WISSENSCHAFTLICHE BEITRÄGE 2017
21. Jahrgang (2017)
ISSN: 0949-8214

Wiss Beitr TH Wildau 21:23–30
doi: 10.15771/0949-8214_2017_3
Februar 2017

Das Projekt SecAware4job: Auf spielerischem Weg zu erhöhtem Informationssicherheitsbewusstsein für den Berufseinstieg

Margit Scholl, Frauke Fuhrmann, Denis Edich, Peter Ehrlich, Benjamin Leiner, Robin Scholl, Peter Koppatz*

Zusammenfassung

Die fortschreitende Digitalisierung durchdringt zunehmend alle Lebensbereiche und erfordert ein stärkeres Bewusstsein sowie verbesserte Kompetenzen im Bereich der Informationssicherheit – sowohl im Privat- als auch im Arbeitsleben. Das Projekt SecAware4job dient der Steigerung des Informationssicherheitsbewusstseins von Studierenden an der TH Wildau. Als zukünftige Mitarbeiter/innen sollen die Studierenden spielerisch für Informationssicherheit sensibilisiert werden und entsprechende Kenntnisse für ihren Berufseinstieg erwerben. Dieser Beitrag skizziert Methoden und Übungen, die in dem Fach Sensibilisierung für Informationssicherheit zur Anwendung kommen. Diese innovativen Lehr- und Lernmethoden basieren auf dem Game-based-Learning-Ansatz, denn durch die Einbeziehung spielerischer Elemente kann insbesondere die Motivation gefördert werden und lassen sich Verhaltensänderungen anregen. Damit widmet sich SecAware4job aktuellen Forschungsfragen zum spielebasierten und kooperativen Lernen im Bereich der Awareness/Bewusstseins-Förderung. Es wird angestrebt, Sensibilisierung für Informationssicherheit als Wahlpflichtfach in allen Studiengängen der TH Wildau zu etablieren.

Abstract

The constant proliferation of digitalization is increasingly penetrating all areas of life and requires a greater awareness and improved skills for information security – both in private and in working life. The project SecAware4job aims at increasing the information security awareness of students at the Technical University of Applied Sciences (TUAS) Wildau. As prospective employees, students should become aware of information security in a playful way, and they should acquire the appropriate skills and knowledge for their career entry. This paper (a "work in progress") outlines methods and exercises applied in the lecture Sensitization for Information Security. These innovative teaching and learning methods are based on the game-based learning approach because the inclusion of playful elements is particularly suitable to develop motivation and encourage behavioural change. Thereby, SecAware4job addresses current research issues of playful and cooperative learning within the area of raising awareness. We aim at establishing Sensitization for Information Security as a compulsory elective subject in all courses at the TUAS Wildau.

1. Einleitung

Aufgrund der weltweit voranschreitenden Digitalisierung aller wirtschaftlichen und gesellschaftlichen Bereiche durchzieht die Informationstechnik (IT) heutzutage nahezu alle Lebensbereiche. Während jedoch die meisten Menschen mit der oberflächlichen Nutzung vertraut sind, bieten die zunehmende Verbreitung und Komplexität von Soft- und Hardware eine stetig wachsende Anzahl an Möglichkeiten zu deren Missbrauch. Da diese Möglichkeiten sowohl technischer (z. B. Hacking) als auch zwischenmenschlicher (z. B. Social Engineering) Natur sein können, sind ein höheres Bewusstsein und verbesserte Kenntnisse hinsichtlich der mit der Digitalisierung einhergehenden Gefahren und entsprechenden Schutzmaßnahmen für Privat- und Arbeitsleben unerlässlich. Informationssicherheit ist keineswegs nur eine Aufgabe von IT-Fachkräften. Vielmehr sind alle Nutzergruppen angesprochen und sollten diesbezügliches Bewusstsein und entsprechende Kompetenzen zum Schutz sensibler Informationen aufweisen.
Da die Mehrheit der Vorfälle von Verletzung der Informations- oder Datensicherheit auf unbewusstes oder bewusstes Verschulden von Mitarbeiter/innen zurückzuführen ist (Guo et al. 2011, EnBW et al. 2008, DSV-Gruppe et al. 2006), kann Sensibilisierung und die Vermittlung von Kompetenzen im Hinblick auf Informationssicherheit nicht früh genug beginnen. Die Technische Hochschule Wildau (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 die Vorbereitung der Studierenden auf den Berufseinstieg von zentraler Bedeutung. Die Ausbildung der Studierenden als zukünftige Mitarbeiter/

* korrespondierende Autorin

innen 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 die Sensibilisierung für Informationssicherheit. Dies betrifft vor allem auch die Studierenden der weniger technik-affinen Studiengänge wie Betriebswirtschaftslehre (BWL) und Verwaltungswissenschaft.

Ziel des von der Horst Görtz Stiftung finanzierten Forschungsprojektes „Informationssicherheitsbewusstsein für den Berufseinstieg: SecAware4job" ist es daher, bei den Studierenden der TH Wildau, insbesondere der nicht technischen Studiengänge, ein stärkeres Bewusstsein für Informationssicherheit und Datenschutz unter besonderem Einsatz von didaktischen Kreativmethoden – spielebasierten analogen und digitalen Lernszenarien – zu entwickeln. So sollen sie als zukünftige Mitarbeiter/innen für die alltäglichen Herausforderungen des Schutzes von sensiblen Informationen und der digitalen Infrastruktur sensibilisiert werden und ihr Sicherheitsbewusstsein soll fundiert gefördert werden.

