

Sicher unterwegs in der digitalen Welt – spielend begreifen

Frauke Fuhrmann/Peter Koppatz/Denis Edich/Margit Scholl

Wie sollte ich meinen Arbeitsplatz verlassen, auch wenn ich nur kurz abwesend bin, um mir einen Kaffee zu holen oder zur Toilette zu gehen? Worauf sollte ich bei Reisen achten? Wer oder was verbirgt sich hinter dem Begriff „Social Engineering“? Welche E-Mails sollte ich besser nicht öffnen? Antworten auf diese Fragen konnten Teilnehmende des vierten Workshops der Glienicker Gespräche spielbasiert erarbeiten und erfahren.

Informationen sind das wertvolle Gut der heutigen Wissensgesellschaft.¹ Mitarbeitende jeglicher Organisationen arbeiten tagtäglich mit sensiblen Informationen der eigenen Organisation, von Unternehmen, Bürgerinnen und Bürger, Kundinnen und Kunden, Patientinnen und Patienten usw. Eine aktuelle Befragung von 591 Führungskräften im deutschsprachigen Raum zu den erforderlichen Kompetenzen von Beschäftigten in einer digitalisierte Arbeitswelt ergab neben Hard Skills wie

Informationstechnologie (IT)-Grundkompetenz, technischem Know-how und Medienkompetenz eine Reihe von Soft Skills, die jeder Beschäftigte besitzen sollte, bei denen aber nach Meinung der Befragten Handlungsbedarf für eine optimale Ausprägung besteht.²

Das Projekt „SecAware4job“, gefördert von der Horst Görtz Stiftung, wurde im Jahre 2015 an der Technischen Hochschule (TH) Wildau ins Leben gerufen,

um Studierende für ihren Berufseinstieg mit Informationssicherheitsbewusstsein und -kenntnissen auszustatten. Ihnen soll somit eine wichtige Kompetenz für ihren Berufseinstieg in der digitalen Welt mitgegeben werden. In den vergangenen zwei Jahren wurde das (Wahlpflicht-)Fach „Sensibilisierung für Informationssicherheit“ entwickelt und in drei Durchläufen in betriebswirtschaftlichen und verwaltungswissenschaftlichen Studiengängen erprobt. Da alle Mitarbeitenden, nicht nur IT-Fachkräfte, Informationssicherheitsbewusstsein besitzen sollten, wurde ein methodischer Ansatz gewählt, der Vortrag, analoge und digitale spielbasierte Lernszenarien und interaktive Übungen vereint.

Teilnehmende des vierten Workshops der Glienicker Gespräche konnten einen Eindruck von dieser Art der Vermittlung gewinnen und selbst ihre Kenntnisse und ihr Bewusstsein zu Informationssicherheit mittels ausgewählter spielbasierter analoger Lernszenarien testen und erweitern. Für den Einstieg in den Workshop wurde die Storytelling-Methode gewählt. Durch das Erzählen einer Geschichte soll das Wissen besser verinnerlicht werden – sowohl beim Erzählenden als auch beim Zuhörenden.³ Üblicherweise erhalten Studierende diese Aufgabe gegen Ende der Veranstaltung, um das Gelernte in einem Zusammenhang zu präsentieren. Im Workshop wurde die in SecAware4job entwickelte digitale Anwendung (s. Abb. 1) der Storytelling-Methode allerdings zu Beginn eingesetzt, um anhand gewürfelter Symbole das Projekt vorzustellen und die



Frauke Fuhrmann

Dipl.-Kffr., wissenschaftliche Mitarbeiterin und operative Projektleiterin im Projekt SecAware4job.



Peter Koppatz

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



Denis Edich

M.Sc., wissenschaftlicher Mitarbeiter im Projekt SecAware4job und zuständig für digitale Anwendungen, Web-Entwicklung und Design.



