Jahrestagung
„Informationssicherheitsbeauftragte (ISB)“
26. Oktober 2026, Messe Nürnberg



Eines ist trotz verbesserter Technik sicher: Cyber-Angreifende hacken Mitarbeitende und Führungskräfte – was sollten Verwaltungen, Institutionen und Unternehmen tun?

Prof. Dr. rer. nat. Margit Scholl
Dipl.-Wirt.-Inf. (FH) Peter Ehrlich





margit.scholl@th-wildau.de
http://www.th-wildau.de/scholl

wille@twz-ev.de
http://www.twz-ev.org/

Ausgangslage

- Die Gesamtlage der Cybersicherheit in Deutschland bleibt **angespannt**.
- Cybersicherheit benötigt **nicht nur Technik**…
- Informationssicherheit ist *kein Produkt*, *kein Projekt*, sondern ein **Prozess mit kontinuierlicher Verbesserung** – und ist, entgegen der Praxis, Sache des Managements!



- Sicherheit auf ein Niveau zu heben, das die Resilienz unseres Landes gegenüber Cyberangriffen insgesamt signifikant erhöht, bedeutet auch, die **Awareness der Menschen für mehr Informationssicherheit zu stärken**.

Was ist Security Awareness?



Agentische KI kann Security-Awareness-Schulungen in Echtzeit an Verhalten von Mitarbeitenden und aktuelle Angriffsmuster anpassen.
(Bild: Gemini / Vogel IT-Medien GmbH / KI-generiert)

Was ist Security Awareness?

Bewusste Wahrnehmungen

Achtsamkeit

… durch Sensibilisierung





Agentische KI kann Security-Awareness-Schulungen in Echtzeit an Verhalten von Mitarbeitenden und aktuelle Angriffsmuster anpassen.
(Bild: Gemini / Vogel IT-Medien GmbH / KI-generiert)

… zur Informationssicherheit im eigenen Umfeld
… Angriffsarten & Gefährdungen & Auswirkungen
… Maßnahmen & Regeln & Meldungen
… Verantwortlichkeiten & Austausche

Wie erreichen wir Security Awareness?

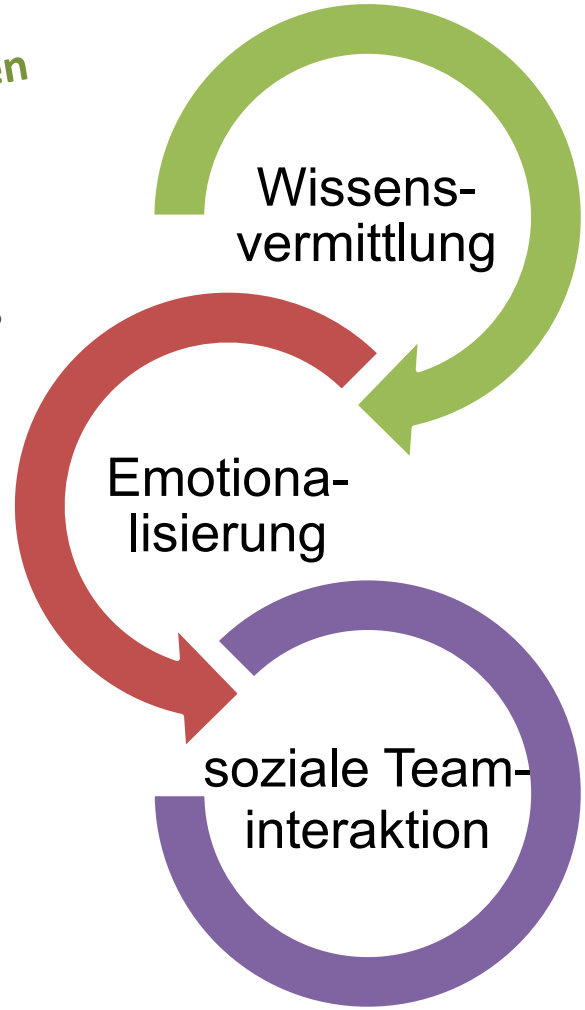
Sensibilisierung ist der erste Schritt…

Bewusste Wahrnehmungen

Achtsamkeit

… durch Sensibilisierung





- Wir müssen uns über die **Ziele** klar werden…
- Wir müssen die spezifischen **Themen** definieren…
- Wir müssen die **Zielgruppen** bestimmen…
- Wir müssen die Ziele mit den Themen und den Zielgruppen für die **konkrete Tätigkeit** in Einklang bringen…
- Wir benötigen zur Schulung und Sensibilisierung passende **Methoden** …
- Wir sollten den **Erfolg** und die **Effektivität** kontrollieren…

Wie erhöhen wir Security Awareness?

