Detlef Rätz [et. al.] (Hrsg.): Digitale Transformation:
Methoden, Kompetenzen und Technologien für die Verwaltung
Lecture Notes in Informatics (LNI), Gesellschaft für Informatik, Bonn 2016 101

Analog – digital? Wie sich mithilfe analoger Methoden Bewusstsein für Informationssicherheit in der digitalen Welt fördern lässt

Margit Scholl[1] und Frauke Fuhrmann

Abstract: Mit der fortschreitenden Digitalisierung, die alle Lebensbereiche beeinflusst, werden das Bewusstsein und die Kompetenzen zur Sicherung sensibler Informationen immer wichtiger. Diese Notwendigkeit unterstreichen auch die Ergebnisse einer aktuellen Befragung zu Informationssicherheitsbewusstsein und -kenntnisse der Studierenden der Technischen Hochschule Wildau. Wie auf innovative Weise mittels einer Kombination aus spielerischen analogen und digitalen Lernszenarien Bewusstsein für Informationssicherheit und entsprechende Verhaltensweisen gefördert werden können, zeigen die dargestellten Projektbeispiele. Des Weiteren wird ein Modell in Form einer Spirale vorgestellt, mit dem die transformative Wechselwirkung zwischen top-down Vorgaben einer Organisation und der bottom-up Beeinflussung durch Mitarbeiter zur Entwicklung einer gelebten Sicherheitskultur erläutert wird.

Keywords: Digitale Transformation, Informationssicherheit, IT-Sicherheit, Bewusstsein, Verhalten, Game-based Learning, spielerische Lernszenarien

1 Einleitung

Die computergestützte Technisierung ist in den Industrienationen unter dem Schlagwort Digitalisierung ein zentrales Faktum aller Lebensbereiche und beeinflusst zunehmend sowohl das Arbeits- als auch das Privatleben. Wie der Präsident des Bundesamtes für Sicherheit in der Informationstechnik (BSI) auf dem 14. Deutschen IT-Sicherheitskongress verdeutlichte [BS15], bietet die Digitalisierung Potenziale, auf die eine hochentwickelte Industrienation wie Deutschland nicht verzichten kann – gleichzeitig gehen damit aber neue Herausforderungen für die Cybersicherheit einher. Bisherige IT-Sicherheitsmechanismen stoßen an ihre Grenzen und Zuverlässigkeit und Beherrschbarkeit können nicht vorausgesetzt werden [BS15]. Es besteht kein Zweifel, dass die fortschreitende digitale Transformation in allen gesellschaftspolitischen und wirtschaftlichen Bereichen zu einer Zunahme der Bedeutung von Informationssicherheit und IT-Sicherheit sowie Datenschutz und Datensicherheit führt.

[1] Technische Hochschule Wildau, FB Wirtschaft, Informatik, Recht, Hochschulring 1, 15745 Wildau, {margit.scholl| frauke.fuhrmann}@th-wildau.de

Betroffen von den damit verbundenen Herausforderungen sind sowohl jeder Einzelne[2] als auch alle Organisationen (Unternehmen, Verwaltungen etc.). So ist „gut die Hälfte (51 Prozent) aller Unternehmen in Deutschland … in den vergangenen zwei Jahren Opfer von digitaler Wirtschaftsspionage, Sabotage oder Datendiebstahl geworden“ [BI15: 1]. Die Mehrzahl der Geschäftsprozesse und Fachaufgaben in Unternehmen und öffentlichen Verwaltungen sind inzwischen von einem einwandfreien Betrieb der vernetzten Informationstechnik (IT) abhängig. Die Bedeutung von Informationssicherheit ist zwar grundsätzlich bekannt, sie ist jedoch keineswegs allen Mitarbeitern so bewusst und ausreichend verinnerlicht, dass das eigene Verhalten danach ausgerichtet wird. So ergab die BITKOM-Studie, dass nach dem Diebstahl von IT- und Kommunikationsgeräten an zweiter Stelle der Verbrechen Social Engineering rangiert [BI15: 1]. Social Engineering „bedeutet auf das Thema Informationssicherheit bezogen die zwischenmenschliche Manipulation, mit dem Ziel – unter Vortäuschung falscher Tatsachen – unberechtigten Zugang zu Informationen oder IT-Systemen zu erlangen“ [kn15: 4]. Es zeigte sich, dass das Phänomen „Social Engineering“ und der entsprechende Begriff, der aufgrund seiner Bestandteile „Social“ und der positiven Wahrnehmung von Ingenieuren (Engineer) sogar eher positive Assoziationen weckt, noch relativ unbekannt sind [kn15: 36]. Um den vielfältigen Herausforderungen zur Gewährleistung von Informationssicherheit zu begegnen, müssen zielgruppenorientierte Sensibilisierungsmaßnahmen nachhaltig etabliert werden. So empfiehlt das Aktionsbündnis „Deutschland sicher im Netz e.V.“, dem Sicherheitsgefälle mit Aufklärung zu begegnen, denn viele Risiken sind abwehrbar, wenn grundlegende Verhaltensregeln beachtet werden [Ds15]. Doch ist eine breit gelebte Sicherheitskultur bislang eher selten [Wi15a]. Weder direkte Anweisungen noch einfache Awareness-Maßnahmen reichen aus, um Informationssicherheit als Teil der Organisationkultur zu etablieren [Wi15b: 66].