2. Internationaler Forschungsstand

2.1 Game-based Learning

Traditionell wird Game-based Learning (GBL) als pädagogische Methode angewandt, um Lernende zu motivieren und sie für Lernprozesse zu begeistern (Hsu et al. 2008). Digitales Game-based Learning (DGBL) ist durch (mobile) Hightech-Geräte und Software die moderne Möglichkeit, den Lernenden neue Erfahrungen näherzubringen. Nach Hsu et al. (2008) haben beide GBL-Strategien ihre eigenen Vorteile und die Schwierigkeit liegt darin, diese beiden Arten von Lernstrategien zu verbinden und ein ausgewogenes Verhältnis zwischen ihnen zu finden. Die Betrachtung des internationalen Forschungsstandes zeigt, dass keine konsequente Zuordnung GBL = analog und DGBL = digital vorgenommen wird: So bezieht sich die aktuelle internationale Forschung überwiegend auf „digital serious games" und auch unter dem Begriff GBL finden sich Forschungsergebnisse, die digitale Spielszenarien zum Inhalt haben. In SecAware4job wird konsequent zwischen GBL und DGBL unterschieden und beide Lernstrategien werden mit Studierenden sowohl getrennt als auch in ihrer Kombination erforscht (Scholl & Fuhrmann 2016a). Dies stellt eine Besonderheit im internationalen Vergleich dar. Die kombinierte Anwendung von analogen und digitalen spielebasierten Lernszenarien nutzt die Vorteile jeder Lernstrategie aus und sollte in der Summe zu einem höheren Lernerfolg führen. Die Vorteile analoger Lernszenarien bestehen in der gemeinsamen Lösung im Team, im dadurch möglich werdenden sozialen Erfahrungs- und Wissensaustausch vor Ort sowie in der Stärkung der Team- und Kommunikationsfähigkeiten. Digitale Lernszenarien dienen der individuellen Vertiefung der Lerninhalte. Dies kann orts- und zeitunabhängig erfolgen und orientiert sich somit an der Lebenssituation sowie den Bedürfnissen und Wissensständen der Lernenden.

Unabhängig von der genauen Zuordnung hat sich GBL/DGBL international als anerkannte Lehr- und Lernmethode im Bildungsbereich (Hamari et al. 2016, Hsiao & Chen 2016, Abdul Jabbar & Felicia 2015, Spires 2015) und in der Weiterbildung (Zweck et al. 2015, Helisch & Pokoyski 2009) etabliert. Gleichwohl besteht nach wie vor Forschungsbedarf im Hinblick auf die Wirkungsweise, auf die Lernleistung (Chen & Law 2016, Eseryel et al. 2013) und das Design von Lernarrangements (Halverson et al. 2015). Die Befürworter von GBL argumentieren, dass Lernspiele die Teilnehmenden stärker involvieren und ihr Engagement fördern und somit zu besseren Lernergebnissen führen. Denn sie ermöglichen aktives, erlebnisorientiertes Lernen durch Ausprobieren, unmittelbares Feedback zum Lernfortschritt, Wiederholen und die Möglichkeit, aus eigenen Fehlern zu lernen (Zweck et al. 2015, Institute of Play 2013, Helisch & Pokoyski 2009). Darüber hinaus üben nach Le et al. (2013) hochwertig produzierte, digitale Spiele eine große Faszinationskraft auf Spielende aus und virtuelle Explorationsräume sind für die Initiierung von Lernprozessen gut geeignet.

Insbesondere die Förderung der Motivation und die Anregung von Verhaltensänderungen sind angestrebte Ziele. Studienergebnisse legen nahe, dass die Motivation, das Engagement und die Entwicklung von Problemlösungskompetenzen stark von der Natur und Gestaltung der Spielaufgaben beeinflusst werden (Eseryel et al. 2013). Shi & Shih (2015) entwickelten daher für DGBL ein „Game-Based Learning Design Model", das sich aus elf Faktoren zusammensetzt: Spielziele, Spielmechanismus, Spielfantasie, Spielwert, Interaktion, Freiheit, Erzählung, Empfindung, Herausforderungen, Sozialität und Mysterien.

Des Weiteren werden die Effektivität spielerischer Elemente wie Feedbackfunktionen und Wettbewerbskomponenten empirisch untersucht. So sollen Rückmeldungen eine tiefe kognitive Verarbeitung auslösen und die Erinnerung von Lernenden verbessern, was zum besseren Lernen beiträgt (Erhel & Jamet 2013, Sweller et al. 1998, Leutner 1993). Allerdings ergeben Untersuchungen verschiedener Spielarten und Feedbacktypen bislang keine belastbaren Wirkungsunterschiede (Tsai et al. 2015). Doch die Spielenden erfahren, was ihr Handeln bewirkt oder woran sie arbeiten müssen. Die Forschungsergebnisse zur Integration einer Wettbewerbskomponente sind ebenfalls nicht eindeutig: So führt in einem Experiment von Zaphiris et al. (2007) ein E-Learning-Spiel mit Wettbewerbskontext im Vergleich zu einem nicht kompetitiven Spiel zu einer niedrigeren Lernverbesserung. Abweichend davon zeigen die Untersuchungen von Admiraal et al. (2011), dass Wettbewerb zwischen Teams sich positiv auf den Lernerfolg auswirkt.

Plass et al. (2015) reflektieren Lerntheorien und kommen zu dem Schluss, dass eine Kombination von kognitiven, affektiven, motivationalen und soziokulturellen Perspektiven für das Spieldesign und die Spielforschung notwendig ist, um in vollem Umfang zu erfassen, was Spiele für das Lernen zu bieten haben. Die größte Herausforderung für das Instruktions- und Spieldesign liegt nach Le et al. (2013) in der Integration von Lerninhalten und Spielmechanik. Somit ist es nicht einfach, interessante und wirksame spielebasierte Lernszenarien zu ent-

wickeln. Nach einem systematischen Literaturreview zu GBL kommen Abdul Jabbar & Felicia (2015) zu dem Ergebnis, dass das Spieldesign mit unterschiedlichen Lerntools und interessanten Materialien begleitet sein muss, die es den Lernenden ermöglichen, die Spiel- und Lernaktivitäten in Übereinstimmung mit ihren Bedürfnissen und Fähigkeiten zu erkunden. Eine besondere Schwierigkeit stellt das Entwerfen von Spielszenen in Kombination mit einem konkreten Kursunterricht und Curriculum dar (Lai et al. 2014). Als eine der zentralen Herausforderungen bleibt, die Lernenden dabei zu unterstützen, die Verbindungen zwischen dem Wissen, das im Spiel gelernt wird, und dem Wissen, das unterrichtet wird, zu ziehen. Damit hängt die Fragestellung zusammen, wie viele Vorgaben bei gleichzeitig hohem Maß an (Eigen-) Engagement gemacht werden sollten (Barzilai & Blau 2014). Sowohl Feedback als auch Vorgaben sollten abhängig von den Lernanforderungen in verschiedenen Formen zur Verfügung stehen (Abdul Jabbar & Felicia 2015).

