Margit Scholl (Hrsg.)

Informationssicherheitsbewusstsein für den Berufseinstieg

SecAware4job

Shaker Verlag
Aachen 2017

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

Printed in Germany.

ISBN 978-3-8440-5466-8

Shaker Verlag GmbH • Postfach 101818 • 52018 Aachen
Telefon: 02407 / 95 96 - 0 • Telefax 02407 / 95 96 - 9
Internet: www.shaker.de • E-Mail: info@shaker.de

Abschlussbericht

Informationssicherheitsbewusstsein für den Berufseinstieg (SecAware4job)

Projektlaufzeit 1.9.2015–31.8.2017

Fuhrmann, Frauke
Scholl, Margit (Prof. Dr.)
Edich, Denis
Koppatz, Peter
Scholl, L. Robin
Leiner, K. Benjamin
Ehrlich, E. Peter

Technische Hochschule Wildau
Technical University of Applied Sciences
WILDAU

SecAware4job

Gefördert von
HGS
Horst Görtz Stiftung

Inhalt

Abkürzungsverzeichnis

BAköV	Bundesakademie für öffentliche Verwaltung
BITKOM	Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e.V.
BSI	Bundesamt für Sicherheit in der Informationstechnik
BWL	Betriebswirtschaftslehre
DIZ	Digitales Innovationszentrum
DLGI	Dienstleistungsgesellschaft für Informatik mbH
DSB	Datenschutzbeauftragte/r
ECDL	Europäischer Computerführerschein
EU-DSGVO	Datenschutzgrundverordnung der Europäischen Union
ISMS	Informationssicherheitsmanagement
FB INW	Fachbereich Ingenieur- und Naturwissenschaften
ISO/IEC	International Organization for Standardization/International Electrotechnical Commission
IT	Informationstechnik (Informationstechnologie)
ITIL	Information Technology Infrastructure Library
IT-SiBe	IT-Sicherheitsbeauftragte/r (Informationssicherheitsbeauftragte/r)
KVR	Kommunales Verwaltungsmanagement und Recht
LISUM	Landesinstitut für Schule und Medien Berlin-Brandenburg
LOI	Letter of Intent
ÖVBB	Bachelor-Studiengang Öffentliche Verwaltung Brandenburg
SoSe	Sommersemester
StGB	Strafgesetzbuch
TH Wildau	Technische Hochschule Wildau
TWZ e. V.	Technologie- und Weiterbildungszentrum
WBT	Web Based Training
WILLE	Wildau Institut für innovative Lehre, lebenslanges Lernen und gestaltende Evaluation
FB WIR	Fachbereich Wirtschaft, Informatik und Recht
WPF	Wahlpflichtfach
WS	Wintersemester

Abbildungsverzeichnis

Tabellenverzeichnis

Kurzdarstellung

Informationen sind wertvolle Ressourcen in der heutigen Wissens- und Informationsgesellschaft. Sie vor unberechtigten Zugriff oder Missbrauch zu schützen, ist die besondere Herausforderung in Zeiten voranschreitender Digitalisierung aller Lebensbereiche. Das Projekt „Informationssicherheit für den Berufseinstieg (SecAware4job)“, gefördert durch die Horst Görtz Stiftung, möchte Studierende, insbesondere nicht-technischer Studiengänge, als zukünftige Mitarbeitende für die alltäglichen Herausforderungen des Schutzes der Informationssicherheit und der digitalen Infrastruktur sensibilisieren. Dafür wurde in den vergangenen zwei Jahren an der Technischen Hochschule (TH) Wildau eine berufsorientierte Zusatzqualifikation für Studierende in Form einer innovativen Weiterbildung mit Zertifizierung zur Stärkung des Bewusstseins und der Kompetenzen bezüglich Informationssicherheit entwickelt und erprobt.

Um das abstrakte und komplexe Thema Informationssicherheit mit all seinen Facetten (rechtliche Rahmenbedingungen, Normen & Standards, Schutzmaßnahmen, Sicherheitskonzepte etc.) den Studierenden leicht verständlich, greif- und erlebbar zu vermitteln, wurde ein methodischer Ansatz für die Zusatzqualifikation gewählt, der möglichst viele kreative und interaktive Lehr- und Lernmethoden beinhaltet. Auf Basis aktueller Forschungserkenntnisse zur Wirksamkeit von Sensibilisierungsmaßnahmen wurden gemäß dem Game-based-Learning-Ansatz analoge und digitale spielebasierte Lernszenarien entwickelt und erprobt. Es wurden zehn Stationen der „Security-Arena“, die über das Drittmittelprojekt IT-Sicherheit@KMU im Zeitraum 2013/2014 beschafft und mit dem Projektpartner knonwn_sense angepasst worden waren, nun auf die neue Zielgruppe fokussiert und zudem in Englisch übersetzt. Darüber hinaus wurden fünf analoge spielebasierte Lernszenarien neu konzipiert und umgesetzt, darunter das Brettspiel *„Keep your data private. Everyday.“* und das *Social Engineering Rollenspiel*, die zwei sehr umfangreiche Entwicklungen des Forschungsprojektes SecAware4job darstellen. Zur Ergänzung und Vervollständigung der analogen Lernszenarien wurden acht digitale spielebasierte Lernszenarien konzipiert und programmiert, die nach Projektende über die SecAware4job-Webseite (http://secaware4job.wildau.biz) abgerufen und kostenfrei genutzt werden können.

Die entwickelte Zusatzqualifikation wurde in drei Durchläufen als (Wahlpflicht-) Modul „Sensibilisierung für Informationssicherheit“ erprobt. Die wissenschaftliche Begleitforschung zur Wirksamkeit der Zusatzqualifikation und der entwickelten Lernszenarien zeigt, dass die Studierenden mit dem methodischen Ansatz sehr zufrieden sind.

Zudem wird das Ziel erreicht, bei den Teilnehmenden das Bewusstsein für Informationssicherheit und entsprechende Kenntnisse zu stärken. Es wird angestrebt, das Modul „Sensibilisierung für Informationssicherheit“ mittel- bis langfristig in allen Studiengängen der TH Wildau als Wahlpflichtfach zu etablieren.

Im Sinne des Authentic-Learning-Ansatzes sind Anpassungen von spielebasierten Lernszenarien an die konkrete Zielgruppe und ihre realen Bezüge für den Lernerfolg von großer Bedeutung. Dabei sind neben der Spezifizierung von Inhalten auch kulturelle und sprachliche Aspekte zu berücksichtigen. Im Projekt SecAware4job wurden englischsprachige Lernstationen konzipiert und erprobt, die nun ab dem kommenden Wintersemester (WS) 2017/2018 in den internationalen Studiengängen, z. B. im Studiengang European Management Bachelor (EM) und Master (EMM), eingesetzt werden können. Damit fördert und unterstützt das Projekt SecAware4job auch die Internationalisierung an der TH Wildau.

1 Ausgangssituation

Informationen sind ein wertvolles Gut in der heutigen Wissens- und Informationsgesellschaft. Sie sind eine der wesentlichen Ressourcen für das langfristige und erfolgreiche Bestehen von Organisationen (Kruger, Drevin & Steyn 2007). Mitarbeitende jeglicher Organisationen arbeiten tagtäglich mit sensiblen Informationen der eigenen Organisation, von Unternehmen, Bürgerinnen und Bürgern, Kundinnen und Kunden, Patientinnen und Patienten usw. Der Schutz dieser personenbezogenen bzw. personenbeziehbaren Daten und sensiblen Informationen ist die große Herausforderung und Aufgabe in Zeiten der voranschreitenden Digitalisierung aller wirtschaftlichen und gesellschaftlichen Bereiche, in denen Informationstechnik (IT) in allen Lebensbereichen präsent ist.

Während jedoch die meisten Menschen sich mit der Nutzung moderner IT-Geräte und -Anwendungen zumindest vertraut machen, bieten die zunehmende Durchdringung, Verbreitung und Komplexität von Soft- und Hardware auch eine stetig wachsende Anzahl an Möglichkeiten zu deren Missbrauch. Da diese Möglichkeiten sowohl technischer (z. B. Cracking) als auch zwischenmenschlicher Natur (z. B. Social Engineering) sein können, sind ein höheres Bewusstsein und verbesserte Kenntnisse hinsichtlich der mit der Digitalisierung einhergehenden Gefahren und entsprechenden Schutzmaßnahmen für Privat- und Arbeitsleben unerlässlich. Die noch so versiertesten technischen Lösungen bieten keinen tatsächlichen Schutz, wenn Mitarbeitenden die Bedeutung von Informationssicherheit und sicherem Verhalten nicht bewusst ist oder sie nicht willens sind, sich sicherheitskonform zu verhalten. Somit wird der Mensch als der „kritische Faktor“ für die Informationssicherheit jeder Organisation angesehen (Kruger, Drevin & Steyn 2007). Dabei hat in jüngster Zeit ein Umdenken stattgefunden, so dass die Mitarbeitenden nicht mehr als „schwächstes Glied“ oder „größte Schwachstelle“ bezeichnet werden, durch die die meisten Informations- und Datenschutz-Vorfälle unbewusst oder bewusst ausgelöst werden (Guo et al. 2011; EnBW et al. 2008; DSV-Gruppe et al. 2006), sondern als stärkster Schutz eines betrieblichen Informationssicherheitsmanagementsystems (ISMS) (Scholl et al. 2016a). Gleichwohl muss aber dafür gesorgt werden, dass die Mitarbeitenden dazu befähigt sind, diese starke Schutzfunktion auszuüben.

Insbesondere kleinen und mittelständischen Unternehmen mangelt es jedoch oftmals an monetären und zeitlichen Ressourcen, um ihre Mitarbeitenden auf die umfassende Weise fortzubilden, die zur Verankerung eines nachhaltigen Informationssicherheitsbewusstseins erforderlich wäre (vgl. Kapitel 3.1). Hier setzt das Projekt „Informationssicherheitsbewusstsein für den Berufseinstieg (SecAware4job)“ der Technischen Hoch-

schule (TH) Wildau, gefördert durch die Horst Görtz Stiftung, an. In diesem sollen Studierende mit Informationssicherheitsbewusstsein und -kenntnissen ausgestattet werden und damit eine wichtige Kompetenz für ihren Berufseinstieg in der digitalen Welt erhalten. Unter Informationssicherheit wird der „Schutz von Informationen jeglicher Art und Herkunft“ verstanden (BAköV 2016: 13). Dieses Verständnis umfasst auch IT-Sicherheit, die auf den „Schutz elektronisch verarbeiteter und gespeicherter Informationen und der zugehörigen technischen Systeme“ (BAköV 2016: 13) abzielt.

Die TH Wildau versteht sich als angewandt forschende Hochschule mit starkem Praxisbezug. Eine konsequente Einheit von Forschung und Lehre dient nicht nur der Bewältigung zukünftiger Herausforderungen, sondern ist auch für den Berufseinstieg von zentraler Bedeutung. Die Ausbildung der Studierenden als zukünftige Mitarbeitende sollte demnach an dem aktuellen Stand der Wissenschaft und an den Anforderungen der Praxis in Betrieben, Verwaltungen und Institutionen orientiert sein. Dazu gehört auch der Wissensaufbau für ein ganzheitliches Technikverständnis und eine Sensibilisierung für Informationssicherheit und IT-Sicherheit. Dies betrifft vor allem auch die weniger technik-affinen Studiengänge wie betriebswirtschaftliche und verwaltungswissenschaftliche Studiengänge. Denn das Bewusstsein und die Kompetenzen für Informationssicherheit können nicht an IT-Fachkräfte delegiert werden. Vielmehr muss jede/r Mitarbeitende ihren/seinen Beitrag zur Informationssicherheit leisten.

2 Zielstellung von SecAware4job

Ziel des durch die Horst Görtz Stiftung geförderten Projektes „Informationssicherheitsbewusstsein für den Berufseinstieg (SecAware4job)“ ist die Entwicklung und Erprobung einer berufsorientierten Zusatzqualifikation für Studierende in Form einer innovativen Weiterbildung mit Zertifizierungsmöglichkeiten zur Stärkung des Bewusstseins und der Kompetenzen bezüglich Informations- und IT-Sicherheit. Studierende, insbesondere nicht-technischer Studiengänge, sollen als zukünftige Mitarbeitende für die alltäglichen Herausforderungen des Schutzes von sensiblen Informationen und der digitalen Infrastruktur sensibilisiert und ihr Sicherheitsbewusstsein fundiert gefördert werden. Konkret soll die Zusatzqualifikation

- Kompetenzen bezüglich Informations- und IT-Sicherheit für den Berufseinstieg vermitteln,
- Bewusstseins- und Verhaltensänderungen anregen und unterstützen,
- Risikobewertung und Treffen von Entscheidungen erleichtern sowie
- nachweisbare, zertifizierte Qualifizierungen für den Berufseinstieg verleihen.

Da alle Mitarbeitenden und nicht nur IT-Fachkräfte Informationssicherheitsbewusstsein besitzen sollen, werden im Projekt SecAware4job insbesondere Studierende nicht-technischer Studiengänge als Zielgruppe der Zusatzqualifikation angesprochen. Um das Interesse der Studierenden für dieses komplexe Thema und deren Bereitschaft zu wecken, sich auf das Thema einzulassen, wird ein methodischer Ansatz gewählt, der möglichst viele kreative Lehr- und Lernmethoden einsetzt und Vortrag, analoge und digitale spielebasierte Lernszenarien und interaktive Übungen vereint (vgl. Kapitel 3.4). Es wird angestrebt, die Zusatzqualifikation mittel- bis langfristig vor allem in den nicht-technischen Studiengängen der TH Wildau als festen Bestandteil zu integrieren.

3 Methodische Grundlagen

3.1 Security und Privacy Awareness

In vielen Organisationen beschränkt sich Sensibilisierung für Informationssicherheit und die Ausbildung entsprechender Kompetenzen auf Maßnahmen des Wissenstransfers. Dieser findet beispielsweise als Vortrag mit entsprechender Präsentation, als Awarenesskampagnen mittels Flyern, Postern, Broschüren etc. oder auch in Form eines Web Based Trainings (WBT) statt, das die Mitarbeitenden zu einer beliebigen Zeit und in individuellem Tempo absolvieren können bzw. müssen. Ungeachtet dieser Vorteile von WBT zeigen Studien, dass Ansätze, die sich nur auf Wissenstransfer konzentrieren, kein nachhaltiges Sicherheitsbewusstsein bei den Beschäftigten bewirken (SanNicolas-Rocca, Schooley & Spears 2014; Albrechtsen 2007; DSV-Gruppe et al. 2006; Straub & Welke 1998). Wir nennen diese Ansätze der Sensibilisierung für Informationssicherheit „1.0 Lerntheoretische Ansätze“ (s. Abbildung 1). Basierend auf diesen empirischen Befunden entstanden Sensibilisierungsmaßnahmen, die zusätzlich zur Wissensvermittlung Marketingelemente enthalten, die die Aufmerksamkeit der Adressatinnen und Adressaten wecken und sie für das Thema Informationssicherheit emotionalisieren sollen – gemäß unserer Klassifizierung „2.0 Werbliche Ansätze“ (s. Abbildung 1). Psychologische Forschung zeigt jedoch, dass neben dem theoretischen Ansatz für den Wissenstransfer und dem marketingorientierten Ansatz einer Emotionalisierung ein umfassenderer systemischer Ansatz mit Emotionen und sozialer Teilhabe im Team sowie mit persönlicher Kommunikation und Interaktion in erlebbaren Szenarien benötigt wird, um dauerhafte Sensibilisierung für Informationssicherheit und sicherheitsrelevante Verhaltensweisen zu erzielen (Khan et al. 2011; Helisch & Pokoyski 2009; Albrechtsen 2007). Deshalb orientiert sich der methodische Ansatz des entwickelten und erprobten (Wahlpflicht-) Moduls „Sensibilisierung für Informationssicherheit“ im Projekt SecAware4job an den „3.0 Systemischen Ansätzen“ (s. Abbildung 1) (Scholl et al. 2016b).

Abbildung 1: Ansätze der Security und Privacy Awareness

3.2 Spirale der transformativen Wechselwirkung

In Anlehnung an den Ansatz von Hewlett Packard zur Förderung eines stärkeren Einsatzes von Mitarbeitenden für Informationssicherheit (Beyer et al. 2015) wurde in SecAware4job ein Modell in der Form einer Spirale entwickelt, das die Wechselwirkung zwischen institutionellen Vorgaben (top-down) und freiwilligem Engagement der Beschäftigten (bottom-up) zur Etablierung einer organisationalen Sicherheitskultur verdeutlichen soll (Scholl & Fuhrmann 2016). Die Spirale der transformativen Wechselwirkung (s. Abbildung 2) besteht aus drei Bereichen, die sich gegenseitig beeinflussen: Die Organisation (rechts abgebildet) ist der Ort, an dem Informationssicherheit gelebt werden soll und der durch Vorgaben, Abläufe und Strukturen geprägt ist (von oben nach unten). Die einzelnen Beschäftigten (in der Mitte abgebildet) sind die Akteurinnen und Akteure, die durch ihre Einstellung und ihr Verhalten eine gelebte Sicherheitskultur erst ermöglichen. Um jedoch eine Sicherheitskultur leben zu können, ist ein Lernprozess (links abgebildet) erforderlich, in dem die einzelnen Beschäftigten und die Organisation als Ganzes relevantes Wissen und Bewusstsein zur Informationssicherheit erwerben und entsprechendes Verhalten einüben (von unten nach oben).

Abbildung 2: Spirale der transformativen Wechselwirkung

In der heutigen Wissens- und Informationsgesellschaft sind Informationen und Wissen ein wesentlicher Vermögenswert von Organisationen (Khan et al. 2011). Zum Schutz erfolgskritischer Informationen sollte jede/r Beschäftigte für Informationssicherheit entsprechend ihren/seinen Aufgaben und Verantwortlichkeiten informiert, fortgebildet und sensibilisiert werden. Der dafür notwendige Lernprozess ist auf der linken Seite der Spirale veranschaulicht. So fördert eine gezielte Qualifizierung den Erwerb und die Aneignung fundierten Wissens sowie Kompetenz- und Erkenntnisgewinn. Um jedoch ein nachhaltiges Bewusstsein für Informationssicherheit und entsprechende Verhaltensweisen zu erzielen, bedarf es emotionalen Interesses und Motivation sowie die Bereitschaft jeder/jedes Einzelnen (Khan et al. 2011).

Gemäß dem in Kapitel 3.1 erläuterten systemischen Ansatz der Security und Privacy Awareness kann dies mittels interaktiver Methoden (z. B. Simulationen), die Wissensvermittlung, Emotionalisierung und Anwendung in einem Team vereinen, erreicht werden. Denn dadurch sollen Emotionen bei den Beschäftigten geweckt und ihre Motivation und Bereitschaft, sensible Informationen zu schützen, gefördert werden. In Verbindung mit der zunehmenden Kompetenz im Bereich Informationssicherheit sollte dies zu

höherer Akzeptanz von Richtlinien und Maßnahmen zum Schutz sensibler Informationen führen. Letztendlich resultieren im Idealfall ein aktives Engagement und eine Selbstverpflichtung (Commitment) für Informationssicherheit, so dass sensible Informationen weniger als Befolgung von Vorgaben und Richtlinien, sondern aus eigener Überzeugung geschützt werden (vgl. Mitte der Spirale).

Die Rahmenbedingungen innerhalb einer Organisation, die für eine gelebte Sicherheitskultur förderlich sind, sind auf der rechten Seite der Spirale abgebildet. Ausgehend von der Transparenz der Organisationsziele sollten die Beschäftigten die Möglichkeit erhalten, sich an wichtigen Entscheidungsprozessen beteiligen zu können. Dies fördert die Zusammenarbeit und den Wissenstransfer in der Organisation, so dass individuelles Wissen und persönliche Erfahrungen geteilt werden und in organisatorische Abläufe einfließen. Dadurch können Geschäftsprozesse verbessert werden, die durch umfangreiche IT-Anwendungen unterstützt werden, welche für einen reibungslosen Ablauf integriert und kontinuierlich optimiert werden sollten. Die IT-Anwendungen enthalten sensible Informationen. Damit windet sich die Spirale zu den Lern- und Sensibilisierungsprozessen für Informationssicherheit. Da Organisationen, ihr (Geschäfts-) Umfeld sowie Regelungen und technische Entwicklungen einem ständigen Wandel unterliegen, müssen die in der Organisation vorhandenen Kompetenzen, das Bewusstsein sowie das Verhalten im Hinblick auf Informationssicherheit und die Rahmenbedingungen für eine gelebte Sicherheitskultur immer wieder überprüft und an aktuelle Gegebenheiten angepasst werden. Die Spirale der transformativen Wechselwirkung ist somit kontinuierlich von oben nach unten und von unten nach oben zu durchlaufen. Dies ist durch die nach unten und oben weisenden Pfeile veranschaulicht.

3.3 Game-based Learning

Game-based Learning erfährt immer mehr Anerkennung als wirkungsvolle Lehr- und Lernmethode im Bildungsbereich bzw. in der Weiterbildung. Game-based Learning wird als unterhaltsame und motivierende Form des Lernens beschrieben (Linek & Albert 2009), bei der Spielelemente (z. B. Punkte, Ranglisten, Spielergebnis, Level, Belohnungen, Fortschrittsanzeigen) in nicht spielerischen Kontexten wie in Arbeitsprozessen oder in der Lehre angewandt werden (Codish & Ravid 2017; Huotari & Hamar 2017; Silic & Back 2017). Spielebasierte Lernszenarien ermöglichen klare Zielvorgaben und direktes Feedback (Fang, Zhang & Chan 2013). Um das vorgegebene Ziel zu erreichen, wählen die Teilnehmenden Aktivitäten, treffen Entscheidungen und erleben unmittelbar die daraus resultierenden Konsequenzen. Spielebasierte Lernszenarien erlauben es somit, durch Fehler machen und Ausprobieren die richtige Weise, etwas zu tun, einzuüben

(Trybus 2014). Zudem können Spiele individuell angepasst werden, so dass sie das richtige Maß an Herausforderungen bieten, um die Fähigkeiten zu stärken und zu erweitern (Bressler & Bodzin 2013). Dies kann insbesondere bei digitalen Lernspielen genutzt werden, um individuell angepasste „Lernpfade“ zu durchlaufen (Haack et al. 2010).

Aufgrund dieser Eigenschaften belegen zahlreiche Studien positive Wirkungen des Einsatzes von Spielen und Spielelementen in der Lehre: Game-based-Learning-Umfelder sind hoch involvierend und fördern dadurch die Motivation und Verhaltensänderungen (Buffum et al. 2015; Bösche & Kattner 2011; Hsu et al. 2008). Durch den Einsatz von Spielen lassen sich bessere Lernleistungen als durch klassischen Unterricht erzielen (Admiraal et al. 2014). Wichtig bei der Konzeption der Lernszenarien ist die zielgruppenspezifische Ausrichtung und Anpassung der Inhalte an die Lebenswelt der Zielgruppen. Gemäß dem Authentic-Learning-Ansatz wird durch das Aufgreifen realer Problemsituationen realitätsnahes Empfinden und Erleben ermöglicht, was die Herstellung von Verbindungen zu realen Situationen und Herausforderungen erleichtert und dadurch den Lernerfolg erhöht (Lombardi 2007).

Analoge und digitale Lernszenarien mit spielerischen Elementen, wie Wettbewerb, Belohnung, unmittelbares Feedback, stellen einen innovativen Lehr- und Lernansatz dar, da sie Wissensvermittlung mit emotionalen und involvierenden Elementen (Silic & Back 2017) sowie sozialem Lernen im Team vereinen (Helisch & Pokoyski 2009). Die kombinierte Anwendung von analogen und digitalen spielebasierten Lernszenarien im Projekt SecAware4job nutzt die Vorteile beider Lernstrategien mit dem Ziel, in der Summe einen höheren Lernerfolg zu erreichen. Die Vorteile analoger Lernszenarien bestehen in der gemeinsamen Lösung durch Gruppen, im dadurch möglich werdenden Erfahrungs- und Wissensaustausch sowie in der Stärkung der Team- und Kommunikationsfähigkeiten. Bei den digitalen Lernszenarien sind die Studierenden individuell gefordert und unterschiedliche Schwierigkeitsgrade können den individuellen Kenntnis- und Wissensstand berücksichtigen. Die Lernszenarien können orts- und zeitunabhängig, in eigenem Tempo und so oft, wie gewünscht, wiederholt werden (Scholl et al. 2017).

3.4 Methodischer Ansatz in SecAware4job

Basierend auf den in diesem Kapitel dargestellten methodischen Grundlagen beinhaltet die berufsorientierte Zusatzqualifikation „Sensibilisierung für Informationssicherheit“ neben herkömmlicher Stoffvermittlung möglichst viele kreative Lehr- und Lernmethoden, um das abstrakte und komplexe Thema Informationssicherheit mit all seinen Facetten (rechtliche Rahmenbedingungen, Normen & Standards, Schutzmaßnahmen,

Konzepte etc.) den Studierenden leichter verständlich, greif- und erlebbar zu vermitteln. Als kreative Methoden kommen u. a. analoge und digitale spielebasierte Lernszenarien (Simulationen) zum Einsatz. Die folgende Abbildung veranschaulicht den interaktiven Methodenmix

Abbildung 3: Methodenmix in SecAware4job

Dieser Methodenmix soll

- komplexe und abstrakte Lerninhalte greif- und erlebbar machen,
- reale (Problem-) Situationen aufgreifen,
- Lernen durch Ausprobieren, Fehler machen und Wiederholen ermöglichen,
- den Austausch von Wissen unterstützen,
- direktes Feedback zum Lernfortschritt geben,
- sich an den Lernenden, ihren Wissensständen und ihren Bedürfnissen orientieren.

4 Spielebasierte Lernszenarien

Im Sinne des Authentic-Learning-Ansatzes sind Anpassungen von spielebasierten Lernszenarien an die konkrete Zielgruppe und ihre realen Bezüge für den Lernerfolg von großer Bedeutung. Dabei sind neben der Spezifizierung von Inhalten auch kulturelle und

sprachliche Aspekte zu berücksichtigen. Im Projekt SecAware4job wurden existierende deutschsprachige Lernstationen der „Security-Arena“ für und mit den Studierenden nicht-technischer Studiengänge erprobt. Es handelt sich dabei um zehn analoge Spielstationen, die auf Entwicklungen des Projektpartners known_sense mit T-Systems unter dem Label Security Parcours basieren. Anhand unserer eigenen Bewertungen mit den Studierenden und unseren Erfahrungen in Workshops auf internationalen Veranstaltungen wurden auch die englischsprachigen Übersetzungen konzipiert. Diese nun vorliegenden englischsprachigen Lernstationen können im kommenden Wintersemester (WS) 2017/2018 z. B. auch im Studiengang European Management Bachelor (EM) und Master (EMM) eingesetzt werden. Damit fördert und unterstützt das Projekt SecAware4job auch die Internationalisierung an der TH Wildau.

In SecAware4job wurden fünf analoge und acht digitale spielebasierte Lernszenarien sowie vier innovative Lehrmethoden neu entwickelt. In den folgenden Kapiteln werden alle Lernszenarien vorgestellt und im Anhang findet sich eine tabellarische Übersicht.

In vielen unterschiedlichen Veranstaltungen an der TH Wildau wurden und werden alle Lernszenarien mit verschiedenen Zielgruppen erprobt, so dass ihr Einsatz als breitenwirksam und nachhaltig bezeichnet werden kann. Mit Abschluss der Förderung werden die entwickelten digitalen Lernszenarien als Creative Commons License frei zugänglich auf der Projektwebseite (http://secaware4job.wildau.biz) zur kostenfreien Nutzung bereitgestellt.

4.1 Übersetzung Security-Arena

In dem früheren Drittmittelprojekt IT-Sicherheit@KMU wurde gemeinsam mit dem schon damaligen Praxispartner known_sense die Security-Arena – ein Line Extender des „SECURITY PARCOURS“ von T-Systems, mitentwickelt durch die Firma known_sense – mit analogen Lernszenarien-Stationen entwickelt. Gemäß dem Lehr- und Lernansatz Stationenlernen, der zurückgeht auf das Zirkeltraining im Sportbereich (Morgan & Adamson 1961), durchlaufen Teams aus idealerweise 4–5 Mitgliedern die Arena mit 6–10 Stationen im Wettbewerb. Jedes Team beginnt an einer anderen Station. Der Aufbau jeder Station ist identisch:

- fünf Minuten Einführung, Erläuterung des spielerischen Lernszenarios und Erfahrungs- und Wissensaustausch zum Thema der Lernstation,
- fünf Minuten Durchspielen des Lernszenarios und
- fünf Minuten Auflösung des Lernszenarios, Klärung von Fragen und Missverständnissen sowie Punktevergabe.

Alle Stationen (15 Minuten/Station) werden von den Teams synchron in einer Art Wettbewerb durchlaufen. Das Absolvieren der Security-Arena oder einzelner Stationen startet eine intensive Auseinandersetzung mit einem konkreten Thema, das in digitalen Lernszenarien wiederholt und in eigenem Tempo eingeübt werden kann (vgl. Kapitel 4.4). Der Wettbewerb fördert die Teamkommunikation, da gemeinsam möglichst viele Punkte erzielt werden wollen.

Zehn analoge Spielstationen der Security-Arena, die auf Entwicklungen des Projektpartners known_sense mit T-Systems basieren, wurden an die Bedürfnisse von Studierenden, die kurz vor dem Berufseinstieg stehen bzw. berufsbegleitend studieren, angepasst und in Englisch übersetzt (s. Abbildung 4).

Die Station *Clear Desk* sensibilisiert die Studierenden dafür, welche Gegenstände und Informationen auch nur bei einem kurzzeitigen Verlassen des (zukünftigen) Arbeitsplatzes sicher verwahrt werden sollten.

An der Station *Data Security* sollen die Studierenden wichtige Merksätze im Hinblick auf Informationssicherheit zusammensetzen und auf diese Weise verinnerlichen.

Bei der Station *Incident Management* geht es um die Zuordnung von Informationssicherheits-, Datenschutz- und Compliance-Vorfällen zu vorgegebenen Themenfeldern und insbesondere um die Identifikation der richtigen Meldestellen für die entsprechenden Vorfälle.

Die Station *Internet Services* widmet sich der zunehmenden Nutzung von Internet-Diensten und Apps im beruflichen Kontext. Neun beispielhafte Anwendungen werden im Hinblick auf acht ausgewählte Risiken von den Studierenden bewertet.

An der *Password Hacking* Station werden die Studierenden für die Verwendung unterschiedlicher und starker Passwörter sensibilisiert, indem sie in die Rolle einer/eines Kriminellen schlüpfen und das Passwort von Max Schuster für die fiktive Social Media Plattform der TH Wildau zu knacken versuchen. Behilflich sind ihnen dabei die Informationen, die Max Schuster in einem fiktiven Facebook-Profil über sich veröffentlicht.

Die Station *Phishing* lädt die Studierenden zum Angeln realer E-Mails ein, die sie anhand vorher kennengelernter Merkmale (z. B. falsche Rechtschreibung, unpersönliche Anrede, Dringlichkeit, verdächtiger Anhang) als Phishing-Versuche oder harmlose E-Mails einordnen sollen.

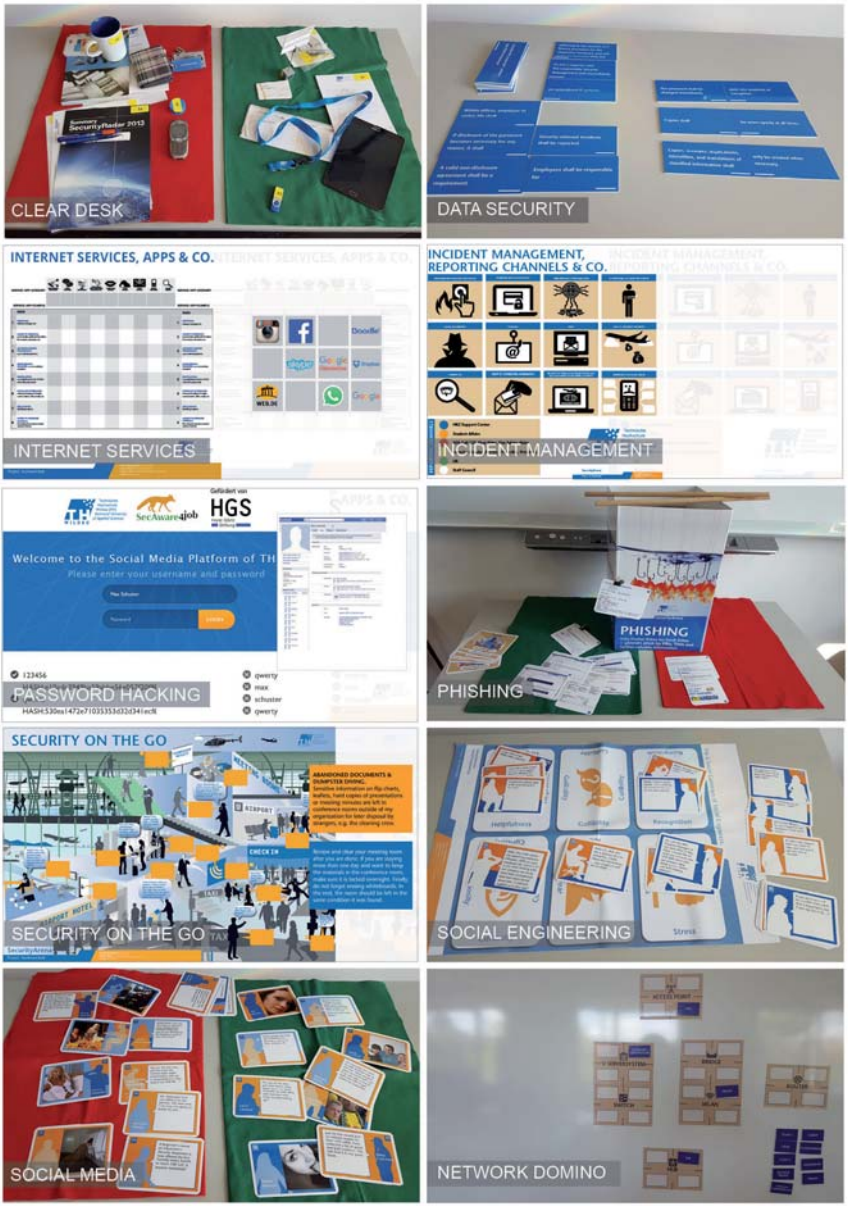


Abbildung 4: Analoge Lernszenarien der *englischen Security-Arena*

An der Station *Security on the Go* lernen die Studierenden mögliche Gefahren und entsprechende Schutzmaßnahmen auf Dienstreisen kennen.

Die Lernstation *Social Engineering* soll den Studierenden bewusst machen, welche menschlichen Eigenschaften (auch „Soziale Einfalltore“ genannt) von kriminellen Kontaktpersonen (Social Engineers) häufig ausgenutzt werden, um an sensible Informationen von Organisationen oder einzelnen Personen zu gelangen.

Welche Bilder und Beiträge unbedenklich in Sozialen Netzwerken geteilt werden können und welche lieber nicht hochgeladen werden sollten, entscheiden die Studierenden an der Station *Social Media*.

An der Station *Network Domino* wird von den Studierenden gefordert, ein Netzwerk zu konfigurieren, welches die vorgegebenen Anforderungen an Sicherheit und Funktionalität erfüllt. Damit sollen Kenntnisse über die Arbeitsweise von Netzwerkkomponenten und ihre sinnvolle sichere Anordnung vertieft werden. Je nach Wissens- und Kenntnisstand kann der Schwierigkeitsgrad dieser Station variiert werden. Diese Station existierte bislang nicht in der Security-Arena. Sie wurde vom Forschungsteam von Professorin Dr. Scholl an der TH Wildau im Rahmen der Zertifizierung zum IT-Sicherheitsbeauftragten (IT-SiBe) neu entwickelt und von known_sense produziert.

4.2 Analoge Lernszenarien

Zur Vertiefung und Anwendung der Kenntnisse zu Sicherheitsmaßnahmen, die Organi-

Abbildung 5: Analoges Lernszenario *Schutzspiel*

sationen zum Schutz ihrer sensiblen Informationen und ihrer IT-Infrastruktur einsetzen können, wurde das *Schutzspiel* (s. Abbildung 5) entwickelt. Für neun ausgewählte Gefahrenszenarien müssen die Studierenden eine Sicherheitsmaßnahme von vier vorgegebenen Alternativen, die sich hinsichtlich Kosten und Schutzlevel unterscheiden, auswählen. Um eine realitätsnahe Entscheidung zu simulieren, verfügen die Teams nur über ein begrenztes Budget. Dies erlaubt es ihnen nicht, alle Gefahrenszenarien mit dem höchsten Schutzlevel abzusichern. Ziel dieses Lernszenarios ist es, Gefahrenszenarien und entsprechende Schutzmaßnahmen zu kennen und letztgenannte hinsichtlich deren Absicherungslevel bewerten zu können. Zudem soll ein Bewusstsein für den sinnvollen Einsatz von Schutzmaßnahmen und deren Kosten entwickelt werden.

Zur anschaulichen Vermittlung und Vertiefung der Schadensszenarien nach *BSI-Standard 100-2 IT-Grundschutz-Vorgehensweise* sind die Studierenden eingeladen, beispielhafte Vorfälle den Schadensszenarien-Kategorien zuzuordnen und die entsprechenden verletzten Grundwerte zu identifizieren (s. Abbildung 6). Studierende sollen zudem geeignete Praxisbeispiele, beispielsweise aus ihrer eigenen beruflichen Erfahrung, einbringen und mögliche Schadensszenarien diskutieren und bewerten. Dadurch werden die theoretischen Grundlagen mit lebendigem Inhalt angereichert und eine bessere Wissensverankerung ermöglicht.

