Gesellschaft für Informatik, Bonn.
[24] Sailer, M, Homner, L (2020): The Gamification of Learning: a Meta-analysis. Educational Psychology Review, 32(1):77–112.
[25] Frühwirth, G (2020): Selbstbestimmt unterrichten dürfen – Kontrolle unterlassen können. Springer Fachmedien Wiesbaden, Wiesbaden.
[26] Mazarakis, A (2021): Gamification Reloaded. i-com, 20(3):279–294.
[27] Bezerra Rodrigues, RA (2020): GAMIFICATION IN ENGINEERING EDUCATION IN CANADA: A SYSTEMATIC REVIEW OF THE LITERATURE. Proceedings of the Canadian Engineering Education Association (CEEA).
[28] Stavropoulos, V (2018): Cybersecurity Culture Guidelines: Behavioural Aspects of Cybersecurity.
[29] MITRE Corporation (2021): ATT&CK Matrix for Enterprise. https://attack.mitre.org/. Abgerufen am 12.03.2022.
[30] Crowdstrike (2022): Die 14 häufigsten Cyberangriffe. https://www.crowdstrike.de/cybersecurity-101/cyberattacks/most-common-cyberattacks/. Abgerufen am 11.06.2022.
[31] Verizon (2022): DBIR. Data Breach Investigation Report.
[32] Bundesamt für Sicherheit in der Informationstechnik (n.a.): Open Vulnerability Assessment System (OpenVAS). https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Informationen-und-Empfehlungen/Freie-Software/Tools/OpenVAS/OpenVAS_node.html. Abgerufen am 17.06.2022.
[33] Reiser, H (2018): Kapitel 4: Social Engineering - der Faktor Mensch in der IT-Sicherheit. https://www.nm.ifi.lmu.de/teaching/Vorlesungen/2019ws/itsec/_skript/itsec-k4-v12.0.pdf. Abgerufen am 21.06.2022.
[34] Hader, JA (2019): Social Engineering. Wenn Angreifer Menschen statt Systeme hacken. https://www.maschinenmarkt.vogel.de/wenn-angreifer-menschen-statt-systeme-hacken-a-884707/. Abgerufen am 24.06.2022.
[35] n. a. (2021): Social Engineering Handbuch. Ein Leitfaden für die Praxis. https://digitalsecurityguide.eset.com/de/social-engineering-erkennen. Abgerufen am 25.06.2022.
[36] Laufenburg, R (2019): Social Engineering. Zehn beliebte Social-Engineering-Methoden im Überblick. https://it-service.network/blog/2019/03/29/social-engineering-methoden/. Abgerufen am 25.06.2022.
[37] n. a. (2022): Shoulder Surfing - eine unterschätzte Gefahr? https://www.ionos.de/digitalguide/server/sicherheit/shoulder-surfing/. Abgerufen am 25.06.2022.
[38] Autorengemeinschaft (2020): Spionage, Sabotage und Datendiebstahl – Wirtschaftsschutz in der vernetzten Welt. Studienbericht 2020. https://www.bitkom.org/sites/default/files/2020-02/200211_bitkom_studie_wirtschaftsschutz_2020_final.pdf. Abgerufen am 21.06.2022.
[39] Bundesamt für Sicherheit in der Informationstechnik (2019): Cyber-Sicherheits-Umfrage 2018. Cyber-Risiken & Schutzmaßnahmen in Unternehmen.
[40] Schumacher, S (2014): Die psychologischen Grundlagen des Social-Engineerings. Information - Wissenschaft & Praxis, 65(4-5).
[41] Kumpa, CM (2019): Die häufigsten Social-Engineering-Angriffe. https://netzpalaver.de/2019/04/03/die-haeufigsten-social-engineering-angriffe/. Abgerufen am 25.06.2022.
[42] Wikipedia (2005): Politik (Aristoteles). https://de.wikipedia.org/wiki/Politik_(Aristoteles)#Der_Mensch_als_zoon_politikon. Abgerufen am 03.04.2022.
[43] Mai, J (2021): Reziprozitäts-Effekt: Wie du mir, so ich dir. https://karrierebibel.de/reziprozitaet-gefaelligkeitsfalle/. Abgerufen am 02.04.2022.
[44] Jhala, N (10.07.2014): Network Scanning and Vulnerability Assessment with Report Generation. Masterarbeit, Nirma Universität.
[45] Weber, K, Schütz, AE, Fertig, T (2019): Grundlagen und Anwendung von Information Security Awareness. Springer Fachmedien Wiesbaden, Wiesbaden.
[46] Helisch, M, Pokoyski, D, Beyer, M, Reibenspies, W (Hrsg) (2009): Security Awareness. Neue Wege zur erfolgreichen Mitarbeiter-Sensibilisierung. 1. Auflage. Vieweg + Teubner, Wiesbaden.
[47] dasWirtschaftslexikon.com (2016): Identifikation und Loyalität. http://www.daswirtschaftslexikon.com/d/identifikation_und_loyalit%C3%A4t/identifikation_und_loyalit%C3%A4t.htm. Abgerufen am 24.08.2022.

Copyright

[48] Cunningham, M (2019): Denkfehler durch kognitive Verzerrungen. Psychologie trifft IT-Sicherheit. https://www.it-daily.net/it-sicherheit/cloud-security/psychologie-trifft-it-sicherheit. Abgerufen am 29.06.2022.
[49] n. a. (2022): Semiotik - Wie du Codes für deine Markensprache nutzt. https://blacklimedesign.de/designblog/semiotik/. Abgerufen am 29.06.2022.
[50] Stavropoulos, V (2018): TECHNICAL ANNEX: EVIDENCE REVIEWS. Review of Behavioural Sciences Research in the Field of Cybersecurity.
[51] Fogg, BJ (2022): Fogg Behaviour Model. https://behaviormodel.org/. Abgerufen am 24.08.2022.
[52] 13th European Conference on Game Based Learning.
[53] Pelz, A: Das Fogg Behavior Model - Nutzerverhalten verstehen. https://ux-ui-design.de/das-fogg-behavior-model-nutzerverhalten-und-ux-design/. Abgerufen am 25.03.2022.
[54] Eyal, N (2019): Hooked. Wie Sie Produkte erschaffen, die süchtig machen. 5. Auflage. REDLINE Verlag, München.
[55] Pieter, A, Fröhlich, M, Emrich, E, Papathanassiou, V (2010): Rationale Verhaltensalternativen und selbstbestimmtes Handeln als Komponenten des Gesundheitsverhaltens. Prävention und Gesundheitsförderung, 5(4):300–306.
[56] Hermann, D, Pöge, A (Hrsg) (2018): Kriminalsoziologie. Handbuch für Wissenschaft und Praxis. 1. Auflage. Nomos Verlagsgesellschaft mbH & Co. KG, Baden-Baden.
[57] StudySmarter UG: Grundlagen der Psychologie. Persönlichkeitsentwicklung. https://www.studysmarter.de/schule/psychologie/grundlagendisziplinen-der-psychologie/persoenlichkeitsentwicklung/. Abgerufen am 05.07.2022.
[58] Wikipedia Autorenschaft (2022): Big Five (Psychologie). https://de.wikipedia.org/wiki/Big_Five_(Psychologie). Abgerufen am 04.07.2022.
[59] Grüling, B: Videospiele im Alter: Warum immer mehr Senioren spielen. https://www.game.de/publikationen/videospiele-im-alter-warum-immer-mehr-senioren-spielen/. Abgerufen am 05.07.2022.
[60] StudySmarter UG: Grundlagen der Psychologie. Arten von Motiven. https://www.studysmarter.de/schule/psychologie/grundlagendisziplinen-der-psychologie/arten-von-motiven/. Abgerufen am 05.07.2022.
[61] Fathi, R, Fiedrich, F (2020): Digital Freiwillige in der Katastrophenhilfe - Motivationsfaktoren und Herausforderungen der Partizipation. Gesellschaft für Informatik e.V.
[62] Maslow, AH (1943): A theory of human motivation. Psychological Review, 50(4):370–396.
[63] Herzberg, F, Mausner, B, Snyderman, BB (1959): The motivation to work. 2. Auflage. Wiley; Chapman & Hall, New York, London.
[64] Elton Mayo (1949): The Social Problems of an Industrial Civilisation. Tijdschrift Voor Filosofie, 11(4):643–644.
[65] Jacobs, D, Mcgregor, D, Heil, G, Bennis, W, Stephens, DC (2004): Book Review Essay: Douglas Mcgregor: The Human Side of Enterprise in Peril. The Academy of Management Review, 29(2):293.
[66] Deci, EL, Ryan, RM (2008): Self-determination theory: A macrotheory of human motivation, development, and health. Canadian Psychology / Psychologie canadienne, 49(3):182–185.
[67] Stangl, W (2019): Online Lexikon für Psychologie und Pädagogik. Selbstbestimmungstheorie der Motivation. https://lexikon.stangl.eu/28413/selbstbestimmungstheorie-der-motivation. Abgerufen am 20.03.2022.
[68] Deci, EL, Ryan, RM (1993): Die Selbstbestimmungstheorie der Motivation und ihre Bedeutung für die Pädagogik. Zeitschrift für Pädagogik 39, 2:223–238.
[69] Thomas, AE, Müller, FH (2011): Skalen zur motivationalen Regulation beim Lernen von Schülerinnen und Schülern. Skalen zur akademischen Selbstregulation von Schüler/innen SRQ-A, online.
[70] Banfield, J, Wilkerson, B (2014): Increasing Student Intrinsic Motivation And Self-Efficacy Through Gamification Pedagogy. Contemporary Issues in Education Research (CIER), 7(4):291–298.
[71] Knaf, C (2018-2022): Motivationswelten - Für dich und deine Motivation. Extrinsische Motivation. https://www.motivationswelten.de/motivation/extrinsische/. Abgerufen am 29.05.2022.
[72] PodBean (26.05.2021): Motivationspsychologie. Zu sicherem Verhalten motivieren, 7. https://www.securityawarenessinsider.ch/e/motivationspsychologie-zu-sicherem-verhalten-motivieren/. Abgerufen am 27.03.2022.
[73] Schmidhuber, D, Krug, M, Aufderheide, T, Bühler, M: Interdisziplinäre Initiative "Gamification, Simulationen & Serious Games" an der HTWG in Zusammenarbeit mit anderen internationalen Hochschulen. Ein Webprojekt zur Bestandsaufnahme. https://www.htwg-

Copyright

konstanz.de/de/hochschule/einrichtungen/open-teaching-lab/open-space/small-digitalisation-projects/neugamification-simulations-serious-games/. Abgerufen am 07.09.2022.
[74] Wikipedia Autorenschaft (29.01.2022): Feedback (Kommunikation). https://de.wikipedia.org/wiki/Feedback_(Kommunikation). Abgerufen am 17.08.2022.
[75] Schroer, K: AIDA-Modell. https://www.bwl-lexikon.de/wiki/aida-modell/. Abgerufen am 27.04.2022.
[76] Seng, L (2018): Erinnern mit Gefühl. https://www.dasgehirn.info/denken/gedaechtnis/erinnern-mit-gefuehl. Abgerufen am 27.04.2022.
[77] TreeSolution Consulting GmbH (2020): Security Awareness Kampagnen. https://uploads-ssl.webflow.com/5be814fa637b425d212a7f53/5e673c66592da73b19f8b33a_brochure-campaigns-DE-04-web.pdf. Abgerufen am 07.07.2022.
[78] McCarthy, EJ (1971): Basic marketing. A managerial approach. 4. Auflage. Irwin; Irwin-Dorsey, Homewood/Ill., Georgetown/Ont.
[79] Studyflix (2022): Marketing Mix. https://studyflix.de/wirtschaft/marketing-mix-1418. Abgerufen am 07.07.2022.
[80] Sbrandolino, F (2021): 12 Ideen zur Verkaufsförderung, die Sie schnell umsetzen können. https://blog.hubspot.de/sales/verkaufsfoerderung. Abgerufen am 07.07.2022.
[81] Digital Guide IONOS (2018): Informationsüberflutung in Zeiten der Massenmedien. https://www.ionos.de/digitalguide/online-marketing/verkaufen-im-internet/informationsueberflutung-das-zuviel-an-werbung/. Abgerufen am 08.07.2022.
[82] Circlewise Institut (2016): Storytelling und Was passiert im Gedächtnis wirklich? Geschichten als eine Hälfte des Wissens. https://circlewise.org/blog/artikel/storytelling/. Abgerufen am 08.07.2022.
[83] PodBean (27.01.2021): Storytelling - Awareness mit Geschichten, 1. https://www.securityawarenessinsider.ch/e/storytelling-awareness-mit-geschichten/. Abgerufen am 08.07.2022.
[84] Helisch, M, Pokoyski, D (2009): Awareness Stories im Dialog. In: Helisch, M, Pokoyski, D, Beyer, M, Reibenspies, W (Hrsg), *Security Awareness. Neue Wege zur erfolgreichen Mitarbeiter-Sensibilisierung.* Vieweg + Teubner, Wiesbaden.
[85] Lönneker, J (2014): Zielgruppe war gestern – Mit Verfassungsmarketing zur strategischen Einordnung von Kauf- und Konsumverhalten. In: Halfmann, M (Hrsg), *Zielgruppen im Konsumentenmarketing.* Springer Fachmedien Wiesbaden, Wiesbaden.
[86] Meisen, H (16.05.2008): Von der Zielgruppe zum Verfassungsmarketing - bringen Sie Ihre Kunden in Weinstimmung, Bernkastel-Kues.
[87] HRK (2018): Informationssicherheit als strategische Aufgabe der Hochschulleitung. Empfehlung der 25. HRK-Mitgliederversammlung vom 06.11.2018. https://www.hrk.de/positionen/beschluss/detail/informationssicherheit-als-strategische-aufgabe-der-hochschulleitung/. Abgerufen am 10.07.2022.
[88] Kühl, S (2007): Von der Hochschulreform zum Veränderungsmanagement von Universitäten? Verwaltung & Management, 13(4):212–216.
[89] Vinke, P (2011): Need-States-basierte Segmentierung. Märkte konsumentengerecht segmentieren mit Motive&Use-Segmentation. planung&analyse, (5).
[90] Schulmeister, R (2014): Auf der Suche nach Determinanten des Studienerfolgs. In: Brockmann, J., Pilniok, A. (Hrsg), *Studieneingangsphase in der Rechtswissenschaft.* Nomos, Baden-Baden.
[91] Metzger, C, Schulmeister, R, Martens, T (2012): Motivation und Lehrorganisation als Elemente von Lernkultur. Zeitschrift für Hochschulentwicklung, 7(3).
[92] Baumann, N, em Kuhl, J (2019): Dorsch - Lexikon der Psychologie. Fremdbestimmtheit. https://dorsch.hogrefe.com/stichwort/fremdbestimmtheit. Abgerufen am 26.06.2022.
[93] Wahl, D (2002): Mit Training vom trägen Wissen zum kompetenten Handeln? Zeitschrift für Pädagogik 48:227-241.
[94] Csikszentmihalyi, M (1991): Flow. The psychology of optimal experience. HarperPerennial, New York.
[95] Grüblbauer, J (2012): Status Quo der Interessenforschung: vom Interesse als Persönlichkeitsmerkmal zu situativem Involvement, online.
[96] Zander, S, Heidig, S (2018): Motivationsdesign bei der Konzeption multimedialer Lernumgebungen. In: Kracht, S, Niedostadek, A, Sensburg, P (Hrsg), *Praxishandbuch Professionelle Mediation.* Springer Berlin Heidelberg, Berlin, Heidelberg.
[97] Reinmann, G: Didaktisches Handeln. Die Beziehung zwischen Lerntheorien und Didaktischem Design. In: , *L3T. Lehrbuch für Lernen und Lehren mit Technologien*.

Copyright

[98] Jaehnig, J (2021): Was ist Verhaltenslernen? https://alai-web.org/de/was-ist-verhaltenslernen/. Abgerufen am 19.05.2022.
[99] Urton, K: Selbstwirksamkeitserwartung. Was bedingt sie und wie kann sie gefördert werden?, online.
[100] Franzkowiak, P, Franke, A (2018): Stress und Stressbewältigung. BZGA - Federal Centre for Health Education, online.
[101] Stiller Dipl-Kfr., G (2017): Kognitiv wirkende Reize. http://www.wirtschaftslexikon24.com/e/kognitiv-wirkende-reize/kognitiv-wirkende-reize.htm. Abgerufen am 19.04.2022.
[102] Hielscher, J (Hrsg): Warum IT-Sicherheit in Organisationen einen Neustart braucht - 18. BSI Kongress - Sasse et al_.
[103] Growth Engineering (2016): What Is Game-Based Learning? https://www.growthengineering.co.uk/what-is-game-based-learning/. Abgerufen am 26.04.2022.
[104] Fabula Games GmbH (2022): Projekt: The Secret of Photonorvin. Kunde: Bayer AG. https://fabula-games.de/serious-games/informationssicherheit-gamification-referenz/. Abgerufen am 11.05.2022.
[105] Fabula Games GmbH (2020): myRo P7 Erklärvideo. https://youtu.be/Vtgt2lOecMc. Abgerufen am 08.05.2022.
[106] Fabula Games GmbH (2020): myRo P7 - Serious Game für die Informationssicherheit: Webinar-Aufzeichnung. https://youtu.be/e5hOqwirEY0. Abgerufen am 18.05.2022.
[107] Tolks, D, Sailer, M (2021): Gamification als didaktisches Mittel in der Hochschulbildung. In: , *Digitalisierung in Studium und Lehre gemeinsam gestalten. Innovative Formate, Strategien und Netzwerke.* Springer VS, Wiesbaden.
[108] Robin Hunicke, Marc G. Leblanc, Robert Zubek: MDA : A Formal Approach to Game Design and Game Research. In: , *Proceedings of the Challenges in Game AI Workshop, Nineteenth National Conference on Artificial Intelligence*.
[109] Katsantonis, NM, I. Kotini, P. Fouliras, I. Mavridis (2019): Conceptual Framework for Developing Cyber Security Serious Games. In: , *2019 IEEE Global Engineering Education Conference (EDUCON)*.
[110] Katsantonis, M, Mavridis, I (2021): Evaluation of HackLearn COFELET Game User Experience for Cybersecurity Education. International Journal of Serious Games, 8(3):3–24.
[111] Lim, T., Carvalho, M. B., Bellotti, F., Arnab, S., Freitas, S., Louchart, S., Suttie, N., Berta, R., De Gloria, A. (2016): The LM-GM framework for Serious Games Analysis. https://seriousgamessociety.org/wp-content/uploads/2016/09/lmgm_framework.pdf. Abgerufen am 20.07.2022.
[112] Carvalho, MB, Bellotti, F, Berta, R, Gloria, A de, Sedano, CI, Hauge, JB, Hu, J, Rauterberg, M (2015): An activity theory-based model for serious games analysis and conceptual design. Computers & Education, 87:166–181.
[113] Chou, Y: Actionable Gamification. Beyond Points, Badges, and Leaderboards.
[114] Hosang, K (2022): Heldenreise: 10 Schritte-Prozess für deine Entwicklung. https://karlhosang.de/heldenreise/. Abgerufen am 26.08.2022.
[115] Campbell, J (1949): Der Heros in tausend Gestalten. S. Fischer, Frankfurt am Main.
[116] Hosang, K (2020): Gamification-Elemente:. 3 Ebenen der Gamification-Pyramide. https://karlhosang.de/gamification-elemente/. Abgerufen am 26.07.2022.
[117] Deißler, N (2013): Spielelemente - Das Herzstück der Spiele. http://digitalfit.de/spielelemente-das-herzstueck-der-spiele/. Abgerufen am 26.07.2022.
[118] Fromme, J, Jörissen, B, Unger, A (2008): Computerspiele und Videogames in formellen und informellen Bildungskontexten | Computer- and Videogames in Formal and Informal Educational Contexts. MedienPädagogik: Zeitschrift für Theorie und Praxis der Medienbildung, 15(Computerspiele und Videogames):1–23.
[119] OTL Hochschule Konstanz: Interdisziplinäre Initiative "Gamification, Simulationen & Serious Games" an der HTWG in Zusammenarbeit mit anderen internationalen Hochschulen. Ein Webprojekt zur Bestandsaufnahme. https://www.htwg-konstanz.de/de/hochschule/einrichtungen/open-teaching-lab/open-space/small-digitalisation-projects/neugamification-simulations-serious-games/. Abgerufen am 28.07.2022.
[120] Rackwitz, R (2016): Gamification als Führungselement. Warum Führungskräfte über Gamification nachdenken sollten. https://www.zielbar.de/magazin/gamification-fuehrungskraefte-10211/. Abgerufen am 28.07.2022.

Copyright

[121] Radikant GmbH: UI & UX Design. Was ist der Unterschied zwischen User Interface und User Experience Design? https://www.radikant.com/wissen/unterschied-ux-ui-design/. Abgerufen am 28.07.2022.
[122] Tralau, M: Productive games. Dissertation, Shaker Verlag; Helmut-Schmidt-Universität.
[123] Becker, W, Metz, M (2022): Digitale Lernwelten – Serious Games und Gamification. Didaktik, Anwendungen und Erfahrungen in der Beruflichen Bildung. Springer VS, Wiesbaden.
[124] Institut für Ludologie: Spielertypen. https://www.ludologie.de/spielforschung/spielertypen/. Abgerufen am 10.01.2022.
[125] Bartle, RA (1996): HEARTS, CLUBS, DIAMONDS, SPADES: PLAYERS WHO SUIT MUDS. https://mud.co.uk/richard/hcds.htm. Abgerufen am 22.03.2022.
[126] Burmester, N (2022): The Bartle Test of Gamer Psychology - Gamer Types. https://www.gamify.com/gamification-blog/the-make-up-of-gamers-the-bartle-test-of-gamer-psychology. Abgerufen am 22.03.2022.
[127] Mostafa, M, Faragallah, OS (2019): Development of Serious Games for Teaching Information Security Courses. IEEE Access, 7:169293–169305.
[128] Wirtz, B (2021): The Complete Guide to Video Game Genres: From Scrollers, Shooters, to Sports. https://www.gamedesigning.org/gaming/video-game-genres/. Abgerufen am 05.01.2022.
[129] Bundesministerium für Digitales und Verkehr (2022): Computerspieleförderung-Projekte. https://www.bmvi.de/SiteGlobals/Forms/Listen/DE/Computerspielfoerderung-Projekte/computerspielfoerderung-projekte_Formular.html?resourceId=460868&input_=460836&pageLocale=de&templateQueryString=&cl2Categories_Themen3=&cl2Categories_Themen3.GROUP=1&cl2Categories_Themen=&cl2Categories_Themen.GROUP=1&cl2Categories_Themen2=abgeschlossen&cl2Categories_Themen2.GROUP=1&cl2Categories_Themen4=&cl2Categories_Themen4.GROUP=1&submit=Ergebnisse+filtern&resultsPerPage=12&resultsPerPage.GROUP=1&selectSort=commonSortDate_dt+desc&selectSort.GROUP=1. Abgerufen am 31.07.2022.
[130] Nitschke, S (2022): Umfrage_212741. Einsatz von Gamification an deutschen Hochschulen/Universitäten zum Zweck der Sensibilisierung für Informationssicherheit, Umfrage mit limesurvey.
[131] Nerdinger, FW, Blickle, G, Schaper, N (2011): Arbeits- und Organisationspsychologie. Mit 34 Tabellen. 2. Auflage. Springer, Berlin, Heidelberg.
[132] Behnke, D (2019): Was ist Gamification – und was ist es nicht?! https://digital-spielend-lernen.de/was-ist-gamification-und-was-ist-es-nicht. Abgerufen am 04.08.2022.
[133] Behnke, D (2020): Spiele und Game-Based Learning. https://digital-spielend-lernen.de/wp-content/uploads/2020/02/Spiele-und-Game-Based-Learning.pdf. Abgerufen am 04.08.2022.
[134] Behnke, D (2018): Chocolate-Covered Broccoli – Wenn Lerninhalte und Spielelemente NICHT zusammenpassen. https://digital-spielend-lernen.de/chocolate-covered-broccoli-wenn-lerninhalte-und-spielelemente-nicht-zusammenpassen. Abgerufen am 04.08.2022.
[135] Finster, R, Grogorick, L, Robra-Bissantz, S (2019): Motivation and Technology Use. Sind bescheidene Masterminds wirklich konfliktscheu? Der Einfluss von Persönlichkeit und Spielertypen auf Spielelemente in spielbasierten Lernanwendungen. https://dl.gi.de/bitstream/handle/20.500.12116/34905/geneme2019-39.pdf?sequence=1&isAllowed=y. Abgerufen am 07.08.2022.
[136] Scholl, M: Serious Games für KMU im produzierenden Gewerbe: Social Engineering und Security Risk Management. Für das Projekt "Mittelstand 4.0-Kompetenzzentrum Stuttgart". Technische Hochschule, Wildau.
[137] Fritz, J (2011): Wie Computerspieler ins Spiel kommen. Theorien und Modelle zur Nutzung und Wirkung virtueller Spielwelten. Vistas, Berlin.
[138] Rheinberg, F, Vollmeyer, R, Engeser, S (2003): Die Erfassung des Flow-Erlebens. In: Stiensmeier-Pelster, J., Rheinberg, F. (Hrsg), *Diagnostik von Motivation und Selstkonzept.* Hogrefe, Göttingen.
[139] Julius-Maximilians-Universität Würzburg: Potentialanalyse/Kompetenzprofil. https://www.uni-wuerzburg.de/career/beratung/potentialanalyse-kompetenzprofil/. Abgerufen am 19.08.2022.

Copyright

11. Bilderverzeichnis

Bild 1: Altersstruktur der Beschäftigten im öffentlichen Dienst, 2020 ... 10
Bild 2: Ergebnisse der Auswertung von 81 Biografien an 81 deutschen Universitäten ... 10
Bild 3: nicht ausgenutzte Potenziale von Games ... 15
Bild 4: Unterscheidung Serious Game und Gamification ... 16
Bild 5: Studien zu Trainings mit Gamification-Kontext ... 18
Bild 6: Studien im E-Learning mit Gamification-Kontext ... 19
Bild 7: Darstellung eines Angriffsverlaufs im Mitre Att&ck Navigator ... 23
Bild 8: Entwicklung der Verwendung von Ransomware für Cyberangriffe ... 25
Bild 9: Hauptangriffswege zum Eindringen in fremde Systeme ... 26
Bild 10: Top 3 Angriffscluster im Bildungssektor ... 27
Bild 11: Verlauf der Angriffsmethoden im Cluster „Angriffe auf Webanwendungen“ ... 27
Bild 12: Durchschnittliche Anzahl an Angriffsschritten ... 28
Bild 13: Ursachen von Informationssicherheitsvorfällen ... 30
Bild 14: Prozess der Verhaltensbildung ... 37
Bild 15: Darstellung des Fogg-Verhaltensmodells ... 38
Bild 16: Modelle der Persönlichkeitstypen ... 44
Bild 17: mögliche Ausprägungen der einzelnen Persönlichkeitstypen im „Big Five“-Modell ... 45
Bild 18: Voraussetzung für das Zustandekommen einer Handlung ... 48
Bild 19: Darstellung der vier Typen der extrinsischen Motivation ... 52
Bild 20: Kategorien von Nudges ... 54
Bild 21: emotionales Plakat ... 57
Bild 22: Phishing-Mail an der HSA mit Erläuterungen zu Identifikationsmerkmalen ... 57
Bild 23: Bereitstellung eines online-Kurses in der moodle-Lernumgebung ... 58
Bild 24: Dashboard-Ansicht der kostenfreien Phishing-Simulation „gophish“ ... 58
Bild 25: Marketing-Mix ... 59
Bild 26: Informationsreizüberflutung in den verschiedenen Altersklassen ... 60
Bild 27: verändertes Awareness-Konzept ... 63
Bild 28: Spannungsfeld der Informationssicherheit ... 65
Bild 29: Facetten der Informationssicherheit ... 66
Bild 30: mögliche Anlässe für Informationssicherheit ... 67
Bild 31: Profile unterschiedlicher Lernmotivation (5-Klassen-Lösung) ... 73
Bild 32: Gründe für Nicht-Interesse ... 77
Bild 33: Strategien zur Förderung des Selbstwirksamkeitserlebens ... 81
Bild 34: Szene aus dem Serious Game „myRo P7“ ... 87
Bild 35: Kreislauf eines erfolgreichen Produkts ... 88
Bild 36: abgewandeltes MDA-Framework ... 91
Bild 37: Einsatz von Gamification ... 91
Bild 38: COFELET-Framework ... 92
Bild 39: 8 Kernantriebe für Verhalten ... 94
Bild 40: Einordnung der Spielelemente in die Spielphasen ... 100
Bild 41: Einordnung der Spielelemente in das MDA-Framework ... 101
Bild 42: Merkmale für ein erfolgreiches Spiel ... 106
Bild 43: Spielertypen nach Bartle ... 108
Bild 44: Vorgehensweise zur Entwicklung der Anwendung ... 116
Bild 45: Zielgruppen an der Hochschule Anhalt ... 117
Bild 46: Soll-Profil für die Zielgruppe „sachbearbeitend“ ... 122
Bild 47: beispielhafte Darstellung für hochschulinterne Abzeichen ... 127
Bild 48: Zuordnung der Funktionen zu den Spielertypen ... 128
Bild 49: QR-Code des erstellten Bounds ... 131
Bild 50: Ablauf der Aufgabe 11 im selbst erstellten Bound ... 134
Bild 51: beispielhafte Darstellung von Soll- und Ist-Kompetenz-Profil für Stufe 1 ... 137
Bild 52: Zusammenspiel der Security Awareness ... 140

Copyright

12. Tabellenverzeichnis

Tabelle 1: häufigste Arten von Cyberangriffen 25
Tabelle 2: Weitere Social Engineering-Methoden 30
Tabelle 3: weitere Formen des digitalen Social Engineering 31
Tabelle 4: Merkmale der Motivationen 53
Tabelle 5: Einordnung der Kernantriebe in die Phasen der Heldenreise 95
Tabelle 6: Einordnung der Game-Design-Elemente nach Art und psychologischem Bedürfnis 103
Tabelle 7: Zuordnung der verschiedenen Typen zum Octalysis-Framework 108
Tabelle 8: Spielgenres 110
Tabelle 9: Wichtigste Kompetenzen für schützenswerte Hochschulbereiche 115
Tabelle 10: Projektion der BrainHex-Spielertypen auf die Bartle-Spielertypen 118
Tabelle 11: Definition der Kompetenzstufen 121
Tabelle 12: erweiterte Grundkenntnisse für die ausgewählte Zielgruppe 123
Tabelle 13: Darstellung von zu erlernendem Wissen und Nutzen für die ausgewählte Zielgruppe 123
Tabelle 14: Kenntnisse für die ausgewählte Zielgruppe in der Stufe 2 123
Tabelle 15: Übersicht der im online- und offline-Medium verwendeten Spielelemente 127
Tabelle 16: Checkliste für die Einhaltung einer hohen Selbstwirksamkeit 136

Copyright

13. Anhang

Anlage 1: Fragebogen zur Ermittlung der Spielertypen

Quelle: http://matthewbarr.co.uk/bartle/ (abgerufen am 31.07.2022)

Copyright

The Bartle Test of Gamer Psychology

The Bartle Test classifies players of multiplayer online games (including MUDs and MMORPGs) into categories based on Bartle's taxonomy of player types. Each player type (Socialiser, Explorer, Achiever and Killer) is defined by the gaming elements which they find most enjoyable.

Which is more enjoyable to you?

○ Killing a big monster ○ Bragging about it to your friends

Which do you enjoy more in quests?

○ Getting involved in the storyline ○ Getting the rewards at the end

Would you rather be:

○ Popular? ○ Wealthy?

Which do you enjoy more in an online game?

○ Getting the latest gossip ○ Getting a new item

Which would you rather have, as a player in an online game?

○ A private channel, over which you and your friends can communicate ○ Your own house, worth millions of gold coins

Which would you enjoy more as an online game player?

○ Running your own tavern? ○ Making your own maps of the world, then selling them

What's more important in an online game to you?

○ The number of people ○ The number of areas to explore

What's more important to you?

○ The quality of roleplaying in an online game ○ The uniqueness of the features, and game mechanic

You are being chased by a monster in an online game. Do you:

○ Ask a friend for help in killing it ○ Hide somewhere you know the monster won't follow?

You're a player in an online game, and about to go into an unknown dungeon. You have your choice of one more person for your party. Do you bring:

○ A bard, who's a good friend of yours and who's great for entertaining you and your friends ○ A wizard, to identify the items that you find there?

Would you rather

○ Vanquish your enemies ○ Convince your enemies to work for you, not against you?

Which is more exciting?

○ A well-roleplayed scenario ○ A deadly battle

Which would you enjoy more?

○ Winning a duel with another player ○ Getting accepted by a clan (a group of other players)

What's worse:

○ To be without power ○ To be without friends?

Would you rather:

○ Hear what someone has to say ○ Show them the sharp blade of your axe?

Copyright

In an online game, a new area opens up. Which do you look forward to more?

○ Exploring the new area, and finding out its history ○ Being the first to get the new equipment from the area

In an online game, would you rather be known as:

○ Someone who can run from any two points in the world, and really knows their way around ○ The person with the best, most unique equipment in the game?

Would you rather:

○ Become a hero faster than your friends ○ Know more secrets than your friends?

Would you rather:

○ Know where to find things ○ Know how to get things?

Which would you rather do:

○ Solve a riddle no one else has solved ○ Getting to a certain experience level faster than anyone else?

In an online game, would rather be known for

○ Knowledge ○ Power?

Would you rather:

○ Defeat an enemy ○ Explore a new area?

If you're alone in an area, do you think:

○ It's safe to explore ○ You'll have to look elsewhere for prey?

You learn that another player is planning your demise. Do you:

○ Go to an area your opponent is unfamiliar with and prepare there ○ Attack them before he attacks you?

You meet a new player. Do you think of them as:

○ Someone who can appreciate your knowledge of the game ○ As potential prey?

In an online game, would you rather:

○ Have a sword twice as powerful as any other in the game ○ Be the most feared person in the game?

In an online game, would you be more prone to brag about:

○ How many other players you've killed ○ Your equipment?

Would you rather have:

○ A spell to damage other players ○ A spell that increases the rate at which you gain experience points?

Would you rather receive as a quest reward:

○ Experience points ○ A wand with 3 charges of a spell that lets you control other players, against their will?

When playing a video game, is it more fun to:

○ Have the highest score on the list ○ Beat your best friend one-on-one?

copyright

Anlage 2: Interviews

Quelle: eigene Befragung

Copyright

EXPERTENBEFRAGUNG

01

03
2022

BEFRAGUNG ZUR MASTERARBEIT:
„EINSATZ VON GAMIFICATION ZUR SENSIBILISIERUNG FÜR INFORMATIONSSICHERHEIT IM KONTEXT DEUTSCHER HOCHSCHULEN"

Expert-Time

Abbildung 1: Dietmar Pokoyski.
Quelle: https://www.take-aware-events.com/speaker/pokoyski

EINSATZ VON GAMIFICATION

Fragen an Dietmar Pokoyski

Zur Person

Dietmar Pokoyski ist Gründer und Geschäftsführer der Awareness-Agentur known_sense aus Köln, Mitorganisator der TAKE AWARE EVENTS und gemeinsam mit Michael Helisch Autor des einzigen Fachbuchs zum Thema Security Awareness in Deutschland. Seit 2005 hat er Awareness-Kampagnen der internen Kommunikation sowie Gamification Events für Mitarbeiter von mehr als 100 Unternehmen in 60 Ländern und 30 Sprachen durchgeführt. Mit known_sense erhielt er zahlreiche Auszeichnungen der Sicherheitsbranche, u. a. den „IT-Sicherheitspreis NRW" (2007) sowie den „OSPA – Outstanding Security Performance Award" (2015) für eine „Herausragende Initiative für Sicherheitsschulungen".

Quelle: https://www.take-aware-events.com/speaker/pokoyski

Gamification ist durch ihre systemischen Bezüge ein erweiterter Rahmen der klassischen Lerntheorie.