2.2 Sensibilisierung für Informationssicherheit

Die aufgezeigten Forschungsbedarfe im Hinblick auf (D)GBL werden in SecAware4job für die Sensibilisierung für Informationssicherheit und das Erlernen entsprechender Kompetenzen adressiert (siehe Forschungsfragen in Kapitel 3). Studien zeigen, dass die zur Stärkung des Bewusstseins (Awareness) und der Kompetenzen für Informations- und IT-Sicherheit oftmals angewandten Sensibilisierungs- und Schulungsmaßnahmen wie Awarenesskampagnen (z. B. Flyer, Broschüren, Poster, Filme), rein IT-basierte Schulungen (z. B. web-basierte Trainings, Videospiele) oder die alleinige Weitergabe von Informationen in Vorträgen ineffektiv sind und zu keinem nachhaltigen Sicherheitsbewusstsein bei den Adressat/innen führen (Albrechtsen 2007, Cone et al. 2007, Straub & Welke 1998). Stattdessen sind Schulungsmaßnahmen, die Möglichkeiten für persönliche Kommunikation und zur Interaktion bieten, erfolgversprechend für die Förderung von Informationssicherheitsbewusstsein und das Auslösen von sicherheitskonformem Verhalten. Als Folge könnte sich auch die Akzeptanz entsprechender technischer, organisatorischer, individueller und administrativer Maßnahmen erhöhen (Albrechtsen 2007).
Aufgrund dieser Erkenntnisse wird in dem Fach Sensibilisierung für Informationssicherheit im Rahmen des Projektes SecAware4job ein integrativer Methodenmix – bestehend aus Präsenzveranstaltung mit Informationsinput, Erfahrungsaustausch, interaktiven Übungen sowie analogen und digitalen spielebasierten Lernszenarien – angewandt (s. Abb. 2 in Kapitel 3).

3. Methodischer Ansatz und Forschungsfragen

Die betriebliche Security und Privacy Awareness ist eine relativ junge Disziplin, die sich methodisch in drei Teildisziplinen einteilen lässt: erstens die lerntheoretischen Ansätze, bei denen die Wissens- und Know-how-Vermittlung im Vordergrund steht; zweitens die werblichen Ansätze, bei denen das Wollen bzw. die Mitwirkung durch Security Marketing und Emotionalisierung erhöht werden soll; drittens die systemischen Ansätze, die das Können adressieren, indem z. B. teamorientierte Anwendungen des erworbenen Wissens im konkreten, sozialen Umfeld gefördert werden. Das Projekt SecAware4job vereint, im Sinne von Blended Learning, diese drei Ansätze, um bei den Studierenden ein nachhaltiges Bewusstsein für Informationssicherheit zu erzielen (vgl. Abb. 2). Wir benennen diese Art des Methodenmixes als Ansatz 3.0 (Scholl et al. 2016a): 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.
Um das abstrakte und komplexe Thema Informationssicherheit mit all seinen Facetten (z. B. rechtliche Rahmenbedingungen, Normen & Standards, Schutzmaßnahmen, Konzepte) verständlich sowie greif- und erlebbar zu vermitteln, werden kreative, auf Spielemechanismen basierende Lehr- und Lernmethoden entwickelt und erprobt. Gemäß den oben zitierten Forschungserkenntnissen sollen die angewandten Methoden ausreichend Raum für persönlichen (Erfahrungs-) Austausch und Interaktion sowie das Sammeln eigener Erfahrungen bieten.
Da Studien gezeigt haben, dass die Beteiligung von Nutzer/innen bei der Entwicklung von Schulungsmaßnahmen für Informationssicherheit den Wissensaustausch und die Einhaltung von Informationssicherheit verbessert (SanNicolas-Rocca et al. 2014), sollen die Studierenden angeregt werden, selbst eine kreative Maßnahme zur Sensibilisierung für Informationssicherheit (weiter) zu entwickeln. Honoriert wird diese freiwillige Leistung mit einem Moderationszertifikat für Sensibilisierungsmaßnahmen im Bereich Informationssicherheit (Abb. 1, Stufe 1). Zudem erhalten die Studierenden im Rahmen des Projektes SecAware4job die Möglichkeit, in der jeweiligen Veranstaltung die Zertifikatstests des international anerkannten Europäischen

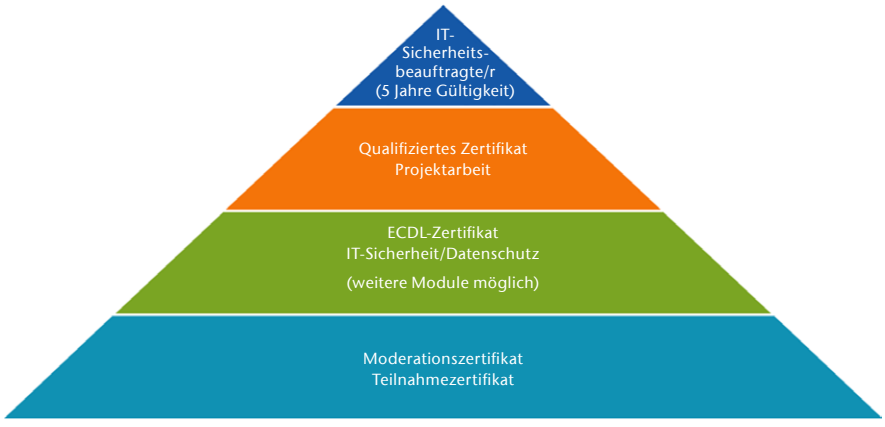

Abb. 1) Zertifizierungshierarchie für die im Projekt SecAware4job teilnehmenden Studierenden.