Abbildung 6: Analoges Lernszenario zu *BSI-Standard 100-2 Schadensszenarien*

In Anlehnung an das Kommunikations-Gesellschaftsspiel Tabu wurden Spielkarten entwickelt, auf denen Fachbegriffe der Informationssicherheit genannt sind, die den Mitgliedern des eigenen Teams erklärt werden sollen, ohne dass bestimmte Begriffe genannt werden dürfen (s. Abbildung 7). Diese „verbotenen" Begriffe würden das Erraten des Fachterminus sehr leicht machen und sind unterhalb der Linie aufgeführt. Ziel dieses *Fachtermini* Lernszenarios ist die sichere An- und Verwendung von Fachbegriffen der Informationssicherheit. Dies ist eine wichtige Voraussetzung für die Beherrschung eines Fachgebietes.

Abbildung 7: Analoges Lernszenario *Fachtermini*

4.3 Brett- und Rollenspiel

Das *Brettspiel „Keep your data private. Everyday."* und das *Social Engineering Rollenspiel* stellen die umfangreichsten und anspruchsvollsten Entwicklungen spielebasierter analoger Lernszenarien in SecAware4job dar. Daher sollen für diese beiden der Entstehungsprozess und die damit verbundenen Herausforderungen ausführlicher erläutert werden.

Das *Brettspiel „Keep your data private. Everyday."* (s. Abbildung 8) trägt der Tatsache Rechnung, dass heutzutage niemand mehr personenbezogene Daten und Informationen vollständig für sich behalten kann. Häufig müssen Informationen preisgegeben werden, um den Alltag bewältigen zu können. Das Brettspiel soll das Bewusstsein der Teilnehmenden schärfen, in welchen alltäglichen Situationen – Zuhause, in der Freizeit, beim Arbeiten, auf Reisen – sie welche Daten (z. B. E-Mail-Adresse, Kontodaten) von sich

preisgeben und durch welche Ereignisse (z. B. Ausspionieren) diese Daten möglicherweise in die Hände unbefugter Dritter gelangen können. Da es sich um ein spielebasiertes Lernszenario handelt, dürfen aber auch spielerische Elemente nicht fehlen. So entscheiden der Zufall und das Glück (z. B. gewürfelte Augenzahl, gezogene Karte) am Ende auch darüber, wer alle Daten und damit Spielpunkte zuerst verloren hat. Denn eines ist bei diesem Spiel sicher: Alle Spielenden verlieren Daten und Punkte!

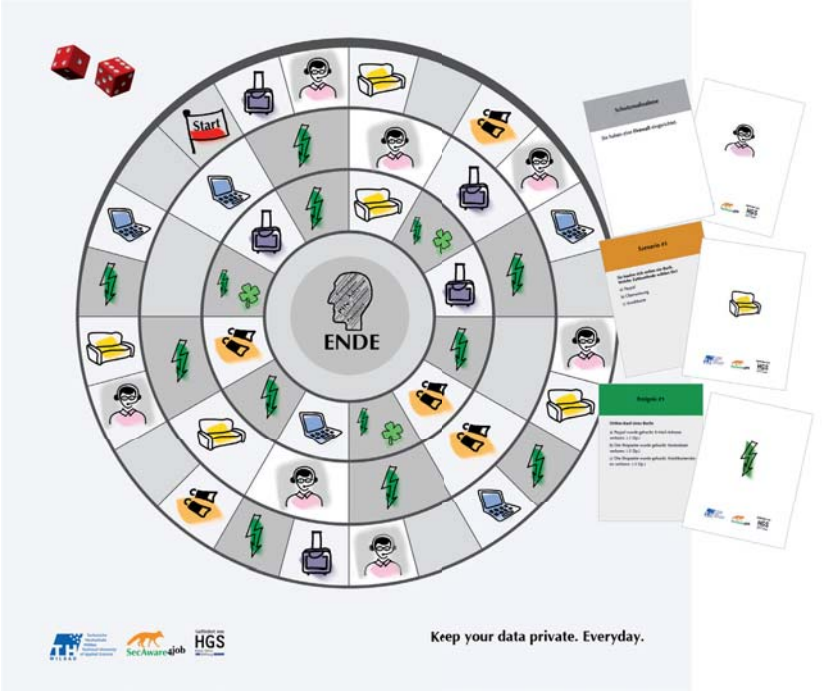


Abbildung 8: Brettspiel *„Keep your data private. Everyday.“*

Zu Beginn des Brettspieles (Abbildung 8) verfügen alle Spielenden über 15 Datenpunkte. Im Laufe des Spieles werden die Spielenden mit Szenarien aus verschiedenen Lebensbereichen konfrontiert (Zuhause symbolisiert durch Couch, Freizeit symbolisiert durch Flossen, Arbeit symbolisiert durch Laptop, Reisen symbolisiert durch Koffer), die jeweils eine Entscheidung erfordern, welche Informationen preisgegeben werden. Die Entscheidungen werden den Spielenden durch die Vorgabe von Entscheidungsalternativen erleichtert. Die Spielenden wählen die Alternative, die ihrem realen Verhalten am ehesten entspricht. Der Spielverlauf wird durch Ereignisfelder (Blitz-Symbol) beein-

flusst. Diese wirken auf von den Spielenden zuvor getroffene Entscheidungen. Beispielsweise können Daten durch einen Hackerangriff gestohlen worden sein. In Abhängigkeit davon, wie sensibel die gestohlenen, verlorenen oder freiwillig preisgegebenen Informationen sind, verlieren die Spielenden Datenpunkte. Mit ein wenig Glück können die Spielenden jedoch auch Datenpunkte aufgrund durchgeführter Sicherheitsmaßnahmen (z. B. Passwortänderung, Löschen des Facebook-Profils) hinzugewinnen oder vor dem Verlust von Datenpunkten durch eine Schutzmaßnahme (z. B. Einsatz einer Firewall, Erstellen eines Back-up) geschützt werden. Diese Belohnungs- und Schutzmaßnahmen-Karten erhalten die Spielenden auf den Feldern der Sicherheits-Fachkraft. Spielende, die fünf Datenpunkte verloren haben, rücken einen Kreis nach innen. Aus dem vorletzten Kreis können die Spielenden sich durch Würfelglück (Kleeblatt-Symbol) noch einmal einen Kreis nach außen retten. Wer jedoch den innersten Kreis erreicht, hat alle Datenpunkte und damit auch das Spiel verloren.

Das Brettspiel *„Keep your data private. Everyday.“* konnte im August 2017 nach weiteren internen Tests und einem Test mit Lehrenden im Rahmen einer Weiterbildungsveranstaltung des Landesinstituts für Schule und Medien Berlin-Brandenburg (LISUM) erfolgreich produziert werden. Die Entwicklungszeit des Brettspiels *„Keep your data private. Everyday.“* von der ersten Idee über mehrere Kreativworkshops, Prototypen mit Diskussionen und Testrunden bis letztendlich zur Umsetzung und Produktion dauerte, bei nur Teilzeitbeschäftigung der Projektmitarbeitenden, in etwa 15 Monate.

Das *Social Engineering Rollenspiel* möchte die häufig noch eher unbekannte Angriffsmethode Social Engineering besser bekannt machen und die Studierenden davor schützen, Opfer eines Social Engineers zu werden. Im Falle von Social Engineering versuchen Kriminelle, durch Täuschung und Manipulation sensible Informationen von Unternehmen, Mitarbeitenden oder Privatpersonen zu sammeln (z. B. Betriebsgeheimnisse, Passwörter). Social Engineers nutzen menschliche Eigenschaften ihrer Kontaktpersonen (auch „Soziale Einfalltore“ genannt), um an sensible Informationen zu gelangen (DATEV & DsiN 2015; known_sense et al. 2015). Durch das Rollenspiel sollen die Teilnehmenden die Sozialen Einfalltore (z. B. Neugier, Hilfsbereitschaft, Anerkennung) und entsprechende Methoden/Techniken von Social Engineers kennen und erkennen lernen. Zudem wird die Beobachtungsgabe geschult, um beispielsweise inkongruentes Verhalten von Social Engineers zu erkennen. Ferner sollen die Spielenden auf die ständige und teilweise unachtsame Nutzung mobiler Endgeräte in der Öffentlichkeit aufmerksam gemacht werden, die auch mögliche Angriffspunkte für Social Engineers bieten kann (z. B. lautes geschäftliches Telefonieren).

Die Teilnehmenden des Rollenspiels (s. Abbildung 9) können entweder einen aktiven Part übernehmen und zum Beispiel in die Rolle eines Social Engineers oder eines Opfers schlüpfen oder sie entscheiden sich für eine Beobachterposition und versuchen, möglichst viele Informationen herauszufinden. Es gibt drei unabhängige Runden: In der ersten Runde wird eine Situation in öffentlichen Verkehrsmitteln simuliert, in der die aktiven Spielenden Smartphone-„Spleens“ mimen (z. B. lautes Telefonieren in der Öffentlichkeit, ständiges Fotografieren und Veröffentlichen in Sozialen Netzwerken) und die beobachtenden Spielenden diese erkennen müssen. In der zweiten Runde werden die Beobachtenden Zeugin/Zeuge einer Social Engineering Situation. Zum Beispiel versucht eine vermeintliche Bankkundin in einem Beratungsgespräch die private Adresse

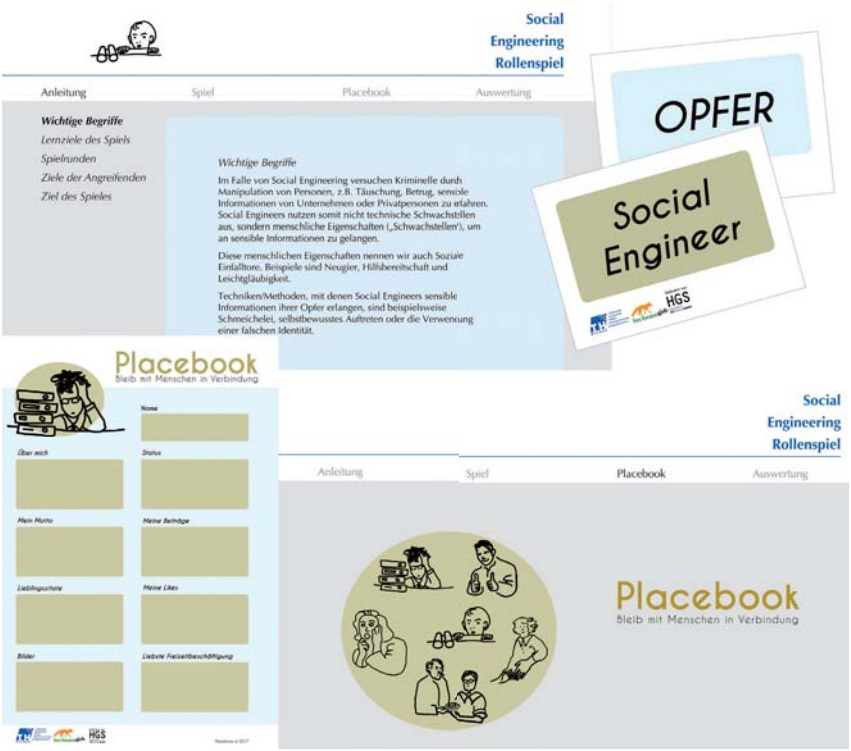


Abbildung 9: Bestandteile des *Social Engineering Rollenspiels*

des Bankangestellten zu erfahren. Die beobachtenden Spielenden haben die Aufgabe, die gespielten Sozialen Einfalltore, Techniken der Social Engineers und die geheime Information, die die/der Social Engineer zu erlangen versucht, herauszufinden. In der

dritten Runde werden alle Spielenden zum Betreten und Herumstöbern in einem Sozialen Netzwerk „Placebook“ eingeladen, um zu erraten, für welches Soziale Einfalltor die sechs präsentierten Personen anfällig sind. Darauf basierend kann ein Social Engineer seine Methode für das Ausspionieren sensibler Informationen wählen.

Die aktiv werdenden Spielenden werden durch Karten unterstützt, auf denen sie eine Rollenbeschreibung und Spieltipps erhalten. Die beobachtenden Spielenden können ihre Erkenntnisse auf einer extra dafür erstellten Webseite mithilfe eines Tablets notieren. Dies ermöglicht eine schnelle und zeitnahe Auswertung. Screenshots der Webseite, die Karten und die Placebook-Profile sind in Abbildung 9 zu sehen.

Die ersten Ideen auch für das *Social Engineering Rollenspiel* entstanden in zwei Kreativworkshops, die im Sommersemester 2016 und Wintersemester 2016/2017 von Dietmar Pokoyski (Praxispartners known_sense) an der TH Wildau durchgeführt wurden. An den Workshops nahmen die Projektmitarbeitenden sowie Studierende freiwillig und kostenfrei teil. Die Weiterführung und schließlich die Ausgestaltung der favorisierten Ideen des Rollenspiels erfolgten ebenfalls hauptsächlich durch die teilzeitbeschäftigten Projektmitarbeitenden mit Unterstützung von Dietmar Pokoyski und einer ehemaligen Studentin des Kurses im Sommersemester 2016. Im Anhang können Bilder der Workshops und der ersten Ideen angesehen werden.

Nach mehreren internen Tests wurde im Sommersemester 2017 als Freizeitaktivität ein „Spielesamstag“ veranstaltet, an dem die Piloten beider Spiele mit Projektmitarbeitenden, Dietmar Pokoyski und externen, unabhängigen Personen getestet wurden. Die Teilnehmenden zeigten sich begeistert, was aus den ersten Ideen der vorangegangenen zwei Kreativworkshops entstanden war. Insbesondere die unabhängigen Testpersonen gaben wertvolles Feedback zur weiteren Überarbeitung beider Spiele, zum Beispiel im Hinblick auf weitere Komplexitätsreduktionen im Falle des Rollenspiels und weitere Spieldynamiken für das Brettspiel.

Während das Brettspiel im August 2017 produziert werden konnte, befindet sich das Rollenspiel noch in Bearbeitung und bedarf weiterer Finanzierungsmöglichkeiten. Es wurde bereits mehrfach mit unterschiedlichen, auch unabhängigen Personen getestet. Jedoch zeigt sich gerade bei einem Rollenspiel zu diesem vielschichtigen Thema, dass die Komplexität gering gehalten, immer wieder reduziert und die Aufgaben sowohl der aktiv Spielenden als auch der Beobachtenden klein und leicht gestaltet sowie angeleitet werden müssen. Nur so kann das Rollenspiel auch von Personen absolviert werden, die mit dem Thema Social Engineering noch nicht oder nur in geringem Maße vertraut sind.

Die in Abbildung 9 gezeigte Webseite und Karten sind daher die gegenwärtigen Prototypen bei Ende des Projektes SecAware4job. Die gestalterische Umsetzung sowohl des Brettspiels als auch des Rollenspieles erfolgte mit der Unterstützung einer externen Grafikerin.

Bei der Entwicklung dieser zwei umfangreichen und komplexen analogen Lernszenarien sammelten die Projektmitarbeitenden wertvolle neue Erfahrungen, waren dabei aber mit verschiedensten Herausforderungen konfrontiert, die es zu meistern galt. Die erste Herausforderung bestand direkt nach den Kreativworkshops darin, die ersten Ideen in funktionierende Spielkonzepte zu überführen. Dies war sehr zeitintensiv und anspruchsvoll. Die ersten Ideen waren zu komplex und mussten deutlich vereinfacht werden. Die Inhalte und die Gestaltung der Spielbestandteile (Brettspiel: Spielbrett, Inhalt und Design der Karten; Rollenspiel: Inhalte, Karten, Webseite etc.) wurde mehrmals verändert und angepasst. Die fortwährenden, aber auch zeitintensiven Tests haben sehr viel bewirkt und zu vielfachen Anpassungen der Spielinhalte, der Spieldynamiken und der Spielabläufe geführt. Eine Herausforderung war auch die Abstimmung und die Einigung innerhalb des Teams. So bestanden unterschiedliche Vorlieben und Interessen in Bezug auf Spiele und Design, die nicht immer miteinander vereinbar waren. Aber dennoch mussten letztendlich Entscheidungen diesbezüglich getroffen werden. Die ständig notwendigen Absprachen mit dem Team machten die Entwicklungen noch zeitintensiver, sie waren aber sehr hilfreich, damit man nicht den Blick von außen verliert und sich immer wieder gegenseitig motiviert. Schließlich war die Unterstützung und Beratung durch Dietmar Pokoyski, dem Experten für spielebasierte Security Awareness, unentbehrlich.

4.4 Digitale Lernszenarien

Zur Vertiefung, Wiederholung und weiteren Beschäftigung mit den Lehrinhalten und den in der Vorlesung bzw. den Veranstaltungen durchgeführten analogen Lernszenarien wurden in SecAware4job acht digitale spielebasierte Lernszenarien entwickelt. Diese können ab September 2017 nach Beendigung des Projektes über die Projektwebseite (http://secaware4job.wildau.biz) abgerufen und kostenfrei genutzt werden.

Das digitale webbasierte Lernszenario *Phishing* (s. Abbildung 10) (http://secaware4job.th-wildau.de/ds/ph4/story.html) besteht aus einer kurzen Einführung, damit es auch von Personen, die diesbezüglich keine Vorkenntnisse haben, erfolgreich absolviert werden kann, und zwei voneinander unabhängigen Übungen.

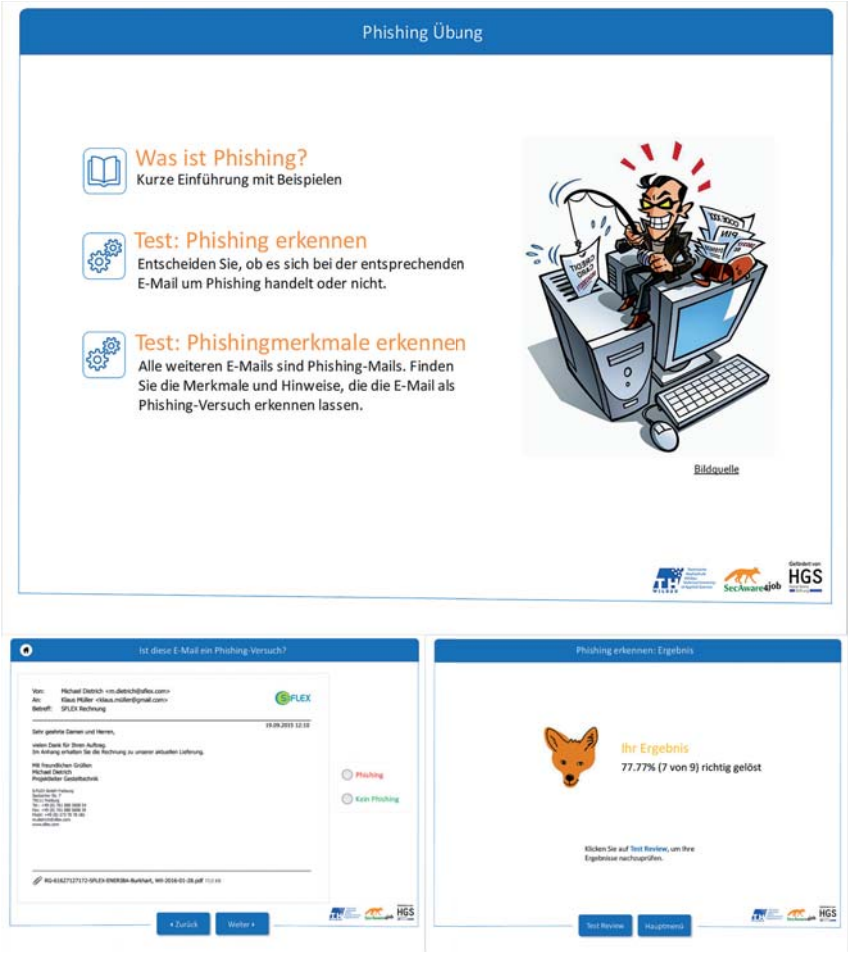


Abbildung 10: Digitales Lernszenario *Phishing*

Analog zur Phishing Station der Security-Arena besteht die erste Übung des digitalen Lernszenarios darin, reale E-Mails als Phishing-Versuch oder harmlose E-Mail zu erkennen. Die zweite Übung erhöht den Schwierigkeitsgrad und erweitert die analoge Station und andere existierende digitale Phishing-Übungen (z. B. http://www.it.tum.de/it-sicherheit/glossar/phishing-mails/selbstlerntest-phishing/) dadurch, dass bei präsentierten Phishing-E-Mails Merkmale benannt werden müssen, die auf den Phishing-Versuch hinweisen. Am Ende jeder Übung erhalten die Teilnehmenden Feedback über den Anteil richtig gelöster Aufgaben und sie haben die Möglichkeit, sich alle Aufgaben inklusive

der Musterlösung anzuschauen. Ein Mehrwert dieses digitalen Lernszenarios ist, dass das Erkennen von Phishing-E-Mails in einer realitätsnahen Umgebung eingeübt wird, denn Phishing-E-Mails liest man i.d.R. am Computer oder auf einem mobilen Endgerät. Dieses digitale Lernszenario ist mit einer Protokollierungsfunktion ausgestattet, so dass nachvollzogen werden kann, wie viele Personen zu welchen Zeitpunkten mit welchen Ergebnissen die Anwendung absolviert haben. Diese Protokollierung erfolgt anonym, so dass keine Rückschlüsse auf einzelne Personen möglich sind.

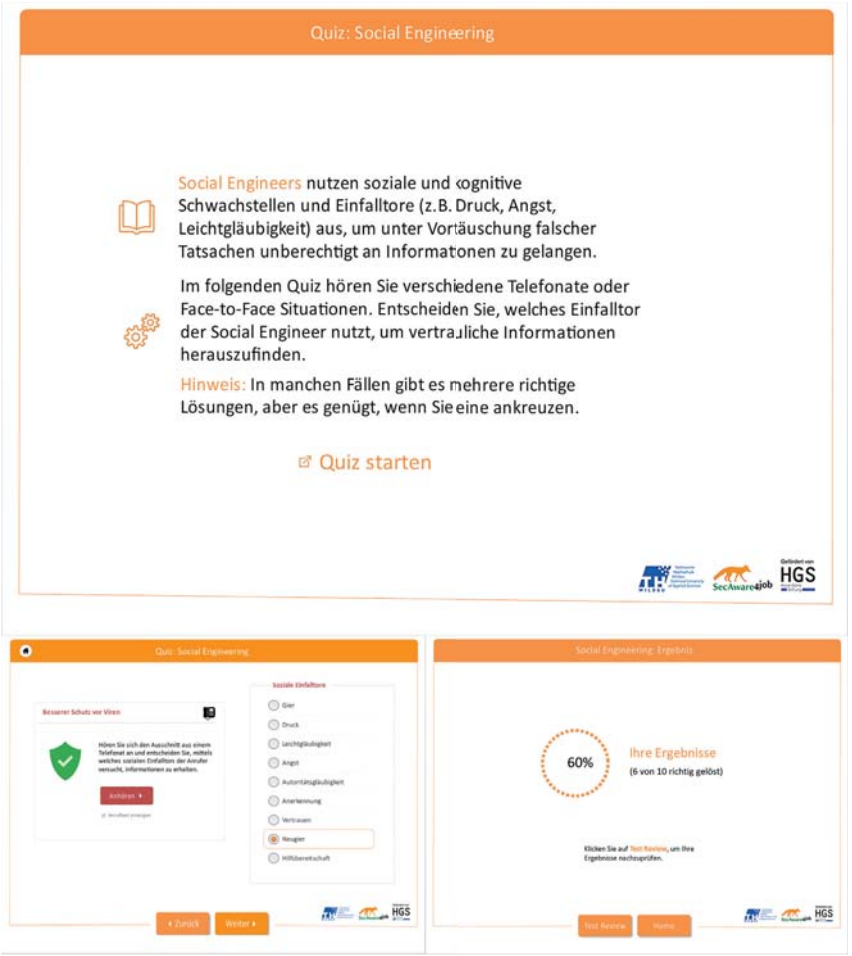


Abbildung 11: Digitales Lernszenario *Social Engineering*

Mit dem digitalen webbasierten Lernszenario *Social Engineering* (s. Abbildung 11) (http://secaware4job.wildau.biz/ds/se/story.html) können Studierende das Erkennen von Sozialen Einfalltoren wiederholen und vertiefen. Projektmitarbeitende entwickelten dafür fiktive, aber realitätsnahe Telefonanrufe und persönliche Ansprachen – häufig verwendete Methoden von Social Engineers – und nahmen diese auf. Nach dem Anhören dieser müssen die Studierenden entscheiden, welches Soziale Einfalltor der Social Engineer adressiert. Es besteht die Möglichkeit, sich den eingesprochenen Text anzeigen zu lassen. Auch dieses digitale Lernszenario beinhaltet eine kurze Einführung in das Thema. Ebenso gibt es eine Protokollierungsfunktion, mittels der die Anzahl, die Zeitpunkte und die Ergebnisse der Zugriffe auf die Anwendung ohne Zuordnung zu einer bestimmten Person nachvollzogen werden können.

Zwei digitale Entwicklungen dienen der Vertiefung und Wiederholung wichtiger Begrifflichkeiten der Informationssicherheit. In dem webbasierte Lernszenario *Hangman* (s. Abbildung 12) (http://secaware4job.wildau.biz/ds/hangman/) werden zentrale Begriffe aus Cybercrime-Gesetzen des Strafgesetzbuches (StGB) erfragt. Die Spielenden wählen Buchstaben, um das Lösungswort zu erraten. Für jeden falsch geratenen Buchstaben erhalten sie einen weiteren Strich zur Zeichnung eines Galgenmännchens. Nach

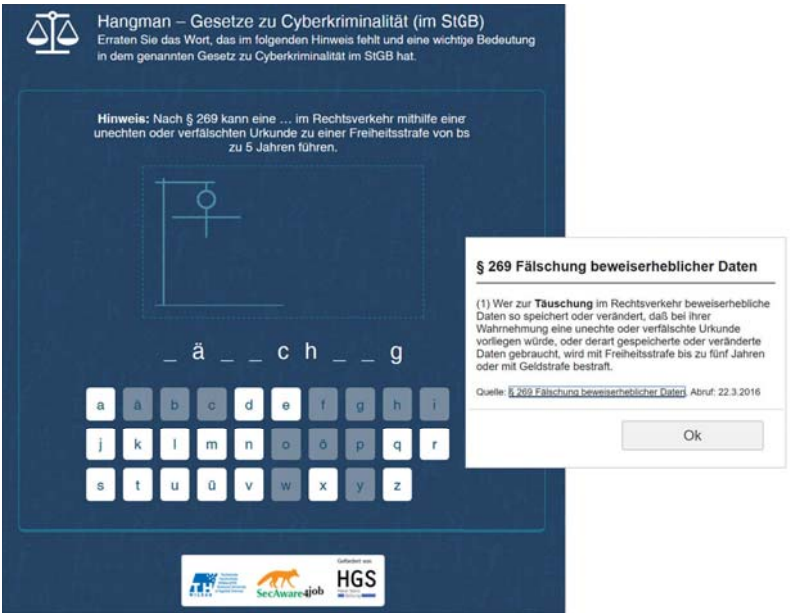


Abbildung 12: Digitales Lernszenario *Hangman*

der Beendigung einer Aufgabe können sich die Nutzenden den entsprechenden Paragraphen des Cybercrime-Gesetzes als Lösung anzeigen lassen. Diese digitale Anwendung kann beliebig um Fachbegriffe aus anderen Themenbereichen der Informationssicherheit erweitert werden.

In der Andriod-App *CBubbles* (s. Abbildung 13) werden Fragen zu Informationssicherheit gestellt, die durch die richtige Anordnung von Buchstaben-Blasen gelöst werden müssen. Die App vergibt für jede richtige Lösung Punkte in Abhängigkeit der benötigten Zeit. Kann die Frage in einer gegebenen Zeit nicht gelöst werden, verliert die/der Spielende ein Leben. Wurde der Begriff nicht erraten und sind alle Leben erloschen, wird die Antwort eingeblendet, damit sich der Begriff besser einprägt. Er muss noch einmal eingegeben werden, bevor der nächste Begriff zu erraten ist. Mittels dieser App kann somit auch gleich die korrekte Schreibweise wichtiger Fachbegriffe der Informationssicherheit gelernt werden.

Abbildung 13: App *CBubbles*

Die App *CBubbles* kann unter https://play.google.com/store/apps/details?id=com.vocaword.cbubbles.demo abgerufen und kostenfrei genutzt werden. Die Beschreibung der Listen ist unter den folgenden URL zu finden:

- https://blog.cbubbles.com/de/posts/publist-0000065-secaware4job/

- https://blog.cbubbles.com/posts/publist-0000058/

Neu ist die Möglichkeit, über geeignete Suchbegriffe die Ratelisten in der App zu finden und zu laden. Dazu muss über »+« in der App eine Suche mit den Begriffen »security« bzw. »passwort« gestartet werden.

Aus dem Unterricht von Professorin Dr. Scholl waren dem Projektteam und den Studierenden bereits analoge Storytelling-Lernszenarien mit realen Würfeln und Geschichten erzählen mit Know-how auf Flipchart-Papier bekannt. In dem webbasierten und mobilen digitalen Lernszenario *Storytelling* (s. Abbildung 14) (https://story-telling-3d.methopedia.eu/) würfeln die Studierenden sechs bis zehn Symbole, mit denen sie eine realistische Geschichte zum Thema Informationssicherheit unter Verwendung zentraler Inhalte und wichtiger Fachbegriffe schreiben sollen. Gemäß der Storytelling-Methode wird durch das Erzählen einer Geschichte das Wissen besser verinnerlicht – sowohl beim Erzählenden als auch beim Zuhörenden (Collins 1999). Üblicherweise erhalten Studierende diese Aufgabe gegen Ende der Veranstaltung, um das Gelernte in einem Zusammenhang zu präsentieren. Die digitale Version des Storytelling ist in der, durch das ehemalige Drittmittelprojekt COMBLE finanzierten, webzugänglichen Methodensammlung erreichbar: https://methopedia.eu/de/posts/storytelling/storytelling/

Abbildung 14: Digitales Lernszenario *Storytelling*

Eine digitale Entsprechung zur Clear Desk Station der Security-Arena ist das Lernszenario *Clear Room* (s. Abbildung 15). In der webbasierten 3D-Darstellung eines realistischen Büroraumes müssen die Spielenden in einer begrenzten Zeit Gegenstände und

Informationen (z. B. vertrauliches Dokument im Drucker, nicht gesperrter PC) entdecken, die sie beispielweise einschließen, sperren, verschließen, vernichten etc. müssen. Im Vergleich zum analogen Lernszenario Clear Desk ist der Schwierigkeitsgrad in der digitalen Fortführung erheblich höher, da die Beobachtungsgabe gefordert ist, alle sensiblen Gegenstände und Informationen zu entdecken und dann die richtige Aktion zu wählen (z. B. Computer abmelden). Die Entwicklung einer 3D-Anwendung ist sehr komplex, anspruchsvoll und zeitintensiv, so dass dieses Lernszenario nach Beendigung der Förderung noch weiterentwickelt werden muss, bevor es einsatzbereit ist. Dieser mit Ende des Projekts SecAware4job existierende Prototyp bedarf weiterer finanzierter Personalmittel.

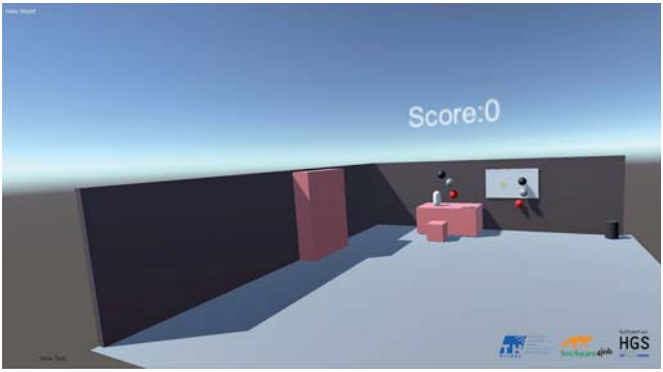


Abbildung 15: Screenshot des Prototyps *Clear Room*

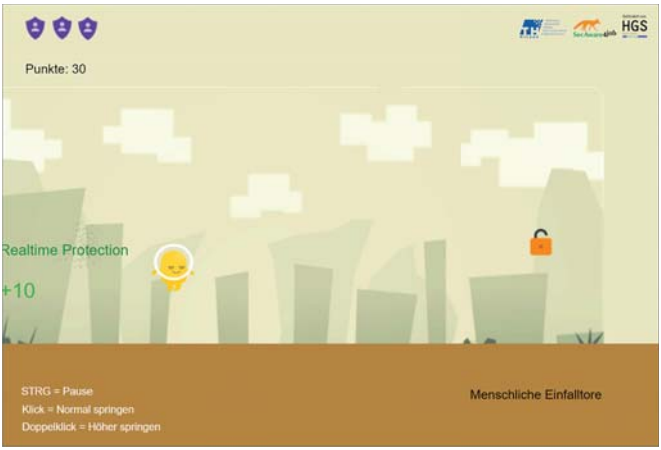


Abbildung 16: Prototyp des digitalen Lernszenarios *Security Runner*

In dem sich ebenfalls noch in der Entwicklung befindlichen webbasierten digitalen Lernszenario *Security Runner* (http://secaware4job.wildau.biz/ds/security_runner) (s. Abbildung 16) besteht die Aufgabe darin, Icons, die Gefahren oder Schutzmaßnahmen im Bereich der Informationssicherheit symbolisieren, schnell zu erkennen, um Gefahren auszuweichen und Schutzmaßnahmen „einzufangen“. Der Schwierigkeitsgrad kann gesteigert werden, indem eine spezielle Aufgabe gelöst wird (z. B. „Sammeln Sie alle Symbole, die etwas mit Social Engineering zu tun haben.“). Dieser mit Ende des Projekts SecAware4job existierende Prototyp bedarf weiterer finanzierter Personalmittel.

Eine weitere Pilotversion ist die eines digitalen webbasierten Informationssicherheits-Memory *Security Match* (s. Abbildung 17) (http://secaware4job.wildau.biz/ds/memory_match/). Sie fordert die Studierenden heraus, zwei zueinander passende Bilder des Themenbereichs Informationssicherheit aufzudecken (z. B. Virus und Anti-Virus-Software). Der Schwierigkeitsgrad kann von den Spielenden gewählt werden: In der leichten Variante gilt es, drei Paare zu finden, in der normalen müssen sechs Paare gefunden werden und die schwierige Variante lässt bei sechs zu findenden Paaren nur eine begrenzte Anzahl an Aufdeckungs-Schritten zu. Zu jedem aufgedeckten zueinander passenden Bilder-Paar können die Studierenden eine kurze Information lesen.

Abbildung 17: Digitales Lernszenario *Security Match*

Die Herausforderungen bei der Entwicklung digitaler Lernszenarien liegen in einem guten didaktischen Aufbau sowie in einer Begrenzung der Inhalte und der erforderlichen Informationen auf das Wesentliche, da i.d.R. nur eine begrenzte Zeit zum Absolvieren des Lernszenarios zur Verfügung steht. Um diesen Herausforderungen zu begegnen, wurden existierte Projekte, Studien bzw. praktische Anwendungen und Best-Practice-

Beispiele analysiert. Das Ziel der digitalen Lernszenarien ist es, vorhandene Kenntnisse zu erweitern, zu vertiefen und nachhaltig zu verankern. Um dies zu erreichen, wurde die Zielgruppe im Vorfeld genau definiert, um deren Bedürfnisse und Kenntnisse bei der Entwicklung zu berücksichtigen.

Unentbehrlich im Laufe der Entwicklung sind ständige Tests durch verschiedene Personen und unter unterschiedlichen Bedingungen (z. B. unterschiedliche Betriebssysteme, Browser). Die technische Umsetzung erfolgte mittels verschiedenen Technologien (Unity 3D, Articulate Studio, Construct 2, Vue-Framework, Blender/Blend4Web, Java/Androidstudio, Adobe Suite (Photoshop, Illustrator, InDesign)).

4.5 Innovative Lehr- und Lernmethoden

Neben den spielebasierten analogen und digitalen Lernszenarien wurden in SecAware-4job weitere innovative Lehr- und Lernmethoden entwickelt, die in der Vorlesung „Sensibilisierung für Informationssicherheit“ eingesetzt und erprobt wurden.

Durch die Erörterung aktueller öffentlich bekannter Sicherheitsvorfälle wurde die Methode *Problemorientiertes Lernen* (s. Abbildung 18) in den Unterricht aufgenommen.

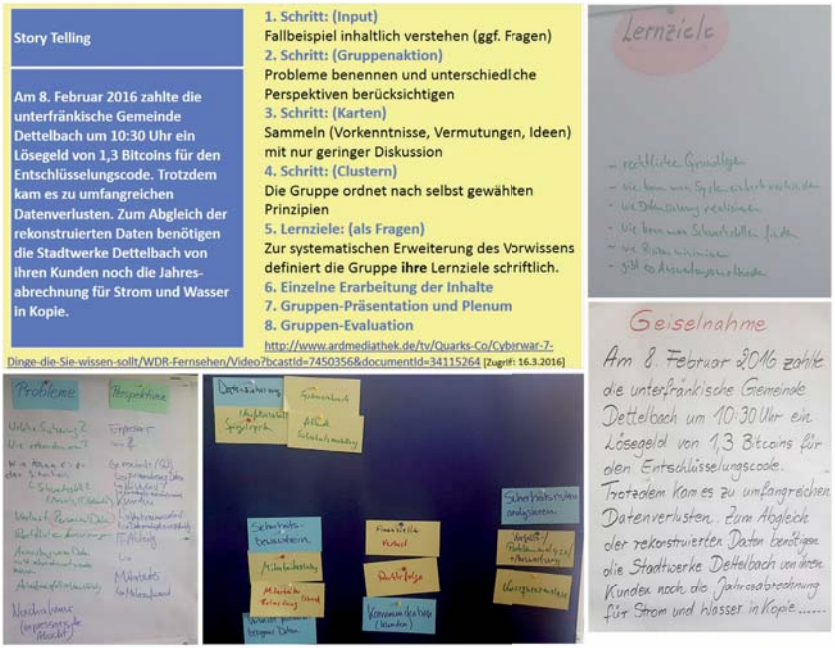


Abbildung 18: Interaktive Übung *Problemorientiertes Lernen*

Die Studierenden machen sich mit einem aktuellen Beispiel vertraut, bewerten dieses, ermitteln Schwachstellen und definieren selbst eigene Lernziele. Dies soll neben der kritischen Urteilsfähigkeit das Bewusstsein für die Relevanz des Themas Informationssicherheit fördern.