Er ist mit Michael Helisch Autor des einzigen Fachbuchs zum Thema Security Awareness in Deutschland und Gründer der Awareness-Agentur known_sense in Köln. Seit 2002 sensibilisiert Dietmar Pokoyski in gamifizierten Events Unternehmen zum Thema Informationssicherheit. In der Befragung spricht er u. a. über die Kunst, eine gute Story zu erarbeiten und mit einer gamifizierten Lösung gekonnt in Szene zu setzen.

1. Herr Pokoyski Sie haben 2002 das Unternehmen known_sense gegründet. Ihr Slogan lautet: „awareness you can touch". Was genau meinen Sie damit?

Eine unserer Kernbotschaften lautet „Wer Menschen sensibilisieren will, muss sie berühren." Der Claim spielt also erstens darauf an, dass wir nachhaltige Awareness nur dadurch erreichen können, die Zielgruppen auch emotional anzusprechen, um Security sichtbar werden zu lassen und mit mehr als nur Compliance bzw. Prozessen zur Sicherung dieser zu assoziieren. Zweitens ist gemeint, wie es da steht, also dass wir unsere Aufgabe primär darin sehen, Kommunikationsbeschleuniger zu entwickeln, die man anfassen kann. Ausschließlich digitale Awareness-Kampagnen funktionieren nachweislich nicht. Sensibilisierung braucht einen ausgeglichen Mix aus digital und analog. Und wir positionieren uns sehr stark im Analogen, im Zwischenmenschlichen, in der systemischen Kommunikation – frei nach dem Motto „Talking Security", also dem Sprechen über Sicherheit, weil der Diskurs der wichtigste Enabler von Awareness ist.

2. Ich habe gesehen, dass Sie eine Kooperation mit der Hochschule Niederrhein gestartet haben. Dürfen Sie mir sagen, worum es in dieser Kooperation geht?

Wir entwickeln gemeinsam für einen guten Kunden gamifizierte Trainingsmaterialien, also quasi Awarenessspiele, ein größeres Projekt. Aber wir wollen auch in Zukunft kooperieren – bei Projekten, ggf. im Rahmen von Events, auf jeden Fall in Bezug auf Know-how-Transfer. Das funktioniert gut, weil wir mit Prof. Matthias Mehrtens schon sehr gut zusammengearbeitet haben im Rahmen von Awareness-Maßnahmen für seinen früheren Arbeitgeber Kärcher.

3. Wissen Sie, welche Merkmale ausschlaggebend sind für die Tauglichkeit von Gamification oder Serious Games an deutschen Hochschulen?

Ich würde zumindest theoretisch keine so harte Linie ziehen zwischen Unternehmen und Organisationen aus dem Bildungsbereich wie z. B. Hochschulen. Zwar sollte man meinen, Hochschulen wären aufgrund ihres Bildungsauftrags näher dran an didaktischen Innovationen, die Gamification in den letzten 2 Jahrzehnten über uns ausgegossen hat – aber dem ist leider nicht so. Hochschulen leiden in Bezug auf die Akzeptanz von z. B. echter diskursiver oder konstruktivistischer Didaktik offenbar immer noch an einem gewissen Eskapismus, jedenfalls ist es in der Tat leichter, Unternehmen, inzwischen selbst kleinere KMU, von Gamification zu überzeugen als die meisten Hochschulen – von Ausnahmen abgesehen. Z.B. hatten wir bereits vor knapp 15 Jahren Tools für die RUB in Bochum gebaut, die TH Wildau ist dem Gamification-Thema ebenso recht nahe.

4. Was macht ein gutes Serious Game bzw. eine gute gamifizierte Lösung / Anwendung aus?

Sie involviert die Menschen, eben auch emotional, sie ist idealerweise teamfähig, lässt Anforderungen an die InfoSec in einem geschützten Rahmen einüben, gibt in diesem Kontext ein produktives Feedback, nutzt vielleicht bekannte Popcodes, um schwierige Themen „leichter" zu kommunizieren. Sie erzählt eine gute, aber auch wertvolle Story – Thema „Purpose"! Sie lässt sich im Sinne einer widerspruchsfreien, integrierten Kommunikation mit anderen Maßnahmen gut verbinden und schafft so Synergien auf allen Kanälen

5. Wie findet man eine zu einem bestimmten Thema passende und spannende Story?

Es gibt zahlreiche Methoden des Storytelling bzw. systemische Tools, die Narrative triggern. Wir bieten hierzu Workshops auf Grundlage diverser narrativer Kreationsmodule an, oft nehmen wir z. B. auch unseren Illustrator zum Live-Zeichenen mit zu Kunden-Workshops, dann etwa, wenn wir eine Leitfigur entwickeln sollen oder eine komplette Figurenfamilie für Awareness-Comics. Sehr hilfreich ist u.a. das Buch „Die systemsiche Metaphern-Schatzkiste" von Holger Lindemann.

6. Was muss bei der Gestaltung eines Serious Game / einer gamifizierten Lösung beachtet werden damit es erfolgreich in einer Hochschule angewendet wird?

Für Hochschulen gilt dasselbe wie für andere Organisationen – on top käme allenfalls, wenn z.B. eine Entwicklung forschungsgestützt erfolgen soll. Aber das haben wir eh dauernd im Gepäck, z. B. tiefenpsychologischer Wirkungsanalyse, die Spielentwicklung bei uns stets begleitet.

7. Gibt es Hochschulen in Deutschland, die Serious Games / Gamification zur Sensibilisierung einsetzen?

Wie bereits erwähnt, fallen mir die RUB oder die TH Wildau ein.

8. Hat der Einsatz von Gamification die Haltung der Hochschulen auf die Stellung der Informationssicherheit verändert?

Das kann ich kaum beurteilen. Wie gesagt, partnern wir mit Hochschulen und die, die mit uns arbeiten, haben sicherlich eine andere Sicht auf die InfoSec durch Awarenss und den Einsatz von Gamification – etwa die TH Wildau oder die Hochschule Niederrhein. Die TH Wildau ist und war in den letzten 10 Jahren in zahlreiche Forschungsprojekte zum Thema Gamification in der Sensibilisierung involviert – für Schulen oder KMU. Awareness und Gamification sind also durchaus ein Thema für Forschung und Projekte.

Copyright

Informationen zu known_sense

Nach Stationen in Verlagen und in der TV- und Videoproduktions-Branche mit Filmen für ARD, arte, Canon oder Philips sowie als Berater und Creative Director für verschiedene Kommunikationsagenturen wurde known_sense 2002 von Dietmar Pokoyski gegründet.

In Folge von Kreationsprojekten für Werbemittel und Retail im Spielebereich mit Produktentwicklungen für unter anderem ASS Altenburg, Cartamundi, und dem Moses-Verlag sowie Marken wie Disney, Mattel oder UEFA entstand als eine Biertischidee das Kartenspiel „Computerluder – das Virusquartett", das als erstes nicht-technisches IT-Tool als Produkt des Monats bei ComputerPartner ausgezeichnet wurde und Rezensionen bei brand eins, manager magazin, Spiegel-Online, WDR, ZDF u. v. m. erhielt.

Quelle: https://www.known-sense.de/kopie-home

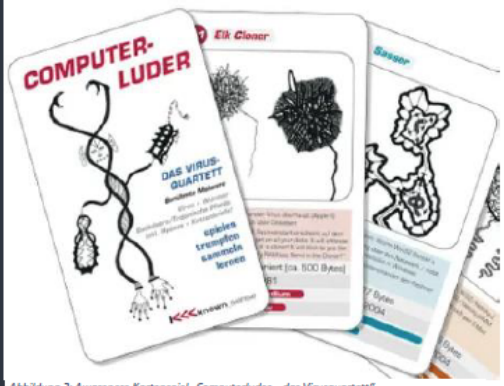


Abbildung 2: Awareness-Kartenspiel „Computerluder – das Virusquartett"
Quelle: https://www.known-sense.de/newpage6354ae55

Was Sie über Gamification wirklich wissen müssen.

Fragen an einen Experten aus der Security-Awareness-Branche.

9. Welche weiteren Erfahrungen haben Sie mit solchen Tools bei deutschen Hochschulen gemacht?

Es ist manchmal schwierig, in einen emotionalen Flow zu geraten, weil Teilnehmer aus Hochschulen bei gamifizierten Tools häufig nicht aus ihrer intellektuellen, methodischen Metaebene ins Spiel finden können. Das braucht dann manchmal eine etwas längere Warming-up, um das Denken zu erden.

10. Ist Gamification bzw. der Einsatz von Serious Games auch in der Führungsebene von Unternehmen / Hochschulen das richtige Werkzeug (um die notwendige Aufmerksamkeit für das Thema zu schaffen)?

„Spielen" wird in zahlreichen Führungsebenen grundsätzlich immer noch widerständlich als „bloßer Zeitvertreib" betrachtet, aber die Reaktanz bröckelt, je erfolgreicher Gamification im Kontext Weiterbildung oder Change eingesetzt wird. Manager haben leider häufig Angst, sich vor ihren Teams zu blamieren. Wenn der Chef verliert, braucht er eine souveräne Haltung – das ist leider nicht jedem gegeben.

"Um ein gutes Serious Game zu gestalten, benötigen Sie eine ganze Menge Wissen über…"

Psychologie, insbes. Tiefenpsychologie und Gestalt, Design, Storytelling, diskursive und konstruktivistische Didaktik

11. Was sind Ihrer Meinung nach die Vorteile von Gamification oder Serious Games im Gegensatz zu konventionellen Lehr- und Lernmethoden?

Teilweise hatte ich das ja schon in den letzten Antworten benannt, zumindest implizit. Spielend lernen heißt, sich mit Erfahrungswissen zu konfrontieren, teilweise mit anderen im Team zu kollaborieren und Soziales bzw. Kreativität auszuleben. Ohne Spiele keine Kreativität. Nichts wäre langweiliger als ein unkreatives, asoziales Lernen, z. B. Auswendiglernen vom Blatt, das ist öder Bullshit. Das spielerische Lernen hilft uns bei unserem Drang, uns weiterentwickeln zu müssen, ohne Entwicklung würden wir sterben. Das wäre ein ähnlicher Tod wie das Eingesperrtsein in einer Burg, in der wir zwar sicher sind, aber nichts tun können. Eine Art Goldener-Käfig-Effekt. Sicherheit und Spielen sind sich aber auch über diese Metapher hinaus sehr ähnlich. Spiele bestehen u.a. aus regelbasierten Konflikten – genauso wie Sicherheit auch.

12. Wie kann die Effektivität und Nachhaltigkeit (der „Belohnungseffekt" für erfolgreiches Lernen) von Gamification/Serious Games gemessen werden?

Ich halte die klassische betriebswirtschaftliche Erbsenzählerei, d. h. quantitative Methoden, für völlig abgewrackt und daher absolut überholt. Eines unserer Kernbotschaften lautet: Erzählen statt Zählen D.h. führen Sie zweistündige Interviews mit Spielern als Probanden durch und erstellen Sie qualitative Wirkungsanalysen auf Basis tiefenpsychologischer Forschung. Damit machen Sie Erfolge nicht nur sichtbar, sondern generieren über die Probanden auch gute Ideen oder Geschichten für weitere Maßnahmen oder Spiele.

13. Warum ist Lernen nicht ausreichend, um erfolgreich zu sensibilisieren?

Das Thema Sicherheit ist grundsätzlich sehr emotional aufgeladen, siehe auch Phänomene wie „gefühlte Sicherheit", „German Angst" etc. Hinzu kommt, dass alle neueren Angriffsvektoren mit „alten" manipulativen Methoden arbeiten, es wird sehr schnell sehr menschlich, wenn der Social Engineer etwas herausfinden will und mich eben auf einer sozialen Ebene anspricht. Wir Menschen sind nun mal soziale Wesen, die Anerkennung, Angst, Neugier für unsere Entwicklung benötigen. Wir können uns dann z. B. in Kommunikationssituationen mit Fremden verhalten, als würden wir ständig angegriffen, das wäre sozial unsinnig und unerwünscht.- Also müssen wir neben intellektuellen, rationalen, kognitiven Ebenen auch intuitiv, emotionale Intelligenz nutzen. Das kann man zwar einüben, aber nur in einem erweiterten Rahmen der klassischen Lerntheorie. Gamification mit ihren systemischen Bezügen ist so eine Erweiterung, wo wir sagen, die reine kognitive Weitergabe von Wissen macht nur ein paar Promille aus, um resilient zu sein. Awareness hat daher stärker mit z. B. Aufmerksamkeit – auch der eigenen, nach innen gerichteten – mithin so etwas wie Achtsamkeit, Mindfulness zu tun, als mit reinem Know-how-Transfer.

14. Warum ist Spielen das neue Lernen?

Über Vorteile hatte ich ja bereits gesprochen. Entwicklungspsychologisch betrachtet, lernen wir als Kind fast ausschließlich über das Spielen. In der Schule bricht das plötzlich ab, weil Lernen in der Schule überwiegend noch oldschool ist. Hier wird Lernen meist mit Arbeit gleichgesetzt und Spielen eher mit Freizeit assoziiert, typisch deutsch, alte Gymnasialkultur eben. Wir sollten uns jedoch das Spielen als Lernform bewahren. Ich betrachte uns in Bezug auf Digitalisierung oder InfoSec entwicklungspsychologisch eh noch auf Kleinkindniveau, d.h. das Spielen mit Digitalem wird uns helfen, uns langsam weiterzuentwickeln – wir sind aktuell noch nicht erwachsen-reif für das, was uns in den letzten 2,3 Jahrzehnten quasi überrannt hat. Wir sind noch zu analog, aber das ist gut so, denn so bleiben wir menschlich, emotional. Ein Buchtipp hierzu: „Rettet das Spiel" von Gerald Hüther und Christoph Quarch.

15. Spielen Sie in Ihrer Freizeit? Wenn ja, was?

Wenn Sie damit meinen, ob ich z. B. Gesellschaft- oder Rollenspiele etc. spiele – nein, relativ wenig. Mir reicht die praktisch alltägliche Spielentwicklung bzw.-testung oder -moderation für Unternehmen. Allerdings bedeutet dies nicht, dass ich nicht ein „verspielter" Typ bin. Ich experimentiere gerne – und Experimente unterliegen Spielprinzipien. Dies realisiere ich gerne bei der Arbeit, z. B. bei der Entwicklung von Layouts, Naming, schräges Wording o.ä. oder in der Freizeit in meinem Garten oder meiner Küche. Denn ich koche gerne, braue Bier oder mache Schokolade – dies alles auf der Suche nach Neuem, Überraschendem – und das ist nichts anderes als Spielen.

16. Welche negativen Aspekte und Grenzen hat Gamification oder haben Serious Games möglicherweise mit Ihrem Einsatz an deutschen Hochschulen?

Negative Konnotationen fallen mir gerade nicht ein. Sorry.

17. Wie können diese negativen Aspekte vermieden werden?

Siehe oben.

18. Haben Sie persönliche Empfehlungen für mich in Bezug auf den Einsatz von Gamification?

Kommt darauf an, wie Sie sich im Bereich Gamification verorten, als Spielerin oder Spieledesignerin? Als Spielerin: offen sein, als Designerin bzw. Anbieterin: halten Sie Spiele zum Thema Security so einfach wie möglich und so komplex wie nötig.

Copyright

EXPERTENBEFRAGUNG

02

03
2022

BEFRAGUNG ZUR MASTERARBEIT:
„EINSATZ VON GAMIFICATION ZUR SENSIBILISIERUNG FÜR INFORMATIONSSICHERHEIT IM KONTEXT DEUTSCHER HOCHSCHULEN"

Expert-Time

Zur Person

Ivona Matas ist Diplom-Psychologin und systemische Therapeutin. Sie verfügt über mehr als 15 Jahre Agenturerfahrung, u. a. als Senior-Projektleiterin von Marktforschungs- und wirtschaftspsychologischen Studien. Neben ihrer Arbeit im Bereich der „analogen" Sicherheit im Rahmen von Kriseninterventionen und Traumatherapien nach Unfällen, Gewaltverbrechen oder Raubüberfällen ist sie Spezialistin für IT-(Security)-Studien und Human factor im Bereich Digitalisierung und Cybersicherheit.

Quelle: https://www.cyber-akademie.de/dozenten/ivona-matas/

Abbildung 1: Ivona Matas.
Quelle: https://www.cyber-akademie.de/dozenten/ivona-matas/

EINSATZ VON GAMIFICATION

Fragen an Ivona Matas

Gamification hat sich als Lernmethode noch nicht herumgesprochen.

Sie ist Diplom-Psychologin, Therapeutin und Gutachterin und weiß, dass es ohne die Psychologie kein Verständnis von Fehlerkultur, vom Faktor Mensch und insgesamt von der Security Awareness gibt. In der Befragung spricht sie u. a. über die Kunst, die richtige Richtung für Sensibilisierungsmaßnahmen zu wählen und mit einer gamifizierten Lösung gekonnt in Szene zu setzen.

1. Herr Pokoyski hat 2002 das Unternehmen known_sense gegründet, in dem auch Sie beschäftigt sind. Der Unternehmensslogan lautet: „awareness you can touch". Was genau ist damit gemeint?

Der Begriff Awareness in seiner deutschen Übersetzung von „Bewusstheit" oder „Gewahrsein" stellt eher eine Geisteshaltung dar. Dieses Bewusstsein für IT-Sicherheitsthemen muss natürlich auch zunächst entwickelt werden. Gleichzeitig reicht es aber nicht, dass sich Mitarbeitende oder Führungskräfte der Sicherheitsthemen bewusst sind – also eine Awareness entwickelt haben –, dieses Bewusstsein muss auch in konkretes Handeln umgesetzt werden und somit sichtbar und spürbar sein. Das Gleiche gilt für unsere Sensibilisierungsmaßnahmen: diese bleiben nicht auf einer abstrakten Ebene stehen, sondern sind Maßnahmen zum Anfassen.

2. Was macht ein gutes Serious Game bzw. eine gute gamifizierte Lösung/Anwendung aus?

Es geht immer um eine gelungene Verbindung von Spiel und Thema. Am Ende eines ‚guten' Spiels wird nicht über das Spiel gesprochen, sondern über das Thema, das damit transportiert wurde. Wenn Kommentare kommen, dass es eine spannende Darbietungsform war, freut es zwar, aber das Spielen ist nicht das Ziel.

3. Wie findet man eine zu einem bestimmten Thema passende und spannende Story?

Diese Frage zeigt, wie wichtig die Zusammenarbeit zwischen Kreativen, Psychologen und Kunden ist. Denn passgenaue Storys, die die Mitarbeitenden auch abholen, entwickeln sich nur im Miteinander.

4. Was muss bei der Gestaltung eines Serious Game/einer gamifizierten Lösung beachtet werden damit es erfolgreich in einer Hochschule angewendet wird?

Die Frage ist insofern spannend, als sie impliziert, dass Hochschulen ganz anders ticken als etwa Unternehmen, kommunale Einrichtungen oder Schulen – was ich nicht bestätigen kann. Die Auswahl der Themen und die Tonalität ist sicherlich zu beachten, aber wie Menschen Lernen und was für eine dauerhafte Verhaltensänderung notwendig ist – da unterscheiden sich die Mitarbeitenden von Hochschulen nicht von anderen.

5. Ist Gamification bzw. der Einsatz von Serious Games auch in der Führungsebene von Unternehmen/Hochschulen das richtige Werkzeug (um die notwendige Aufmerksamkeit für das Thema zu schaffen)?

Unbedingt! Die Annahme, dass die Führungsebene andere, ggf. „seriösere" Werkzeuge benötigt, hat sich nicht bestätigt. Vielmehr gelingt auch bei reinen Führungszirkeln über Serious Games eine schnelle Einführung in bestimmte Themen – zumal die IT-Sicherheit auch für Führungskräfte nicht das zentrale Arbeitsgebiet darstellt und somit eine Sensiilisierung für diese Themen unabdingbar ist.

"Um ein gutes Serious Game zu gestalten, benötigen Sie eine ganze Menge Wissen über …"

die Mechanik des Lernens und die dabei wirksamen Faktoren.

6. Was sind Ihrer Meinung nach die Vorteile von Gamification oder Serious Games im Gegensatz zu konventionellen Lehr- und Lernmethoden?

Es ist commen sense, dass das bloße theoretische (oder verbale Wissen) nicht unbedingt zu einem verbesserten konkreten Verhalten führt. Hierbei greift Gamifikation wichtige Aspekte auf, wie bspw. Motivation, Einstellungen und soziales Lernen.

Copyright

Informationen zu known_sense

Ivona Matas ist bei known_sense verantwortlich für Beratung und Management im Umfeld Information bzw. Corporate Security, d. h. im Einzelnen u. a. für die Durchführung von Wirkungsanalysen zur Sicherheitskultur sowie zu Digitalisierungs- bzw. Informationssicherheitsthemen, für Seminare und Trainings sowie die Erforschung, Kreation und Durchführung von Awareness- und Präventionsmaßnahmen zu den Themen Travel Security, personelle Sicherheit, Social Engineering und zu weiteren Themenfeldern rund um Manipulation im Unternehmensumfeld, z. B. Fake News, Trolling, Desinformation & Co.

Quelle: https://fake-aware-events.com/speaker/matas

Als eine Biertischidee entstand bei known_sense u. a. das Kartenspiel „Computerluder – das Virusquartett", das als erstes nicht-technisches IT-Tool als Produkt des Monats bei ComputerPartner ausgezeichnet wurde und Rezensionen bei brand eins, manager magazin, Spiegel-Online, WDR, ZDF u. v. m. erhielt.

Quelle: https://www.known-sense.de/kopie-home

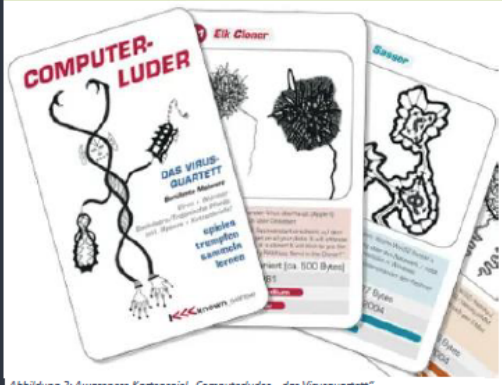


Abbildung 2: Awareness-Kartenspiel „Computerluder – das Virusquartett"
Quelle: https://www.known-sense.de/newpage6354ae55

Was Sie über Gamification wirklich wissen müssen.

Fragen an eine Expertin aus der Security-Awareness-Branche.

7. Wie kann die Effektivität und Nachhaltigkeit (der „Belohnungseffekt" für erfolgreiches Lernen) von Gamification/Serious Games gemessen werden?

Die Messbarkeit einzelner Awareness-Maßnahmen ist ein generelles Thema, das nicht nur Serious Games betrifft. Um über (ggf. wenig aussagekräftige) Kennzahlen hinaus einen sog. Key Performance Indicator (KPI) zu erhalten, sind verschiedene Vorgehensweisen möglich – ein weites Feld und Thema für ein weiteres Interview! .

8. Warum ist Lernen nicht ausreichend, um erfolgreich zu sensibilisieren?/

Gamification sollte nicht dem Lernen gegenübergestellt werden, sondern vielmehr als eine Methode des Lernens betrachtet werden. Der Einsatz von spielerischen Methoden hat mehrere Vorteile: Es ermöglicht eine stärkere Kompetenzwahrnehmung, und aktive und auf die bestehenden Kenntnisse zugeschnittene „Spiele" stärken das soziale Miteinander. Der direkt erfahrbare konkrete Anwendungsnutzen lässt eine sonst durchaus erkennbare Abwehr gegenüber IT-Sicherheitsthemen schmelzen. Das spielerische eigene Handeln ermöglicht es, Inhalte sofort umzusetzen, und das gewünschte Verhalten wird dadurch sofort eingeübt, was eine Steigerung des Lernerfolgs bewirkt. Für das Lernen notwendige Wiederholungen sind bei Serious Games weniger störend. Greift man Aspekte auf, etwa den Wettbewerb zwischen Abteilungen oder Gruppen, trägt dies zu einer Erhöhung der Sichtbarkeit bei. Das erhöht die Awareness für das Thema zusätzlich.

9. Spielen Sie in Ihrer Freizeit? Wenn ja, was?

Ja!. Wir spielen mit unseren Kindern und mit Freunden. Aber auch in meinem persönlichen Alltag versuche ich Aspekte von Belohnung und Nudging anzuwenden. Schon der Besitz einer Bahncard bspw. greift Aspekte des Gamings auf.

10. Welche negativen Aspekte und Grenzen hat Gamification oder haben Serious Games möglicherweise mit ihrem Einsatz an deutschen Hochschulen?

Die einzige Limitierung sehe ich darin, dass sich das Prinzip von Gamification als hervorragende Komponente von Lernmethoden noch nicht herumgesprochen hat.

11. Wie können diese negativen Aspekte vermieden werden?

Siehe Frage 10: Gerade Hochschulen sollten sich neuen Forschungsergebnissen und deren Umsetzung öffnen.

12. Haben Sie persönliche Empfehlungen für mich in Bezug auf den Einsatz von Gamification?

Der Einsatz von Games sollte stets in ein Gesamtkonzept eingebunden werden. Auch wenn die Vorteile von Games bei der Sensibilisierung gut aufzuzeigen sind: Spiele allein erhöhen Awareness, diese müssen in ein Gesamtkonzept integriert werden, dass auch von Führungskräften mitgetragen wird.

Copyright

EXPERTENBEFRAGUNG

03

03
2022

BEFRAGUNG ZUR MASTERARBEIT:
„EINSATZ VON GAMIFICATION ZUR SENSIBILISIERUNG FÜR INFORMATIONSSICHERHEIT IM KONTEXT DEUTSCHER HOCHSCHULEN"

Expert-Time

EINSATZ VON GAMIFICATION

Fragen an Martin Fischer

Abbildung 1: Martin Fischer.
Quelle: https://www.xing.com/profile/Martin_Fischer31i

Zur Person

Martin Fischer verfügt über ein tiefgehendes Fachwissen in den Bereichen der Informationssicherheit sowie dem Datenschutz. Darüber hinaus hat er langjährige Erfahrungen im IT Service Management nach ITIL, dem Qualitätsmanagement und dem Geschäftsprozess-management.

Quelle:https://www.hidden-awareness.de/about-us

Um dem Bedarf an ein effizientes und sofort umsetzbares Lernen gerecht zu werden, hat er es sich zum Ziel gesetzt, Dinge anders zu machen: Er setzt vorrangig auf Serious Games, um Wissen spielerisch zu vermitteln.Dadurch werden seiner Ansicht nach Berührungsängste abgebaut und Themen wie Informationssicherheit, Datenschutz und / Qualität verinnerlicht. Relevante Situationen werden so künftig ohne Angst, etwas falsch zu tun, angegangen und wissensbasiert bewältigt.

Quelle:https://www.xing.com/profile/Martin_Fischer31

Gamification soll den emotionalen Anker für das sichere Verhalten in der Praxis setzen.

Er ist Geschäftsführender Gesellschafter der HIDDEN Awareness UG. Er sensibilisiert in gamifizierten Events Unternehmen zum Thema Informationssicherheit. In der Befragung spricht er u. a. über die Kunst, eine gute Story zu erarbeiten und mit einer gamifizierten Lösung gekonnt in Szene zu setzen.

1. Herr Fischer Sie haben 2021 das Unternehmen HIDDEN Awareness UG (haftungsbeschränkt) gegründet. Auf Ihrer Webseite schreiben Sie: „Awareness ist kein Lerninhalt, sondern eine nachhaltige Verhaltensänderung." Was genau meinen Sie damit?

Ich will es mit einem Vergleich erklären: Immer und immer wieder werden Diäten angepriesen. Eine hilft besser als die andere, die angesammelten Pfunde zu verlieren. Dabei ist der einhergehende Jojo Effekt allgemein bekannt. Möchte man etwas Nachhaltiges gegen sein Übergewicht unternehmen, hilft meist nur regelmäßiges Training, sowie eine Umstellung der (Ess-)Gewohnheiten. Dieses Beispiel kann 1:1 auf Awareness im Bereich der Informationssicherheit (und im Allgemeinen) übertragen werden: wer das Bewusstsein und die Wahrnehmung zu einem Thema regelmäßig trainiert, wird sich auch nachhaltig in seinem Handeln ändern. Viele, vormals vielleicht unbeachtete Details, werden - wie selbstverständlich - wahrgenommen. Man handelt instinktiv.

2. Haben Sie auch Kooperationen mit deutschen Hochschulen oder bereits erste Erfahrungen mit Kunden aus dem Hochschulsektor?

Die HIDDEN Awareness ist ein junges Unternehmen, dass gerade in dieser, durchaus schwierigen Zeit, durchstartet. Es gibt Gespräche im Hochschulsektor aber auch im Bildungssektor allgemein. Kernstück ist ein eigens entwickeltes Web Application Framework, dass modular zusammensetzbare (Rätsel-/Spiel-)Bausteine bereitstellt und in ein Narrativ eingebunden werden kann. Eine erste Umsetzung erfolgte mit dem Serious Online Game D:BRFIN' [Aussprache nach IPA: /diː ˈbriːfɪŋ/], welches auf dem Prinzip des Game-based Learning beruht und das Lernen durch eine interaktive Gestaltung fördern soll. In diesem Serious Game erleben die Lernenden den (Büro)-Alltag und müssen sich der täglichen Herausforderung stellen, kein leichtes Ziel für die Hacker abzugeben. Für den Hochschulsektor müsste eine eigene Story entwickelt werden, um den Alltag besser abzubilden.

3. Wissen Sie, welche Merkmale ausschlaggebend sind für die Tauglichkeit von Gamification oder Serious Games an deutschen Hochschulen?

Diverse Studien haben die wichtigsten Merkmale für den Hochschulsektor herausgearbeitet. Dabei denke ich, dass sich diese Merkmale nicht wesentlich von den allgemeinen unterscheiden: Im Vorfeld muss klar definiert sein, was mit Game-based Learning erreicht werden soll. Die (intrinsischen) Motivation der Lernenden sollte anregt werden, um das Verständnis zu einem Sachverhalt zu vertiefen. Es sollten Anreize zum selbstgesteuertem Lernen forciert werden, die dazu beitragen, die Bereitschaft aufrecht zu erhalten. Doch nicht jeder Lernende kann über Spiele bzw. spielerisch erreicht werden. Auch dies muss im Vorfeld Beachtung finden.

4. Was macht ein gutes Serious Game bzw. eine gute gamifizierte Lösung / Anwendung aus?

Das sollten besser die Lernenden beantworten. ;-) Nein, im Ernst: Die Norm DIN EN 9001:2015 spricht hier von der sog. "Wirksamkeit von Schulungen". Dies kann z.B. durch die Lernenden selbst bewertet, über Prüfungen ermittelt oder das Ergebnis / das Verhalten über einen längeren Zeitraum beobachtet werden. Wenn also die Lerninhalte nachhaltig verinnerlicht und bestenfalls in den Alltag integriert werden, dann sind wir dort angekommen, was ich mit der Aussage "Awareness ist kein Lerninhalt, sondern eine nachhaltige Verhaltensänderung." unterstreichen möchte.

5. Wie findet man eine zu einem bestimmten Thema passende und spannende Story?

Das kann ich nicht pauschal beantworten. Ich denke, dass die eigenen Erfahrungen die Geschichten schreiben. In meinen Präsenzschulungen bekomme ich oft positives Feedback, da ich "Geschichten aus dem Leben" erzähle, die zum Thema passen. Wenn sich die Lernenden darin wiederfinden oder die Situationen vertraut erscheinen, dann hat man einen "emotionalen Anker" gesetzt. Diesen Effekt erlebe ich z.B. bei jedem Einsatz des Escape Game Trucks - The Honeypot. Die Teilnehmenden können sich schnell in die Story hineindenken und sprechen mich auch nach langer Zeit darauf an, wie viel Spaß sie dabei hatten.

6. Was muss bei der Gestaltung eines Serious Game / einer gamifizierten Lösung beachtet werden damit es erfolgreich in einer Hochschule angewendet wird?

Bei Game-based Learning Angeboten halte ich es für besonders wichtig, die Eigenmotivation der Lernenden zu aktivieren. Dies gilt insbesondere bei digitalen Angeboten, da hier das Lernen meist in einer Selbstlernphase stattfindet. Unabhängig davon, sollten die Themen möglichst die digitalen Arbeits- und/oder Alltagswelt der Lernenden widerspiegeln. Dadurch wird eine höhere Identifikation mit den Inhalten der jeweiligen Gefährdungslagen erreicht und der Wille zur Problemlösung wird gesteigert. Idealerweise erhebt ein Serious Game auch den Wissensstand sowie den Lernerfolg, um die erreichte Sensibilisierung und Kompetenz zu ermitteln.

7. Gibt es Hochschulen in Deutschland, die Serious Games / Gamification zur Sensibilisierung einsetzen? 8. Hat der Einsatz von Gamification die Haltung der Hochschulen auf die Stellung der Informationssicherheit verändert?

Hierzu liegen mir keine verlässlichen Informationen vor. Jedoch stelle ich fest, dass das Interesse an Serious Games im Bildungssektor in den letzten zwei Jahren zunimmt.

9. Welche weiteren Erfahrungen haben Sie mit solchen Tools bei Unternehmen (vielleicht auch bei deutschen Hochschulen) gemacht?

Wir erleben eine gesteigerte Spielmotivation in der Gesellschaft. 2018 wurde zum Beispiel der Escape Game Truck - The Honeypot auf der it-sa Fachmesse für IT-Security in Nürnberg vorgestellt.

Copyright

Informationen zu HIDDEN Awareness

Als Geschäftsführer einer Agentur für Kommunikation beriet er Kunden im B2B-Kontext und hat an einer Vielzahl von Projekten erfolgreich mitgewirkt. Durch seine langjährige Berufserfahrung kennt er die Abläufe, sowie die Anforderungen einer prozess- und qualitätsorientierten Organisation und bleibt dabei dennoch ein kreativer Kopf. Zusammen mit der Hidden Industries GmbH gründete er die HIDDEN Awareness UG und ist seit Anfang des Jahres 2022 alleiniger Eigentümer der HIDDEN Awareness UG (haftungsbeschränkt).

Hinter der Hidden Industries GmbH stehen sieben weitere Gründer. Sie bringen die verschiedensten Spezialgebiete und Fähigkeiten mit. Von Programmierern, über Rechtsanwälte, Marketing-experten, Betriebswirten, Ingenieuren und Kreativköpfen ist so ziemlich alles vertreten. Gemeinsam mit ihren Mitarbeitern und Freelancern sind sie verantwortlich für die Konzeption, Produktion und Vermarktung von Krimi- und Rätselspielen. Nebenbei leiten sie drei Escape Room Standorte in Hamburg, Braunschweig und Hannover und werden dabei durch ein tatkräftiges Team aus Standortleitern, Bürokräften, Spielleitern und Tischlern unterstützt.

Quelle: https://www.hidden-awareness.de/about-us

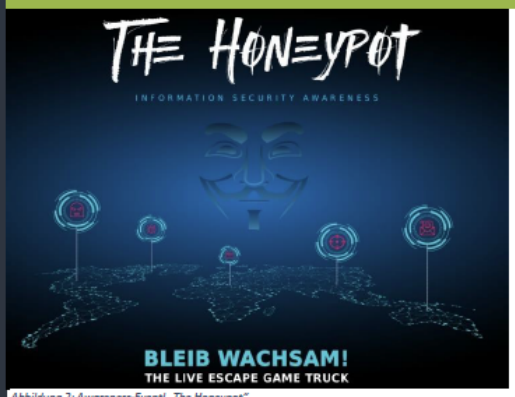


Abbildung 2: Awareness-Event „The Honeypot"
Quelle: https://www.hidden-awareness.de/images/attachements/Broschuere_The_Honeypot.pdf

Was Sie über Gamification wirklich wissen müssen.

Fragen an einen Experten aus der Security-Awareness-Branche.

Meine Erfahrungen und die Rückmeldungen der Spieler und Auftraggeber sind seit dem durchweg positiv. Die Unternehmen erkennen den Mehrwert dieser Lösungen, da die Möglichkeit besteht, dass sich die Lernenden mit anderen Spielern messen oder gemeinsam spielen und interagieren. Dies steigert nicht nur die Eigenmotivation, sondern führt (meist) zu einem nachhaltigeren Lernerfolg, da sich die Lernenden gerne an das Erlebte erinnern. Die Themen sind omnipräsent.

