DOI: 10.13140/RG.2.2.34339.53286

Technische Hochschule Wildau
Technical University of Applied Sciences

Awareness Lab SME (ALARM) Information Security
https://alarm.wildau.biz/en

Sustainable Information Security Sensitization in SMEs: Designing Measures with Long-Term Effect

Prof. Margit Scholl, PhD

IT-Sicherheit
IN DER WIRTSCHAFT

Gefördert durch:

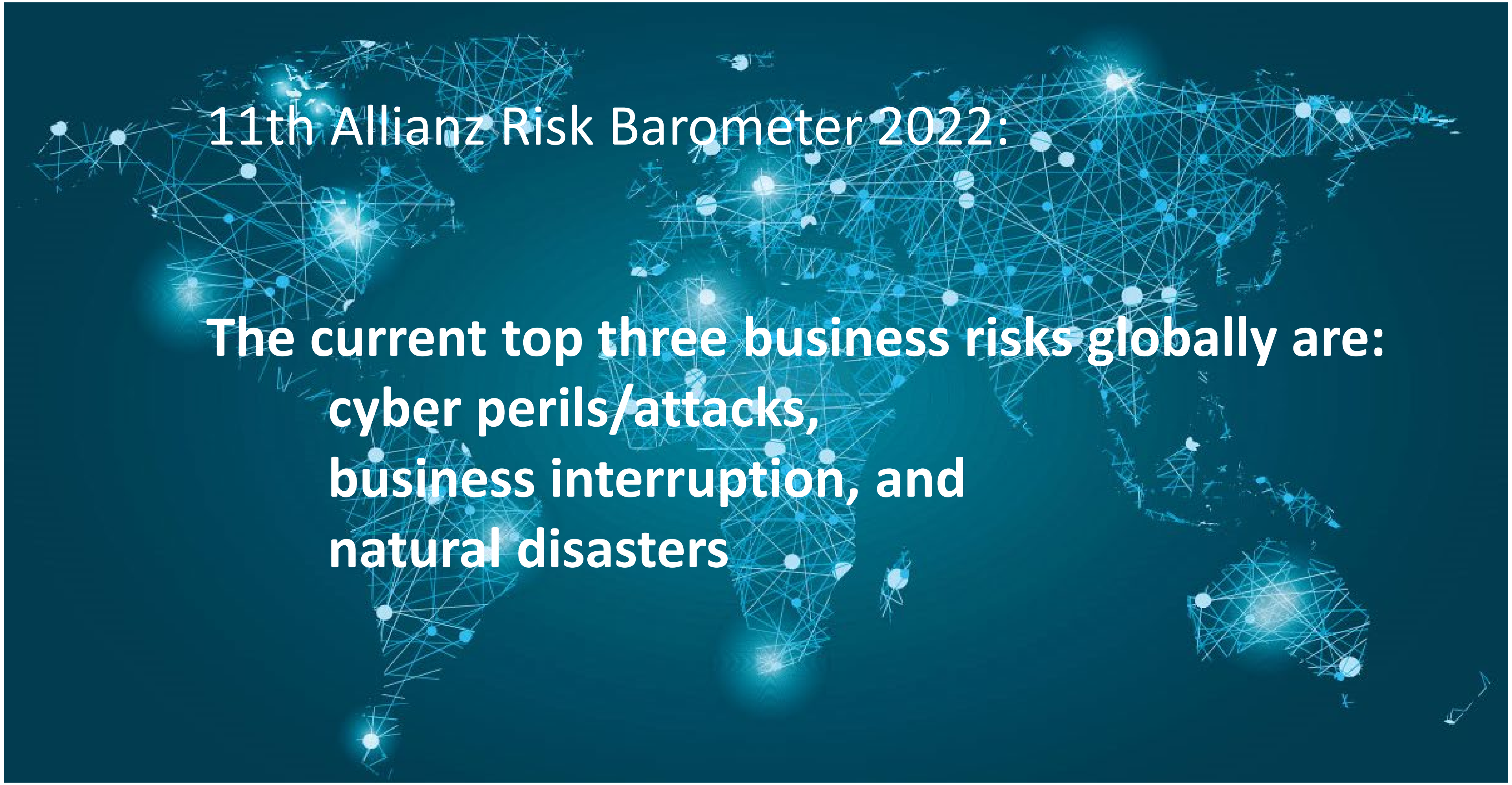
Bundesministerium
für Wirtschaft
und Klimaschutz

aufgrund eines Beschlusses
des Deutschen Bundestages

Outline

1. Background
2. The project “Awareness Lab SME (ALARM) Information Security”
3. Methodological approaches
4. Lessons learned
5. Outlook
6. Acknowledgements
7. References

1. Extensive Digitization as a Background



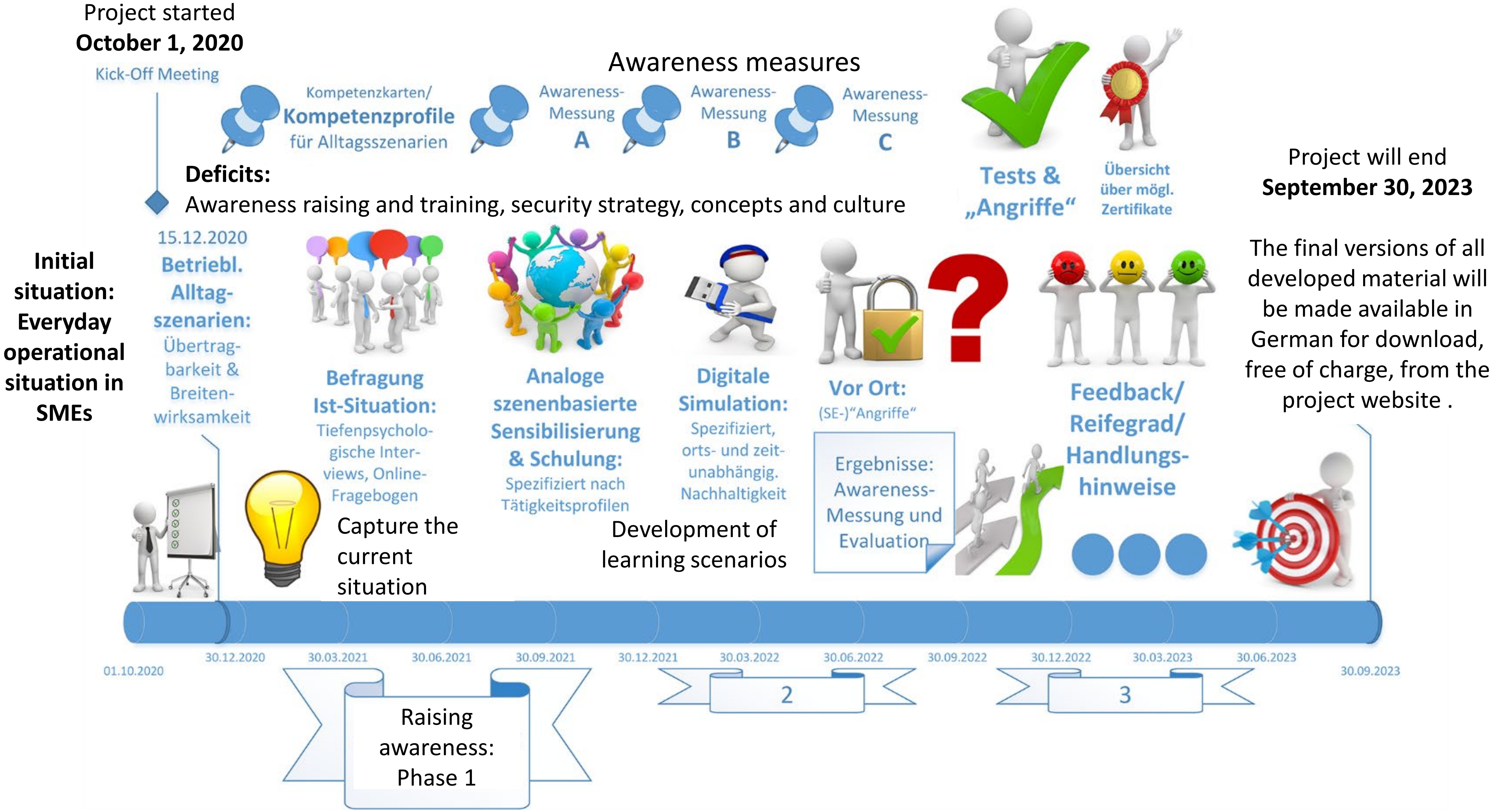
11th Allianz Risk Barometer 2022:

The current top three business risks globally are:

cyber perils/attacks,
business interruption, and
natural disasters

Picture: Ministererklärung: G20 Digital Economy Ministerial Declaration - Shaping Digitalization for an Interconnected World, April 06 and 07, 2017 in Düsseldorf; b20-effective-g20.jpg; https://www.b20germany.org/documents/g20-b20-data/, last access: June 08, 2021.

2. The Project “ALARM Information Security”



Project started **October 1, 2020**

Kick-Off Meeting

Deficits:
Awareness raising and training, security strategy, concepts and culture

Awareness measures

Kompetenzkarten/ Kompetenzprofile für Alltagsszenarien

Awareness-Messung A

Awareness-Messung B

Awareness-Messung C

Tests & „Angriffe“

Übersicht über mögl. Zertifikate

Initial situation: Everyday operational situation in SMEs

15.12.2020 Betriebl. Alltagszenarien: Übertragbarkeit & Breitenwirksamkeit

Befragung Ist-Situation: Tiefenpsychologische Interviews, Online-Fragebogen

Capture the current situation

Analoge szenenbasierte Sensibilisierung & Schulung: Spezifiziert nach Tätigkeitsprofilen

Digitale Simulation: Spezifiziert, orts- und zeitunabhängig. Nachhaltigkeit

Development of learning scenarios

Vor Ort: (SE-)“Angriffe“

Ergebnisse: Awareness-Messung und Evaluation

Feedback/ Reifegrad/ Handlungshinweise

Project will end **September 30, 2023**

The final versions of all developed material will be made available in German for download, free of charge, from the project website .