Für Studierende nicht rechtswissenschaftlicher Studiengänge ist die Behandlung von Gesetzen, Vorschriften und Regeln häufig ein trockener und schwer zugänglicher Lehrgegenstand. Daher wurde für die *Cybercrime-Gesetze* des Strafgesetzbuches (StGB) eine neue Unterrichtseinheit konzipiert und umgesetzt (s. Abbildung 19).

Abbildung 19: Materialien der Unterrichtseinheit zu *Cybercrime-Gesetzen*

Um die Studierenden mit der Relevanz und dem Ausmaß dieses Themengebietes vertraut zu machen, werden sie zu Beginn der Vorlesung eingeladen, geschwärzte und fehlende Inhalte in aktuellen Statistiken zu schätzen. Im Anschluss erarbeiten sie in Kleingruppen verschiedene Fälle des Cybercrimes und versuchen herauszufinden, welche Paragraphen des StGB bei den einzelnen Fällen betroffen sind. Die Lösungen werden anschließend mit allen Studierenden diskutiert. Als Nachbereitung der Unterrichtseinheit

und zur Verinnerlichung der relevanten Gesetze erhalten die Studierenden Gitterrätsel, in denen sie wichtige Begriffe bestimmter Paragraphen finden müssen. Zu allen Aufgaben erhalten die Studierenden unmittelbar Feedback, um einen optimalen Lernprozess zu unterstützen. Weitere Vertiefung und Wiederholung der Cybercrime-Gesetze bietet das oben präsentierte digitale Lernszenario Hangman (vgl. Kapitel 4.4).

Zur Bewusstmachung der Relevanz zentraler Themen der Informationssicherheit dienen auch die erstellten *Poster zu Cybercrime, Phishing, Social Engineering und Social Media* mit aktuellen Fakten und Zitaten. Diese finden sich im Anhang.

Die BSI-Standards sind ebenfalls für die Studierenden häufig ein schwer zugängliches Lehr- und Lernthema. Da weithin bekannt ist, dass Bilder leichter wahrgenommen und besser gemerkt werden als Texte, wurden die zentralen Inhalte des *BSI-Standards 100-1 bzw. 2001-1 „Managementsysteme für Informationssicherheit“* zur besseren Einprägung für die Studierenden visualisiert. Diese entwickelte bildliche Lernkarte findet sich im Anhang. Für die anderen BSI-Standards 100/200-2 IT-Grundschutz Vorgehensweise, 100/200-3 Risikoanalyse und 100/200-4 Notfallmanagement sollen in den nächsten Semestern ebenfalls Lernkarten visualisiert werden.

Wie bereits in Kapitel 3.4 dargelegt, wird bei der Durchführung der Vorlesung bzw. Seminare bzw. Veranstaltungen darauf Wert gelegt, möglichst viele interaktive Elemente einzusetzen. Dies sind beispielsweise Erfahrungs- und Wissensaustausch der Lehrenden mit den Studierenden und der Studierenden untereinander, Erarbeitung von Lehr- und Lerninhalten in Kleingruppen durch die Studierenden. Es wird darauf geachtet, dass möglichst wenig „Frontalunterricht“ stattfindet und die Lehrenden eher die Rolle von Coaches, Lernbegleitenden und Unterstützenden einnehmen.

Im folgenden Kapitel wird auf die Durchführung des (Wahlpflicht-) Moduls „Sensibilisierung für Informationssicherheit“ näher eingegangen.

5 Das Modul „Sensibilisierung für Informationssicherheit“

5.1 Vorbereitung

Die Zusatzqualifikation wurde in Abstimmung mit den Studiengangsverantwortlichen als Modul „Sensibilisierung für Informationssicherheit“ in existierende Studiengänge integriert, da ein freiwilliges Angebot der Weiterbildung in der freien Zeit der Studierenden das Risiko barg, dass sich nicht genügend Teilnehmende für die Weiterbildung anmelden. Zudem erleichtert die Integration der Zusatzqualifikation als (Wahlpflicht-)

Modul die angestrebte Implementierung der Weiterbildungsinhalte in allen Studiengängen zur nachhaltigen Verankerung der Thematik und zur Verstetigung des Projektes über die Förderung hinaus.

Die Basis der Auswahl der Themen des Moduls „Sensibilisierung für Informationssicherheit“ bilden die generellen, mit der Digitalisierung verbundenen Herausforderungen und technischen Trends im beruflichen und organisatorischen Kontext (siehe Abbildung 20).

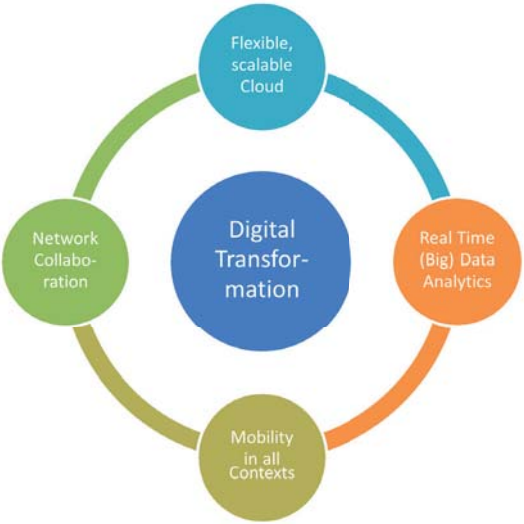


Abbildung 20: Herausforderungen und technische Trends der Digitalisierung

Die Bedeutung von Informationssicherheit steht zunächst im Vordergrund. Danach werden die Vorgänge und Methoden, die zu Informationssicherheitsvorfällen wie Wirtschaftsspionage und Datendiebstahl führen, realitätsnah veranschaulicht, um Schutzmaßnahmen einzuüben und nachhaltig zu verinnerlichen. So liegt ein Fokus z. B. auf Social Engineering, die zweithäufigste Verbrechensart, wenn es um das Ausspionieren von Daten geht (BITKOM 2015).

Zur Bewusstmachung und Gewährleistung von Informationssicherheit werden angemessene Maßnahmen spielerisch vermittelt und gelernt. Dazu gehören Themen wie Verschlüsselungsverfahren, verantwortungsvolle Nutzung von Social-Media-Anwendungen, gewissenhaftes Verhalten in der Öffentlichkeit. Ebenso werden aktuelle Trends und die damit verbundenen Vorteile und Risiken thematisiert wie z. B. steigende Mobilität,

Cloud Computing und vernetzte Zusammenarbeit. Ferner lernen die Studierenden rechtliche Rahmenbedingungen kennen wie zum Beispiel Datenschutzgesetze, rechtssichere Gestaltung von Webseiten, Internet-Nutzung am Arbeitsplatz und Aspekte des Strafgesetzbuches. Standards und Normen (BSI-Standards 100-1 bis 100-4, Normfamilie ISO/IEC 2700x, ITIL und ISO 20000 etc.) sind ebenfalls Themen des Moduls.

Zusammengefasst behandelt das Modul „Sensibilisierung für Informationssicherheit" die folgenden Themen. Die Modulbeschreibung findet sich im Anhang.

1. Informationssicherheit – warum?
2. Rechtliche Rahmenbedingungen für Informationssicherheit
3. Informationssicherheitsmanagement (ISMS)
4. Sicherheitsrelevantes Verhalten
5. Maßnahmen für Informationssicherheit
6. Verschlüsselung und digitale Signatur
7. Entwurf von Sicherheitskonzepten, insbesondere nach IT-Grundschutz (BSI)
8. Aktuelle Themen zur Informationssicherheit

Diese Inhalte wurden einerseits mit bestehenden bewährten, allerdings herkömmlich durchgeführten, Fortbildungen wie IT-Sicherheitsbeauftragte/r (IT-SiBe) und Fortbildungen zum Europäischen Computerführerschein (ECDL) abgeglichen. Andererseits wurde zu Beginn des Projektes eine hochschulweite Befragung der Studierenden der TH Wildau durchgeführt, um das Nutzungsverhalten technischer Geräte und digitaler Anwendungen sowie das vorhandene Bewusstsein und die Kenntnisse der Studierenden im Hinblick auf Informationssicherheit zu ermitteln. Dieses Vorgehen stellte sicher, dass die geplanten Inhalte der interaktiven Zusatzqualifikation alle relevanten Inhalte abdecken und an den Bedürfnissen der Zielgruppe – Studierende als zukünftige Mitarbeitende – orientiert sind.

An der hochschulweiten Befragung nahmen insgesamt 128 Studierende, davon 37,5 % weiblich, teil. Die Verteilung männlicher und weiblicher Teilnehmenden entspricht nahezu den Anteilen weiblicher (36,7 %) und männlicher (63,3 %) Studierender der TH Wildau (TH Wildau 2016). Es nahmen mehr Studierende aus dem Fachbereich Ingenieur- und Naturwissenschaften (INW) (64,1 %) als aus dem Fachbereich Wirtschaft, Informatik und Recht (WIR) (35,9 %) an der Befragung teil. Dies deutet auf ein größeres Interesse der erstgenannten hin, denn die Studierenden an der TH Wildau verteilen sich nahezu hälftig auf die zwei Fachbereiche (TH Wildau 2016).

Zentrale Ergebnisse der Befragung, die auch die Inhalte des Moduls beeinflussen, sind: Die überwiegende Mehrheit (71 %) nutzt täglich einen Laptop und nahezu fast alle Befragten (98 %) nutzen täglich ihr Smartphone bzw. Handy. Die Mehrheit greift täglich auf das Internet (94 %), den E-Mail-Account (84 %) und Soziale Netzwerke (57 %) zu. Dies sind keine überraschenden Ergebnisse, sie verdeutlichen aber die Relevanz von Informations- und IT-Sicherheit. Die Wichtigkeit, Studierende für Informationssicherheit zu sensibilisieren, wird deutlich in den Antworten zum Verhalten in Sozialen Netzwerken und zum Umgang mit Passwörtern. Von den 104 Teilnehmenden, die Mitglied eines Sozialen Netzwerkes sind, teilen 74 Personen ihren Namen, 56 Personen ihr Geburtsdatum, 51 Personen ihren Wohnort und 70 Personen ihre Hochschule. Damit sind mehr als die Hälfte der Befragten sehr gut zu identifizieren.

Im Hinblick auf Passwörter zeigt sich, dass die Mehrheit der Befragten ein Bewusstsein für sichere Passwörter hat. 62,5 % verwenden lediglich für drei und weniger Geräte (z. B. Laptop, Smartphone) und/oder Online-Anwendungen (z. B. WLAN, E-Mail, Online-Banking) dasselbe Passwort, die Hälfte davon nutzt für jedes Gerät bzw. Anwendung ein anderes Passwort. Zudem bestehen die Passwörter von 96,1 % der Teilnehmenden aus sieben und mehr Zeichen. Dabei setzen sich die Passwörter der Mehrheit (60,9 %) aus Klein-, Großbuchstaben, Zahlen und Sonderzeichen zusammen. Es muss allerdings bedacht werden, dass viele Internet-Dienste vorgeben, welche Bestandteile ein Passwort und wie viele Zeichen es mindestens umfassen muss. Gleichwohl ändern die Befragten ihre Passwörter nur sehr selten bzw. nie. Abbildung 21 zeigt dies für Geräte und Anwendungen, die nahezu alle Befragten nutzen.

Die Antworten auf die Fragen zur Ermittlung der Kenntnisse der Studierenden im Bereich Informationssicherheit zeigen, dass eine große Mehrheit der Teilnehmenden Bedrohungen wie Phishing (75,6 %) oder Spyware (80,2 %) kennen. Jedoch bestehen Wissenslücken hinsichtlich der Angriffsmethode Social Engineering. Nur 31,8 % der Teilnehmenden wählten die richtige Antwort und 34,9 % gaben an, nicht zu wissen was Social Engineering ist. Dies unterstützt die inhaltliche Planung, einen Fokus auf Social Engineering zu legen. Zudem sollten die Grundwerte der Informationssicherheit behandelt werden, denn diese waren ebenfalls nur der Hälfte oder wenigen der Befragten bekannt: Integrität (50,8 %), Verfügbarkeit (28,2 %), Vertraulichkeit (30,7 %). Der Fragebogen und weitere Ergebnisse finden sich im Anhang.

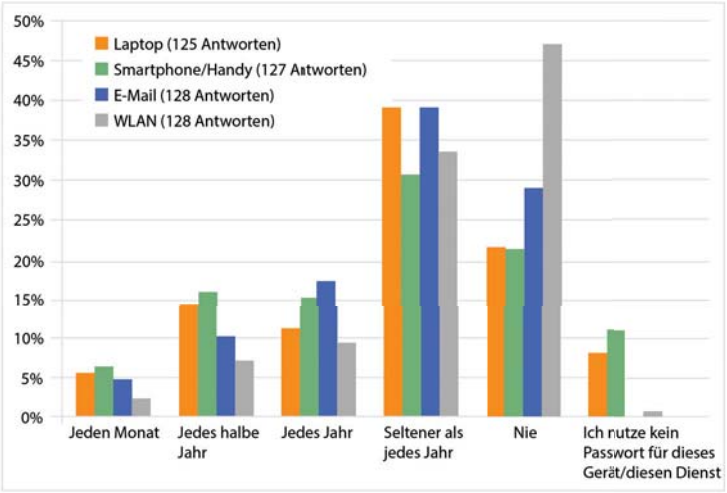


Abbildung 21: Häufigkeit der Änderung von Passwörtern (hochschulweite Befragung)

5.2 Durchführung

Das Modul „Sensibilisierung für Informationssicherheit“ wurde im Sommersemester (SoSe) 2016 und 2017 als Wahlpflichtfach im 8. Semester des berufsbegleitenden Studiengangs Betriebswirtschaftslehre (BWL) und im Wintersemester (WS) 2016/17 im Rahmen des Moduls „Allgemeine Verwaltungsinformatik/E-Government“ im 5. Semester des Studiengangs Kommunales Verwaltungsmanagement und Recht (KVR) durchgeführt. Dadurch konnte untersucht werden, ob die Zusatzqualifikation als Wahlpflichtfach oder Pflichtfach angeboten werden sollte. Das Angebot als Pflichtveranstaltung ermöglicht die Sensibilisierung von Studierenden, die sich nicht sowieso bereits für das Thema interessieren und erreicht somit einen weiteren Personenkreis. Gleichwohl spricht für das Angebot als Wahlpflichtfach, für das die Studierenden sich bewusst entscheiden, dass die Bereitschaft, sich mit dem Thema Informationssicherheit auseinanderzusetzen, vermutlich höher ist und dadurch eine höhere Wirksamkeit erzielt werden kann. Denn Motivation und Emotionalisierung sind i.d.R. bei freier Wahl größer.

Im Sommersemester 2016 nahmen fünf Studierende (2 weiblich, 3 männlich) an der Lehrveranstaltung teil, durchschnittlich waren vier Teilnehmende anwesend. Die Studierenden zeigten sich sehr motiviert und beteiligten sich rege an der Lehrveranstaltung. Ihre hohe Motivation spiegelte sich auch darin wider, dass alle fünf Teilnehmenden das im Rahmen der Zusatzqualifikation angebotene höchste Zertifikat zur/zum IT-Sicherheitsbeauftragten (IT-SiBe) anstrebten (vgl. Kapitel 5.3).

Im Wintersemester 2016/17 nahmen elf Studierende (9 weiblich, 2 männlich) an dem regulären Fach „Allgemeine Verwaltungsinformatik/E-Government“, in dem die Themen des Moduls „Sensibilisierung für Informationssicherheit“ integriert wurden, teil. Der Studiengang KVR sieht in der vorlesungsfreien Zeit berufspraktische Phasen in der öffentlichen Verwaltung vor. Daher besitzen auch diese Teilnehmenden bereits berufliche Praxiserfahrung. In dieser Veranstaltung wurde eine innovative Prüfungsleistung, bestehend aus der bekannten Prüfungsleistung „Projektarbeit“ und der neuen Prüfungsleistung „Präsentation in Form eines Plakates“, erprobt. Aufgrund des geringeren Interesses und der geringeren Vorkenntnisse der Studierenden dieses Kurses wurden die Studierenden motiviert, an der IT-Sicherheit- oder Datenschutz-Prüfung des Europäischen Computerführerscheins (ECDL) teilzunehmen (vgl. Kapitel 5.3). Die Lehrinhalte wurden entsprechend vereinfacht und stärker an den ECDL-Prüfungen anstatt der IT-SiBe-Prüfung ausgerichtet. Dieses Modul konnte des Weiteren durch einen Gastvortrag über das Datenschutzrecht und die Aufgaben eines Datenschutzbeauftragten von Herrn Tessendorf, Datenschutzbeauftragter (DSB) und Geschäftsführer der proca-do Consulting, IT- & Medienservice GmbH, Berlin bereichert werden. Für die Teilnehmenden im Wintersemester 2016/17 wurde ein neuer Einstiegsfragebogen zu ihren Kenntnissen und ihrem Bewusstsein zu Informations-/IT-Sicherheit im beruflichen Alltag entwickelt. Die Fragen basieren auf bestehenden aus der Literatur. Der Fragebogen wurde in der ersten Veranstaltung von den Studierenden ausgefüllt, um die Inhalte der Lehrveranstaltung entsprechend anzupassen. Der Fragebogen und interessante Ergebnisse der Befragung finden sich im Anhang.

Im Sommersemester 2017 entschieden sich sechs Studierende (1 weiblich, 5 männlich) für das Wahlpflichtmodul. Ebenso wie die Studierenden des berufsbegleitenden Studiengangs im Sommersemester 2016 strebten fünf der sechs Teilnehmenden das Zertifikat zum IT-SiBe an. Das Modul „Sensibilisierung für Informationssicherheit“ in den drei Pilot-Durchläufen wurde von Professorin Dr. Scholl, ihrem Laboringenieur Peter Ehrlich und den Projektmitarbeitenden durchgeführt. Neben den interaktiven Lehr- und Lernmethoden trug auch das Teamteaching zur Abwechslung und Besonderheit des Moduls bei. Dies wurde von den Studierenden sehr positiv wahrgenommen (vgl. Kapitel 5.4). Es wäre erstrebenswert, Teamteaching in die Stundenplanung aufzunehmen, doch müssen hierzu die Anrechnungsfaktoren für das Lehrdeputat der Beteiligten erst noch geklärt werden.

Als Test der Übertragbarkeit der IT-SiBe-Prüfung auf technische Studiengänge wurde im Sommersemester 2017 ein Pilot-Angebot für Wahlpflichtfächer (WPF) mit Themen

der Informationssicherheit im Studiengang Wirtschaftsinformatik durchgeführt: In zwei WPF zu Informationssicherheit des Studiengangs Wirtschaftsinformatik sollte getestet werden, inwieweit diese Studierenden mit ihren vertieften Vorkenntnissen, durch Eigenengagement und aus eigenem Antrieb (ohne zusätzliche Vorlesung) heraus die IT-SiBe-Prüfung bestehen werden. Ein entsprechendes kostenpflichtiges Angebot wird ab dem Wintersemester 2017/18 bereitgestellt. Den Studierenden wurde dazu das BAköV-Handbuch ausgeliehen und ein kurzer Leitfaden zur Prüfungsvorbereitung von Professorin Dr. Scholl zur Verfügung gestellt. Die Studierenden der Wirtschaftsinformatik waren sehr begeistert von dem durch SecAware4job gesponserten Angebot, die Prüfung kostenlos absolvieren zu können. Die Nachfrage nach dem Angebot war sehr hoch, so dass aus Kapazitätsgründen eine Auswahl getroffen werden musste und zehn Studierende zur IT-SiBe-Prüfung zugelassen wurden. Auch aus anderen technischen Studiengängen lagen Anfragen vor, so dass davon ausgegangen werden kann, dass eine zukünftige Verstetigung dieses dann kostenpflichtigen Prüfungsangebotes zur/zum IT-SiBe möglich ist, vor allem dann, wenn Unternehmen/öffentliche Verwaltungen den Studierenden eine solchen Zertifikatsprüfung sponsern werden.

5.3 Zertifikatshierarchie in SecAware4job

Zum Nachweis ihrer erworbenen Informationssicherheits-Kompetenzen können die Studierenden des Moduls „Sensibilisierung für Informationssicherheit“ unterschiedliche Zertifikate für ihren Berufseinstieg erwerben (s. Abbildung 22). Die Basis bildet das „Teilnahmezertifikat“, das die Studierenden durch ihre aktive Teilnahme an der Zusatzqualifikation erhalten. Entwickeln und modifizieren die Studierenden zudem eigenständig kreative Methoden (z. B. Lernszenarien, Übungen) zur Sensibilisierung für Informationssicherheit und erproben diese (im Kurs, in ihrer Semestergruppe, in ihrem Unternehmen), erhalten sie zudem ein „Moderationszertifikat“.

Durch das Projekt SecAware4job wurde die Akkreditierung der TH Wildau als ECDL-Prüfungszentrum, ausgeführt durch Professorin Dr. Scholl, angestoßen und verwirklicht. Damit konnte das zu absolvierende Zertifikatsspektrum für die Studierenden erweitert und den variierenden Bedürfnissen und Wissensständen der Studierenden besser angepasst werden. Die ECDL-Zertifikate bieten die Möglichkeit einer „Zwischenprüfung“ vor der umfangreicheren und anspruchsvolleren Prüfung zur/zum IT-Sicherheitsbeauftragten. So besteht inzwischen die generelle Möglichkeit für alle Studierenden, an den kostenpflichtigen Prüfungen IT-Sicherheit und Datenschutz des Europäischen Computerführerscheins (ECDL) teilzunehmen und ein entsprechendes ECDL-Zertifikat zu

erhalten. Entsprechendes ist für den aus fünf Modulen bestehenden Datenschutzführerschein möglich, da die TH Wildau im Verlauf des Projektes SecAware4job und auf Initiative von Professorin Scholl auch Prüfungszentrum der Dienstleistungsgesellschaft für Informatik mbH (DLGI) für den Datenschutzführerschein geworden ist.

Für die Anfertigung einer praxisorientierten Projektarbeit im WPF „Sensibilisierung für Informationssicherheit“ erhalten die Studierenden das „Qualifizierte Zertifikat Projektarbeit“. Sie dient ebenfalls als Belegarbeit für die Note im WPF. Die Projektarbeit kann darüber hinaus prinzipiell für die Prüfung zur/zum IT-Sicherheitsbeauftragten nach BAköV/BSI, die über das Institut WILLE an der TH Wildau angeboten wird, anerkannt werden. Mit erfolgreichem Abschluss einer zusätzlichen, umfangreichen schriftlichen Prüfung zur/zum IT-Sicherheitsbeauftragten (IT-SiBe) am PC erhalten die Studierenden bei Bestehen ein für fünf Jahre gültiges offizielles Zertifikat. Durch Nachweise entsprechender Weiterbildungen im Verlauf der fünfjährigen Gültigkeit kann das Zertifikat verlängert werden. Während der Projektlaufzeit von SecAware4job konnten die Studierenden des Moduls „Sensibilisierung für Informationssicherheit“ freiwillig und kostenfrei an den ECDL-Prüfungen und der IT-SiBe-Prüfung teilnehmen.

Abbildung 22: Zertifikatshierarchie des Projektes SecAware4job

Aus den drei Pilot-Durchläufen des Moduls „Sensibilisierung für Informationssicherheit“ nutzten neun Studierende und ein studentischer Mitarbeiter des Projektes das An-

gebot, kostenfrei an der IT-SiBe-Prüfung teilzunehmen. Zusätzlich nahmen zehn Studierende des Studiengangs Wirtschaftsinformatik an der TH Wildau, die andere Module zum Thema Informationssicherheit besuchten, das Pilot-Angebot im WS 2017 wahr, unabhängig vom Modul „Sensibilisierung für Informationssicherheit“ die IT-SiBe-Prüfung kostenfrei bzw. gesponsert durch SecAware4job abzulegen. 15 Teilnehmende haben die IT-SiBe-Prüfung erfolgreich bestanden, eine Person hat auch die Wiederholungsprüfung nicht bestanden und vier Studierende werden Mitte August die Wiederholungsprüfung absolvieren.

Drei Studierende der Lehrveranstaltung im Wintersemester 2016/17 und ein Projektmitarbeiter nutzten erfolgreich die Möglichkeit, Prüfungen des ECDL abzulegen. Zwei Projektmitarbeitende werden dieses Angebot voraussichtlich Mitte August noch in Anspruch nehmen.

5.4 Evaluation

Neben der hochschulweiten Befragung zu Beginn von SecAware4job (vgl. Kapitel 5.1) bestand die wissenschaftliche Begleitforschung in der Evaluation der Wirkung der eingesetzten Methoden sowie in der Ermittlung des Lernerfolges.

Die abschließende Evaluation (s. Abbildung 23) in den einzelnen Semestern zeigt, dass die Studierenden der drei Pilot-Durchläufe mit der Lehrveranstaltung und dem angewandten methodischen Ansatz – bestehend aus einer Kombination aus Vortrag, analogen und digitalen spielebasierten Lernszenarien sowie interaktiven Übungen – zufrieden waren.

Es fällt allerdings auf, dass die Teilnehmenden im WS 2016/17, die das Modul als regulären Kurs besuchten, die Lehrveranstaltung weniger interessant fanden als die Teilnehmenden der Wahlpflichtfächer. Da es sich um einen regulären Kurs handelte, wurde im WS 2016/17 die letzte Frage nach der Zufriedenheit mit der Entscheidung für diese Lehrveranstaltung nicht gestellt. Der Fragebogen kann im Anhang eingesehen werden. Im SoSe 2016 beantworteten vier Teilnehmende, im WS 2016/17 zehn bzw. neun Teilnehmende und im SoSe 2017 drei bzw. zwei Teilnehmende die Evaluation. Die verwendete Skala hat die Endpunkte „1 = Stimme nicht zu“ und „5 = Stimme zu“.

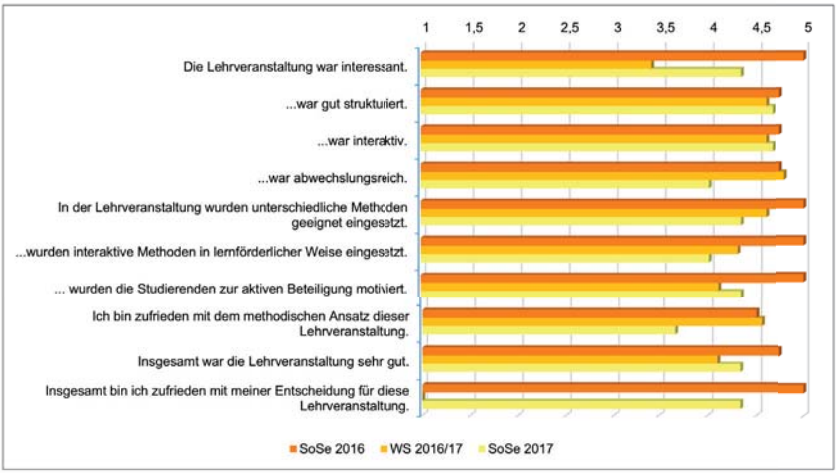


Abbildung 23: Evaluation der drei Pilot-Lehrveranstaltungen

Insbesondere in der ersten Pilot-Durchführung wurde nahezu in jeder Veranstaltung ausführliches Feedback von den Studierenden zu den eingesetzten spielebasierten Lernszenarien und den durchgeführten interaktiven Übungen erbeten. Hierbei wurde die Komplementarität aus analogen und digitalen Lernszenarien gelobt. Die analogen Lernszenarien besitzen den Vorteil, dass man sie im Team lösen und so an dem Wissen und den Kenntnissen der anderen Studierenden teilhaben kann. Es besteht auch die Möglichkeit, sich einmal zurückzulehnen und die anderen machen zu lassen. Die digitalen Lernszenarien bieten hingegen den Vorteil, dass man persönlich gefordert ist und die Aufgabe alleine lösen muss und Feedback zu seinen Leistungen erhält.

Das Ziel des Projektes, Informationssicherheitsbewusstsein zu stärken und entsprechende Kenntnisse zu verbessern sowie idealerweise Verhaltensänderungen auszulösen, wurde gemäß der Selbsteinschätzung der Teilnehmenden insbesondere bei den Studierenden der Wahlpflichtfächer im SoSe 2016 und 2017 und für deren Arbeitsleben erreicht (s. Abbildung 24). Die Skalenendpunkte waren wiederum mit „1 = Stimme nicht zu“ und „5 = Stimme zu“ bezeichnet.

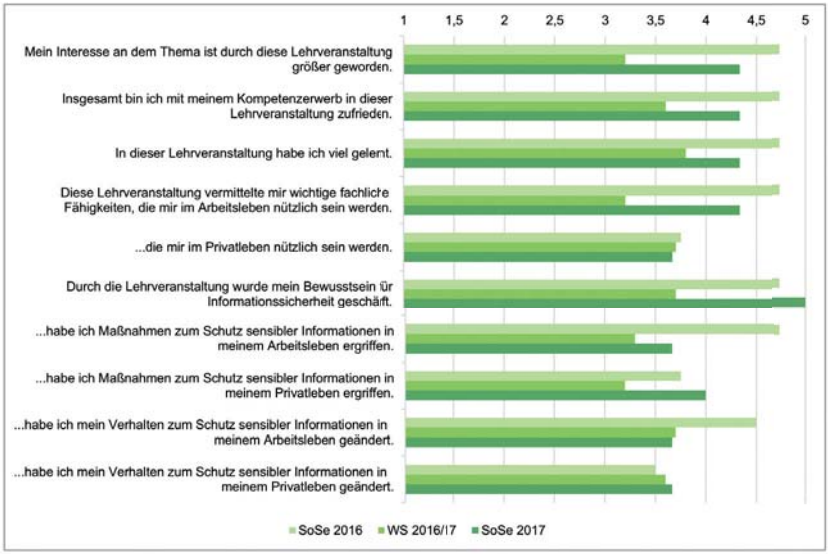


Abbildung 24: Selbsteinschätzung der Wirksamkeit durch Studierende

Auch die Antworten auf die offenen Fragen spiegeln die Zufriedenheit der Teilnehmenden wieder. Am zufriedensten waren, wie auch die Abbildungen 23 und 24 zeigen, die Studierenden im SoSe 2016, wo alle Projektmitarbeitenden in den Unterricht einbezogen waren und spezifisch Spezialthemen behandelten.

Was hat gut gefallen? / Was sollte beibehalten werden? (SoSe 2016)

- „*Wieder sehr gut abwechslungsreich in Methoden* ☺"
- „*Endlich mal ein interaktiv gestaltetes Modul. Super! Weiter so! Danke* ☺"
- „*dass ein Übungsteil dabei war*"
- „*kleine Gruppe*"
- „*technische Ausstattung*"
- „*Anschauungsmaterial*"
- „*verschiedene (viele) Ansprechpartner*"
- „*gut strukturiert (was erwartet mich?!, abwechslungsreich (Vortragende), Wechsel zwischen Theorie/Praxisbeispiel (Übung), Auflockerung durch Methoden (verschiedene – z. B. das ‚Spiel' mit den Karten), Verweise auf Inhalt der Vorlesung – wo finde ich mehr Info dazu*"
- „*Spiele zur Auflockerung / Teambildung"*
- „*Interaktivität*"
- „*Spaß*"

Anregungen und Verbesserungsvorschläge (SoSe 2016)

- „*Teilweise sehr knapp wegen Zeitnot.*"

- „E*in bisschen zu viel für die Zeit, deswegen Eingehen auf einzelne Themen und Diskussionen schwierig.*“
- „*Die Vielfalt des Kurses (Video, Spiele, Vorträge) ist bei großer Teilnehmerzahl eher schwierig.*“
- „*Die IT-SiBe-Prüfung mit Spielen verbinden; also dass man eine Art „Begriff und Lösung“ Karten den Studenten gibt zum Lernen zu Hause, Bsp. Was ist VPN?*“

Was hat gut gefallen? / Was sollte beibehalten werden? (WS 2016/17)

- *„spielerische Untermalung“*
- *„abwechslungsreiche Gestaltung“*
- *„spielerisch komplexe und abstrakte Themen erarbeiten bzw. verinnerlichen“*
- *„angenehme Atmosphäre“*
- *„Auflockerung der Vorlesung durch Spiele“*
- *„Angenehme Sprechweise der Dozenten“*
- *„Guter Zugang auch für Menschen mit geringer Vorbildung“*
- *„Spielerische Darbietungen“*
- *„Trotz anfänglicher Skepsis waren die Spiele zum Thema sehr hilfreich zur Stoffvermittlung und Auflockerung der Themen“*
- *„Spielerisch lernen“*
- *„Abwechslungsreiche Gestaltung des Unterrichts“*
- *„Verschiedene Lehrmethodiken“*

Anregungen und Verbesserungsvorschläge (WS 2016/17)

- *„Datenschutzrechtliche Stellen werden in den Verwaltungen direkt durch dafür ausgebildete Fachleute besetzt, daher für unseren Studiengang nicht vollständig anwendbar“*
- *„Die Themen sind sehr fachlich gewesen – für jemanden ohne Erfahrung in diesem Bereich oftmals schwer nachzuvollziehen“*
- *„Vorlesungsinhalte für Laien sehr schwer, wird im Arbeitsalltag nicht so benötigt“*
- *„Project Libre: Vermittlung wäre für die Prüfung besser gewesen“*
- *„Project Libre besser erklären“*
- *„Bessere Abstimmung auf den beruflichen Hintergrund – wir sind alle in der Verwaltung angestellt und werden mit der hintergründigen IT-Sicherheit wenig Berührungspunkte haben“*

Was hat gut gefallen? / Was sollte beibehalten werden? (SoSe17)

- *„überschaubare Gruppe“*
- *„viel Zeit für Fragen“*
- *„Skripte“*
- *„Wiederholungen zu vorherigem Seminar“*
- *„zwei Ansprechpartner“*

Anregungen und Verbesserungsvorschläge (WS 2016/17)

- *„mehr praktische Anwendung“*
- *„je nach Vorkenntnissen teilweise zu tiefgreifende Infos“*

Rückschluss auf den erzielten Lernerfolg bietet auch die Teilnahme der Studierenden an den von der TH Wildau unabhängigen, komplexen Prüfungen zur/zum IT-SiBe nach BaköV/BSI und für den ECDL. Das erfolgreiche Bestehen nahezu aller Studierenden, die an diesen Prüfungen teilgenommen haben, belegen die praktische und erfolgreiche Anwendbarkeit der in SecAware4job entwickelten analogen und digitalen Lernszenarien sowie der innovativen Lehrmethoden – gerade auch für weniger technik-affine Personen. Im Hinblick auf die Frage, ob das Modul „Sensibilisierung für Informationssicherheit“ als regulärer Kurs oder als Wahlpflichtfach angeboten werden sollte, sprechen die Ergebnisse der Evaluationen und auch das Interesse an den Zertifikatsprüfungen dafür, das Modul als Wahlpflichtfach zu konzipieren.

Darüber hinaus erfuhr die Anwendung der Materialien und Methoden in vielen anderen Veranstaltungen mit weiteren Zielgruppen, z. B. Mitarbeitenden und Gästen der Hochschule, stets ein äußerst positives Feedback (vgl. Kapitel 6.2).

6 Bekanntmachung des Projektes und der Projektergebnisse

6.1 Öffentlichkeitsarbeit

Für das Projekt wurden begleitende Designelemente und Informationen entworfen, um das Projekt bekannt zu machen und es von anderen Projekten abzugrenzen. Das Projektlogo mit uneingeschränkten Nutzungsrechten wurde mit der Unterstützung einer externen Grafikerin entwickelt und ist in Abbildung 25 zu sehen. Als Bestandteil des Logos wurde ein Fuchs gewählt, da der Fuchs als kluges und wachsames Tier gilt. Diese Eigenschaften sind im Bereich der Informationssicherheit sehr wichtig. Auf die Zugehörigkeit des Projektes zur TH Wildau und auf die Förderung des Projektes durch die Horst Görtz Stiftung wurde jeweils mit den entsprechenden Logos verwiesen (vgl. z. B. Titel des Abschlussberichts).

Abbildung 25: Logo des Projektes

Es wurden weitere Fuchs-Ansichten entworfen, um diese beispielsweise im Rahmen von Lernszenarien (vgl. z. B. digitales Lernszenario Phishing), für weitere kommunikative Zwecke und für Flyer einzusetzen. In Abbildung 26 sind beispielhaft ein paar dieser entwickelten Fuchs-Ansichten, auch mit verschiedenen Emotionen versehen, gezeigt.