Ziel des vorliegenden Beitrages ist es, eine innovative Herangehensweise vorzustellen, mit der an der Technische Hochschule (TH) Wildau sowohl bei Mitarbeitern und Studierenden als auch Besuchern ein nachhaltiges Bewusstsein für Informationssicherheit in der digitalen Welt geschaffen wird. In Kapitel 2 wird zunächst die Ausgangssituation erläutert. In Kapitel 3 werden Ergebnisse einer aktuellen Befragung von Studierenden an der TH Wildau zu Informationssicherheitsbewusstsein und -kenntnisse vorgestellt, die die Notwendigkeit der Förderung von Bewusstsein und Kompetenzen für Informationssicherheit unterstreichen. Anschließend wird in Kapitel 4 anhand eines neu entwickelten Modells dargelegt, wie Bewusstsein für Informationssicherheit und entsprechende Verhaltensweisen in einer transformativen Wechselwirkung zwischen organisationalen top-down Vorgaben zu Informationssicherheit und individueller bottom-up Beeinflussung entwickelt bzw. gefördert werden können. Kapitel 5 stellt die an der TH Wildau durchgeführten Projekte zur Stärkung des Informationssicherheitsbewusstseins und die bisherigen Erkenntnisse der Erprobung der innovativen Herangehensweise kurz vor. Der Beitrag schließt in Kapitel 6 mit einem Ausblick.

[2] Für eine bessere Lesbarkeit wird die männliche Form für Personenbezeichnungen verwendet. In jedem Fall sind aber sowohl weibliche als auch männliche Personen eingeschlossen.

2 Ausgangssituation

Der Begriff Informationssicherheit ist auf den „Schutz von Informationen jeglicher Art und Herkunft ausgerichtet“ [BA16: 13]. Er beinhaltet auch, aber nicht nur, die IT-Sicherheit, die auf den „Schutz elektronisch verarbeiteter und gespeicherter Informationen und der zugehörigen technischen Systeme“ [BA16: 13] abzielt. Sicherheitskommunikation, Bildung und Training soll das Verhalten der Mitarbeiter an den Sicherheitszielen der Organisation auszurichten, aber dies geschieht nicht immer in einer erfolgversprechenden Art und Weise [Be15: 3]. Vielmehr ist eine Reihe von Schritten erforderlich, um eine gelebte Sicherheitskultur in einer Organisation zu erreichen. Das Geheimnis ist die Einbeziehung der Mitarbeiter in der richtigen Weise, sodass sie Gelerntes in konkretes sicheres Verhalten umsetzen [Be15: 3].

Die betriebliche Security und Privacy Awareness ist eine relativ junge Disziplin, die sich methodisch in drei Ansätze einteilen lässt [HP09]: Erstens in lerntheoretische Ansätze, die auf Wissensvermittlung ausgerichtet sind, zweitens in werbliche Ansätze, die neben Informationen zum Thema werbliche Elemente beinhalten, um Aufmerksamkeit, Emotionen und „Involvement“ bei den Mitarbeitern auszulösen. Der dritte systemische Ansatz verbindet Wissensvermittlung und Emotionalisierung mit Übungen in einem Team, um durch kommunikative Prozesse und die Anwendung des erworbenen Wissens in einer sozialen Situation adäquate Verhaltensweisen einzuüben. Dabei sollten insbesondere die psychologischen Auswirkungen des Sicherheitsverhaltens berücksichtig und eine lebendige und praktische Vermittlung von Bedrohungen und Sicherheitsmaßnahmen angestrebt werden, um ein dauerhaftes Bewusstsein (Awareness) zu erzeugen [kn15] [En08] [DS06].