Erlebnisorientierte Sensibilisierung ist notwendig …





Wir müssen Sicherheit *interaktiver* behandeln: *Austausch* über *Erfahrungen*, konkrete *Beispiele*, *Simulationen*

BSI, Oktober 2024

Cyber-Awareness-Programm in 8 Schritten

Folgende acht Schritte, entwickelt von der European Union Agency for Cybersecurity – ENISA, helfen Ihnen, ein Cyber-Awareness-Programm zugeschnitten auf Ihr Unternehmen zu entwickeln:

Kontinuierliche Fortbildung
Vermittlung: Gamification, Infotainment & Simulationen
Transparente Kommunikation
Eine positive Fehlerkultur



1 Sensibilisierungsziele ermitteln

2 Finanzielle Mittel sicherstellen

3 Personelle Ressourcen sicherstellen

4 Zielgruppen identifizieren

5 Passende Methoden für Zielgruppe wählen

6 Zeitplan erstellen

7 Mit der Durchführung starten

8 Programm evaluieren und überarbeiten

https://www.wildau.biz/





Gegen Fake News und Datenspionage

SecAware4job

KMU InterKomp 2.0

iBaMs

MOBS

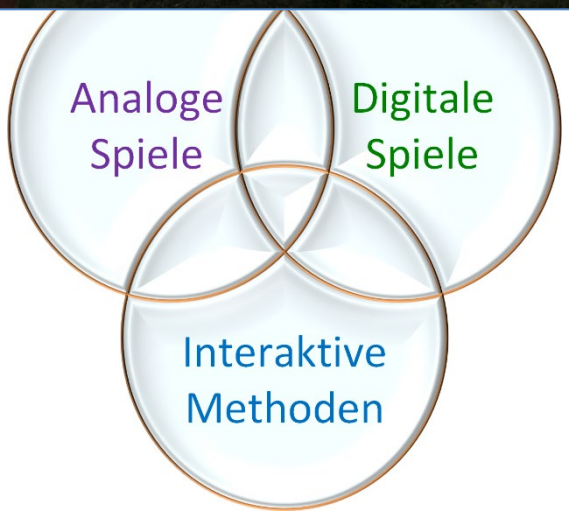


- Social Engineering Theater
- Security Risk Roulette

Security

Willkommen beim Forschungsteam Scholl

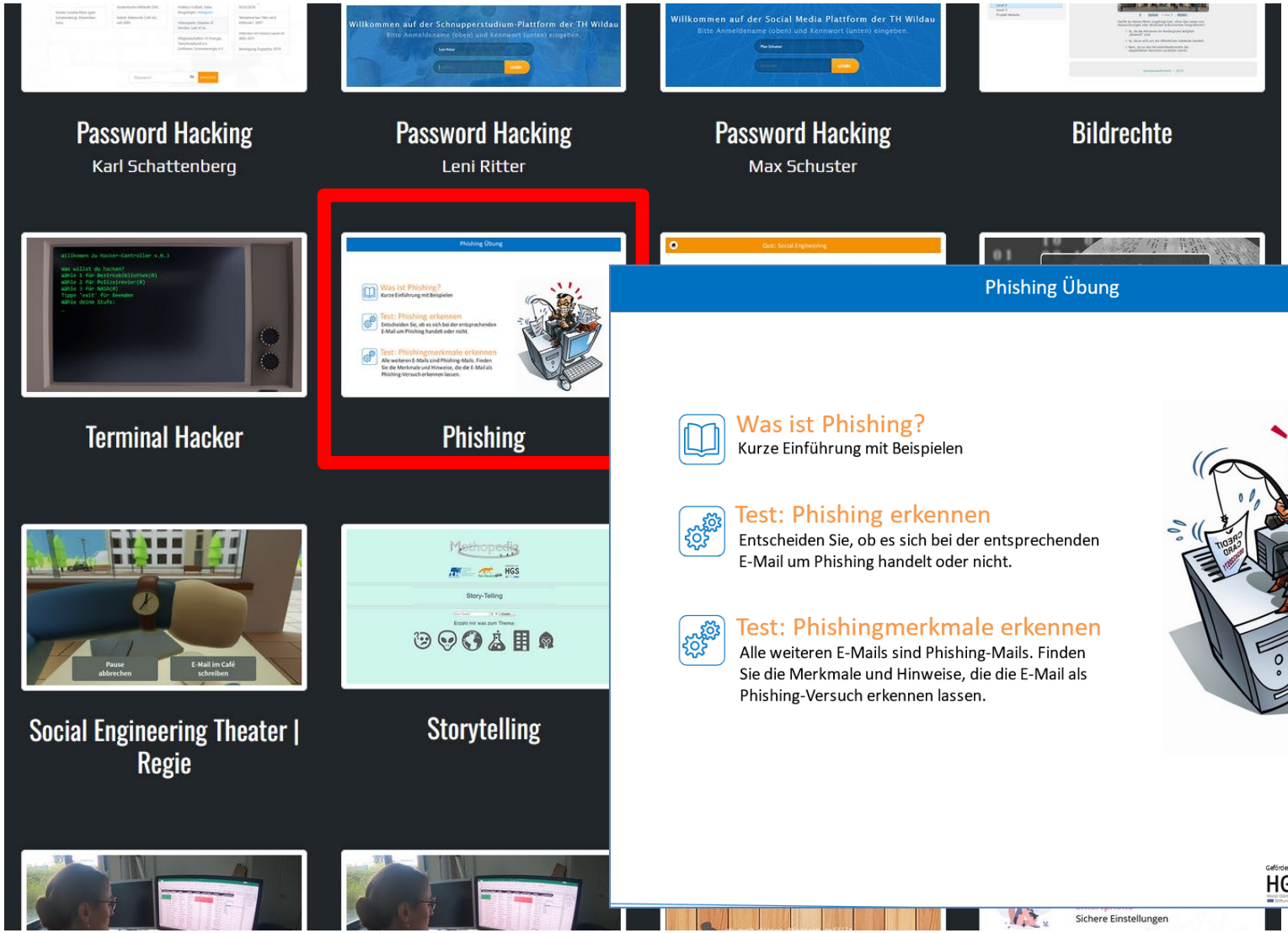
ALLE PROJEKTE AUF EINEN BLICK





ALARM
Awareness Labor KMU Informationssicherheit

https://szenarien.wildau.biz/



Phishing Übung

Was ist Phishing?
Kurze Einführung mit Beispielen

Test: Phishing erkennen
Entscheiden Sie, ob es sich bei der entsprechenden E-Mail um Phishing handelt oder nicht.

Test: Phishingmerkmale erkennen
Alle weiteren E-Mails sind Phishing-Mails. Finden Sie die Merkmale und Hinweise, die die E-Mail als Phishing-Versuch erkennen lassen.