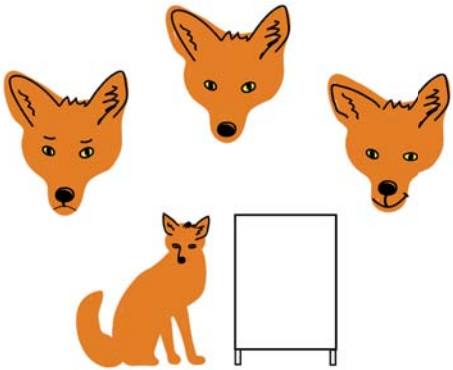


Abbildung 26: Entworfene Fuchs-Ansichten

Eine Projektwebseite wurde gleich zu Beginn des Projektes konzipiert und programmiert, auf der Interessierte aktuelle Informationen zu SecAware4job in Deutsch und Englisch abrufen können. Mit der Beendigung des Projektes können die digitalen Lernszenarien über die Webseite abgerufen und kostenfrei genutzt werden. Die Projektwebseite ist erreichbar über http://secaware4job.wildau.biz. Für einen ersten Eindruck finden sich Screenshots im Anhang. Nach dem Web-Relaunch der Webseiten der TH Wildau, der im September 2017 stattfinden soll, werden die Projektseiten ebenfalls unter der TH Wildau Webpräsenz zur Verfügung stehen.

Zudem wurden Plakate und Flyer in Deutsch und Englisch entworfen, mit denen interessierte Personen, Multiplikatorinnen und Multiplikatoren sowie zukünftige Projektpartner auf das Projekt aufmerksam gemacht wurden. Die Plakate und Flyer finden sich ebenfalls im Anhang. Das Projekt SecAware4job wurde auch im Forschungsbericht 2015 und 2016 der TH Wildau vorgestellt und wird im Forschungsbericht 2017, der im Frühjahr 2018 erscheinen wird, ausführlicher beschrieben werden.

Zu wichtigen Anlässen im Projekt wurden Presseberichte erstellt. Dies geschah zur Akkreditierung der TH Wildau als ECDL-Prüfungszentrum (15. Januar 2016), zum Besuch

des SPD Arbeitskreises „Digitale Gesellschaft“ (25. Mai 2016), zu den Kreativworkshops, in denen die ersten Ideen für das Brettspiel „Keep your data private. Everyday.“ und das Social Engineering Rollenspiel entstanden, (25. Oktober 2016) sowie zum Test dieser beiden neu entwickelten analogen Lernszenarien (9. Mai 2017, 11. Mai 2017). Mitte August 2017 ist noch der Besuch der regionalen CDU im Trainingszentrum für Informationssicherheit von Professorin Scholl an der TH Wildau geplant – auch hier wird es um die entwickelten spielebasierten Lernmethoden für Informationssicherheit und Awareness gehen.

Im Zuge des Besuches von Frau Goll, Leiterin Digitales Innovationszentrum in Stuttgart (DIZ), und zwei ihrer Mitarbeitenden am 11. Mai 2017 in Wildau zur Besichtigung der spielebasierten Aktivitäten wird noch im August 2017 eine Kooperationsvereinbarung zwischen der TH Wildau und dem DIZ schriftlich unterzeichnet. Das DIZ ist zudem zur Unterzeichnung von Letter of Intent (LOI) für weitere Projektanträge bereit, da es von dem Engagement und den Ergebnissen der Forschungsgruppe von Professorin Dr. Scholl im Projekt SecAware4job sehr überzeugt ist.

Zum Abschluss des Projektes ist erneut eine Berichterstattung auf der Campusseite der Märkischen Allgemeinen Zeitung geplant. Diese Berichte in öffentlichen Medien tragen zur weiten Bekanntmachung des Projektes und seiner Ergebnisse bei. Die bisherigen sind im Anhang aufgeführt.

6.2 Veranstaltungen

Bei zahlreichen Gelegenheiten – Konferenzen, persönlichen Gesprächen, Veranstaltungen der TH Wildau – wurden die in SecAware4job entwickelten analogen und digitalen Lernszenarien sowie innovativen Lehrmethoden vorgestellt und zum Testen angeboten. Damit wurden die Lernszenarien mit verschiedenen Zielgruppen erprobt, so dass ihr Einsatz als breitenwirksam und nachhaltig bezeichnet werden kann. Diese Präsentationen stießen stets auf großes Interesse und Begeisterung, wie die folgenden Zitate zeigen.

> *„Mit der Integration von Wissen im Bereich der Informationssicherheit in die Studiengänge, auch die nicht-technischen, ist die TH Wildau aus unserer Sicht führend. Darin eingeschlossen sind alle Aktivitäten der Forschungsgruppe bei der Entwicklung und Anwendung von Methoden und Werkzeugen zur Sensibilisierung und Schulung in der Informationssicherheit…Die Teilnehmenden des Treffens zeigten sich besonders beeindruckt von den umfangreichen Ergebnissen der Forschungsgruppe, wie spielebasierte analoge und digitale Lernszenarien zu aktuellen Gefährdungslagen wie Phishing, Password Hacking oder Social Engineering in den Lehrbetrieb an der TH Wildau integriert werden.“* (Dr. Alexander Eisvogel, Präsident der BAköV)

„*Der Zweiklang aus digitalen und analogen Simulationen ermöglicht einen interaktiven Ansatz, um wirkungsvolle Schutzmaßnahmen verständlich zu vermitteln.*“ (Eric Makswitat, Sprecher des Arbeitskreises „Digitale Gesellschaft“ der SPD Brandenburg)

6.3 Wissenschaftliche Konferenzen und Publikationen

Das Projekt wurde in verschiedenen Formen – als Vortrag, als Poster oder als Workshop mit einem Ausschnitt an Lernszenarien – auf nationalen und internationalen wissenschaftlichen Konferenzen vorgestellt. Auch hier war die Resonanz stets sehr positiv und es ergaben sich neue Kontakte (s. u. a. Fuhrmann et al. 2017). Die besuchten Konferenzen und die daraus entstandenen bzw. geplanten Veröffentlichungen können der folgenden Tabelle entnommen werden.

Darüber hinaus sind weitere Publikationen wie ein Beitrag in den *Wissenschaftlichen Beiträgen* der TH Wildau (Scholl et al. 2017), in der TH Info Ausgabe 01/2016 (https://www.th-wildau.de/aktuelles/presse-und-medien/hochschulmedien-und-publikationen/th-info.html) und in den Forschungsberichten 2015 und 2016 der TH Wildau (https://www.th-wildau.de/forschung/forschungsbericht.html) erschienen. Für den Forschungsbericht 2017 ist eine längere Darstellung des Projektes vorgesehen. Dieser erscheint im Frühjahr 2018.

Konferenz	Datum	Ort	Präsentation	Titel des Beitrags/Veröffentlichung
IFIP EGOV-ePart 2016	5.–8.9.16	Guimarães, Portugal	Workshop	Scholl, M., Fuhrmann, F. & Pokoyski, D. (2016a): The human factor: How can information security awareness be sustainably achieved in E-Government?, In: Scholl, H. et al. (eds): Joint Proceedings Electronic Government and Electronic Participation, 403–404.
Gemeinsame Fachtagung Verwaltungsinformatik (FTVI) und Fachtagung Rechtsinformatik (FTRI) 2016	21.–23.9.16	Dresden	Vortrag	Scholl, M. & Fuhrmann, F. (2016): Analog – digital? Wie sich mithilfe analoger Methoden Bewusstsein für Informationssicherheit in der digitalen Welt fördern lässt. In: Rätz, D. et al. (eds.): Digitale Transformation: Methoden, Kompetenzen und Technologien für die Verwaltung. Bonn: Gesellschaft für Informatik e.V., Band 261, 101–112.
CENTERIS – Conference on ENTERprise Information Systems	5.–7.10.16	Porto, Portugal	Poster-Paper	Scholl, M., Fuhrmann, F. & Pokoyski, D. (2016b): Information security awareness training 3.0 for young professionals. In: Varajão, J. E. et al. (eds.): Book of industry papers, poster papers and abstracts of the International Conference on enterprise Information Systems (CENTERIS), 433-436.
London International Conference on Education (LICE-2016)	14.–17. 11. 16	London, England	Vortrag	Fuhrmann, F., Scholl, M., Edich, D., Ehrlich, P., Leiner, K. B. & Scholl, L. R. (2016): Raising Awareness for Information Security in a Playful Way. Proceedings of London International Conference on Education LICE-2016, 190–191.
Take Aware	15.–16.3.2017	Köln	Impulsreferat	Spirale der transformativen Wechselwirkung
II CONFERENCE URBAN E-PLANNING	20–21.4.17	Lissabon, Portugal	Vortrag	Scholl, M. (2017a): IT-Security Awareness in the Field of Urban and Regional Planning; *Veröffentlichung folgt*
28. Glienicker Gespräch	11.–13.5.17	Berlin, Deutschland	Workshop	Fuhrmann, F., Koppatz, P., Edich, D. & Scholl, M. (2017): Sicher unterwegs in der digitalen Welt – spielend begreifen. Verwaltung und Management (forthcoming).
21st World Multi-Conference on SYSTEMICS, CYBERNETICS AND INFORMATICS: WMSCI 2017	8–11.7.17	Orlando, Florida, U.S.A.	Keynote und Workshop	Keynote: Scholl, M. (2017b): Living in a Digital World – Improving skills to meet the challenges of the digital transformation through authentic and game-based learning*; Veröffentlichung folgt* Vortrag und Paper: Scholl, M., Leiner, K. B. & Fuhrmann, F. (2017): Blind spot: Do you know the effectiveness of your information security awareness-raising program?, In: Proceedings Volume I of The 21st World Multi-Conference on Systemics, Cybernetics and Informatics (WMSCI 2017), 361–366.

7 Ausblick

7.1 Verstetigung des Moduls

Das in SecAware4job konzipierte (Wahlpflicht-) Modul „Sensibilisierung für Informationssicherheit“ inklusive der Übungen und spielebasierten analogen und digitalen Lernszenarien werden auf jeden Fall im Studiengang Öffentliche Verwaltung Brandenburg (ÖVBB) integriert, der seit dem Wintersemester 2016/17 an der TH Wildau angeboten wird und in dem im sechsten Semester (somit ab Sommersemester 2019) IT-Sicherheit als Wahlpflichtfach gewählt werden kann. Zudem wird das Modul nach Förderende als Wahlpflichtfach in den nicht-technischen Studiengängen angeboten. Darüber hinaus können alle Studierenden der TH Wildau ab Wintersemester 2017/2018 an der Prüfung zur/zum Informationssicherheitsbeauftragten (IT-SiBe) zu einer ermäßigten Prüfungsgebühr über das Institut WILLE von Professorin Dr. Scholl teilnehmen.

7.2 Nachhaltige Nutzung der entwickelten Lernszenarien und -methoden

Mit der Beendigung des Projektes werden die digitalen spielebasierten Lernszenarien als Creative Commons License über die SecAware4job-Webseite (http://secaware4job.wildau.biz) zur Verfügung gestellt, so dass sie kostenfrei genutzt werden können. Diese Möglichkeit der kostenfreien Nutzung soll innerhalb der Hochschule und außerhalb in Netzwerken bekannt gemacht werden.

Das in SecAware4job entwickelte Brettspiel *„Keep your data private. Everyday.“* wird auf der Social-Engineering-Konferenz „Bluff City“ am 14. September 2017 in Berlin einem breiten Publikum vorgestellt und in einem Workshop getestet. Es ist gut vorstellbar, dass daraus Anfragen für Sensibilisierungsmaßnahmen und zukünftige Kooperationen entstehen. Dies geschah bereits bei anderen öffentlichkeitswirksamen Präsentationen der Projektergebnisse. Die Interessenten kommen aus ganz unterschiedlichen Bereichen – von Schulen und Hochschulen, über öffentliche Verwaltungen, bis hin zu kleinen und großen Unternehmen.

Die in SecAware4job entwickelten analogen und digitalen Lernszenarien sowie innovativen Lehrmethoden werden auch in Fort- und Weiterbildungskursen integriert, die Professorin Dr. Scholl anbietet. Sie bereichern nicht nur diese zertifizierten Fortbildungskurse, sondern inspirieren die Teilnehmenden für ihre Arbeit. Folgendes Weiterbildungsangebot bietet Professorin Dr. Scholl zur Informationssicherheit und zum Datenschutz über ihr Institut WILLE gegen Bezahlung an (https://twz-ev.org/institute/wildau-institut-fuer-innovative-lehre-lebenslanges-lernen-und-gestaltende-evaluation/#tab-id-1):

- Seit 2010 kostenpflichtige zertifizierte Fortbildung zur/zum Informationssicherheitsbeauftragten (IT-SiBe) nach BAköV/BSI; dieser Kurs erhält seit dem öffentlichen Bekanntwerden des Projekts SecAware4job größere Aufmerksamkeit. (https://twz-ev.org/weiterbildungen/it-sicherheitsbeauftragte-i/)
- Ab Oktober 2017 kostenpflichtiger zertifizierter Fortbildungslehrgang „Datenschutzbeauftragte“ nach EU-DSGVO, in dem die entwickelten Lernszenarien ebenfalls zum Einsatz kommen werden. (https://twz-ev.org/weiterbildungen/datenschutzbeauftragte/)
- Seit Januar 2016 ist die TH Wildau, vertreten durch Professorin Dr. Scholl, akkreditiertes Prüfungszentrum der Dienstleistungsgesellschaft für Informatik mbH (DLGI) zur Abnahme von Prüfungen des ECDL und seit Februar 2017 DLGI-Prüfungszentrum für den Datenschutzführerschein; die Prüfungen werden kostenpflichtig abgenommen; Teilnehmende können Mitarbeitende der TH Wildau, interne/externe Studierende und Schülerinnen und Schüler sein. (https://www.th-wildau.de/weiterbildung/kurse-seminare/europaeischer-computerfuehrerschein.html)
- Seit 2016 kostenpflichtige Tagesschulungen zur Vertiefung für die ECDL-Prüfungen. In diesen Schulungen werden ebenfalls die in SecAware4job entwickelten Lernszenarien und -methoden eingesetzt. (https://www.th-wildau.de/weiterbildung/kurse-seminare.html)

Das Projekt SecAware4job hat somit dazu geführt, dass die in Abbildung 27 gezeigten Zertifikatsangebote für Informationssicherheit und Datenschutz/-sicherheit von Professorin Dr. Scholl systematisiert und komplementiert aufgebaut wurden und auch nachhaltig angeboten werden.

Der Bekanntheitsgrad der TH Wildau hinsichtlich innovativer Lehre zur Informationssicherheit und zum Datenschutz ist durch das Projekt SecAware4job deutlich gestiegen.

Die Fort- und Weiterbildungskurse des Instituts WILLE im Verbund mit dem Technologie- und Weiterbildungszentrum (TWZ e.V.) werden inzwischen verstärkt nachgefragt. Sowohl für die Mitarbeitenden und Studierenden der TH Wildau als auch für externe Studierende sowie Schülerinnen und Schüler konnten neue, abgestufte Qualifizierungs- und Zertifizierungsmöglichkeiten nachhaltig geschaffen werden.

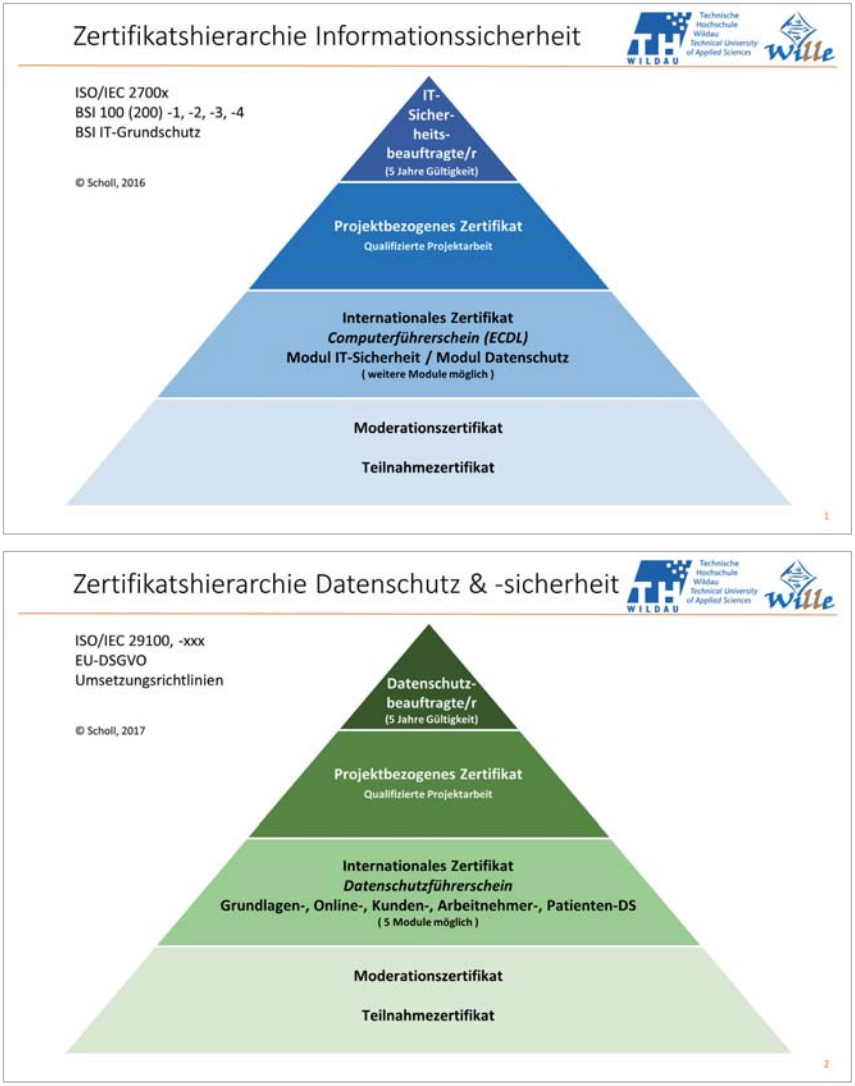


Abbildung 27: Zertifikatsangebote von Professorin Dr. Scholl

7.3 Anschließende Forschungsaktivitäten

Die Messung des Bewusstseins für Informationssicherheit und der entsprechenden Kenntnisse erfolgte in SecAware4job mittels Fragebögen zur Selbsteinschätzung (vgl.

Kapitel 5.1 und 5.4). Für eine umfassende und objektive Awareness-Messung sind Befragungen jedoch nicht ausreichend (Scholl, Leiner & Fuhrmann 2017). Seit 2016 entwickeln Professorin Dr. Scholl und Unternehmenspartner daher einen umfangreichen Antrag zur Förderung eines Projektes, das u. a. die Konzeption, Entwicklung und Erprobung einer systematischen Awareness-Messung für KMU/KKU beinhaltet. Bislang konnte allerdings mit einem solchen Großprojekt noch nicht begonnen werden, da die Zusage eines Drittmittelgebers fehlt.

Im Zuge des Projekts SecAware4job konnte auch die internationale Ausrichtung der Forschungsgruppe von Professorin Dr. Scholl gestärkt und ausgeweitet werden. Nach Abschluss des Projektes wird dazu an drei eingereichten Veröffentlichungen weiter gearbeitet (Scholl & Fuhrmann 2017a, Scholl & Fuhrmann 2017b, Scholl et al. 2018).

Die Sensibilisierung für Informationssicherheit kann nicht früh genug beginnen. Daher sollten bereits Schulkinder für einen bewussten und achtsamen Umgang mit ihren Daten und neuen technischen Möglichkeiten sensibilisiert und ausgebildet werden. Auch für diese Zielgruppe bieten sich spielebasierte Lernszenarien an, die an unterschiedliche Altersgruppen angepasst werden müssen. Eltern sowie Lehrerinnen und Lehrer sind wichtige erwachsene Bezugspersonen für Kinder. Aus diesem Grund stellen auch sie wichtige Zielgruppen bei der digitalen Bildung von Kindern dar. Sie sollten durch Fortbildungsangebote unterstützt werden, damit wiederum sie ihren Kindern bei der Entdeckung der digitalen Möglichkeiten behilflich sein können. Es ist geplant, ein Förderantrag in diesem Themenbereich einzureichen.

Nach wie vor wählen Frauen MINT-Studiengänge und MINT-Berufe zu einem deutlich geringeren Anteil als Männer. Um den Frauenanteil in diesen Disziplinen zu erhöhen, widmen sich Frau Professorin Dr. Scholl und ein Teil ihres Forschungsteam ab September 2017 dem neuen Projekt „Gendersensible Studien- und Berufsorientierung für den Beruf Security Spezialistin (Security)“. Das Ziel des Vorhabens liegt in der Weckung des Interesses von jungen Frauen (Schülerinnen) für den Beruf der Security Spezialistin. Dadurch sollen Studiengänge und Ausbildungen mit Informatikbezug für junge Frauen attraktiver werden. Den Schülerinnen soll durch eine ansprechende Darstellung des Berufsbildes der Security Spezialistin sowie durch Porträts von weiblichen Rollenvorbildern, die im Bereich Informationssicherheit tätig sind, und in einer interaktiven und erlebnisorientierten Pilotmaßnahme gezeigt werden, dass diese Studiengänge und Ausbildungen nicht nur technisch, sondern sehr vielseitig sind. Das Vorhaben wird für eine Laufzeit von zwei Jahren durch das Bundesministerium für Bildung und Forschung gefördert.

Literatur

Admiraal, W., Huizengab, J., Heemskerkc, I., Kuiperb, E., Volmanb, M. & Damb, G. t. (2014): Gender-inclusive Game-based Learning in Secondary Education. *International Journal of Inclusive Education*, 18(11), 1208–1218.

Albrechtsen, E. (2007): A Qualitative Study of Users' View on Information Security. *Computers and Security*, 26(4), 276–289.

Bundesakademie für öffentliche Verwaltung im Bundesministerium des Innern (BAköV) (Hrsg.) (2016): *Handbuch: IT-Sicherheitsbeauftragte in der öffentlichen Verwaltung. Fortbildungslehrgang der BAköV mit Zertifikat in Zusammenarbeit mit dem BSI*. 5. Auflage.

Beyer, M., Ahmed, S., Doerlemann, K., Arnell, S., Parkin, S., Sasse, M. A. & Passingham, N. (2015): *Awareness is only the first step. A framework for progressive engagement of staff in cyber security*. Hewlett Packard, Business white paper.

Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e.V. (BITKOM) (2015): *Digitale Angriffe auf jedes zweite Unternehmen*. Presseinformation vom 16. April 2015. http://www.bitkom-research.de/Presse/Wirtschaftsschutz, letzter Zugriff 8.8.2017.

Bösche, W. & Kattner, F. (2011): Fear of (Serious) Digital Games and Game-based Learning? Causes, Consequences and a Possible Countermeasure. *International Journal of Game-Based Learning*, 1(3), 1–15.

Bressler, D. & Bodzin, A. (2013): A Mixed Methods Assessment of Students' Flow Experiences During a Mobile Augmented Reality Science Game. *Journal of Computer Assisted Learning*, 29(6), 505–517.

Buffum, P. S., Boyer, K. E., Wiebe, E. N., Mott, B. W. & Lester, J. C. (2015): Mind the Gap: Improving Gender Equity in Game-Based Learning Environments with Learning Companions. *AIED: International Conferences on Artificial Intelligence in Education 2015*.

Codish, D. & Ravid, G. (2017): Gender Moderation in Gamification: Does One Size Fit All?. *Proceedings of the 50th Hawaii International Conference on System Sciences 2017*, 2006–2015.

Collins, F. (1999): The Use of Traditional Storytelling in Education to the Learning of Literacy Skills. *Early Child Development and Care*, 152(1), 77–108.

DATEV & Deutschland sicher im Netz e. V. (DsiN) (2015): *Verhaltensregeln zum*

Thema „Social Engineering“. https://www.sicher-im-netz.de/sites/default/files/download/leitfaden_social_engineering.pdf, letzter Zugriff 28.6.2017.

DSV-Gruppe, EnBW, <kes>, known_sense; nextsolutions & Pallas (Hrsg.) (2006): *Entsicherung am Arbeitsplatz – die geheime Logik der IT-Security in Unternehmen*. Köln & München.

EnBW, known_sense, pallas, SAP, Sonicwall, Steria Mummert Consulting & Trend Micro (Hrsg.) (2008): *Aus der Abwehr in den Beichtstuhl – qualitative Wirkungsanalyse*. CISO & Co. Köln.

Fang, X., Zhang, J. & Chan, S. S. (2013): Development of an Instrument for Studying Flow in Computer Game Play, *International Journal of Human-Computer Interaction*, 29(7), 456–470.

Fuhrmann, F., Scholl, M., Edich, D., Ehrlich, E., Leiner, K., & Scholl, L. (2016): Raising Awareness for Information Security in a Playful Way. *London International Conference on Education (LICE), Heathrow Windsor Marriott Hotel*, London, 190–191.

Guo, K., Yuan, Y., Archer, N. P. & Connelly, C. E. (2011): Understanding Nonmalicious Security Violations in the Workplace: A Composite Behavior Model. *Journal of Management Information Systems*, 28(2), 203–236.

Haack, B., Koppatz, P., Scholl, M., Sistenich, F., & Tippe, U. (2010): E-Learning and Further Education: How do Individual Learning Paths support Personal Learning Processes *Journal of Systemics, Cybernetics and Informatics*. 8(1), 75–79.

Helisch, M. & Pokoyski, D. (Hrsg.) (2009): *Security Awareness: Neue Wege zur erfolgreichen Mitarbeiter-Sensibilisierung*. Vieweg & Teubner: Wiesbaden.

Hsu, S. H., Wu, P. H., Huang, T. C., Jeng, Y. L. & Huang, Y. M. (2008): From Traditional to Digital: Factors to Integrate Traditional Game-based Learning into Digital Game-based Learning Environment. *Proceedings 2nd IEEE International Conference on Digital Game and Intelligent Toy Enhanced Learning, DIGITEL*, 83–89.

Huotari, K. & Hamari, J. (2017): A Definition for Gamification: Anchoring Gamification in the Service Marketing Literature. *Electronic Markets*, 27(1), 21–31.

Khan, B., Alghathbar, K. S., Nabi, S. I. & Khan, M. K. (2011): Effectiveness of information security awareness methods based on psychological theories. *African Journal of Business Management*, 5(26), 10862–10868.

known_sense, Lanxess, Technische Hochschule Wildau & <kes> (2015): *Bluff me if u can – Gefährliche Freundschaften am Arbeitsplatz*. http://www.known-sense.de/BluffMeIfUCanAuszug.pdf, letzter Zugriff am 28.6.2017.

Kruger H., Drevin, L. & Steyn T. (2007): Email Security Awareness — a Practical Assessment of Employee Behaviour. In: Futcher, L. & Dodge, R. (eds.): *Fifth World Conference on Information Security Education, IFIP — International Federation for Information Processing*, 237, Springer, Boston, MA, 33–40.

Linek, S. B. & Albert, D. (2009): Game-based Learning: Gender-specific Aspects of Parasocial Interaction and Identification. *Conference: International Technology, Education and Development Conference (INTED)*.

Lombardi, M. M. (2007): Authentic Learning for the 21st Century: An Overview. *Educause Learning Initiative – advancing learning through IT innovation, ELI Paper 1: 2007*. https://net.educause.edu/ir/library/pdf/ELI3009.pdf, letzter Zugriff 17.2.15.

Morgan, R. E. & Adamson, G. T. (1961): *Circuit Training*. 2nd edition, HarperCollins Publishers: London.

SanNicolas-Rocca, T., Schooley, B. & Spears, J. L. (2014): Designing Effective Knowledge Transfer Practices to Improve IS Security Awareness and Compliance. *47th Hawaii International Conference on System Sciences (HICSS)*, 3432–3441.

Scholl, M. & Fuhrmann, F. (2016): Analog – digital? Wie sich mithilfe analoger Methoden Bewusstsein für Informationssicherheit in der digitalen Welt fördern lässt. In: Rätz, D., Breidung, M., Lück-Schneider, D., Kaiser, S. & Schweighofer, E. (Hrsg.): *Digitale Transformation: Methoden, Kompetenzen und Technologien für die Verwaltung*. Bonn: Gesellschaft für Informatik e.V. (GI) (Lecture Notes in Informatics (LN), Band 261), 101–112.

Scholl, M., Fuhrmann, F. & Pokoyski, D. (2016a): The human factor: How can information security awareness be sustainably achieved in E-Government?. In: Scholl, H. J., Glassey, O., Janssen, M., Klievink, B., Lindgren, I., Parycek, P., Tambouris, E., Wimmer, M., Janowski, T. & Soares, D. S. (eds.): *Electronic Government and Electronic Participation*. Amsterdam: IOS Press BV (Innovation and the Public Sector), 403–404.

Scholl, M., Fuhrmann, F. & Pokoyski, D. (2016b): Information Security Awareness 3.0 for Job Beginners. In: Varajão, J. E., Cruz-Cunha, M.M., Martinho, R., Rijo, R., Bjørn-Andersen, N., Turner, R. & Alves, D. (eds.): *Conference on ENTERprise Information Systems (CENTERIS)*, 433–436.

Scholl, M., Fuhrmann, F., Edich, D., Ehrlich, P., Leiner, B., Scholl, R. & Koppatz, P. (2017): Das Projekt SecAware4job: Auf spielerischem Weg zu erhöhtem Informationssicherheitsbewusstsein für den Berufseinstieg. *Wissenschaftliche Beiträge TH Wildau*, 23–30.

Scholl, M., Leiner, K. B. & Fuhrmann, F. (2017): Blind spot: Do you know the effectiveness of your information security awareness-raising program?. *Proceedings of the 21st World Multi-Conference on Systemics, Cybernetics and Informatics (WMSCI 2017)*, 361–366.

Scholl, M. & Fuhrmann, F. (2017a submitted): Information Security Awareness in the Field of Urban and Regional Planning. Submitted to *International Journal of E-Planning Research (IJEPR)*.

Scholl, M. & Fuhrmann, F. (2017b submitted): Information Security Awareness in the Field of Urban and Regional Planning. Invited article associated to the plenary keynote address submitted to *Journal on Systemics, Cybernetics and Informatics (JSCI)*.

Scholl, M., Fuhrmann, F. & Scholl, R. (2018 submitted): Scientific knowledge of information security as a basis for sustainable trainings in organizational practices. Submitted to *Proceedings of the 51th Hawaii International Conference on System Sciences 2018*.

Silic, M. & Back, A. (2017): Impact of Gamification on User's Knowledge-Sharing Practices: Relationships between Work Motivation, Performance Expectancy and Work Engagement. *Proceedings of the 50th Hawaii International Conference on System Sciences 2017*, 1308–1317.

Straub, D. W. & Welke, R. J. (1998): Coping with Systems Risk: Security Planning Models for Management Decision Making. *MIS Quarterly*, 22(4), 441–469.

Technische Hochschule (TH) Wildau (2016): *Bericht zum Jahreswechsel 2015 | 2016. Rückblicke. Einblicke. Ausblicke*. Wildau.

Trybus, J. (2014): Game-Based Learning: What it is, Why it Works, and Where it's Going. *New Media Institute.* http://newmedia.org/game-based-learning--what-it-is-why-it-works-and-where-its-going.html, letzter Zugriff 28.6.2017.

Projektmitarbeitende

Margit C. Scholl (Prof. Dr. rer. nat.)
Professorin für Wirtschafts- und Verwaltungsinformatik an der Technischen Hochschule Wildau, Fachbereich Wirtschaft, Informatik, Recht. Sie ist verantwortlich für die Projektleitung und das Projektmanagement von SecAware4job.

Frauke Fuhrmann (Dipl.-Kffr.)
Wissenschaftliche Mitarbeiterin und operative Projektleiterin im Projekt SecAware4job.

Denis Edich (M.Sc.)
Wissenschaftlicher Mitarbeiter im Projekt SecAware4job und zuständig für digitale Anwendungen, Web-Entwicklung und Design.

Peter Koppatz
Zeitweiliger wissenschaftlicher Mitarbeiter im Projekt SecAware4job und freier Trainer und Software-Entwickler.

L. Robin Scholl
Studentischer Mitarbeiter mit Schwerpunkt Didaktik.

K. Benjamin Leiner
Studentischer Mitarbeiter mit Schwerpunkt Programmierung.

E. Peter Ehrlich (Dipl.-Wirt.-Inf. [FH])
Zeitweiliger wissenschaftlicher Mitarbeiter im Projekt SecAware4job. Labor-Ing. am FB WIR bei Prof. Dr. M. Scholl.