Raising awareness: Phase 1

2. The project “ALARM Information Security”

ALARM

Thinking Objects

known_sense
awareness you can touch.

gamebook

sudile
supported distance learning

IHK Ostbrandenburg

IHK Potsdam

IHK Cottbus

DIZ DIGITALES INNOVATIONS ZENTRUM

2 Pilot SME

located in Brandenburg

2 Pilot SME

located in Baden-Württemberg

it's.BB
DAS IT-SICHERHEITSNETZWERK BERLIN-BRANDENBURG

Mittelstand 4.0
Kompetenzzentrum
IT-Wirtschaft

Mittelstand 4.0
Kompetenzzentrum
Cottbus

IT-Sicherheit
IN DER WIRTSCHAFT

Mittelstand-
Digital

Technische
Hochschule
Wildau
Technical University
of Applied Sciences
TH WILDAU

Gefördert durch:

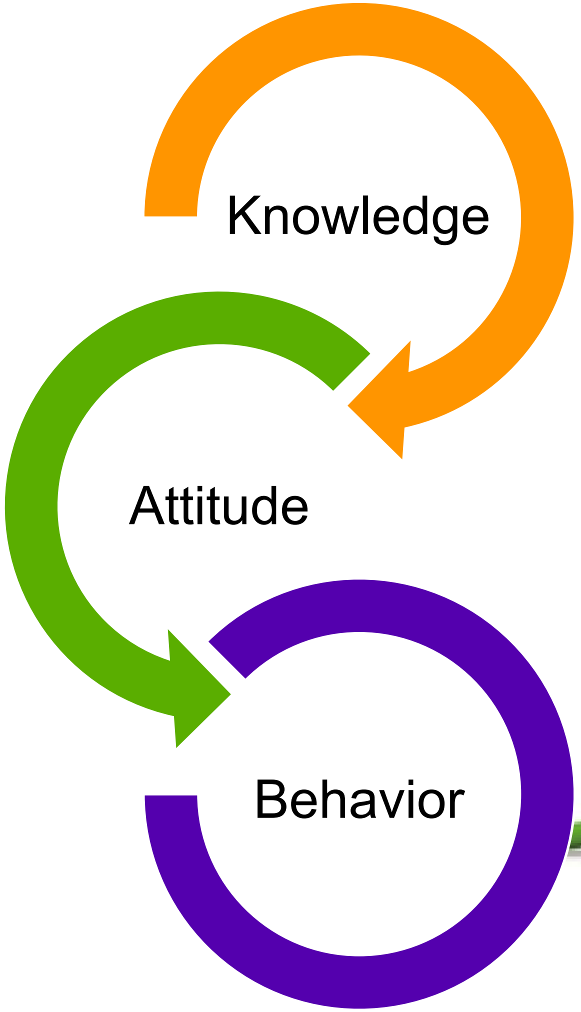
Bundesministerium
für Wirtschaft
und Klimaschutz

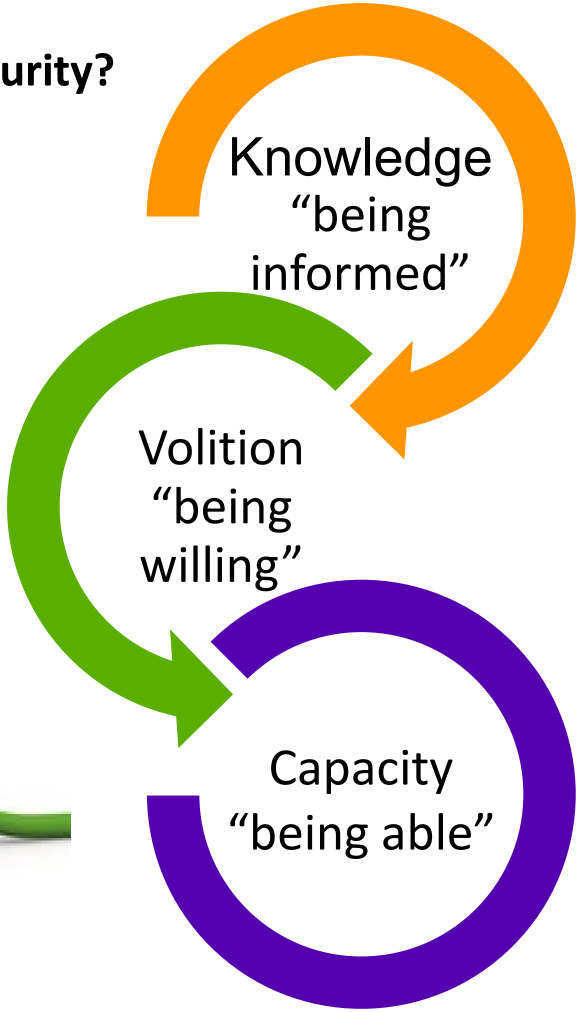
aufgrund eines Beschlusses
des Deutschen Bundestages

2. The project “ALARM Information Security”

How do we increase risk perception and achieve more awareness of information security?

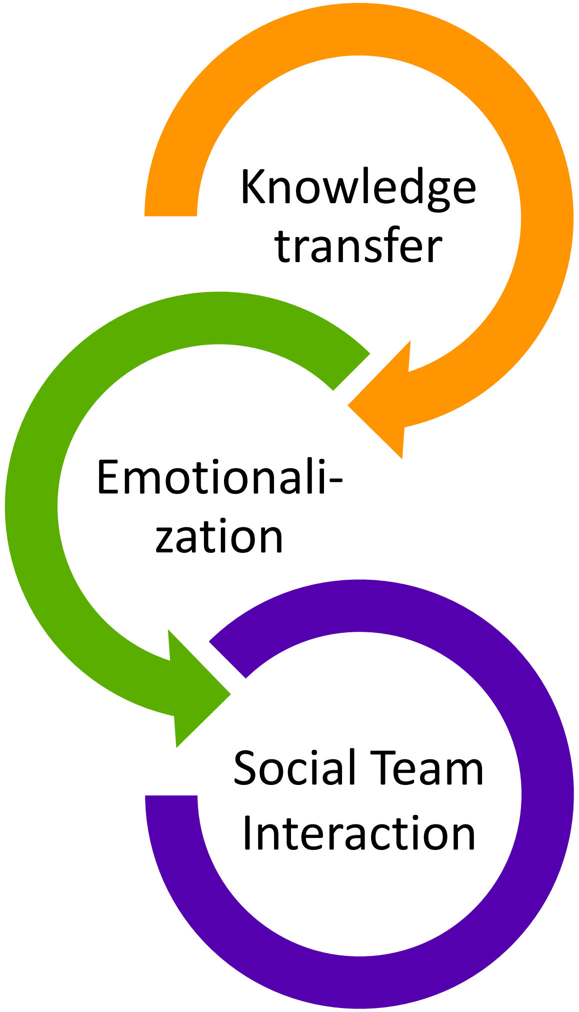
INTERNATIONAL





GERMANY

2. The project “ALARM Information Security”



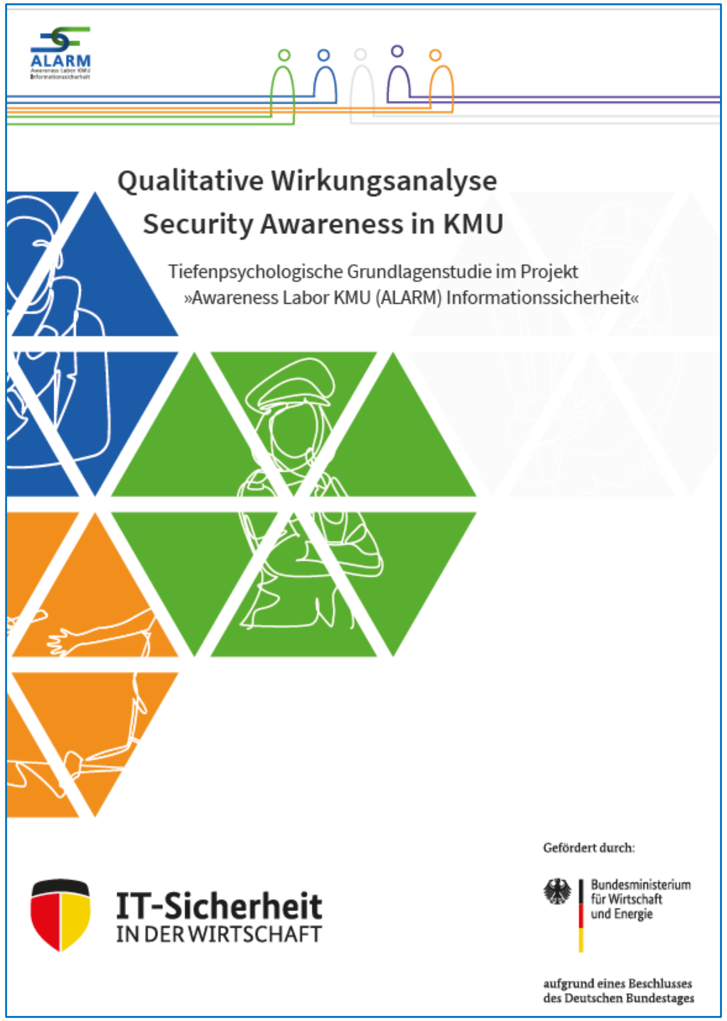
How do we increase risk perception and achieve more awareness of information security?

Exchanging experience
Telling real stories
Understanding
Interacting
Practicing
Feeling empathy

3. Methodological Approaches: Study 1

known_sense
awareness you can touch.

ALARM



ALARM

Qualitative Wirkungsanalyse
Security Awareness in KMU

Tiefenpsychologische Grundlagenstudie im Projekt
»Awareness Labor KMU (ALARM) Informationssicherheit«

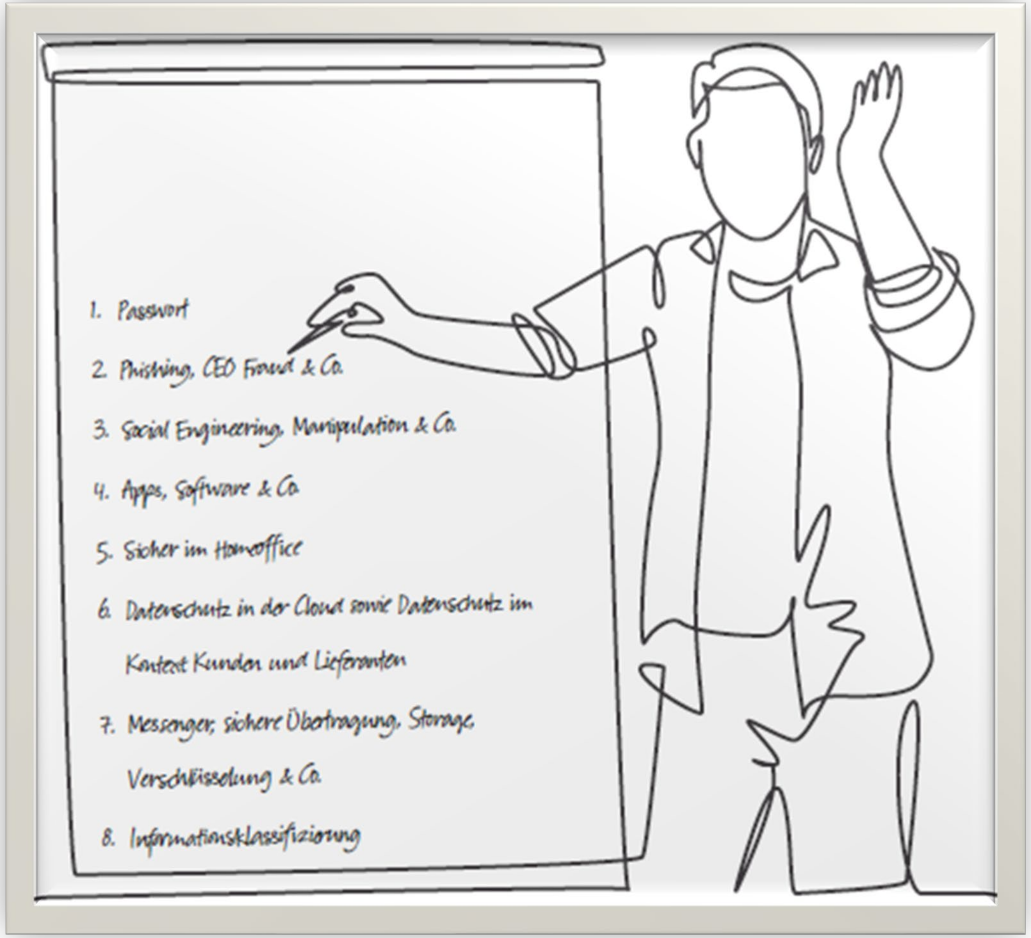
IT-Sicherheit
IN DER WIRTSCHAFT

Gefördert durch:

Bundesministerium
für Wirtschaft
und Energie

aufgrund eines Beschlusses
des Deutschen Bundestages

16 in-depth interviews



1. Passwort
2. Phishing, CEO Fraud & Co.
3. Social Engineering, Manipulation & Co.
4. Apps, Software & Co.
5. Sicher im Homeoffice
6. Datenschutz in der Cloud sowie Datenschutz im Kontext Kunden und Lieferanten
7. Messenger, sichere Übertragung, Storage Verschlüsselung & Co.
8. Informationsklassifizierung

3. Methodological Approaches: Report 1

Evaluation of 73 questions on work activity

ALARM

IT-Sicherheit
IN DER WIRTSCHAFT

2021

Report zur Informationssicherheit in KMU – Sicherheitsrelevante Tätigkeitsprofile

Mittelstand-Digital

Gefördert durch:

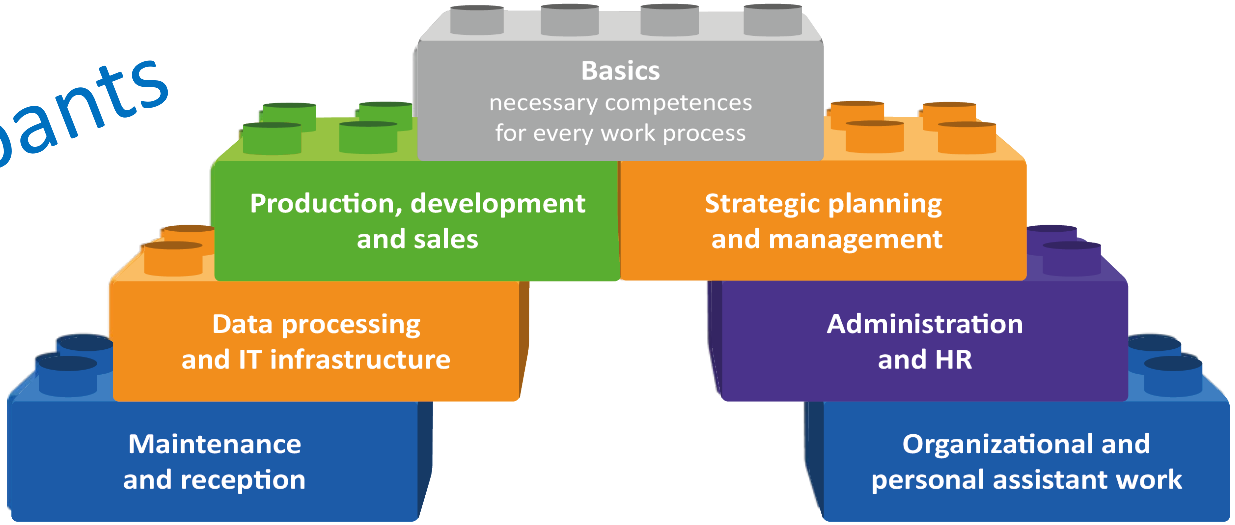
Bundesministerium für Wirtschaft und Klimaschutz

aufgrund eines Beschlusses des Deutschen Bundestages

108 participants

The “Profile Arc” presents developed job profiles as a planning aid for training needs

Development of the “Profile Arc”



Basics
necessary competences for every work process
Production, development and sales
Strategic planning and management
Data processing and IT infrastructure
Administration and HR
Maintenance and reception
Organizational and personal assistant work

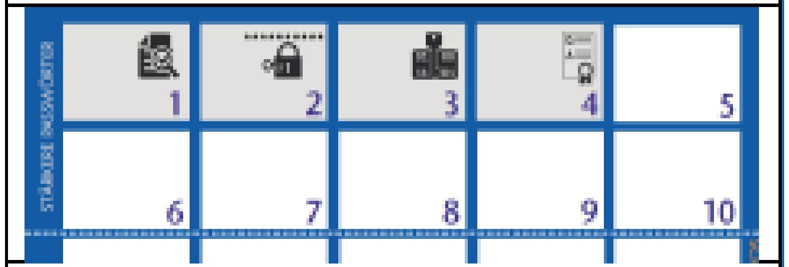
- Fields of activity require several competence profiles
- Competence profile modules overlap and intertwine
- Identification of core and gatekeeper modules
- Module-like structure of learning events necessary

3. Methodological Approaches: Analog

known_sense
awareness you can touch.

ALARM

1: Home Office



2: Password & Data Protection & Cloud

3: CEO Fraud

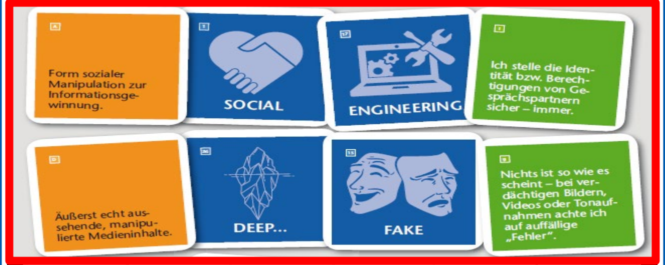
DIVERSITY & FLEXIBILITY

- 3 Iterations per game
- Reduceable to 15 min.
- Many tests in practice

Abbildungen von Personen aus sozialen Netzwerken
Biometrische Daten
Mitarbeitende (Name, Kontakt, Geburtsdatum, Konfession, Bank)

- Feedbacks used
- Improvements

4: Software & Apps


Form sozialer Manipulation zur Informationsgewinnung.
SOCIAL
ENGINEERING
Ich stelle die Identität bzw. Berechtigungen von Gesprächspartnern sicher – immer.
Äußerst echt aussehende, manipulierte Medieninhalte.
DEEP...
FAKE
Nichts ist so wie es scheint – bei verdächtigen Bildern, Videos oder Tonaufnahmen achte ich auf auffällige „Fehler".

5: Social Engineering (Cyber Pairs)

GROBKONZEPT LS 6:
New:
Data protection

6: Idea for Messenger & Encryption

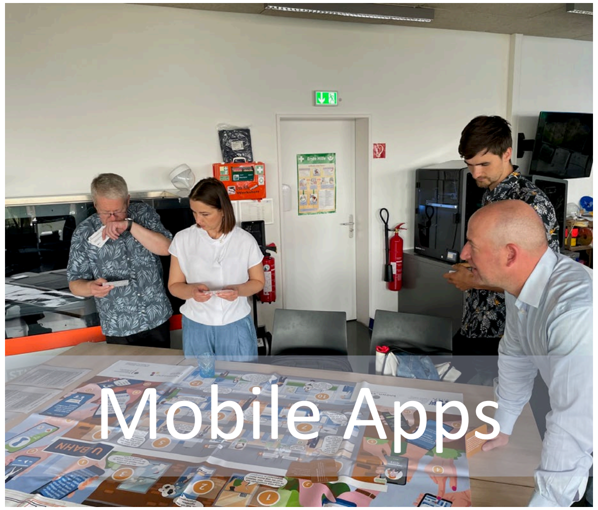
7: Idea for Information Classification

3. Methodological Approaches: Awareness Trainings

I'm never in the home office. I clearly separate work and private life.

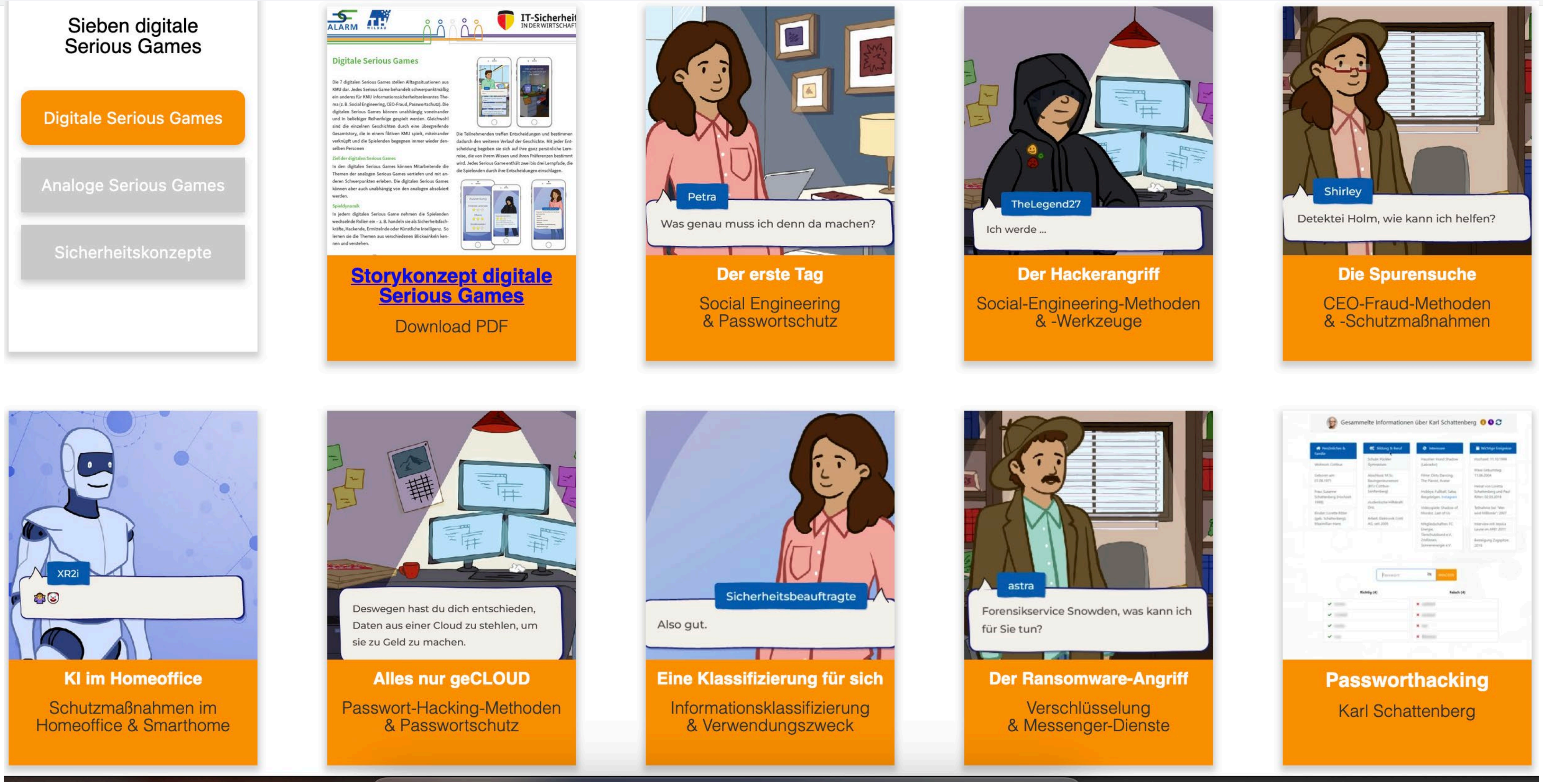
We receive inquiries from our bank about large transactions.