Computerführerscheins (ECDL) in den Modulen IT-Sicherheit und/oder Datenschutz zu absolvieren (Abb. 1, Stufe 2). Darüber hinaus können sich die Studierenden zusätzlich zum Absolvieren der umfangreichen Prüfung zum IT-Sicherheitsbeauftragten (IT-SiBe) nach Bundesakademie für öffentliche Verwaltung (BAköV)/Bundesamt für Sicherheit in der Informationstechnik (BSI) entschließen (Abb. 1, Stufe 3 und 4). Deren erfolgreicher Abschluss wird mit einem offiziellen, für fünf Jahre gültigen Zertifikat gekrönt. Diese Zertifikate belegen nachweislich die erworbenen Kompetenzen der Studierenden im Hinblick auf Informationssicherheit und sind für deren Berufseinstieg wertvoll. Sowohl der Erwerb der ECDL-Zertifikate als auch des IT-SiBe-Zertifikats werden im Rahmen von SecAware4job den Studierenden kostenfrei ermöglicht.
SecAware4job beinhaltet eine begleitende Forschung, die die Wirkung der eingesetzten Methoden und den Lernerfolg analysiert. Um diese Untersuchungen durchführen zu können, müssen zum einen Unterrichtsinhalte angepasst und zum anderen die Inhalte als neues Wahlpflichtfach (WPF) Sensibilisierung für Informationssicherheit in den Studiengängen etabliert werden. Im Sommersemester 2016 wurde ein erster Durchlauf als WPF im berufsbegleitenden BWL-Studiengang (BFG) durchgeführt. Die teilnehmenden Studierenden entschieden sich alle für die höchste Stufe der Zertifizierung zum IT-SiBe. Das Projekt befindet sich weiterhin in der Umsetzung. Der verfolgte Forschungsansatz (Abb. 2) orientiert sich dabei an den Zielgruppen, dem Kenntnisstand der Einzelnen, den organisatorischen Notwendigkeiten in Unternehmen und Verwaltungen sowie den technologischen Unterstützungsmöglichkeiten. Durch die Einbeziehung der teilnehmenden Studierenden in die Konzeption und Evaluation der spielebasierten Lernszenarien ist der Forschungsansatz sowohl partizipativ und klientenzentriert gestaltet als auch integrativ hinsichtlich der genutzten Methoden- und Medienvielfalt. Entsprechend der Projektlaufzeit wird der Forschungsansatz im Wintersemester 2016/17 mit dem Studiengang Kommunales Verwaltungsmanagement (KVR) und im Sommersemester 2017 erneut im BFG-Studiengang erprobt und praktisch umgesetzt.

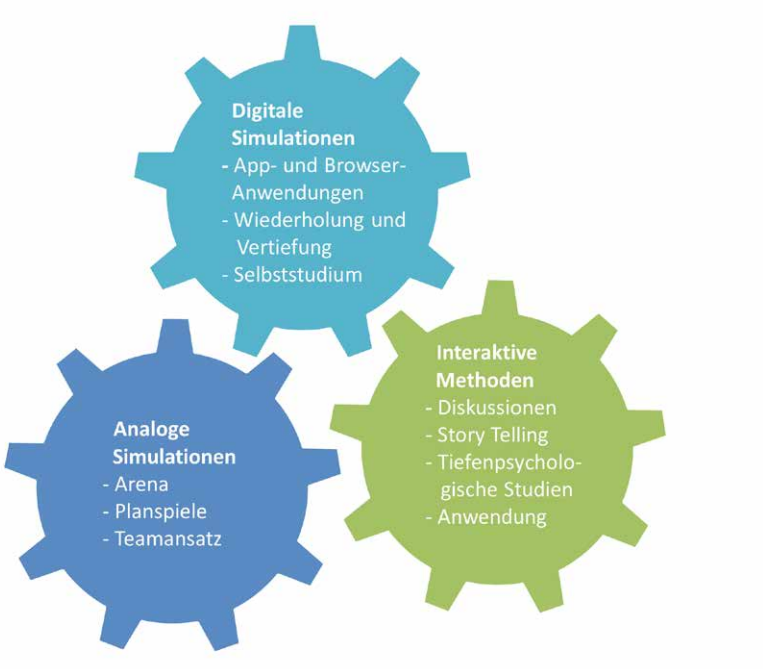

Abb. 2) Der in SecAware4job angewandte Methodenmix und Forschungsansatz.

Die mit dem Projekt verbundenen Forschungsfragen zur spielebasierten Vermittlung von Informationssicherheit basieren auf dem internationalen Forschungsstand zu (D)GBL (vgl. Kapitel 2) und entwickeln sich sukzessive im Projektverlauf. Sie können zum jetzigen Zeitpunkt noch nicht beantwortet werden.

Die Forschungsfragen (FF) lauten derzeit:

FF#1: Welche Faktoren des „Game-Based Learning Design Model" von Shi und Shih (2015) sollten in welcher Weise bei der Entwicklung und Anwendung (a) der analogen spielebasierten Lernszenarien und (b) der digitalen Varianten berücksichtigt werden?

FF#2: Durch welche spielerischen Elemente (z. B. Belohnung, Feedback, Wettbewerb) lässt sich (a) das Engagement, (b) die Motivation und (c) der Lernprozess der Studierenden fördern?

FF#3: Wie lassen sich (a) analoge und digitale spielebasierte Lernszenarien effektiv verbinden, so dass (b) ihre eigenständigen Einsatzbereiche sinnvoll erhalten werden?

FF#4: Wie lassen sich die spielebasierten Lernszenarien in ein zeitgemäßes Lehr- und Lernkonzept integrieren?

FF#5: Wie (a) motiviert sind die Studierenden, die angebotene Zertifizierungshierarchie zu absolvieren? Wie (b) erfolgreich absolvieren sie welche Stufe?

FF#6: Wie lassen sich (a) die Wirksamkeit der Lernszenarien sowie (b) der Lernerfolg und (c) das Informationssicherheitsbewusstsein der Lernenden messen?

4. Beispiele spielebasierter Lernszenarien

Im Folgenden werden Beispiele von auf Spielemechanismen basierenden Lehr- und Lernmethoden vorgestellt, die im Fach Sensibilisierung für Informationssicherheit eingesetzt werden. Sie wurden mehrheitlich im Rahmen des Projektes SecAware4job entwickelt.