10. Ist Gamification bzw. der Einsatz von Serious Games auch in der Führungsebene von Unternehmen / Hochschulen das richtige Werkzeug (um die notwendige Aufmerksamkeit für das Thema zu schaffen)?

Ich stelle die These auf, dass nicht jede Führungskraft zugleich auch ein Experte für jedes Thema ist. Game-based Learning fördert dabei Sensibilisierung zu gewissen Themen und bereitet idealerweise unzugängliche oder theoretische Inhalte so auf, dass ein Bezug zur Praxis geschaffen wird. Die Lösungen bieten dem Management die Möglichkeit, sich spielerisch mit diesen Inhalten auseinander zu setzen. Die Führungskräfte erfahren die Auswirkungen ihrer Handlungen in einem "geschützten Raum" unmittelbar und lernen ggf. Entscheidungsalternativen kennen. Die Erkenntnisse lassen sich gut auf das Team übertragen und führen zu einem besseren Verständnis realer Geschäftsabläufe.

11. Was sind Ihrer Meinung nach die Vorteile von Gamification oder Serious Games im Gegensatz zu konventionellen Lehr- und Lernmethoden?

Im Gegensatz zu den konventionellen Methoden wird durch die spielerische Umsetzung die Eigenmotivation und das Engagement zum Lernen gesteigert. Gamification sollte meiner Meinung nach den bereits erwähnten "emotionalen Anker" setzen. Durch diesen Bezug festigt sich das erlernte Wissen und kann in vergleichbaren Situationen Anwendung finden. Oftmals werden Game-based Learning Angebote im Team erlebt. Durch die Interaktion und den unmittelbaren Austausch untereinander, entsteht eine Form von "Schwarmintelligenz". So schließen sich alle Teilnehmenden für die Sache zusammen und arbeiten gemeinsam an der Lösung. Die Teilnahme an konventionellen Methoden gehen meist mit einem gewissen Zwang einher, sich qualifizieren zu müssen. Gelernt wird für ein gutes Ergebnis und die Nachhaltigkeit hält sich dann in Grenzen.

12. Wie kann die Effektivität und Nachhaltigkeit (der „Belohnungseffekt" für erfolgreiches Lernen) von Gamification / Serious Games gemessen werden?

Nun, dies hängt natürlich stark vom Inhalt ab. Natürlich sollte stets eine Wirksamkeitsmessung einer Schulungsmassnahme erfolgen. Bezogen auf meinen Schwerpunkt der Informationssicherheit, gibt es viele Möglichkeiten die Effektivität zu messen. Dies kann z.B. durch Phishing Simulationen, Penetration Testing, Social Engineering Assessments, Tailgating oder andere Massnahmen erfolgen.

13. Warum ist Lernen Ihrer Meinung nach nicht ausreichend, um erfolgreich zu sensibilisieren?

Im Gegensatz zum konventionellen Lernen, werden beim Game-based Learning Inhalte meist durch einen Narrativ so aufbereitet, dass im Ideal die intrinsische Motivation der Lernenden angeregt wird. Sie müssen in möglichst spannende Situationen hineinversetzt werden, um Ihr vorhandenes Wissen anzuwenden oder Neues zu erlernen. Es gibt da diesen Begriff "Lernen durch Einsicht". Das spielerische Lernen sollte das konventionelle Lernen sinnvoll ergänzen.

14. Ist Spielen das neue Lernen?

Nein! Um ein tiefgehendes Fachwissen zu erlangen, werden konventionelle Lernmethoden die Mittel der Wahl sein. Spielen regt aber die Bereitschaft an, sich mit einem Thema zu befassen. Durch das Erleben, idealerweise mit einem Praxisbezug und in simulierten, realitätsnahen Situationen, können die Lernenden ihr bereits erlerntes Wissen anwenden und testen.

15. Spielen Sie in Ihrer Freizeit? Wenn ja, was?

Eigentlich gibt es zwei Genres, die ich seit Jahren verfolge. Das sind zum einen klassische Aufbauspiele bzw. Wirtschaftssimulationen und Adventurespiele. Tatsächlich finde ich dazu nur selten die Zeit. Mein 10-jähriger Sohn hingegen, möchte natürlich am Liebsten jeden Tag ein Adventurespiel mit mir spielen. ;) Da kommt es dann schon eher vor, dass wir stattdessen als Familie auch mal ein klassisches Brett- oder Kartenspiel spielen.

16. Welche negativen Aspekte und Grenzen hat Gamification oder haben Serious Games möglicherweise mit ihrem Einsatz an deutschen Hochschulen?

Mit Gamification werden, ganz im Allgemeinen gesprochen, nicht immer alle Menschen erreicht werden. So gibt es unterschiedliche Lerntypen und ihre bevorzugte Lernmethoden. Der Anwendungsorientierte (nach J. Schrader) wird vermutlich mit Begeisterung ein Serious Game spielen, wogegen der Unsichere das Spielen nicht als solches, sondern vielleicht als Zwang erfährt. Auch können integrierte Leaderboards oder die Vergabe von Badges Menschen psychisch unter Druck setzen und somit demotivierend wirken, um nur einige, wenige Nachteile aufzuzählen. Dies ist ein zu großes Feld, um es in zwei, drei Sätzen zu beschreiben. ;)

17. Wie können diese negativen Aspekte vermieden werden?

Gamification sollte sich an den fünf anerkannten Grundpfeilern ("The 5 Pillars of #Gamification", Roman Rackwitz) orientieren: Transparente Informationen, (Echtzeit)Feedback, klare Ziele und Regeln, Freiheiten, Herausforderung. Auch sollte Gamification nicht als die "Allzweckwaffe" für ein motiviertes Lernen angesehen werden, sondern dort zum Einsatz kommen, wo auch ein Nutzen erzeugt werden kann. Es handelt sich nicht um "Spielchen", die einfach ausgepackt werden und sofort ein Feuerwerk an Motivation entfachen.

18. Haben Sie persönliche Empfehlungen für mich in Bezug auf den Einsatz von Gamification?

Gamification funktioniert nur, wenn sie das Interesse, die Bedürfnisse und die Instinkte der Lernenden erreicht. Ich empfehle daher, sich im Vorfeld ausführlich mit Lehrenden, Lernenden und weiteren Experten auszutauschen, um eine Strategie zu entwickeln, wie und mit welchen Mitteln die Zielgruppe motiviert werden kann. Eine wohlüberlegte Strategie und erreichbare Ziele sind der Schlüssel zum Erfolg.

Original

EXPERTENBEFRAGUNG

04

03
2022

BEFRAGUNG ZUR MASTERARBEIT:
„EINSATZ VON GAMIFICATION ZUR SENSIBILISIERUNG FÜR INFORMATIONSSICHERHEIT IM KONTEXT DEUTSCHER HOCHSCHULEN"

Expert-Time

EINSATZ VON GAMIFICATION

Fragen an Eric Flury

Abbildung 1: Eric Flury.
Quelle: https://www.take-aware-events.com/speaker/flury

Zur Person

Eric Flury ist der Leiter vom Business Development der Fabula Games GmbH. Studiert hat er Geographie und um die weite Welt und die Menschen an diesen Orten zu entdecken, hat er in verschiedenen Ländern Europas gelebt und gearbeitet. Er ist fasziniert von der Vielfalt an Orten und Menschen in der Schweiz, Deutschland, Schweden, Spanien und Italien und ihrer Art und Weise, sich individuell weiterzuentwickeln und ihr Können und Wissen in Unternehmen einzubringen. Da es schon lange zu seinen Aufgaben gehört, Mitarbeiter weiterzubilden, hat er selbst mehrere Lernutensilien entwickelt.

Quelle:https://www.take-aware-events.com/speaker/flury

Das Prinzip des spielerischen Lernens ist tief in uns verwurzelt.

Er lenkt zusammen mit Tomislav Bodrozic die Geschicke der Fabula Games GmbH. Seit 2017 entwickeln sie Serious Games als Fabula Games GmbH in verschiedenen Bereichen – relativ neu ist die Schulung von Mitarbeitern im Bereich der Informationssicherheit. So verschieden wie die Themen dort sind, so verschieden sind auch die Erwartungen ihrer Kunden an ein Serious Game. In der Befragung spricht er u. a. über die Kunst, eine gute Story zu erarbeiten und mit einer gamifizierten Lösung gekonnt in Szene zu setzen.

1. Herr Flury die Fabula Games GmbH wurde 2017 gegründet. Ihr Slogan lautet: „We are Serious. In Games". Was genau meinen Sie damit?

Was wir damit sagen wollen, ist, dass jeder von uns den Großteil seines Wissens durch Spielen erworben hat. Und das, bevor wir überhaupt einen Fuß in die Schule gesetzt haben. Zuerst allein mit Spielzeug, mit dem man körperliche Regeln lernen, zählen und zeichnen konnte, dann spielte man mit seinen ersten Freunden und lernte so die wichtigsten sozialen Regeln. Wissenschaftliche Studien zeigen es deutlich, dass das Prinzip des spielerischen Lernens tief in uns verwurzelt ist und sehr effektiv funktioniert.

2. Ich habe gesehen, dass Sie 2021 eine Kooperation mit der Firma known_sense und mybreev eingegangen sind. Dürfen Sie mir sagen, worum es in dieser Kooperation geht?

mybreev hat eine Plattform mit Inhalten in Form von Filmen entwickelt, insbesondere zur Sensibilisierung der Mitarbeiter für Cyberrisiken. Die Idee ist, ihre Plattform mit Inhalten in Form von Serious Games zu füttern, um ihren Abonnenten einen neuen pädagogischen Ansatz zu bieten. Known_sense berät Unternehmen bei ihren Sensibilisierungskampagnen und schlägt unsere Serious Games vor, wenn diese in das Konzept der Kampagne passen.

3. Wissen Sie, welche Merkmale ausschlaggebend sind für die Tauglichkeit von Gamification oder Serious Games an deutschen Hochschulen?

Hochschulen stehen an der Spitze der pädagogischen Forschung und wissen, wie effektiv Gamification und Serious Games bei der Vermittlung von Inhalten an Lernende funktionieren. Die Entwicklung von Serious Games für alle Inhalte würde jedoch einen Kostenaufwand bedeuten, der für diese Art von Institutionen oft noch als unüberwindbar gilt. Einige Schulen begnügen sich damit, Serious Games in Form von Teasern zu entwickeln, um die Inhalte des Kurses hervorzuheben. Andere Schulen gehen den Weg der eigenen Produktion von Inhalten. Für diese bieten wir ein ideales Produkt mit dem Namen "Serious Games Creator" an, mit dem man ein Serious Game entwickeln kann, ohne eine einzige Zeile Code programmieren zu müssen.

4. Was macht ein gutes Serious Game bzw. eine gute gamifizierte Lösung / Anwendung aus?

Das ist eine großartige Frage, über die wir viel nachgedacht haben. Wir haben fünf "Geheimnisse" identifiziert, die in jedes Serious Game eingebaut werden müssen. Ohne ins Detail zu gehen (wir organisieren zweitägige Workshops, um diese Punkte zu vertiefen) kann ich sie hier nennen: - Der Lernende muss aktiviert werden: sofort und ständig. - Die intrinsische Motivation der Lernenden soll durch die Prinzipien der Gamification entwickelt werden. - Lernen erfordert eine Investition der Lernenden, die sich wiederum auf den Verlauf des Lernens auswirkt. - Lernen muss durch Simulation erfolgen: Der Lernende muss die Möglichkeit haben, zu testen, auszuprobieren, zu entdecken, Fehler zu machen und es erneut zu versuchen. Und nicht nur lesen, zuhören oder zuschauen. - Die Ausbildung muss immersiv sein: Der Lernende vergisst sich selbst, so sehr ist er in seine Ausbildung eingetaucht (z. B. durch Storytelling).

Wir versuchen, diese fünf Regeln in jeder unserer Produktionen umzusetzen.

5. Wie findet man eine zu einem bestimmten Thema passende und spannende Story?

Es ist wirklich ein Beruf für sich. Das merke ich bei jeder unserer Entwicklungen. Wir haben zwei interne Spezialisten, die dieses Gebiet studiert haben und über viel Erfahrung im Storytelling verfügen. Wenn ich sie beobachte, sehe ich, dass es sich um ein feines Gleichgewicht zwischen Komplexität, Spannung, Details, Verständnis, verfügbarer Zeit und vielen anderen Kriterien handelt.

Es ist eine komplexe Aufgabe, aber man kann sie lernen.

6. Was muss bei der Gestaltung eines Serious Game / einer gamifizierten Lösung beachtet werden damit es erfolgreich in einer Hochschule angewendet wird?

Die pädagogischen Kriterien sind die gleichen wie anderswo. Dagegen sind die Erwartungen des Zielpublikums an Hochschulen aus offensichtlichen Gründen noch anspruchsvoller als im Corporate-Bereich. Wir wenden uns an Menschen, die praktisch mit einer Konsole in der Hand geboren wurden. Nun darf man aber nicht vergessen, dass die Entwicklung von Spielen für die breite Öffentlichkeit zig Millionen kostet. Wir müssen also die Erwartungen erfüllen (vor allem in Bezug auf die Grafik) und gleichzeitig ein viel kleineres Budget zur Verfügung haben. Das ist eine echte Herausforderung ... die wir gerne annehmen!

7. Gibt es Hochschulen in Deutschland von denen Sie wissen, dass sie Serious Games / Gamification zur Sensibilisierung einsetzen?

Copyright

Informationen zu fabula games

Zu ihren Referenzen gehören die Bayer AG, die Deutsche Telekom AG, die Daimler AG oder auch Vergabe24.

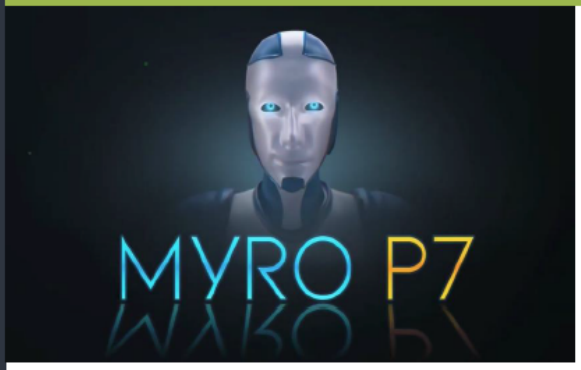
https://fabula-games.de/serious-games-referenzen/

Mit ihren Gamification Lösungen und Serious Games sorgen sie seit ihrer Gründung im Jahr 2017 für Weiterbildung in nahezu allen Unternehmensbereichen.

https://www.startbase.de/organization/fabula-games/

Die Gründung der Fabula Games GmbH erfolgte durch die Ausgliederung der Serious Games aus dem Filmagentur-Geschäft, welche viele Jahre in der Firma Fabula Film entwickelt wurden, aber grundsätzlich ein anderes Produkt als ein Film sind. Fabula Games entwickelt im Gegensatz zu anderen Unternehmen der Branche ausschließlich Serious Games. Aufgrund der positiven Rückmeldungen zu ihrem für einen bestimmten Kunden entwickelten Serious Game „myRo P7" hat das Unternehmen den Entschluss gefasst, ein eigenes InfoSec Serious Game zu entwickeln, welches über entsprechende Lizenzkosten dann auch für KMUs und Mittelständler zur Verfügung steht.

Quelle: https://www.take-aware-events.com/storage/app/media/pdf/takeawaresecandlifemagazine04.pdf



Was Sie über Gamification wirklich wissen müssen.

Fragen an einen Experten aus der Security-Awareness-Branche.

Abbildung 2: Beispiel eines Serious Games
Quelle: https://www.youtube.com/watch?v=AmT0tnhfmYE

Ja, wir arbeiten mit mehreren Hochschulen in Deutschland und der Schweiz zusammen, insbesondere im Bereich der Sensibilisierung für Cyberrisiken. Aus Gründen der Vertraulichkeit kann ich sie hier nicht nennen, aber ich lade Sie ein, mich zu kontaktieren, wenn Sie weitere Details wünschen.

8. Hat der Einsatz von Gamification die Haltung der Hochschulen auf die Stellung der Informationssicherheit verändert?

Was sich ändert, ist das Bewusstsein der Mitarbeiter oder Studenten nach dem Training. Studien zeigen, dass durch diesen Ansatz die Lerneffizienz im Vergleich zu herkömmlichem E-Learning um 360% höher ist. Dies hat zwei Gründe: Erstens sind die Lernenden motiviert, den Kurs bis zum Ende zu absolvieren (90% gegenüber 25% bei E-Learning). Und zweitens ist der Inhaltstransfer viel effektiver und langfristig einprägsamer. Bei den täglich steigenden Risiken lohnt sich das auf jeden Fall!

9. Welche weiteren Erfahrungen haben Sie evtl. mit solchen Tools bei deutschen Hochschulen gemacht?

Wir arbeiten auf drei Arten mit Hochschulen zusammen. Einige haben uns beauftragt, ein Serious Game mit spezifischen Inhalten für Studierende zu entwickeln. Andere haben Serious Games aus unserem Katalog gekauft, die hauptsächlich für ihre internen Mitarbeiter bestimmt sind. Und schließlich arbeiten wir mit mehreren Hochschulen zusammen, die unseren "Serious Games Creator" nutzen, um ihre eigenen gamifizierten Schulungen zu entwickeln. Eine gemeinsame Erfahrung, die wir mit diesen Organisationen machen, ist, dass ihre Erwartungen hoch sind (vor allem in Bezug auf die Grafik) und ... die Budgets leider ein wenig kleiner ☺

10. Ist Gamification bzw. der Einsatz von Serious Games auch in der Führungsebene von Unternehmen / Hochschulen das richtige Werkzeug (um die notwendige Aufmerksamkeit für das Thema zu schaffen)?

Absolut, solange die Kultur des Unternehmens/der Organisation dies zulässt. Ein Training mit einem Serious Game wird immersiv sein und daher wird die Führungskraft in ihr Training involviert sein, um zu versuchen, das bestmögliche Ergebnis zu erzielen. Der Inhalt des Trainings wird auf kognitive und emotionale Weise vermittelt, was bei jeder Person funktioniert.

"Um ein gutes Serious Game zu gestalten, benötigen Sie eine ganze Menge Wissen über..." Psychologie.

11. Was sind Ihrer Meinung nach die Vorteile von Gamification oder Serious Games im Gegensatz zu konventionellen Lehr- und Lernmethoden?

Sie können in zwei Punkten zusammengefasst werden: in die Abschlussquote von 90% (vs. 25% bei klassischem E-Learning) und in die Effektivität des Lernens durch Simulationen und praktische Übungen, die viel mehr behalten werden als das Lesen von Inhalten (90 % gegenüber 10 %).

12. Wie kann die Effektivität und Nachhaltigkeit (der „Belohnungseffekt" für erfolgreiches Lernen) von Gamification/Serious Games gemessen werden?

Ich möchte die Frage zurückgeben. Meiner Meinung nach ist es Aufgabe der akademischen Welt, dieses Thema zu erforschen, und es gibt sie auch. Für ein Unternehmen ist es sehr kompliziert, das zu organisieren. Man bräuchte drei repräsentative Gruppen von Personen, einschließlich: diejenigen, die eine klassische Ausbildung absolvieren, die die eine Ausbildung mit einem Serious Game absolvieren und diejenigen, die kein Training absolvieren. Und für jede dieser Gruppen sollte das Wissen vor dem Training, direkt nach dem Training und nach einiger Zeit gemessen werden. Meines Wissens hat keiner unserer Kunden jemals eine solche Studie durchgeführt.

13. Warum ist Lernen Ihrer Meinung nach nicht ausreichend, um erfolgreich zu sensibilisieren?

Denn es liegt in der Natur der Menschen, immer zu denken, dass es nur den anderen passiert. Um für ein Risiko richtig sensibilisiert zu sein, muss man einmal mit den möglichen Folgen konfrontiert werden. Dies ist nur mit einer Ausbildung möglich, die Simulationen einbezieht, wie wir es mit unseren Serious Games tun. Erleben statt lernen.

14. Ist Spielen das neue Lernen?

Nein, der Mensch lernt seit Urzeiten spielend. Jeder von uns hat wahrscheinlich 80% seines Wissens beim Spielen erworben, noch bevor er einen Fuß in die Schule gesetzt hat (Sprache, physikalische Regeln, soziale Interaktion...). Diese Form des Lernens ist tief in uns verwurzelt.

15. Spielen Sie in Ihrer Freizeit? Wenn ja, was?

Ich bin von Natur aus sehr kompetitiv und dieses Spielprinzip funktioniert bei mir besonders gut. Ich spiele also Spiele, bei denen ich mich mit anderen messen kann, möglichst mit Leuten, die ich kenne. Dazu gehören Sportspiele (virtuell oder real), Schach (hauptsächlich online) oder verschiedene Spiele, die mir meine Kinder zeigen.

16. Welche negativen Aspekte und Grenzen hat Gamification oder haben Serious Games möglicherweise mit ihrem Einsatz an deutschen Hochschulen?

Die Entwicklung von Serious Games erfordert Zeit und Ressourcen, die intern nicht immer zur Verfügung stehen. Es erfordert daher Budgets, um die Entwicklung auslagern zu können. Diese Budgets stehen nicht immer zur Verfügung.

17. Wie können diese negativen Aspekte vermieden werden?

Wie bereits oben erwähnt, ist es für eine Hochschule möglich, ihre Kompetenzen bei der Entwicklung von Schulungen in Form von Serious Games auszubauen. Wir können diesen Prozess sowohl pädagogisch-didaktisch als auch technisch mit unserem Tool "Serious Games Creator" begleiten.

18. Haben Sie persönliche Empfehlungen für mich in Bezug auf den Einsatz von Gamification?

Eine Empfehlung, die mir in den Sinn kommt, ist die Lesung des Buches "Hooked: How to Build Habit-Forming Products" von Nir Eyal, in dem man nachlesen kann, wie die Mechanismen der Gamification bei den beliebtesten Apps funktionieren. Diese Prinzipien sind auch auf Serious Games anwendbar.

Copyright

EXPERTENBEFRAGUNG

05

04
2022

BEFRAGUNG ZUR MASTERARBEIT:
„EINSATZ VON GAMIFICATION ZUR SENSIBILISIERUNG FÜR INFORMATIONSSICHERHEIT IM KONTEXT DEUTSCHER HOCHSCHULEN"

Expert-Time

Zur Person

Vladyslav Moyerer ist Treasurer und Membership Officer bei ASIS Germany e. V. und unterstützt die Bestands- und Neumitglieder. Nach seinem Bachelorstudium der Betriebswirtschaftslehre an der Hochschule Niederrhein mit dem Schwerpunkt International Management absolvierte er den berufsbegleitenden Masterstudiengang „Digital Business Managements" an der RFH Köln. Heute ist er als Business Development Manager beim Unternehmen mybreev tätig.

Quelle: https://www.asis-germany.org/das-board?pgid=kw11ftt-c1884df6-2010-40cc-b131-6e409c4a60b0

Abbildung 1: Vladyslav Moyerer.
Quelle: https://www.asis-germany.org/das-board?pgid=kw11ftt-c1884df6-2010-40cc-b131-6e409c4a60b0

EINSATZ VON GAMIFICATION

Fragen an Vladyslav Moyerer

In Spielen geht es um das Üben für den Ernstfall.

Vladyslav Moyerer ist Mitarbeiter des Awareness-Unternehmens mybreev GmbH in Viersen. Seit 2009 sensibilisiert mybreev Unternehmen zu verschiedenen Themen, auch im Bereich der Informationssicherheit. In der Befragung spricht Vladyslav Moyerer u. a. über die Kunst, eine gute Story zu erarbeiten und mit einer gamifizierten Lösung gekonnt in Szene zu setzen.

1. Herr Moyerer mybreev wurde 2009 gegründet. In Ihrem Firmen-Slogan wird Oscar Wilde zitiert: „Er sagt Dinge, die mich ärgern. Er gibt mir gute Ratschläge". Was genau ist damit gemeint?

Nun ja Präventionskonzepte müssen sich ja nicht nur in der Theorie entfalten, sondern am besten in der Praxis wirken. Oftmals muss man mit dem Kunden denkbare Szenarien für das jeweilige Business Model durchspielen und geeignete Awarenessmaßnahmen implementieren. Natürlich will das nicht jeder hören, was passieren könnte. Vorbereitet zu sein, ist jedoch essentiell.

2. Ich habe gesehen, dass mybreev zusammen mit known_sense 2021 eine Kooperation mit der Firma Fabula Games GmbH eingegangen sind. Dürfen Sie mir sagen, worum es in dieser Kooperation geht?

Wir bieten eine kleine Mini-Game-Cloudplattform an, wo fertige Cyber Security Spiele lizensiert werden können.

3. Wissen Sie, welche Merkmale ausschlaggebend sind für die Tauglichkeit von Gamification oder Serious Games an deutschen Hochschulen?

Laufen sie überhaupt auf älteren Computern? :D - Spaß beiseite, das müsste ich raten, aber die Usability ist immer wichtig.

4. Was macht ein gutes Serious Game bzw. eine gute gamifizierte Lösung / Anwendung aus?

Das Spiel lässt die Teilnehmenden intuitiv in eine neue Handlung eintauchen und man lernt noch was nebenbei.

5. Wie findet man eine zu einem bestimmten Thema passende und spannende Story?

Das ist unser täglich Brot. Die Story zu finden ist im Gegensatz zur Überprüfung der konkreten Faktenlage, der geringste Aufwand für uns. Wichtig ist, dass die Story die Spielenden „berührt" und Parallelen zum Berufsalltag hergestellt werden können, wenn es zu einem Vorfall kommt.

6. Was muss bei der Gestaltung eines Serious Game / einer gamifizierten Lösung beachtet werden damit es erfolgreich in einer Hochschule angewendet wird?

Wie überhaupt der Rollout an alle organisiert wird und wie der Relevanzfaktor für jeden Einzelnen hergestellt wird.

7. Gibt es Hochschulen in Deutschland von denen Sie wissen, dass sie Serious Games / Gamification zur Sensibilisierung einsetzen?

-

8. Hat der Einsatz von Gamification die Haltung der Hochschulen auf die Stellung der Informationssicherheit verändert?

-

Copyright

Informationen zu mybreev

Das innovative Unternehmen mybreev GmbH aus Viersen stellt seit 2009 multimediale E-Learnings und seit neuestem Serious Games her. Dabei liegt der Fokus auf allen sicherheitsrelevanten Themen sowie seit 2019 auch sog. Leadership Themen wie z.B. Kommunikation am Arbeitsplatz, psychische Resilienz, Diversity, AGG oder auch Inklusion. Seit 2020 verfügt das Unternehmen über einen Standort in Essen im Future Safe House, sowie in Hamburg für die mybreev international.

Quelle: https://www.security-island.com/de/blog/post/kooperation-zwischen-cogniport-gmbh-und-mybreev-gmbh

Mit der E-Learning Kurslibrary „Security Island", die über 50 sofort abrufbare E-Learning Kurse enthält, hat der erfahrene E-Learning Anbieter mybreev eine 360 Grad Lösung entwickelt, bei der die Attraktivität des Themas „Awareness Schulungen" sowohl für die Entscheidenden als auch für die Mitarbeitenden gesteigert wird.

Quelle: Röniger, U. (2020): Mit Security Island zu 360° Awareness- eLearning Journal Online. mybreev GmbH, Viersen.

Abbildung 2: Das E-Learning-Portfolio von mybreev
Quelle: https://www.security-island.com/de/sal

Was Sie über Gamification wirklich wissen müssen.

Fragen an einen Experten aus der Security-Awareness-Branche.

9. Ist Gamification bzw. der Einsatz von Serious Games auch in der Führungsebene von Unternehmen / Hochschulen das richtige Werkzeug (um die notwendige Aufmerksamkeit für das Thema zu schaffen)?

Es ist auf jeden Fall ein guter Alternativkanal, um die Zielgruppen systematisch zu durchdringen. Den einen Weg gibt es sowieso nicht.

"Um ein gutes Serious Game zu gestalten, benötigen Sie eine ganze Menge Wissen über…"

Produktionskosteneffizienz. Eine Spieleentwicklung ist teuer und es sind diverse mediale Gewerke involviert. Das genaue Austarieren, was kann was bewirken und welche Art von Gamegestaltung ist Spielerei und was entfaltet Wirkung ist die Kernfrage jeder Produktion.

10. Was sind Ihrer Meinung nach die Vorteile von Gamification oder Serious Games im Gegensatz zu konventionellen Lehr- und Lernmethoden?

Ich würde nicht unbedingt von Vorteilen sprechen. Es geht bei Spielen eher darum, den User selbst Entscheidungen treffen zu lassen und selbst auch den Katastrophenfall durchspielen zu lassen. Es geht also um das Involvement. Trotzdem ist anderseits der klassische Wissensaufbau von digitalen Lernmodulen ein wichtiger Kanal, wenn die Wissensbasis in der Fläche fehlt.

11. Wie kann die Effektivität und Nachhaltigkeit (der „Belohnungseffekt" für erfolgreiches Lernen) von Gamification/Serious Games gemessen werden?

Der „spielerische Trieb" ist bei den Menschen von Natur aus vorhanden. Werden also typische Gamification-Elemente wie Badges oder Rang- und Bestenlisten und das Aufsteigen in diesen in einem nicht-spielerischem Kontext eingesetzt, so fördert dies den Belohnungseffekt und die Lernenden sind bereit, sich länger mit einer Aufgabe auseinanderzusetzen. Idealerweise kommen sie dabei in einen sogenannten „Flow-Zustand", also einen Zustand, bei dem sie die Zeit vergessen und sich ganz in ihre Tätigkeit vertiefen.

Bei der Messung ist es grundsätzlich möglich sich der Flow Short Scale (FKS-Skala) zu bedienen, um festzustellen, ob das Flow-Erlebnis bei der Nutzung eines Lernangebots eingetroffen ist. Allerdings ist es üblicher die Performance der Lernenden vor und nach dem Bildungsangebot zu erheben. Wenn sie also nach der Teilnahme die vorgesehenen Lernziele erfüllen, dann kann die Maßnahme als erfolgreich betrachtet werden.

12. Warum ist Lernen Ihrer Meinung nach nicht ausreichend, um erfolgreich zu sensibilisieren?

Weil die Themen oft abstrakt sind ohne wirklichen Realbezug zur täglichen Arbeit. In Summe wirkt das Wissen erstmal logisch, aber ich brauche es heute nicht. Dann passiert etwas und man erinnert sich hinterher „ahh das wusste ich doch. Reingefallen."

13. Ist Spielen das neue Lernen?

Wir werden uns nicht zum CEO hochspielen können. Das erfordert auch Skills, die nicht spielerisch erworben werden können.

14. Spielen Sie in Ihrer Freizeit? Wenn ja, was?

Immer unregelmäßiger. Früher einige Spiele von Rockstar - heute maximal ein paar Handyspiele.

15. Haben Sie persönliche Empfehlungen für mich in Bezug auf den Einsatz von Gamification?

Kurze Mini-Spiele, die ganz bewusste Verhaltensempfehlungen trainieren, wirken besser als komplexe Strategiespiele. Das ist im Unternehmensumfeld und bei der täglichen Arbeitslast gut gemeint, aber schlecht gedacht.

Copyright

EXPERTENBEFRAGUNG

06

04
2022

BEFRAGUNG ZUR MASTERARBEIT:
„EINSATZ VON GAMIFICATION ZUR SENSIBILISIERUNG FÜR INFORMATIONSSICHERHEIT IM KONTEXT DEUTSCHER HOCHSCHULEN"

Expert-Time

Abbildung 1: Foto von Dr. Niklas Hellemann
Credits: SoSafe GmbH

EINSATZ VON GAMIFICATION

Fragen an Dr. Niklas Hellemann

Zur Person

Dr. Niklas Hellemann ist Diplom-Psychologe, langjähriger Unternehmensberater und Geschäftsführer und Mitgründer der Firma SoSafe. Als Experte für Social Engineering und Security Awareness beschäftigt er sich mit innovativen Methoden der Mitarbeitersensibilisierung – und unterstützt Kunden wie Vattenfall, Rossmann oder auch Avira dabei, ihre „Human Layer" abzusichern.

Quelle: https://www.bitkom-akademie.de/beratung/berater/niklas-hellemann

Insbesondere Hochschulen können Gamification im E-Learnning nutzen.

Seit 2018 sensibilisiert die Firma SoSafe Unternehmen zum Thema Informationssicherheit. In der Befragung spricht der Mitbegründer und Geschäftsführer Dr. Niklas Hellemann u. a. über die Kunst, eine gute Story zu erarbeiten und mit einer gamifizierten Lösung gekonnt in Szene zu setzen.

1. Herr Hellemann Sie haben 2018 das Unternehmen SoSafe gegründet. Ihr Slogan lautet: „Aktivieren Sie Ihre menschliche Firewall". Was genau meinen Sie damit?

Von etwa 3.4 Milliarden Phishing-Mails die pro Tag versendet werden, kommen 20 Prozent durch unsere technischen Abwehrsysteme. Die Schnittstelle zwischen Mensch und Maschine bleibt damit weiterhin das Einstiegstor Nummer 1 für Cyberkriminelle – mehr als 85 Prozent aller Angriffe starten beim Faktor Mensch. Das ist nicht überraschend. Denn Menschen lassen sich immer auf eine ähnliche Art und Weise angreifen – über emotionale Manipulation. Menschen somit auf Basis von Verhaltens- und Lernpsychologie über Cybergefahren zu informieren und sie im Umgang mit diesem Risiko zu schulen bietet die Chance, sie als weitere menschliche Firewall zu aktivieren – eine Chance für Unternehmen und für jeden, sich sicher im digitalen Raum zu bewegen.

2. Ich habe gelesen, dass Sie mit mehreren Hochschulen zusammenarbeiten. Dürfen Sie mir sagen, worum es in dieser Zusammenarbeit geht?

Hochschulen sind immer wieder Opfer von Cyberangriffen. Oft sind Forschungsergebnisse das Ziel: Cyberkriminelle versuchen Lösegeldforderungen für Forschungsergebnisse zu erzielen oder diese auszuspähen und für viel Geld weiterzuverkaufen. Wir arbeiten mit mehreren Hochschulen zusammen, um ihre Mitarbeitenden für dieses Risiko zu sensibilisieren und es damit zu senken.

3. Wissen Sie, welche Merkmale ausschlaggebend sind für die Tauglichkeit von Gamification oder Serious Games an deutschen Hochschulen?

Gamification bedeutet, dass spieltypische Elemente in einen spielfremden Kontext übertragen werden. Das funktioniert so gut, weil die Trainings den natürlichen Spieltrieb des Menschen ansprechen, der uns auch über die Kindheit hinaus erhalten bleibt. Komplexe Sachverhalte werden spielerisch vermittelt und somit besser verinnerlicht. Mit nachweislichem Erfolg: Unsere Daten zeigen, dass die Aktivierungsrate beim Einsatz von Gamification um mehr als 40 Prozent steigt. Es absolvieren also deutlich mehr Mitarbeitende das Training, was sich positiv auf die Sicherheitskultur in Organisationen auswirkt. Gamification ist also ein genereller Ansatz, um sich auf Grundlage der Lernpsychologie den Lernerfolg zu steigern. Davon können auch Hochschulen profitieren.

4. Was macht ein gutes Serious Game bzw. eine gute gamifizierte Lösung / Anwendung aus?

Typische Elemente aus Computerspielen werden in den Lernprozess integriert, erhöhen den Spaßfaktor und motivieren zum kontinuierlichen Lernen. Es gibt sechs Tipps, die den Gamification-Ansatz besonders erfolgreich machen: Menschen werden gerne belohnt. Lernende sind daher motivierter, wenn sie für eine erfolgreich absolvierte Lektion Punkte und Lob erhalten. Arbeiten Sie daher mit einem Punktesystem und regelmäßigem positiven Feedback. Menschen sind neugierig und möchten unterhalten werden. Storytelling sorgt daher dafür, dass Lernende sich für die Inhalte begeistern und wissen möchten, wie es weitergeht. Menschen sind soziale Wesen und möchten anderen helfen. Mit Gamification-Elementen können Lernende ihre Hilfsbereitschaft zeigen. Üblicherweise lösen sie Aufgaben und helfen den Protagonisten in einer Geschichte dabei, ein negatives Erlebnis zu verhindern. Menschen möchten sich weiterentwickeln. Schon ein einfacher Fortschrittsbalken kann eine große Wirkung erzielen. Die Visualisierung des eigenen Fortschritts spornt dazu an, 100 Prozent zu erreichen. Menschen suchen Anerkennung. Erhalten Lernende Abzeichen, mit denen sie Erfolg nach außen kommunizieren können, möchten sie möglichst viele solcher Belohnungen sammeln. Menschen möchten aktiv mitmachen. Kleine Spiele oder Aufgaben bringen Abwechslung und sorgen dafür, dass sich Lernende einbezogen fühlen.