The know-how of our company is on the server...that's the gold



The speed scares me at my age.

3. Methodological Approaches: Digital



Sieben digitale Serious Games

IT-Sicherheit IN DER WIRTSCHAFT

Digitale Serious Games

Die 7 digitalen Serious Games stellen Alltagssituationen aus KMU dar. Jedes Serious Game behandelt schwerpunktmäßig ein anderes für KMU informationssicherheitsrelevantes Thema (z. B. Social Engineering, CEO-Fraud, Passwortschutz). Die digitalen Serious Games können unabhängig voneinander und in beliebiger Reihenfolge gespielt werden. Gleichwohl sind die einzelnen Geschichten durch eine übergreifende Gesamtstory, die in einem fiktiven KMU spielt, miteinander verknüpft und die Spielenden begegnen immer wieder denselben Personen

Ziel der digitalen Serious Games

In den digitalen Serious Games können Mitarbeitende die Themen der analogen Serious Games vertiefen und mit anderen Schwerpunkten erleben. Die digitalen Serious Games können aber auch unabhängig von den analogen absolviert werden.

Spieldynamik

In jedem digitalen Serious Game nehmen die Spielenden wechselnde Rollen ein – z. B. handeln sie als Sicherheitsfachkräfte, Hackende, Ermittelnde oder Künstliche Intelligenz. So lernen sie die Themen aus verschiedenen Blickwinkeln kennen und verstehen.

Die Teilnehmenden treffen Entscheidungen und bestimmen dadurch den weiteren Verlauf der Geschichte. Mit jeder Entscheidung begeben sie sich auf ihre ganz persönliche Lernreise, die von ihrem Wissen und ihren Präferenzen bestimmt wird. Jedes Serious Game enthält zwei bis drei Lernpfade, die die Spielenden durch ihre Entscheidungen einschlagen.

Storykonzept digitale Serious Games

Download PDF

Der erste Tag

Social Engineering & Passwortschutz

Der Hackerangriff

Social-Engineering-Methoden & -Werkzeuge

Die Spurensuche

CEO-Fraud-Methoden & -Schutzmaßnahmen

KI im Homeoffice

Schutzmaßnahmen im Homeoffice & Smarthome

Deswegen hast du dich entschieden, Daten aus einer Cloud zu stehlen, um sie zu Geld zu machen.

Alles nur geCLOUD

Passwort-Hacking-Methoden & Passwortschutz

Eine Klassifizierung für sich

Informationsklassifizierung & Verwendungszweck

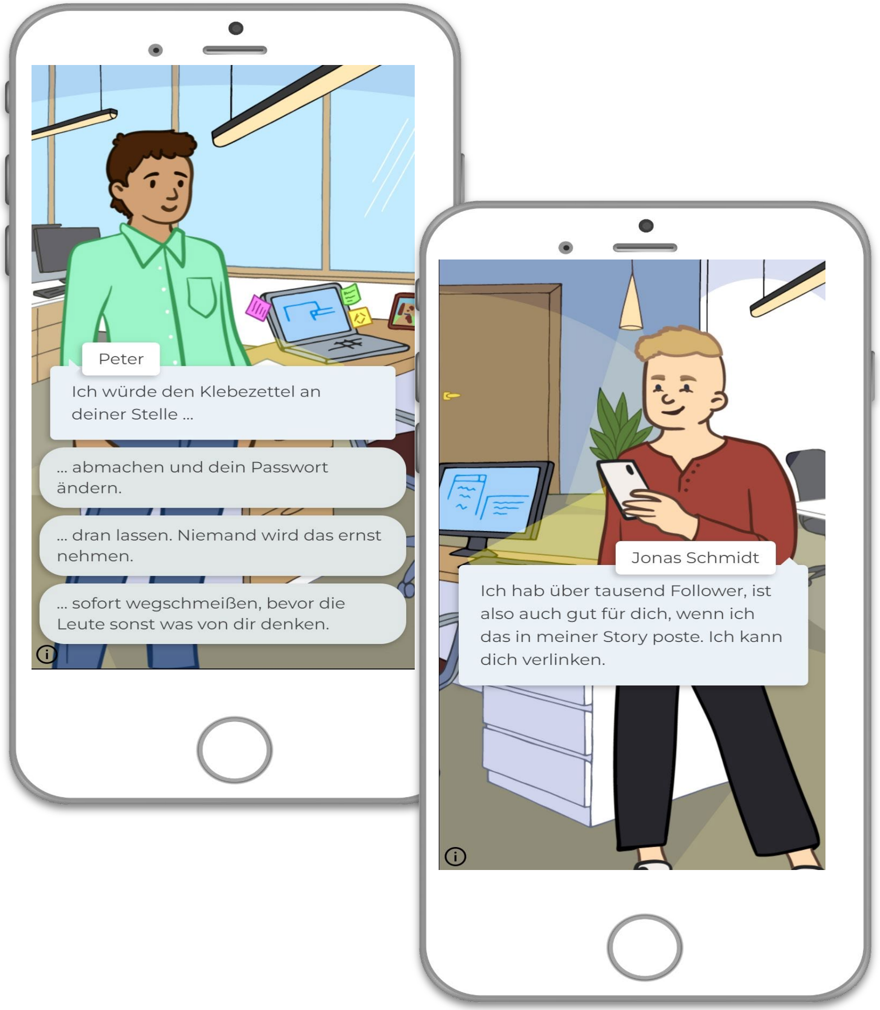
Der Ransomware-Angriff

Verschlüsselung & Messenger-Dienste

Passworthacking

Karl Schattenberg

3. Methodological Approaches: Digital



Peter

Ich würde den Klebezettel an deiner Stelle ...

... abmachen und dein Passwort ändern.

... dran lassen. Niemand wird das ernst nehmen.

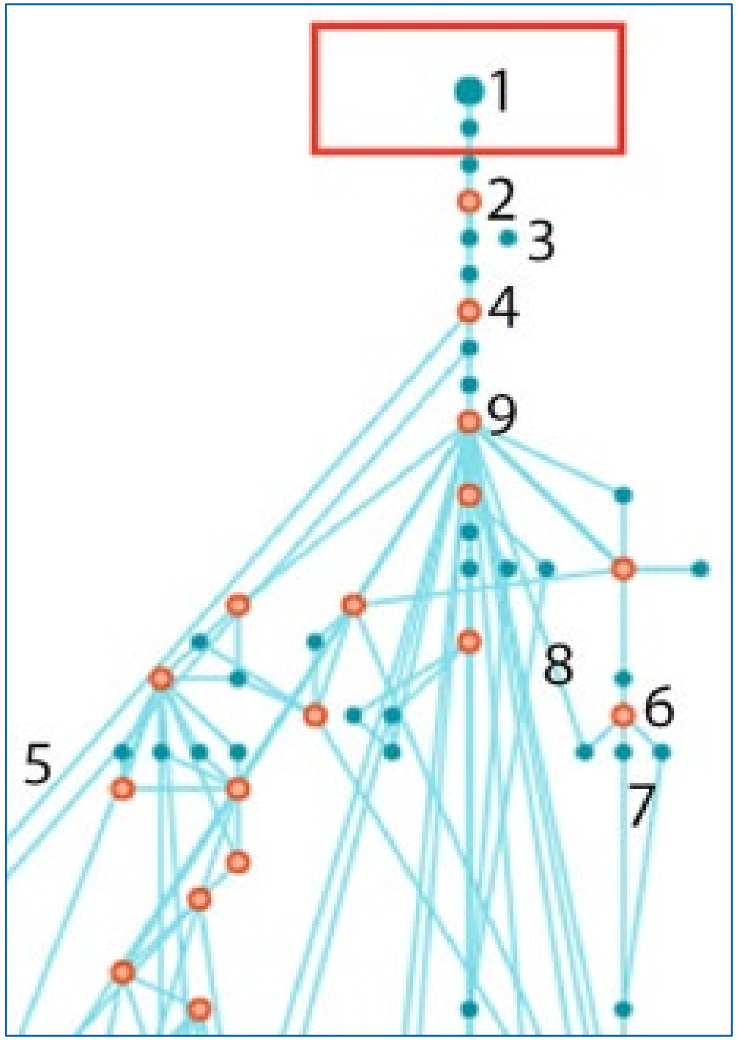
... sofort wegschmeißen, bevor die Leute sonst was von dir denken.

Jonas Schmidt

Ich hab über tausend Follower, ist also auch gut für dich, wenn ich das in meiner Story poste. Ich kann dich verlinken.

DIVERSITY & INDIVIDUALITY

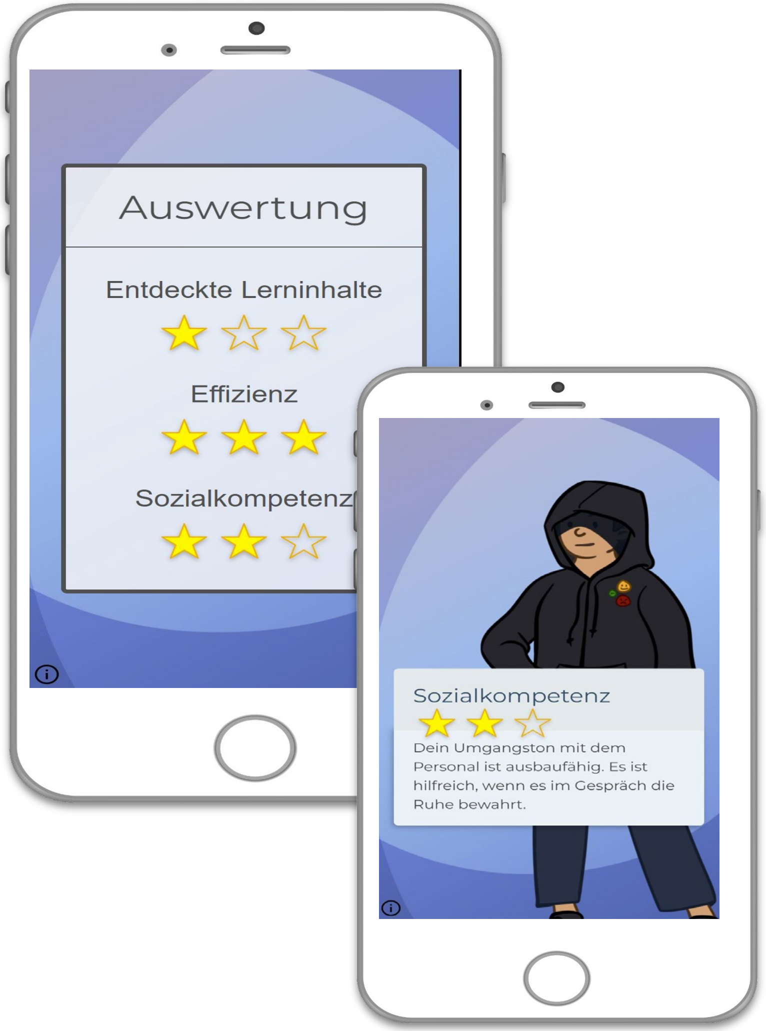
- Different first-person perspectives: you are the hero of the immersive story
- Various issues in visual novel format
- Playable independently in any order



3. Methodological Approaches: Digital

EACH LEARNING SCENARIO CONTAINS:

- 2–3 learning paths
- Differentiation
- 2–3 skills
- Same, well-known game characters
- Emotional design
- Points system with hints



Auswertung

Entdeckte Lerninhalte

★☆☆

Effizienz

★★★

Sozialkompetenz

★★☆

Sozialkompetenz

★★☆

Dein Umgangston mit dem Personal ist ausbaufähig. Es ist hilfreich, wenn es im Gespräch die Ruhe bewahrt.