Lerneinheit Strafgesetzbuch (StGB): Die Lerneinheit zu relevanten Paragraphen des Strafgesetzbuchs (StGB) orientiert sich an didaktisch-metho-

dischen Gesichtspunkten einer Hilfe zur Selbsthilfe bzw. -bildung. Dabei soll der Lerngegenstand so einfach und konkret wie möglich vermittelt werden, um den Studierenden praxisrelevante Bezüge aufzuzeigen, mit denen ein Erlernen des Gegenstandes auch ohne tiefreichende Vorkenntnisse möglich ist. Weiterhin soll die Einheit viele kommunikative und spielerische Methoden beinhalten, um zur Auseinandersetzung mit dem Thema zu motivieren. Als Vorbereitung sollen sich die Teilnehmenden mit den relevanten Paragraphen zum Thema Cybercrime und Informationssicherheit des StGB vertraut machen, indem sie nach aktuellen Fällen bzw. Urteilen recherchieren. Die Ergebnisse werden auf Moodle zur Verfügung gestellt, so dass jede/r Teilnehmer/in mit Hilfe ausgewählter Beispiele alle wichtigen Paragraphen verinnerlicht. Zudem wird vorab auf Moodle zu einer Diskussion der Fälle angeregt, die zu einer vertieften Auseinandersetzung führen kann. Zum Einstieg in die Unterrichtseinheit werden die Studierenden gebeten, die Lücken bei „geschwärzten“ Grafiken zu Cybercrime zu schätzen, z. B. welche Branchen am häufigsten von Angriffen betroffen sind. Hierdurch erhalten die Teilnehmenden einen Einblick in aktuelle Zahlen und Ausmaße des Themengebietes. Anschließend werden den Studierenden aktuelle Straffälle ausgeteilt. In Gruppen sollen sie diskutieren, welche Paragraphen des StGB jeweils betroffen sind. Am Ende werden die entsprechenden Urteile zu den Fällen als Musterlösung ausgegeben. Als Nachbereitung können Gitterrätsel, in welchen zentrale Begriffe der Paragraphen versteckt sind, gelöst werden. Die Musterlösungen können auf Moodle eingesehen werden.

ABC-Liste: Als Training für die Bildung von Assoziationen wichtiger Begriffe eines Themengebietes wird die „ABC-Liste“ eingesetzt (Birkenbihl 2004). Die Studierenden erhalten eine Liste mit allen Buchstaben des Alphabets und sollen zu jedem Buchstaben mindestens einen wichtigen Begriff zum Thema Informations-/IT-Sicherheit sowie Datenschutz/-sicherheit eintragen. Nach Birkenbihl (2004) kann und sollte jeder in kurzen Ruhepausen wie Wartezeiten diese Methode immer wieder anwenden. Je öfter die ABC-Liste zu einem bestimmten Thema gespielt wird, desto mehr entwickelt sich ein assoziatives Denken. Dies kann ad hoc und frei für Statements zum Thema abgerufen werden.

BINGO: Als analoges Lernszenario dient auch ein papierbasiertes BINGO-Spiel zur Informationssicherheit, das in zwei Varianten entwickelt wurde: Die erste Variante bezieht sich auf das persönliche Verhalten; die zweite Variante erfragt den Ist-Stand und die Vorgaben der Organisationen, in denen die Studierenden arbeiten. In beiden Varianten existieren jeweils zwei Bögen (Fragen 1, Fragen 2) für zwei Gruppen (Gruppe 1, Gruppe 2) mit einem 4x4-Fragenfeld. Die enthaltenen Fragen zur Informationssicherheit beziehen sich auf Wissen, Fertigkeiten sowie Verhalten und sind so gestellt, dass sie mit Ja und Nein beantwortet werden können. Teilnehmende der Gruppe 1 befragen Teilnehmende der Gruppe 2 und umgekehrt. In einer Reihe bzw. Spalte des 4x4-Fragenfeldes müssen vier verschiedene Teilnehmende der jeweils anderen Gruppe mit Ja geantwortet haben, damit laut „Bingo“ gerufen werden darf. Nach drei Bingo-Rufen ist das Spiel beendet. Im Rahmen der Auswertung müssen diejenigen, die mit Ja antworteten, ihre Antwort erklären. Sollten sich Defizite oder Fehler zeigen, werden diese im Plenum behandelt und geklärt.

Netzwerk-Domino: Das Netzwerk-Domino wurde vom Forschungsteam Prof. Dr. Scholl entwickelt und in Zusammenarbeit mit known_sense umgesetzt. In diesem Lernspiel vertiefen die Teilnehmenden ihr erworbenes Wissen über die Arbeitsweise von Netzwerkkomponenten und deren sinnvolle Anordnung. Gemäß dem GBL-Ansatz soll die haptische Erfahrung bei der Durchführung zum wirklichen Begreifen der Spielelemente

Abb. 3) Beispiel einer Netzwerk-Architektur beim Netzwerk-Domino.

führen. Ziel des Spieles ist es, mit den vorgegebenen Spielelementen ein Netzwerk zu legen, welches vorgegebene Anforderungen an Sicherheit und Funktionalität erfüllt. Dabei kann der Schwierigkeitsgrad durch die Vorgabe des bereits existierenden Netzwerkes, die Anzahl verfügbarer Elemente sowie die Zielvorgabe flexibel an die Kenntnisse der Studierenden angepasst werden (siehe Abb. 3). Die Teilnehmenden müssen in Teams von 3–6 Personen die Aufgabe innerhalb von 5–15 Minuten lösen. Durch die Kommunikation innerhalb der Gruppe während des selbstständigen Lösens der Aufgabe und die anschließende Besprechung mit dem/der Moderator/in entsteht ein doppelter Lerneffekt, der zu einer nachhaltigen Vertiefung des Unterrichtsinhaltes führen soll.