Bildquelle

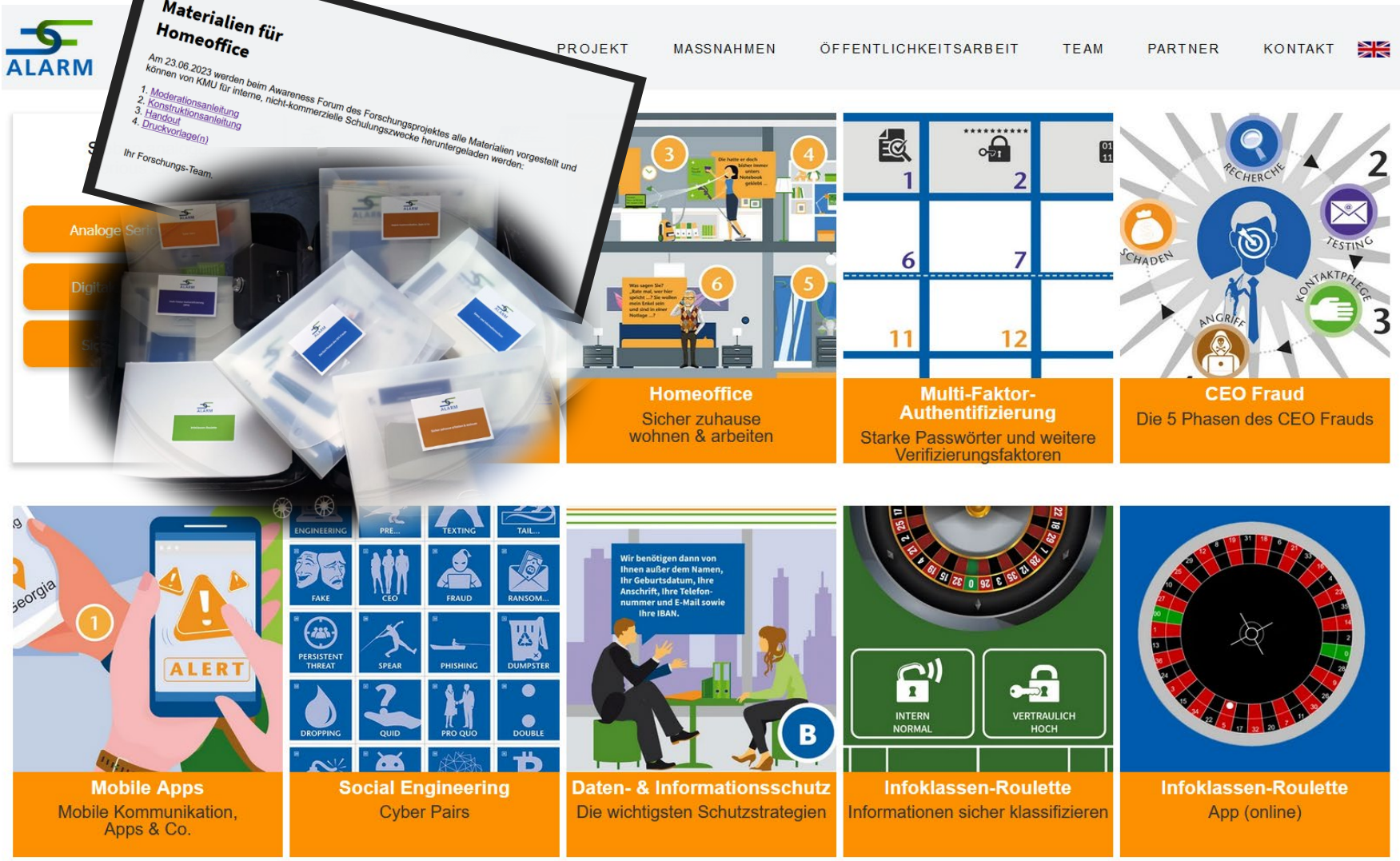
Wie sieht eine erlebnisorientierte Sensibilisierung praktisch aus?

Beispiel: 6 Schadensszenarien nach BSI-Standard 200-2 zur **Schutzbedarfsfeststellung**



- **Beeinträchtigung der persönlichen Unversehrtheit**
- **Negative Innen- oder Außenwirkung**
- **Verstoß gegen Gesetze, Vorschriften oder Verträge**
- **Beeinträchtigung des informationellen Selbstbestimmungsrechts**
- **Beeinträchtigung der Aufgabenerfüllung**
- **Finanzielle Auswirkungen**