3. Methodological Approaches: On-site attacks

Ethical questions:

- Enlightenment
- Information as an aid and training
- Comprehend as promotion of a positive error culture
- Optimization of processes, procedures, responsibilities

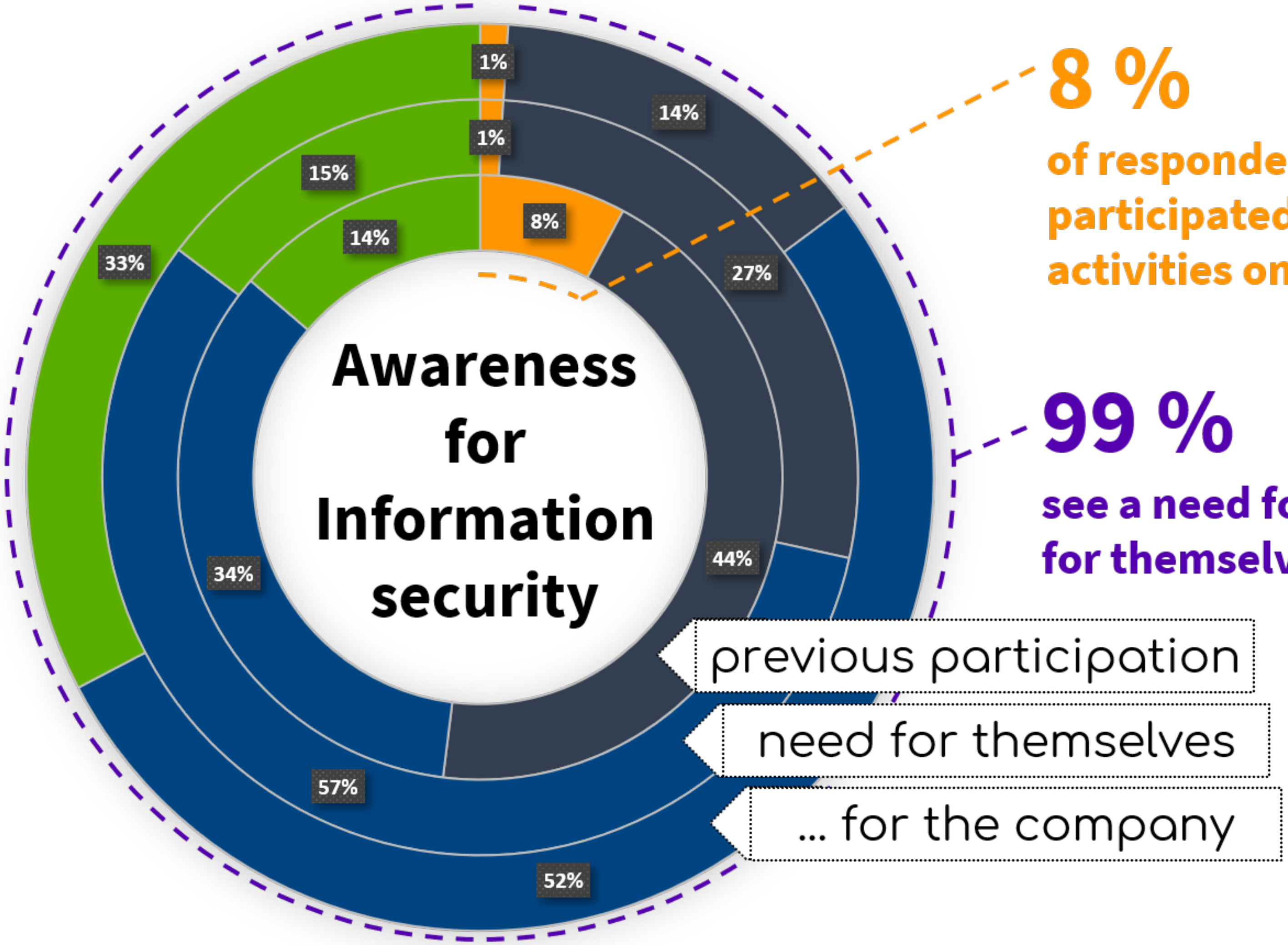
EACH LEARNING SCENARIO CONTAINS:

- Must be done with extreme caution
- Agreed with the top manager
- Practice-oriented instructions and tips
- Low-threshold security concepts

The ethical principles also mean **no** personal

- exposure
- disturbances in the working atmosphere and of processes
- punitive measures

4. Lessons learned: Needs from report 1



8 %

of respondents have "Never" participated in awareness-raising activities on information security

99 %

see a need for training for themselves or the SME

4. Lessons learned: Hypotheses about the training

(H1) It is possible to enable authentic learning by tailoring profile groups to employees' everyday work and user behavior

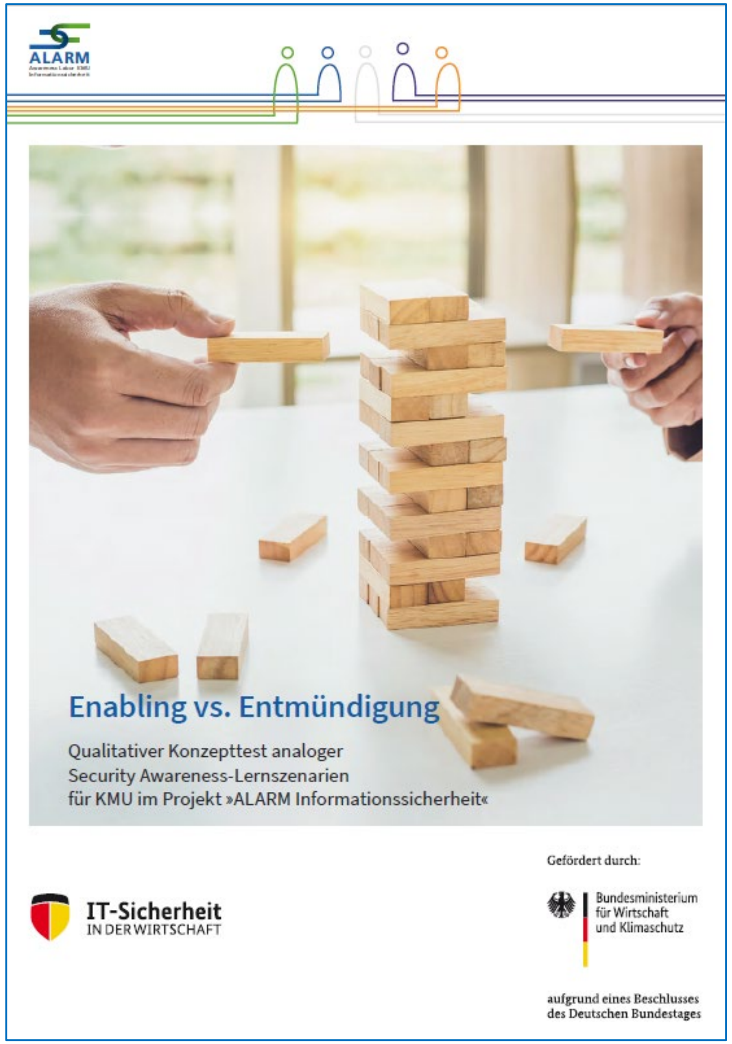
CONFIRMED

…but only in concepts of modules and "lighthouses"

(H2) Information security training is needed for every job profile in SMEs

CONFIRMED

4. Lessons learned: Analog learning scenarios (Study 2)



Enabling vs. Entmündigung

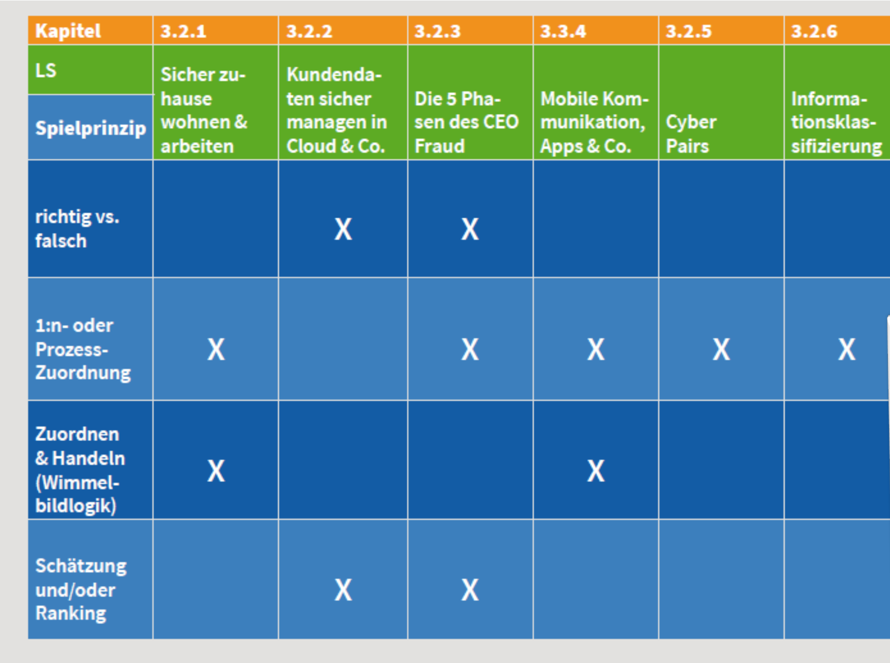
Qualitativer Konzepttest analoger Security Awareness-Lernszenarien für KMU im Projekt »ALARM Informationssicherheit«

Gefördert durch:

IT-Sicherheit IN DER WIRTSCHAFT

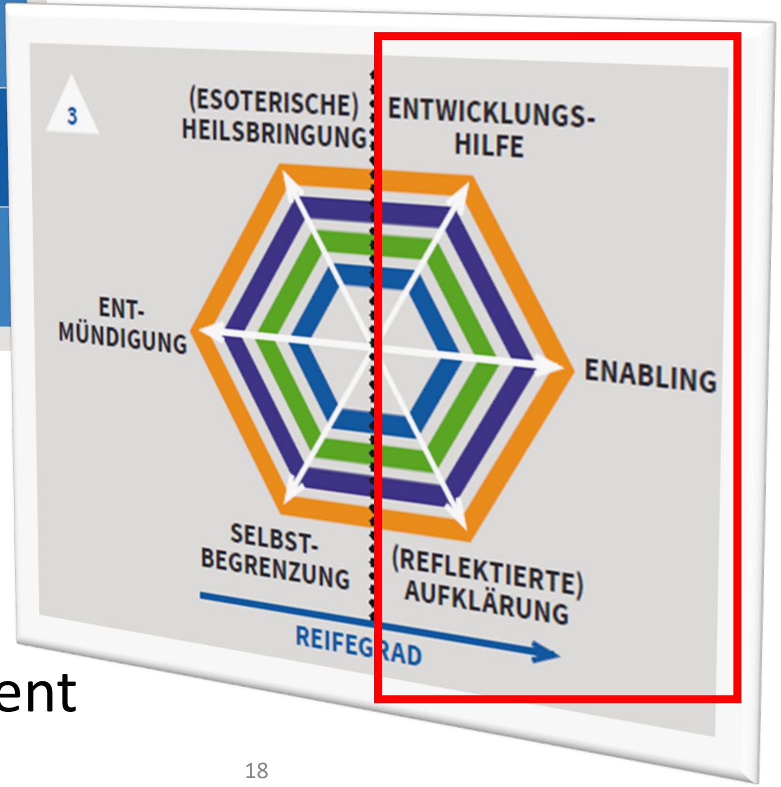
Bundesministerium für Wirtschaft und Klimaschutz

aufgrund eines Beschlusses des Deutschen Bundestages



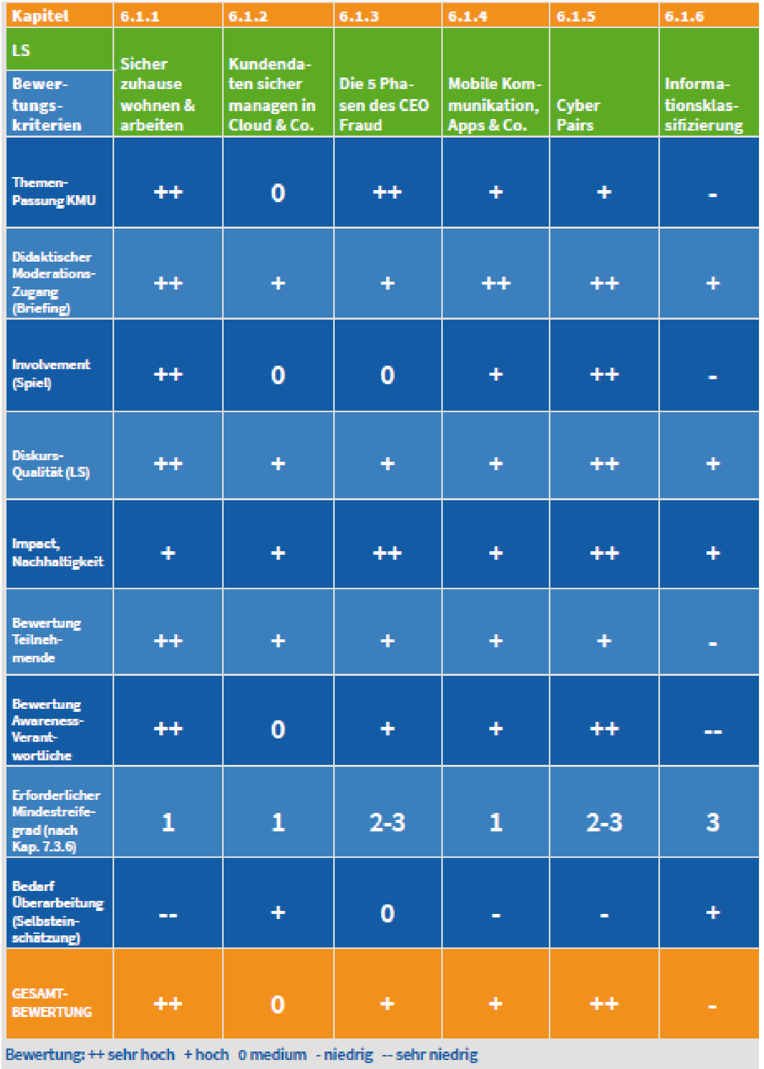
Kapitel	3.2.1	3.2.2	3.2.3	3.3.4	3.2.5	3.2.6
LS Spielprinzip	Sicher zuhause wohnen & arbeiten	Kundendaten sicher managen in Cloud & Co.	Die 5 Phasen des CEO Fraud	Mobile Kommunikation, Apps & Co.	Cyber Pairs	Informationsklassifizierung
richtig vs. falsch		X	X			
1:n- oder Prozess-Zuordnung	X		X	X	X	X
Zuordnen & Handeln (Wimmelbildlogik)	X			X		
Schätzung und/oder Ranking		X	X			

Development Assistance
Empower & Activate
Reflected Enlightenment



Enabling versus disenfranchisement

4. Lessons learned: Analog learning scenarios (Study 2)



Kapitel	6.1.1	6.1.2	6.1.3	6.1.4	6.1.5	6.1.6
LS Bewertungskriterien	Sicher zuhause wohnen & arbeiten	Kundendaten sicher managen in Cloud & Co.	Die 5 Phasen des CEO Fraud	Mobile Kommunikation, Apps & Co.	Cyber Pairs	Informationsklassifizierung
Themen-Passung KMU	++	0	++	+	+	-
Didaktischer Moderations-Zugang (Briefing)	++	+	+	++	++	+
Involvement (Spiel)	++	0	0	+	++	-
Diskurs-Qualität (LS)	++	+	+	+	++	+
Impact, Nachhaltigkeit	+	+	++	+	++	+
Bewertung Teilnehmende	++	+	+	+	+	-
Bewertung Awareness-Verantwortliche	++	0	+	+	++	--
Erforderlicher Mindestreifegrad (nach Kap. 7.3.6)	1	1	2-3	1	2-3	3
Bedarf Überarbeitung (Selbsteinschätzung)	--	+	0	-	-	+
GESAMT-BEWERTUNG	++	0	+	+	++	-

Bewertung: ++ sehr hoch + hoch 0 medium - niedrig -- sehr niedrig

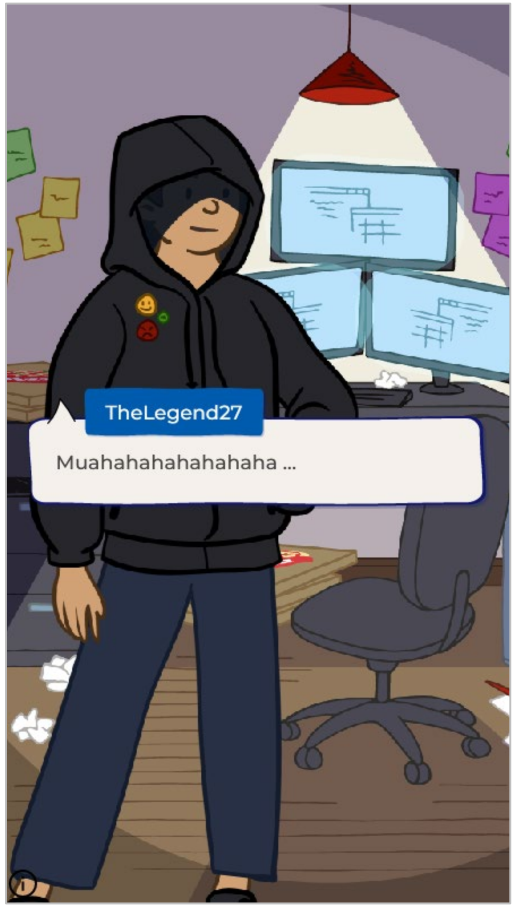
Lessons learned

- Our analog simulations are revitalizing awareness tools
- Communication made easy: “Home office,” cyber pair, mobile communication & apps & co
- All scenarios work well to very well, but not equally well everywhere.

4. Lessons learned: Digital learning scenarios

ALARM

Hacker Attack



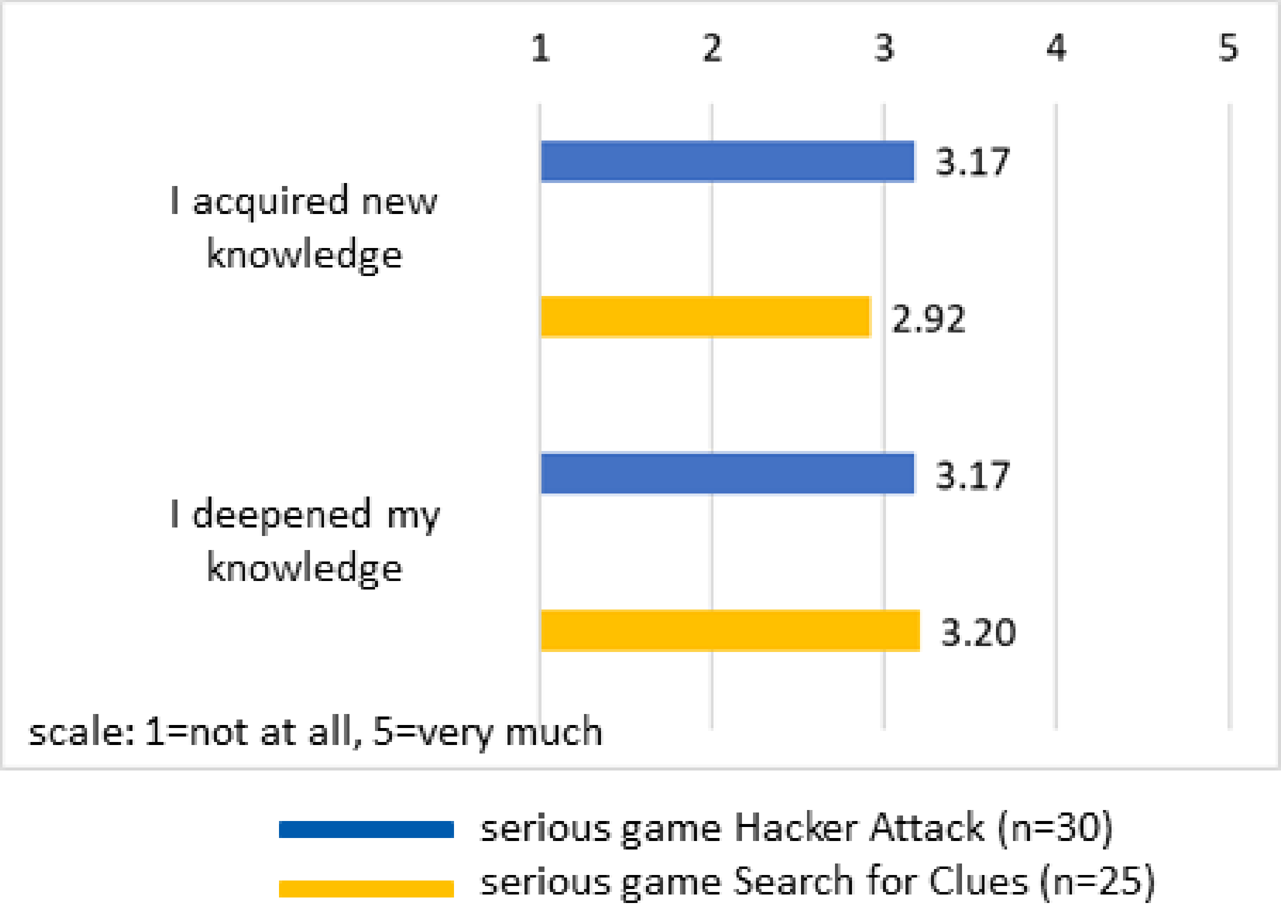
TheLegend27

Muahahahahahahaha ...