Schutzspiel – Gefahrenabwehr mit begrenztem Budget: Lernziel dieses noch im Entwicklungsstadium befindlichen analogen Szenarios ist es, Sicherheitsmaßnahmen zu verstehen sowie verschiedene Level der Absicherung unterscheiden und bewerten zu können. Zudem soll ein Bewusstsein für den sinnvollen Einsatz der Maßnahmen und die damit verbundenen Kosten geschaffen werden. Auf einem Spielfeld sind neun Sicherheitsbedrohungen für eine fiktive Organisation dargestellt. Auf jede Bedrohung kann auf vier Arten, die sich in ihrem Schutzlevel und den erforderlichen Kosten unterscheiden, reagiert werden. Bei Spielstart wird ein bestimmtes Budget an das spielende Team ausgegeben, das – gemäß realen Bedingungen – nicht für den maximalen Schutz aller neun Sicherheitsbedrohungen ausreicht. Die Karten mit den Schutzmaßnahmen enthalten sichtbar auf der Vorderseite die Kosten, nicht aber das entsprechende Schutzlevel. Das spielende Team hat neun Minuten Zeit, ihre Schutzmaßnahmen für die neun Gefahren zu bestimmen. Anschließend erfolgt die Auswertung mit dem/der Moderator/in, wie sinnvoll welche Maßnahme war, wo zu viel oder zu wenig abgesichert wurde. Alternativ kann das Spiel auch mit zwei Teams gespielt werden. Nach der Auswahl der Sicherheitsmaßnahmen werden die Spielfelder mit den neun Gefahren getauscht, ohne dass eine Auswertung stattfindet. Das gegnerische Team darf sich auf der Spielfläche drei Angriffspunkte aussuchen. Die Schutzlevel sehen sie dabei nicht. Wird ein Punkt mit höchstem Schutz gewählt, muss das gegnerische Team vier Fragen, bei zweithöchstem Schutzlevel drei Fragen, bei dritthöchstem Schutzlevel zwei Fragen und bei niedrigstem Schutzlevel lediglich eine Frage beantworten. Der Schwierigkeitsgrad steigt von einer zur nächsten Frage. Sobald eine Frage falsch beantwortet wurde, ist der Angriff an dem Punkt gescheitert und kann nicht fortgesetzt werden.

Interaktive Übung „Phishing“: Im Rahmen der digitalen, webbasierten Anwendung „Phishing“ können sich die Studierenden mit theoretischen Grundlagen zu Phishing vertraut machen und zwei Tests mit unterschiedlichem Schwierigkeitsgrad durchführen. Der Abschnitt „Was ist Phishing?“ beinhaltet eine kurze Zusammenfassung von Definitionen, typischen Phishing-Vorgehensweisen und praktischen Beispielen, wie eine Phishing-Mail und eine gefälschte Seite aussehen können. In dem Test „Phishing erkennen“ müssen die Teilnehmenden entscheiden, ob es sich bei den gezeigten E-Mails um einen Phishing-Angriff handelt oder nicht. Dieser erste Teil des digitalen Lernszenarios unterscheidet sich nicht von anderen digitalen Übungen zum Thema Phishing (z. B. http://www.it.tum.de/it-sicherheit/glossar/phishing-mails/selbstlerntest-phishing/). Der Mehrwert besteht vor allem im zweiten Teil „Phishing-Merkmale erkennen“, in dem es um die Vertiefung der vermittelten Kenntnisse zum Thema Phishing geht. Hier müssen aus mehreren Optionen die Merkmale ausgewählt werden, die in der gezeigten E-Mail auf einen Phishing-Versuch hinweisen. Nach dem Absolvieren jedes Tests wird den Teilnehmenden die erreichte Punktzahl angezeigt und sie haben die Möglichkeit, die Fragen im Review-Modus nochmals durchzugehen und die richtigen Antworten sowie Lösungshinweise einzusehen. Die beiden Tests können unabhängig voneinander durchgeführt werden. Das Absolvieren beider Tests sollte nicht länger als 5–10 Minuten in Anspruch nehmen.

App „CBubbles“: Was als Hilfe für das Erlernen einer Sprache gedacht war, stellte sich im Laufe der Entwicklung als geeignetes Werkzeug für die Verinnerlichung von Fachbegriffen heraus. Ohne eine differenzierte Anwendung des Fachvokabulars kann ein Fachgebiet nicht gemeistert werden. Was liegt näher, als eine App mit Fachbegriffen und Wortlisten zu füllen, die das vermittelte Wissen noch einmal abruft und vertieft? Durch das Projekt SecAware4job steht mit der App-Entwicklung „CBubbles“ eine solche Möglichkeit zum Thema Informationssicherheit zur Verfügung. Für den ersten Test im Sommersemester 2016 wurden zwei spezielle Wortlisten erstellt und erprobt. Zum einen wurde eine Liste der beliebtesten Passwörter im englischsprachigen Raum erstellt,

Abb. 4) Das App-Spiel „CBubbles“ in der Lite-Version für Informationssicherheit.

die zeigt, wie einfach diese Passwörter auch ohne Computerunterstützung zu erraten sind. Eine zweite Liste fragt nach Fachbegriffen, die sich nicht ohne Weiteres einprägen. Im Unterschied zu vielen anderen Vokabel- und Karteikarten-Systemen, die es in vielen Ausprägungen gibt, werden mit „CBubbles“ die Worte in ihre kleinsten Einheiten – Buchstaben – zerlegt (Abb. 4). Das erzeugt, neben der Abfrage der Begriffe selbst, eine zweite Herausforderung: Wie wird das Wort korrekt geschrieben? Das muss nicht immer sofort klar sein und ist ein Mehrwert des Spieles. Das App-Spiel ist damit eine gute Alternative, um in Wartesituationen wie im Zug oder in der S-Bahn wichtige Begrifflichkeiten zu wiederholen.