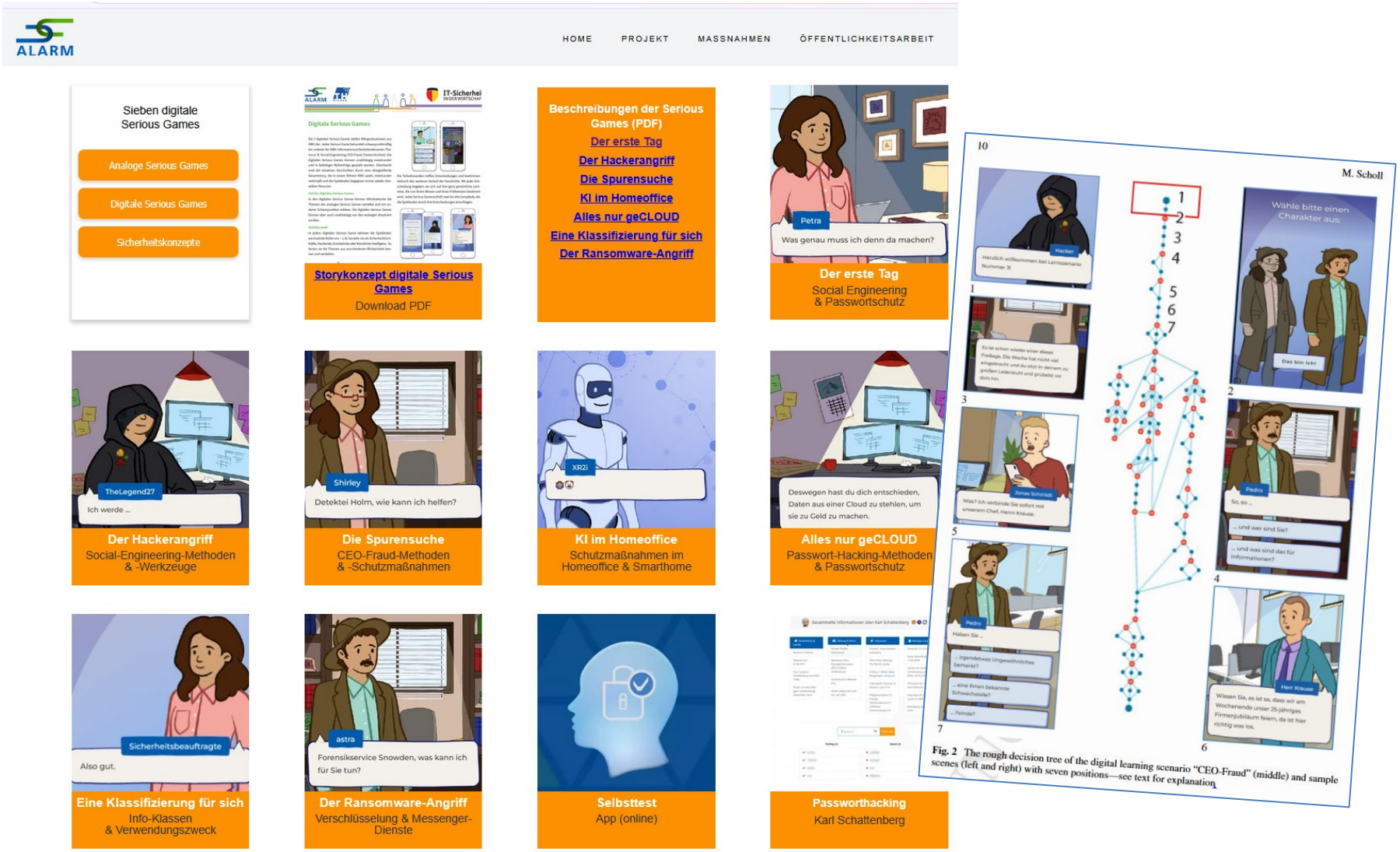
Projekt-Webseite https://alarm.wildau.biz/



Mehrfach in der Praxis erprobt…

Herausforderung	Durchführung	Erfolg
• Ressourcenmangel in Organisationen • Heterogenität der Belegschaft • Geringe Awareness-Reife • Verschwimmende Aufgabenbereiche ⇩ • Breite **Grundlagen** notwendig • Zeitlich, inhaltlich **skalierbare** Sensibilisierung • **15 Minuten bis 1 Stunde**	• **Mitarbeitende** und **Studierende** der TH Wildau • **Pilotunternehmen** des Projektes ALARM • **Verwaltungen** im Rahmen von eigenen Weiter- und Fortbildungsmaßnahmen, wie z. B. Polizei , Landesverwaltungen, Kommunen • **Besucher** bei eigenen Event-Veranstaltungen • **Multiplikatoren** wie z. B. die IHK Brandenburg	• Praxisorientierte Evaluation • Praxisorientierte Verbesserung • Eigene, spezifische Ergänzungen möglich • Merkliche Steigerung des Sicherheitsgefühls ⇩ • **Analoge Serious Games fördern erlebnisorientierte Awareness Trainings**

Projekt-Webseite https://alarm.wildau.biz/



Mehrfach in der Praxis erprobt…

Herausforderung

- Digitale Lernszenarien sind beliebt, in der Annahme, man spare Zeit – sie bleiben jedoch meist unbegleitet
- Nutzende sind auf sich selbst gestellt – einfaches „Durch-klicken“ fördert nicht die Awareness
- Klärung offener Fragen erfolgt nicht aktiv moderiert, sondern in Eigenregie