5. Wie findet man eine zu einem bestimmten Thema passende und spannende Story?

Storytelling führt dazu, dass Lernende wissen wollen, wie es weitergeht und somit kontinuierlich lernen. Besonders wichtig ist für die Story, dass es einen durchgängigen Handlungsstrang gibt sowie interessanten Charakteren, mit denen sich Lernende identifizieren können.

Copyright

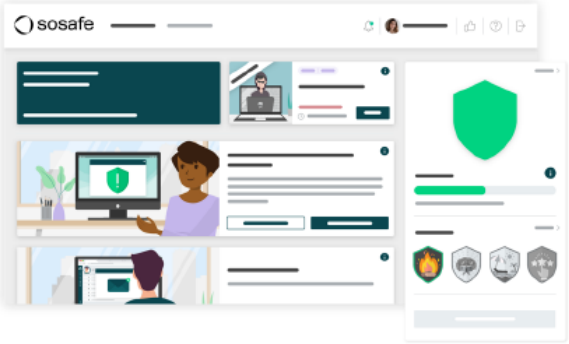
Informationen zu SoSafe

Die Firma SoSafe unterstützt Organisationen mit seiner agilen Awareness-Plattform dabei, ihre Sicherheitskultur zu stärken.

Die dynamischen Schulungen stellen den Menschen in den Mittelpunkt und verbinden verhaltenspsychologische Erkenntnisse mit smarten Algorithmen – so werden die Mitarbeitenden zur menschlichen Firewall ihrer Organisation. Organisationen fördern damit nicht nur das sichere Verhalten ihrer Belegschaft, sondern können mithilfe kontextbezogener Daten Schwachstellen erkennen, die angehen und den ROI ihres Awareness-Programms messen.

Die DSGVO-konforme Lösung von SoSafe zeichnet sich dadurch aus, dass sie besonders einfach implementiert, verwaltet und skaliert werden kann und somit Zeit und Ressourcen spart.

Quelle: Whitepaper der SoSafe GmbH „Wie Gamification das E-Learning revolutioniert"



Was Sie über Gamification wirklich wissen müssen.

Fragen an einen Experten aus der Security-Awareness-Branche.

Abbildung 2: Foto der sosafe-E-Learning-Plattform
Quelle: Dokument der SoSafe GmbH „IT-Sicherheitstraining"

6. Was muss bei der Gestaltung eines Serious Game / einer gamifizierten Lösung beachtet werden damit es erfolgreich in einer Hochschule angewendet wird?

Bei Gamification geht es darum, die Lernmodule an den Menschen anzupassen, der sie konsumieren soll. Der Lernende sollte also immer im Fokus stehen. Die Inhalte und Informationen sollen so einfach und intuitiv wie möglich zur Verfügung gestellt werden, damit die Lernenden sie nachhaltig im Gedächtnis behalten.

7. Welche weiteren Erfahrungen haben Sie mit solchen Tools bei deutschen Hochschulen gemacht?

Unsere Daten belegen, dass das kontinuierliche Lernen über unsere Plattform generell zu signifikanten Erfolgen im Bereich Awareness führt: Nach einem Jahr sind Klickraten durchschnittlich um 70 Prozent gesunken, die Interaktionsraten sogar um 80 Prozent. Gamification ist dabei ein zentrales Element, da es zum kontinuierlichen Lernen anregt – ein essentieller Bestandteil vom langfristigen Erfolg: Nach Lernpausen länger als vier Wochen steigen Klickraten ansonsten um durchschnittlich 30 Prozent.

8. Ist Gamification bzw. der Einsatz von Serious Games auch in der Führungsebene von Unternehmen / Hochschulen das richtige Werkzeug (um die notwendige Aufmerksamkeit für das Thema zu schaffen)?

Viele Menschen empfinden IT- und Informationssicherheit oder Datenschutz als trocken, langweilig und komplex. Daher haben sie keine intrinsische Motivation, sich damit zu beschäftigen oder mehr darüber zu erfahren. Organisationen müssen einen Schritt auf ihre Mitarbeitenden zu machen und ihnen die Informationen in einem möglichst zugänglichen Format zur Verfügung stellen. Die Lerninhalte müssen so gestaltet sein, dass sie sich individuell auf die Ebene der Lernenden begeben und zeigen: das Thema ist nicht nur wichtig, sondern macht auch Spaß. Insbesondere Hochschulen können Gamification daher als Methode im E-Learning nutzen, um die Awareness über Cybersicherheit langfristig zu steigern und festigen.

9. Warum ist Lernen Ihrer Meinung nach nicht ausreichend, um erfolgreich zu sensibilisieren?

Das Erlernte sollte mit zielgerichteten Simulationen kombiniert werden, um sichere Verhaltensweisen im Unternehmen zu fördern und zu etablieren. Smarte Angriffssimulationen lösen gezielt solche Emotionen aus, die im Ernstfall zu unsicherem Verhalten führen können. Sogenanntes Spear-Phishing-Awareness-Training analysiert im Anschluss dieses psychologische Verhalten und zeigt den Mitarbeitenden, wie sie zukünftige Bedrohungen besser erkennen und umgehen können. So werden sichere Verhaltensweisen in herausfordernden Situationen erlernt.

10. Wie kann die Effektivität und Nachhaltigkeit (der „Belohnungseffekt" für erfolgreiches Lernen) von Gamification/Serious Games gemessen werden?

Der Erfolg von Gamification kann anhand unterschiedlicher KPIs gemessen werden. Am sichtbarsten ist die Steigerung der Motivation: Unsere Daten zeigen, dass die Aktivierungsrate beim Einsatz von Gamification um mehr als 40 Prozent steigt. Es absolvieren also deutlich mehr Mitarbeitende das Training, wenn Gamification-Elemente verwendet werden, was sich positiv auf die Sicherheitskultur in Organisationen auswirkt.

Copyright

Anlage 3: Auszüge aus der Umfrage im ZKI-Arbeitskreis

Quelle: [130]

Copyright

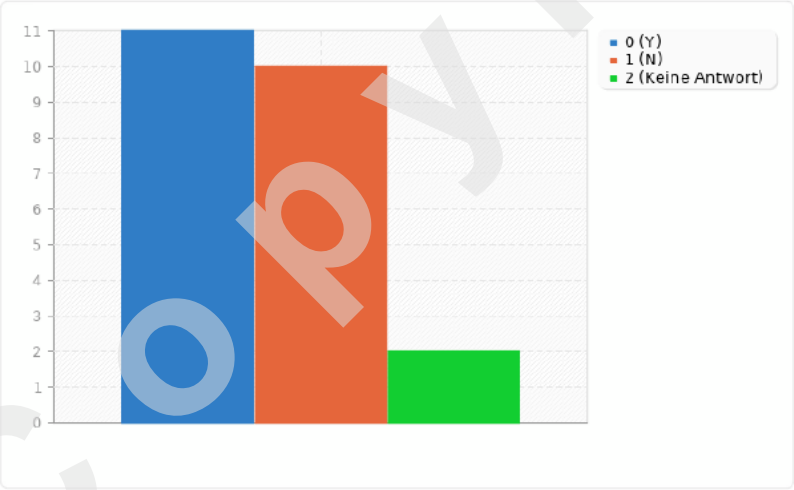
Zusammenfassung für G02Q11

Hatten Sie schon einmal einen ernsten Informationssicherheitsvorfall?

Antwort	Anzahl	Prozent
Ja (Y)	11	47.83%
Nein (N)	10	43.48%
Keine Antwort	2	8.70%

Zusammenfassung für G02Q11

Hatten Sie schon einmal einen ernsten Informationssicherheitsvorfall?



Copyright

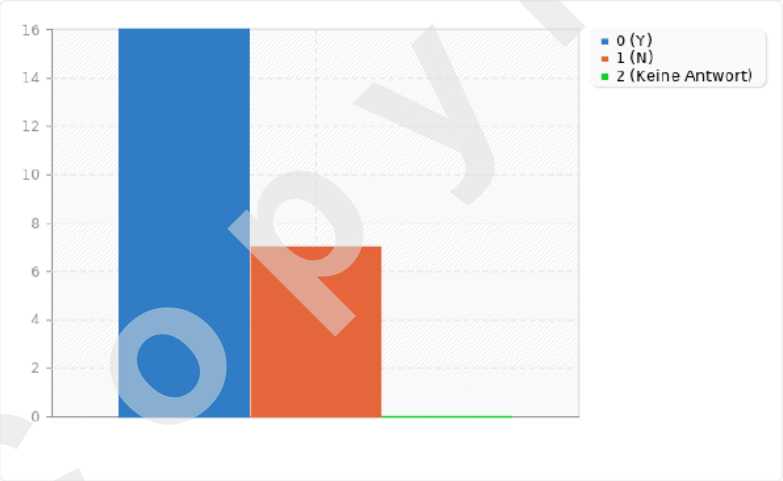
Zusammenfassung für G03Q16

Führen Sie Schulungen zur Benutzersensibilisierung für Informationssicherheit durch?

Antwort	Anzahl	Prozent
Ja (Y)	16	69.57%
Nein (N)	7	30.43%
Keine Antwort	0	0.00%

Zusammenfassung für G03Q16

Führen Sie Schulungen zur Benutzersensibilisierung für Informationssicherheit durch?



Copyright

Zusammenfassung für G03Q19

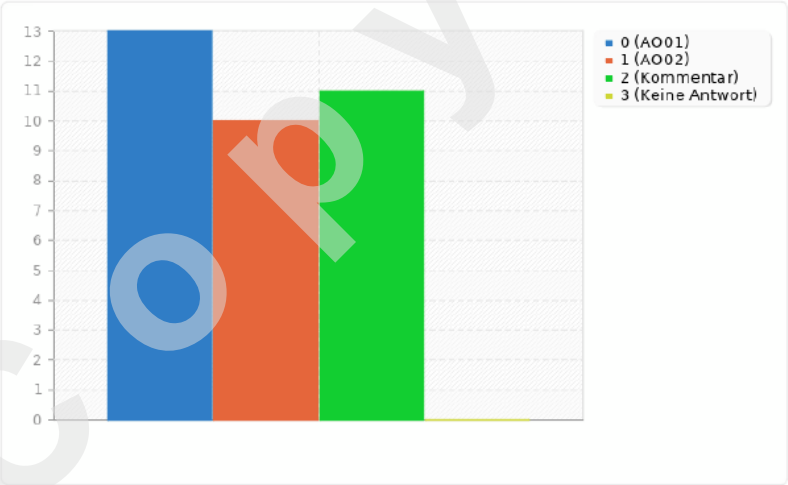
Verwenden Sie bei Ihren Schulungen Gamification-Ansätze (Einsatz spielerischer Elemente im spielfremden Kontext) oder können Sie sich vorstellen, diese zu verwenden?

Antwort	Anzahl	Prozent
ja (AO01)	13	56.52%
nein (AO02)	10	43.48%
Kommentar	11	47.83%
Keine Antwort	0	0.00%

ID	Antwort
13	Zu aufwändig oder zu teuer
21	Bisher nicht, aber ist interessant
28	Setzen wir aktuell nicht ein, ein Einsatz ist aber denkbar.
43	Durchaus denkbar Gamification-Ansätze zu verwenden. Eignung für jüngere Generationen geeignet
49	Nutzung der zentralen Sensibilisierungsplattform BayLern (leider aber keine Verpflichtung dies auch zu nutzen - da gg. wissenschaftlichen Personal leider nicht durchsetzbar)
56	Wäre auf jeden Fall hilfreich
59	Visualisierungsansatz (Print u. Hardware zur Darstellung)
71	Ich halte zwar das Prädikat "Sicherste Mitarbeiterin der Hochschule" oder "Das gesündeste Kind der Stadt" nicht für optimal. Aber ein eigener Punktwert ohne Veröffentlichung finde ich gut.
78	derzeit nicht verwendet, könnten wir uns aber vorstellen
79	Abzeichen nach Wissenscheck
86	Mir sind entsprechende Angebote leider nur in ganz geringem Umfang bekannt; den Ansatz halte ich aber für sehr vielversprechend.

Zusammenfassung für G03Q19

Verwenden Sie bei Ihren Schulungen Gamification-Ansätze (Einsatz spielerischer Elemente im spielfremden Kontext) oder können Sie sich vorstellen, diese zu verwenden?



Copyright

Zusammenfassung für G03Q21

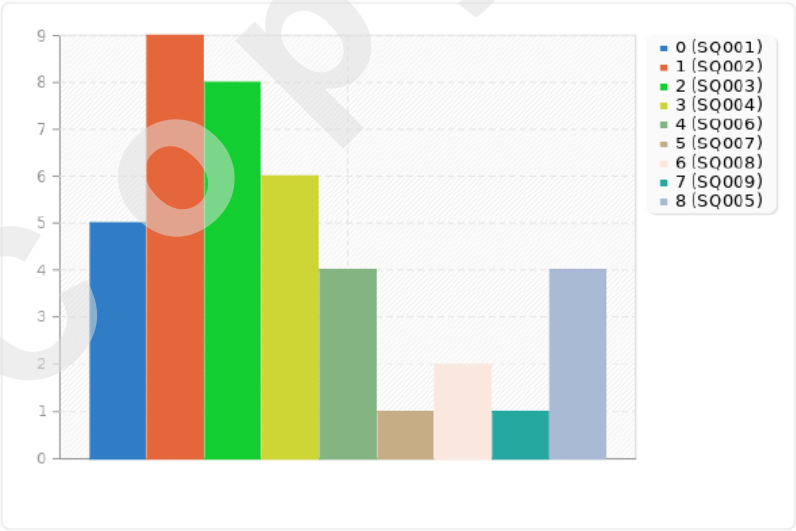
Über welches IT-System/Medium führen Sie die Schulungen durch?

eigene Webseite	**5**	**21.74%**
eigenes Lernmanagementsystem	9	39.13%
online-Kurse (gekauft)	8	34.78%
Awareness-Plattform (gekauft)	6	26.09%
online-Veranstaltungen (Webinare)	4	17.39%
Kampagne (gekauft)	1	4.35%
eigene Kampagne	2	8.70%
eigenes Phishing-Tool	1	4.35%
Sonstige	4	17.39%

ID	Antwort
24	hilft am besten
59	? Dachte, das soll anonym bleiben
12	ILIAS
79	Moodle
13	BayLern steht allen zur Verfügung
43	Layer8
13	SoSafe
28	befristet
12	Seminare mit Workshop-Charakter
21	Zoom-Seminar
71	Sollten wir tun! haben wir noch nicht.
37	ist im aufbau
12	-
11	Präsenzveranstaltungen des Landes
49	Online kostenfrei zur Verfügung gestellt (BayLern)
71	Beispielhafte Rundmails an die Adressaten (oder an alle) über konkrete an der Hochschule eingegangene Phishings
79	BayLern

Zusammenfassung für G03Q21

Über welches IT-System/Medium führen Sie die Schulungen durch?



Copyright

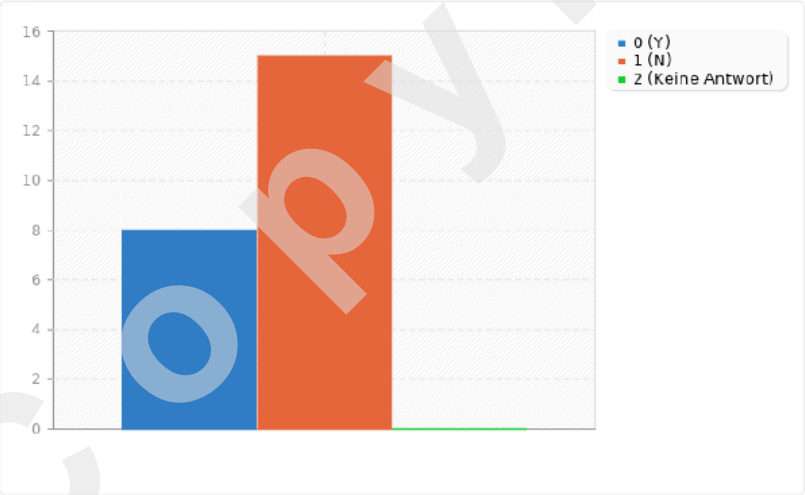
Zusammenfassung für G03Q23

Benutzen Sie in Ihrem Lernmanagementsystem Spieldesign-Elemente (Punkte, Abzeichen, Bestenlisten, Level etc.) zur Lernmotivation?

Antwort	Anzahl	Prozent
Ja (Y)	8	34.78%
Nein (N)	15	65.22%
Keine Antwort	0	0.00%

Zusammenfassung für G03Q23

Benutzen Sie in Ihrem Lernmanagementsystem Spieldesign-Elemente (Punkte, Abzeichen, Bestenlisten, Level etc.) zur Lernmotivation?



Copyright

Zusammenfassung für G03Q24

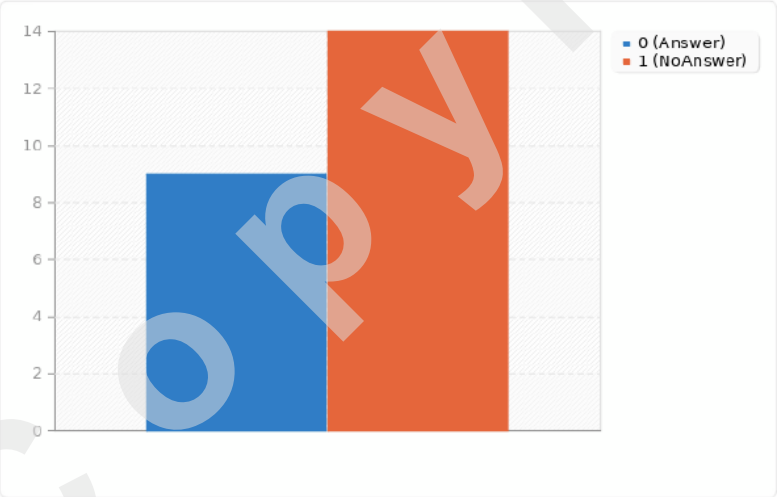
Wenn Sie in Ihrem Lernmanagementsystem bzw. für die online-Lehre Spieldesign-Elemente verwenden, welche sind das (Punkte, Abzeichen, Bestenlisten, Level, Avatare, Narrativ, Herausforderungen, Feedback, Quiz, sonstige)?

Antwort	Anzahl	Prozent
Antwort	9	39.13%
Keine Antwort	14	60.87%

ID	Antwort
11	Punkte
21	Kein Überblick, die Lehrenden verwenden eigenständig sämtliche Moodle-Funktionen
49	Quiz, Feedback, Umfragen
53	Abzeichen, Punkte, Quiz
59	Badges
71	Bestenlisten, Level, Quiz
78	nur wenige für Studierende in der Lehre, nicht für Awareness-Kampagnen eingesetzt
79	Badges
83	Narrativ, Herausforderungen

Zusammenfassung für G03Q24

Wenn Sie in Ihrem Lernmanagementsystem bzw. für die online-Lehre Spieldesign-Elemente verwenden, welche sind das (Punkte, Abzeichen, Bestenlisten, Level, Avatare, Narrativ, Herausforderungen, Feedback, Quiz, sonstige)?



Copyright

Zusammenfassung für G03Q25

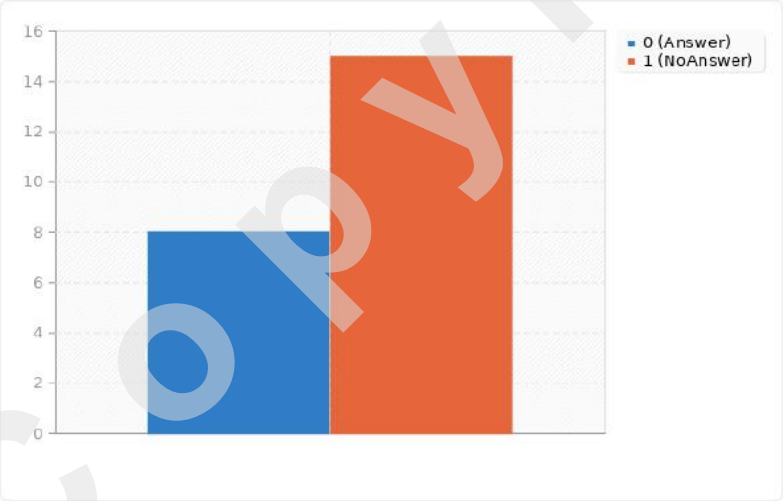
Wenn Sie keine Spieldesign-Elemente verwenden, wie motivieren Sie die Lernenden alternativ (über Noten, Prüfungen, Tests, bestimmte Benefits etc.)?

Antwort	Anzahl	Prozent
Antwort	8	34.78%
Keine Antwort	15	65.22%

ID	Antwort
11	Noten
13	derzeit gar nicht
28	Das ist zurzeit noch eine offene Frage
48	Tests
49	-
60	IT-Sicherheitsschulung als Vorraussetzung zur Home-Office Dienstvereinbarung.
78	über E-Mails und regelmäßige Informationsveranstaltungen zur Informationssicherheit (jeweils ausgewählte Themen)
81	Noten, Prüfungen, Tests

Zusammenfassung für G03Q25

Wenn Sie keine Spieldesign-Elemente verwenden, wie motivieren Sie die Lernenden alternativ (über Noten, Prüfungen, Tests, bestimmte Benefits etc.)?



Copyright

Zusammenfassung für G03Q26

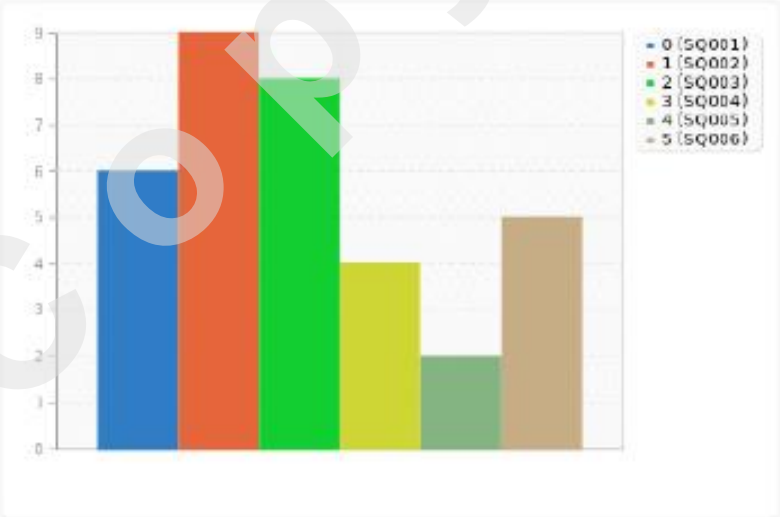
Welche Tools setzen Sie ansonsten im Rahmen der Benutzersensibilisierung ein?

Umfragetools (z. B. menti)	**6**	**26.09%**
Lernmanagementsysteme	9	39.13%
Selbstlernplattformen	8	34.78%
Escape Rooms/Games	4	17.39%
interaktive/Gamification Apps (z. B. Actionbound)	2	8.70%
andere	5	21.74%

ID	Antwort
12	Mentimeter
21	Abfrage im Rahmen jährlicher Nutzerumfragen
59	Limesurvey
71	menti
12	ILIAS
21	E-Learning-Kurs
59	Moodle, ARS Nova
78	Moodle
79	Moodle
49	BayLern
78	BayLern
24	erste erfolgreiche Tests
24	aktueller Versuch
59	Actionbound
13	SoSafe
28	E-Mail
43	Layer8
71	IT-SAD; Verweis auf gehaltene aufgezeichnete eigene Vorträge, Verweis auf Vorträge der Kolleginnen aus anderen Hochschulen (Arbeitsteilung); z.B. "Schaut Euch das VIdeo zum Thema X aus der Hochschule Y an, besonsers ab Minute 5:38 - 7:05"
78	regelmäßige Info-Mails, Infos auf Webseite, Informationsveranstaltungen

Zusammenfassung für G03Q26

Welche Tools setzen Sie ansonsten im Rahmen der Benutzersensibilisierung ein?



Copyright

Anlage 4: Zielgruppenbildung der Hochschulangehörigen der Hochschule Anhalt

Quelle: eigene Darstellung

Copyright

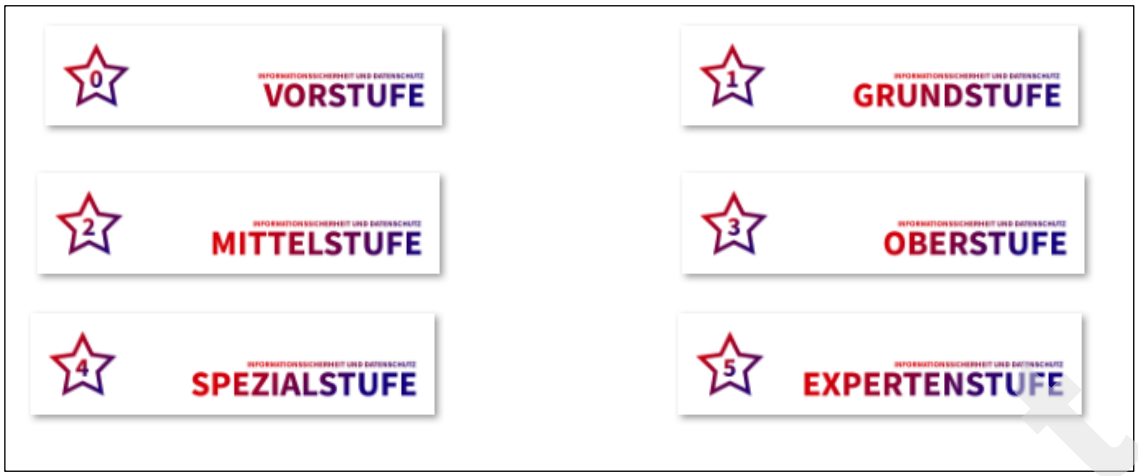
Tätigkeit	Anzahl Personen	Klassifizierung	Differenzierungsmerkmal
Anlagentechniker*in	2	0	handwerkend
Drucker*in	1	0	handwerkend
Elektriker*in	2	0	handwerkend
Fotograf*in	2	0	handwerkend
Gärtner*in	1	0	handwerkend
Haustechniker*in	15	0	handwerkend
Hilfskraft	7	0	handwerkend
Kraftfahrer*in	3	0	handwerkend
Laborant*in	6	0	handwerkend
Modellbauer*in	3	0	handwerkend
Sportkoordinator*in	2	0	handwerkend
Techn. Mitarbeiter*in	1	0	handwerkend
Techniker*in Agrar	2	0	handwerkend
Techniker*in Medien	1	0	handwerkend
Techniker*in Vermessung	1	0	handwerkend
Technische*r Assistent*in	2	0	handwerkend
Werkstattmeister*in	1	0	handwerkend
Vorstufe (0)	**52**	**7,10%**	**handwerkend (0)**
Auszubildende*r	1	1	sachbearbeitend
Assisstent*in	1	1	sachbearbeitend
Dekanatsassistent*in	2	1	sachbearbeitend
IT-Techniker*in	3	1	sachbearbeitend
Mitarbeiter*in HSB	10	1	sachbearbeitend
Mitarbeiter*in MuK	4	1	sachbearbeitend
Sachbearbeiter*in	48	1	sachbearbeitend
Studiengangkoordinator*in	1	1	sachbearbeitend
Verwaltungsmitarbeiter*in	35	1	sachbearbeitend
Grundkurs (1)	**105**	**14,34%**	**sachbearbeitend (1)**
Fachprakt. Mitarbeiter*in	92	1	fachpraktisch
Bronze (2)	**92**	**12,57%**	**fachpraktisch (2)**
Projektmitarbeiter*in	124	2	prozessübergreifend
Bronze (2)	**124**	**16,94%**	**prozessübergreifend (2)**
Wiss. Mitarbeiter*in	133	2	forschend
Bronze (2)	**133**	**18,17%**	**forschend (2)**
Dezernent*in	1	3	leitend
Justitiar*in	1	3	leitend
Leiter*in	6	3	leitend
Leiter*in HSB	1	3	leitend
Leiter*in IT	1	3	leitend
Leiter*in Studienkolleg	1	3	leitend
Leiterin der Verwaltung	1	3	leitend
Sachgebietsleiter*in	4	3	leitend
Technische*r Leiter*in	3	3	leitend
Gastprofessor*in (hb)	1	3	lehrend und leitend
Gastprofessor*in (nb)	1	3	lehrend und leitend
Präsident	1	3	leitend
Lehrkraft f.bes.Aufgaben	22	3	lehrend
Lehrkraft Studienkolleg	14	3	lehrend
Professor*in	133	3	lehrend und leitend
Vertretungsprofessor*in	17	3	lehrend und leitend
Silber (3)	**208**	**28,42%**	**leitend/lehrend (3)**
IT-Systemadministrator*in	18	4	systemverändernd
Gold (4)	**18**	**2,46%**	**systemverändernd (4)**
Gesamtergebnis	**732**	64,89%	

Copyright

Anlage 5: Beispiele für Level-Abzeichen und Abschluss-Zertifikat

Quelle: Hochschule Anhalt

Copyright



HOCHSCHULE ANHALT University of Applied Sciences

ZERTIFIKAT

Informationssicherheit

- Grundstufe -

Max Mustermann

hat den Nachweis zum Erwerb von fach-methodischen sowie umsetzungsorientierten Kompetenzen in den Grundlagen der Informationssicherheit erbracht und verfügt über Kenntnisse in den Bereichen Passwortsicherheit, Netzsicherheit, Umgang mit privaten und dienstlichen Daten sowie Verhalten bei einem Informationssicherheitsvorfall.

Prof. Dr. Lothar Koppers
Vizepräsident für Digitalisierung und Internationales

Copyright

Anlage 6: Storyboard beispielhafter Szenen im entwickelten Bound

Quelle: eigene Darstellung

Copyright

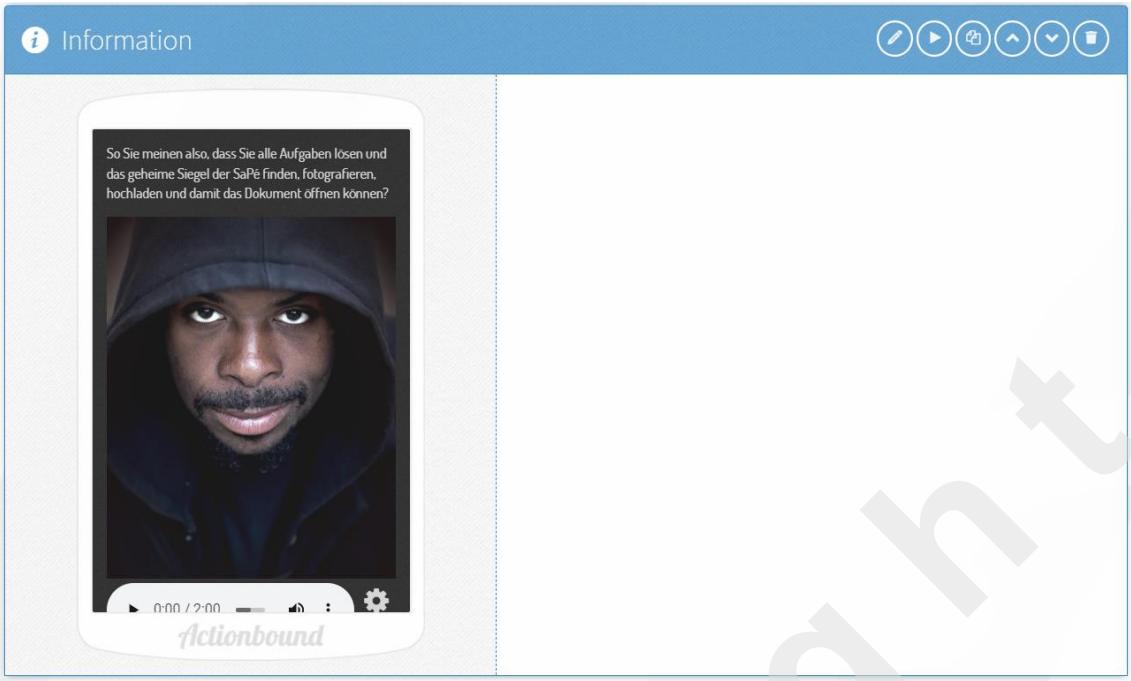
Abschnittsname	Beispielseite	Inhalt	Art des Elements	Punkte	Antwortmöglichkeiten	Wiederholungsversuche	Musik	Bild	Zeitbegrenzung
Einleitung	2	Sind eigentlich **alle** Team-Mitglieder vor Ort? Wenn nicht, haben Sie 10 Minuten ab jetzt Zeit alle Mitglieder zusammen zu holen. Schnell!	Quiz	100; 10 Punkte Abzug bei falscher Antwort; 10 % Abzug bei Zeitüberschreitung von 10	2	2	19th Floor - Bobby Richards.mp3	uhr.jpg	600 Sekunden
Datenschutzeinstellungen bei Apps	10	Schätzen Sie! Wie hoch ca. ist die Anzahl der im Google Play Store verfügbaren Apps zum 1. August 2022?	Quiz	100	schätzen	1	keine	playstore.jpg	keine
Passwortknacker	16	Begeben Sie sich an den gesuchten Ort und suchen Sie nach Hinweisen auf ein Passwort an einem offensichtlich schlecht gesicherten PC-Arbeitsplatz. Es gibt insgesamt **5** Hinweise, die auf **3** Passwörter verweisen. Um welche drei Passwörter handelt es sich?	Aufgabe	keine	Texteingabe	keine	keine	buero.jpg	keine
Passwörter aus dem Browserspeicher auslesen bzw. verwenden	20	Zu Ihrer Sicherheit sollten Sie niemals Passwörter in einem Internet-Browser speichern. Es besteht die Gefahr, dass diese ausgelesen werden. **Deaktivieren Sie die Einstellungen zur Speicherung (siehe Bild).**	Information	keine	keine	keine	keine	BrowserSicherheit.jpg	keine
Klassifizierung von Daten (vertraulich, privat, dienstlich)	22	Warum ist es gut, dienstliche und private Daten zu trennen?	Quiz	100; 10 Punkte Abzug bei falscher Antwort	7	3	keine	serverraum.jpg	keine
Verschlüsselte E-Mails	26	Machen Sie es besser! In einer kleinen Challenge gegeneinander zeigen in der nächsten Aufgabe zwei Personen, die zufällig von der App ausgewählt werden, dass es nach Erfüllung der ersten Teilaufgabe in der zweiten Teilaufgabe mehr als einen Vorschlag zur Verbesserung gibt. Wer die meisten Vorschläge macht,	Turnier mit Siegerehrung	keine	variabel	keine	Stranger Danger - Francis Preve.mp3	challenge.jpg	keine
Reaktion beim Sicherheitsvorfall	29	Was sind die drei häufigsten Ursachen für Informationssicherheitsvorfälle?	Quiz	100; 10 Punkte Abzug bei falscher Antwort	8	3	keine	sicherheit.jpg	keine
Abschluss	34	Herzlichen Glückwunsch! Sie haben das Ziel erreicht. Bitte fotografieren Sie das Dokument und laden es hoch! Sammeln Sie die Figur ein.	Aufgabe	keine	Fotoaufnahme	keine	Honey - Corbyn Kites.mp3	foto_telefon.jpg	keine