5. Erste Forschungsergebnisse

Im Zuge der Durchführung von SecAware4job werden analoge Lernszenarien auch englischsprachig aufbereitet, international vorgestellt (Scholl & Fuhrmann 2016b) und in Auszügen mit einem internationalen Publikum getestet (Scholl et al. 2016b). Durch systematische Versuchsreihen sollen so die Forschungsfragen (s. Kapitel 3) am Ende von SecAware4job umfassend beantwortet werden können.
Die im Sommersemester 2016 durchgeführten Evaluationen mittels wöchentlicher Kurzfeedbackbögen durch die Studierenden des WPF zeigen bereits sehr gute Ergebnisse: So wurde das Fach mit dem angewandten methodischen Ansatz – bestehend aus einer Kombination aus Vortrag, analogen und digitalen spielebasierten Lernszenarien sowie interaktiven Übungen – von den Studierenden sehr gut bewertet. Das Ziel des Projektes, Informationssicherheitsbewusstsein und entsprechende Kenntnisse zu verbessern sowie idealerweise Verhaltensänderungen auszulösen, wurde bei den Teilnehmenden im Sommersemester 2016, insbesondere für das Arbeitsleben, erreicht. Um Aussagen zu den Wirkungsweisen der einzelnen Methoden, zum Lernerfolg und zur Nachhaltigkeit fundiert treffen zu können, ist es allerdings noch zu früh, da die empirische Basis bisher zu gering ist. Für die digitalen Entwicklungen hat die intensive Partizipation der Lernenden bereits zu Verbesserungen geführt. Die Studierenden beurteilten die digitalen Varianten als gute Ergänzung zu den analogen spielebasierten Lernszenarien, da sie in den digitalen Varianten alleine gefordert seien und sich dadurch intensiver und ausführlicher mit den Aufgaben auseinandersetzen könnten und müssten. Als Vorteil der analogen Szenarien betonten sie den Teamansatz sowie den dadurch ermöglichten sozialen Erfahrungs- und Wissensaustausch.

6. Zusammenfassung und Ausblick

Spielend lernen – lernen und spielen, ist das zeitgemäß? Diese Mischung wird bislang eher in der frühkindlichen Erziehung angewendet. Wie ist es aber im Studium, wenn es gilt, Zusammenhänge zu erkennen und neben dem neuen das schon vorhandene Wissen anzuwenden, um Probleme zu lösen?
Allen vorgestellten Methoden und Übungen ist einerseits gemein, dass die Studierenden in Teams kooperativ lernen und von ihrem bereits vorhandenen Wissen gegenseitig im Erfahrungsaustausch und bei der gemeinsamen Lösung der Aufgaben profitieren. Andererseits erhalten die Teilnehmenden durch die sofortige Auflösung der Aufgaben und gemeinsame Besprechung der Ergebnisse ein direktes Feedback zu ihrem Lernerfolg, so dass sich unmittelbar ein Lerneffekt einstellen kann. Die Auswertung der Ergebnisse sollte stets zum Anlass genommen werden, Aspekte zu vertiefen, Unsicherheiten auszuräumen und auf Hilfsmittel hinzuweisen.
In Planung ist die Entwicklung eines umfangreicheren Spieles zum Thema Social Engineering – eine Gefahr, die noch relativ unbekannt ist und dessen Bezeichnung aufgrund seiner Bestandteile „Social“ und „Engineer“ sogar eher positive Assoziationen weckt. Gleichwohl bedeutet Social Engineering „die zwischenmenschliche Manipulation, mit dem Ziel – unter Vortäuschung falscher Tatsachen – unberechtigten Zugang zu Informationen oder IT-Systemen zu erlangen“ (known_sense et al. 2015). In dem geplanten Lernszenario sollen der Tagesablauf eines fiktiven Charakters sowie potentielle Angriffspunkte und Risiken dargestellt und als Rollenspiel erlebt werden. Mit konkreten Gefahren der Digitalisierung konfrontiert, sollen Lernende die Notwendigkeit des Schutzes sensibler Daten begreifen lernen.
Zukünftig werden somit eine Bewertung der Ansätze im Hinblick auf ihre Lernförderlichkeit und eine Awareness-Messung in den Mittelpunkt gerückt. Die Forschungsfragen rund um diesen Praxisbeitrag werden für neue Projektanträge weiterentwickelt. Dazu werden sowohl die theoretischen Ansätze zur Wirksamkeit von GBL/DGBL als auch Gamification-Elemente näher einbezogen, um ein neues, empirisches Design entwickeln zu können, das auch mit anderen Proband/innen getestet werden kann.

Projektwebseite:
http://secaware4job.th-wildau.de/

LITERATUR

Admiraal W, Huizenga J, Akkerman S, Ten Dam G (2011) The concept of flow in collaborative game-based learning. Computers in Human Behavior 27(3):1185–1194. doi:10.1016/j.chb.2010.12.013

Abdul Jabbar AI, Felicia P (2015) Gameplay Engagement and Learning in Game-Based Learning. A Systematic Review. Review of Educational Research 85(4):740–779. doi: 10.3102/0034654315577210

Albrechtsen E (2007) A qualitative study of users' view on information security. Computers & Security 26(4):276–289. doi: 10.1016/j.cose.2006.11.004

Barzilai S, Blau I (2014) Scaffolding game-based learning. Impact on learning achievements, perceived learning, and game experiences. Computers & Education 70:65–79. doi: 10.1016/j.compedu.2013.08.003

Birkenbihl VF (2004) Kopf-Spiele. Breuer und Wardin, Bergisch Gladbach. ISBN: 3937864210

Chen C-H, Law V (2016) Scaffolding individual and collaborative game-based learning in learning performance and intrinsic motivation. Computers in Human Behavior 55:1201–1212. doi: 10.1016/j.chb.2015.03.010

Cone BD, Irvine CE, Thompson MF, Nguyen TD (2007) A video game for cyber security training and awareness. Computers & Security 26(1):63–72. doi: 10.1016/j.cose.2006.10.005

DSV-Gruppe, EnBW, <kes>, known_sense, et al. (eds) (2006) Entsicherung am Arbeitsplatz - die geheime Logik der IT-Security in Unternehmen, München, Köln

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

Erhel S, Jamet E (2013) Digital game-based learning. Impact of instructions and feedback on motivation and learning effectiveness. Computers & Education 67:156–167. doi: 10.1016/j.compedu.2013.02.019

Eseryel D, Law V, Ifenthaler D, Ge X, Miller R (2013) An Investigation of the Interrelationships between Motivation, Engagement, and Complex Problem Solving in Game-based Learning. Educational Technology and Society 17(1):42–53. ISSN: 1176-3647

Guo KH, Yuan Y, Archer NP, Connelly CE (2011) Understanding Nonmalicious Security Violations in the Workplace. A Composite Behavior Model. Journal of Management Information Systems 28(2):203–236. doi: 10.2753/MIS0742-1222280208