Lernen und Wissensmanagement in Organisationen unterliegen einem ständigen Wandel. Darüber hinaus stehen die Medienlandschaft und der Bildungssektor vor erheblichen Umbrüchen [EU14: 38]. Beispielsweise werden Lernszenarien zunehmend spielerisch (game-basiert*)* [Zw15: 90f.]. Die Lern- und Lehrmethode „Game-based Learning“ ermöglicht ein an die konkreten betrieblichen Bedarfe angepasstes, lerner-zentriertes Lernen, bei dem der individuelle Wissensstand, die Bedürfnisse der einzelnen Nutzer im Mittelpunkt stehen [In15: 4f.]. Der Besitz von multifunktionalen, mobilen Endgeräten wie Smartphones wird bei Erwachsenen und Jugendlichen weiterhin steigen und ihre Internetnutzung verändern [Ku13: 15]. Im betrieblichen und gesamtgesellschaftlichen Rahmen ist zudem ein enormer Anstieg der produzierten Datenmenge (in Echtzeitverarbeitung) anzunehmen, die mit neuen Analyseverfahren (Big Data) auch zu Veränderungen der Arbeitswelt führt. Aber wie gehen die Mitarbeiter mit den neuen Endgeräten und der Datenflut um? Wie begegnen Führungskräfte dem digitalen Wandel, den damit einhergehenden Bedrohungen der Geschäftsprozesse und Fragen wie Nutzung privater Geräte im Arbeitsalltag („Bring Your Own Device“)? Nur wenige Organisationen formulieren konkrete Strategien zur Nutzung der Chancen und zur Begegnung der Herausforderungen der Digitalisierung und eine gefährliche Ignoranz ist zu verzeichnen [NKO15].

3 Befragung zu Informationssicherheitsbewusstsein

Die Notwendigkeit einer stärkeren und kontinuierlichen Sensibilisierung für Informationssicherheit verdeutlichen auch die Ergebnisse einer Online-Befragung zu Informationssicherheitsbewusstsein und -kenntnisse an der TH Wildau, an der im Zeitraum vom 18. Januar bis 10. März 2016 128 Studierende teilnahmen. Die geschlechtliche Zusammensetzung der Teilnehmer (37,5 % weiblich, 62,5 % männlich) entspricht den Anteilen weiblicher und männlicher Studierenden an der TH Wildau (36,7 % Frauen und 63,3 % Männer) [TH16: 5]. 64,06 % der Befragungsteilnehmer sind Studierende des Fachbereichs Ingenieur und Naturwissenschaften (FB INW), 35,94 % der Teilnehmer gehören dem Fachbereich Wirtschaft, Informatik und Recht (FB WIR) an. Dies übersteigt das Verhältnis der Studierenden (52,05 % FB INW, 47,95 % FB WIR) und verdeutlicht das geringere Interesse der nicht-technischen Studiengänge.

Um das Bewusstsein der Teilnehmer für Informationssicherheit und ihr diesbezügliches Verhalten zu ermitteln, wurden ihnen u. a. Fragen zu Schutzmaßnahmen wie Passwort-Sicherheit gestellt. Es zeigte sich, dass die Mehrheit der Befragten ein Bewusstsein für sichere Passwörter hat, denn 62,5 % gaben an, dass sie lediglich für drei und weniger Geräte (z. B. Laptop, Smartphone) und/oder Internet-Dienste (z. B. WLAN, E-Mail, Online-Banking) dasselbe Passwort verwenden, die Hälfte davon nutzt, wie empfohlen, für jedes Gerät bzw. für jeden Internet-Dienst ein anderes Passwort. Ferner bestehen die Passwörter von 96,09 % der Teilnehmer aus sieben und mehr Zeichen. Dabei sind die Passwörter der Mehrheit (60,94 %) eine Kombination aus Klein-, Großbuchstaben, Zahlen und Sonderzeichen. Es muss allerdings bedacht werden, dass viele Internet-Dienste vorgeben, welche Bestandteile (z. B. Groß- und Kleinbuchstaben, Zahlen) ein Passwort enthalten und wie viele Zeichen es mindestens umfassen muss. Abbildung 1 zeigt jedoch anhand von Geräten und Internet-Diensten, die von nahezu allen Befragten genutzt werden, dass Passwörter sehr selten bzw. nie geändert werden.

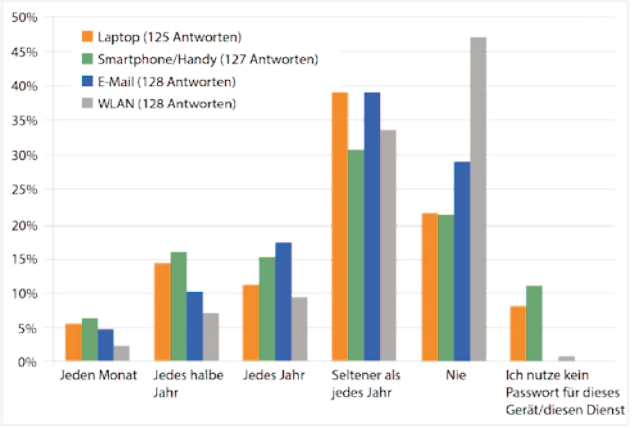

Abb. 1: Häufigkeit der Änderung von Passwörtern

Im Hinblick auf mögliche Gefahren haben die Befragten gute Kenntnisse geläufiger und schon seit längerer Zeit existierender Bedrohungen wie Phishing oder Spyware – 75,59 % bzw. 80,16 % der 127 bzw. 126 Teilnehmer wählten die richtige Lösung. Jedoch bestehen Wissenslücken bei neueren Bedrohungen wie Social Engineering: Hier wurde von lediglich 31,75 % der Teilnehmenden die richtige Antwort gegeben. 34,92 % der 126 Befragten vermerkten, dass sie nicht wissen, was man unter Social Engineering versteht. Aufschlussreich sind auch die Ergebnisse zu Erfahrungen mit Mobbing im Internet oder über das Handy: Selbst erlebt, haben dies nach eigenen Angaben 8,31 %, jedoch haben 26,83 % der 123 Teilnehmer Freunde, denen dies schon einmal widerfahren ist.