Prof. Dr. Margit Scholl

Professorin für Wirtschafts- und Verwaltungsinformatik an der Technischen Hochschule Wildau, Fachbereich Wirtschaft, Informatik, Recht; verantwortlich für das Projekt „SecAware4job“.

1 Kruger/Drevin/Steyn 2007.

2 Hays 2017.

3 Collins 1999.



Abb. 1: Digitale Anwendung Storytelling (s. <https://story-telling-3d.methopedia.eu/>)



Abb. 2: Ausschnitt der „Security Arena“ der TH Wildau: Lernstationen Sicherheit unterwegs, Clear Desk, Phishing und Social Engineering.

Teilnehmenden sich gegenseitig bekannt zu machen.

Anschließend durchliefen die Teilnehmenden aufgeteilt in Teams vier Stationen der „Security Arena“ der TH Wildau (s. Abb. 2) gemäß dem Lehr- und Lernansatz Stationenlernen, das zurückgeht auf das Zirkeltraining im Sport.⁴ Die „Security Arena“ ist ein Line Extender des „SECURITY PARCOURS“ von T-Systems, mit-

entwickelt durch die Firma known_sense. Die Teilnehmenden wurden sensibilisiert, welche Gegenstände und Unterlagen auch nur bei einem kurzzeitigen Verlassen des Arbeitsplatzes sicher verwahrt werden sollten (Station Clear Desk). Sie angelten reale E-Mails und identifizierten sie anhand von vorher gelernten Merkmalen (z.B. falsche Rechtschreibung, unpersönliche Anrede, Dringlichkeit, verdächtiger Anhang) als Phishing-Versuche oder

harmlose E-Mails (Station Phishing). An der Station Sicherheit unterwegs wurden die Teilnehmenden für mögliche Gefahren und entsprechende Schutzmaßnahmen auf (Dienst-) Reisen sensibilisiert. An der vierten Station lernten die Teilnehmenden die noch häufig unbekannte Angriffsmethode Social Engineering kennen. Hierbei versuchen Kriminelle durch Täuschung und Manipulation von Personen sensible Informationen von Unternehmen oder Privatpersonen zu erlangen. Social Engineers nutzen somit vordergründig nicht die technischen Schwachstellen aus, sondern menschliche Eigenschaften ihrer Kontaktpersonen (auch „Soziale Einfalltore“ genannt), um an sensible Informationen zu gelangen.⁵ Durch das gegenseitige Vorlesen und Imitieren von Telefonanrufen – eine häufig genutzte Methode von Social Engineers – wurden diese Sozialen Einfalltore (z.B. Neugier, Hilfsbereitschaft, Anerkennung) den Teilnehmenden bewusst gemacht.

Diese spielbasierten Lernszenarien und weitere im Projekt SecAware4job entwickelte und eingesetzte Übungen basieren auf dem Game-based-Learning-Ansatz. Game-based Learning wird als unterhaltsame und motivierende Form des Lernens beschrieben⁶, bei der Spielelemente (z.B. Punkte, Ranglisten, Spielergebnis, Level, Belohnungen, Fortschrittsanzeigen) in nicht spielerischen Kontexten wie in Arbeitsprozessen oder in der Lehre angewandt werden.⁷ Eigenschaften von Spielen, die den Einsatz von spielbasierten Lernszenarien in der Lehre vielversprechend erscheinen lassen, sind zum einen klare Zielvorgaben und direktes Feedback.⁸ Die Teilnehmenden arbeiten auf ein Ziel hin, wählen und führen Aktionen aus und erleben unmittelbar die daraus resultierenden Konsequenzen. Spielbasierte Lernszenarien erlauben es, Fehler zu begehen, zu experimentieren und dadurch die richtige Art und Weise, etwas zu tun, einzuüben.⁹ Zum anderen können Spiele