Halverson R, Berland M, Owen E V (2015) Assessment in Game-Based Learning. Spector, J M (ed) The SAGE Encyclopedia of Educational Technology. SAGE Publications, Inc., Los Angeles, London, New Delhi, Singapore, Washington DC, Boston. ISBN: 9781452258225. doi:10.4135/9781483346397.n28

Hamari J, Shernoff DJ, Rowe E, Coller B, Asbell-Clarke J, Edwards T (2016) Challenging games help students learn. An empirical study on engagement, flow and immersion in game-based learning. Computers in Human Behavior 54:170–179. doi: 10.1016/j.chb.2015.07.045

Helisch M, Pokoyski D (eds) (2009) Security awareness. Neue Wege zur erfolgreichen Mitarbeiter-Sensibilisierung, 1. Aufl. Edition kes. Vieweg + Teubner, Wiesbaden. ISBN: 978-3834806680

Hsiao H-S, Chen J-C (2016) Using a gesture interactive game-based learning approach to improve preschool children's learning performance and motor skills. Computers & Education 95:151–162. doi: 10.1016/j.compedu.2016.01.005

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 Interna-tional Conference on Digital Game and Intelligent Toy Enhanced Learning, DIGITEL 2008:83–89. doi:10.1109/DIGITEL.2008.24

Institute of Play (2013) Q Design Pack School. http://www.instituteofplay.org/wp-content/uploads/2013/09/IOP_QDesignPack_School_1.0.pdf. Accessed 13 Dec 2016

known_sense, Lanxess, Technische Hochschule Wildau, <kes> (2015) Bluff me if u can – Gefährliche Freundschaften am Arbeitsplatz. Tiefenpsychologische Wirkungsanalyse Social Engineering und seine Abwehr. http://www.known-sense.de/BluffMelfUCanAuszug.pdf. Accessed 13 Dec 2016

Lai C-H, Lin Y-C, Jong B-S, Hsia Y-T (2014) Adding Social Elements to Game-Based Learning. International Journal of Emerging Technologies in Learning 9(3):12–15

Le S, Weber P, Ebner M (2013) Game-Based Learning. Spielend Lernen?. In: Ebner M, Schön S (2013) Lehrbuch für Lernen und Lehren mit Technologien. Epubli, Berlin: 267–275. ISBN: 9783844265941

Leutner D (1993) Guided discovery learning with computer-based simulation games. Effects of adaptive and non-adaptive instructional support. Learning and Instruction 3(2):113–132. doi: 10.1016/0959-4752(93)90011-N

Plass j L, Homer B D, Kinzer C K (2015) Foundations of Game-Based Learning. Educational Psychologist 50(4):258–283. doi:10.1080/00461520.2015.1122533

SanNicolas-Rocca T, Schooley B, Spears (2014) JL Designing Effective Knowledge Transfer Practices to Improve IS Security Awareness and Compliance. In: 2014 47th Hawaii International Conference on System Sciences (HICSS), Waikoloa, HI, pp 3432–3441. doi: 10.1109/HICSS.2014.427

Shi Y-R, Shih J-L (2015) Game Factors and Game-Based Learning Design Model. International Journal of Computer Games Technology. 2015:1–11. doi:10.1155/2015/549684

Scholl M, Fuhrmann F (2016a) Analog – digital? Wie sich mit Hilfe analoger Methoden Bewusstsein für Informationssicherheit in der digitalen Welt fördern lässt. In: FTVI & FTRI (ed) Fachtagungen Verwaltungsinformatik und Rechtsinformatik, 21.-23.09.2016, Dresden

Scholl M, Fuhrmann F (2016b) Information Security Awareness 3.0 for Job Beginners. In: Book of industry papers, poster papers and abstracts, CENTERIS 2016 – International Conference on Enterprise Information Systems: 433–436

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

Scholl M, Fuhrmann F, Pokoyski D (2016b) The Human Factor: How Can Information Security Awareness Be Sustainably Achieved in E-Government? In: Scholl HJ, Glassey O, Janssen MFWHA (eds) Electronic government and electronic participation. Joint proceedings of ongoing research, PhD papers, posters and workshops of IFIP EGOV and ePart 2016. Innovation and the Public Sector, 23. IOS Press, Netherlands, ISBN: 1614996709, pp 403–404

Spires HA (2015) Digital Game-Based Learning. Journal of Adolescent and Adult Literacy 59(2):125–130. doi: 10.1002/jaal.424

Straub DW, Welke RJ (1998) Coping with Systems Risk. Security Planning Models for Management Decision Making. MIS Quarterly 22(4):441 –469. doi: 10.2307/249551

Sweller J, van Merrienboer JJG, Paas FGWC (1998) Cognitive Architecture and Instructional Design. Educational Psychology Review 10(3):251–296. doi: 10.1023/A:1022193728205

Tsai F-H, Tsai C-C, Lin K-Y (2015) The evaluation of different gaming modes and feedback types on game-based formative assessment in an online learning environment. Computers & Education 81:259–269. doi: 10.1016/j.compedu.2014.10.013

Zaphiris P, Ang C S, Law D (2007) Individualistic versus competitive game-based e-learning. Advanced Technology for Learning 4(4):206–211. doi:10.2316/Journal.208.2007.4.208-0921

Zweck A, Holtmannspötter D, Braun M, Hirt M, Kimpeler S, Warnke Ph (2015) Gesellschaftliche Veränderungen 2030. Ergebnisband 1 zur Suchphase von BMBF-Foresight Zyklus II. VDI Technologiezentrum (ed). http://www.vditz.de/meldung/bmbf-foresight-berichte-so-sieht-die-welt-im-jahr-2030-aus. Accessed 16 March 2016

AUTOREN

Prof. Dr. rer. nat. Margit Scholl
Frauke Fuhrmann
Denis Edich
Ernst Peter Ehrlich
Kai Benjamin Leiner
Lars Robin Scholl
Peter Koppatz
Technische Hochschule Wildau
Fachgebiet Wirtschafts- und Verwaltungsinformatik
Forschungsgruppe "Information Security Awareness"

E-Mail für Korrespondenz:
margit.scholl@th-wildau.de