Die Ergebnisse zeigen, dass zwar ein gewisses Bewusstsein für Informationssicherheit vorhanden ist, sich dies aber nicht zwingend in dem Verhalten der Befragten widerspiegelt. Zudem sind neuere Bedrohungen noch nicht ausreichend bekannt und somit können die damit verbundenen Gefahren nicht kompetent abgewehrt werden. Dies verdeutlicht die Notwendigkeit einer stärkeren und kontinuierlichen Sensibilisierung für Informationssicherheit, die letztendlich zu gelebtem Informationssicherheitsverhalten führen soll. Wie ein nachhaltiges Bewusstsein für Informationssicherheit mit entsprechenden Verhaltensweisen in einer transformativen Wechselwirkung zwischen institutionellen Vorgaben und individuellen Lernprozessen gefördert werden kann, wird im folgenden Kapitel anhand eines neu entwickelten Modells dargelegt.

4 Modell der transformativen Wechselwirkung zwischen Vorgaben und individuellen Lernprozessen für ein nachhaltiges Informationssicherheitsbewusstsein

Zur Etablierung einer gelebten Sicherheitskultur in Organisationen ist eine Kombination aus institutionellen Vorgaben und freiwilligem Engagement der Beschäftigten zur Gewährleistung von Informationssicherheit erforderlich. In Anlehnung an den von Hewlett Packard entwickelten Ansatz für einen stärkeren Einsatz von Mitarbeitern für Informationssicherheit [Be15] wird im Folgenden ein Modell in der Form einer Spirale vorgestellt, das die Wechselwirkung zwischen top-down Vorgaben und individueller bottom-up Beeinflussung zur Etablierung einer organisationalen Sicherheitskultur verdeutlicht. Die Spirale der transformativen Wechselwirkung (s. Abb. 3) besteht aus drei Teilbereichen, 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 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 informationssicherheitsrelevantes Wissen und Bewusstsein erwerben und entsprechendes Verhalten einüben (von unten nach oben). Zum Ziel des Unternehmens gehört die Selbstverpflichtung der Beschäftigten, die Vorgaben zu

leben. Wie kann das gelingen? Die Emotionen der Beschäftigten müssen angesprochen werden!

Abb. 2: Spirale der transformativen Wechselwirkung

Sowohl Organisationen als auch ihre Beschäftigten haben (evtl. divergierende) Ziele. Für das langfristige Bestehen einer Organisation ist es essentiell, die Ziele der Organisation mit denen der Beschäftigten in Einklang zu bringen. Dies kann erzielt werden, indem ein Bezug zwischen den organisatorischen Zielen und den persönlichen Interessen, Bedürfnissen und Zielen der Beschäftigten hergestellt wird. Dafür sollten Organisationsziele transparent sein. Damit die Ziele erreicht werden, müssen organisatorische Rahmenbedingungen und individuelle Möglichkeiten stetig verbessert werden. Die an der Spitze der Spirale dargestellte „stetige Verbesserung" entspricht dem in allen Managementansätzen und –standards enthaltenen **P**(lan)**D**(o)**C**(heck)**A**(ct)-**Loop**. In der heutigen Wissensgesellschaft sind Informationen und Wissen ein wesentlicher Vermögenswert von Organisationen [Kh11: 10862]. Zum Schutz erfolgskritischer Informationen sollte jeder Beschäftigte über Informationssicherheit entsprechend seinen Aufgaben und Verantwortlichkeiten verständlich informiert und insbesondere 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. Damit jedoch ein Bewusstsein für Informationssi-

cherheit und entsprechende informationssicherheitsfördernde Verhaltensweisen bei jedem Beschäftigten ausgebildet werden, bedarf es emotionalen Interesses und Motivation sowie die Bereitschaft des Einzelnen [Kh11: 10864].

Gemäß der dritten Stufe der betrieblichen Security und Privacy Awareness (vgl. Kapitel 2) kann dies mittels kreativer Methoden, die Wissensvermittlung, Emotionalisierung und Übungen in einem Team vereinen, erzielt werden. Denn dadurch werden Emotionen bei den Beschäftigten geweckt und ihre Motivation und Bereitschaft, kritische Informationen angemessen zu sichern, gefördert. Dies führt in Verbindung mit der zunehmenden Kompetenz in Fragen der Informationssicherheit und des Datenschutzes zu einer höheren Akzeptanz und Überzeugung von Richtlinien und Maßnahmen zur Sicherung kritischer Informationen. Letztendlich resultieren im Idealfall ein aktives Engagement und eine Selbstverpflichtung (Commitment) für Informationssicherheit, sodass kritische Informationen weniger als Befolgung von Vorgaben und Richtlinien, sondern aus eigener Überzeugung geschützt werden. Dieser Prozess der Sensibilisierung und Bewusstseinsbildung bei den einzelnen Beschäftigten ist in der Mitte der Spirale gezeigt.