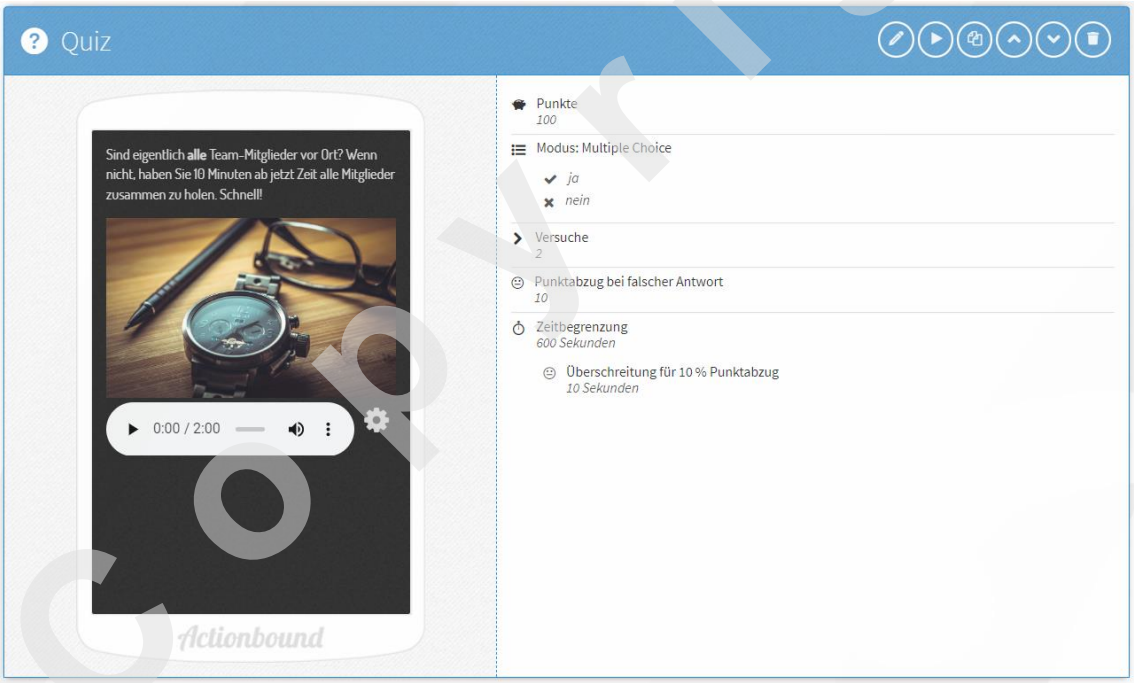
Copyright

Anlage 7: gesamter erstellter Bound

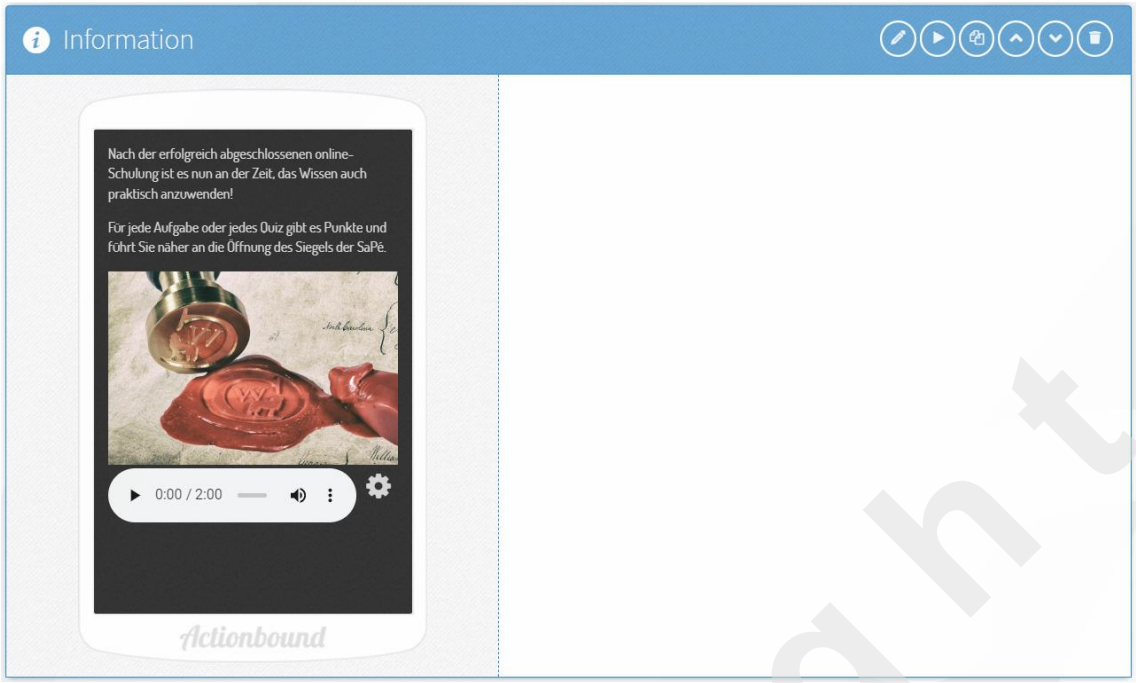
Quelle: eigene Erstellung mit der App Actionbound

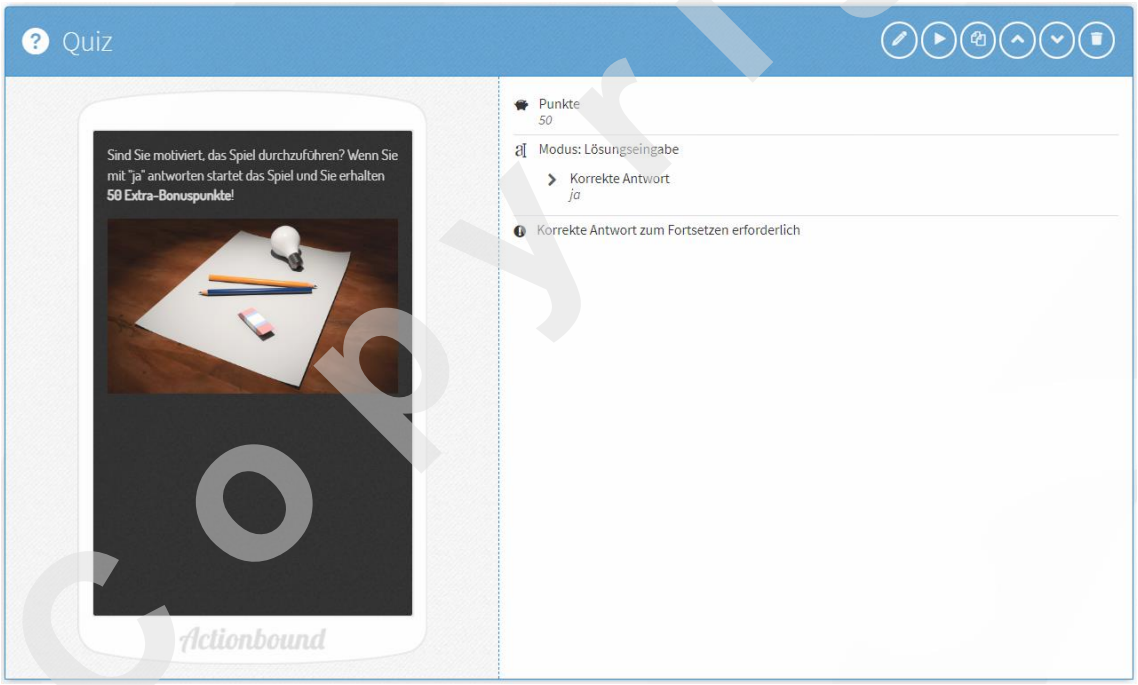
Copyright


Information
So Sie meinen also, dass Sie alle Aufgaben lösen und das geheime Siegel der SaPë finden, fotografieren, hochladen und damit das Dokument öffnen können?
0:00 / 2:00
Actionbound

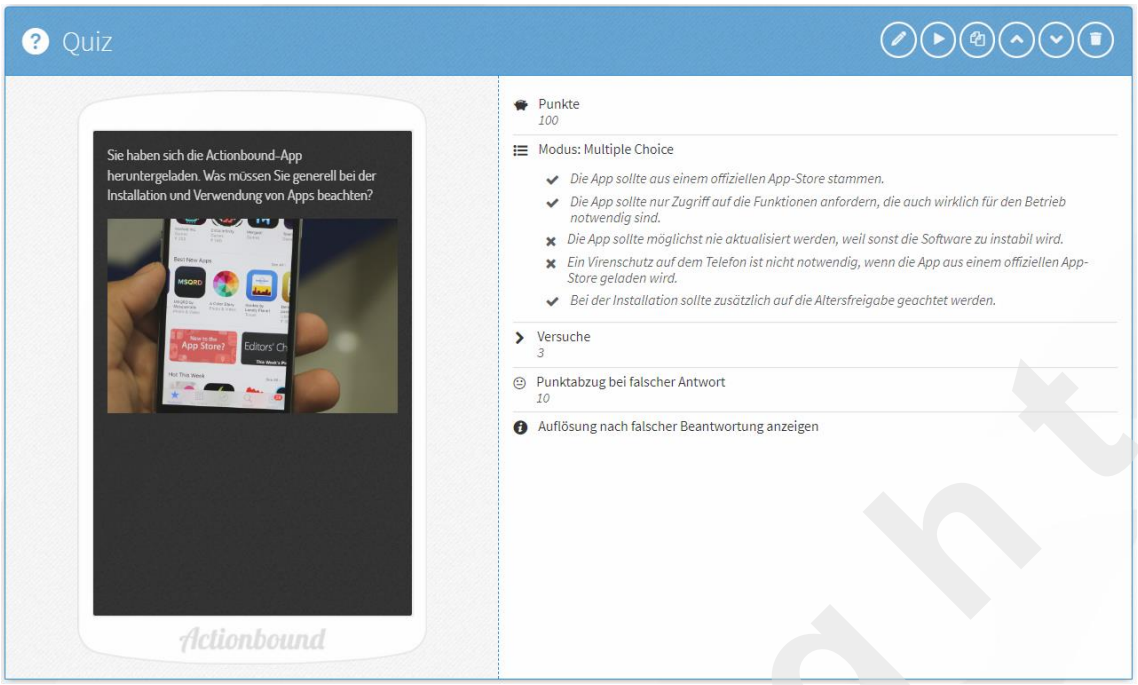

Quiz
Sind eigentlich alle Team-Mitglieder vor Ort? Wenn nicht, haben Sie 10 Minuten ab jetzt Zeit alle Mitglieder zusammen zu holen. Schnell!
0:00 / 2:00
Actionbound
Punkte
100
Modus: Multiple Choice
ja
nein
Versuche
2
Punktabzug bei falscher Antwort
10
Zeitbegrenzung
600 Sekunden
Überschreitung für 10 % Punktabzug
10 Sekunden

Copyright


Information
Nach der erfolgreich abgeschlossenen online-Schulung ist es nun an der Zeit, das Wissen auch praktisch anzuwenden!
Für jede Aufgabe oder jedes Quiz gibt es Punkte und führt Sie näher an die Öffnung des Siegels der SaPé.
0:00 / 2:00
Actionbound

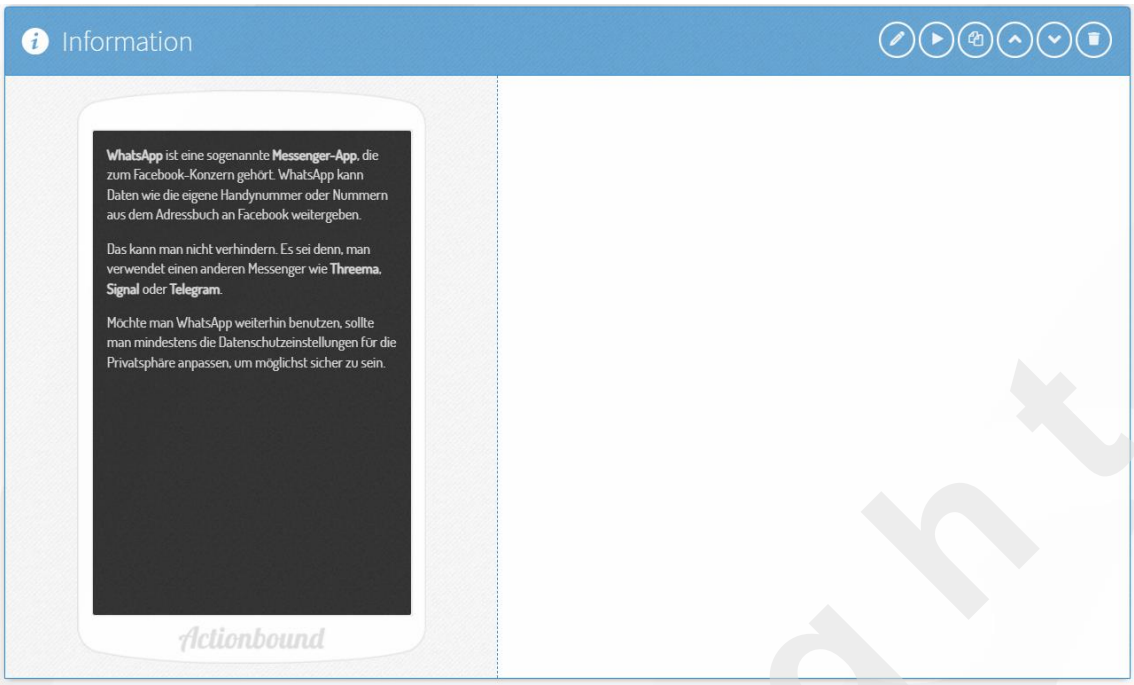

Quiz
Sind Sie motiviert, das Spiel durchzuführen? Wenn Sie mit "ja" antworten startet das Spiel und Sie erhalten 50 Extra-Bonuspunkte!
Actionbound
Punkte
50
Modus: Lösungseingabe
Korrekte Antwort
ja
Korrekte Antwort zum Fortsetzen erforderlich

Copyright

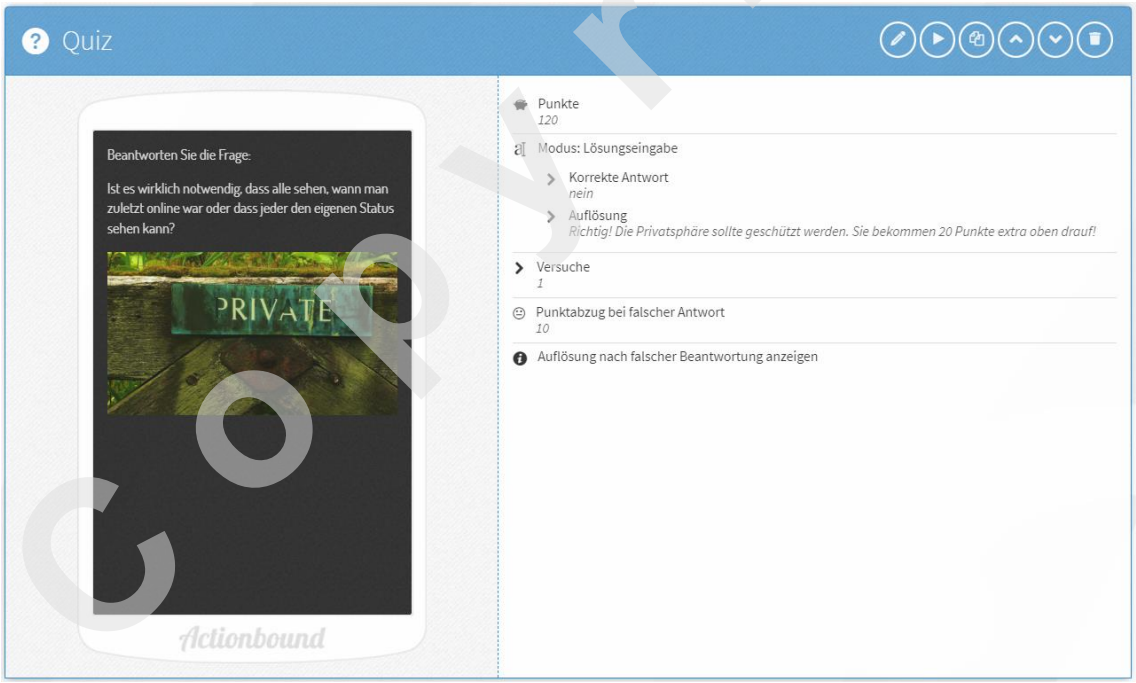

Quiz
Sie haben sich die Actionbound-App heruntergeladen. Was müssen Sie generell bei der Installation und Verwendung von Apps beachten?
Actionbound
Punkte
100
Modus: Multiple Choice
Die App sollte aus einem offiziellen App-Store stammen.
Die App sollte nur Zugriff auf die Funktionen anfordern, die auch wirklich für den Betrieb notwendig sind.
Die App sollte möglichst nie aktualisiert werden, weil sonst die Software zu instabil wird.
Ein Virenschutz auf dem Telefon ist nicht notwendig, wenn die App aus einem offiziellen App-Store geladen wird.
Bei der Installation sollte zusätzlich auf die Altersfreigabe geachtet werden.
Versuche
3
Punktabzug bei falscher Antwort
10
Auflösung nach falscher Beantwortung anzeigen

Information
Eine der beliebtesten Apps ist WhatsApp!
Aber kennen Sie sich auch aus mit den Datenschutzeinstellungen bei WhatsApp?
Actionbound

Copyright

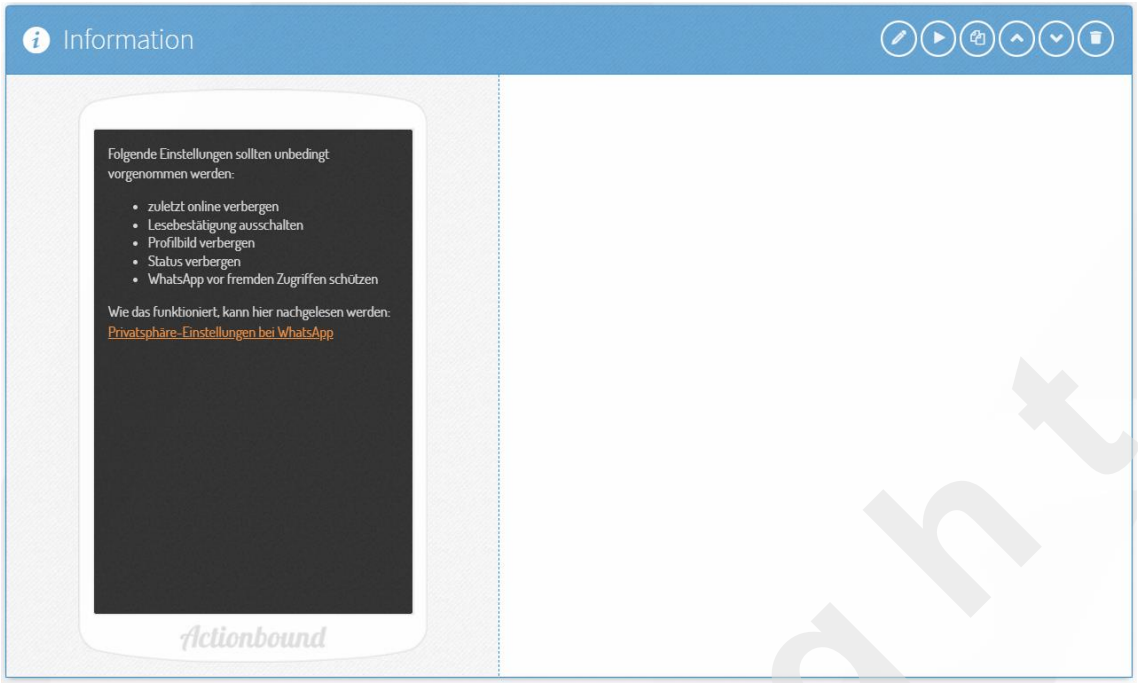


Quelle: Information übernommen und verändert aus:
https://de.actionbound.com/bound/imnetzabersicherlevel1 (abgerufen am 30.08.2022)

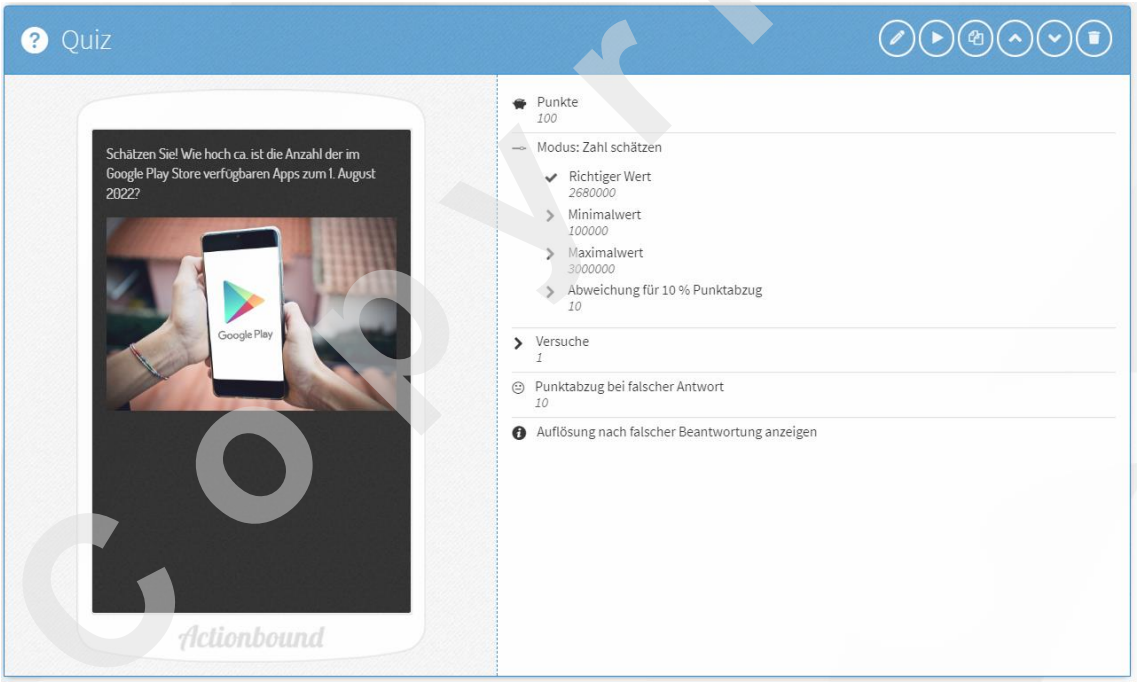


Quelle: Quizfrage übernommen und verändert aus:
https://de.actionbound.com/bound/imnetzabersicherlevel1 (abgerufen am 30.08.2022)

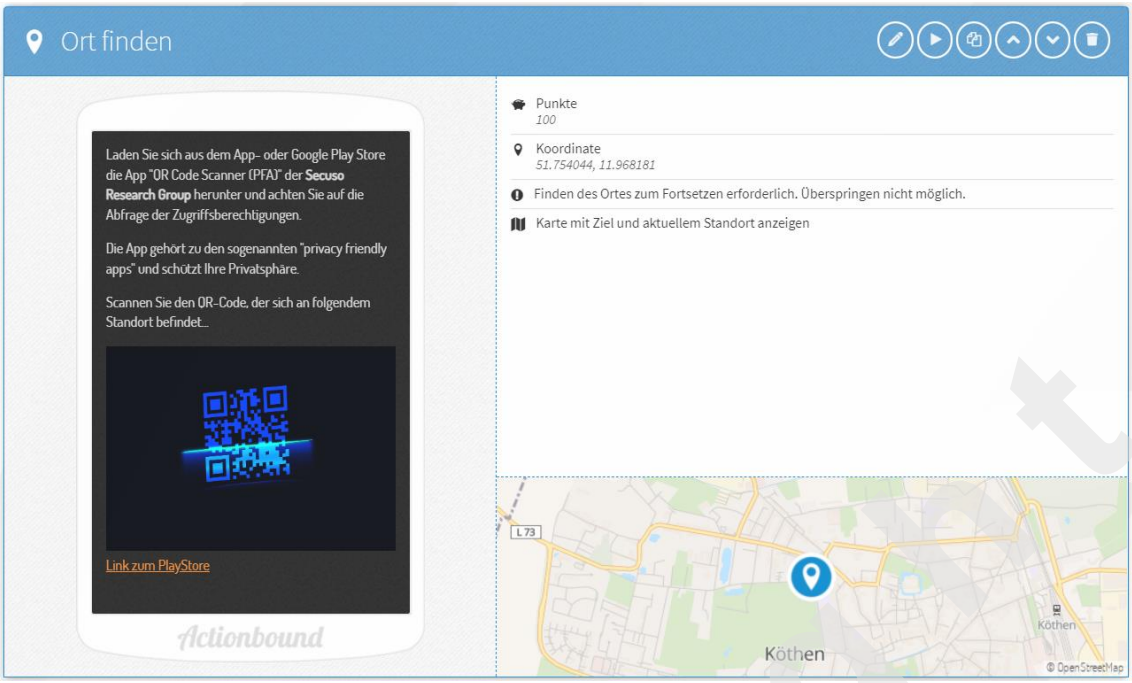
Copyright

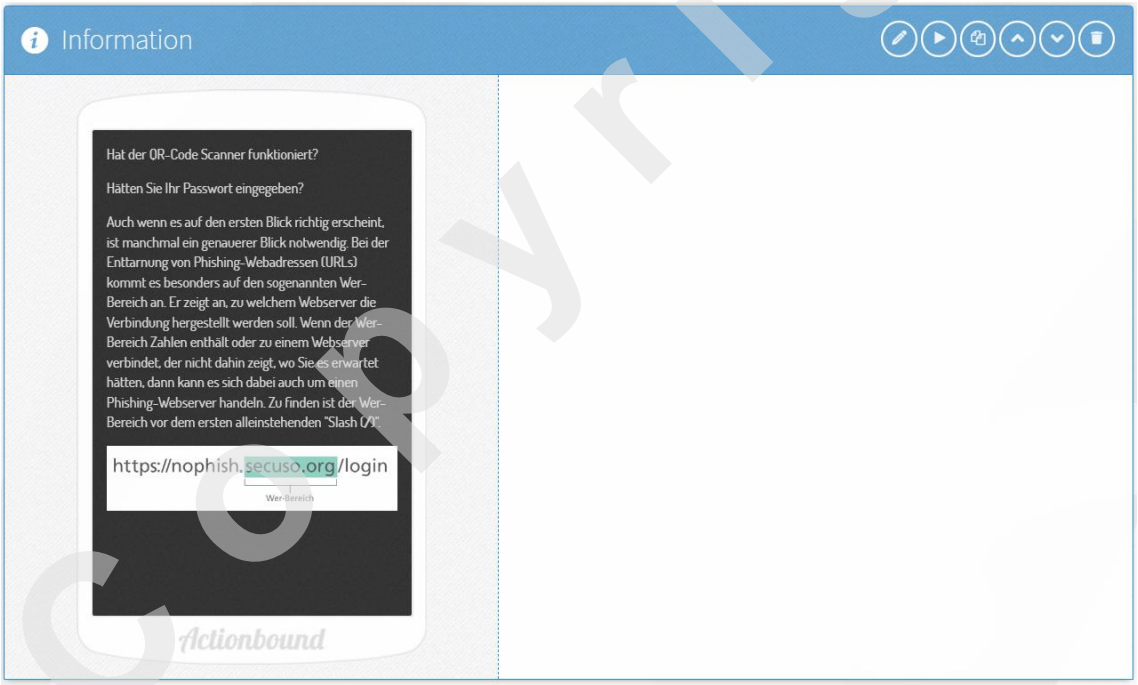


Quelle: Text übernommen aus: https://de.actionbound.com/bound/imnetzabersicherlevel1 (abgerufen am 30.08.2022)

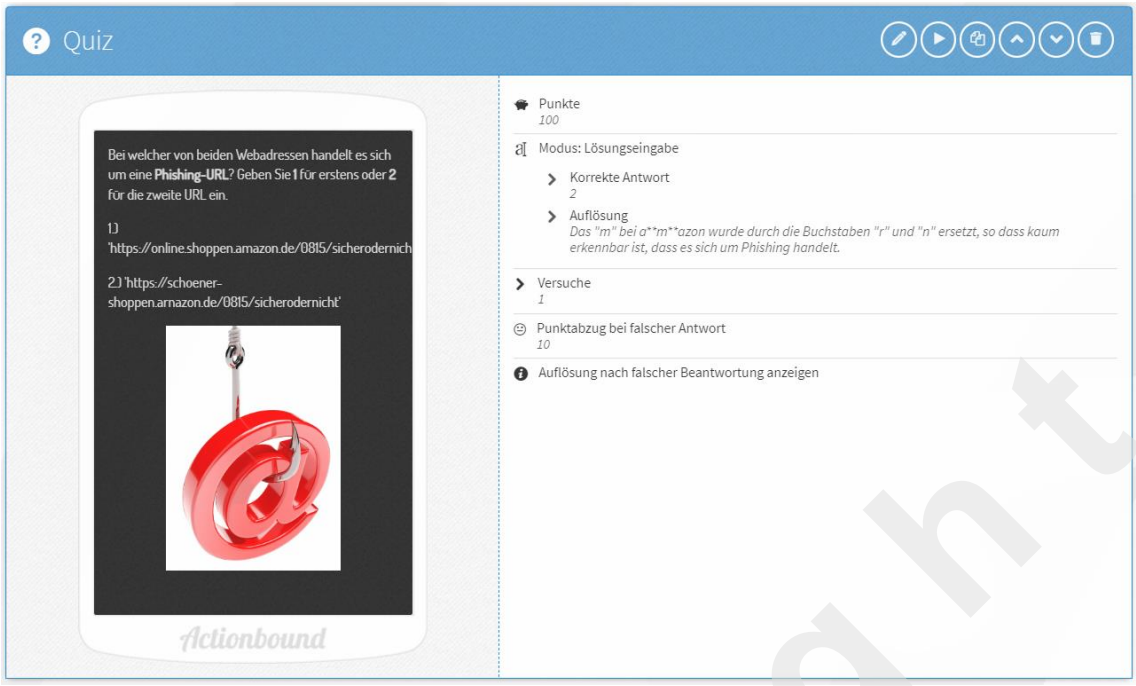


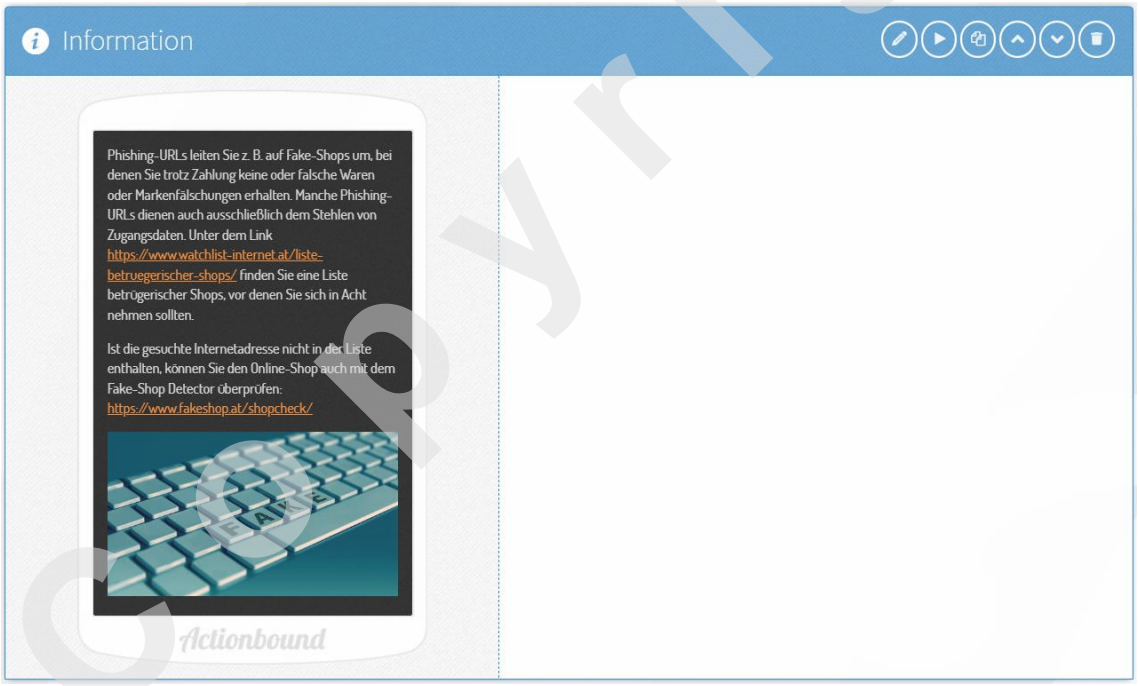
Copyright


Ort finden
Laden Sie sich aus dem App- oder Google Play Store die App "QR Code Scanner (PFA)" der Secuso Research Group herunter und achten Sie auf die Abfrage der Zugriffsberechtigungen.
Die App gehört zu den sogenannten "privacy friendly apps" und schützt Ihre Privatsphäre.
Scannen Sie den QR-Code, der sich an folgendem Standort befindet...
Link zum PlayStore
Actionbound
Punkte
100
Koordinate
51.754044, 11.968181
Finden des Ortes zum Fortsetzen erforderlich. Überspringen nicht möglich.
Karte mit Ziel und aktuellem Standort anzeigen
L 73
Köthen
© OpenStreetMap


Information
Hat der QR-Code Scanner funktioniert?
Hätten Sie Ihr Passwort eingegeben?
Auch wenn es auf den ersten Blick richtig erscheint, ist manchmal ein genauerer Blick notwendig. Bei der Enttarnung von Phishing-Webadressen (URLs) kommt es besonders auf den sogenannten Wer-Bereich an. Er zeigt an, zu welchem Webserver die Verbindung hergestellt werden soll. Wenn der Wer-Bereich Zahlen enthält oder zu einem Webserver verbindet, der nicht dahin zeigt, wo Sie es erwartet hätten, dann kann es sich dabei auch um einen Phishing-Webserver handeln. Zu finden ist der Wer-Bereich vor dem ersten alleinstehenden "Slash (/)".
https://nophish.secuso.org/login
Wer-Bereich
Actionbound