Anhang

zu Kapitel 4: Übersicht entwickelte Lernszenarien und innovative Lehrmethoden

zu Kapitel 4: Bilder der Kreativworkshops

zu Kapitel 4: Themenposter zu Cybercrime, Phishing, Social Engineering und Social Media

zu Kapitel 4: Visualisierte Lernkarte zu BSI-Standard 100-1/200-1

zu Kapitel 5: Modulbeschreibung „Sensibilisierung für Informationssicherheit“

zu Kapitel 5: Fragebogen und Ergebnisse der hochschulweiten Befragung

zu Kapitel 5: Fragebogen und Ergebnisse des Einstiegsfragebogens im WS 2016/17

zu Kapitel 6: Screenshots der Projektwebseite

zu Kapitel 6: Projekt-Plakate

zu Kapitel 6. Projekt-Flyer

zu Kapitel 6: Pressberichte zum Projekt

Anhang zu Kapitel 4

Übersicht entwickelte Lernszenarien und innovative Lehrmethoden

Bilder der Kreativworkshops: Erste Ideen und Teilnehmende

Themenposter zu Cybercrime

Themenposter zu Phishing

Themenposter zu Social Engineering

Themenposter zu Social Media

Visualisierung Lernkarte zu BSI-Standard 100-1/200-1

Anhang zu Kapitel 4:

Übersicht entwickelte Lernszenarien und innovative Lehrmethoden

Lernszenario	Aufgabe	Lernziel(e)
<u>Analoge spielebasierte Lernszenarien</u>		
Schutzspiel	Schutzmaßnahmen für 9 Gefahrenszenarien wählen bei begrenztem Budget	Sicherheitsmaßnahmen verstehen, verschiedene Level der Absicherung unterscheiden und bewerten können
BSI-Standard 100-2 Schadensszenarien	Zuordnung von beispielhaften Vorfällen zu Schadensszenarien des BSI-Standard 100-2, der betroffenen Grundwerte und Einbringen von Praxisbeispielen inkl. Bewertung der Folgen	Schadensszenarien nach BSI-Standard 100-2 und Beispiele für diese kennen, Wiederholung der Grundwerte sowie Diskussion und Bewertung eigener Beispiele
Fachtermini	Erklären und Erraten von Begriffen zu Informationssicherheit ohne Nennung bestimmter Begriffe	Wiederholung und Vertiefung von Informationssicherheits-Fachbegriffen
Brettspiel „Keep your data private. Everyday."	Entscheidungen im Bereich privater und arbeitsbezogener Informationssicherheit treffen	Informationssicherheitsrelevante Entscheidungssituationen, mögliche Folgen und mögliche Schutzmaßnahmen kennen
Social Engineerig Rollenspiel	Soziale Einfalltore, Social Engineering Techniken, Spleens in Verbindung mit mobilen Endgeräten als aktiv Spielende mimen oder als Beobachtende herausfinden	Kenntnis und Verinnerlichung von Sozialen Einfalltoren, der Techniken von Social Engineers, Sensibilisierung für achtsamen Umgang mit mobilen Endgeräten sowie Förderung der Beobachtungsgabe

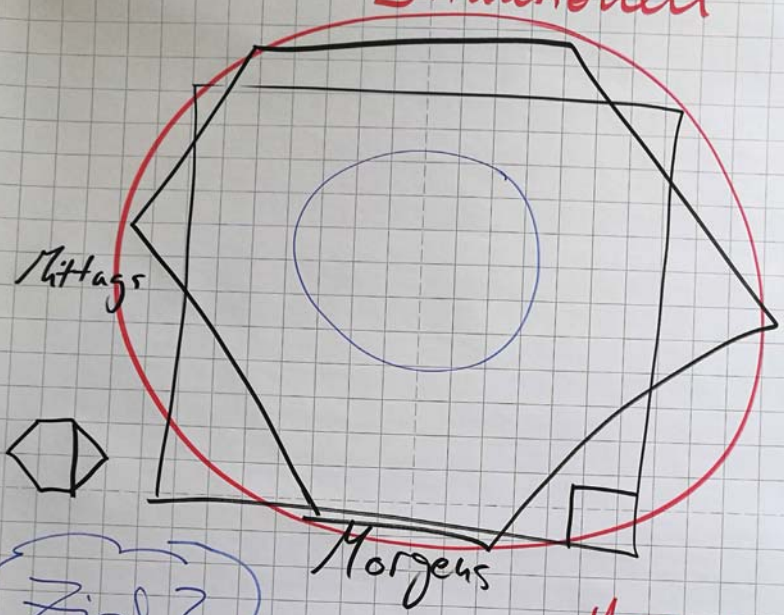
Lernszenario	Aufgabe	Lernziel(e)
Clear Desk (Englische Security-Arena)	Welche Gegenstände und Informationen sollten bei Verlassen des Schreibtisches eingeschlossen werden, welche können offen auf dem Schreibtisch liegen bleiben?	Sensibilisierung für aufgeräumten Arbeitsplatz und sicheres Verwahren sensibler Informationen
Data Security (Englische Security-Arena)	Merksätze aus jeweils zwei Teilen zusammensetzen	Wiederholung und Vertiefung der Kenntnisse
Incident Management (Englische Security-Arena)	Clusterung von Informationssicherheits-, Datenschutz- und Compliance-Vorfällen und Zuordnung zu Meldestellen	Beispielhafte Informationssicherheits-, Datenschutz- und Compliance-Vorfälle und entsprechende Meldestellen kennen
Internet Services (Englische Security-Arena)	Zuordnung von beispielhaften Anwendungen zu gegebenen Kategorien von Internetdiensten und Apps; Bewertung der beispielhaften Dienste und Apps im Hinblick auf 8 Risiken	Risiken gängiger Internet- und App-Dienste kennen und diskutieren
Password Hacking (Englische Security-Arena)	Passwörter erraten anhand fiktivem Facebook-Profil	Sensibilisierung für sichere Passwörter und Vermittlung von Kenntnissen zu Hashwerten
Phishing (Englische Security-Arena)	Phishing-E-Mails erkennen	Erkennen von Phishing-E-Mails
Security on the Go (Englische Security-Arena)	Beispielhafte Gefahrenszenarien in der Öffentlichkeit erkennen und geeignete Schutzmaßnahmen zuordnen	Gefahren und Schutzmaßnahmen für die Informationssicherheit in der Öffentlichkeit und während Reisen kennen
Social Engineering (Englische Security-Arena)	Soziale Einfalltore erkennen	Sensibilisierung für Social Engineering und Soziale Einfalltore kennen

Lernszenario	Aufgabe	Lernziel(e)
Social Media (Englische Security-Arena)	Kritische veröffentlichte Bilder und Informationen in Sozialen Netzwerken erkennen	Sensibilisierung für sicheres Verhalten in Sozialen Netzwerken
Network Domino (Englische Security-Arena, Konzeption TH Wildau)	Mit Spielelementen Netzwerk legen, welches vorgegebene Anforderungen an Sicherheit und Funktionalität erfüllt	Vertiefung der Kenntnisse über die Arbeitsweise von Netzwerkkomponenten und ihre sinnvolle sichere Anordnung
<u>Digitale spielebasierte Lernszenarien</u>		
Phishing http://secaware4job.th-wildau.de/ds/ph4/story.html	Phishing-E-Mails und deren Merkmale erkennen	Kennen von Merkmalen von Phishing-E-Mails und dadurch Erkennen von Phishing-Versuchen
Social Engineering http://secaware4job.wildau.biz/ds/se/story.html	Soziale Einfalltore (er)kennen	Sensibilisierung für Social Engineering, Wiederholung und Vertiefung der Sozialen Einfalltore
Hangman http://secaware4job.wildau.biz/ds/hangman/	Erraten eines wichtigen Begriffs aus einem Cybercrime-Gesetz des StGB (Erweiterung auf andere Themen der Informationssicherheit möglich)	Wiederholung und Vertiefung der Gesetze zu Cybercrime und von wichtigen Fachbegriffen
CBubbles (Android-App) https://play.google.com/store/apps/details?id=com.vocaword.cbubbles.demo	Beantwortung einer Frage zum Thema Informationssicherheit durch die richtige Anordnung der Buchstaben in den Blasen	Wiederholung und Vertiefung von Fachbegriffen und Kenntnissen im Bereich Informationssicherheit

Lernszenario	Aufgabe	Lernziel(e)
Storytelling https://story-telling-3d.methopedia.eu/	Anhand gewürfelter Symbole Aufschreiben einer realistischen Geschichte zum Thema Informationssicherheit unter Verwendung wichtiger Fachbegriffe	Wiederholung und Vertiefung von Informationssicherheitskenntnissen und Fachbegriffen
Clear Room (3D-Anwendung) (in der Entwicklung)	Identifikation von Gegenständen und Informationen, die bei Verlassen des Büros nicht einsehbar sein sollten; Auswahl passender Aktionen zur Verwahrung sensibler Informationen (z. B. Einschließen, Vernichten, Sperren)	Sensibilisierung für das sichere Verwahren sensibler Informationen
Security Runner http://secaware4job.wildau.biz/ds/security_runner	Gefahren und Schutzmaßnahmen der Informationssicherheit erkennen	Gefahren und Schutzmaßnahmen für Informationssicherheit kennen
Security Match http://secaware4job.wildau.biz/ds/memory_match/	Identifikation von zwei zueinander passenden Bildern des Themenbereichs Informationssicherheit	Wiederholung und Vertiefung der Kenntnissen
Innovative Lehrmethoden		
Problemorientiertes Lernen	Aktuelles Beispiel eines Sicherheitsvorfalls verstehen, einordnen, bewerten, Schwachstellen ermitteln und eigene Lernziele definieren	Aktuelle Sicherheitsvorfälle kennen und bewerten; Sensibilisierung für die Relevanz des Themas

Lernszenario	Aufgabe	Lernziel(e)
Unterrichtseinheit StGB	• Schätzen geschwärzter, lückenhafter Statistiken zum Thema Cybercrime • Bewertung und Diskussion aktueller Fälle des Cybercrimes (welche Paragraphen des StGB sind betroffen?) • Finden wichtiger Begriffe aus Cybercrime-Paragraphen des StGB in Gitterrätseln	Relevanz des Themas kennen sowie Cybercrime-Paragraphen des StGB kennen und anwenden können
Themenposter zu Cybercrime, Phishing, Social Engineering und Social Media		Relevanz der Themen einschätzen und kennen
Visualisierung komplexer Sachverhalte	BSI-Standard 100/200-1 ISMS Begriffe der Informationssicherheit und des Datenschutzes	Merkfähigkeit über bildliche Lernkarte stärken

Situationen

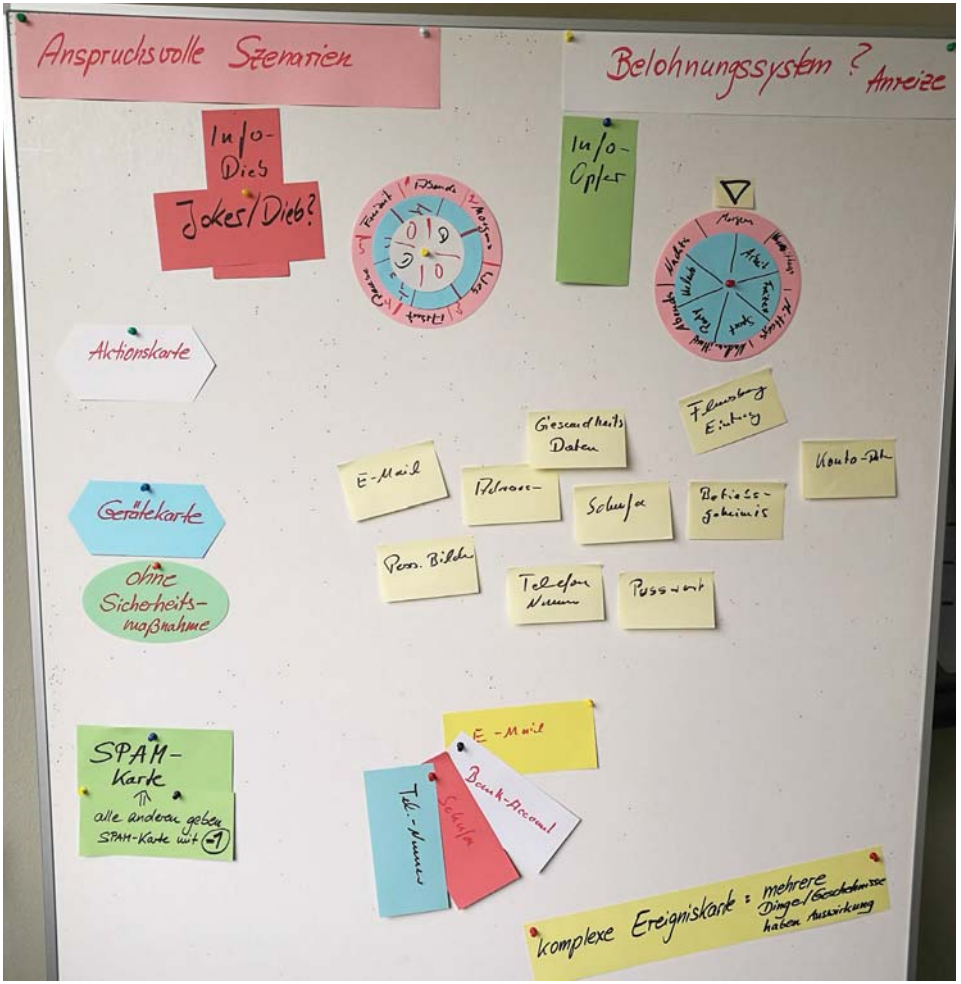


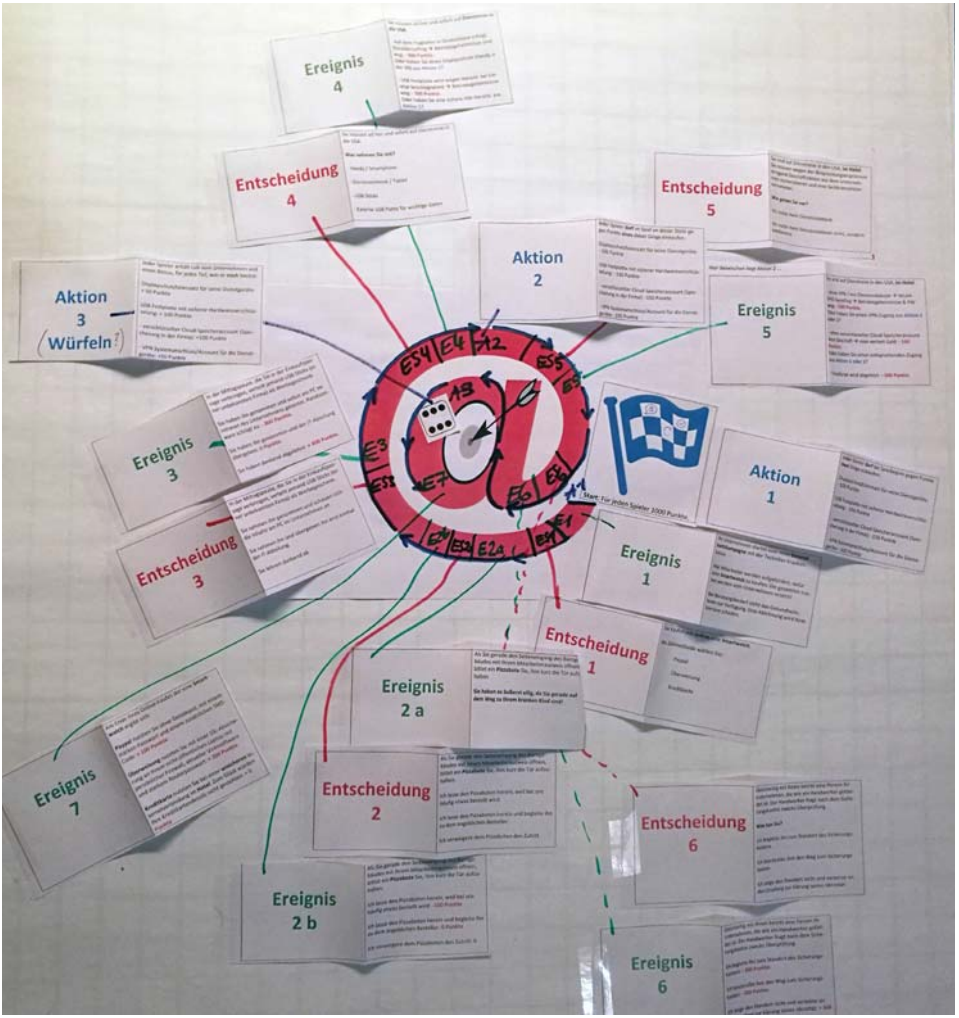
Ziel?

- am Ende soviel Infos wie möglich noch haben!

- Informationen (Person/Team)
- das / der / die } Böse
- das Opfer

- Morgens vor A.
- Mittag Nachm. Weg z. A
- auf d. A
- Mittag / Pause
- ~~Nachhauseweg~~
- nach d. A
- nachts / Abend (Freizeit)


Anspruchsvolle Szenarien
Belohnungssystem ? Anreize
Info-Dieb
Joker/Dieb?
Info-Cplr
Aktionskarte
E-Mail
Gesundheits Daten
Konto-Dat.
Gerätekarte
ohne Sicherheits-maßnahme
Pers. Bilder
Telefon Nummer
Passwort
SPAM-Karte
alle anderen geben SPAM-Karte mit -1
E-Mail
Bank-Account
Schuhe
komplexe Ereigniskarte = mehrere Dinge/Geschehnisse haben Auswirkung


Ereignis 4
Entscheidung 4
Entscheidung 5
Aktion 2
Aktion 3 (Würfeln)
Ereignis 5
Ereignis 3
Aktion 1
Entscheidung 3
Ereignis 1
Entscheidung 1
Ereignis 2 a
Ereignis 7
Entscheidung 2
Entscheidung 6
Ereignis 2 b
Ereignis 6
Start: Für jeden Spieler 1000 Punkte

Cybercrime Aware

Fakten und Zahlen

SecAware4job

Am stärksten betroffene Branchen

68%	66%	60%	58%	58%
Automobil	Chemie & Pharma	Finanzen	Gesundheit	Medien & Kultur

Quelle: Bitkom 2015

Täterkreis

Von welchem Täterkreis gingen diese Handlungen (vermutlich) in den vergangenen zwei Jahren aus?

- **60%** Ehemalige Mitarbeiterinnen und Mitarbeiter
- **16%** Konkurrierende Unternehmen
- **14%** Organisierte Kriminalität
- **13%** KundInnen und Kunden
- **12%** Privatpersonen
- **12%** Lieferanten
- **6%** Derzeitige Mitarbeiterinnen und Mitarbeiter

Quelle: Bitkom 2016

Wo werden Smartphones am häufigsten gestohlen/verloren

Vergessen in der Öffentlichkeit | Gestohlen von Zuhause oder aus dem Auto | Taschendiebstahl

Quelle: Lookout Blog 2016

Monetärer Schaden

durch Cybercrime in Deutschland

42,6 Mio	39,4 Mio	40,5 Mio
2013	2014	2015

Quelle: BKA 2015

Sicherheitsmaßnahmen in Unternehmen

- **100%** Technische IT-Sicherheit (z.B. Firewalls, Verschlüsselung)
- **87%** Organisatorische IT-Sicherheit (z.B. Richtlinien, Notfallpläne)
- **86%** Physische Sicherheit(z.B. Gebäudeschutz, Überwachung)
- **52%** Personelle Sicherheit (z.B. Schulungen, Sicherheitsüberprüfungen)
- **40%** Sicherheitszertifizierungen (z.B. ISO 27001, BSI IT-Grundschutz)

Quelle: Bitkom 2016

Smart guys say

Connected homes leave a door open to hackers…Hackers have already breached Internet-connected camera systems, smart TVs and even baby monitors.
– Molly Wood, Host and Senior Tech Correspondent at Marketplace

Database security is becoming a huge issue. People aren't aware of how vulnerable their databases are now that LANs aren't isolated anymore. But databases today aren't built to handle many security needs.
– Shlomo Kramer, Information Technology Entrepreneur and Investor

One of the hot areas right now is tracking down cyber crime and cyber terrorism.
– Daniel Hamburger, Executive Advisory Council at New Mountain Capital

Straftaten nach Art des Delikts

Anzahl der Straftaten im Bereich Cybercrime in Deutschland nach Art des Delikts im Jahre 2015:

- **23.562** Computerbetrug
- **9.629** Ausspähen, Abfangen von Daten
- **7.187** Datenfälschung, Täuschung im Rechtsverkehr
- **3.537** Datenveränderung, Computersabotage
- **1.878** Betrug mit Zugangsberechtigungen

Quelle: BKA 2015

Weiterführende Informationen

www.secupedia.info
www.bsi.bund.de
www.bitkom.org

Quellen

- Bitkom e. V. (2015): Spionage, Sabotage und Datendiebstahl – Wirtschaftsschutz im digitalen Zeitalter. Studienbericht. Berlin
- Bitkom e. V. (2016): Spezialstudie Wirtschaftsschutz. Berlin
- Bundeskriminalamt (BKA) (2015): Cybercrime: Bundeslagebild 2015. Wiesbaden
- Lookout Blog (2016): Phone Theft in America: What really happens when your phone gets grabbed. May 7, 2014, https://blog.lookout.com/blog/2014/05/07/phone-theft-in-america

Technische Hochschule Wildau Technical University of Applied Sciences

Gefördert von: HGS Hans Gustav Stiftung

Phishing Aware

Fakten und Zahlen

SecAware4job

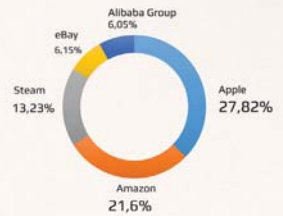
Am häufigsten betroffene Online-Dienste

Erstes Quartal 2016 (Kaspersky Lab)

28%	Globale Internetportale
23%	Banken
11%	Bezahlsysteme
9%	Soziale Netzwerke
8%	Online Shops
6%	Online Games

Betroffene Online-Shops

Erstes Quartal 2016 (Kaspersky Lab)



Betroffene Bezahlsysteme

Erstes Quartal 2016 (Telefónica)

35%	PayPal
22%	American Express
20%	MasterCard International
18%	Visa Inc.
2%	Andere

Weiterführende Informationen

- antiphishing.org
- phishme.com
- security.berkeley.edu/resources/phishing
- secware4job.wildau.biz/ds/phishing/story.html

Quellen

- de.statista.com/statistik/suche/?q=Phishing
- upload.wikimedia.org/wikipedia/commons/a/a1/Phishing.JPG
- securelist.com/analysis/quarterly-spam-reports/75764/spam-and-phishing-in-q2-2016
- Bundeskriminalamt (BKA) (2015): Cybercrime: Bundeslagebild 2015. Wiesbaden

Smart guys say

Phishing is a major problem because there really is no patch for human stupidity.
— Mike Danseglio, Manager in the Microsoft Security Solutions

The Spy Act prohibits keystroke logging, hijacking, and phishing.
— Cliff Stearns, APCO Exucutive Director

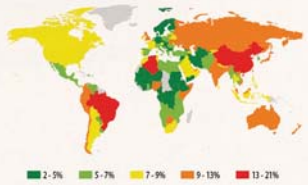
I can go into LinkedIn and search for network engineers and come up with a list of great spear-phishing targets because they usually have administrator rights over the network. Then I go onto Twitter or Facebook and trick them into doing something, and I have privileged access.
— Kevin Mitnick

Phishing im Onlinebanking

2015 (Bundeskriminalamt)

Geografische Verteilung von Phishing-Angriffen

Erstes Quartal 2016 (Kaspersky Lab)



China.....20%
Brasilien.....18%
Algerien.....14%
Großbritannien.....12%
Australien.....12%
Vietnam.....11%

Phishing-Radar: Verdächtige Mails melden

Vermuten Sie bei einer E-Mail eine Gaunerei, dann leiten Sie diese bitte an Phishing-Radar weiter. So können andere Verbraucher gewarnt werden.

phishing@verbraucherzentrale.nrw

Gefördert von:

HGS

Technische Hochschule Wildau

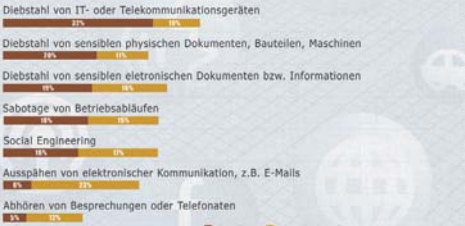
Social Engineering Aware

Fakten und Zahlen

SecAware4job

Täter haben Interesse an Geräten und Daten

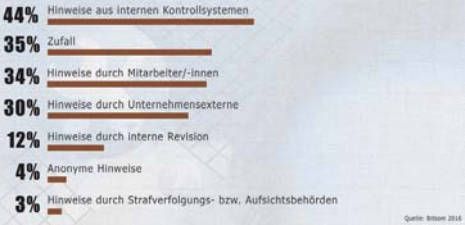
Von welchen der folgenden Handlungen war Ihr Unternehmen innerhalb der letzten zwei Jahre betroffen bzw. vermutlich betroffen?



Quelle: Hiss 2016

Aufklärung der Social Engineering Vorfälle

Wie ist Ihr Unternehmen auf Social Engineering Vorfälle aufmerksam geworden? (Merfachnennungen möglich)



Quelle: Bitkom 2016

Beliebtesten Social Engineering Techniken

SOCIAL NETWORKS
Ihr Profil und andere Daten in sozialen Netzwerken bieten Social Engineers vielfältige Angriffsmöglichkeiten!

LAUSCHANGRIFF
Lauschangriffe finden überall statt! Ob im Büro am PC, unterwegs am mobilen Endgerät oder durch Mithören eines Gesprächs!

TELEFON
Anrufer können mit falschen Angaben versuchen, an interne Informationen zu gelangen!

USB-STICK
Fremde USB-Sticks bieten Kriminellen eine Möglichkeit, Ihre Daten auszulesen oder sogar Ihren PC fernzusteuern!

INNENTÄTER
Sensible Daten dürfen selbst unter Kollegen/innen nur an autorisierte Personen weitergegeben werden!

Quelle: DATEV & DsiN 2015

CEO-Betrugsfälle in Deutschland seit 2013

Sachverhalt: Bei dieser Variante des Social Engineerings werden vorrangig Mitarbeiter/innen im Finanzwesen vorgeblich von einer real existierenden Führungskraft des eigenen Unternehmens per Telefon oder E-Mail angewiesen, eine größere Summe von einem Geschäftskonto auf ein fremdes Konto zu überweisen.

Quelle: Seibel 2016

Weiterbildungsangebote zum Thema Social Engineering

Welche der folgenden Weiterbildungsangebote zum Thema Social Engineering bietet Ihr Unternehmen seinen Mitarbeiter/innen an?

16%
Workshops, Seminare oder Schulungen

9%
Social Engineering Richtlinien für das Verhalten der Mitarbeiter/innen

3%
Simulationen zum Thema Social Engineering

69%
Andere

Quelle: Bitkom 2016

Smart guys say

A company can spend hundreds of thousands of dollars on firewalls, intrusion detection systems and encryption and other security technologies, but if an attacker can call one trusted person within the company, and that person complies, and if the attacker gets in, then all that money spent on technology is essentially wasted.

– Kevin Mitnick, ehemaliger Hacker

There is no technology today that cannot be defeated by social engineering.

– Frank Abagnale, ehemaliger Hochstapler und Scheckbetrüger

Social engineering has become about 75% of an average hacker's toolkit, and for the most successful hackers, it reaches 90% or more.

– John McAfee, Entwickler von Antiviren- und Computersicherheits-Software

Weiterführende Informationen

www.sicher-im-netz.de/downloads/verhaltensregeln-zum-social-engineering
www.bsi.bund.de
www.bitkom.org
www.allianz-fuer-cybersicherheit.de
www.known-sense.de/BluffMeIfUCanAuszug.pdf

Quellen

- Bitkom e. V. (2016): Spezialstudie Wirtschaftsschutz. Berlin
- DATEV und Deutschland sicher im Netz e. V. (DsiN) (2015): Verhaltensregeln zum Thema „Social Engineering". Spezialausgabe: Leitfaden für Mitarbeiter. Berlin.
- Holz, W. (2016): Datendiebstahl, Spionage und Sabotage in der Industrie. Bitkom e.V.
- Seibel, K. (2016): Leoni: Betrüger machen 110 Millionen mit der „Chef-Masche". welt.de/Geld. Veröffentlicht am 21.08.2016.

Technische Hochschule Wildau (Technical University of Applied Sciences)

Gefördert von: HGS

Social Media Aware

Fakten und Zahlen

SecAware4job

Aktive Nutzer/innen ausgewählter Sozialer Netzwerke weltweit (Januar 2017)

- **1.8 Mrd** Facebook
- **1 Mrd** WhatsApp
- **1 Mrd** Facebook Messenger
- **877 Mio** Twitter
- **600 Mio** Instagram
- **317 Mio** QQ
- **300 Mio** Snapchat
- **300 Mio** Skype
- **106 Mio** LinkedIn

Quelle: Smart Insights 2017

Hindernisse bei der Nutzung von Social Media in Unternehmen

- **49,7%** Datenschutz
- **28,5%** Fehlendes Know-how
- **25,6%** Mangelnde Beteiligung/Wahrnehmung der Zielgruppe
- **24,4%** Falsche Umsetzung
- **23,5%** Kontrollverlust
- **21,5%** Intern zu wenig abteilungsübergreifende Zusammenarbeit
- **21,5%** Zu wenig Ressourcen (Zeit, Budget, Personal)

Quelle: BVDW 2014

Smart guys say

Smart phones and social media expand our universe. We can connect with others or collect information easier and faster than ever. But they also expand our spectrum of attention. In this instance, too much of a good thing can become a distraction, even a false reality — sometimes at the detriment of our relationships.

– Daniel Goleman, Wissenschaftsjournalist.

What is interesting is the power and the impact of social media... So we must try to use social media in a good way.

– Malala Yousafzai, Aktivistin und Bloggerin für BBC Urdu

There are a lot of pros and cons about social media; it's just how you choose to handle it and how you have to be prepared for the negatives as well.

– Aubrey Peeples, Schauspielerin

„Top Fünf"-Gründe für den Einsatz von Social Media in Unternehmen

- **79,6%** Steigerung der Bekanntheit
- **74,3%** Besserer Zugang zur Zielgruppe
- **74,3%** Reagieren auf Probleme/ Unzufriedenheit der Kund/innen
- **74,3%** Verbesserung des Images
- **70,8%** Stärkere Kund/innenbindung

Quelle: BVDW 2014

Gefahren in Sozialen Netzwerken

Verlust der Privatsphäre
Nutzer/innen sind sich oft nicht bewusst, wie viele Leute ihre Profile tatsächlich lesen.

Sammlung von Sekundärdaten
Provider und Dienstanbieter sammeln Daten über alles, was die Internetnutzer/innen in einem sozialen Netzwerk machen.

Unfreiwillige Verlinkung
In vielen sozialen Netzwerken können die Anwender/innen ihre oder fremde Fotos mit Schlagwörter versehen und sich so weiter vernetzen.

Gesichtserkennung
Mittels moderner Gesichtserkennungsprogramme kann das Internet umfangreich nach bestimmten Personenfotos durchsucht werden.

Phishing
Bei einer Phishing-Attacke werden die User auf präparierte Webseiten gelockt, um ihnen dort beispielsweise Bankdaten zu klauen.

Spionage
Leichtgläubige Anwender/innen können Firmeninterna oder persönliche Informationen Dritter preisgeben.

Quelle: botfrei Blog 2013

Deine Checkliste für die Online-Welt

Teile keine persönlichen Informationen
Hilf deinen Kindern, sicher im Netz zu surfen

Sei immer nett
Behandle andere so, wie du behandelt werden möchtest

Deine Kinder & das Internet
Du weißt nie, wer auf der anderen Seite ist

Vorsicht beim Öffnen von Links
Klicke sie nicht direkt an

Benutze sichere Passwörter
Benutze verschiedene Passwörter und ändere sie regelmäßig

Vorsicht bei Handys und Tablets
Sie werden besonders häufig infiziert

Lerne Betrug zu erkennen
Falle nicht auf einen Gewinn herein, wenn du gar nicht gespielt hast

Benutze ein gutes Sicherheitssystem
Schütze deinen PC mit aktueller Sicherheits-software

Sei vorsichtig bei öffentlichem WLAN
Du weißt nicht, wer sich alles in einem öffentlichen Netz befindet

Quelle: Panda Security 2017

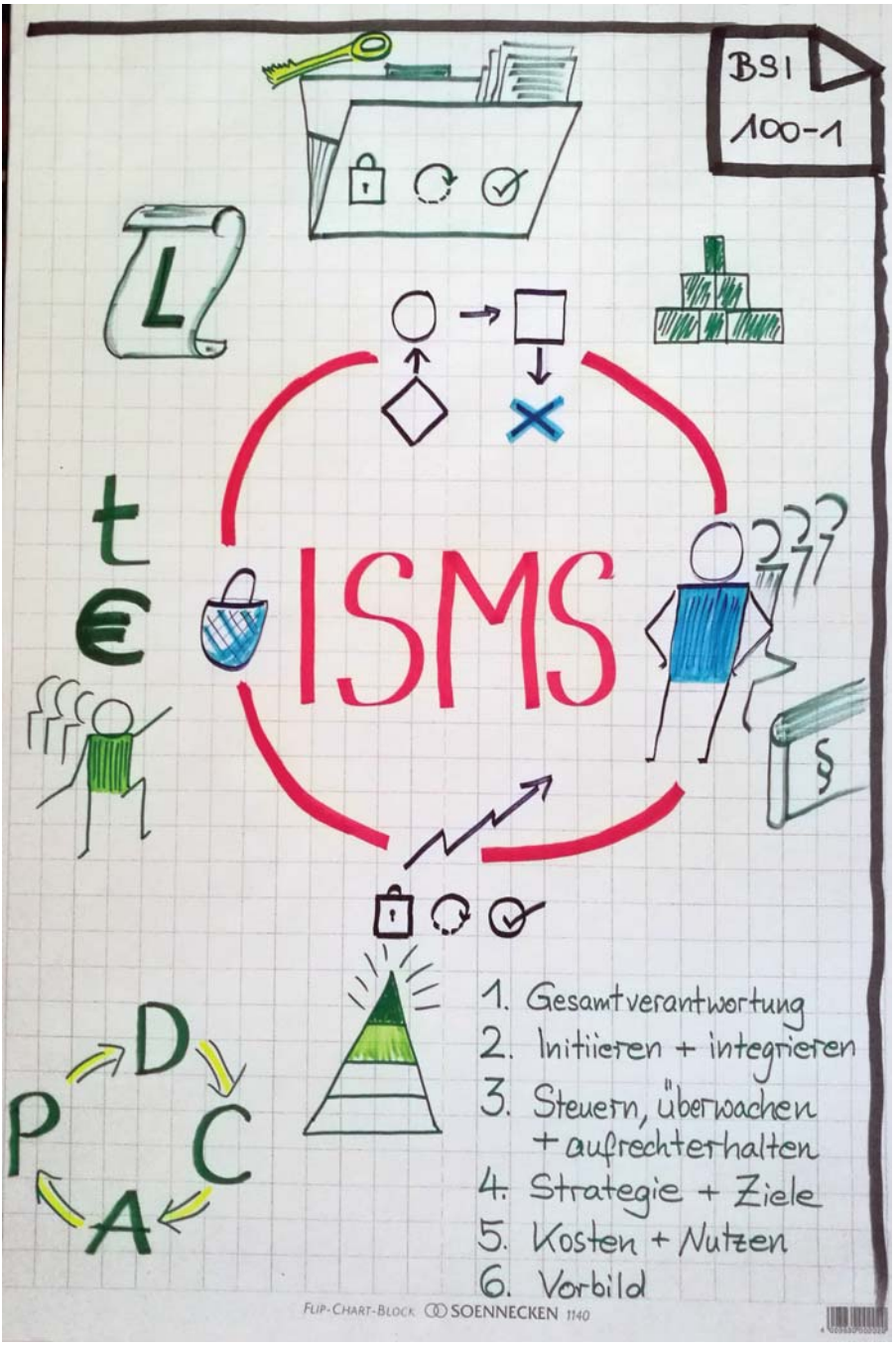
Quellen

- Smart Insights (2017): Top Social Network sites by number of active users 2017. http://www.smartinsights.com/social-media-marketing/social-media-strategy/new-global-social-media-research, letzter Zugriff 28.02.2017.
- Bundesverband Digitale Wirtschaft (BVDW) e.V. (2014): BVDW-Studie: Social Media in Unternehmen. BVDW-Studienergebnisse. Düsseldorf.
- botfrei Blog (2013): Gefahren in sozialen Netzwerken. https://blog.botfrei.de/2013/10/gefahren-in-sozialen-netzwerken, letzter Zugriff 28.02.2017.
- Panda Security (2017): International Safer Internet Day 2016. http://www.pandasecurity.com/mediacenter/security/safer-internet-day-infographic, letzter Zugriff 28.02.2017.

Gefördert von:

Technische Hochschule Wildau (Wildau Technical University of Applied Sciences)

HGS Hanse Gate Solutions


BSI
100-1
L
t
€
ISMS
§
P
D
C
A
1. Gesamtverantwortung
2. Initiieren + integrieren
3. Steuern, überwachen + aufrechterhalten
4. Strategie + Ziele
5. Kosten + Nutzen
6. Vorbild
FLIP-CHART-BLOCK © SOENNECKEN 1140

Anhang zu Kapitel 5

Modulbeschreibung „Sensibilisierung für Informationssicherheit“

Fragebogen und Ergebnisse der hochschulweiten Befragung

Fragebogen und Ergebnisse des Einstiegsfragebogens im WS 2016/17

Sensibilisierung für Informationssicherheit

Modul: Sensibilisierung für Informationssicherheit	
Studiengang: Öffentliche Verwaltung Brandenburg	**Abschluss:** Bachelor
Modulverantwortliche/r: Prof. Dr. rer. nat. Margit Scholl	

Semester: 8	**Dauer:** 1	
SWS: 3	**davon V/Ü/L/P:** 1/1/1/0	**CP nach ECTS:** 5.0
Art der Lehrveranstaltung: **Wahlpflicht**	**Sprache:** Deutsch	**Stand vom:** 2017-8-11
Pflicht Voraussetzungen: Office- und Online-Produkte nutzen können: Textverarbeitung, Präsentation, Tabellenkalkulation und Web-Recherche.		
Empfohlene Voraussetzungen: Der Europäische Computerführerschein (ECDL) ist als internationaler Standard für Digitale Kompetenz eine empfohlene Basis.		
Pauschale Anrechnung von:		
Besondere Regelungen: Es werden Lern-Teams gebildet und vielfältige Lernformen eingesetzt wie Serious Games (analog/digital), Blended Learning (BL), selbsorganisiertes Lernen (SOL), Moodle-Lernplattform mit Diskussionsforen etc. sowie Genetisches Lernen als Nachvollzug wichtiger Erkenntnisprozesse und Forschendes Lernen (FL) als aktive Teilnahme an aktuellen Forschungsaufgaben. Auch Kritisches Lernen zum Entwickeln eines Bewusstseins für die grundsätzlichen Fragen und Herausforderungen der Disziplin ist explizit erwünscht. Das WPF bietet die Möglichkeit, ein "Moderatorenzertifikat" zu erwerben, falls Teilnehmer eigenständig kreative Methoden wie Serious Games zur Sensibilisierung für Informationssicherheit entwickeln, modifizieren und im Kurs praktisch demonstrieren. Die praxisorientierte Projektarbeit des WPF soll 30 h umfassen und ist prinzipiell anrechenbar bei der Prüfung des zertifizierten Fortbildungslehrgang zum IT-Sicherheitsbeauftragten, die über das Institut WILLE an der TH Wildau angeboten wird.		

Aufschlüsselung des Workload	**Stunden:**
Präsenz:	45
Vor- und Nachbereitung:	55
Projektarbeit:	30
Prüfung:	20
Gesamt:	150.

Lernziele	**Anteil**
Fachkompetenzen	

Kenntnisse/Wissen • Informationssicherheit in Deutschland verstehen: Bedrohungen - Schwachstellen - Gefährdungen • BSI-Standards 100-1, -2, -3 und 4 sowie den IT-Grundschutz kennen. • BSI-Standards und IT-Grundschutz im Vergleich der internationalen Normfamilie ISO 2700X einordnen können. • Rechtliche Rahmenbedingungen für Informationssicherheit in Deutschland. • Sicherheitsgerechtes Verhalten in Verbindung mit Schulungs- und Sensibilisierungskonzepten. • Maßnahmen für Informationssicherheit kennen. • Verschlüsselung und elektronische Signatur. • Informationssicherheitsmanagementsystem (ISMS) und Sicherheitskonzepte • Aktuelle Themen zur Informationssicherheit (Biometrie, nPA, DE-Mail, Cloud Computing, Soziale Netze)	40 %
Fertigkeiten • Sensibilisierungsmaßnahmen initiieren und durchführen können. • Über einzelne Themen der Informationssicherheit fundiert referieren können. • Formen der modernen Zusammenarbeit in Teams praktizieren können. • BSI-Standards 100-1, -2, -3 und 4 anwenden können. • Softwaregestützt IT-Grundschutz planen können. • Maßnahmen für Informationssicherheit nachfragen und erklären können. • Verschlüsselung und elektronische Signatur verstehen und anwenden können. • Im Informationssicherheitsmanagementsystem (ISMS) mitarbeiten und Sicherheitskonzepte entwickeln können. • Rechtliche Rahmenbedingungen für Informationssicherheit in Deutschland erläutern können. • Wissenschaftliches Arbeiten im dynamischen Prozess von Forschen und Lernen sowie Reflexion anwenden können. • Als Moderator/in Serious Games zur Informationssicherheit einsetzen können.	30 %
Personale Kompetenzen	
Soziale Kompetenz • Teamfähigkeit, Verantwortung und gegenseitige Anerkennung • Aktive Teilnahme am Erkenntnisprozess lernen • Kooperations- und Kommunikationsfähigkeit • Netzwerkartige Zusammenarbeit und Empathie-Steigerung • Kritik-, Konflikt- und Kompromissfähigkeit • Interkulturelle Kompetenz, Wertschätzung und Respekt • Erwerb von Digitaler Kompetenz im Team	30 %
Selbständigkeit • Steigerung des Selbstvertrauens und des Selbstwertgefühls • Motivation, Selbstbeobachtung und Selbstdisziplin • Eigenverantwortung und Beharrlichkeit • Vorbildfunktion • Steigerung der sozio-technischen Affinität im gesellschaftlichen Umfeld	

• der Unternehmensmodernisierung • Kritisches, Genetisches und Forschendes Lernen praktizieren	

Inhalt:

1. Informationssicherheit – warum?
2. Rechtliche Rahmenbedingungen für Informationssicherheit
3. Informationssicherheitsmanagement (ISMS)
4. Sicherheitsrelevantes Verhalten
5. Maßnahmen für Informationssicherheit
6. Verschlüsselung und digitale Signatur
7. Entwurf von Sicherheitskonzepten, insbesondere nach IT-Grundschutz (BSI)
8. Aktuelle Themen zur Informationssicherheit

Prüfungsform:

Praxisrelevante Projektarbeit auf dem Gebiet der Informationssicherheit
Zusätzliche Regelungen: Verteidigung der Projektarbeit durch Vortrag mit Präsentation.