Die Rahmenbedingungen innerhalb einer Organisation, die für eine gelebte Sicherheitskultur förderlich sind, sind auf der rechten Seite der Spirale abgebildet. Ausgehend von der oben genannten Transparenz der Organisationsziele und der Intention, die Ziele der Organisation mit denen der Beschäftigten in Einklang zu bringen, sollten die Beschäftigten die Möglichkeit erhalten, sich an wichtigen Entscheidungsprozessen beteiligen zu können. Dies fördert die Zusammenarbeit und den Wissenstransfer in der Organisation, sodass individuelles Wissen und persönliche Erfahrungen geteilt werden und in organisatorische Abläufe einfließen. Dadurch können Geschäftsprozesse verbessert werden, die durch umfangreiche IT-Anwendungen unterstützt werden. Diese IT-Anwendungen sind für einen reibungslosen Ablauf idealerweise integriert und sollten aufgrund der fortschreitenden digitalen Transformation kontinuierlich optimiert werden. Diese IT-Anwendungen enthalten kritische Informationen. Hier schließt sich der Kreis bzw. windet sich die Spirale zu den oben dargelegten Lern- und Sensibilisierungsprozessen für Informationssicherheit. Da Organisationen, ihr (Geschäfts-)Umfeld sowie Regelungen und technische Entwicklungen einem ständigen Wandel unterliegen, sollten 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 (Abb. 2) 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.

5 Projekte und Erprobungserkenntnisse

Die Ausbildung von Studierenden als zukünftige Mitarbeiter muss an den aktuellen Stand der Wissenschaft und an den Anforderungen der Praxis in Betrieben, Verwaltun-

gen und Institutionen orientiert sein. Dazu gehört auch der Wissensaufbau für ein ganzheitliches Technikverständnis und die Sensibilisierung für Informationssicherheit und im Besonderen IT-Sicherheit. Dies betrifft vor allem auch die weniger technik-affinen Studiengänge wie Betriebswirtschaftslehre sowie insbesondere Verwaltung und Recht und Kommunales Verwaltungsmanagement, denn gerade die öffentlichen Verwaltungen des Bundes, der Länder und der Kommunen verarbeiten als Arbeit- und Auftraggeber nicht nur eine Vielzahl von (sensiblen) Daten und Informationen der Bürger und der Wirtschaft, sondern unterliegen besonderen Schutz- und Rahmenbedingungen. Hier existieren einerseits eine besondere Verantwortung staatlicher Institutionen und andererseits ein Vertrauensvorschuss der Bürger. Dies sollte Anlass sein, eine weit intensivere Aufklärung und Ausbildung in Fragen der Informationssicherheit zu etablieren, als es bislang der Fall ist. Im aktuellen, von der Horst Görtz Stiftung geförderten Projekt „Informationssicherheitsbewusstsein für den Berufseinstieg: SecAware4job[3]“ sollen daher Studierende als zukünftige Mitarbeiter für die alltäglichen Herausforderungen des Schutzes der Informationssicherheit sensibilisiert und ihr Informationssicherheitsbewusstsein und ihre entsprechenden Kompetenzen fundiert gefördert werden. Um das abstrakte und komplexe Thema Informationssicherheit mit all seinen Facetten (z. B. rechtliche Rahmenbedingungen, Normen & Standards, Schutzmaßnahmen, Konzepte) leicht verständlich sowie greif- und erlebbar zu vermitteln, werden spielerische Lernszenarien und interaktive Lehr- und Lernmethoden, z. B. Story Telling über Sicherheit, eingesetzt.

Über das Drittmittelprojekt IT-Sicherheit@KMU konnte eine „SecurityArena“ [my15] (ein Line Extender des „SECURITY PARCOURS“ von T-Systems, mitentwickelt durch die Firma known_sense) eingerichtet werden. Für diese wurden mit dem Verbundpartner known_sense spielerische analoge Lernszenarien entwickelt und an die TH Wildau sowie ihre Zielgruppen angepasst. Gemäß einem partizipativen Forschungsansatz werden diese Lernszenarien mit Mitarbeitern, Besuchern, Teilnehmern des zertifizierten Fortbildungskurses zum IT-Sicherheitsbeauftragten und Studierenden erprobt. Themen dieser spielerischen analogen Lernszenarien sind u. a. Password-Hacking, Clear Desk, Informationsschutz, Informationsklassifizierung, Social Media, Social Engineering, Sichere Server, Vernetzung, Phishing, Sicher unterwegs. In SecAware4job werden die spielerischen analogen Lernszenarien als Vorbereitung der Studierenden für den Berufseinstieg angepasst sowie erprobt und gemäß dem Ansatz „Blended Learning“ um spielerische digitale Lernszenarien ergänzt. Die digitalen Varianten sollen dabei keineswegs die analogen Lernszenarien ersetzen, sondern zeit- und ortsunabhängiges Wiederholen und Vertiefen ermöglichen. Durch eine zielorientierte Kombination von spielerischen analogen und digitalen Lernszenarien soll eine nachhaltige Sensibilisierung für Informationssicherheit als wichtige Voraussetzung für Bewusstseinsentwicklung und Verhaltensänderung erreicht werden.