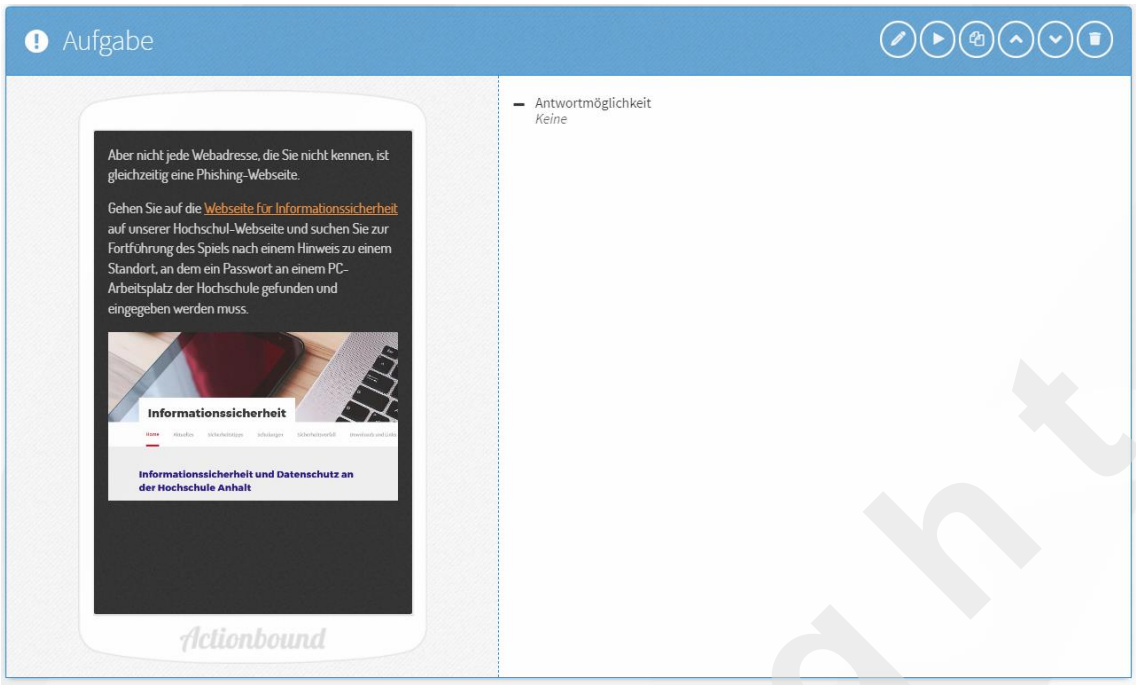
Copyright

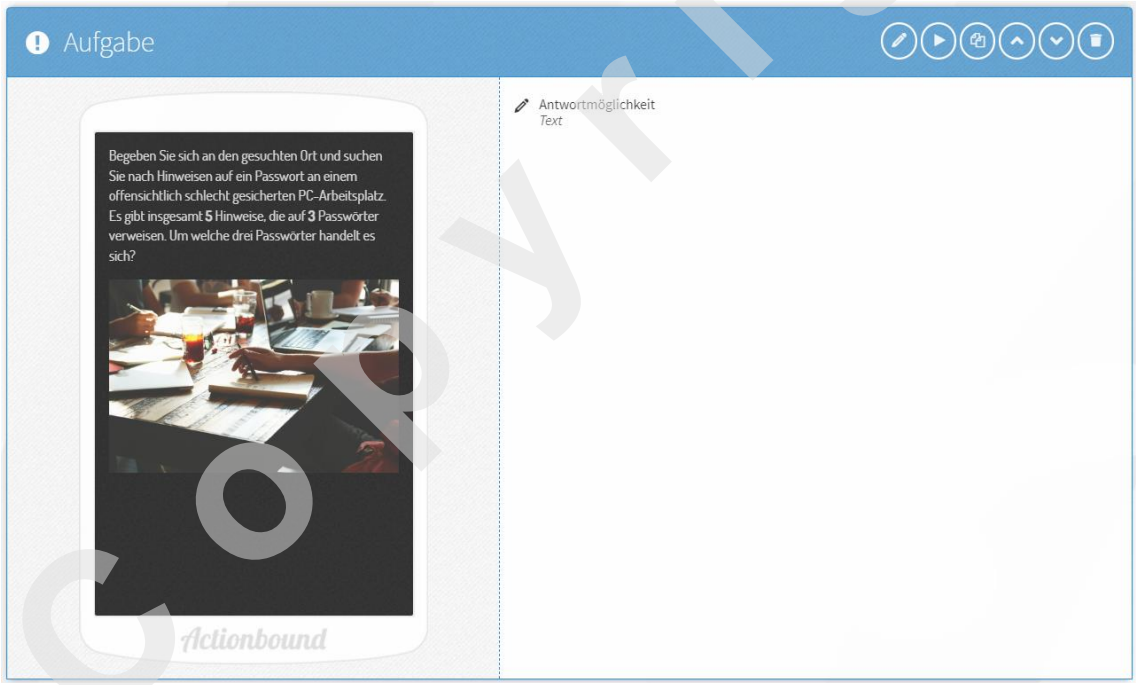




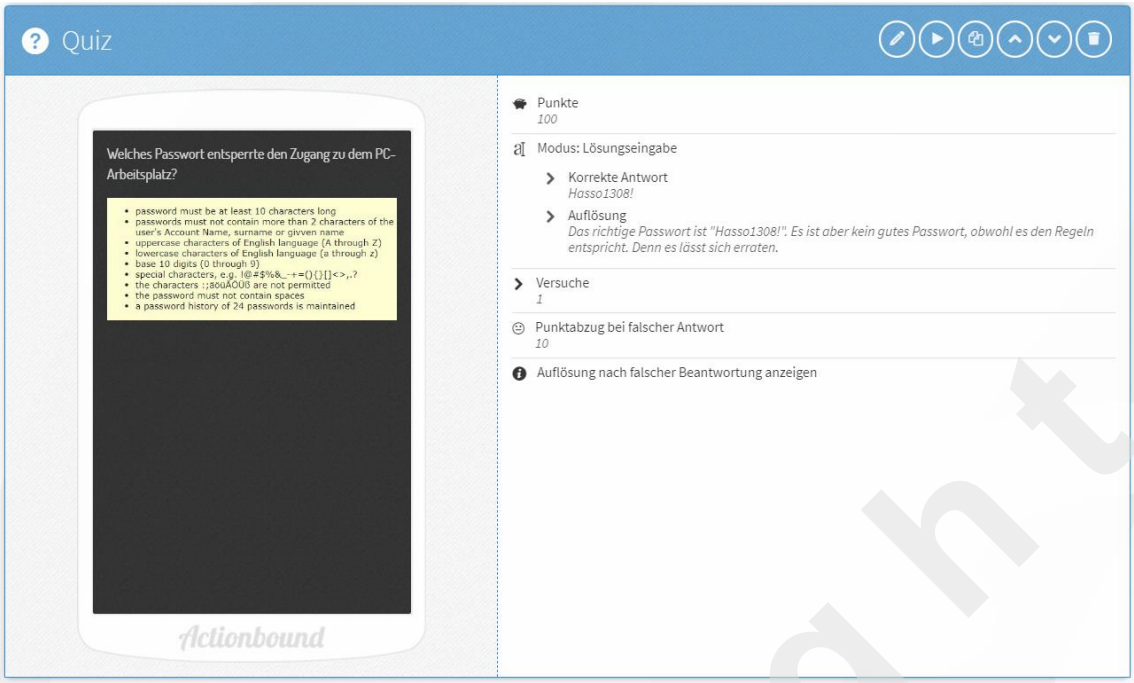
Quelle: Text übernommen und verändert aus:
https://www.watchlist-internet.at/online-shops-ueberpruefen/ (abgerufen am 30.08.2022)

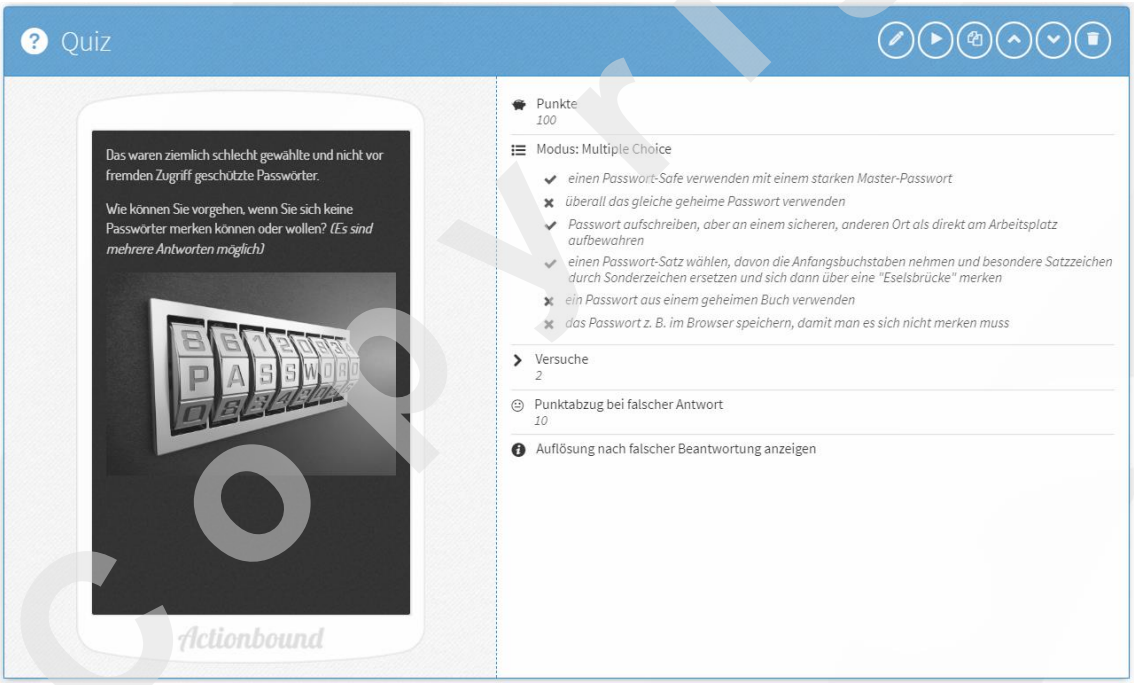
Copyright


Aufgabe
Aber nicht jede Webadresse, die Sie nicht kennen, ist gleichzeitig eine Phishing-Webseite.
Gehen Sie auf die Webseite für Informationssicherheit auf unserer Hochschul-Webseite und suchen Sie zur Fortführung des Spiels nach einem Hinweis zu einem Standort, an dem ein Passwort an einem PC-Arbeitsplatz der Hochschule gefunden und eingegeben werden muss.
Informationssicherheit
Informationssicherheit und Datenschutz an der Hochschule Anhalt
Actionbound
Antwortmöglichkeit
Keine

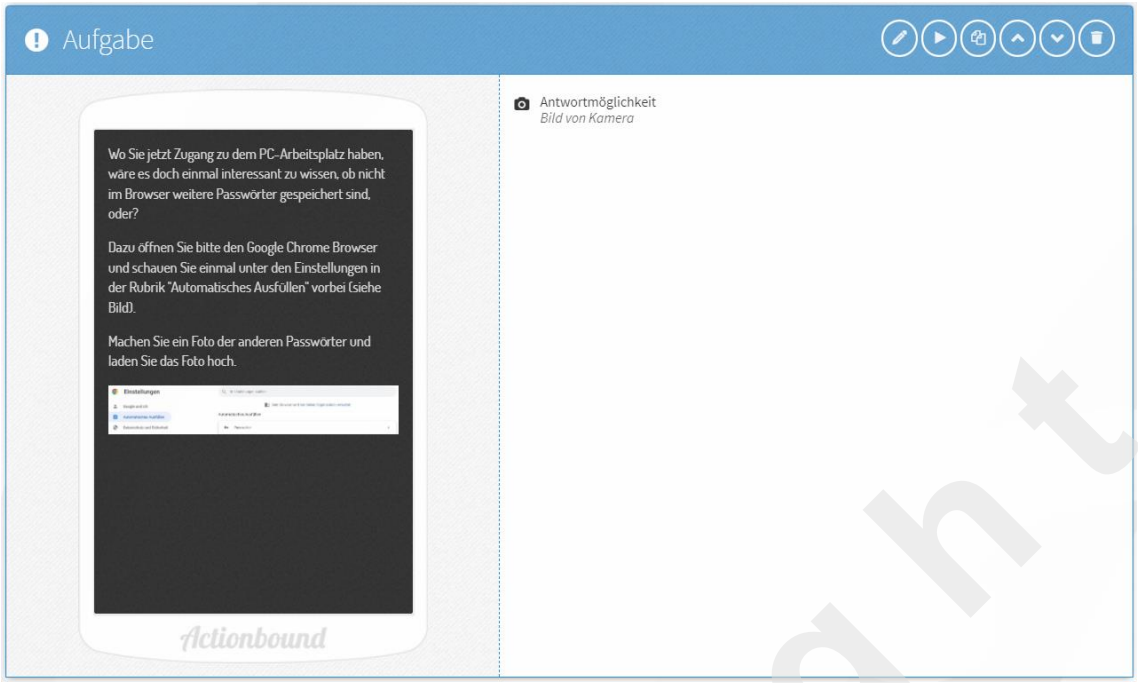

Aufgabe
Begeben Sie sich an den gesuchten Ort und suchen Sie nach Hinweisen auf ein Passwort an einem offensichtlich schlecht gesicherten PC-Arbeitsplatz. Es gibt insgesamt 5 Hinweise, die auf 3 Passwörter verweisen. Um welche drei Passwörter handelt es sich?
Actionbound
Antwortmöglichkeit
Text

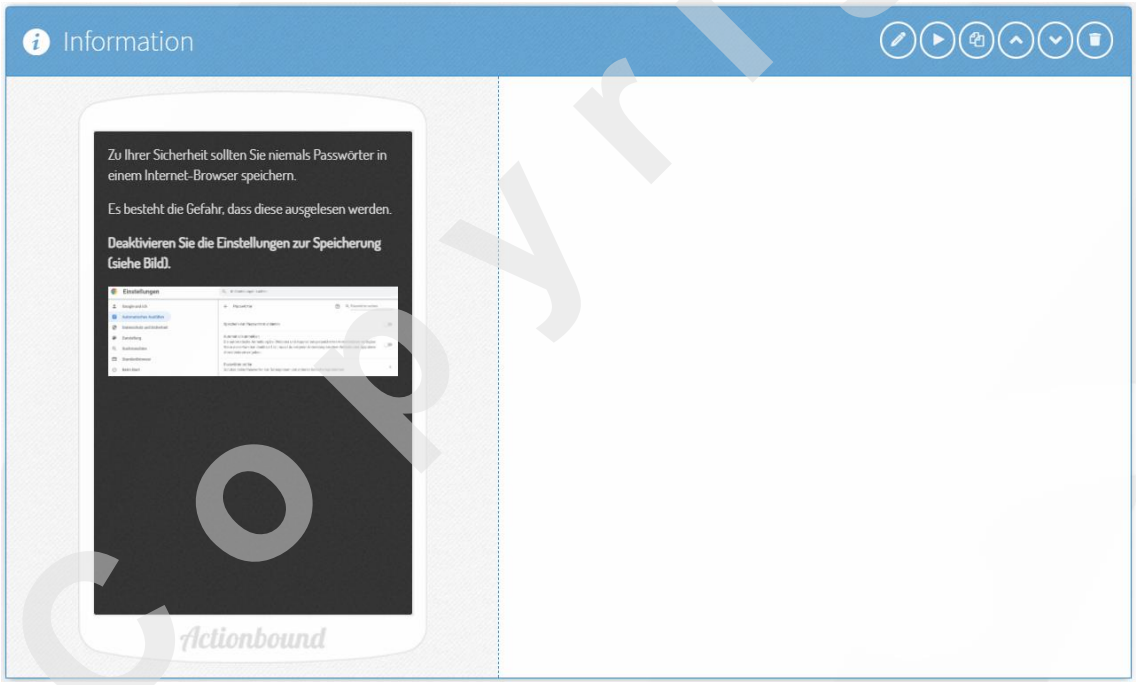
Copyright


Quiz
Welches Passwort entsperrte den Zugang zu dem PC-Arbeitsplatz?
password must be at least 10 characters long
passwords must not contain more than 2 characters of the user's Account Name, surname or given name
uppercase characters of English language (A through Z)
lowercase characters of English language (a through z)
base 10 digits (0 through 9)
special characters, e.g. !@#$%&_-+=(){}[]<>,.?
the characters :;äöüÄÖÜß are not permitted
the password must not contain spaces
a password history of 24 passwords is maintained
Actionbound
Punkte
100
Modus: Lösungseingabe
Korrekte Antwort
Hasso1308!
Auflösung
Das richtige Passwort ist "Hasso1308!". Es ist aber kein gutes Passwort, obwohl es den Regeln entspricht. Denn es lässt sich erraten.
Versuche
1
Punktabzug bei falscher Antwort
10
Auflösung nach falscher Beantwortung anzeigen

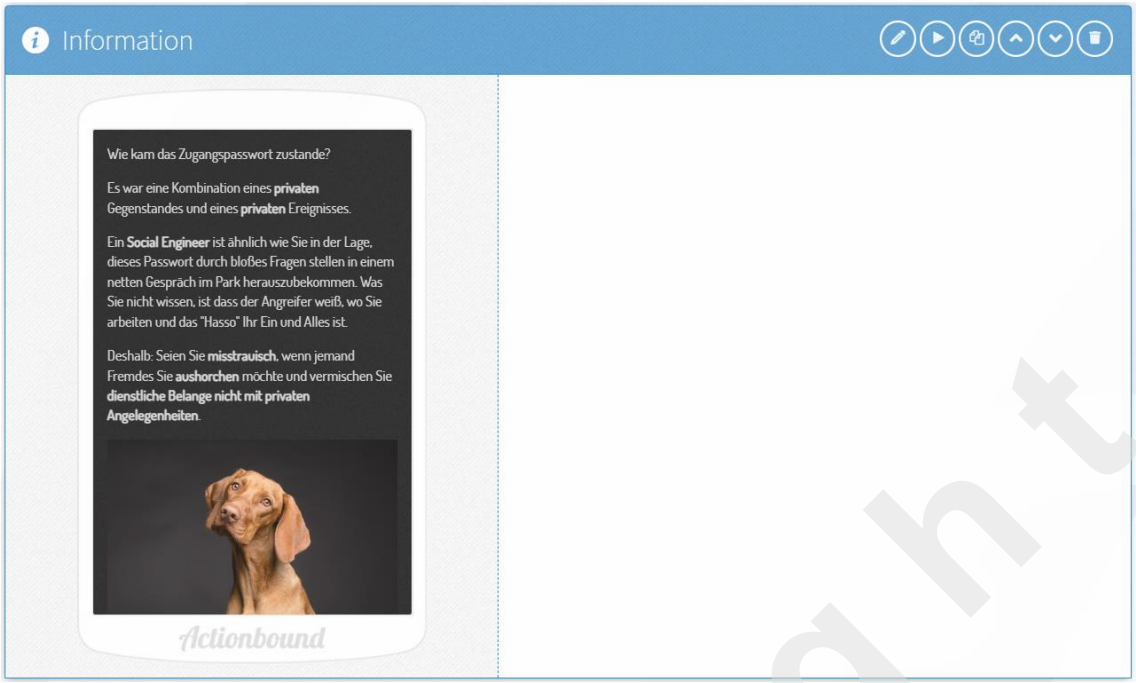

Quiz
Das waren ziemlich schlecht gewählte und nicht vor fremden Zugriff geschützte Passwörter.
Wie können Sie vorgehen, wenn Sie sich keine Passwörter merken können oder wollen? (Es sind mehrere Antworten möglich)
Actionbound
Punkte
100
Modus: Multiple Choice
einen Passwort-Safe verwenden mit einem starken Master-Passwort
überall das gleiche geheime Passwort verwenden
Passwort aufschreiben, aber an einem sicheren, anderen Ort als direkt am Arbeitsplatz aufbewahren
einen Passwort-Satz wählen, davon die Anfangsbuchstaben nehmen und besondere Satzzeichen durch Sonderzeichen ersetzen und sich dann über eine "Eselsbrücke" merken
ein Passwort aus einem geheimen Buch verwenden
das Passwort z. B. im Browser speichern, damit man es sich nicht merken muss
Versuche
2
Punktabzug bei falscher Antwort
10
Auflösung nach falscher Beantwortung anzeigen

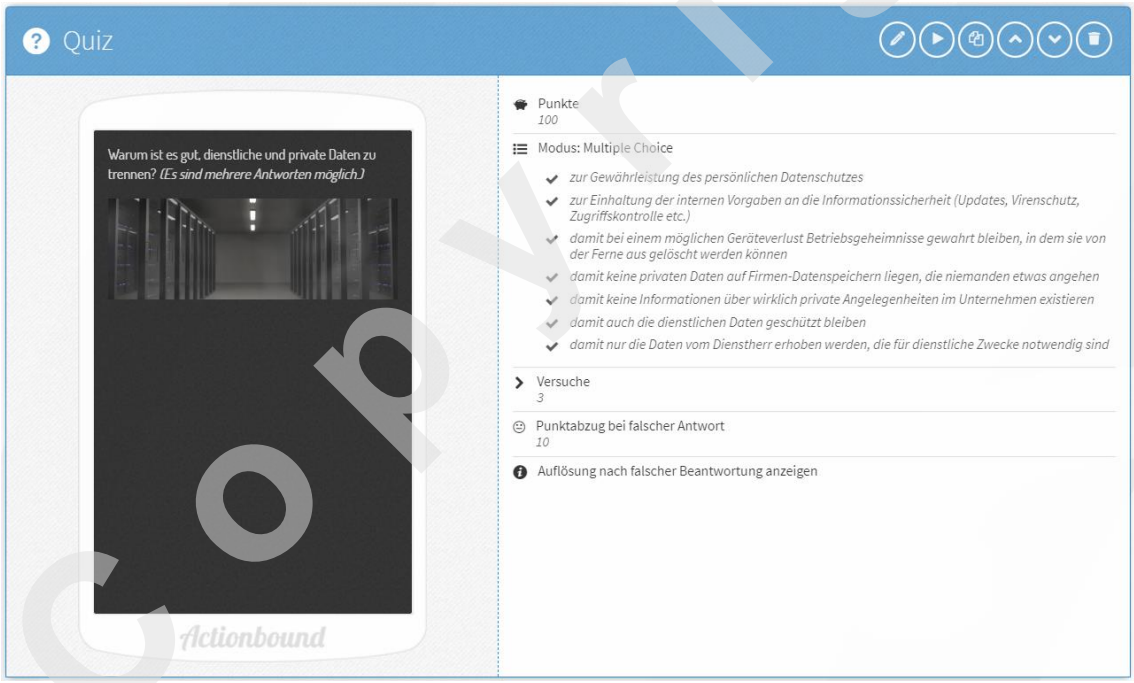
Copyright


Aufgabe
Wo Sie jetzt Zugang zu dem PC-Arbeitsplatz haben, wäre es doch einmal interessant zu wissen, ob nicht im Browser weitere Passwörter gespeichert sind, oder?
Dazu öffnen Sie bitte den Google Chrome Browser und schauen Sie einmal unter den Einstellungen in der Rubrik "Automatisches Ausfüllen" vorbei (siehe Bild).
Machen Sie ein Foto der anderen Passwörter und laden Sie das Foto hoch.
Antwortmöglichkeit
Bild von Kamera
Actionbound

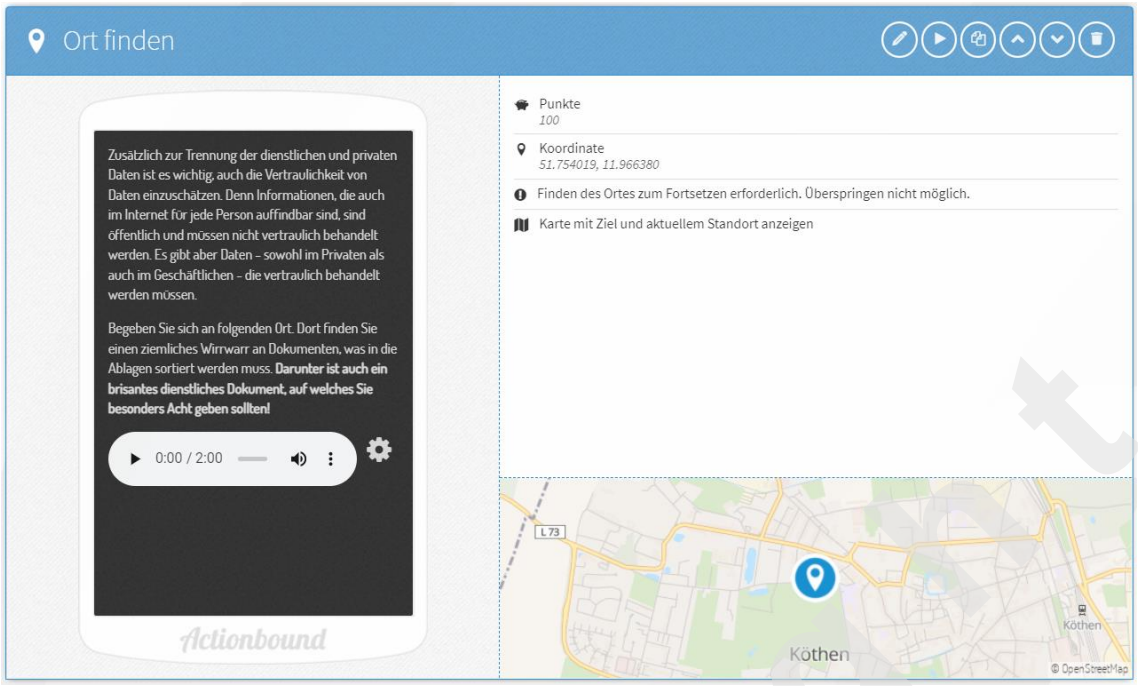

Information
Zu Ihrer Sicherheit sollten Sie niemals Passwörter in einem Internet-Browser speichern.
Es besteht die Gefahr, dass diese ausgelesen werden.
Deaktivieren Sie die Einstellungen zur Speicherung (siehe Bild).
Actionbound

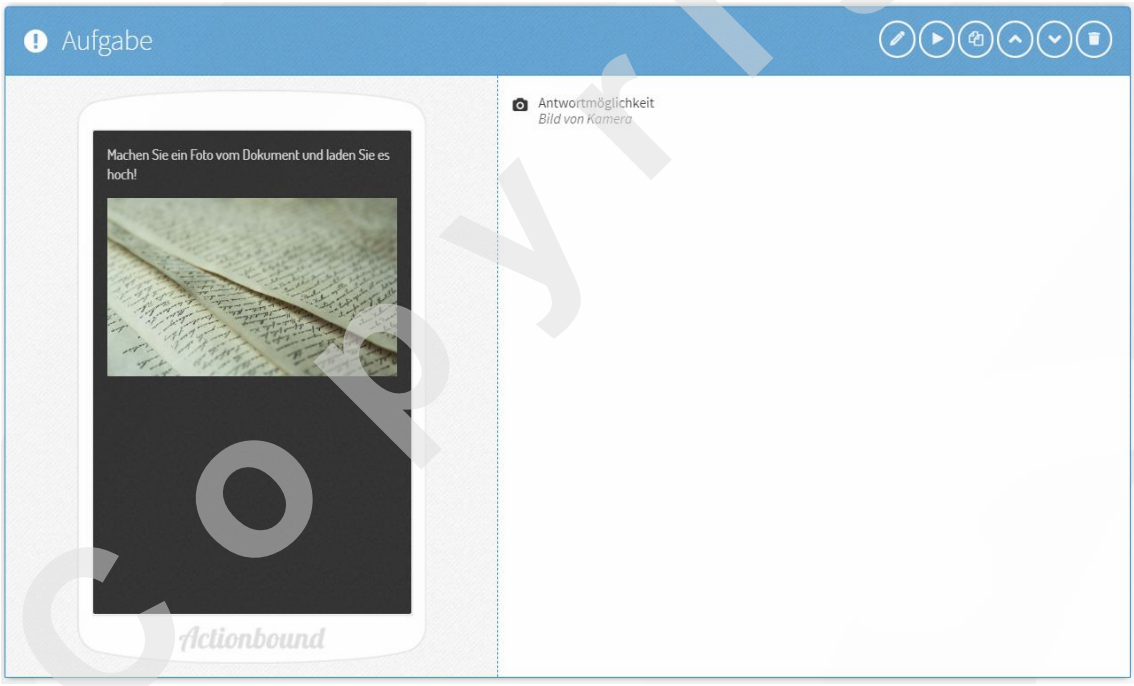
Copyright


Information
Wie kam das Zugangspasswort zustande?
Es war eine Kombination eines **privaten** Gegenstandes und eines **privaten** Ereignisses.
Ein **Social Engineer** ist ähnlich wie Sie in der Lage, dieses Passwort durch bloßes Fragen stellen in einem netten Gespräch im Park herauszubekommen. Was Sie nicht wissen, ist dass der Angreifer weiß, wo Sie arbeiten und das "Hasso" Ihr Ein und Alles ist.
Deshalb: Seien Sie **misstrauisch**, wenn jemand Fremdes Sie **aushorchen** möchte und vermischen Sie **dienstliche Belange nicht mit privaten Angelegenheiten**.
Actionbound

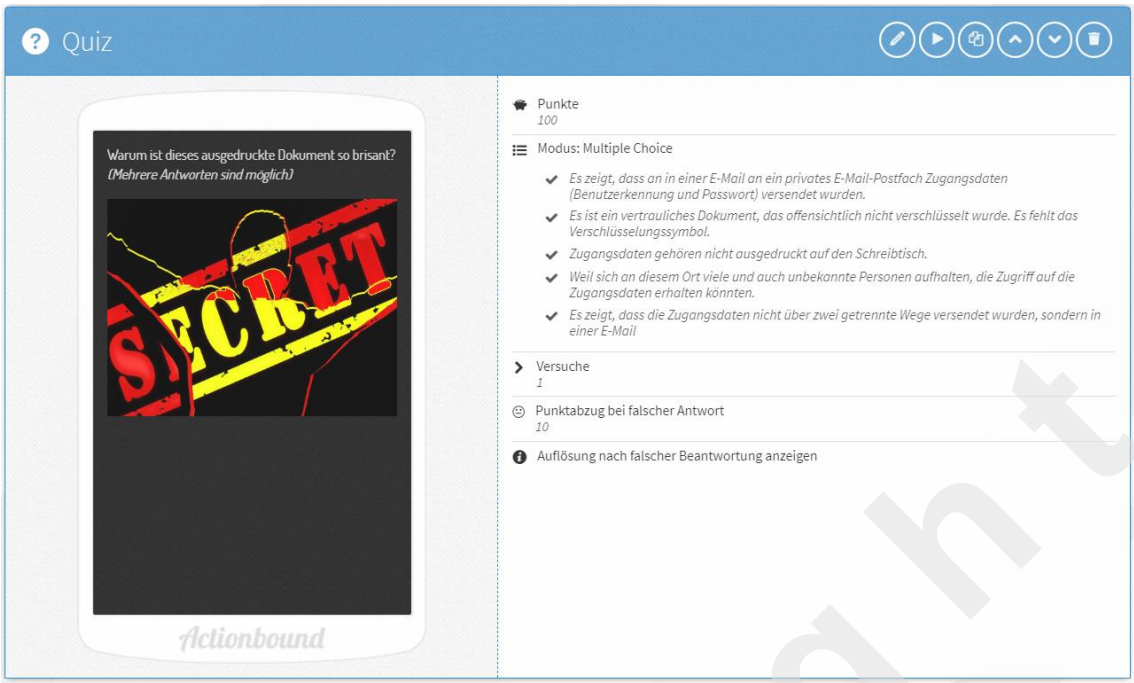

Quiz
Warum ist es gut, dienstliche und private Daten zu trennen? *(Es sind mehrere Antworten möglich.)*
Actionbound
Punkte
100
Modus: Multiple Choice
zur Gewährleistung des persönlichen Datenschutzes
zur Einhaltung der internen Vorgaben an die Informationssicherheit (Updates, Virenschutz, Zugriffskontrolle etc.)
damit bei einem möglichen Geräteverlust Betriebsgeheimnisse gewahrt bleiben, in dem sie von der Ferne aus gelöscht werden können
damit keine privaten Daten auf Firmen-Datenspeichern liegen, die niemanden etwas angehen
damit keine Informationen über wirklich private Angelegenheiten im Unternehmen existieren
damit auch die dienstlichen Daten geschützt bleiben
damit nur die Daten vom Dienstherr erhoben werden, die für dienstliche Zwecke notwendig sind
Versuche
3
Punktabzug bei falscher Antwort
10
Auflösung nach falscher Beantwortung anzeigen

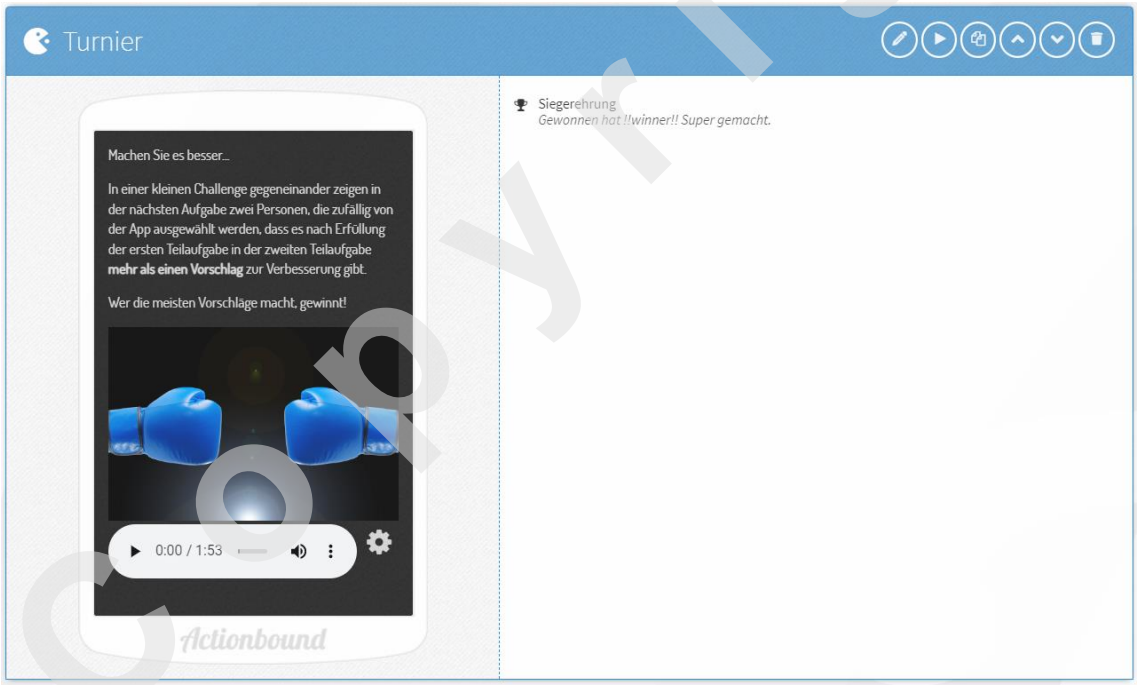
Copyright


Ort finden
Zusätzlich zur Trennung der dienstlichen und privaten Daten ist es wichtig, auch die Vertraulichkeit von Daten einzuschätzen. Denn Informationen, die auch im Internet für jede Person auffindbar sind, sind öffentlich und müssen nicht vertraulich behandelt werden. Es gibt aber Daten – sowohl im Privaten als auch im Geschäftlichen – die vertraulich behandelt werden müssen.
Begeben Sie sich an folgenden Ort. Dort finden Sie einen ziemliches Wirrwarr an Dokumenten, was in die Ablagen sortiert werden muss. Darunter ist auch ein brisantes dienstliches Dokument, auf welches Sie besonders Acht geben sollten!
0:00 / 2:00
Actionbound
Punkte
100
Koordinate
51.754019, 11.966380
Finden des Ortes zum Fortsetzen erforderlich. Überspringen nicht möglich.
Karte mit Ziel und aktuellem Standort anzeigen
L 73
Köthen
© OpenStreetMap

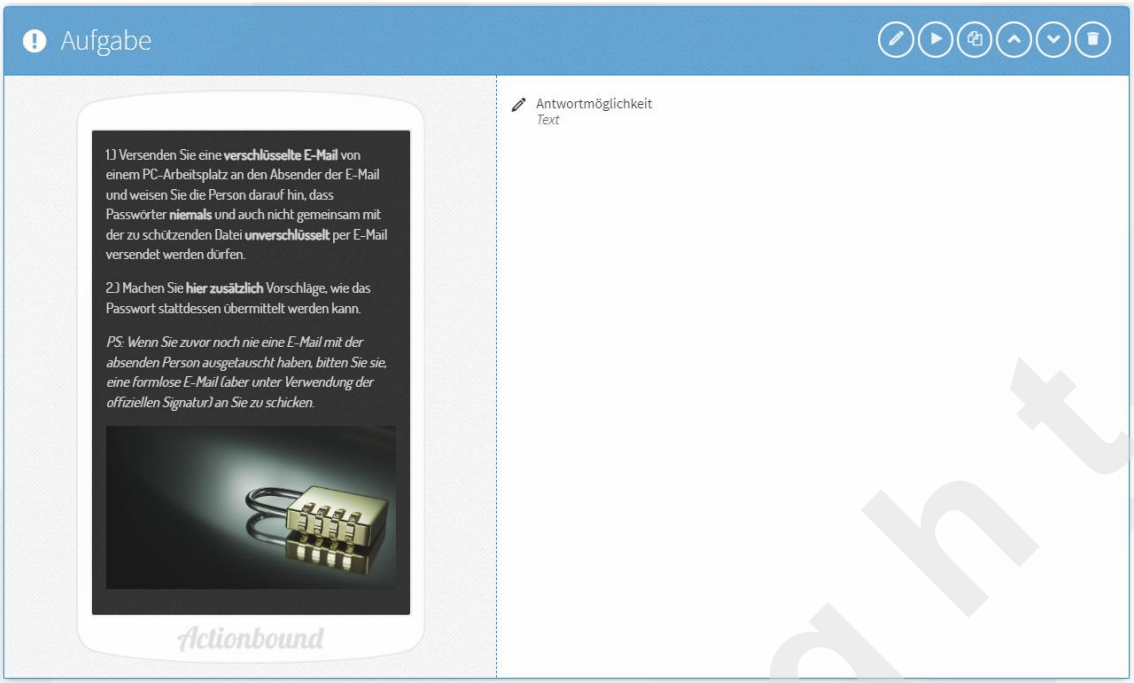

Aufgabe
Machen Sie ein Foto vom Dokument und laden Sie es hoch!
Actionbound
Antwortmöglichkeit
Bild von Kamera