- Digitales benötigt eine gute **Geschichte**, ansprechendes **Design** und **Vielfalt** in reduzierter Komplexität
- Inhaltlich **kompakt** und **verständlich** sowie **skalierbare** Sensibilisierung
- **Zeitlich reduziert** auf ca. **15 Minuten**

Durchführung

- Die sieben digitalen Lern-szenarien decken inhaltlich ein **breites Spektrum** ab
- Sie sind durch eine **Gesamtstory** miteinander verknüpft
- Je nach Lernszenario ist die **Rolle** der Spielenden **unterschiedlich**
- Jedes Serious Game enthält **mehrere Lernpfade**, je nach eigener Entscheidung führt der Weg zu unterschiedlichen Ergebnissen
- Im Laufe der Durchführung erhalten die Spielenden **Hinweise zu** ihren **Entscheidungen**
- Am Ende erhalten die Teilnehmenden ein **Feedback** zu ihrem Spielerfolg
  und
- Eine **Zusammenfassung** der „Lessons Learned“.

Erfolg

- Die sieben digitalen Lernszenarien basieren auf der anerkannten Methode „Storytelling“
- Sie versetzen die Nutzenden in unterschiedliche Rollen, seien sie Opfer, Angreifende, Sicherheits-beauftragte oder KI
- Die Nutzenden lernen die verschiedenen Facetten der Sicherheit eines kleinen Unternehmens beispielhaft kennen und einschätzen



- Sie sind **gut** in ein betriebliches Trainingskonzept **integrierbar**
- Durch **Vor- und Nachbereitung mit betrieblichen Spezifikationen** können eigene Maßnahmen verdeutlicht werden
- Eigenständiges **vertiefendes Erlebnis** wird gefördert

Projekt-Webseite https://alarm.wildau.biz/

















Mehrfach in der Praxis erprobt…

Herausforderung

- Abgestimmte „Vor-Ort-Angriffe“ simulieren nah am **Social Engineering** eine gängige Angriffssituation
- Die **Geschäftsführung** bzw. Amtsleitung muss über jeden Schritt informiert sein
- **Geschäftsabläufe** dürfen nicht übermäßig gestört werden
- **Mitarbeitende** dürfen nicht bloßgestellt werden
- **Ethische Grundsätze** sind zu beachten

- **Delikate Vorbereitung** notwendig

Durchführung

- **Aufklärung**, **Feingefühl** und **Förderung einer gesunden Fehlerkultur** in der Organisation sind durchgängig beachtet worden
- Im direkten Austausch mit den Verantwortlichen stand ein **rücksichtvoller und maßvoller Umgang** im Vordergrund
- Maßnahmen wurden nur nach **Zustimmung** durchgeführt, wenn alle **Voraussetzungen** erfüllt waren
- Stets wurden **Motivation**, **Zweck**, **Strategie**, **Ziele** und **Ergebnisse** aufeinander **abgestimmt** und **kommuniziert**

Erfolg

- Die Ergebnisse der analogen und digitalen Tests blieben vertraulich
- Sie dienen i.d.R. individuellen Sicherheitskonzeptionen und für akuter Maßnahmen sowie für spezifische IT-Sicherheitsstrategien

- Sieben allgemeine **Informationsblätter** für Nutzende wurden erarbeitet
- Sieben allgemeine **niederschwellige Sicherheitskonzepte** für Geschäftsführungen und IT-Verantwortliche wurden abgeleitet

Polizei Brandenburg: Cyber Security Awareness

LAND BRANDENBURG

Informationssicherheit / Cyber Security Awareness in der Polizei Brandenburg

Maßnahmen zur Schulung und Sensibilisierung der Bediensteten











Unsere Empfehlung für Nachhaltigkeit

Lebendiger Erfahrungsaustausch im Methoden-Mix



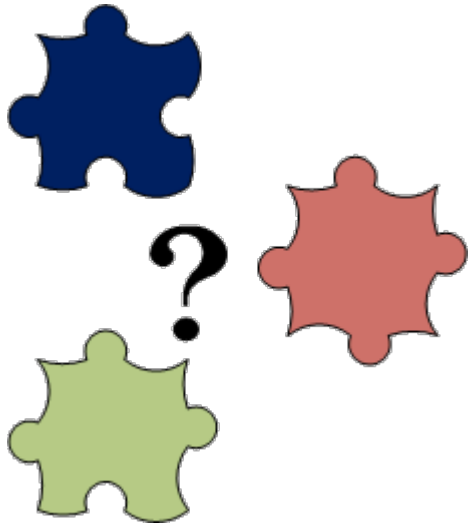
Foto von David McEachan: https://www.pexels.com/de-de/foto/lichterkette-mit-blauer-gluhbirne-91413/