Spielerische analoge (narrative) Lernszenarien ermöglichen greifbares/haptisches Erleben und Erfahren abstrakter und komplexer Sachverhalte der Informationssicherheit. Sie

[3] http://secaware4job.wildau.biz/

können als „Arena“ mit mehreren Stationen aufgebaut und als Team im Wettbewerb absolviert werden. Diese Methode des „Stationenlernens“ basiert auf dem aus dem Sport bekannten Zirkeltraining [MA61]. Der Ablauf der einzelnen Stationen ist jeweils gleich und beginnt mit einer kurzen Einführung in das Thema (ca. 5 Minuten). Dabei werden die Teilnehmenden aktiv einbezogen, indem nach ihren Erfahrungen mit dem Thema gefragt wird. Auch der Moderator der Lernstation sollte neben der Erläuterung von 2–3 Regeln zur Abwehr des Sicherheitsrisikos möglichst auch persönliche Bezüge einfließen lassen. Danach folgt das „Durchspielen“ des Lernszenarios (ca. 5 Minuten). Im Anschluss werden die erzielten Punkte und das Ergebnis zum Anlass genommen, Aspekte zu vertiefen, Unsicherheiten ausräumen und auf Hilfsmittel sowie Tipps hinzuweisen (ca. 5 Minuten). Die Teams (mit jeweils 4–6 Personen) werden synchron durch die Lernstationen geführt.

In einem analogen Lernszenario wird beispielsweise das digitale Thema Phishing im übertragenen Sinne verbildlicht, indem die Teilnehmer ausgedruckte E-Mails aus einem Aufsteller fischen und entscheiden müssen, ob es sich um eine Phishing-Mail handelt oder nicht. Eingeführt und abgerundet wird das Angeln durch persönliche Erfahrungen und Diskussionen der Teilnehmer im Team und mit dem Moderator. Ergänzt wird das analoge Lernszenario durch eine digitale Variante. Die Teilnehmer erhalten wie im Berufsalltag E-Mails, bei denen sie entscheiden müssen, ob sie einen Phishing-Versuch darstellen oder nicht. Der erste Teil des digitalen Lernszenarios unterscheidet sich demnach nicht von der analogen Variante hinsichtlich der Aufgabenstellung, aber durch die realitätsgetreuere Situation und die Anforderung, die Aufgabe alleine zu lösen. Kann sich ein Teilnehmer bei einer Teamaufgabe auch einmal zurücknehmen, ist er hier voll und ganz gefordert. Der zweite Teil des digitalen Lernszenarios unterscheidet sich von der analogen Aufgabe und bestehenden digitalen Übungen zu Phishing dadurch, dass Merkmale in den E-Mails identifiziert werden müssen, die auf einen Phishing-Versuch hinweisen. Die digitale Variante des Lernszenarios dient somit nicht nur der Wiederholung, sondern auch der Vertiefung der Kenntnisse zum Thema. Somit sind analoge und digitale Methoden nicht als Widerspruch oder Alternativen zu verstehen, sondern als sinnvolle Ergänzungen, um das Bewusstsein und Kompetenzen für Informationssicherheit in Zeiten der fortschreitenden Digitalisierung zu fördern.

In SecAware4job liegt darüber hinaus ein Schwerpunkt in der Entwicklung einer nachweisbaren, stufigen Qualifizierung in Informationssicherheit für Studierende insbesondere der nicht-technischen Studiengänge für den Berufseinstieg in Unternehmen, Verwaltungen und Institutionen (s. Abb. 3). Es ist wichtig, dass alle Mitarbeiter und nicht nur IT-Fachkräfte über Informationssicherheitsbewusstsein und entsprechende Kompetenzen verfügen und sich der Gefahren von Cyberangriffen, Wirtschaftsspionage und Datendiebstahl bewusst sind und ihr Mögliches tun, um sensible Daten und Informationen zu schützen. Basis der Auswahl der Themen der Qualifizierung sind daher die mit der Digitalisierung verbundenen Herausforderungen und technischen Trends, die in den Kontexten Beruf und Organisation konkretisiert werden. In der höchsten, d. h. der vierten Qualifizierungsstufe können die Studierenden zertifizierte Kompetenzen erwerben, um in der Organisation als IT-Sicherheitsbeauftragter eine Leitlinie vorzubereiten, die Einführung

eines Informationssicherheitsmanagements in Unternehmen bzw. Verwaltungen zu begleiten und Kollegen für Informationssicherheit zu sensibilisieren.