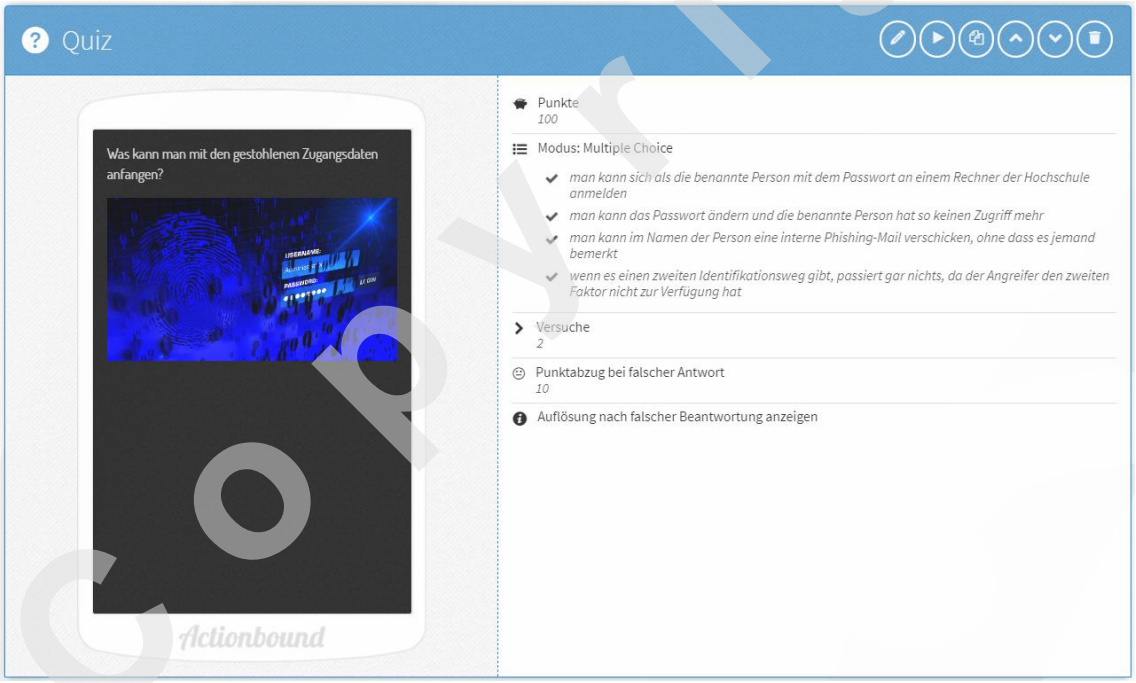
Copyright


Quiz
Warum ist dieses ausgedruckte Dokument so brisant?
(Mehrere Antworten sind möglich)
SECRET
Actionbound
Punkte
100
Modus: Multiple Choice
Es zeigt, dass an in einer E-Mail an ein privates E-Mail-Postfach Zugangsdaten (Benutzerkennung und Passwort) versendet wurden.
Es ist ein vertrauliches Dokument, das offensichtlich nicht verschlüsselt wurde. Es fehlt das Verschlüsselungssymbol.
Zugangsdaten gehören nicht ausgedruckt auf den Schreibtisch.
Weil sich an diesem Ort viele und auch unbekannte Personen aufhalten, die Zugriff auf die Zugangsdaten erhalten könnten.
Es zeigt, dass die Zugangsdaten nicht über zwei getrennte Wege versendet wurden, sondern in einer E-Mail
Versuche
1
Punktabzug bei falscher Antwort
10
Auflösung nach falscher Beantwortung anzeigen

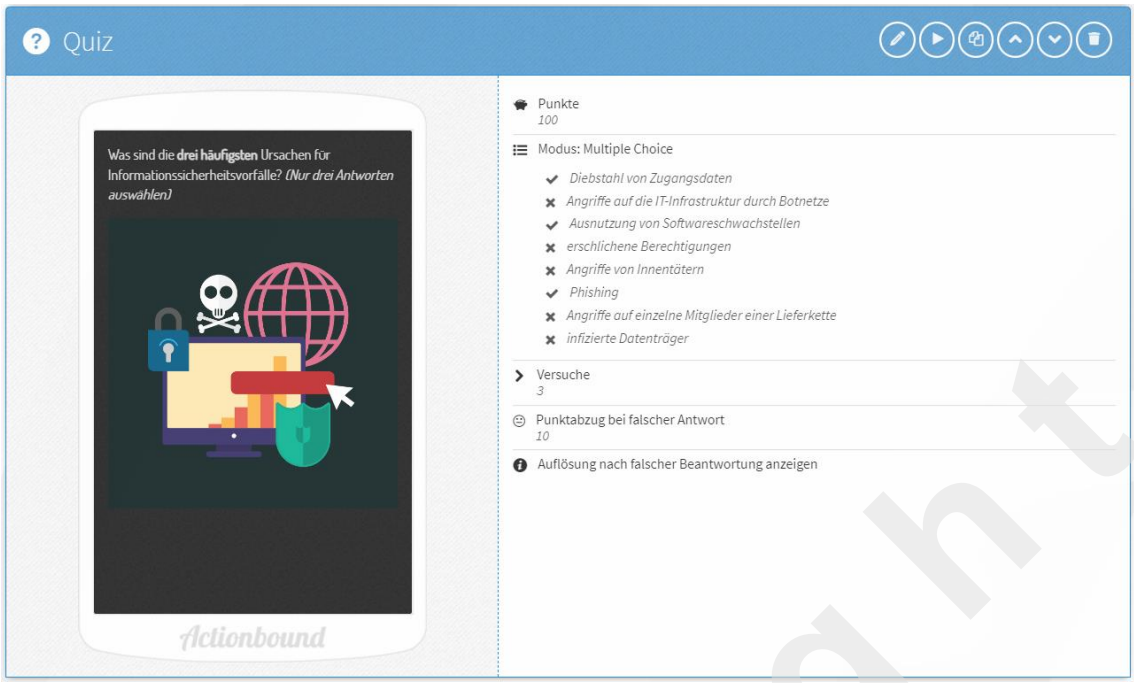

Turnier
Machen Sie es besser...
In einer kleinen Challenge gegeneinander zeigen in der nächsten Aufgabe zwei Personen, die zufällig von der App ausgewählt werden, dass es nach Erfüllung der ersten Teilaufgabe in der zweiten Teilaufgabe mehr als einen Vorschlag zur Verbesserung gibt.
Wer die meisten Vorschläge macht, gewinnt!
0:00 / 1:53
Actionbound
Siegerehrung
Gewonnen hat !!winner!! Super gemacht.

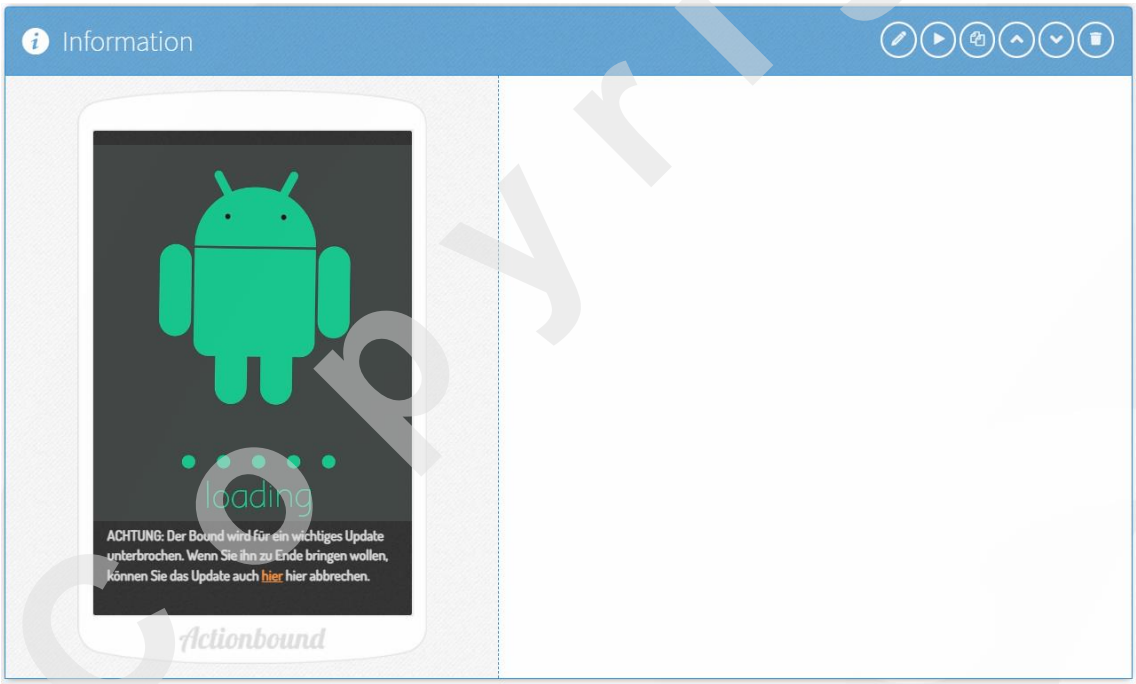
Copyright


Aufgabe
1.) Versenden Sie eine **verschlüsselte E-Mail** von einem PC-Arbeitsplatz an den Absender der E-Mail und weisen Sie die Person darauf hin, dass Passwörter **niemals** und auch nicht gemeinsam mit der zu schützenden Datei **unverschlüsselt** per E-Mail versendet werden dürfen.
2.) Machen Sie **hier zusätzlich** Vorschläge, wie das Passwort stattdessen übermittelt werden kann.
PS: Wenn Sie zuvor noch nie eine E-Mail mit der absenden Person ausgetauscht haben, bitten Sie sie, eine formlose E-Mail (aber unter Verwendung der offiziellen Signatur) an Sie zu schicken.
Actionbound
Antwortmöglichkeit
Text

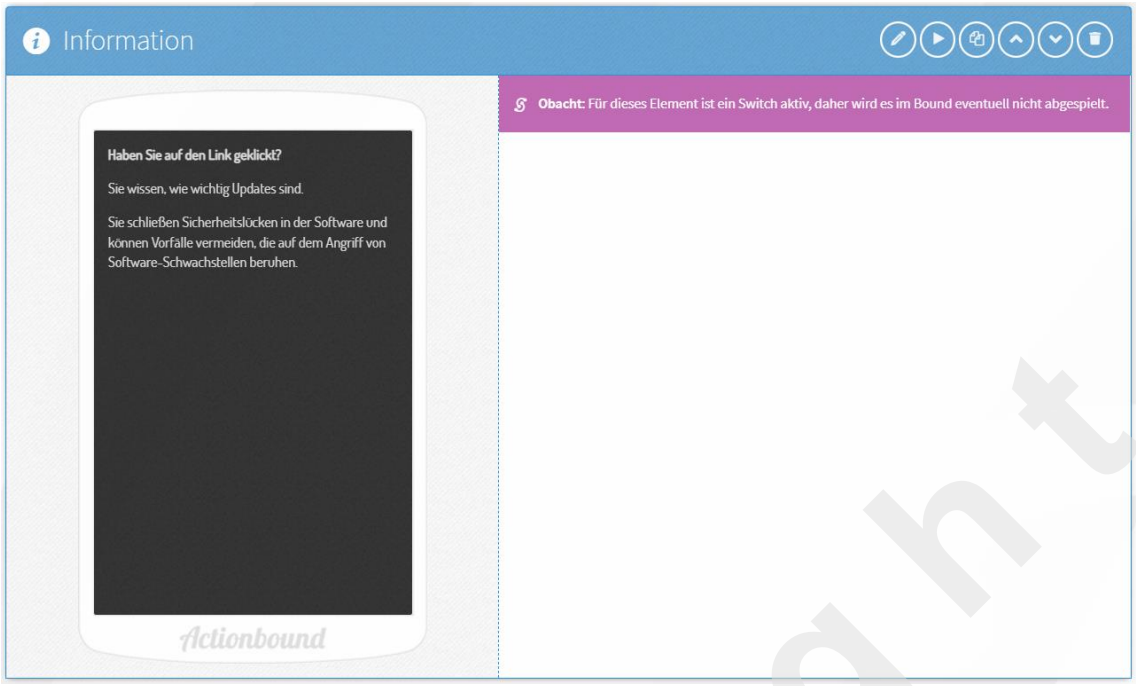

Quiz
Was kann man mit den gestohlenen Zugangsdaten anfangen?
Actionbound
Punkte
100
Modus: Multiple Choice
man kann sich als die benannte Person mit dem Passwort an einem Rechner der Hochschule anmelden
man kann das Passwort ändern und die benannte Person hat so keinen Zugriff mehr
man kann im Namen der Person eine interne Phishing-Mail verschicken, ohne dass es jemand bemerkt
wenn es einen zweiten Identifikationsweg gibt, passiert gar nichts, da der Angreifer den zweiten Faktor nicht zur Verfügung hat
Versuche
2
Punktabzug bei falscher Antwort
10
Auflösung nach falscher Beantwortung anzeigen

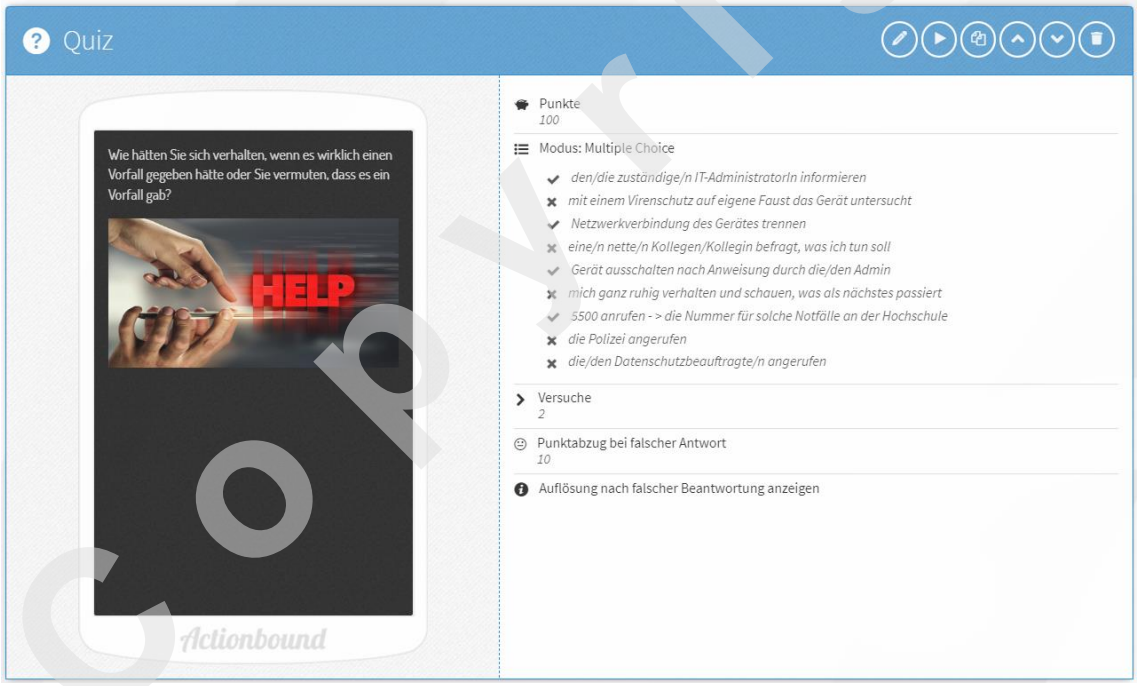
Copyright


Quiz
Was sind die drei häufigsten Ursachen für Informationssicherheitsvorfälle? (Nur drei Antworten auswählen)
Actionbound
Punkte
100
Modus: Multiple Choice
Diebstahl von Zugangsdaten
Angriffe auf die IT-Infrastruktur durch Botnetze
Ausnutzung von Softwareschwachstellen
erschlichene Berechtigungen
Angriffe von Innentätern
Phishing
Angriffe auf einzelne Mitglieder einer Lieferkette
infizierte Datenträger
Versuche
3
Punktabzug bei falscher Antwort
10
Auflösung nach falscher Beantwortung anzeigen

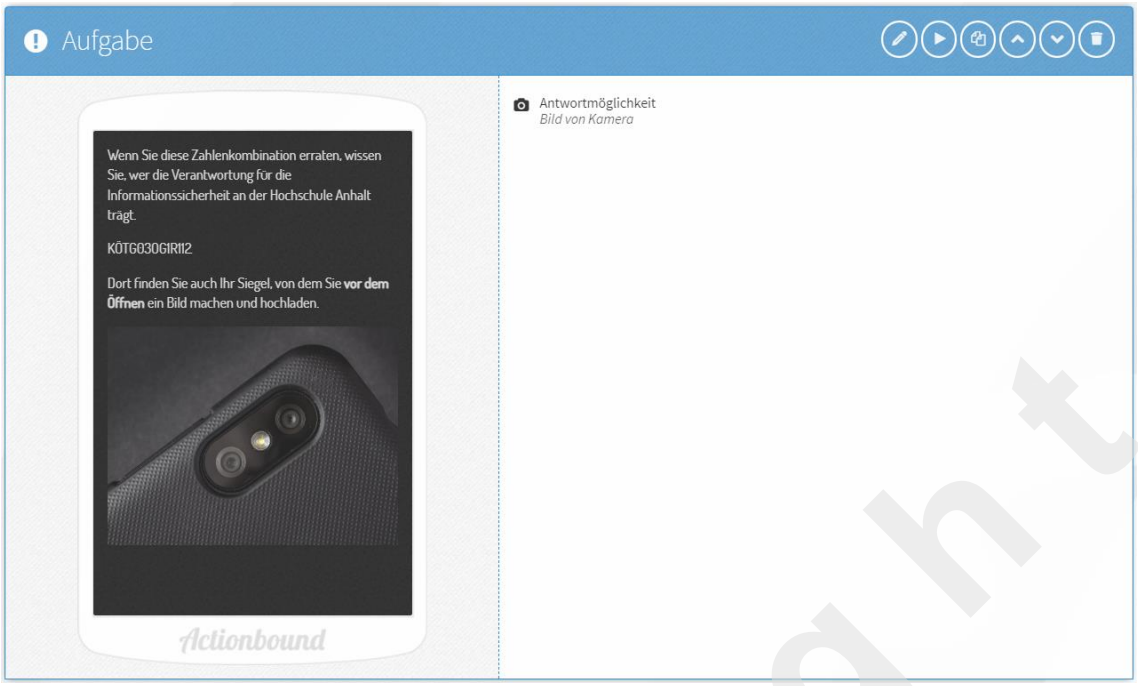

Information
loading
ACHTUNG: Der Bound wird für ein wichtiges Update unterbrochen. Wenn Sie ihn zu Ende bringen wollen, können Sie das Update auch hier hier abbrechen.
Actionbound

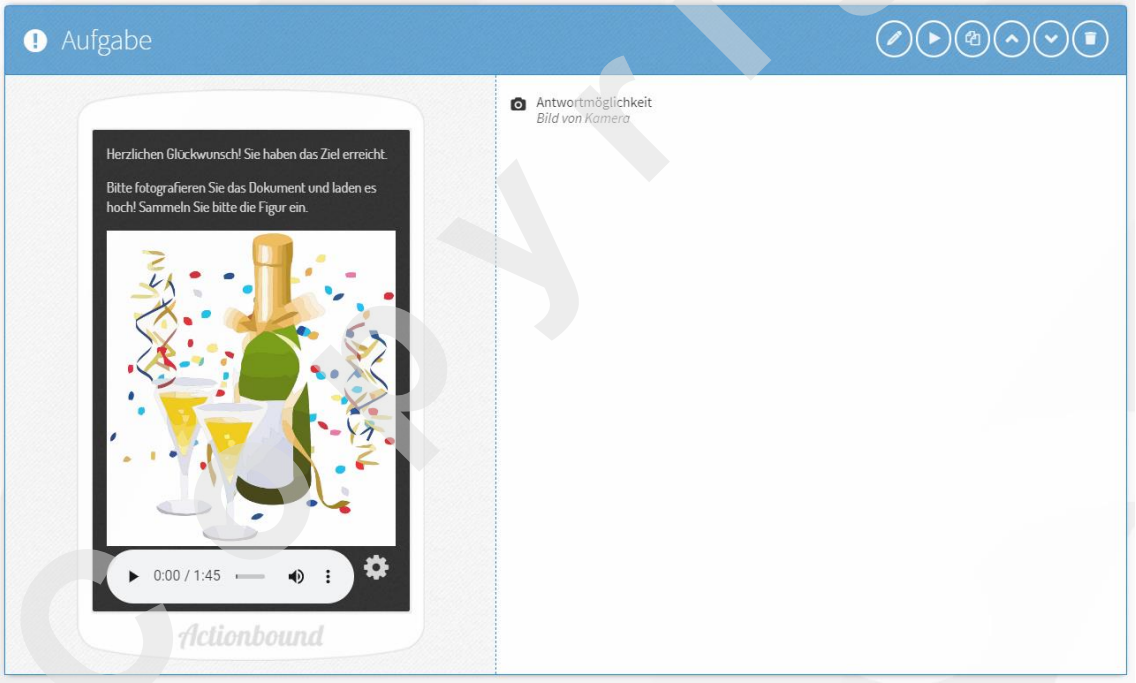
Copyright


Information
Obacht: Für dieses Element ist ein Switch aktiv, daher wird es im Bound eventuell nicht abgespielt.
Haben Sie auf den Link geklickt?
Sie wissen, wie wichtig Updates sind.
Sie schließen Sicherheitslücken in der Software und können Vorfälle vermeiden, die auf dem Angriff von Software-Schwachstellen beruhen.
Actionbound


Quiz
Wie hätten Sie sich verhalten, wenn es wirklich einen Vorfall gegeben hätte oder Sie vermuten, dass es ein Vorfall gab?
HELP
Actionbound
Punkte
100
Modus: Multiple Choice
den/die zuständige/n IT-AdministratorIn informieren
mit einem Virenschutz auf eigene Faust das Gerät untersucht
Netzwerkverbindung des Gerätes trennen
eine/n nette/n Kollegen/Kollegin befragt, was ich tun soll
Gerät ausschalten nach Anweisung durch die/den Admin
mich ganz ruhig verhalten und schauen, was als nächstes passiert
5500 anrufen - > die Nummer für solche Notfälle an der Hochschule
die Polizei angerufen
die/den Datenschutzbeauftragte/n angerufen
Versuche
2
Punktabzug bei falscher Antwort
10
Auflösung nach falscher Beantwortung anzeigen

Copyright


Aufgabe
Wenn Sie diese Zahlenkombination erraten, wissen Sie, wer die Verantwortung für die Informationssicherheit an der Hochschule Anhalt trägt.
K0TG030GIR112
Dort finden Sie auch Ihr Siegel, von dem Sie **vor dem Öffnen** ein Bild machen und hochladen.
Actionbound
Antwortmöglichkeit
Bild von Kamera


Aufgabe
Herzlichen Glückwunsch! Sie haben das Ziel erreicht.
Bitte fotografieren Sie das Dokument und laden es hoch! Sammeln Sie bitte die Figur ein.
0:00 / 1:45
Actionbound
Antwortmöglichkeit
Bild von Kamera

Copyright

Anlage 8: Flow-Kurzskala

Quelle: [138]

Copyright

Flow-Kurzskala (FKS)
von Falko Rheinberg, Regina Vollmeyer & Stefan Engeser (2003), Univ. Potsdam.

Alter: ☐ Jahre

Geschlecht: weiblich ☐
männlich ☐

Ich mache gerade _____ Uhrzeit _____
(Beziehen Sie sich bitte auf die eben unterbrochene Tätigkeit.)

	Trifft nicht zu			teils-teils			Trifft zu
• **Ich fühle mich optimal beansprucht.**	○	○	○	○	○	○	○
• **Meine Gedanken bzw. Aktivitäten laufen flüssig und glatt.**	○	○	○	○	○	○	○
• **Ich merke gar nicht, wie die Zeit vergeht.**	○	○	○	○	○	○	○
• **Ich habe keine Mühe, mich zu konzentrieren.**	○	○	○	○	○	○	○
• **Mein Kopf ist völlig klar.**	○	○	○	○	○	○	○
• **Ich bin ganz vertieft in das was ich gerade mache.**	○	○	○	○	○	○	○
• **Die richtigen Gedanken/Bewegungen kommen wie von selbst.**	○	○	○	○	○	○	○
• **Ich weiß bei jedem Schritt, was ich zu tun habe.**	○	○	○	○	○	○	○
• **Ich habe das Gefühl, den Ablauf unter Kontrolle zu haben.**	○	○	○	○	○	○	○
• **Ich bin völlig selbstvergessen.**	○	○	○	○	○	○	○
• **Es steht etwas für mich Wichtiges auf dem Spiel.**	○	○	○	○	○	○	○
• **Ich darf jetzt keine Fehler machen.**	○	○	○	○	○	○	○
• **Ich mache mir Sorgen über einen Misserfolg.**	○	○	○	○	○	○	○

Flow: Item 1 -10; Worry: Item11 – 13. T- Norms: Rheinberg (2004) *Motivationsdiagnostik*. Göttingen Hogrefe.

Copyright

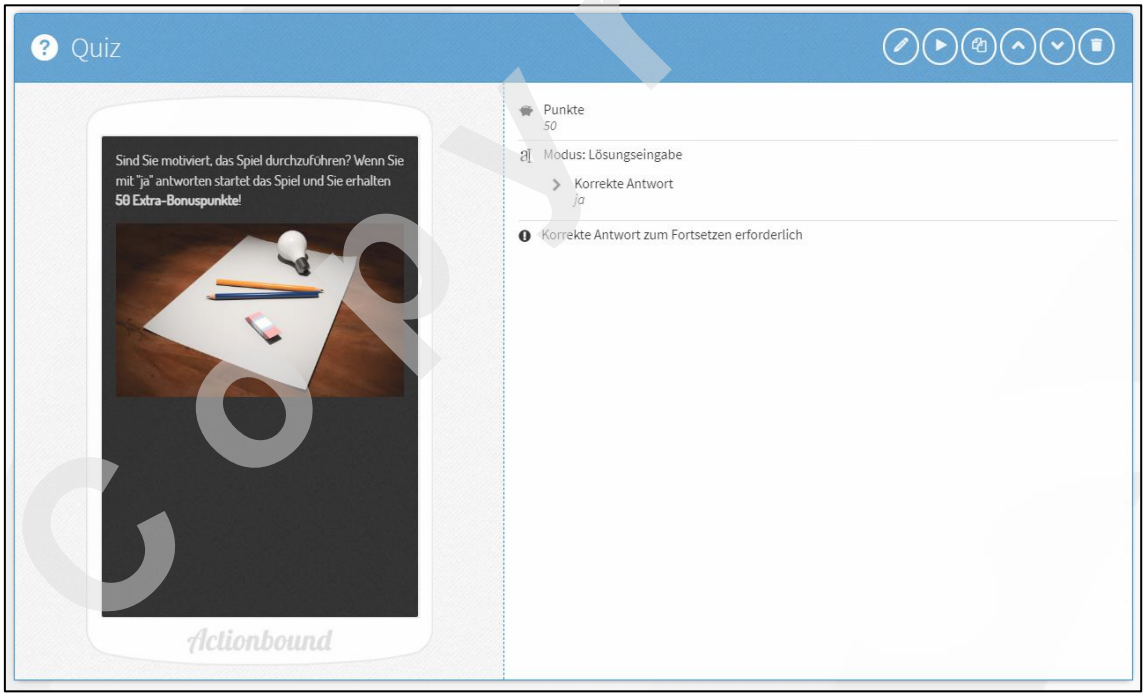
Anlage 9: Beispiele der Einhaltung der Design-Empfehlungen

Quellen: eigene Darstellungen aus der Lernplattform Moodle und der Anwendung Actionbound

Copyright

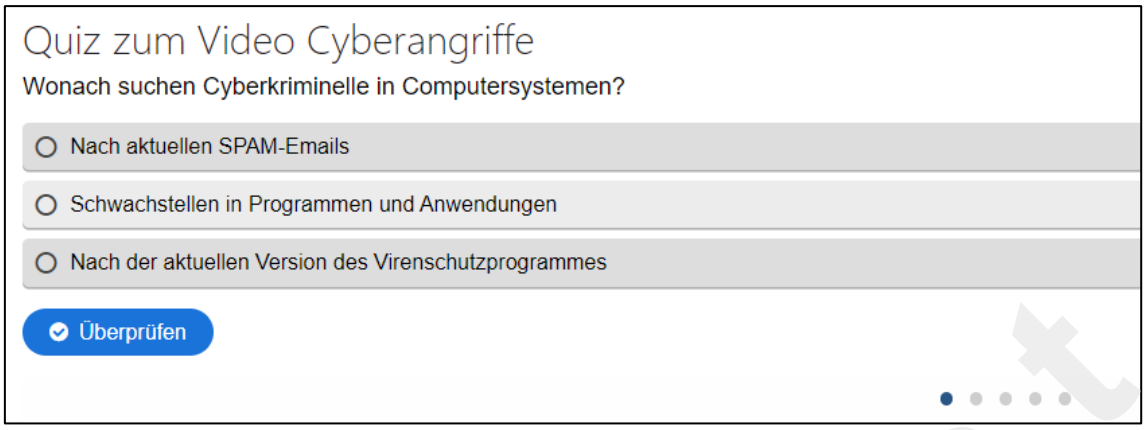
schnelles Erfolgserlebnis durch Verleih von Level-Abzeichen bei wenigen Erfahrungspunkten (Moodle):

schnell und einfach verdiente Punkte (Actionbound):

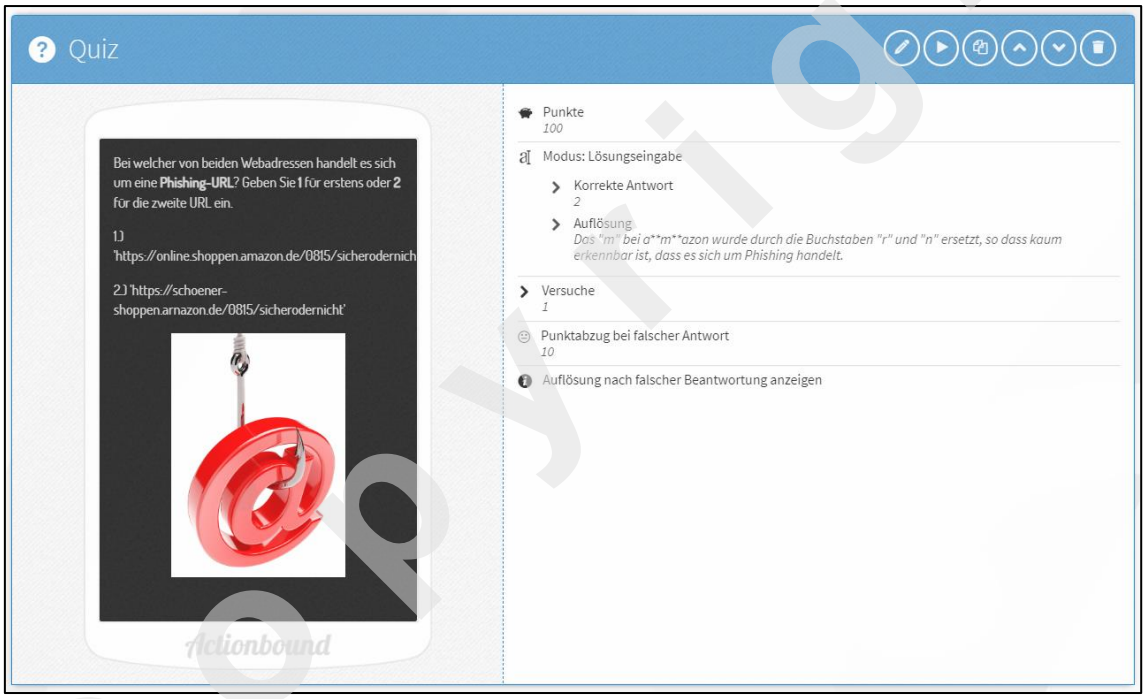


Copyright

Quiz auf freiwilliger Basis (Moodle):

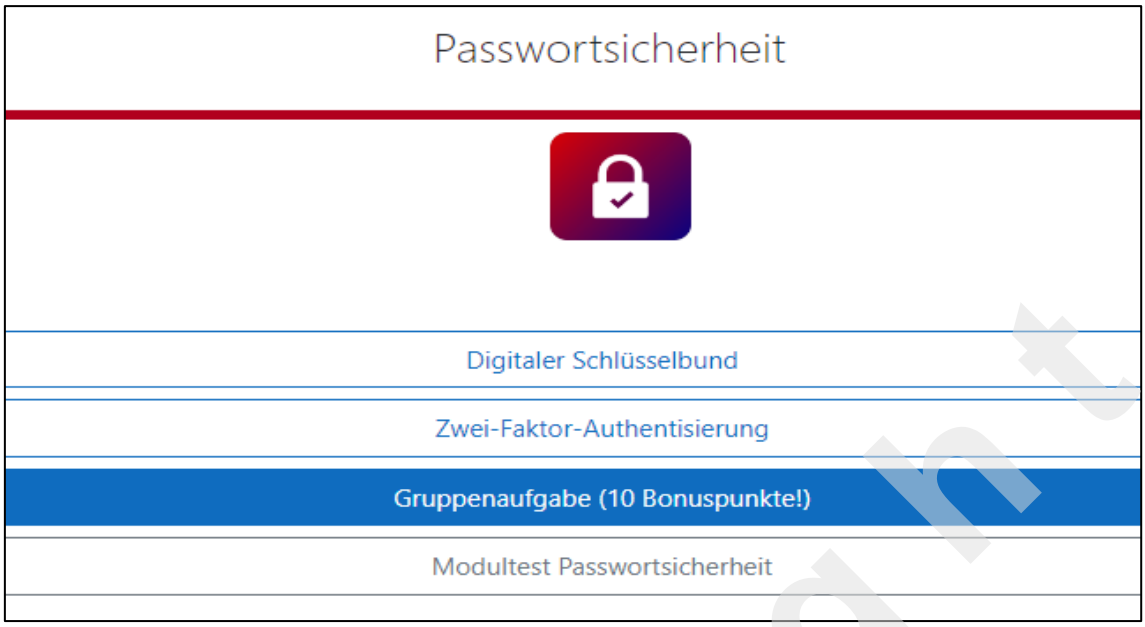


Quiz zum Selbsttest (Actionbound):

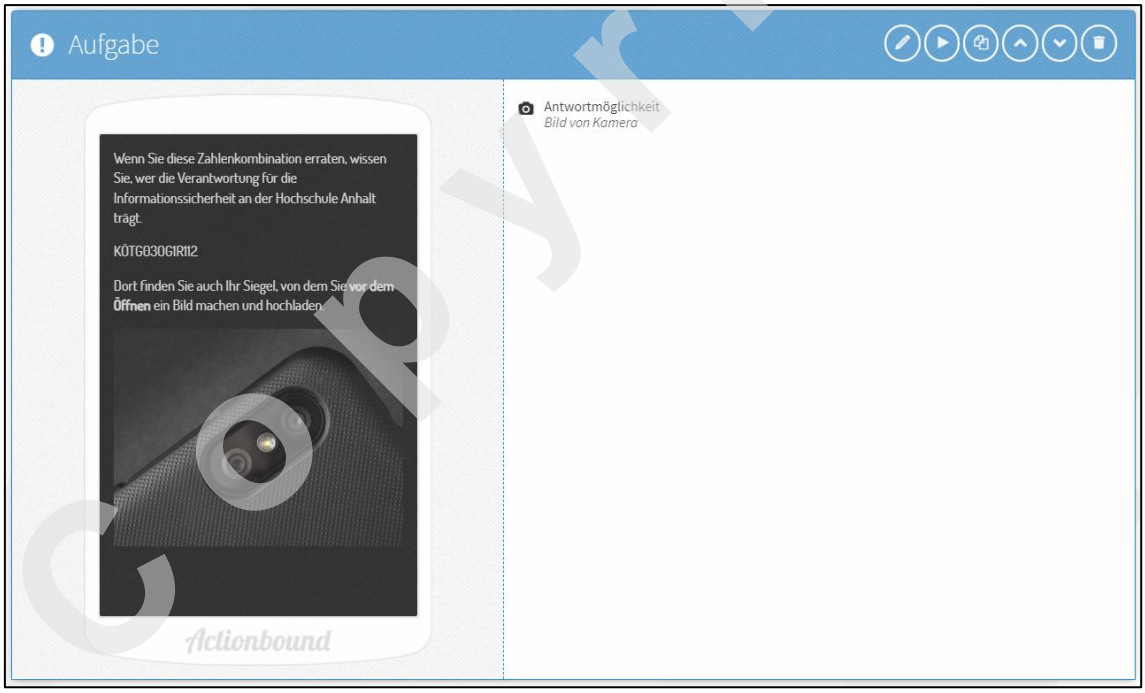


Copyright

Gruppenaufgabe im Lernmanagementsystem (Moodle):

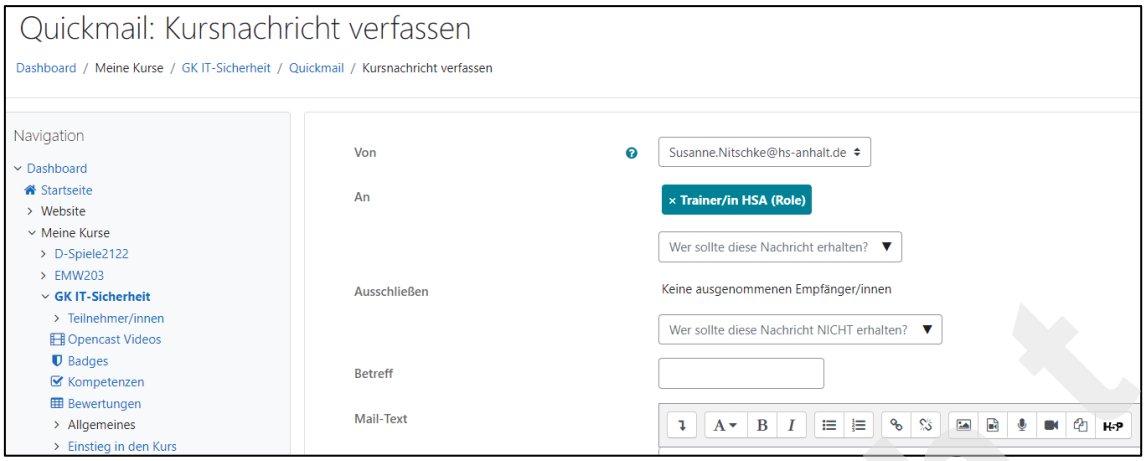


Lösung in der Gruppe finden (Actionbound):



Copyright

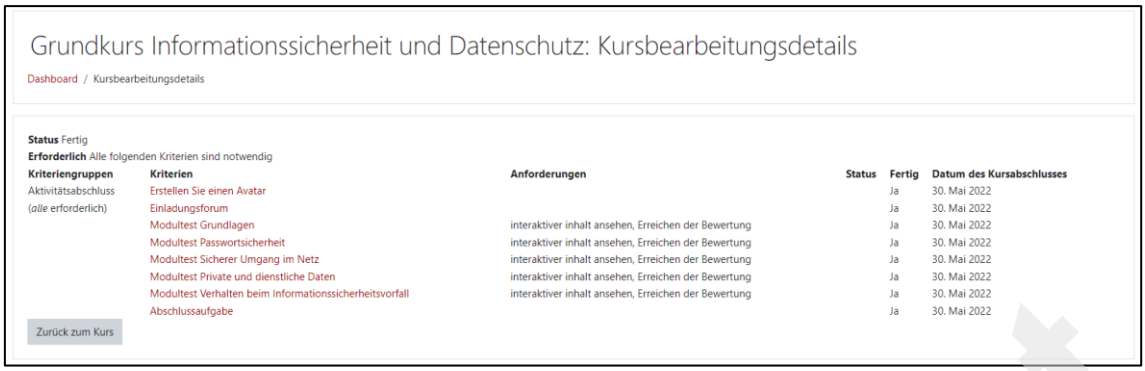
unabhängige Kommunikation außerhalb des Kurses (Moodle):



Bei der Durchführung des Bounds findet die persönliche Begleitung durch die Mentoren statt, so dass die Aufgabenlösung jederzeit begleitet ist. Zusätzlich wird nach jeder richtigen Antwort ein Feedback gegeben (siehe nächstes Bild).