4 Morgan/Adamson 1961.

5 DATEV/DsIN 2015, known_sense et al. 2015.

6 Linek/Albert 2009.

7 Huotari/Hamar 2016, Codish/Ravid 2017, Silic/Back 2017.

8 Fang et al. 2013.

9 Trybus 2014.

individuell angepasst werden. Sie können das richtige Maß an Herausforderungen bieten, das die Lernenden nicht überfordert, aber die Erweiterung ihrer Fähigkeiten anregt.¹⁰ 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 Verhaltensänderungen¹¹ und verbessern kurz- und langfristige Lernergebnisse.¹² Durch den Einsatz von Spielen lassen sich

- Kein Studierender verlässt die Hochschule ohne Sensibilisierung für Informationssicherheit!
- Informationssicherheit betrifft jeden Beschäftigten an seinem Arbeitsplatz! Sie ist nicht delegierbar!
- Es sollten sowohl verlässliche Informationen und Grundkenntnisse vermittelt als auch entsprechende Verhaltensweisen interaktiv eingeübt werden.

Ergänzend zu These 1 wird im Sinne der Nachhaltigkeit und Fortführung des hier

»Kein Studierender verlässt die Hochschule ohne Sensibilisierung für Informationssicherheit! Informationssicherheit betrifft jeden Beschäftigten an seinem Arbeitsplatz! Sie ist nicht delegierbar!«

bessere Lernleistungen als durch klassischen Unterricht erzielen.¹³ Analoge und digitale Lernszenarien mit spielerischen Elementen wie Wettbewerb, Belohnung, unmittelbarem Feedback stellen einen innovativen Lehr- und Lernansatz dar, da sie Wissensvermittlung mit emotionalen und involvierenden Elementen¹⁴ sowie sozialem Lernen im Team vereinen.¹⁵ Die kombinierte Anwendung von analogen und digitalen spielbasierten Lernszenarien im Projekt SecAware4job nutzt die Vorteile beider Lernstrategien mit dem Ziel, in der Summe einen höheren Lernerfolg zu erreichen.¹⁶

Die im Workshop gezeigten beispielhaften analogen Lernszenarien dienen der Sensibilisierung und sind der Einstieg in eine intensivere Auseinandersetzung mit einem Thema, das in digitalen Lernszenarien wiederholt und in eigenem Tempo eingeübt werden kann. Die Teilnehmenden waren sich schnell einig, dass die Erfahrungen und das im Workshop Gelernte in den folgenden Thesen festgehalten werden sollten:

vorgestellten Projektes SecAware4job an der TH Wildau das Ziel verfolgt, Sensibilisierung für Informationssicherheit als Wahlpflichtfach in allen Studiengängen zu etablieren.

Literatur

- Admiraal et al. (2014): Gender-inclusive Game-based Learning in Secondary Education, in: International Journal of Inclusive Education Nr. 11/2014, S. 1208-1218.
- Bösche, W./Kattner, F. (2011): Fear of (Serious) Digital Games and Game-based Learning? Causes, Consequences and a Possible Countermeasure, in: International Journal of Game-Based Learning, Nr. 3/2011, S. 1-15.
- Bressler, D./Bodzin, A. (2013): A Mixed Methods Assessment of Students' Flow Experiences During a Mobile Augmented Reality Science Game, in: Journal of Computer Assisted Learning, Nr. 6/2013, S. 505-517.
- Buffum, P.S. et al. (2015): Mind the Gap: Improving Gender Equity in Game-Based Learning Environments with Learning Companions, in: AIED: International Conferences on Artificial Intelligence in Education 2015.
- Codish, D./Ravid, G. (2017): Gender Moderation in Gamification: Does One Size Fit All?, in: Proceedings of the 50th Hawaii International Conference on System Sciences 2017, S. 2006-2015.
- Collins, F. (1999): The Use of Traditional Storytelling in Education to the Learning of Literacy Skills, in: Early Child Development and Care, Nr. 1/1999, S. 77-108.
- Connolly, T.M. et al. (2012): A Systematic Literature Review of Empirical Evidence on Computer Games and Serious Games, in: Computers & Education, Nr. 2/2012, S. 661-686.
- DATEV und 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.
- Fang, X./Zhang, J./Chan, S.S. (2013): Development of an Instrument for Studying Flow in Computer Game Play, in: International Journal of Human-Computer Interaction, Nr. 7/2013, S. 456-470.
- Hays (2017): HR-Report 2017: Schwerpunkt Kompetenzen für eine digitale Welt, Mannheim, Zürich, Wien.
- Helisch, M./Pokoyski, D. (Hrsg.) (2009): Security Awareness: Neue Wege zur erfolgreichen Mitarbeiter-Sensibilisierung, Wiesbaden.
- Hsu, S.H. et al. (2008): From Traditional to Digital: Factors to Integrate Traditional Game-based Learning into Digital Game-based Learning Environment, in: Proceedings 2nd IEEE International Conference on Digital Game and Intelligent Toy Enhanced Learning, DIGITEL, S. 83-89.
- Huotari, K./Hamari, J. (2017): A Definition for Gamification: Anchoring Gamification in the Service Marketing Literature, in: Electronic Markets, Nr. 1/2017, S. 21-31.
- 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: Fletcher, L./Dodge, R. (Hrsg.): Fifth World Conference on Information