Sprechen wir über Informationssicherheit, um

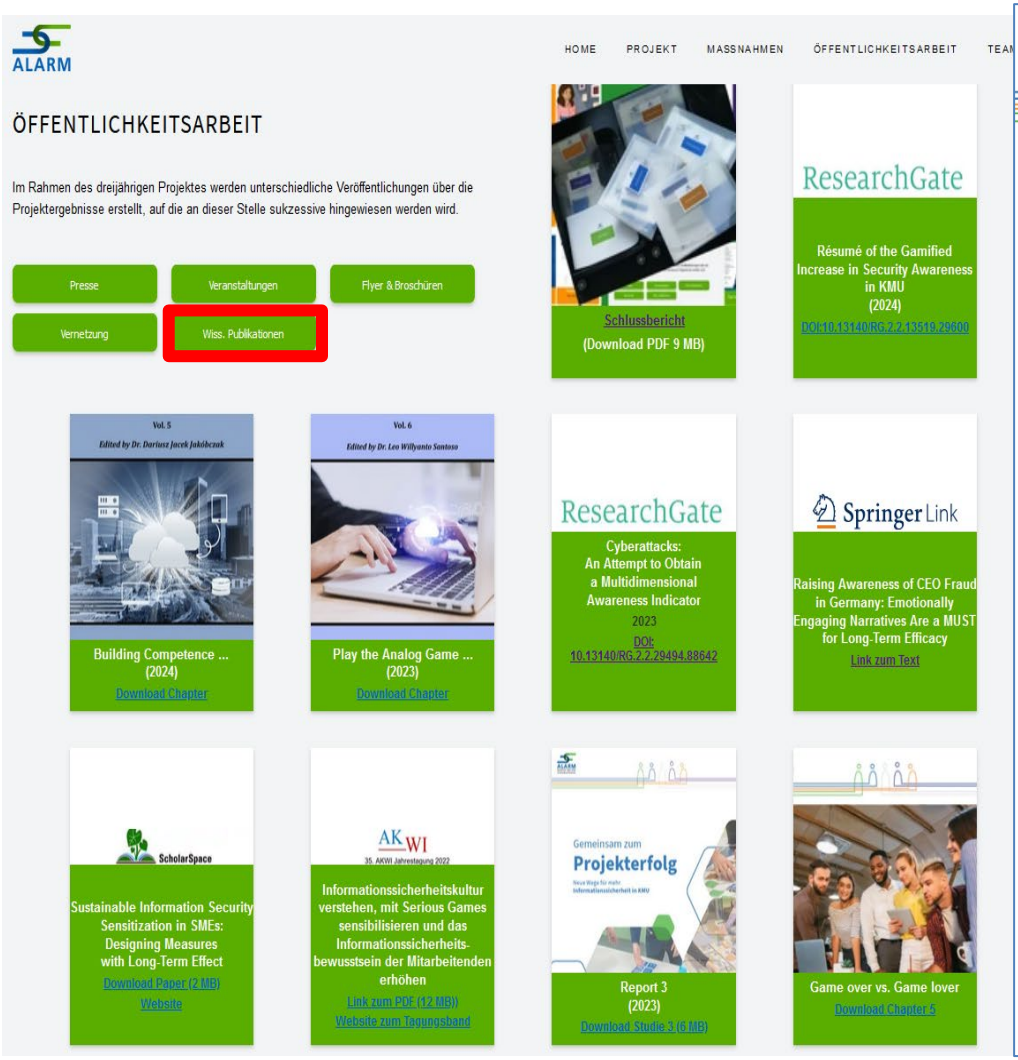
- einerseits den Zusammenhang mit den konkreten und zunehmend digitalen Arbeitsprozessen **(be-)greifbar** machen
- andererseits die Menschen **emotional berühren** und **aktiv einbeziehen**

Austausch / Diskussion

Danke für Ihre Aufmerksamkeit.



Ergänzungen https://alarm.wildau.biz/





Ergänzung: dokumentierte Ergebnisse



Für Informationssicherheitsbeauftragte