Copyright

Abgleich zu gesetzten Zielen (Moodle):



Grundkurs Informationssicherheit und Datenschutz: Kursbearbeitungsdetails

Dashboard / Kursbearbeitungsdetails

Status Fertig
Erforderlich Alle folgenden Kriterien sind notwendig

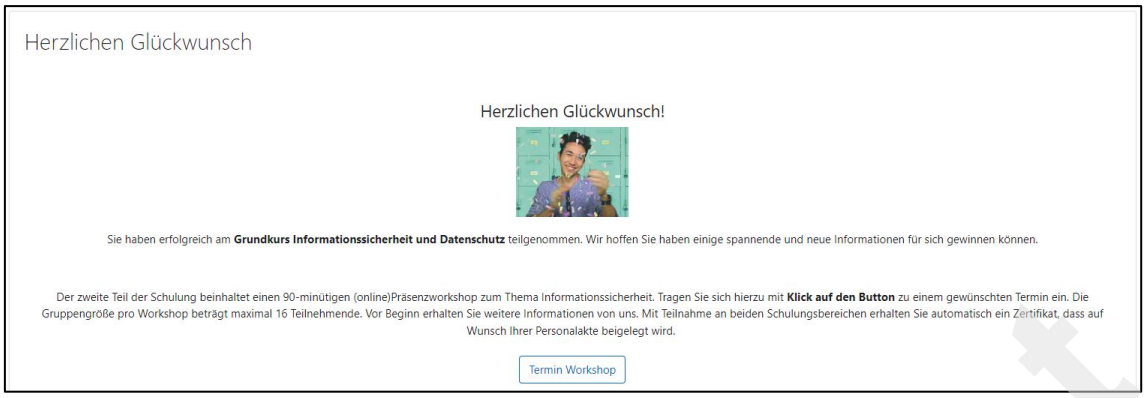
Kriteriengruppen	Kriterien	Anforderungen	Status	Fertig	Datum des Kursabschlusses
Aktivitätsabschluss (*alle* erforderlich)	Erstellen Sie einen Avatar			Ja	30. Mai 2022
	Einladungsforum			Ja	30. Mai 2022
	Modultest Grundlagen	interaktiver inhalt ansehen, Erreichen der Bewertung		Ja	30. Mai 2022
	Modultest Passwortsicherheit	interaktiver inhalt ansehen, Erreichen der Bewertung		Ja	30. Mai 2022
	Modultest Sicherer Umgang im Netz	interaktiver inhalt ansehen, Erreichen der Bewertung		Ja	30. Mai 2022
	Modultest Private und dienstliche Daten	interaktiver inhalt ansehen, Erreichen der Bewertung		Ja	30. Mai 2022
	Modultest Verhalten beim Informationssicherheitsvorfall	interaktiver inhalt ansehen, Erreichen der Bewertung		Ja	30. Mai 2022
	Abschlussaufgabe			Ja	30. Mai 2022

Zurück zum Kurs

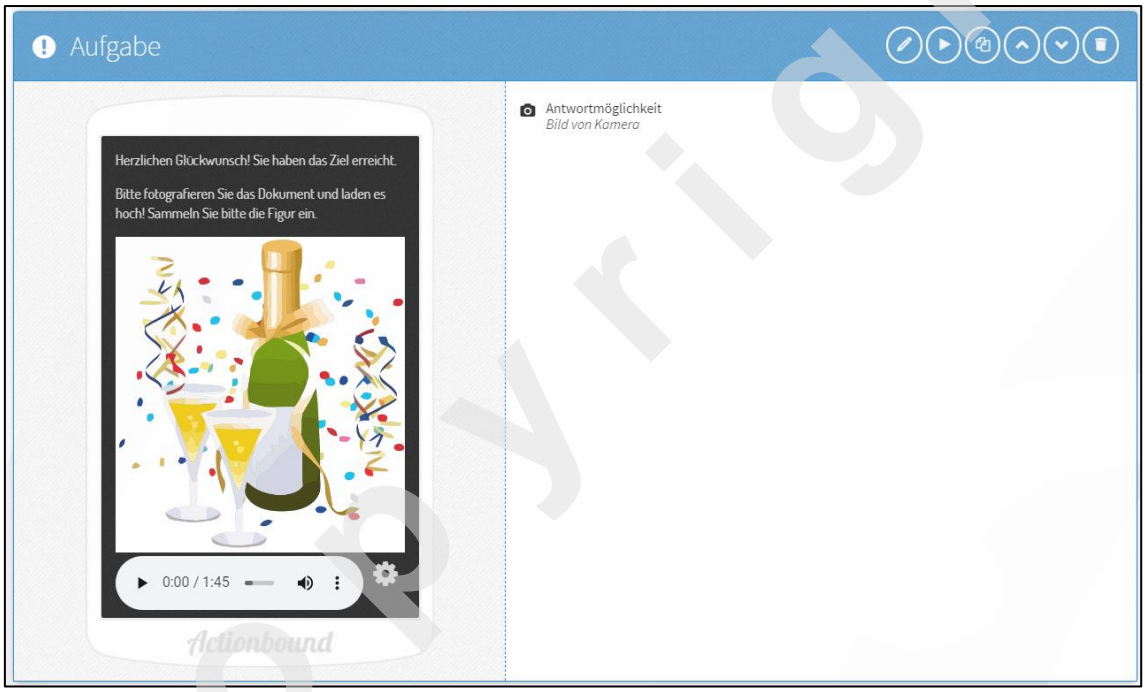
neutrale Darstellung des Fortschritts auf dem Weg zur Zielerreichung (Actionbound):

Copyright

positives Feedback bei Abschluss des online-Grundkurses (Moodle):



positives Feedback am Ende des Bounds (Actionbound):



Copyright

Anlage 10: Beispiel für Leitfragen zur Selbsteinschätzung von Kompetenzen

Quelle: [139]

Copyright

Methodenkompetenz

CAREER CENTRE
Universität Würzburg

Welche Methoden habe ich mir angeeignet? Die Methodenkompetenz beschreibt kognitive und metakognitive Fähigkeiten, die Sie situationsübergreifend anwenden können, um komplexe Aufgaben zu lösen – beispielsweise durch die Anwendung von bestimmten Arbeitstechniken, Verfahrensweisen oder Lernstrategien.

Die Leitfragen der Methodenkompetenzen sind fachübergreifend zu verstehen, trotzdem lassen sie sich nicht immer eindeutig von den Leitfragen der Fachkompetenz abgrenzen.

Leitfragen

Angeeignete Methoden	Welche Methoden habe ich mir angeeignet? Zum Beispiel EDV- oder Statistikprogramme, Präsentations-, Moderations- oder Kreativitätstechniken, Projekt- oder Zeitmanagement-Tools etc.
EDV-Kenntnisse	Beherrsche ich den Umgang mit ausgewählten Computerprogrammen?
Lern- und Arbeitstechniken	Weiß ich, wie ich mir Neues effektiv aneignen kann?
Präsentationstechniken	Kann ich komplexe Inhalte anschaulich und zielgruppengerecht darstellen?
Projektmanagement	Plane und steuere ich Projekte von der Auftragserklärung bis zum erfolgreichen Abschluss?
Schriftliches Ausdrucksvermögen	Ist meine Schriftsprache sehr deutlich und verständlich? Verfüge ich über einen umfangreichen Wortschatz und Stilsicherheit, die eine situationsgerechte Wortwahl garantieren?
Sprachen	Welche Sprachen beherrsche ich auf welchem Niveau?

Copyright

Quellen

Deutsches Jugendinstitut e.V. (2016). *Infos und Materialien zur Kompetenzbilanz aus Freiwilligen-Engagement.* Abgerufen von https://www.dji.de/fileadmin/user_upload/5_kompetenznachweis/KB_Infos_281206.pdf

Meienberger, B. (2007/2008). *Bewerbungsratgeber für Hochschulabsolventen – Sicher im Umgang mit der Bewerbung* (7. überarb. Aufl.). St. Gallen: Career Service Center.

Fachkompetenz

CAREER CENTRE
Universität Würzburg

Die Fachkompetenz umfasst spezifische Kenntnisse und Fähigkeiten, um berufstypische Tätigkeiten auszuführen. Hierfür wird oftmals auch kontextspezifisches Wissen benötigt, das Sie sich in einem bestimmten Tätigkeitsfeld, einer Branche oder Position angeeignet haben.

Obwohl sich die Leitfragen der Fachkompetenz primär auf spezifische Fähigkeiten und Kompetenzen beziehen, sind die Grenzen zur fachübergreifenden Methodenkompetenz nicht immer klar zu bestimmen.

Leitfragen

Auslandsaufenthalte	Habe ich Erfahrungen im Ausland gesammelt?
Branchenkenntnisse	Welche branchen- oder positionsspezifischen Kenntnisse bringe ich bereits mit?
Berufspraktische Erfahrungen	Welche praktischen Erfahrungen habe ich bereits gesammelt (z.B. Praktika, Nebentätigkeiten, Ehrenamt, Hobby, Auslandsaufenthalte etc.)?
EDV-Kenntnisse	Beherrsche ich den Umgang mit ausgewählten Computerprogrammen?
Fachliche Schwerpunkte	Welche fachlichen Schwerpunkte habe ich in meiner (akademischen) Ausbildung gesetzt? Woran sind diese Schwerpunkte erkennbar (z.B. Studiengang, belegte Module, Studien- oder Abschlussarbeiten, Spezialfächer, Weiterbildungen etc.)?
Interdisziplinäres Denken	Bin ich in der Lage die Perspektiven verschiedener Fachrichtungen zusammen zu bringen, um eine Aufgabe besser zu lösen?
Vernetztes Wissen	Kann ich die Verbindung zwischen Informationen herstellen und dadurch Zusammenhänge besser verstehen?

Copyright

Quellen
Deutsches Jugendinstitut e.V. (2016). *Infos und Materialien zur Kompetenzbilanz aus Freiwilligen-Engagement.* Abgerufen von https://www.dji.de/fileadmin/user_upload/5_kompetenznachweis/KB_Infos_281206.pdf
Meienberger, B. (2007/2008). *Bewerbungsratgeber für Hochschulabsolventen – Sicher im Umgang mit der Bewerbung* (7. überarb. Aufl.). St. Gallen: Career Service Center.

Sozialkompetenz

CAREER CENTRE
Universität Würzburg

Wie gehe ich mit anderen Menschen in verschiedenen Situationen wie Zweierbeziehungen, Teams oder Gemeinschaften um? Die Sozialkompetenz beinhaltet Kompetenzen, um Ziele und Pläne in sozialen Interaktionssituationen erfolgreich zu realisieren.

Leitfragen

Einfühlungsvermögen (Empathie)	Zeige ich Interesse an anderen Menschen und ihren Themen und Situationen? Kann ich mich in die Probleme anderer hineinversetzen und Zuhören, ohne mir die Probleme anderer dabei zu eigen zu machen?
Fähigkeit andere zu motivieren	Kann ich andere für eine Sache begeistern von der ich überzeugt bin? Sichere ich dabei eine tragfähige Leistungsbereitschaft durch positive Rückmeldung und Anerkennung der Leistung?
Führungsverhalten	Übernehme ich Verantwortung und leite Teams? Hierbei spielen unterschiedliche Führungstechniken, Konfliktmanagement, interkulturelle Kompetenzen sowie Teamarbeit eine Rolle.
Interkulturelle Sensitivität	Bin ich mir über vorherrschende Unterschiede in verschiedenen Kulturen bewusst und weiß, dass politische, wirtschaftliche und soziale Verhältnisse das Denken beeinflussen? Kann ich mich flexibel auf Menschen anderer Kulturen einstellen und begegne ihnen offen und wertschätzend?
Kommunikations-fähigkeit	Wie kontaktfreudig bin ich? Kann ich mit mehreren Partnern ein Gespräch führen, einzelnen aufmerksam zuhören oder einen schwierigen Dialog aufrechterhalten? Vermittle ich meinen Gesprächspartnern dabei Wertschätzung und Achtung.
Umgang mit Konflikten	Ich erkenne die Ursache von Konflikten und kann mit verschiedenen Sichtweisen und Interessen umgehen, diese ansprechen und bin in der Lage Lösungen zu entwickeln, in denen niemand als Verlierer zurückbleibt.
Kritikfähigkeit	Kann ich Probleme ansprechen und Kritik an andere oder ihre Arbeit mit Wertschätzung rückmelden sowie andere Standpunkte und kritische Rückmeldungen annehmen?
Teamfähigkeit / Teamorientierung	Arbeite ich fair und kollegial im Team, um Ziele zu definieren und zu erreichen? Kann ich mich für die gemeinsamen Ziele einsetzten und dabei meine eigenen Fähigkeiten konstruktiv einbringen aber auch mit Kritik umgehen?
Toleranz	Sehe ich Verschiedenheit als Chance für Entwicklung? Akzeptiere ich andere, auch wenn sie mir in ihrer Art missfallen und lasse andere Meinungen und Wertvorstellungen zu?
Verhandlungsfähigkeit	Entwickle ich Strategien für mein Vorgehen und trete in Verhandlungen selbstsicher und souverän auf? Vertrete ich meine eigenen Interessen? Komme ich mit Verhandlungspartnern erfolgreich und diplomatisch zu einem gemeinsamen Ergebnis?
Zuverlässigkeit	Halte ich mich an vereinbarte Regeln und Absprachen? Können sich andere auf meine Aussagen verlassen? Erledige ich Aufgaben in zugesagter Qualität?

Copyright

Quellen
Deutsches Jugendinstitut e.V. (2016). *Infos und Materialien zur Kompetenzbilanz aus Freiwilligen-Engagement.* Abgerufen von https://www.dji.de/fileadmin/user_upload/5_kompetenznachweis/KB_Infos_281206.pdf
Meienberger, B. (2007/2008). *Bewerbungsratgeber für Hochschulabsolventen –Sicher im Umgang mit der Bewerbung* (7. überarb. Aufl.). St. Gallen: Career Service Center.

Selbstkompetenz

CAREER CENTRE
Universität Würzburg

Die Selbstkompetenz steht für Einstellungen, Wertehaltungen und Motive, die das Arbeitshandeln beeinflussen. Zugleich umfasst dieser Kompetenzbereich Fähigkeiten zur Selbstwahrnehmung und -organisation.

Leitfragen

Anpassungsfähigkeit	Kann ich mich auf veränderte Bedingungen einlassen? Wie gehe ich mit wechselnden Situationen um?
Auftreten	Was ist meine persönliche Wirkung und kann ich sie bewusst für eine erfolgreiche Präsentation einsetzten?
Ausdauer und Durchhaltevermögen	Kann ich mit schwierigen Bedingungen wie Druck, Widerständen, Störungen konstruktiv umgehen? Auch über längere schwierige Phasen hinweg?
Durchsetzungs-vermögen	Kann ich selbstbewusst eine eigene, von anderen abweichende Meinung vertreten und plausibel argumentieren?
Eigenverantwortung	Ich bin für mein Leben und meine Entscheidungen selbst verantwortlich.
Entscheidungsfähigkeit	Kann ich mich zügig festlegen und Entscheidungen konsequent verfolgen?
Fähigkeit sich in Strukturen bewegen zu können	Erkenne ich den Aufbau von Organisationen sowie meinen Platz und kann mich entsprechend meiner Position verhalten?
Flexibilität	Kann ich mein gewohntes Denken und Handeln an neue Situationen anpassen?
Initiative ergreifen	Kann ich selbstständig Ideen und Wünsche in die Tat umsetzten?
Kreativität	Bin ich bereit neue Wege zu gehen und kann unkonventionelle neue Ideen entwickeln? Bin ich einfallsreich und probiere gerne neues aus?
Leistungsbereitschaft	Bin ich bereit Arbeitsaufgaben freiwillig und motiviert zu übernehmen und dabei hohes Engagement zu zeigen?
Lernbereitschaft	Bin ich Neuem gegenüber aufgeschlossen und lerne aus (Miss-)Erfolgen? Kann ich mir in angemessener Zeit neues Wissen und Fähigkeiten aneignen?
Logisches Denken	Kann ich Zusammenhänge schnell erfassen und auf den Punkt bringen?
Selbststeuerung	Erkenne ich Arbeitsaufgaben und Zuständigkeiten in meinem Umfeld selbstständig und kann Schritte zu ihrer Umsetzung entwickeln?
Selbstbeobachtung und -reflexion	Beobachte und reflektiere ich mein Verhalten und Erleben aufmerksam und kritisch? Kenne ich meine Stärken und Schwächen?
Sorgfalt	Erledige ich Arbeitsaufträge gewissenhaft, gründlich, vollständig und verlässlich?
Umgang mit Stress	Erkenne ich Warnzeichen der Überlastung frühzeitig und etabliere Schutzmechanismen?
Verantwortungs-bereitschaft	Kann ich die Folgen meiner Entscheidungen abschätzen und mir ein selbstständiges Urteil bilden und handle daher umsichtig und überlegt?
Verbales Ausdrucksvermögen	Kann ich Gedanken, Pläne, Ziele, Präsentationen auf den Punkt bringen und diese für andere verständlich und präzise erklären?
Zielorientiertes Handeln	Setzte ich mir Ziele und passe meine Schritte zur Zielerreichung flexibel an?

Quellen
Deutsches Jugendinstitut e.V. (2016). *Infos und Materialien zur Kompetenzbilanz aus Freiwilligen-Engagement.* Abgerufen von https://www.dji.de/fileadmin/user_upload/5_kompetenznachweis/KB_Infos_281206.pdf
Meienberger, B. (2007/2008). *Bewerbungsratgeber für Hochschulabsolventen –Sicher im Umgang mit der Bewerbung* (7. überarb. Aufl.). St. Gallen: Career Service Center.

Copyright

Anlage 11: Negativaspekte von Gamification

Quelle: [14]

Copyright

Mögliche Risiken / Nebenwirkungen	Referenz
Motivation	
Demotivation / Verringerung von Interesse und Engagement	Andrade, Mizoguchi & Isotani, 2019; Callan, Bauer & Landers, 2015; Hyrynsalmi, Smed & Kimppa, 2017
Motivationskontamination / Ersetzen intrinsischer Motivation durch Streben nach extrinsischer Belohnung	Hyrynsalmi, Smed & Kimppa, 2017; Korn & Schmidt, 2015
Gleichgültigkeit / fehlende Motivation	Callan, Bauer & Landers, 2015; Toda, Valle & Isotani, 2018
Entmutigung	Šimůnková, 2018
Gewöhnung an Belohnung	Hyrynsalmi, Smed & Kimppa, 2017
Intention	
Ablenkung von der Zielaktivität / dem Hauptzweck	Andrade, Mizoguchi & Isotani, 2019; Callan, Bauer & Landers, 2015; Hyrynsalmi, Smed & Kimppa, 2017
Falsche Verstärkung / Spieloptimierung anstatt Aufgabenkonzentration	Callan, Bauer & Landers, 2015; Hyrynsalmi, Smed & Kimppa, 2017
Unerwünschter Wettbewerb / konkurrierende Interessen / Teamarbeitsschädigung	Andrade, Mizoguchi & Isotani, 2019; Hyrynsalmi, Smed & Kimppa, 2017
Betrug / Fälschen / Vortäuschung / soziale Erwünschtheit	Callan, Bauer & Landers, 2015; Hyrynsalmi, Smed & Kimppa, 2017
Verstärkung falscher Denkweisen	Korn & Schmidt, 2015
Kommerzielle Zwecke	Šimůnková, 2018
Fehlender zusätzlicher Nutzen	Bai, Hew & Huang, 2020
Schwierige Differenzierung zwischen Spiel und Werbung oder Unterhaltung und Marketing	Šimůnková, 2018
Trivialisierung ernsthafter Probleme	Korn & Schmidt, 2015
Begrenzte Reichweite	Kim, 2015
Leistung	
Verringerte Informationsaufnahme / mangelnde Konzentration	Callan, Bauer & Landers, 2015; Hyrynsalmi, Smed & Kimppa, 2017
Leistungsverlust / Produktivitätsverlust	Hyrynsalmi, Smed & Kimppa, 2017; Toda, Valle & Isotani, 2018
Rückzug von den Aufgaben	Callan, Bauer & Landers, 2015
Abnehmende Effekte	Toda, Valle & Isotani, 2018
Erhöhtes Zielverhalten aber Abnahme anderer Verhaltensweisen	Callan, Bauer & Landers, 2015
Voreingenommenheit oder verminderte Genauigkeit	Callan, Bauer & Landers, 2015
Daten	
Verstärkte Offenlegung von (privaten) Informationen	Callan, Bauer & Landers, 2015; Trang & Weiger, 2019
Datenüberwachung	Šimůnková, 2018
Data Mining	Šimůnková, 2018

Copyright

Mögliche Risiken / Nebenwirkungen	Referenz
Verhalten	
(Gefühl der) Manipulation	Hyrynsalmi et al., 2017; Kim, 2015; Kopeć, 2015; Peterson, 2018; Šimůnková, 2018
(Gefühl der) Ausnutzung / Missbrauch	Hyrynsalmi, Smed & Kimppa, 2017; Kim, 2015; Korn & Schmidt, 2015
Sucht und Abhängigkeit	Andrade, Mizoguchi & Isotani, 2019; Hyrynsalmi, Smed & Kimppa, 2017; Tazijan, Bakar & Ramli, 2018
Unerwünschtes Verhalten	Toda, Valle & Isotani, 2018
Unbeabsichtigtes unethisches Verhalten	Laato et al., 2020
Ermutigung, Verhaltensweisen nur dann zu zeigen, wenn sie belohnt werden	Hyrynsalmi, Smed & Kimppa, 2017
Kontraproduktives Verhalten	Callan, Bauer & Landers, 2015
Anpassungszwang	Hyrynsalmi et al., 2017
Inakzeptanz	Callan, Bauer & Landers, 2015
Geringere Wachsamkeit / riskante Verhaltensweisen, die nichts mit der eigentlichen Aktivität zu tun haben	Trang & Weiger, 2019

Mögliche Risiken / Nebenwirkungen	Referenz
Emotion	
Ängste	Bai, Hew & Huang, 2020
Vertrauensverlust	Callan, Bauer & Landers, 2015
Erhöhter Verlust des Selbstbewusstseins	Trang & Weiger, 2019
Eifersucht	Bai, Hew & Huang, 2020
Negative Wahrnehmung der Fairness / Gefühl der unfairen Behandlung	Callan, Bauer & Landers, 2015

Copyright

14. Abkürzungsverzeichnis

ATT&CK	Adversarial Tactics, Techniques und Common Knowledge
BSI	Bundesamt für Sicherheit in der Informationstechnik
DDoS	Distributed Denial of Service
ENISA	European Network and Information Security Agency
GPS	Global Positioning System
HSA	Hochschule Anhalt
HTTPS	Hypertext Transfer Protocol over SSL
IDS	Intrusion Detection System
IoT	Internet of Things
IP	Internet-Protokoll
IPS	Intrusion Prevention System
LAN	Local Area Network
NAT	Network Address Translation
OSINT	Open Source Intelligence
QR	Quick Response
SIEM	Security Information & Event Management
UI	User Interface
URL	Uniform Resource Locator
UX	User Experience
VPN	Virtual Private Network
WLAN	Wireless Local Area Network
XSS	Cross-Site-Scripting
ZKI	Zentren für Kommunikationsverarbeitung in Forschung und Lehre

Copyright

15. Glossar

Backdoor

Eine Backdoor (Hintertür) ist ein Programm, das Dritten einen unbefugten Zugang zum Computer ermöglicht unter Umgehung der Sicherheitsmaßnahmen. Sie werden oft für sogenannte DoS-Angriffe benutzt.

[Quelle: https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Informationen-und-Empfehlungen/Glossar-der-Cyber-Sicherheit/Functions/glossar.html]

Botnetz

Ein Botnetz oder auch eine Zombie-Armee ist eine Gruppe von Computern, die ohne Wissen ihres Besitzers von einem fernsteuerbaren Schadprogramm (Bot) befallen sind und Teil von Command-and-Control Infrastrukturen sind.

[Quelle: https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Informationen-und-Empfehlungen/Glossar-der-Cyber-Sicherheit/Functions/glossar.html]

Command-and-Control Infrastrukturen

Command-and-Control Infrastrukturen sind Netzwerke, die aus mehreren Command-and-Control Servern bestehen, über welche mit Bots befallene Opfersysteme von Angreifenden ihre Befehle erhalten und kontrolliert werden.

Credential Dumping

Credential Dumping ist eine Technik, bei der Angreifer Systeme kompromittieren und versuchen, Passwörter zu erlangen und auszuschleusen.

Denial of Service (DoS)

Denial-of-Service-Angriffe, kurz DoS, wollen die Verfügbarkeit von Diensten, Webseiten, einzelnen Systemen oder Netzen zunichtemachen. Erfolgt der Angriff mit mehreren Systemen zur gleichen Zeit, spricht man von einem verteilten DoS- oder DDoS-Angriff (DDoS = Distributed Denial of Service).

[Quelle: https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Informationen-und-Empfehlungen/Glossar-der-Cyber-Sicherheit/Functions/glossar.html]

Dumpster Diving

Durchforsten von Papierkörben in öffentlich zugänglichen Bereichen oder an zentralen Druckerstationen auf der Suche nach vergessenen oder falsch entsorgten Dokumenten.

Ego-Shooter

Ein Ego-Shooter ist ein Computerspiel-Genre, bei dem eine ständig kämpfende Spielfigur aus der Ich-Perspektive steuert.

Exploit

Copyright

Exploit ist eine Befehlsfolge, die einen noch weitgehend unbekannten Fehler oder eine noch nicht durch Updates behobene Schwachstelle ausnutzt, um die Sicherheit eines Computers oder Netzwerksystems zu gefährden.

IDS

Ein IDS (Intrusion Detection System) ist eine Anwendung, die Eindringversuche auf IT-Systeme erkennt und entsprechend alarmiert.

Internet der Dinge (IoT)

Zum Internet der Dinge gehören "intelligente" Gegenstände, die zusätzliche "smarte" Funktionen enthalten. Sie werden in vielen Fällen drahtlos an Netze angeschlossen und können sogar oft auf das Internet zugreifen und darüber erreicht werden.

[Quelle: https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Informationen-und-Empfehlungen/Glossar-der-Cyber-Sicherheit/Functions/glossar.html]

IPS

Ein IPS (Intrusion Prevention System) ist eine Anwendung, die bereits vor dem Eindringen, bösartige Aktivitäten erkennt, alarmiert und zu stoppen versucht.

Media Dropping

Das absichtliche Verlieren eines mit Schadcode ausgestatteten USB-Sticks im Unternehmensumfeld, um die Neugierde des Personals anzusprechen und ein Anstecken des Sticks an den Firmenrechner zu provozieren.

Monitoring-Tool

Ein Monitoring-Tool ist eine Anwendung, die zur Überwachung von spezifischen Merkmalen von IT-Systemen eingesetzt wird.

Next-Generation Firewall

Eine Next-Generation Firewall ist eine Schutzeinrichtung, die über die üblichen Funktionen einer Firewall hinausgeht. Sie verwendet beispielsweise Funktionen eines sogenannten IPS.

OSINT

OSINT (Open Source Intelligence) ist eine zentrale Ansammlung von öffentlich verfügbaren Informationen aus verschiedenen öffentlich zugänglichen Quellen.

Passwortmanager

Ein Passwortmanager ist ein Programm, welches die Erstellung und Verwaltung von Passwörtern für unterschiedliche Anwendungen unterstützt.

Peers

Unter Peers werden gleiche, ebenbürtige Partner verstanden.

Copyright

Phishing

Phishing setzt sich aus den Begriffen Passwort und Fishing zusammen. Ein Angreifer versucht ein Passwort eines Nutzers auszuspionieren beispielsweise durch einen gefährlichen Anhang oder Link in einer E-Mail.

Protokollierungsserver

Ein Server, der bestimmte Aktionen, Zeiten und Benutzerinformationen aufzeichnet.

Quid pro Quo

Quid pro Quo wird von Social Engineers verwendet, um ihren Opfern etwas scheinbar Wertvolles anzubieten und dafür als Gegenleistung die Herausgabe einer bestimmten Information verlangen.

Ransomware

Als Ransomware werden Schadprogramme bezeichnet, die den Zugriff auf Daten und Systeme einschränken oder verhindern und nur gegen Zahlung eines Lösegeldes (englisch "ransom") wieder freigeben.

[Quelle: https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Informationen-und-Empfehlungen/Glossar-der-Cyber-Sicherheit/Functions/glossar.html]

Reziprozität

Die Reziprozität beschreibt das soziale Prinzip der Gegenseitigkeit. Es bedeutet, dass Menschen, die etwas erhalten, in der Regel dafür auch eine Gegenleistung erbringen.

ROI

Der ROI, auch Return on Investment genannt, bezeichnet eine wirtschaftliche Kennzahl, bei welcher der erzielte Erfolg eines Produktes dem dafür eingesetzten Kapital gegenübergestellt wird.

Schwachstellenanalyse

Durch die Schwachstellenanalyse werden verschiedene Sicherheitslücken in Computer-Systemen und Unternehmensorganisationen festgestellt.

Security Awareness

Mit Security Awareness ist das Bewusstsein oder Gewahrsein der Menschen für Gefahren der Informationssicherheit gemeint.

Sextortion

In diesem Fall wird mit der Veröffentlichung höchst privater und intimer Informationen gedroht.

SIEM-System

Copyright

Ein SIEM (Security Information & Event Management) ist eine komplexe Anwendung, die Informationen verschiedener IT-Sicherheitskomponenten zentral sammelt und auswertet.

Signatur

Unter Signatur wird hier ein bestimmtes Muster verstanden.

Signaturbasiert

Bei einer signaturbasierten Erkennung basiert diese auf einem bestimmten Muster.

Social Engineering

Social Engineering bedeutet, jemanden zu ungewollten Handlungen zu bringen, um an wichtige oder persönliche Informationen wie Benutzernamen und Passwörter zu kommen.

Tailgating

Physisches Eindringen in geschlossene Firmengelände oder Räume durch Vorspiegelung falscher Identitäten (z. B. als Paketbote oder Reinigungskraft).

Update

Updates sind neue Versionen oder Ergänzungen von Programmen zur Korrektur und Verbesserung selbiger.

Verhaltensbasiert

Bei der verhaltensbasierten Erkennung basiert diese auf einem bestimmten abnormalen Verhalten.

Copyright

16. Thesen

Master-Thesis	Einsatz von Gamification zur Sensibilisierung für Informationssicherheit im Kontext deutscher Hochschulen
Eingereicht am:	13.09.2022
Betreuerin:	Prof. Dr.-Ing. Antje Raab-Düsterhöft
Zweitbetreuer:	Prof. Dr. Stefan Schlechtweg

- Gamification leistet einen besonderen Beitrag zur Motivationserhaltung und -steigerung im Lernprozess und kann deshalb auch im Rahmen von Schulungen zur Sensibilisierung von Mitarbeitenden für Informationssicherheit eingesetzt werden.

- Das Ausmaß der individuellen Selbstwirksamkeit bestimmt maßgeblich das informationssichere Verhalten eines Menschen.

- Gamification liefert positive Emotionen, die zum Ausführen erwünschter Verhaltensweisen führen.

- Feedback ist ein besonderes Element, dass bei richtigem Einsatz den Übergang von der extrinsischen zur intrinsischen Motivation unterstützt.

- Gamification hat negative Aspekte, die auch an deutschen Hochschulen auftreten können, welche aber durch die abgestimmte Kombination und den gezielten Einsatz der Spielelemente sowie den Abgleich mit den Lernzielen unter Berücksichtigung der Spielertypen vermieden werden können.

Copyright

17. Selbständigkeitserklärung

Hiermit erkläre ich, dass ich die vorliegende Arbeit selbständig verfasst und keine anderen als die angegebenen Hilfsmittel benutzt habe. Die Stellen der Arbeit, die anderen Quellen im Wortlaut oder dem Sinn nach entnommen wurden, sind durch Angaben der Herkunft kenntlich gemacht. Dies gilt auch für Zeichnungen, Skizzen, bildliche Darstellungen sowie für Quellen aus dem Internet. Ich erkläre ferner, dass ich die vorliegende Arbeit in keinem anderen Prüfungsverfahren als Prüfungsarbeit eingereicht habe oder einreichen werde. Die eingereichte schriftliche Fassung entspricht der auf dem Medium gespeicherten Fassung.

Ort, Datum (Unterschrift)

Copyright