Abb. 3: Mehrstufige Zertifikatshierarchie im Projekt SecAware4job für eine berufsorientierte Zusatzqualifikation in Informationssicherheit

Die Erprobung der spielerischen analogen Lernszenarien, als eine lebendige und praktische Vermittlung von Bedrohungen und Sicherheitsmaßnahmen, brachte bisher durchweg positive Beurteilungen von allen Zielgruppen. Es ist jedoch festzuhalten, dass ein Szenario umso besser wirkt, desto spezifischer die eingesetzten Materialien die berufliche bzw. private Situation der Zielgruppe simulieren bzw. abbilden. Das bedeutet, für jedes relevante Thema muss ein spezifisches Lernszenario für die ausgewählte Zielgruppe den Zusammenhang mit Informationssicherheit/IT-Sicherheit und Risikobewertung aufzeigen. Dafür müssen ein zielgruppenorientiertes, realitätsnahes und spielerisch aufbereitetes Lernszenario mit Moderations- und Train-the-Trainer-Konzept entwickelt werden. Diese Vorgehensweise führt zur Entwicklung einer organisationsweiten gelebten Sicherheitskultur, denn zum einen ermöglicht nur die „echte Einbindung aller Betroffenen und Beteiligten und ihrer Interessenvertreter“ den Aufbau einer Sicherheitskultur in einer komplexen Umgebung [Wi15b: 67]. Zum anderen müssen „menschliche Faktoren“ ernst genommen werden und bei Entscheidungsprozessen muss eine gute, interdisziplinäre Kommunikation stattfinden [Wi15b: 68]. „Zielgruppengerechte Awareness-Maßnahmen für alle Unternehmensangehörige halten das Thema im Bewusstsein und vermitteln die Fähigkeit, sicherheitsorientiert zu arbeiten“ [Wi15b: 71].

6 Ausblick

Technik allein löst die Sicherheitsprobleme in Organisationen nicht, sondern erst eine „gute Partnerschaft zwischen Mensch und Technik [hebt] das Sicherheitsniveau“ [Wi15b: 70]. Im Rahmen von Sensibilisierungsmaßnahmen zu Informationssicherheit

und Datenschutz sind insbesondere die psychologischen Auswirkungen des Sicherheitsverhaltens zu berücksichtigen [kn15] [En08] [DS06]. Dies bedeutet, dass erst eine lebendige und praktische Vermittlung von Bedrohungen und Sicherheitsmaßnahmen ein nachhaltiges Bewusstsein (Awareness) erzeugt. Dieser innovative Zugang zur Förderung des Bewusstseins für Informationssicherheit in der digitalen Welt erfordert die Einbeziehung kreativer Methoden für eine praktische Bebilderung der Tätigkeiten von Menschen. Wie die konkrete Umsetzung der integrativen und ganzheitlichen Sichtweise von Digitalisierung, digitale Mediennutzung und Informationssicherheit durch den kombinierten Einsatz von spielerischen analogen und digitalen Lernszenarien erfolgen kann, wurde anhand der „SecurityArena“ und dem Projekt SecAware4job dargelegt, die mithilfe innovativer Methoden Informationssicherheit in der digitalen Welt stärken möchten. In zukünftigen Projekten sollen die gesammelten Erfahrungen auf neue Praxisbereiche ausgedehnt werden. Dabei bestimmen die konkreten Qualifizierungsbedarfe der anvisierten Zielgruppen die Entwicklung weiterer analog-digitaler Lernszenarien. Hierbei ist ein partizipativer Forschungsansatz zu verfolgen, denn eine Informationssicherheitskultur kann nur in einem strategisch eingebetteten, strukturierten Prozess, wie ihn die Spirale der transformativen Wechselwirkung verdeutlicht, aufgebaut werden. Dies benötigt Zeit und eine kreative Herangehensweise unter Einbindung aller Beteiligten.

Literaturverzeichnis

[BA16] Bundesakademie für öffentliche Verwaltung im Bundesministerium des Innern (BAköV) (Hrsg.): Handbuch: IT-Sicherheitsbeauftragte in der öffentlichen Verwaltung. Fortbildungslehrgang der BAköV mit Zertifikat in Zusammenarbeit mit dem BSI, 5. Auflage, 2016.

[Be15] Beyer, M.; Ahmed, S.; Doerlemann, K.; Arnell, S.; Parkin, S.; Sasse, M. A.; Passingham, N.: Awareness is only the first step. A framework for progressive engagement of staff in cyber security, Hewlett Packard, Business white paper, 2015.