Pflichtliteratur:

(1990). *Bundesdatenschutzgesetz (BDSG)*. http://www.gesetze-im-internet.de/bdsg_1990/.
(2013). *E-Government-Gesetz (E-GovG)*. http://www.bmi.bund.de/DE/Themen/IT-Netzpolit.
(2015). *IT-Sicherheitsgesetz Deutschland*. http://www.bmi.bund.de/SharedDocs/Pressemitte.
Bundesakademie für öffentliche Verwaltung im Bundesministerium des Innern (BAköV) (Hrsg.) (2016): *Handbuch: IT-Sicherheitsbeauftragte in der öffentlichen Verwaltung. Fortbildungslehrgang der BAköV mit Zertifikat in Zusammenarbeit mit dem BSI.* 5. Auflage.
Datenschutzgesetz Brandenburg http://bravors.brandenburg.de/gesetze/bbgdsg_2015, Zugriff: 12.8.2015
Digitale Verwaltung 2020, Deutsche Verwaltung innovativ http://www.verwaltunginnovativ.de/DE/Startseite/startseite_node.html, Zugriff:12.8.2015
GGO Brandenburg http://bravors.brandenburg.de/de/verwaltungsvorschriften-219623, Zugriff: 12.8.2015
IT-Standardisierungsrichtlinie Brandenburg http://bravors.brandenburg.de/de/verwaltungsvorschriften-220943, Zugriff: 12.8.2015

Empfohlene Literatur:

Brandenburg Schnellsuche http://bravors.brandenburg.de/de/vorschriften Schnellsuche, Zugriff: 12.8.2015

Begrüßungsseite

Liebe Studierende der TH Wildau,

im Rahmen des Projektes „SecAware4job: Informationssicherheitsbewusstsein für den Berufseinstieg“ führen wir eine hochschulweite **anonyme** Befragung zur Nutzung von neuen Technologien und zum Umgang mit persönlichen Daten durch.

Wir möchten Sie daher bitten, diesen Fragebogen auszufüllen. Dies dauert ca. 15 Minuten.

Bitte antworten Sie möglichst spontan. Es gibt keine richtigen oder falschen Antworten. Uns interessiert allein Ihre ganz persönliche Meinung und zwar **anonymisiert**. Bitte denken Sie bei der Beantwortung der Fragen jeweils an Ihren privaten Gebrauch von digitalen Geräten und Internet-Dienstleistungen.

Wichtig für die Untersuchung ist, dass Sie alle Fragen beantworten. Sollte es Ihnen einmal schwer fallen, wählen Sie bitte die Antwort, die am ehesten zutrifft. Bei manchen Fragen kann der Eindruck entstehen, dass sie sich wiederholen. Lassen Sie sich hiervon bitte nicht irritieren.

Ihre Antworten werden selbstverständlich vertraulich und anonym behandelt. Die erhobenen Daten können nicht einzelnen Studierenden zugeordnet werden.

Als Dankeschön können Sie an einer Verlosung von 3 Gutscheinkarten Ihrer Wahl (z. B. dm, Ikea, Media Markt) im Wert von jeweils 20 € teilnehmen. Falls Sie an dieser Verlosung teilnehmen möchten, werden Sie am Ende der Befragung durch Klick auf einen entsprechenden Link zu einer anderen Webseite weitergeleitet und können hier Ihre E-Mail-Adresse für die Teilnahme an der Verlosung angeben. Diese wird getrennt von den Antworten der Befragung gespeichert, sodass Ihre Antworten anonym bleiben und keinerlei Verbindung zwischen der angegebenen E-Mail-Adresse zur Teilnahme am Gewinnspiel und den Antworten besteht.

Für Ihre Unterstützung bedanken wir uns recht herzlich!

Für Rückfragen können Sie sich gerne an die operative Projektleiterin, Frauke Fuhrmann (frauke.fuhrmann@th-wildau.de), wenden. Informationen zu dem Projekt finden Sie unter secaware4job.wildau.biz

Mit besten Grüßen

Prof. Dr. Margit Scholl und ihr Projektteam

Fragebogen:

Zu Beginn möchten wir Sie bitten, wenige **Angaben zu Ihrer Person** zu machen.

1. Welches **Geschlecht** haben Sie?	O männlich	O weiblich

2. Wie **alt** sind Sie?	_____

3. Was **studieren** Sie?

Auswahlmenü:

- Fachbereich Wirtschaft, Informatik, Recht
  - Bachelor:
    - Betriebswirtschaft
    - Betriebswirtschaft berufsbegleitend

        - Europäisches Management
        - Kommunales Verwaltungsmanagement und Recht
        - Öffentliche Verwaltung Brandenburg
        - Verwaltung und Recht
        - Wirtschaftsinformatik
        - Wirtschaft und Recht
    - Master
        - Business Management
        - Europäisches Management
        - Master of Business Administration (MBA) - durchgeführt vom Wildau Institute of Technology (WIT)
        - Wirtschaftsinformatik
        - Wirtschaft und Recht
- Fachbereich Ingenieur und Naturwissenschaften
    - Bachelor:
        - Automatisierungstechnik (inkl. duales Studiensystem)
        - Biosystemtechnik / Bioinformatik
        - Ingenieurwesen (inkl. duales Studiensystem)
        - Maschinenbau
        - Physikalische Technik
        - Logistik
        - Luftfahrttechnik / Luftfahrtlogistik
        - Telematik
        - Verkehrssystemtechnik (inkl. duales Studiensystem)
        - Wirtschaftsingenieurwesen (inkl. duales Studiensystem)
    - Master:
        - Aviation Management (berufsbegleitend, weiterbildend)
        - Biosystemtechnik / Bioinformatik
        - Maschinenbau
        - Luftfahrttechnik / Luftfahrtlogistik
        - Photonics
        - Technisches Management und Logistik
        - Telematik

4. In welchem **(Fach-) Semester** sind Sie?	_____

5. Inwieweit stimmen Sie den folgenden Aussagen zu?

	Stimme zu 5	4	3	2	Stimme nicht zu 1
Ich versuche Situationen mit Risiko zu meiden.	○	○	○	○	○
Ich bin im Allgemeinen vorsichtig, wenn ich etwas Neues ausprobiere.	○	○	○	○	○
Ich mag es nicht, nicht zu wissen, was passieren wird.	○	○	○	○	○
Ich würde mich eher als risikoscheu bezeichnen.	○	○	○	○	○
Ich gehe regelmäßig Risiken ein.	○	○	○	○	○
Ich bin eher mutig und furchtlos in meinen Handlungen.	○	○	○	○	○
Ich betrachte Risiken normalerweise als Herausforderung.	○	○	○	○	○

Nun möchten wir gerne etwas über Ihr **Nutzungsverhalten** von **elektronischen Geräten** und **Internet-Dienstleistungen** erfahren.

6. Bitte geben Sie an, wie häufig Sie folgende **Geräte** nutzen.

	täglich	Mind. 1x pro Woche	Mind. 1x im Monat	Seltener als 1x pro Monat	nie
Desktop-Computer	□	□	□	□	□
Laptop	□	□	□	□	□
Smartphone	□	□	□	□	□
Tablet	□	□	□	□	□

7. Bitte geben Sie an, wie häufig Sie folgende **Internet-Dienste** nutzen.

	täglich	Mind. 1x pro Woche	Mind. 1x im Monat	Seltener als 1x pro Monat	nie
WWW (Surfen)	□	□	□	□	□
WLAN	□	□	□	□	□
E-Mail	□	□	□	□	□
Soziale Netzwerke	□	□	□	□	□
Online Banking	□	□	□	□	□
Online Shopping	□	□	□	□	□
Cloudspeicher	□	□	□	□	□

Im Folgenden möchten wir gerne etwas über Ihr Verhalten in Sozialen Netzwerken erfahren.

8. Sind Sie Mitglied in einem sozialen Netzwerk?
- □ Ja und zwar (Mehrfachnennungen möglich)
  - □ Facebook
  - □ Twitter
  - □ Xing
  - □ Linkedin
  - □ Instagram
  - □ Google+
  - □ Sonstige
- □ Nein

9. Welche Informationen teilen Sie in Sozialen Netzwerken? (Mehrfachnennungen möglich)
(Frage wird nur angezeigt, wenn Befragter Mitglied in einem Sozialen Netzwerk ist)

- ☐ Meinen Namen
- ☐ Mein Geburtsdatum
- ☐ Meinen Wohnort
- ☐ Meine Hochschule
- ☐ Meinen Arbeitgeber
- ☐ Aktuellen Aufenthaltsort
- ☐ Urlaubsfotos
- ☐ Fotos meiner Freizeitaktivitäten (z. B. Treffen mit Freunden, Partys)
- ☐ Links zu z. B. Videos
- ☐ Meine Meinung über aktuelle Ereignisse
- ☐ Keine der genannten Daten
- ☐ Sonstiges:_____

10. Wann haben Sie zuletzt Ihre Privatsphäre-Einstellungen in folgenden Sozialen Netzwerken überprüft? *(Anmerkung: Hier werden nur die Sozialen Netzwerke angezeigt, in denen der Befragte Mitglied ist)*

	vor ca. 1 Monat	vor ca. 1 halben Jahr	vor ca. 1 Jahr	länger als vor 1 Jahr	noch nie
Facebook	☐	☐	☐	☐	☐
Twitter	☐	☐	☐	☐	☐
Xing	☐	☐	☐	☐	☐
Linkedin	☐	☐	☐	☐	☐
Instagram	☐	☐	☐	☐	☐
Google+	☐	☐	☐	☐	☐

Als nächstes möchten wir gerne von Ihnen wissen, inwieweit Sie **Passwörter** nutzen.

11. Wie häufig wechseln Sie die Passwörter für folgende Geräte?
(Anmerkung: Es tauchen nur die Geräte auf, die der Befragte nutzt)

	Jeden Monat	Jedes halbe Jahr	Jedes Jahr	Seltener als jedes Jahr	nie	Ich nutze kein Passwort für dieses Gerät
Desktop-Computer	☐	☐	☐	☐	☐	☐
Laptop	☐	☐	☐	☐	☐	☐
Smartphone/ Handy	☐	☐	☐	☐	☐	☐
Tablet	☐	☐	☐	☐	☐	☐

12. Wie häufig wechseln Sie die Passwörter für folgende Dienste?
(Anmerkung: Es tauchen nur die Dienste auf, für die am Anfang des Fragebogens angegeben wurde, dass sie genutzt werden)

	Jeden Monat	Jedes halbe Jahr	Jedes Jahr	Seltener als jedes Jahr	nie	Ich nutze kein Passwort für diesen Dienst
WWW (Surfen)	☐	☐	☐	☐	☐	☐
WLAN	☐	☐	☐	☐	☐	☐
E-Mail	☐	☐	☐	☐	☐	☐
Soziale Netzwerke	☐	☐	☐	☐	☐	☐
Online Banking	☐	☐	☐	☐	☐	☐
Online Shopping	☐	☐	☐	☐	☐	☐
Cloudspeicher	☐	☐	☐	☐	☐	☐

13. Für wie viele Geräte und/oder Dienste nutzen Sie dasselbe Passwort?
- ☐ Ich nutze für jedes Gerät/Dienst ein anderes Passwort.
- ☐ Für 3 und weniger Geräte/Dienste.
- ☐ Für 4–6 Geräte/Dienste.
- ☐ Für 7–9 Geräte/Dienste.
- ☐ Für 10 und mehr Geräte/Dienste.

14. Aus welchen Bestandteilen bestehen Ihre Passwörter in der Regel?
(Mehrfachnennungen möglich)

- ☐ Kleinbuchstaben
- ☐ Großbuchstaben
- ☐ Zahlen
- ☐ Sonderzeichen
- ☐ Muster
- ☐ Sonstiges

15. Wie viele Zeichen umfassen Ihre Passwörter in der Regel?
- ☐ 3 Zeichen und weniger
- ☐ 4–6 Zeichen
- ☐ 7–9 Zeichen
- ☐ 10 Zeichen und mehr

16. Enthalten Ihre Passwörter in der Regel… (Mehrfachnennungen möglich)
- ☐ …Ihren Namen?
- ☐ …ganze Wörter?
- ☐ …Zeichenfolgen, die mit Ihnen in Verbindung gebracht werden können (z. B. Geburtsdatum, KFZ-Kennzeichen)?
- ☐ Meine Passwörter enthalten keine dieser Angaben.

17. Wo haben Sie Passwörter notiert/gespeichert? (Mehrfachnennungen möglich)
- ☐ am Computer, Bildschirm oder an/unter der Tastatur geheftet/geklebt
- ☐ im Portemonnaie
- ☐ unverschlüsselt auf dem Computer, Handy, Smartphone etc. gespeichert
- ☐ im Kalender
- ☐ in einem Passwortsafe (z. B. xpass, keepass)
- ☐ Nirgendwo
- ☐ Sonstiges:_____

18. Wer kennt eines oder mehrere Ihrer Passwörter? (Mehrfachnennungen möglich)
- ☐ Mein Partner/meine Partnerin
- ☐ Ein Freund/eine Freundin
- ☐ Meine Eltern
- ☐ Meine Geschwister
- ☐ Ein Kollege/eine Kollegin
- ☐ Niemand außer mir
- ☐ Sonstige: :_____

Im Folgenden möchten wir gerne erfahren, inwieweit Sie neben Passwörtern weitere **Schutz-Maßnahmen** durchführen.

19. Nutzen Sie für den Zugriff auf das Internet ein Benutzerkonto mit eingeschränkten Rechten (z. B. keine Admin-Rechte; keine Rechte zur Installation von Software oder zur Öffnung bestimmter Internetseiten)?
- ☐ Ja.
- ☐ Nein.
- ☐ Ich weiß es nicht.

20. Installieren Sie regelmäßig von den jeweiligen Herstellern bereitgestellte (Sicherheits-) Updates und/oder Patches für Ihr Betriebssystem und die von Ihnen installierten Programme (zum Beispiel Internet-Browser, Office, Flash Player, Adobe Reader)?
- ☐ Ja.
- ☐ Nein.
- ☐ Das ist ganz unterschiedlich.
- ☐ Ich weiß es nicht.

21. Wie verhalten Sie sich, wenn Sie einen Link oder einen Dateianhang per E-Mail erhalten? (Mehrfachnennungen möglich)
- ☐ In der Regel schaue ich mir den Link oder die Datei sofort an.
- ☐ In der Regel prüfe ich sehr genau, von wem die E-Mail kommt und ob der Absender vertrauenswürdig ist, bevor ich einen Link oder eine Datei öffne.
- ☐ Ich öffne nur Links und Dateien, die ich erwartet habe.
- ☐ Das ist ganz unterschiedlich.
- ☐ Keine Angabe
- ☐ Sonstiges: _____

22. Von welchen Seiten laden Sie Software herunter? (Mehrfachnennungen möglich)

- ☐ Nur von der Webseite des jeweiligen Herstellers.
- ☐ Von dem Link, der mir bei Google als erster Treffer angezeigt wird.
- ☐ Von einem Downloadportal (z. B. www.Chip.de, www.Heise.de)
- ☐ Das ist ganz unterschiedlich.
- ☐ Keine Angabe.
- ☐ Ich lade nur von folgender/n Webseite/n Software herunter: _____

23. Auf welchen der folgenden Geräte haben Sie ein Virenschutzprogramm installiert? *(Anmerkung: Es werden nur die Geräte aufgeführt, die oben als genutzt angekreuzt wurden)*

	Ja	Unsicher	Nein
Desktop-Computer	☐	☐	☐
Laptop	☐	☐	☐
Smartphone / Handy	☐	☐	☐
Tablet	☐	☐	☐

24. Auf welchen der folgenden Geräte haben Sie eine persönliche Firewall-Software aktiviert? *(Anmerkung: Es werden im Folgenden nur die Geräte aufgeführt, die oben als genutzt angekreuzt wurden)*

	Ja	Unsicher	Nein
Desktop-Computer	☐	☐	☐
Laptop	☐	☐	☐
Smartphone / Handy	☐	☐	☐
Tablet	☐	☐	☐

25. Wie häufig überprüfen Sie den Sicherheitsstatus Ihres Computers, z. B. mittels kompletten Systemscan?

- ☐ 1 x pro Monat
- ☐ 1x pro halbem Jahr
- ☐ 1x pro Jahr
- ☐ Seltener als 1x pro Jahr
- ☐ nie
- ☐ Ich weiß es nicht.

26. Wie häufig erstellen Sie Sicherheitskopien (Backups) von den Daten der folgenden Geräte? *(Anmerkungen: Es werden nur die Geräte aufgeführt, die vorher als genutzt angegeben wurden)*

	Jede Woche	Jeden Monat	Jedes halbe Jahr	Jedes Jahr	nie
Desktop-Computer	☐	☐	☐	☐	☐
Laptop					
Smartphone/ Handy	☐	☐	☐	☐	☐
Tablet	☐	☐	☐	☐	☐

Mit den folgenden Fragen möchten wir gerne herausfinden, inwieweit Ihnen die folgenden **Begriffe bekannt** sind. Sind Ihnen die Begriffe nicht bekannt, kreuzen Sie ruhig an, dass Sie es nicht wissen. Dies ist sehr hilfreich für uns.

27. Woran erkennen Sie, dass eine Internetseite Daten verschlüsselt?
    - Man muss sich mit einem Kennwort anmelden.
    - http://
    - https://
    - Ich weiß es nicht.

28. Wissen Sie, was man unter Cookies versteht?
    - Cookies speichern nutzerspezifische Informationen über besuchte Webseiten lokal ab.
    - Cookies sind ein Programm zur Verwaltung von Lesezeichen im Browser.
    - Cookies sind ein als lustiges Gimmick (Zugabe) getarntes Schadprogramm.
    - Ich weiß es nicht.

29. Was ist Phishing?
    - Wahlloses Verschicken von Werbe-E-Mails
    - Erlangen von Daten (z. B. Kontonummer, TANs) über z. B. gefälschte Links
    - Erraten von Passwörtern
    - Ich weiß es nicht.

30. Was versteht man unter einer Qualifizierten Digitalen Signatur?
    - Verschlüsselung des Hashwerts eines Dokumentes.
    - Elektronische Unterschrift, die unter eine E-Mail kopiert wird.
    - Gescannte Unterschrift, die anstelle einer persönlichen Unterschrift verwendet wird.
    - Ich weiß es nicht.

31. Was versteht man unter Hacking?
    - Verwenden eines fremden Accounts in sozialen Netzwerken
    - Zerlegen einer Datei in mehrere kleinere Dateien
    - Sicherheitslücken von Computern suchen und nutzen
    - Ich weiß es nicht.

32. Was versteht man unter Social Engineering?
    - Eine Form der Manipulation, bei der ein Unbefugter unter Vortäuschung falscher Tatsachen versucht, unberechtigten Zugang zu Informationen.
    - Verbesserung sozialer Netzwerke mithilfe gesammelter Nutzerdaten durch den Betreiber.
    - Gemeinsames Arbeiten in einem Projekt.
    - Ich weiß es nicht.

33. Was ist der Unterschied zwischen einem Virus und einem Wurm?
    - Ein Virus verbreitet sich selbstständig über das Internet.
    - Ein Wurm verbreitet sich selbstständig über das Internet.
    - Es gibt keinen Unterschied.
    - Ich weiß es nicht.

34. Wissen Sie, was Spyware ist?
- Programm, das es einem anderen Nutzer erlaubt, ein fremdes System zu kontrollieren.
- Programm, das sich selbstständig weiterverbreitet und in andere Programme einschleust.
- Programm, das Informationen über die Tätigkeiten des Nutzers sammelt und an Dritte weiterleitet.
- Ich weiß es nicht.

35. Wissen Sie, was unter Pharming zu verstehen ist?
- Verkauf von Medikamenten übers Internet.
- Methode, um den Nutzer auf gefälschte Webseiten zu leiten.
- Sammeln von Daten durch Webseitenbetreiber.
- Ich weiß es nicht.

36. Wenn sichergestellt ist, dass Informationen von der angegebenen Quelle erstellt wurden, spricht man von…

- …Vertraulichkeit.
- …Authentizität.
- …Identifizierbarkeit.
- Ich weiß es nicht.

37. Wenn der Begriff Integrität auf "Daten" angewendet wird, drückt er aus, dass…
- …Daten seriös sind.
- …Daten konsistent sind.
- …Daten vollständig und unverändert sind.
- Ich weiß es nicht.

38. Die Verfügbarkeit von Informationen ist vorhanden, wenn sie…
- …für jeden Internetnutzer zugänglich sind.
- …von den Anwendern wie vorgesehen genutzt werden können.
- …ohne Hindernisse abgerufen werden können.
- Ich weiß es nicht.

39. Wenn Daten lediglich von autorisierten Benutzern gelesen bzw. modifiziert werden dürfen, spricht man von...
- …Verschlüsselung.
- …Integrität.
- …Vertraulichkeit.
- Ich weiß es nicht

Zum Abschluss möchten wir Sie gerne zu Ihren **persönlichen Erfahrungen und Einschätzungen** im Umgang mit neuen Technologien und Anwendungen befragen.

40.	ja	nein	keine Angabe
Haben Sie es schon einmal bereut, etwas in einem sozialen Netzwerk geteilt zu haben?	☐	☐	☐
Hatten Sie in den vergangenen zwei Jahren Probleme aufgrund eines Virus auf Ihrem Computer, Laptop, Smartphone etc.?	☐	☐	☐
Hatten Sie in den vergangenen zwei Jahren Spyware auf Ihrem Computer, Laptop, Smartphone etc. (Programme, die Informationen über die Tätigkeiten des Benutzers sammeln und an Dritte weiterleiten)?	☐	☐	☐
Wurde über Sie schon einmal etwas Falsches oder Beleidigendes im Internet verbreitet?	☐	☐	☐
Wurden von Ihnen schon einmal peinliche oder beleidigende Videos, ohne Ihr Wissen, online gestellt?	☐	☐	☐
Hatten Sie schon einmal das Gefühl, dass Sie im Internet (z. B. in Communities, Sozialen Netzwerken, Chats) oder über das Handy beleidigt, gemobbt wurden oder man sich über Sie lustig gemacht hat?	☐	☐	☐
Wurde eine/r Ihrer Freunde/Freundinnen bereits einmal im Internet oder über das Handy beleidigt oder gemobbt?	☐	☐	☐

41. Inwieweit stimmen Sie den folgenden Aussagen zu?	Stimme zu				Stimme nicht zu
	5	4	3	2	1
Ich verwende sichere Passwörter.	○	○	○	○	○
Ich schütze meine Daten sehr gut.	○	○	○	○	○
Ich weiß gut Bescheid, wie ich meine Daten schütze.	○	○	○	○	○
Ich kenne mich gut aus, was den Schutz von vertraulichen Informationen betrifft.	○	○	○	○	○
Ich habe Erfahrung auf dem Gebiet der Informationssicherheit.	○	○	○	○	○

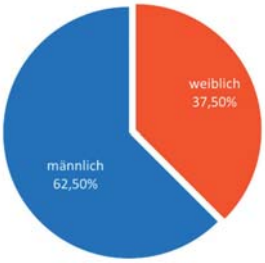
Herzlichen Dank für Ihre Teilnahme!

Wenn Sie an der Verlosung von 3 Gutscheinkarten Ihrer Wahl (z. B. dm, Ikea, Media Markt) im Wert von jeweils 20 € teilnehmen möchten, klicken Sie bitte auf den folgenden Link. Sie werden dann auf eine neue Webseite weitergeleitet, auf der Sie Ihre E-Mail-Adresse für die Teilnahme an der Verlosung angeben können. Durch die Weiterleitung auf eine andere Webseite können Ihre Antworten nicht mit Ihrer E-Mail-Adresse in Verbindung gebracht werden, sodass Ihre Antworten anonym bleiben.

Ausgewählte Ergebnisse der hochschulweiten Befragung zu Informationssicherheitsbewusstsein und -kenntnisse an der TH Wildau

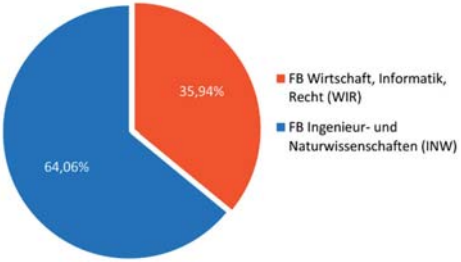
128 Teilnehmer

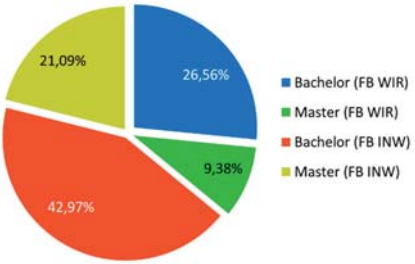
Frage 1: Geschlecht der Teilnehmenden



→ Anteil der weiblichen und männlichen Befragten entspricht den Anteilen weiblicher und männlicher Studierender an der TH Wildau (36,7 % Frauen und 63,3 % Männer).

Frage 3: Studienfächer der Teilnehmenden

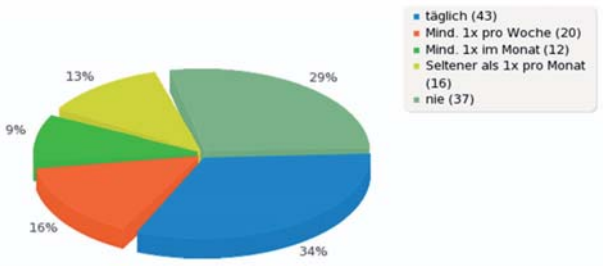




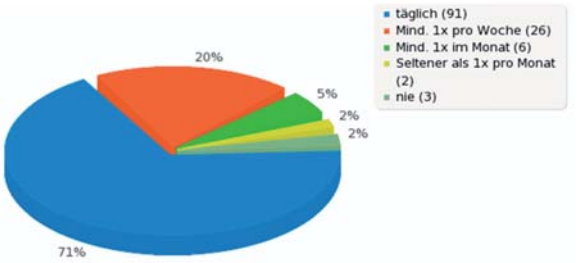
→ Größeres Interesse der Studierenden des Fachbereichs Ingenieur- und Naturwissenschaften (INW). Die Studierenden der TH Wildau verteilen sich über die Fachbereiche wie folgt: 52,05 % FB INW und 47,95 % FB WIR

Frage 6: Nutzung technischer Geräte

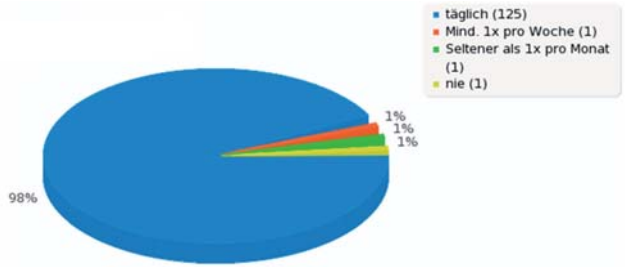
Desktop-Computer



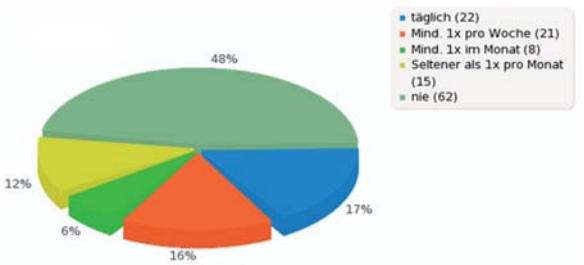
Laptop



Smartphone / Handy

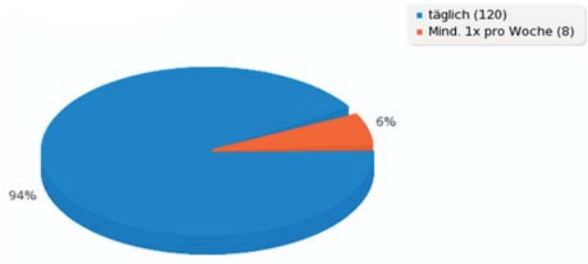


Tablet

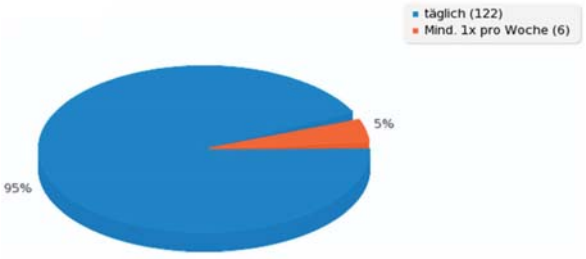


Frage 7: Nutzung Internet-Dienste

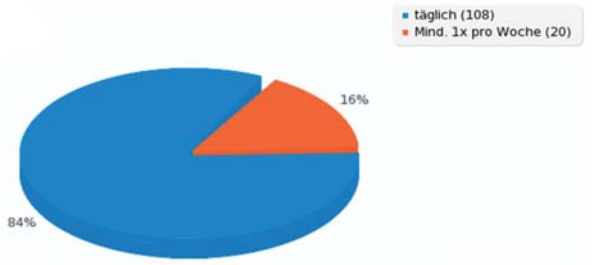
WWW (Surfen)



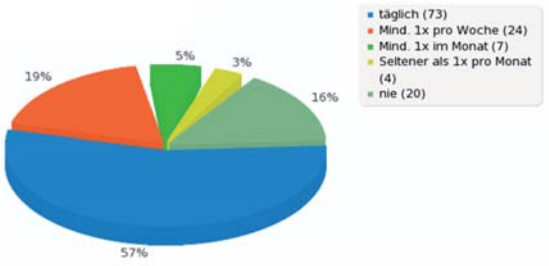
WLAN



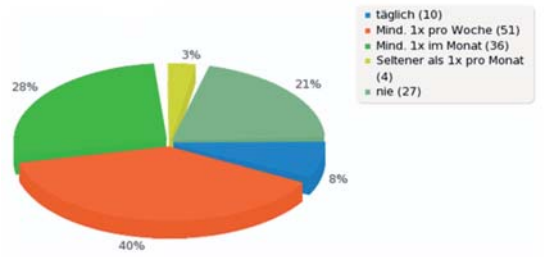
E-Mail



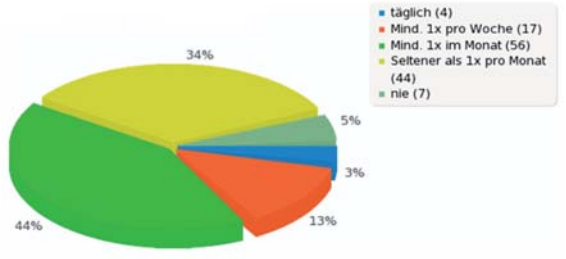
Soziale Netzwerke



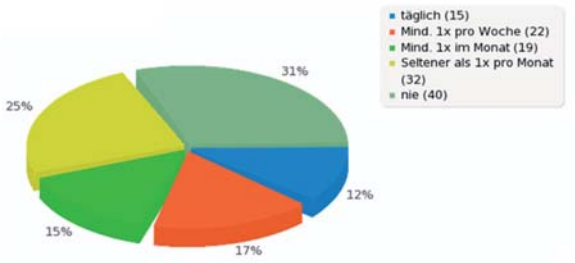
Online-Banking



Online-Shopping

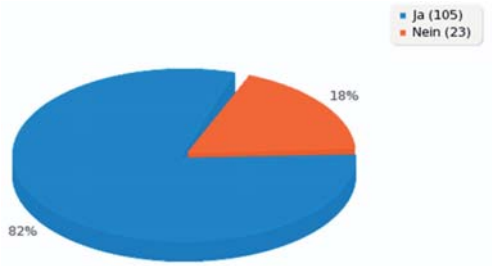


Cloudspeicher

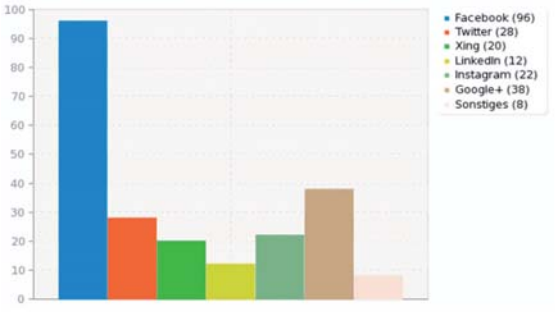


Fragen 8–10: Soziale Netzwerke

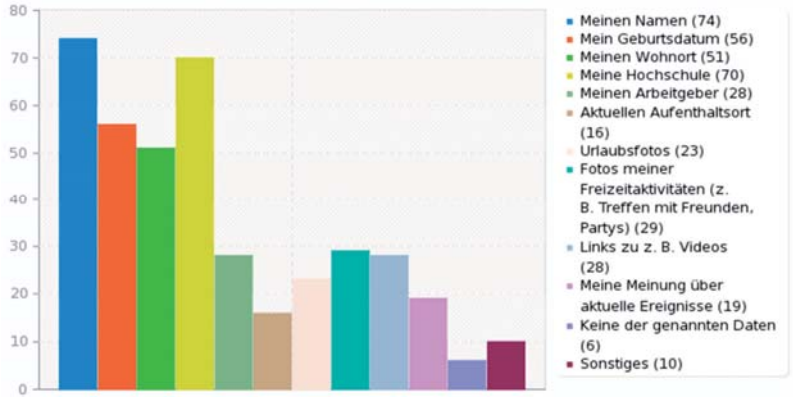
Mitglied



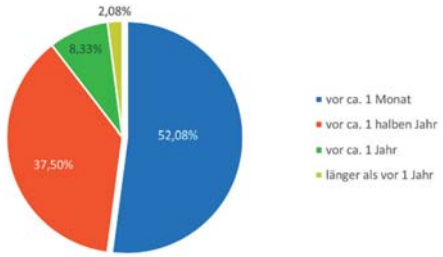
Genutzte Soziale Netzwerke



Geteilte Informationen

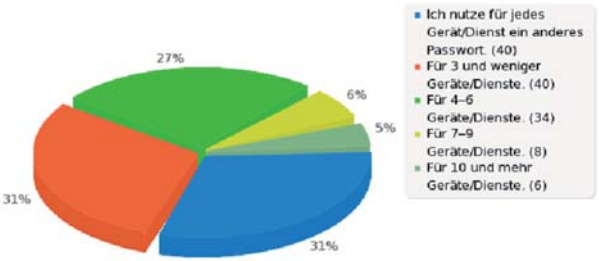


Änderung Privatsphäre-Einstellungen (Facebook)

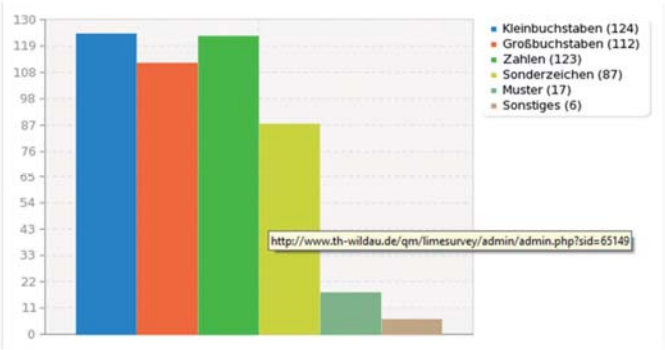


Fragen 13–16: Passwort-Stärke

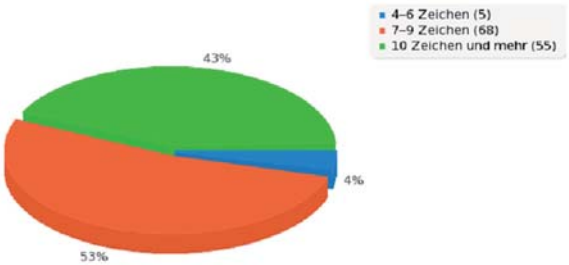
Verwendung desselben Passwortes für unterschiedliche Geräte/Dienste



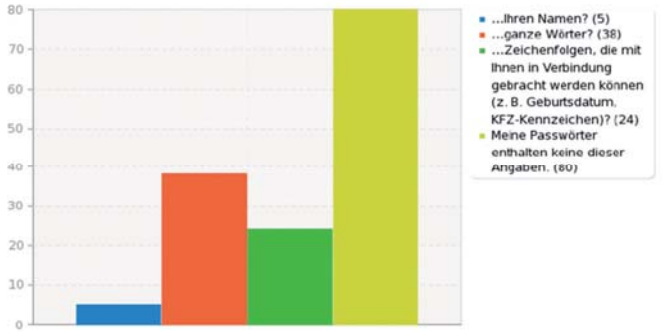
Passwort-Zusammensetzung (Mehrfachnennungen möglich)



Anzahl Zeichen pro Passwort

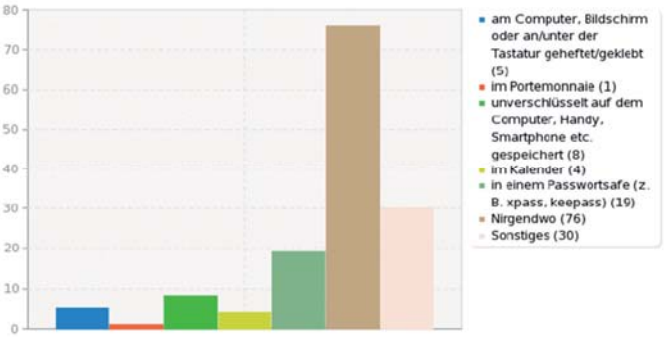


Informationen in Passwörtern

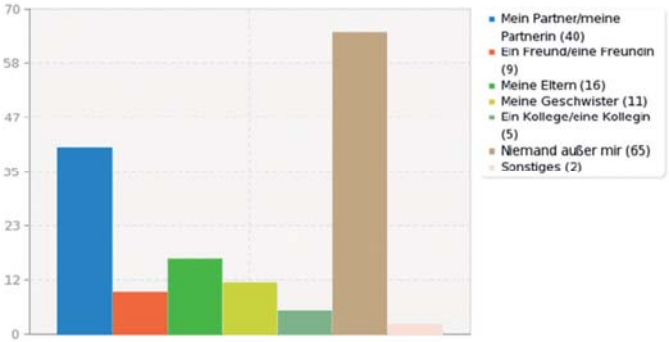


Fragen 17–18: Passwort-Aufbewahrung

Aufbewahrung von Passwörtern



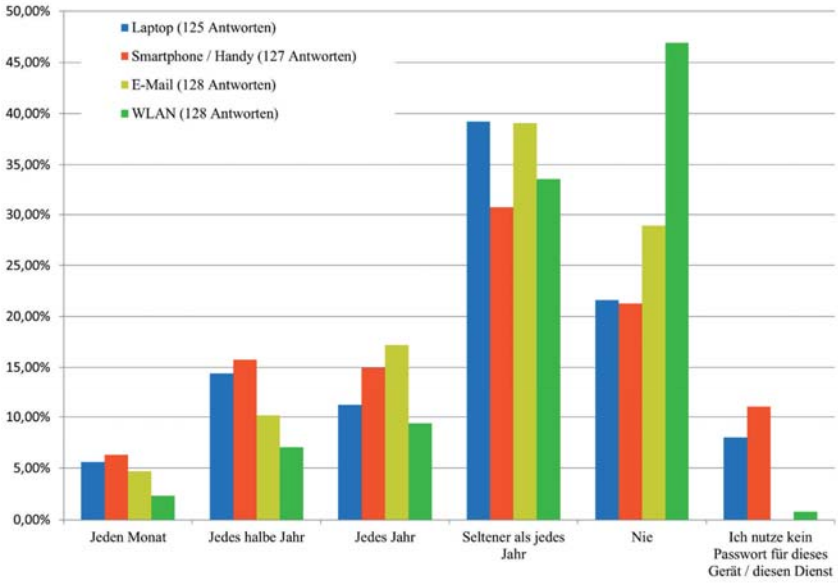
Teilen von Passwörtern



→ Die Mehrheit weiß, was sichere Passwörter und wie sie zu schützen sind.