10 Bressler/Bodzin 2013.

11 Hsu et al. 2008, Bösche/Kattner 2011, Buffum et al. 2015.

12 Connolly et al. 2012; Wouters et al. 2013.

13 Admiraal et al. 2014.

14 Silic/Back 2017.

15 Helisch/Pokoyski 2009.

16 Scholl et al. 2017.

Security Education, IFIP — International Federation for Information Processing, Vol. 237, Springer, Boston, MA, S. 33-40.

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

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

Scholl, M. et al. (2017): Das Projekt Sec-Aware4job: Auf spielerischem Weg zu erhöhtem Informationssicherheitsbewusstsein für den Berufseinstieg, in: Wissenschaftliche Beiträge TH Wildau 2017, Wildau, S. 23-30.

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

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.

Wouters, P. et al. (2013): A Meta-analysis of the Cognitive and Motivational Effects of Serious Games, in: Journal of Educational Psychology, Nr. 2/2013, S. 249-265.

Neu in der Reihe Controlling & Business Analytics



Nachhaltigkeitsbericht- erstattung in West-, Mittel- und Osteuropa

Ein Ländervergleich

Von Dr. Judith Maja Pütter

2017, 300 S., brosch., 59,— €

ISBN 978-3-8487-4140-3

eISBN 978-3-8452-8448-4

(Controlling & Business Analytics)

nomos-shop.de/29811

Die vorliegende Arbeit beschäftigt sich erstmalig mit der Nachhaltigkeitsberichterstattung von Unternehmen aus 13 West-, Mittel- und Osteuropäischen Ländern. Die Arbeit kann in zwei Teile aufgeteilt werden: Zur Darstellung des Status quo und zur Aufdeckung von Unterschieden in der Nachhaltigkeitsberichterstattung wurde im ersten Teil eine **Inhaltsanalyse** bei den jeweils 50 größten Unternehmen aus Mittel- und Osteuropa sowie aus Westeuropa durchgeführt.

Im zweiten Teil wurden mit Hilfe von **Experteninterviews** unternehmensinterne Faktoren aufgedeckt, die einen Einfluss auf die Nachhaltigkeitsberichterstattung der Unternehmen haben. In einer Umfrage wurde überprüft, ob sich die internen Faktoren zwischen Unternehmen, die berichten, und Unternehmen, die nicht berichten, unterscheiden. Ferner wurde analysiert, ob sich diese regional unterscheiden.

Aus den Erkenntnissen der Untersuchungen werden entsprechend Implikationen für Wirtschaft, Wirtschaftspolitik und Wissenschaft abgeleitet.



Bestellen Sie jetzt telefonisch unter (+49)7221/2104-37.
Portofreie Buch-Bestellungen unter www.nomos-shop.de

Alle Preise inkl. Mehrwertsteuer