Search for Clues

Shirley

Wenn wir uns beeilen, schaffen wir es vielleicht, den Scam zu verhindern.



4. Lessons learned: On-site attacks

Pros

- Improving awareness through announcement
- Concrete cognition after the evaluation
- Rated better than theoretical papers/ training (both by management and employees)

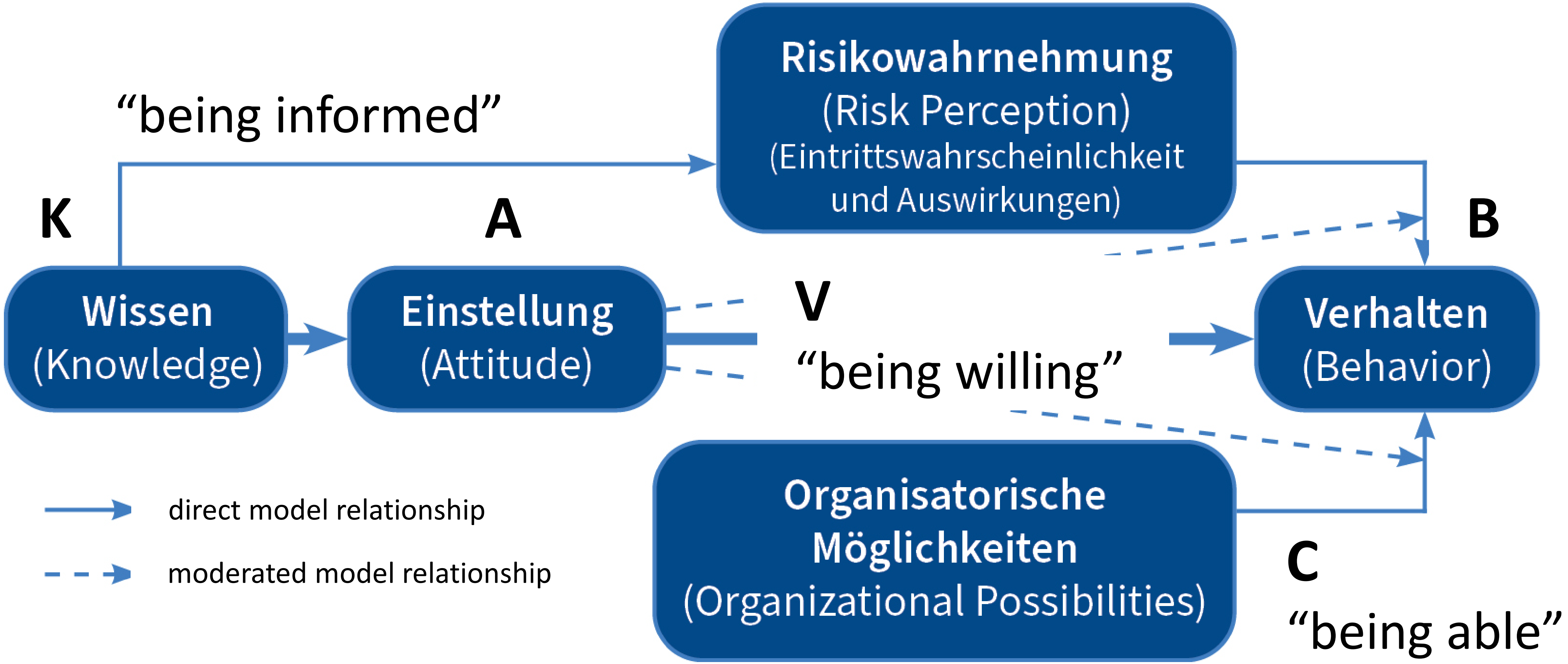
Cons

- Delays in completing surveys
- High organizational and communicative outlay
- Corrections in the processes cannot be checked (would require a repetition of the attacks)

4. Lessons learned: What and how do we measure?

- What do we need?
- What are we measuring?
- How can we measure what?
- What information do self-interviews provide?
- Do questionnaires and tests with knowledge surveys reflect reality?
- How can we infer awareness from understanding?
- How can we infer consciousness from a person's understanding or attitude?
- How can we infer actual behavior from the answers?
- …

4. Lessons learned: Idea of model integration

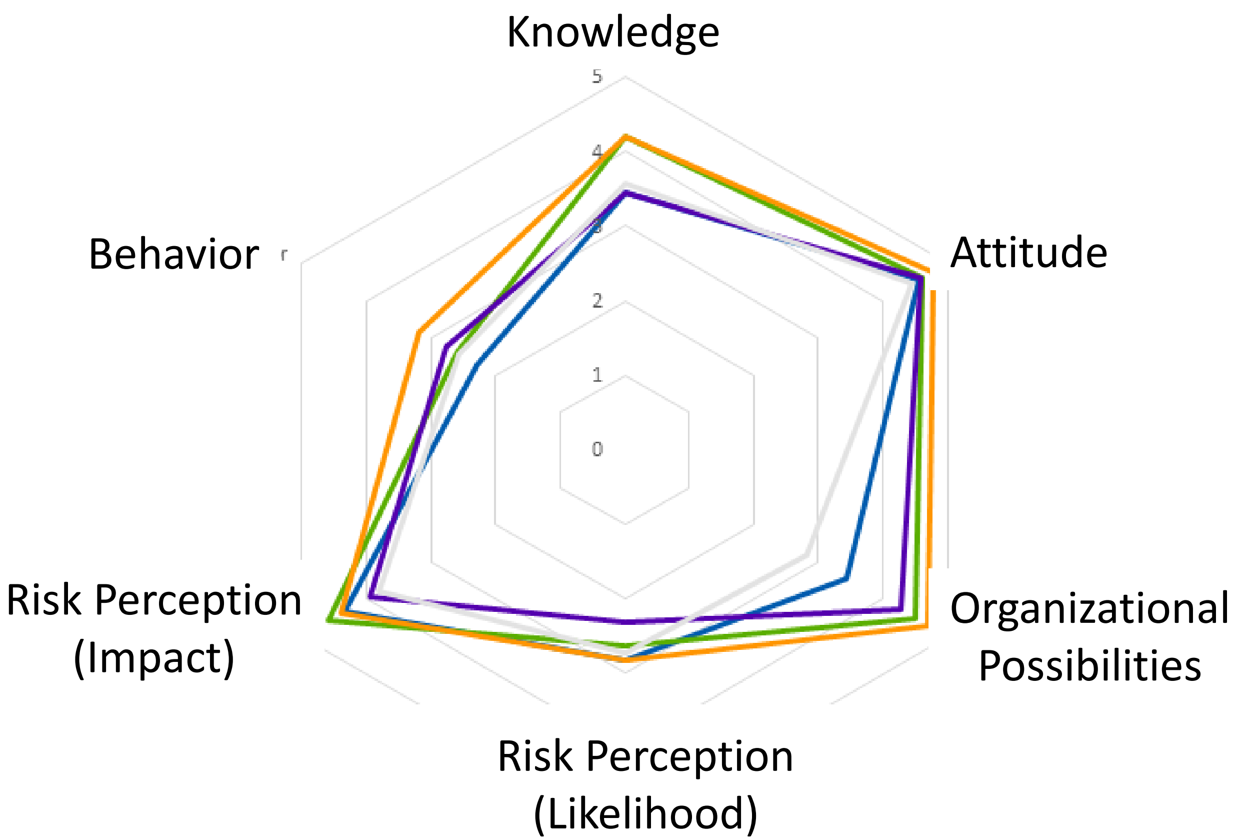


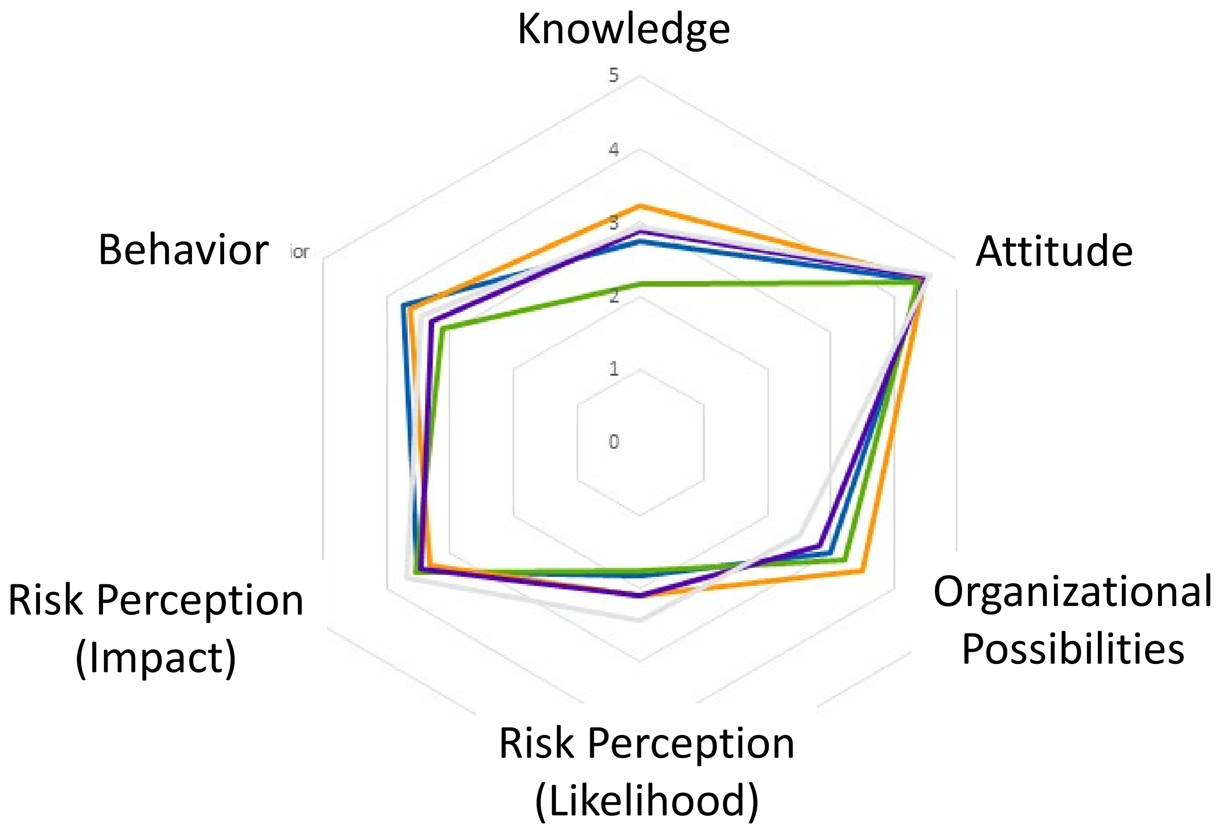
4. Lessons learned: Measurements (ongoing research)