→ Vorstellung Passwortsafe sinnvoll – wird bisher selten genutzt.

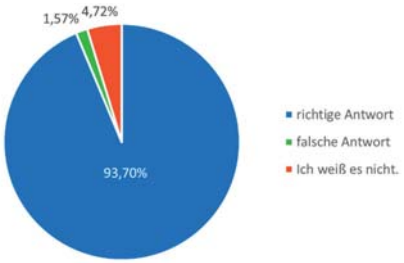
Frage 12: Änderung von Passwörtern



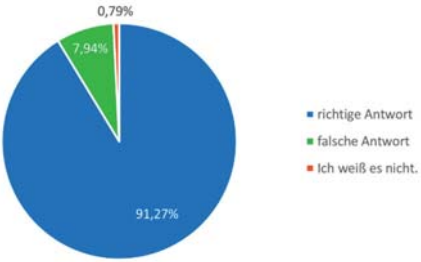
→ Passwörter sind zwar stark, werden aber selten geändert.

Fragen 27–29, 31, 34: Kenntnisse: Bekannte Gefahren und Schutzmaßnahmen

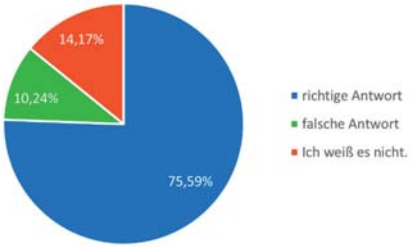
Cookies



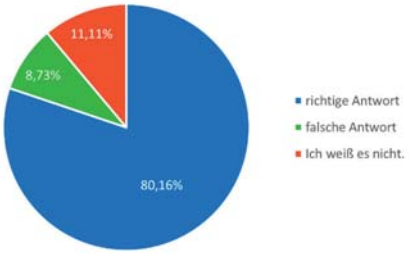
Hacking



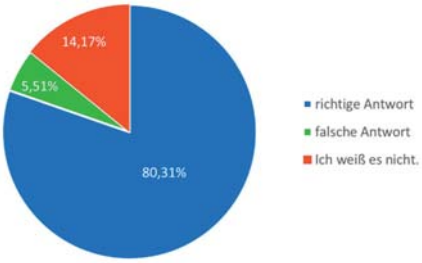
Phishing



Spyware

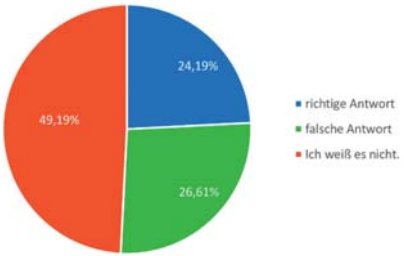


Verschlüsselte Datenübertragung

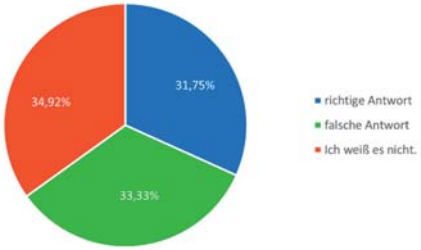


Fragen 30, 32–33, 35: Kenntnisse: Weniger bekannte Gefahren, Schutzmaßnahmen

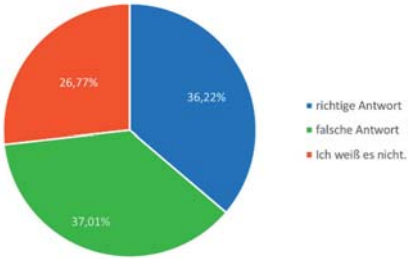
Pharming



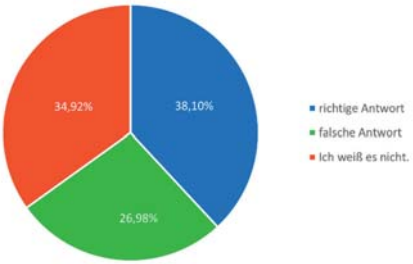
Social Engineering



Qualifizierte Digitale Signatur

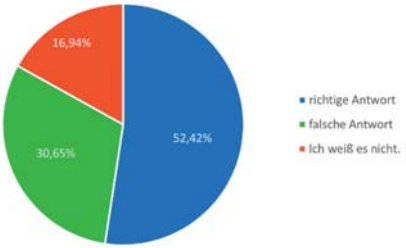


Wurm vs. Virus

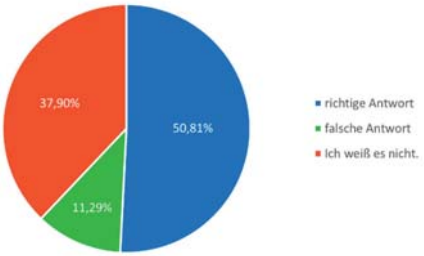


Fragen 36–39: Kenntnisse: Die Grundwerte sind weniger gut bekannt

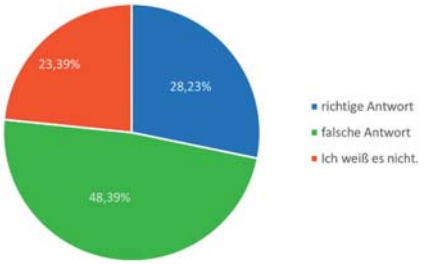
Authentizität



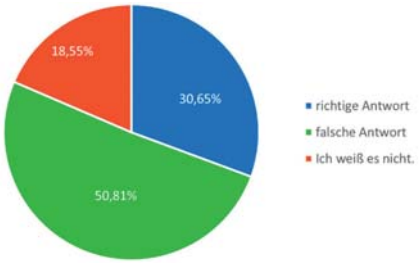
Integrität



Verfügbarkeit

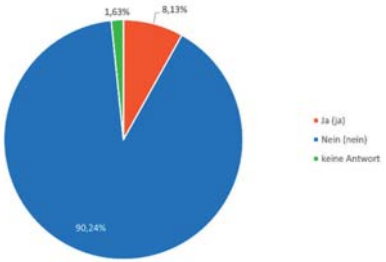


Vertraulichkeit

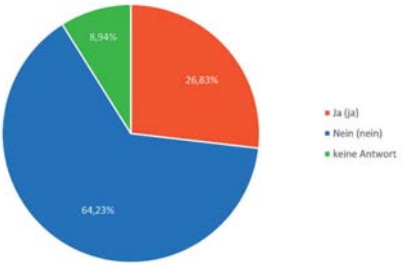


Frage 40: Mobbing

Mobbing selbst erfahren



Freunde haben Mobbing erlebt



Befragung
Information Security Awareness
WS 2016/2017

1. Gibt es in Ihrer Organisation Richtlinien...	Ja und ich kenne diese gut.	Ich habe davon gehört, kenne sie aber nicht.	Ich weiß es nicht.	Es gibt keine Richtlinien dafür.
...zum Umgang mit E-Mail-Anhängen?	○	○	○	○
...zur Nutzung des Internets?	○	○	○	○
...zur Nutzung von Computern?	○	○	○	○
...zum Umgang mit vertraulichen Daten?	○	○	○	○
...zum Herunterladen und zur Installation von Software von Drittanbietern (keine der Organisation)	○	○	○	○

2. Gibt es in Ihrer Organisation eine Person, die sich um Informations-/IT-Sicherheit kümmert?

○	Ja.
○	Nein.
○	Ich weiß es nicht.

3. Wissen Sie, wen Sie kontaktieren, falls Sie den Verdacht haben, dass Ihr Arbeitscomputer gehackt oder infiziert wurde?

○	Ja.
○	Nein.

4. Hatten Sie schon einmal einen Virus oder einen Trojaner auf Ihrem Arbeitscomputer?

○	Ja.
○	Nein.
○	Ich weiß es nicht.
○	Ich weiß nicht, was ein Virus oder ein Trojaner ist.

5. Wissen Sie, wie Sie feststellen, ob Ihr Arbeitscomputer gehackt oder infiziert wurde?

○	Ja.
○	Nein.

6. Haben Sie in Ihrer Organisation an einer Fortbildung zu folgenden Themen teilgenommen?	Ja.	Nein.	Es gibt keine Fortbildung.
Informations-/IT-Sicherheit	○	○	○
Mitarbeiterbezogene IT-Sicherheitsmaßnahmen	○	○	○
Verhalten bei Auftreten eines Computervirus	○	○	○
Passwörter	○	○	○
Datenschutz/Umgang mit personenbezogenen Daten	○	○	○
Notfallmaßnahmen (Feuer, Unfall...)	○	○	○
Sonstige themenrelevante Fortbildungen, an denen Sie teilgenommen haben:	_____		

7. Teilen Sie sich mit Kollegen Logins und Passwörter für Geräte bzw. Anwendungen?

○	Ja.
○	Nein.

8. Nutzen Sie dasselbe Passwort für berufliche Accounts und private Accounts wie Facebook, Twitter oder private E-Mails?

○	Ja.
○	Nein.

9. Nutzen Sie dasselbe Passwort für mehrere berufliche Geräte und Anwendungen?

○	Ja.
○	Nein.

10. Welche der folgenden Passwörter sind Ihrer Meinung nach starke Passwörter?
(Sie können mehrere auswählen)

○	Administrator
○	$jel&F2bxCb5
○	%4Btv
○	Rooney315
○	secret22

11. Wie häufig ändern Sie durchschnittlich Ihre dienstlichen Passwörter? _____

12. Wie viele Zeichen haben Ihre beruflichen Passwörter in der Regel? _____

13. Haben Sie Ihre dienstlichen Passwörter schriftlich hinterlegt?

○	Ja.
	Falls ja, wo? _____
○	Nein.

14. Ist die Firewall auf Ihrem Arbeitscomputer aktiviert?

○	Ja.
○	Nein.
○	Ich weiß es nicht.
○	Ich weiß nicht, was eine Firewall ist.

15. Ist auf Ihrem Arbeitscomputer ein Anti-Virus-Programm installiert, aktiviert und wird regelmäßig aktualisiert?

○	Ja.
○	Nein.
○	Ich weiß es nicht.
○	Ich weiß nicht, was ein Anti-Virus-Programm ist.

16. Ist Ihr Arbeitscomputer so konfiguriert, dass Updates automatisch ausgeführt werden?

○	Ja.
○	Nein.
○	Ich weiß es nicht.

17. Wie häufig führen Sie Datensicherungen durch?

○	alle ..... Tage/Wochen/Monate *(bitte zeitlichen Rahmen eintragen und Zutreffendes (Tag, Wochen, Monate unterstreichen)*
○	unregelmäßig
○	bei Bedarf
○	Dies wird zentral von der IT-Abteilung übernommen.

18. Wenn jemanden Ihnen einen Anhang oder einen Link per E-Mail sendet, der nichts mit Ihrer Arbeit zu tun hat, wie wahrscheinlich ist es, dass Sie diesen öffnen?

○	Nicht sehr wahrscheinlich.
○	Es ist möglich, dass ich ihn öffne – abhängig davon, um was es sich handelt.
○	Sehr wahrscheinlich.
○	Ich öffne Anhänge und Links immer.

19. Bitte wählen Sie die Antworten aus, die die Risiken von E-Mail-Anhängen gut beschreiben. *(eine oder mehrere Antworten können richtig sein)*

○	Nur Anhänge mit der Endung „.exe“ stellen ein wirkliches Risiko dar.
○	Alle Anhänge können schädlich sein und Viren enthalten.
○	Wenn man den Absender kennt und ihm vertraut, kann man den Anhang öffnen.
○	Wenn man eine Firewall auf dem Computer installiert hat, können Anhänge gefahrlos geöffnet werden.
○	Ein Antivirus-Programm reduziert das Risiko, durch einen E-Mail-Anhang mit Viren infiziert zu werden.

20. Nutzen Sie Ihre privaten mobilen Endgeräte (z. B. Smartphone, Tablet, Laptop), um Dateien/Informationen Ihrer Organisation zu speichern und zu übertragen?

○	Ja.
○	Ja, aber ich nutze immer die von meiner Organisation dafür bereitgestellten Lösungen.
○	Nein.

21. Haben Sie schon einmal unbefugt oder von einer fragwürdigen Quelle Software auf Ihrem Arbeitscomputer heruntergeladen und installiert?

○	Ja.
○	Nein.

22. Haben Sie sich schon einmal von öffentlichen Computern, z. B. in der Bibliothek, im Internetcafé, in der Hotellobby, auf Ihren beruflichen Accounts eingeloggt?

○	Ja.
○	Nein.

23. Nutzen Sie öffentliche WLANs, deren Ursprung Sie nicht kennen?

○	Ja.
○	Nein.

24. Welche Sicherheitsmaßnahme nutzen Sie bei der Verbindung aus einem öffentlichen WLAN zu Ihrem Unternehmen?

○	Verschlüsselte Verbindung
○	VPN (Virtual Private Network)
○	Ich nutze keine Sicherheitsmaßnahme.
○	Ich verbinde mich nicht mittels öffentlichen WLANs mit meinem Unternehmen.

25. Sie finden auf dem Gelände oder im Gebäude Ihrer Organisation einen USB-Stick. Wie verhalten Sie sich?

○	Ich frage das IT-Team, was ich damit tun soll.
○	Ich schaue mir den USB-Stick später an, wenn ich zu Hause bin.
○	Ich lasse ihn liegen.
○	Ich stecke den USB-Stick in meinen Computer, um zu schauen, was drauf ist.
○	Ich schmeiße ihn in den Mülleimer.

26. Wenn Sie eine Datei von Ihrem Computer oder einem USB-Stick löschen, kann diese Information nicht wieder hergestellt werden.

O	Richtig.
O	Falsch.

27. Wenn Sie Ihren Arbeitsplatz kurzfristig verlassen, um sich einen Kaffee zu holen oder zur Toilette zu gehen, wie hinterlassen Sie Ihren Computer?
(Sie können mehrere Antworten ankreuzen)

O	Ich schalte meinen Monitor aus.
O	Ich logge mich aus allen Anwendungen aus.
O	Ich sperre den Computer.
O	Ich schalte den Computer aus.
O	Ich nutze einen passwortgeschützten Bildschirmschoner.
O	Ich tue nichts von dem Genannten.
Sonstiges: _____	

28. Wenn gefälschte E-Mails, Textnachrichten und Webseiten so gestaltet sind, dass sie den Anschein erwecken, sie seien von realen Unternehmen, handelt es sich um:

O	Phishing
O	Spyware
O	Pharming

29. Worauf müssen Sie achten, wenn Sie auf einer Webseite sicher Daten eingeben möchten (z. B. Online-Banking)?

O	Anmeldung mit einem Kennwort
O	Schlosssymbol und https
O	http

30. Was kann ein Trojaner tun?

O	Dokumente löschen.
O	Sie durch Ihre Webcam beobachten.
O	Tastenanschläge protokollieren.
O	Alles oben Genannte.

31. Worin besteht das größte Risiko für die Informations-/IT-Sicherheit Ihrer Organisation?

O	Computerviren und andere Malware
O	Schadhafte Anwendungen/Software
O	Schadhafte Hardware
O	Menschliche Fehler, Täuschungen etc.

Quellen

Bundesamt für Sicherheit in der Informationstechnik (BSI): Hilfsmittel: PC-Fragebogen. IT-Grundschutzhandbuch: Stand Juli 1999. https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Hilfsmittel/ChecklistenundFormulare/checklistenundformulare_node.html. Letzter Zugriff 20.9.2016

Hohmann, U. (2011): Mind the Gap! Dienstleistungsqualität und Informationssicherheit in Behörden. Masterarbeit Universität Kassel.

SANS Securing The Human (2012): Security Awareness Survey. https://www.sans.edu/student-files/awareness/employee-security-awareness-survey.pdf. Letzter Zugriff 20.9.2016.

Thompson Rivers University (2013): Cyber Security Awareness Day: CyberMonthCard1.1, CyberMonthCard2.1. Method only Susan Swift/TRU 2013. http://www.tru.ca/its/infosecurity/news/CyberSecurityAwarenessQui2013.html. Letzter Zugriff 20.9.2016.

Warwick – Governance (2012): Information Security Awareness Questionnaire. http://www2.warwick.ac.uk/services/gov/informationsecurity/questionnaire/. Letzter Zugriff 20.9.2016.

Winnipeg – Audit Department (2008): Assessment of Information Security Awareness. http://www.winnipeg.ca/audit/pdfs/reports/ITSecurityAwareness.pdf. Letzter Zugriff 20.9.2016.

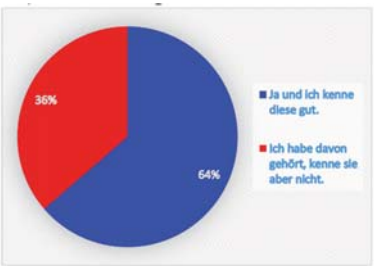
Gibbyi End User Security Awareness Quiz. ProProfs Quiz Maker. http://www.proprofs.com/quiz-school/story.php?title=end-user-security-awareness-quiz. Letzter Zugriff 20.9.2016.

Ausgewählte Ergebnisse der Befragung zu Informationssicherheitsbewusstsein und -kenntnisse zu Beginn des Wintersemesters 2016/17

Frage 1: Gibt es in Ihrer Organisation Richtlinien…

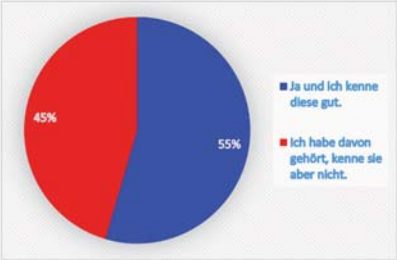
a) ...zum Umgang mit E-Mail-Anhängen?

b) ...zur Nutzung des Internets?



c) ...zur Nutzung von Computern?

d) ...zum Umgang mit vertraulichen Daten?

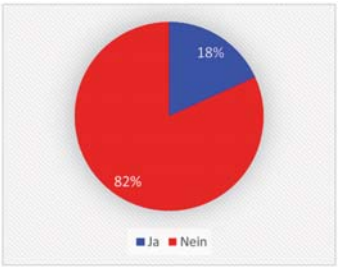


e) … zum Herunterladen und zur Installation von Software von Drittanbietern? (keine der Organisationen)

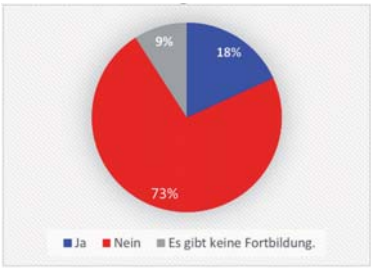
→ Existierende Richtlinien in den Verwaltungen im Hinblick auf Informationssicherheit müssen besser bekannt gemacht werden. Die Studierenden/Mitarbeitende müssen dafür sensibilisiert werden, dass sie diese aktiv nachfragen.

<u>Frage 6: Haben Sie in Ihrer Organisation an einer Fortbildung zu folgenden Themen teilgenommen?</u>

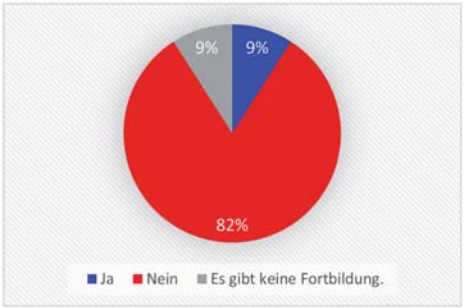
a) Informations-/IT-Sicherheit



b) Mitarbeiterbezogene IT-Sicherheitsmaßnahmen

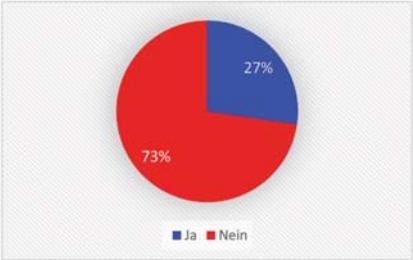


c) Verhalten bei Auftreten eines Computervirus

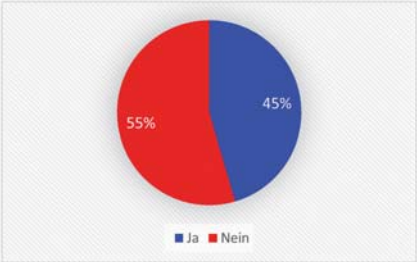


d) Passwörter

e) Datenschutz/Umgang mit personenbezogenen Daten

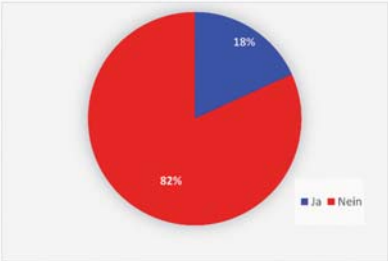


f) Notfallmaßnahmen (Feuer, Unfall...)



→ Es sollte in den Verwaltungen ein größeres Angebot an (verpflichtenden) Fortbildungen zu informationssicherheitsrelevanten Themen geben.

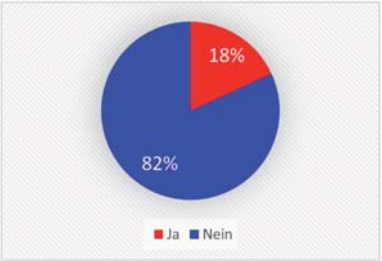
Frage 5: Wissen Sie, wie Sie feststellen, ob Ihr Arbeitscomputer gehackt oder infiziert wurde?



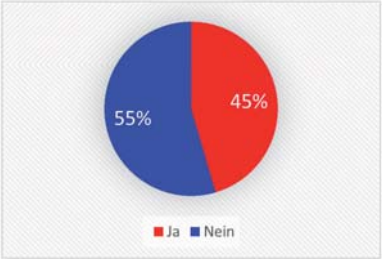
→ Hinweise auf einen infizierten Computer müssen besser bekannt werden, damit die Mitarbeitende im Falle eines Angriffs diesen auch bemerken und beheben können.

Fragen 7–13: Passwörter

Teilen Sie sich mit Kollegen Logins und Passwörter für Geräte bzw. Anwendungen?

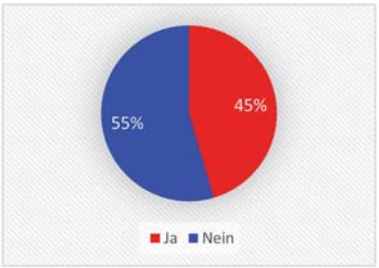


Nutzen Sie dasselbe Passwort für mehrere berufliche Geräte und Anwendungen?

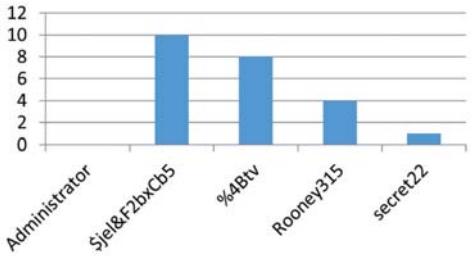


Nutzen Sie dasselbe Passwort für berufliche Accounts und private Accounts?

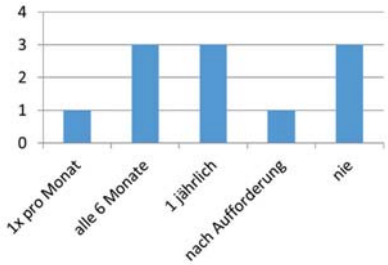
Haben Sie Ihre dienstlichen Passwörter schriftlich hinterlegt?



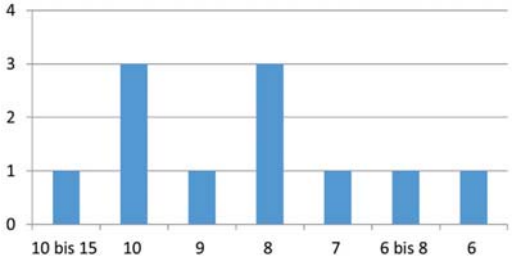
Welche der folgenden Passwörter sind Ihrer Meinung nach starke Passwörter? (Mehrfachnennungen möglich)



Wie häufig ändern Sie durchschnittlich Ihre dienstlichen Passwörter?



Wie viele Zeichen haben Ihre beruflichen Passwörter in der Regel?

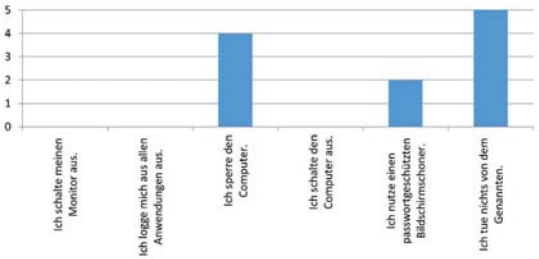


→ Es besteht noch Sensibilisierungsbedarf für die Verwendung von Passwörtern (z. B. für jede Anwendung ein eigenes Passwort, starke Passwörter, Wechsel von Passwörtern).

Fragen 18 und 27: Sicherheitsbewusstes Verhalten

Wenn jemanden Ihnen einen Anhang oder einen Link per E-Mail sendet, der nichts mit Ihrer Arbeit zu tun hat, wie wahrscheinlich ist es, dass Sie diesen öffnen?

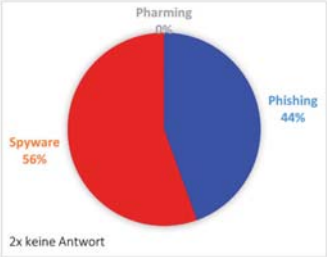
Wenn Sie Ihren Arbeitsplatz kurzfristig verlassen, um sich einen Kaffee zu holen oder zur Toilette zu gehen, wie hinterlassen Sie Ihren Computer?
(Mehrfachnennungen möglich)



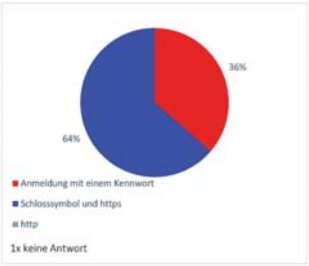
→ Einfache und leicht auszuführende Schutzmaßnahmen für die Informationssicherheit müssen noch stärker im Bewusstsein verankert werden.

Fragen 28–31: Kenntnisse

Wenn gefälschte E-Mails, Textnachrichten und Webseiten so gestaltet sind, dass sie den Anschein erwecken, sie seien von realen Unternehmen, handelt es sich um:

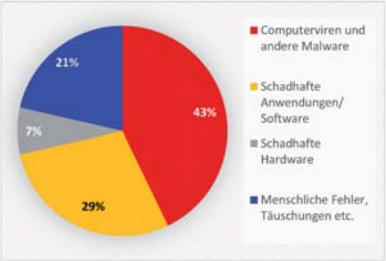


Worauf müssen Sie achten, wenn Sie auf einer Webseite sicher Daten eingeben möchten (z. B. Online-Banking)?



Was kann ein Trojaner tun?

Worin besteht das größte Risiko für die Informations-/IT-Sicherheit Ihrer Organisation?



→ Kenntnisse können noch ausgebaut werden und insbesondere ist die Bewusstmachung des „menschlichen Faktors“ der Informationssicherheit sehr wichtig.

Anhang zu Kapitel 6

Screenshots der Projektwebseite

Projekt-Plakat in Deutsch und Englisch

Projekt-Flyer in Deutsch und Englisch

Pressberichte zum Projekt

Ziele und Inhalte

Das Projekt „SecAware4job: Informationssicherheitsbewusstsein für den Berufseinstieg" möchte Studierende nicht-technischer Studiengänge als zukünftige Mitarbeiter/innen für die alltäglichen Herausforderungen des Schutzes der digitalen Infrastruktur und der Informationssicherheit sensibilisieren. Konkret bestehen die Ziele von *SecAware4job* darin,

- Kompetenzen bzgl. Informations- und IT-Sicherheit für den Berufseinstieg zu vermitteln.
- Bewusstseins- und Verhaltensänderungen anzuregen und zu unterstützen.
- Risikobewertung und Treffen von Entscheidungen zu erleichtern.
- nachweisebare, zertifizierte Qualifizierungen für den Berufseinstieg zu verleihen.

Die inhaltlichen Schwerpunkte der Weiterbildung sind:

1. Informationssicherheit – warum?
2. Rechtliche Rahmenbedingungen für Informationssicherheit
3. Informationssicherheitsmanagement (ISMS)
4. Sicherheitsrelevantes Verhalten
5. Maßnahmen für Informationssicherheit
6. Verschlüsselung und digitale Signatur
7. Entwurf von Sicherheitskonzepten, insbesondere nach IT-Grundschutz (BSI)
8. Aktuelle Themen zur Informationssicherheit

Gefördert von HGS

SecAware4job

Informationssicherheitsbewusstsein
für den Berufseinstieg

Informationssicherheitsbewusstsein für den Berufseinstieg

In dem Projekt *SecAware4job* wird eine berufsorientierte Zusatzqualifikation für Studierende in Form einer innovativen Weiterbildung zur Stärkung des Bewusstseins und der Kompetenzen bezüglich Informations- und insbesondere IT-Sicherheit entwickelt und erprobt.

Diese Zusatzqualifikation ist zielgruppen-spezifisch aufgebaut und wird vor allem in den nicht-technischen Studiengängen der Technischen Hochschule (TH) Wildau integriert. Die Studierenden erhalten die Möglichkeit, ein vierstufiges Zertifikat zu erwerben: vom einfachen Teilnahme-, über ein Moderations-, ECDL-Zertifikat IT-Sicherheit / Datenschutz bis hin zum fünf-Jahre-gültigen Zertifikat zur/m IT-Sicherheitsbeauftragten (IT-SiBe).

Neben herkömmlicher Stoffvermittlung kommen möglichst viele kreative Lehr- und Lernmethoden zum Einsatz, um das abstrakte und komplexe Thema Informationssicherheit mit all seinen Facetten (rechtliche Rahmenbedingungen, Normen & Standards, Schutzmaßnahmen, Konzepte etc.) den Studierenden leicht verständlich, greif- und erlebbar zu vermitteln. Als kreative Methoden werden u. a. analoge und digitale simulierte Szenarien eingesetzt.

SecAware4job wird gefördert von der Horst Görtz Stiftung.

Gefördert von HGS

SecAware4job

Technische Hochschule Wildau Technical University of Applied Sciences

Gefördert von HGS

» Forschung in Wildau – innovativ und praxisnah «

Informationssicherheitsbewusstsein für den Berufseinstieg

Ausgangssituation

Chancen und Herausforderungen der Digitalisierung

- Hackerangriffe, Datendiebstahl und Wirtschaftsspionage
- „Fehlleistungen" und Täterschaft von (aktuellen und ehemaligen) Mitarbeitern und Führungskräften
- Bewusstsein für Informations- und IT-Sicherheit für alle Dienstleistungs- und Industriebereiche notwendig, da Informatik eine Querschnittsfunktion besitzt
- Security-Spezialisten als einer der erwarteten Top-Ten-Berufe in 2020

Alle Mitarbeiter, nicht nur IT-Fachkräfte, sollten über Informationssicherheitsbewusstsein und -Kompetenz verfügen!

Informationssicherheitsbewusstsein für den Berufseinstieg

In dem Projekt *SecAware4job* soll eine berufsorientierte Zusatzqualifikation für Studierende in Form einer innovativen Weiterbildung zur Stärkung des Bewusstseins und der Kompetenzen bezüglich Informations- und insbesondere IT-Sicherheit entwickelt werden.

Diese Zusatzqualifikation soll zielgruppenspezifisch aufgebaut und vor allem in den nicht-technischen Studiengängen der Technischen Hochschule [TH] Wildau integriert werden.

Neben herkömmlicher Stoffvermittlung sollen möglichst viele kreative Lehr- und Lernmethoden zum Einsatz kommen, um das abstrakte und komplexe Thema Informationssicherheit mit all seinen Facetten (rechtliche Rahmenbedingungen, Normen & Standards, Schutzmaßnahmen, Konzepte etc.) den Studierenden leicht verständlich, greif- und erlebbar zu vermitteln.

Als kreative Methoden kommen u. a. analoge und digitale simulierte Szenarien zum Einsatz.

Ziele und Inhalte von SecAware4job

SecAware4job möchte Studierende nicht-technischer Studiengänge als zukünftige Mitarbeiter für die alltäglichen Herausforderungen des Schutzes der digitalen Infrastruktur und der Informationssicherheit sensibilisieren.

Konkret bestehen die Ziele von *SecAware4job* darin,

- Kompetenzen bzgl. Informations- und IT-Sicherheit für den Berufseinstieg zu vermitteln.
- Bewusstseins- und Verhaltensänderungen anzuregen und zu unterstützen.
- Risikobewertung und Treffen von Entscheidungen zu erleichtern.
- nachweisebare, zertifizierte Qualifizierungen für den Berufseinstieg zu verleihen.

Die inhaltlichen Schwerpunkte der Weiterbildung sind:

Zertifikate für den Berufseinstieg

Mit der Teilnahme an der Weiterbildung *SecAware4job* können die Studierenden als Nachweis unterschiedliche Zertifikate erwerben:

Methodischer Ansatz

Diese Methoden

- lassen komplexe und abstrakte Lerninhalte greif- und erlebbar werden,
- greifen reale (Problem-) Situationen aus dem beruflichen Alltag auf,
- ermöglichen Lernen durch Ausprobieren, Fehler machen und Wiederholen, Zusammenarbeit und Kommunikation,
- unterstützen die Weitergabe und den Austausch von Wissen,
- bieten direktes Feedback zum Lernfortschritt,
- orientieren sich an den Lernenden, ihren Wissensständen und ihren Bedürfnissen (Lernendenzentriertes Lernen).

Evaluation

Das Projekt beinhaltet eine begleitende Forschung, um den Lernerfolg und die Wirkung des Weiterbildungsangebotes zu ermitteln.

Homepage: secaware4job.wildau.biz
E-Mail: margit.scholl@th-wildau.de

Projektmanagement: Prof. Dr. Margit Scholl
Operative Projektleitung: Frauke Fuhrmann
KMU-Partner: known_sense (Köln), sudile (Potsdam)

SecAware4job

Technische Hochschule Wildau Technical University of Applied Sciences

sponsored by HGS

» Research in Wildau – innovative and practical «

Information Security Awareness for Young Professionals

Initial situation

Opportunities and challenges of digitalisation

- Hacker attacks, data theft and economic espionage
- Blunders and offences committed by (active and former) employees and managers
- Necessity of awareness for information and IT security in all tertiary and industrial sectors as information technology (IT) has a cross-sectional function
- Security specialist is one of the top ten anticipated jobs in 2020

Not only IT qualified personnel but every employee should be aware of and competent in information security!

Information Security Awareness for young professionals

Within the project *SecAware4job*, an additional job-related qualification for students should be developed in the form of an innovative further education aimed at strengthening the awareness and skills with regard to information and IT security.

The concept of this additional qualification should be closely oriented to the target group and the training should be integrated particularly in non-technical degree courses of the Technical University of Applied Sciences (TUAS) Wildau.

It is an important concern of this project to use as many creative learning and teaching methods as possible, in addition to conventional teaching procedures, to make students understand this abstract and complex theme with all its facets (regulatory framework, norms and standards, protective measures, concepts, etc.) more easily and make the topic tangible for and to be experienced by them.

Amongst other aspects, narrative/analog and digital simulated scenarios will be applied.

Goals and contents of SecAware4job

SecAware4job aims to sensitise students of non-technical study courses to the daily challenges of information security as well as to the protection of digital infrastructure.