[BI15] Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e.V. (BITKOM): Digitale Angriffe auf jedes zweite Unternehmen. Presseinformation vom 16. April 2015, http://www.bitkom.org/files/documents/BITKOM-Presseinfo_Digitaler_Wirtschaftsschutz_16_04_2015_final.pdf, Stand: 10.03.2016.

[BS15] Bundesamt für Sicherheit in der Informationstechnik (BSI): 14. Deutscher IT-Sicherheitskongress. https://www.bsi.bund.de/DE/Service/Aktuell/Veranstaltungen/IT-Sicherheitskogress/14_ITSicherheitskongress/14_ITSiKongress.html;jsessionid=FF00E65C2777E24627FD276D81913E0D.2_cid286?nn=6600506, Stand: 18.3.2016.

[Ds15] Deutschland sicher im Netz e.V. (DsiN): Digitale Aufklärung 2.0. 2015.

[DS06] DSV-Gruppe; EnBW; <kes>; known_sense; nextsolutions; Pallas (Hrsg.): Entsicherung am Arbeitsplatz – die geheime Logik der IT-Security in Unternehmen. Köln & München, 2006.

[En08] EnBW; known_sense; pallas;, SAP; Sonicwall; Steria Mummert Consulting; Trend Micro (Hrsg.): Aus der Abwehr in den Beichtstuhl – qualitative Wirkungsanalyse CISO & Co. Köln, 2008.

[EU14] EU/EFRE: Masterplan IKT, Medien und Kreativwirtschaft, Berlin-Brandenburg, 2020. http://www.berlin.de/projektzukunft/fileadmin/user_upload/pdf/IKT-Wirtschaft/MP-IMK2020_Endbericht_141021.pdf, 2014, Stand: 16.03.2016.

[HP09] Helisch, M.; Pokoyski, D. (Hrsg.): Security Awareness: Neue Wege zur erfolgreichen Mitarbeiter-Sensibilisierung. Vieweg + Teubner, Wiesbaden, 2009.

[In15] Institute Of Play: Q Design Pack School. http://www.instituteofplay.org/wp-content/uploads/2013/09/IOP_QDesignPack_School_1.0.pdf, 2015, Stand: 10.3.2016.

[Kh11] Khan, B.; Alghathbar, K. S.; Nabi, S. I.; Khan, M. K.: Effectiveness of information security awareness methods based on psychological theories. African Journal of Business Management 5/26, S. 10862–10868, 2011.

[kn15] known_sense; Lanxess; Technische Hochschule Wildau; <kes> (Hrsg.): Bluff me if u can – Gefährliche Freundschaften am Arbeitsplatz. Tiefenpsychologische Wirkungsanalyse Social Engineering und seine Abwehr, http://www.known-sense.de/BluffMeIfUCanAuszug.pdf, 2015, Stand: Zugriff 16.03.2016.

[Ku13] Kulhay, J.: Die Mediengeneration. Jugendliche, ihr Medienkonsum und ihre Mediennutzung. Ausarbeitung zum Forschungsstand, Handreichung zur politischen Bildung, Band 11, Konrad Adenauer Stiftung, 2013.

[MA61] Morgan, R. E.; Adamson, G. T.: Circuit Training. 2nd edition, HarperCollins Publishers, London, 1961.

[my15] mynewsdesk: Neues Trainingszentrum soll IT-Sicherheitsbewusstsein bei Studierenden und Praktikern stärken. Pressemitteilung 01.03.2015, http://www.mynewsdesk.com/de/th-wildau/pressreleases/neues-trainingszentrumsoll-it-sicherheitsbewusstsein-bei-studierenden-und-praktikern-staerken-1123559, 2015, Stand: 16.03.2016

[NKO15] Niehaves, B.; Köffer, S.; Ortbach, K.: Gefährliche Ignoranz? – Bring-Your-Own-Device, IT Consumerization und Co in der öffentlichen Verwaltung. Berlin: Nationales E-Government Kompetenzzentrum e.V. (Hrsg.), 2015.

[TH16] Technische Hochschule (TH) Wildau: Bericht zum Jahreswechsel 2015 | 2016. Rückblicke. Einblicke. Ausblicke., 2016.

[Wi15a] Wiele, J.: Sicherheitskultur (1): Kultur, Cooltour oder Couture? <kes> 4/2015, S. 6– 8.

[Wi15b] Wiele, J.: Sicherheitskultur (2): Kommunikation führt zu Kultur. <kes> 5/2015, S. 66–71, 2015.

[Zw15] Zweck, A.; Holtmannspötter, D.; Braun, M.; Hirt, M.; Kimpeler, S.; Warnke, Ph: Gesellschaftliche Veränderungen 2030. Ergebnisband 1 zur Suchphase von BMBF-Foresight Zyklus II, VDI Technologiezentrum (Hrsg,), http://www.vditz.de/meldung/bmbf-foresight-berichte-so-sieht-die-welt-im-jahr-2030-aus, 2015, Stand: 16.03.2016.