Information security in general

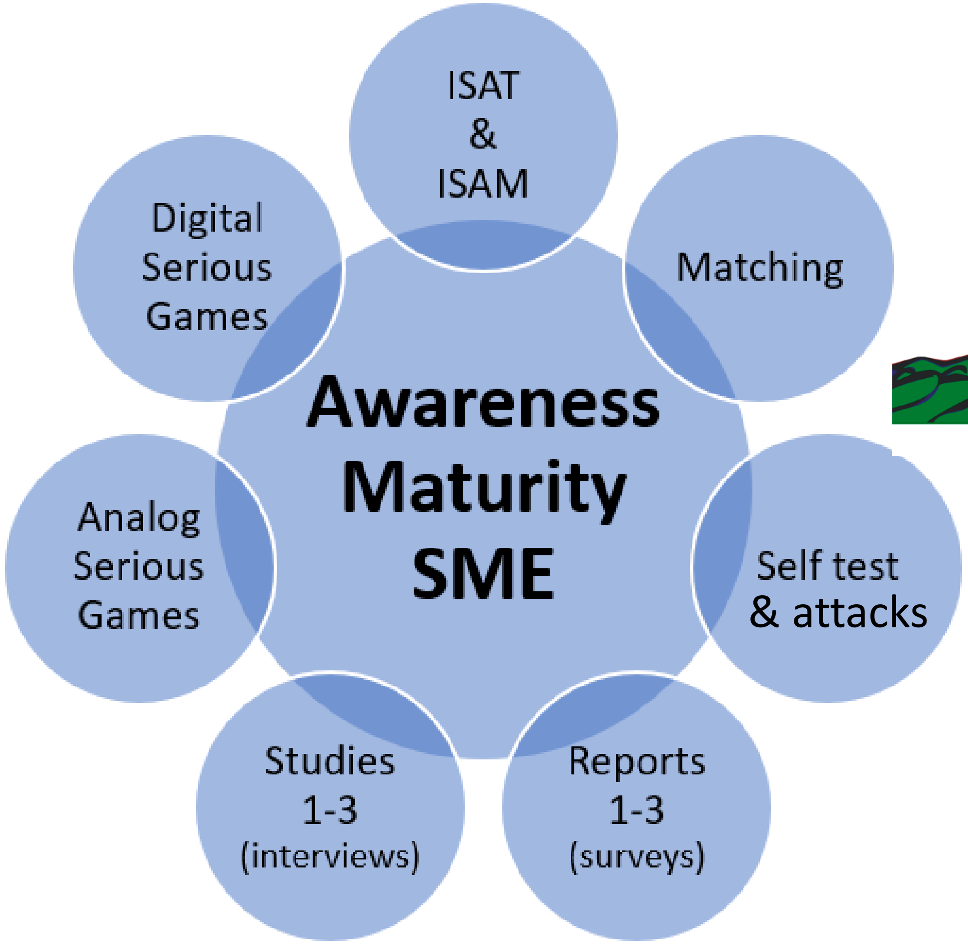
Mobile apps

Test group 1 *Test group 2* *Control group* *Test group 3* *Test group 4*





5. Outlook



sudile
supported distance learning

ALARM

Technische Hochschule Wildau
Technical University of Applied Sciences
WILDAU

Awareness Lab SME (ALARM) Information Security
https://alarm.wildau.biz/en

Sustainable Information Security Sensitization in SMEs: Designing Measures with Long-Term Effect

Prof. Margit Scholl, PhD

IT-Sicherheit IN DER WIRTSCHAFT

Thank you for attention & listening!

Gefördert durch:

Bundesministerium für Wirtschaft und Klimaschutz

aufgrund eines Beschlusses des Deutschen Bundestages

6. Acknowledgements

As the initiator of “Awareness Lab SME (ALARM) Information Security” and project manager, I would like to thank the Federal Ministry for Economic Affairs and Climate Action for funding this project.

I am grateful to our long-standing security awareness partner, the company known_sense, and the other subcontractors, Gamebook Studio, Thinking Objects, and sudile, whose special input into the project can be found on the project website https://alarm.wildau.biz/en.

My special thanks to the pilot companies for their active involvement and to my research team—also featured on the project website—who have moved the project forward in different constellations.

Finally, I would like to acknowledge the anonymous reviewers for their helpful critical comments.

Many thanks, too, to Simon Cowper for his detailed and professional proofreading of the text.

7. References

- AGCS—Allianz Global Corporate & Specialty SE (Ed.) (2022a). *Allianz risk barometer 2022. https://www.agcs.allianz.com/content/dam/onemarketing/agcs/agcs/reports/Allianz-Risk-Barometer-2022.pdf* (English version: worldwide results).
- AGCS—Allianz Global Corporate & Specialty SE (Ed.) (2022b). *Allianz Risk Barometer 2022* (German version: results of Germany)
- Arriaga, P., Esteves, F., & Fernandes, S. (2013). Playing for better or for worse? Health and social outcomes with electronic gaming. In M. M. Cruz-Cunha, I. M. Miranda & P. Gonçalves (Eds.), *Handbook of research on ICTs for human-centered healthcare and social care services* (pp. 48–69). IGI Global.
- Bada, M., Sasse, A.M., & Nurse, J.R. (2019). Cyber Security Awareness Campaigns: Why do they fail to change behaviour? ArXiv, abs/1901.02672
- Bernardes, O., Amorim, V., & Moreira, A. C. (2022) (Eds.). *Handbook of Research on Cross-Disciplinary Uses of Gamification in Organizations*. IGI Global.
- Burke, M. J., Sarpy, S. A., Smith-Crowe, K., Chan-Serafin, S., Salvador, R. O., & Islam, G. (2006). Relative effectiveness of worker safety and health training methods. American journal of public health, 96(2), 315-324.
- Cialdini, R. B. (2007). Descriptive social norms as underappreciated sources of social control. Psychometrika, 72(2), 263-268.
- Collard, A. (2022). „Verhaltensdesign in Security Awareness Programmen, Webinar of KnowBe4, May 20, 2022)"/ "Behavioral Design in Security Awareness Programs".
- DIHK—Deutscher Industrie- und Handelskammertag e. V. (Ed.) (2022). *Zeit für den digitalen Aufbruch: Die IHK-Umfrage zur Digitalisierung/Time for the digital awakening. The IHK survey on digitization.*
- ENISA—European Union Agency for Network and Information Security (2019). *Cybersecurity Culture Guidelines: Behavioural Aspects of Cybersecurity*.
- BSI —Federal Office for Information Security (Ed.) (2020). *BSI-Kompendium, Baustein ORP.3*.
- BSI—Federal Office for Information Security (Ed.) (2017). *BSI-Standards*.

7. References

- Fogg, B. J. (n.d.). *Fogg Behavior Model*. Retrieved May 26, 2022, from https://behaviormodel.org/
- Hallsworth, M., Snijders, V., Burd, H., Prestt, J., Judah, G., Huf, S., & Halpern, D. (2016). Applying behavioral insights: simple ways to improve health outcomes. World Innovation Summit for Health, Doha, Qatar, 29–30 November.
- Helisch, M., & Pokoyski, D. (Eds.) (2009). *Security Awareness – Neue Wege zur erfolgreichen Mitarbeiter- Sensibilisierung/ Security Awareness - New ways to successfully raise employee awareness.* Wiesbaden: Springer Vieweg.
- ISF (2014). *From Promoting Awareness to Embedding Behaviors, Secure by choice not by chance*.
- ISO/IEC 27001: 2017. Berlin: Beuth, 2017.
- ISO/IEC 27000:2018(E), Information technology — Security techniques — Information security management systems — Overview and vocabulary. INTERNATIONAL STANDARD ISO/IEC 27000, fifth edition 2018-02.
- known_sense (ed.) (2016). *Security Awareness Framework*. Cologne.
- Kruger, H. A., & Kearney W. D. (2006). A prototype for assessing information security awareness, Computers & Security, Vol. 25, No. 4, pp. 289–296.
- Lacey, D. (2009). *Managing the Human Factor in Information Security: How to win over staff and influence business managers*. John Wiley & Sons.
- Lacruz, A. J., & Américo, B. L. (2018). Debriefing's Influence on Learning in Business Game: An Experimental Design. *BBR. Brazilian Business Review*, *15*, 192-208.
- Naul, E., & Liu, M. (2020). Why Story Matters: A Review of Narrative in Serious Games. Journal of Educational Computing Research, Vol. 58, No. 3, pp. 687-707.
- Pokoyski, D., Matas, I., Haucke, A., & Scholl, M. (2021). *Qualitative Wirkungsanalyse Security Awareness in KMU* (Projekt "ALARM Informationssicherheit") (p. 72). Wildau: Technische Hochschule Wildau.

7. References

- Sasse, M. A., Hielscher, J., Friedauer, J., & Peiffer, M. (2022). Warum IT-Sicherheit in Organisationen einen Neustart braucht/Why IT security in organizations needs a fresh start. Federal Office for Information Security (BSI) (ed.) (2022): Proceedings of the 18. Deutscher IT-Sicherheitskongress des BSI/18th German IT Security Congress of the BSI, Februar 2022. At: Virtual Event Volume: ISBN 978-3-922746-84-3.
- Schell, J. (2020). *Die Kunst des Game Designs: bessere Games konzipieren und entwickeln*. BoD–Books on Demand. 2. Edition, 2016.
- Scholl, M. C., Fuhrmann, F., & Scholl, L. R. (2018). Scientific knowledge of the human side of information security as a basis for sustainable trainings in organizational practices, Proceedings of the 51st Hawaii International Conference on System Sciences.
- Slusky, L., & Partow-Navid, P. (2012). Students Information Security Practices and Awareness, Journal of Information Privacy and Security, Vol. 8, No. 4, 2012, pp. 3–26.
- Volkamer, M., Sasse, M. A., & Boehm, F. (2020). Analysing Simulated Phishing Campaigns for Staff. *European Symposium on Research in Computer Security* (pp. 312-328). Cham: Springer.
- Tippelskirch, H., Schuktomow, R., Scholl, M., & Walch, M. C. (2022). *Report zur Informationssicherheit in KMU – Sicherheitsrelevante Tätigkeitsprofile (Report 1)* (p. 111). Wildau: TH Wildau. Report 1 of the project (2022) (in German), retrieved from https://alarm.wildau.biz/static/3b60581edae4d016e4c20290c0936f55/220623_alarm_report1_web.pdf
- Zerr, K. (2007). Security-Awareness-Monitoring. *DuD Datenschutz und Datensicherheit 31*. Wiesbaden: Springer Gabler.