Concrete goals of SecAware4job are

- to teach skills in information and IT security for young professionals,
- to motivate and support a change of awareness and behaviour,
- to facilitate risk assessment and decision making,
- to offer verifiable and accredited qualifications for the career entry.

The focus of content of the further education is

Certificates for career entry

Through participation in *SecAware4job*, students will be able to receive different certificates as confirmation.

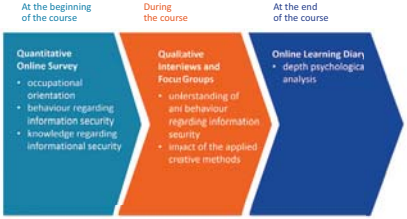
Methodical approach

These methods

- make complex and abstract learning contents understandable and tangible,
- deal with real (problem) situations of everyday professional life,
- enable learning by trial and error, repetition, team work and communication,
- support knowledge transfer and exchange,
- offer immediate feedback regarding the learning progress,
- are oriented towards the learners, their level of knowledge and their needs (learner-centred approach).

Evaluation

The project is accompanied by research that will evaluate the learning success as well as the impact of this further education.



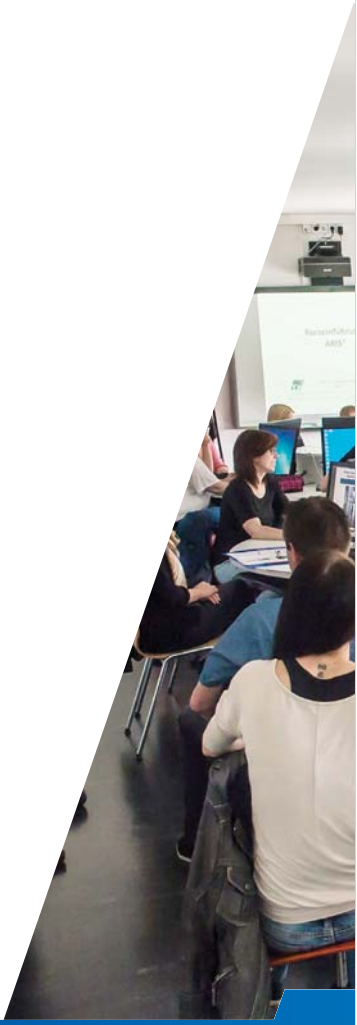
Homepage: secaware4job.wildau.biz
E-Mail: margit.scholl@th-wildau.de

Project Management: Prof. Dr. Margit Scholl
Operational Project Management: Frauke Fuhrmann
SME Partners: known_sense (Köln), sudile (Potsdam)

Technische Hochschule Wildau
Hochschulring 1
15745 Wildau

Projektmanagement
Frau Prof. Dr. rer. nat. Margit Scholl
margit.scholl@th-wildau.de

Gefördert durch
SecAware4job
HGS Horst Görtz Stiftung



Technische Hochschule Wildau
Technical University of Applied Sciences

» Forschung in Wildau – innovativ und praxisnah «

INFORMATIONS-SICHERHEITS-BEWUSSTSEIN FÜR DEN BERUFSEINSTIEG: SECAWARE4JOB

Mehr Informationen unter:
secaware4job.th-wildau.de

Informationssicherheitsbewusstsein für den Berufseinstieg

Ausgangssituation

In SecAware4job wird eine berufsorientierte Zusatzqualifikation für Studierende in Form einer innovativen Weiterbildung zur Stärkung des Bewusstseins und der Kompetenzen bezüglich Informations- und insbesondere IT-Sicherheit entwickelt und erprobt. Diese Zusatzqualifikation wird vor allem in den nicht-technischen Studiengängen der Technischen Hochschule Wildau integriert.

Alle Mitarbeiter/innen, nicht nur IT-Fachkräfte, sollten über Informationssicherheitsbewusstsein und -Kompetenz verfügen!

Ziele von SecAware4job

- Kompetenzen bzgl. Informations- und IT-Sicherheit für den Berufseinstieg vermitteln
- Bewusstseins- und Verhaltensänderungen anregen und unterstützen
- Risikobewertung und Treffen von Entscheidungen erleichtern
- Nachweisebare, zertifizierte Qualifizierungen für den Berufseinstieg verleihen

Drei Ansätze der betrieblichen Security und Privacy Awareness

Version 1.0

In vielen Organisationen findet nur ein Wissenstransfer statt: Bereitstellung von Informationen (z. B. Präsentationen oder Plakate) oder eines Web Based Trainings (WBT). Trotz möglicher Vorteile von WBT zeigen Studien, dass die Ansätze, die sich nur auf den Wissenstransfer konzentrieren, nicht in der Lage sind, dauerhaftes Bewusstsein für Informationssicherheit zu schaffen.

Version 2.0

Auf der Basis empirischer Befunde integriert ein Bewusstseinstrainings 2.0 marketingorientierte Werbeelemente, die neben dem Wissenstransfer insbesondere Aufmerksamkeit erzielen sollen. Durch eine gute Geschichte (Storytelling) kann die Beteiligung und das Engagement der Teilnehmenden stimuliert werden.

Version 3.0

Die psychologische Forschung zeigt, dass neben dem theoretischen Ansatz für den Wissenstransfer und dem marketingorientierten Ansatz ein systemischer Ansatz mit Emotionen und sozialer Teilhabe im Team und Interaktion in erlebbaren Szenarien benötigt wird, um dauerhafte Sensibilisierung für Informationssicherheit zu erreichen. Deshalb basiert der methodische Ansatz von SecAware4job auf Version 3.0.

Einsatz von möglichst vielen kreativen Lehr- und Lernmethoden, um

- komplexe und abstrakte Lerninhalte greif- und erlebbar zu machen,
- reale (Problem-) Situationen aufzugreifen,
- Lernen durch Ausprobieren, Fehler machen und Wiederholen zu ermöglichen,
- den Austausch von Wissen zu unterstützen,
- direktes Feedback zum Lernfortschritt zu geben,
- sich an den Lernenden, ihren Wissensständen und ihren Bedürfnissen zu orientieren.

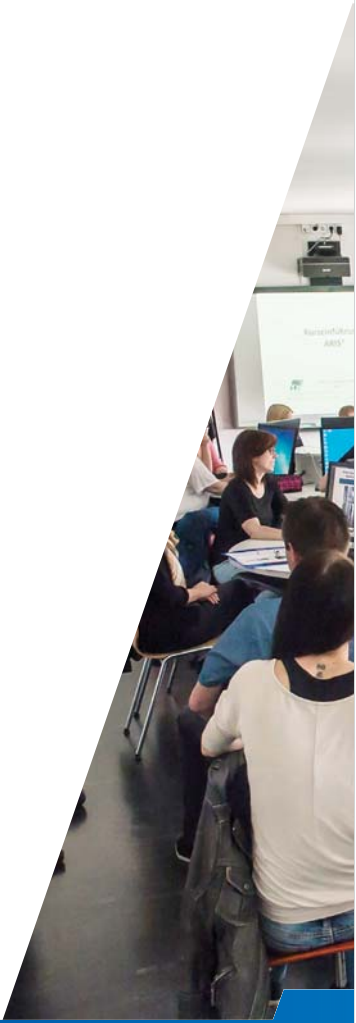
Die Studierenden können in SecAware4job unterschiedliche Zertifikate erwerben:

- IT-Sicherheitsbeauftragte/r (5 Jahre Gültigkeit)
- Qualifiziertes Zertifikat
  Projektarbeit
- ECDL-Zertifikat
  IT-Sicherheit / Datenschutz
- Modereationszertifikat
  Teilnamezertifikat

Technical University of Applied Sciences Wildau
Hochschulring 1
15745 Wildau

Project Management
Prof. Dr. rer. nat. Margit Scholl
margit.scholl@th-wildau.de

Sponsored by
SecAware4job
HGS



Technische Hochschule Wildau
Technical University of Applied Sciences

» Research in Wildau – innovative and practical «

INFORMATION SECURITY AWARENESS FOR YOUNG PROFESSIONALS: SECAWARE4JOB

Further information:
secaware4job.th-wildau.de

Information Security Awareness for Young Professionals

Initial situation

Within the project SecAware4job, an additional job-related qualification for students is developed and tested in the form of an innovative further education aimed at strengthening the awareness and skills with regard to information and IT security. This additional qualification is integrated particularly in the non-technical degree courses of the Technical University of Applied Sciences Wildau.

Not only IT qualified personnel but every employee should be aware of and competent in information security!

Goals of SecAware4job

- To teach skills in information and IT security for the career entry
- To motivate and support a change of awareness and behaviour
- To facilitate risk assessment and decision making
- To offer verifiable and accredited qualifications for the career entry

3 approaches of security and privacy awareness

Version 1.0

Information security awareness training is limited in many organizations to knowledge transfer in terms of providing information (e.g. as presentations or posters) or offering web-based training (WBT). While recognizing the advantages of WBT, several studies show that the approaches that only focus on knowledge transfer are not sufficient to create lasting awareness.

Version 2.0

Based on empirical findings, awareness trainings 2.0 integrate marketing-oriented promotional elements that should attract attention in addition to knowledge transfer. A good story can stimulate participants' involvement and engagement with information security awareness (story telling).

Version 3.0

Psychological research activities show that in addition to the theoretical approach to knowledge transfer and the marketing-oriented approach, a systematic approach with emotions and social participation in a team as well as interactions in experienceable scenarios is needed to achieve lasting information security awareness that results in both a clear intention and actual behaviour to protect confidential information. Therefore, the methodological approach of SecAware4job is based on version 3.0.

Use of as many creative learning and teaching methods as possible in order to

- make complex and abstract learning contents understandable and tangible,
- deal with real (problem) situations of everyday professional life,
- enable learning by trial and error and repetition,
- support knowledge transfer and exchange,
- offer immediate feedback regarding the learning progress,
- orient the learning content towards the learners, their level of knowledge and their needs.

Students are able to acquire different certificates in SecAware4job:

DLGI Dienstleistungsgesellschaft für Informatik mbH

PRESSEMITTEILUNG 15. Januar 2016

Technische Hochschule Wildau wird ECDL-Prüfungszentrum

Bonn/Wildau. Anfang Januar hat die Technische Hochschule Wildau erfolgreich das Akkreditierungsverfahren für die Zulassung als Prüfungszentrum zum Europäischen Computerführerschein (ECDL) durchlaufen. Damit erhalten die Studenten der Hochschule Zugang zum internationalen Zertifizierungssystem des ECDL und können die ECDL-Prüfungen im Rahmen des Studiums absolvieren.

Die Technische Hochschule Wildau (FH) ist eine innovative, zukunftsorientierte und praxisverbundene Hochschule südlich von Berlin. In den beiden Fachbereichen Ingenieur- und Naturwissenschaften (INW) sowie Wirtschaft, Informatik, Recht (WIR) können dreizehn Bachelor und zehn Master-Abschlüsse erworben werden. Die TH Wildau ist die größte Fachhochschule des Landes Brandenburg.

Mit der ECDL-Zertifizierung will die Hochschule eine einheitlich, an einem internationalen Standard ausgerichtete informatische Grundbildung für ihre Studenten einführen, denn die sichere Handhabung der Anwendungssoftware ist Voraussetzung für das Fachstudium, kann aber auch heute noch längst nicht bei allen Studienanfängern vorausgesetzt werden. Frau Professor Dr. Scholl vom Fachbereich Wirtschaft, Informatik, Recht erläutert dazu: „Mit dem ECDL können wir eine Messlatte anlegen, die für die Studenten die grundlegenden Propädeutischen IT-Kenntnisse definiert, die jeder Student als Voraussetzung für sein fachwissenschaftliches Studium benötigt. Da der ECDL von den europäischen Fachgesellschaften für Informatik getragen wird, haben wir die Sicherheit, dass er stets auf dem aktuellen Stand der Technik ist."

Die Dienstleistungsgesellschaft für Informatik (DLGI) als die in Deutschland für den ECDL zuständige Organisation sieht in der Akkreditierung der TH Wildau eine Bestätigung der zunehmenden Bedeutung informatischer Grundbildung. „Man hat die informatische

Kontakt
DLGI mbH
Am Bonner Bogen 6
53227 Bonn
Tel.: +49228/688-448-0
Fax: 0228- 688-448-99
info@dlgi.de

Grundbildung ja schon totgesagt", erklärt Thomas Michel, Geschäftsführer der DLGI, „weil man glaubte, dass die sogenannten ‚digital natives' ganz automatisch in diese Techniken hineinwachsen. Das war natürlich nie der Fall. Heute erkennen wir sogar einen entgegengesetzten Trend. Da viele Jugendliche nur noch Mobilgeräte nutzen, fehlen ihnen vielfach auch die geringen Vorkenntnisse, die frühere Generationen mitbrachten. Wir freuen uns deshalb sehr über die Akkreditierung der Hochschule Wildau."

Über den ECDL

Der Europäische Computerführerschein (ECDL) ist eine international anerkannte Zertifizierung für Computernutzer. Er ist weltweit in 148 Ländern anerkannt und wird in 38 Sprachen unterrichtet. Unternehmen schätzen ihn als Nachweis der Computerkompetenz. Er vermittelt Schlüsselkompetenzen im Umgang mit dem Computer und bietet eine umfangreiche Auswahl an Modulen, von Computergrundlagen über Office bis hin zu IT-Sicherheit und Datenschutz.

Weitere Informationen unter https://www.ecdl.de.

Pressemitteilungen

50 Elemente in dieser Kategorie

SPD-Arbeitsgemeinschaft für Bildung testete innovative digitale Sensibilisierungskonzepte der Technischen Hochschule Wildau

veröffentlicht 25.05.2016 14:25 Uhr von Bernd Schlütter

Sind Sie „digital save" unterwegs? Dieser Frage gingen die Mitglieder des Arbeitskreises „Digitale Gesellschaft" der SPD Brandenburg am 12. Mai 2016 mit Prof. Dr. Margit Scholl und ihren Mitarbeitern der Forschungsgruppe „IT-Sicherheit und digitale Medien in der Bildung" der TH Wildau nach. Dabei ging es um analoge und digitale Methoden, die das Bewusstsein für Informationssicherheit fördern.

Sind Sie „digital save" unterwegs? Dieser Frage sind die **Mitglieder des Arbeitskreises „Digitale Gesellschaft" der SPD Brandenbur**g am 12. Mai 2016 mit *Forschungsprofessorin Dr. Margit Scholl* und ihren Mitarbeitern von der **Forschungsgruppe „IT-Sicherheit und digitale Medien in der Bildung" der Technischen Hochschule Wildau** nachgegangen. Die Vorsitzende der Arbeitsgemeinschaft für Bildung der SPD-LDS *Martina Mieritz* lud zu diesem Treffen ein, bei dem es darum ging, wie sich mithilfe analoger und digitaler Methoden das Bewusstsein für Informationssicherheit in der digitalen Welt fördern lässt.
Der SPD-Arbeitskreis nutzte den fachlichen Austausch mit den Wildauer Wissenschaftlern vor dem Hintergrund, dass in den ab 2017/18 neu geltenden schulischen Rahmenlehrplänen die Medienbildung als Querschnittsthema in allen Unterrichtsfächern dazu gehört. Der Datenschutz ist ein wesentlicher Bestandteil der Medienbildung. Auch die Volkshochschule und andere Bildungsträger bieten Kurse zur Sicherheit im Umgang mit digitalen Medien an.
„Insgesamt gibt es aber noch kein einheitliches und ausfinanziertes Medienbildungskonzept, was alle Gesellschaftsgruppen von Junior bis Senior umfassend schult und damit einer digitalen Spaltung entgegenwirkt", erklärte *Martina Mieritz*.
Mit der fortschreitenden Digitalisierung werden die Kompetenzen zur Sicherung sensibler Informationen für alle Gesellschaftsgruppen zu Hause und unterwegs immer wichtiger. Dies unterstreichen auch die Ergebnisse einer aktuellen Befragung zu Informationssicherheitsbewusstsein und -kenntnisse der Studierenden der TH Wildau. Wie auf innovative Weise mit spielerischen analogen und digitalen Lernszenarien Bewusstsein für Informationssicherheit und entsprechende Verhaltensweisen gefördert werden können, zeigten die von *Professorin Scholl* präsentierten Projektbeispiele in der **IT-Security-Arena**, dem Trainingszentrum für Informationssicherheit. Zudem bietet das Team im Rahmen des Projektes „**SecAware4job – Informationssicherheitsbewusstsein für den Berufseinstieg**" eine berufsorientierte Zusatzqualifikation für Studierende an. Die innovative Weiterbildung zur Stärkung des Bewusstseins und der Kompetenzen bezüglich Informations- und insbesondere IT-Sicherheit wird von der Horst Görtz Stiftung unterstützt.
„Der Zweiklang aus digitalen und analogen Simulationen ermöglicht einen interaktiven Ansatz, um wirkungsvolle Schutzmaßnahmen verständlich zu vermitteln", lobte *Eric Makswitat*, Sprecher des Arbeitskreises.
Wer Interesse am Thema, den innovativen Ideen und dem ganz anders ausgestatteten Medienraum der Arbeitsgruppe um *Professorin Scholl* gefunden hat, kann am 28. Mai 2016 beim **Hochschulinformationstag auf dem Campus der TH Wildau** auch dort hineinschnuppern. An diesem Tag haben alle Besucher die Möglichkeit, die erprobten Methoden selbst einmal zu testen.
Überprüfen Sie Ihr Informationssicherheitsbewusstsein und Ihre Medienkompetenz! Auch Medienvertreter sind dazu herzlich eingeladen.

Fachliche Ansprechpartnerin:
Prof. Dr. Margit Scholl
Fachgebiet Wirtschafts- und Verwaltungsinformatik
Tel. +49 3375 508-917
margit.scholl@th-wildau.de

Dipl.-Ing. Bernd Schlütter
Kommunikation und Medien
bernd.schluetter@th-wildau.de

Zurück

Diesen Artikel auf MyNewsDesk anzeigen »

Pressemitteilungen

50 Elemente in dieser Kategorie

Im Fokus der TH-Forschung: „Social Engineering" – ein noch weitgehend unbekanntes Phänomen zum Datenklau

veröffentlicht 25.10.2016 09:11 Uhr von Bernd Schlütter

Das Team „Wirtschaft-/Verwaltungsinformatik und Digitale Medien" von Forschungsprofessorin Dr. Margit Scholl am Fachbereich Wirtschaft, Informatik, Recht untersucht das noch weitgehend unbekannte Phänomen "Social Engineering". Hacker wollen auf diesem Wege das Vertrauen von Mitarbeiterinnen oder Mitarbeitern ausnutzen, um ihnen sensible Daten wie Passwörter und Zugangscodes zu entlocken.

„Was haben zwischenmenschliche Kontakte im Unternehmensalltag mit Datensicherheit zu tun?" Dieser Frage geht das Team „Wirtschaft-/Verwaltungsinformatik und Digitale Medien" von Forschungsprofessorin Dr. Margit Scholl am Fachbereich Wirtschaft, Informatik, Recht der Technischen Hochschule Wildau nach.
Im Rahmen des von der Horst Görtz Stiftung geförderten Projektes „Informationssicherheitsbewusstsein für den Berufseinstieg" (SecAware4job) veranstaltete die Forschungsgruppe dazu einen Kreativworkshop. Im Mittelpunkt stand das Thema „Social Engineering" (SE).
Bei diesem neuen Phänomen von Angriffen auf Informationen oder IT-Systeme versuchen Hacker, zum Beispiel durch geschickte, fachlich relevante Fragestellungen während eines Telefonanrufs das Vertrauen von Mitarbeiterinnen oder Mitarbeitern zu gewinnen und ihnen nebenbei sensible Daten wie Passwörter und Zugangscodes zu entlocken. Dabei tritt der Angreifer nicht immer erkennbar auf. Oft erfährt das Opfer niemals, dass es getäuscht und ausgenutzt wurde.
„Die Bedeutung von Informationssicherheit ist zwar in Unternehmen, Einrichtungen und Verwaltungen grundsätzlich bekannt", erläutert Professorin Scholl. „Aber viele Mitarbeiterinnen und Mitarbeitern verkennen leider häufig die realen Gefährdungen."
Um das individuelle Verhalten zu schulen und an den aktuellen Erfordernissen der Informationssicherheit auszurichten, entwickelt die Forschungsgruppe spielbasierte (Lern-)Szenarien für Schulungsmaßnahmen. Dabei werden solche Angriffe simuliert, um die Teilnehmerinnen und Teilnehmer zu sensibilisieren – nicht in „grauer" Theorie sondern mit praxisnahen Formen, die auch Spaß machen.
Im Kreativworkshop wurden neue Ideen und Stories für zwei unterschiedliche Spielszenarien entwickelt und diskutiert. Dabei geht es um ein ereignisorientiertes Tischspiel und ein rollenbasiertes Spiel für Studierende bzw. Beschäftigte in kleinen und mittleren Unternehmen. Die Prototypen sollen im Jahr 2017 vorgestellt und in einer Testreihe erprobt werden.

Fachliche Ansprechpartnerin:
Prof. Dr. Margit Scholl
Forschungsgruppe Wirtschafts-/Verwaltungsinformatik und Digitale Medien
Tel. +49 3375 508-917
margit.scholl@th-wildau.de

Dipl.-Ing. Bernd Schlütter
Kommunikation und Medien
bernd.schluetter@th-wildau.de

Zurück

Diesen Artikel auf MyNewsDesk anzeigen »

Pressemitteilungen

50 Elemente in dieser Kategorie

Serious Games zur Informationssicherheit an der TH Wildau: Simulation und Tests zu den Themen „Datenschutz" und „Social Engineering"

veröffentlicht 09.05.2017 16:53 Uhr von Bernd Schlütter

In der „IT Security Arena", dem Trainingszentrum für Informationssicherheit der Technischen Hochschule Wildau, werden unter anderem Lernszenarien und didaktische Spiele zum Umgang mit sensiblen persönlichen und Geschäftsdaten entwickelt. Bei einem Kreativworkshop wurden die Prototypen eines neuen Brettspiels zum Thema Datenschutz und eines Rollenspiels zum Thema Social Engineering erprobt.

In der **„IT Security Arena**", dem **Trainingszentrum für Informationssicherheit** von *Forschungsprofessorin Dr. Margit Scholl*, werden unter anderem **Lernszenarien und didaktische Spiele zum Umgang mit sensiblen persönlichen und Geschäftsdaten** entwickelt. Ziel ist es, sicherheitsrelevante Herausforderungen anschaulich zu verdeutlichen und möglichen individuellen Fehlleistungen beispielsweise durch Leichtgläubigkeit oder Hilfsbereitschaft vorzubeugen. Die Forschungsergebnisse fließen in die akademische Lehre, aber auch in die Weiterbildungsangebote der TH Wildau für Unternehmen und Institutionen ein.
Am Samstag, dem 29. April 2017, fand der dritte **Kreativworkshop** im Rahmen des von der Horst Görtz Stiftung geförderten Projektes „SecAware4job" statt. Mitglieder des Projektteams erprobten dabei gemeinsam mit unabhängigen Testpersonen die Prototypen eines Brettspiels zum Thema Datenschutz und eines Rollenspiels zum Thema Social Engineering.
Didaktisches Ziel des neuen **Brettspiel**s ist es, den Teilnehmenden alltägliche Situationen bewusst zu machen, bei denen sie personenbezogene oder personenbeziehbare Daten von sich preisgeben, z.B. bei der Art der Bezahlung beim Online-Buchkauf oder bei der Buchung eines Hotelzimmers für die nächste Dienstreise. Da das Thema „**Social Engineering**" vielen noch nicht als Angriffsszenario bekannt ist, greift das **Rollenspiel** Alltags-Szenarien auf, die menschliche Eigenschaften („Einfalltore") verdeutlichen, die zur unbewussten Preisgabe von sensiblen Informationen führen können. Im Mittelpunkt steht dabei das teilweise unbekümmerte Verhalten beim Kommunizieren in der Öffentlichkeit mittels Smartphone oder Tablet-PC.
Das Projektteam erhielt beim „Spiele-Samstag" an der TH Wildau von den unabhängigen Testern wertvolle Hinweise, insbesondere bezüglich der Verringerung der Komplexität des Rollenspiels und der Verbesserung der Antwortmöglichkeiten im Brettspiel. Bis zum Ende der Projektlaufzeit von SecAware4job imAugust 2017werden die Spielszenarien weiter überarbeitet, so dass sie zukünftig in Schulungsmaßnahmen zur Sensibilisierung für Informationssicherheit eingesetzt werden können.

Fachliche Ansprechpartnerin:
Forschungsprofessorin Dr. Margit Scholl
Fachgebiet Wirtschafts- und Verwaltungsinformatik
Tel. +49 3375 508-917
margit-scholl@th-wildau.de

Dipl.-Ing. Bernd Schlütter
Kommunikation und Medien
bernd.schluetter@th-wildau.de

Zurück

Diesen Artikel auf MyNewsDesk anzeigen »

Spielen für mehr Sicherheit

Projekt für bewussten Internet-Umgang

Geht es um Sicherheitsfragen im IT-Bereich, dann ist Margit Scholl die erste Ansprechpartnerin. Die Forschungsprofessorin der Technischen Hochschule Wildau hat nicht nur die „IT Security Arena" als Trainingszentrum für Informationssicherheit aufgebaut, sie bildet auch mit ihrem Team IT-Sicherheitsbeauftragte aus, zum Beispiel für öffentliche Verwaltungen. Seit kurzem beteiligt sie sich mit ihrem Team an einem internationalen Forschungsprojekt, bei dem in der Arbeitswelt gefragte Kompetenzen konkret ermittelt werden sollen, um diese künftig sinnvoll in Lehrinhalte an Hochschulen einfließen zu lassen. Kurz vor dem Abschluss steht ein weiteres Projekt der Professorin für Wirtschafts- und Verwaltungsinformatik: „SecAware4job", gefördert von der Horst-Görtz-Stiftung. Studierende sollen – so das Ziel – ein größeres Bewusstsein für das Thema Informationssicherheit erhalten, um für den Berufseinstieg dahingehend besser gewappnet zu sein.

Gerade fand dafür noch einmal ein Kreativworkshop statt. Prototypen eines Brettspiels wurden dabei erprobt. Beteiligt waren Mitglieder des Projektteams sowie unabhängige Testpersonen. Die Teilnehmer begreifen spielerisch einiges über das Thema Datenschutz, lernen während einer Partie, wie viel sie beispielsweise bei Online-Käufen über sich preisgeben. Alltägliche Situationen, über deren mögliche Nachwirkung kaum noch jemand nachdenkt. Ziel ist, solche Spiele später in Schulungen für Studierende und Mitarbeiter einzusetzen, um so noch intensiver für das Thema Informationssicherheit zu sensibilisieren.

Entwickelt wurde außerdem ein Rollenspiel zum Thema Social Engineering. Auch damit kann den Teilnehmern bewusster werden, welche Gefahren das permanente Kommunizieren via Smartphone in der Öffentlichkeit birgt. Dank der Eindrücke der Tester kann das Team um Margit Scholl den Spielszenarien nun den letzten Schliff verpassen, damit sie bald eingesetzt werden können. *kg*

Margit Scholl ist an der TH Professorin für Wirtschafts- und Verwaltungsinformatik. FOTO: K. GRUNOW

Internationales Flair

Einen „Internationalen Nachmittag" veranstaltet die Technische Hochschule zweimal im Jahr. Zahlreiche der Studierenden aus aller Welt stellen dann ihre Heimatländer vor, kochen spezielle Gerichte und zeigen typische traditionelle Trachten. Die Neugier beim Internationalen Nachmittag in dieser Woche war wieder groß. Nicht nur andere Studierende, auch Hochschulmitarbeiterinnen und -mitarbeiter schauten gern in der Cafeteria vorbei, um die länderspezifischen Stände zu besuchen. Derzeit sind 942 Studentinnen und Studenten aus dem Ausland eingeschrieben, das sind 24,9 Prozent aller Studierenden. Internationale Studierende kommen vor allem aus Lateinamerika, Europa, Afrika, Ost- und Südasien sowie von der arabischen Halbinsel. FOTO: TH WILDAU/BERND SCHLÜTER

Kind und Karriere

Der Senat der Technischen Hochschule Wildau hat ein neues Gleichstellungskonzept verabschiedet

Von Karen Grunow

Das neue Gleichstellungskonzept ist für uns das Arbeitsprogramm für die nächsten vier Jahre", sagt Olga Rösch, Professorin für Interkulturelle Kommunikation an der Technischen Hochschule Wildau und Gleichstellungsbeauftragte. Nun wurde das Konzept vom Senat der TH verabschiedet. Eine Projektgruppe, der neben Ulrike Tippe als Vertreterin der Hochschulleitung auch Professorinnen und Professoren verschiedener Studiengänge, ein Student und mit Andrea Schmid außerdem die Koordinatorin der „Familiengerechten Hochschule" angehörten, erarbeiteten dieses Konzept mit Olga Rösch. „Wir folgen damit der gesetzlichen Verpflichtung, die jede Hochschule hat", berichtet diese.

„Das Konzept orientiert sich am heutigen Stand der Gleichstellungspolitik im Lande und in der Bundespolitik." Grundsätzlich, so die Professorin, habe sich nach und nach in der Gleichstellungsidee vieles zum Besseren verändert. Ein wichtiges Vorbild sind für sie die strukturellen Gleichstellungsstandards der Deutschen Forschungsgemeinschaft (DFG). Durchgängigkeit, Transparenz, Chancengleichheit und Leistungsgerechtigkeit sind die darin formulierten wesentlichen Punkte. Bei Berufungsverfahren an der Hochschule wird Olga Rösch immer beteiligt. Es sei nicht immer einfach, ihre Anliegen als Gleichstellungsbeauftragte durchzusetzen. Am Ende sollten einzig die Qualifikation und Leistung zählen, nicht das Geschlecht. „Bei den Kollegen und Bewerbern soll das Gefühl entstehen können, dass gerecht gehandelt wird", sagt sie.

> Das Konzept orientiert sich am heutigen Stand der Gleichstellungspolitik.
>
> **Olga Rösch,** TH-Gleichstellungsbeauftragte

Die Vereinbarkeit von Familie, Studium und Beruf ist seit 2011 fest im Leitbild der Hochschule verankert. Sämtliche Professorenstellen werden nun auch als „teilzeitgeeignet" ausgeschrieben. An der TH ist Familienfreundlichkeit längst ein großes Thema. „Ich bin sehr glücklich darüber", sagt Olga Rösch. Mehr Studentinnen für die so genannten Mint-Fächer – Mathematik, Informatik, Naturwissenschaft und Technik – zu gewinnen und Frauen in den Bereich besser zu fördern, ist auch ein Aspekt der Gleichstellungsarbeit. Etwa ein Viertel der Studierenden im Fachbereich Ingenieur- und Naturwissenschaften sind Frauen. Ein Viertel aller Professorenstellen der TH sind mit Frauen besetzt. Ähnlich ist der Anteil akademischer Mitarbeiterinnen an der Hochschule. Ein „ausgewogenes Verhältnis von Frauen und Männern und Qualifizierungsmöglichkeiten für Absolventinnen und Absolventen" gehört deshalb zu den im neuen Gleichstellungskonzept erklärten Zielen. „Es ist eine Fortsetzung der Gleichstellungsarbeit", verweist Olga Rösch auf das erste, von ihrer Vorgängerin 2008 entwickelte Konzept und bereits 1997 an der TH verabschiedete Richtlinien zur Frauenförderung.

Seit 2009 bereits kümmert sich Olga Rösch nun intensiv um das große Thema. Sie ist bereits seit 1995 an der 1991 begründeten Hochschule. Dem damaligen Gründungsdirektor Wilfried Ärlt hatte sie ein Konzept für ein Sprachenzentrum vorgelegt, das dann im April 1995 gegründet und von ihr acht Jahre lang geleitet wurde. Seit 2001 ist sie Professorin für Interkulturelle Kommunikation, hat dazu eine Wildauer Schriftenreihe entwickelt und Tagungen zum Thema „Technik und Kultur" organisiert. Sie engagiert sich in den Präsidien der Bundesvereinigung und des Landesverbandes des Hochschullehrerbundes und ist mit anderen Gleichstellungsbeauftragten an Hochschulen vernetzt.

Nach der Wende wurde sie mit eigentlich doch längst überholten, in der alten Bundesrepublik damals aber durchaus noch etablierten Rollenbildern konfrontiert. Sie habe gespürt, dass sie als zweifache Mutter und erfolgreiche, promovierte Wissenschaftlerin für westdeutsche Verhältnisse eine ziemlich untypische Erscheinung war. Kind oder Karriere, das sei die Entscheidung gewesen, mit der Frauen sich auch zu der Zeit noch auseinandersetzen mussten. Und auch heute noch, erzählt Olga Rösch, erlebe sie es immer wieder mal, dass talentierte junge Ingenieurinnen den Weg in ein erfolgreiches Berufsleben nicht finden, weil sie dafür eben nicht auf eine Familie verzichten wollen. „In Zusammenarbeit mit der Familienbeauftragten Andrea Schmid setze ich mich dafür ein, dass Frauen, allen voran die Studentinnen, Beruf und Familie vereinbaren können."

IN KÜRZE

Dreidimensionale Vermessung

Mit einer speziellen Technik zur 3D-Vermessung von Frachtgut ist die Technische Hochschule Wildau derzeit auf der Messe „transport logistic 2017" präsent. Entwickelt wurde das sehr präzise und schnelle System im „CVision:Lab", das von Telematik-Professor Ralf Vandenhouten geleitet wird. Während die bisher in der Logistikbranche üblichen Systeme oft sehr wartungsintensiv sind, ist das Wildauer System nahezu wartungsfrei und lässt sich leicht in vorhandene Strukturen integrieren.

Antibiotika Thema bei Sonntagsvorlesung

Oliver Steinberg, Oberarzt in der Abteilung für Innere Medizin im Königs Wusterhausener Achenbach-Krankenhaus, spricht bei der nächsten Medizinischen Sonntagsvorlesung an der TH Wildau am 14. Mai über „Antibiotic Stewardship. Neue Wege im Umgang mit Antibiotika". Die kostenlose Vorlesungsreihe wird veranstaltet von der Klinikum Dahme-Spreewald GmbH. Der Vortrag beginnt 11 Uhr im großen Hörsaal in Halle 14.

Dritte Wildauer Logistikwerkstatt

Über zukunftsweisende Lösungen in der Logistik und alternative Technologien wird bei der 3. Wildauer Logistikwerkstatt informiert, die am 17. und 18. Mai an der Hochschule stattfindet. Vorgestellt werden auch Industrieprojekte mit kooperierenden Unternehmen und neue Lehrinhalte. Weitere Informationen gibt es unter www.th-wildau.de/logistikwerkstatt

Strahlentherapie im Seniorenseminar

Über „Die Welt der Strahlentherapie" spricht Sebastian Exner, Assistenzarzt am Centrum Tumormedizin der Klinik für Radioonkologie und Strahlentherapie der Charité Berlin, am 19. Mai beim Seniorenseminar der TH. Los geht es um 15 Uhr im großen Hörsaal in Halle 14.

Infotag für Studieninteressierte

Beim Hochschulinformationstag am 20. Mai von 10.30 bis 16 Uhr ist der gesamte Campus für Interessierte geöffnet, es gibt Infoveranstaltungen zu konkreten Studieninhalten, aber auch zum Thema Studium allgemein, zudem Angebote für große und kleine Begleiter potenzieller künftiger Studenten. Detailliertes Infotag-Programm unter www.th-wildau.de/hit

ZAHL DER WOCHE

132

Stellenangebote bundesweit listet die Jobbörse Stellenticket auf der Homepage der Technischen Hochschule derzeit auf. Darunter sind Angebote für Praktika, aber auch Festanstellungen für Absolventen.

Von Roboter bis Kreativlabor

Die Technische Hochschule ist auch beim 5. Potsdamer Tag der Wissenschaften dabei

Mit gleich zwei interessanten Themen wird die Technische Hochschule Wildau beim 5. Potsdamer Tag der Wissenschaften am kommenden Sonnabend dabei sein: „Wie humanoide Roboter das Leben leichter machen" und „Kreativlabor ‚ViNN:Lab'". Vom Schmuckdesign bis zum Möbelstück."

Von 13 bis 20 Uhr kann dann der Wissenschaftsstandort Potsdam-Golm erkundet werden. Die dort angesiedelten Forschungsinstitute, das Landeshauptarchiv sowie die Potsdamer Uni beteiligen sich. Mittendrin gibt es das Forscher-Camp, in dem zahlreiche Mitmach-Aktionen angeboten werden, von denen sich viele explizit auch an Kinder richten.

Mit humanoiden Robotern der TH Wildau wird Janine Breßler vor Ort sein, um zu zeigen, dass diese beispielsweise auch in der häuslichen Pflege einsetzbar sind oder Gebärdensprache vermitteln können. Außerdem wird sie den TH-Studiengang Telematik vorstellen.

Für die Präsentation des TH-Kreativlabors wird unter anderem ein 3D-Drucker im Einsatz sein. Patrick Grabasch wird das erklären und auch davon berichten, dass im „ViNN:Lab" sogar schon Ausstellungsstücke für Museen entstanden sind. Auch an diesem TH-Stand dürfen die Besucher einiges ausprobieren.

Das komplette Programm des 5. Potsdamer Tages der Wissenschaften gibt es im Internet unter www.potsdamertagderwissenschaften.de. Neben Vorträgen und geführten Rundgängen gibt es auch Live-Musik. In den Forschungsinstituten werden auch zahlreiche für Kinder geeignete Veranstaltungen ausgerichtet. *kg*

Einer der humanoiden Roboter der TH Wildau, die in Potsdam vorgestellt werden. Dieser wurde als DJ programmiert. FOTO: GRUNOW