ALARM
Awareness Labor KMU
Informationssicherheit

Technische Hochschule Wildau
Technical University of Applied Sciences

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.

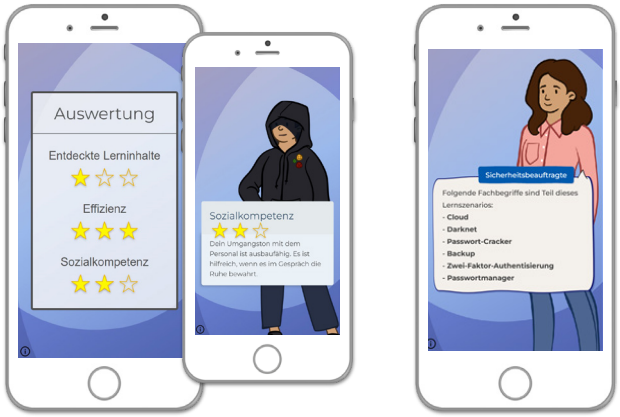

Hacker/in


Sicherheitsexpert/in


Forensiker/in


KI

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.



Am Ende eines Spiels erhalten die Teilnehmenden Feedback zu den erzielten Punkten. Dies beinhaltet Vorschläge und Aufforderungen an die Spielenden sowie eine kurze Zusammenfassung über die im konkreten Spiel gewonnenen Erkenntnisse (lessons learned). Auch bereits im Laufe des Spiels werden Nachrichten eingeblendet, die auf vorteilhafte oder nachteilige Entscheidungen und Verhaltensweisen aufmerksam machen. Zudem bietet ein Lexikonmodul die Möglichkeit, wichtige Begriffe der Informationssicherheit vor und nach dem Spiel nachzulesen.

IT-Sicherheit
IN DER WIRTSCHAFT

Gefördert durch:

Bundesministerium
für Wirtschaft
und Klimaschutz

aufgrund eines Beschlusses
des Deutschen Bundestages

Testen Sie die 7 digitalen Serious Games

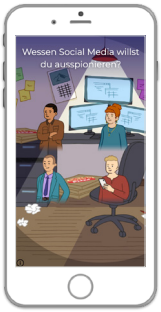
https://alarm.wildau.biz/#learningScenarios

Einsatzmöglichkeiten der einzelnen Serious Games

- Teil eines ganzheitlichen Awareness-Konzepts
- Kombination mit anderen Serious Games dieses Formats als Awareness-Training
- als Einstieg oder Auflockerung einer Schulung zum Thema des Serious Games

Zeitrahmen: 10–25 Minuten
Durchführung: Teilnehmende spielen einzeln, danach erfolgt eine gemeinsame Nachbesprechung/Auswertung und Austausch mit anderen Teilnehmenden online oder in Präsenz

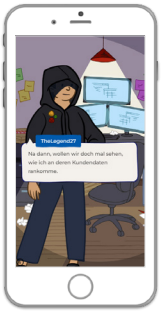
Der erste Tag
Social Engineering & Passwortschutz
Ziel des Spiels ist eine Einführung in das Thema Informationssicherheit anhand klassischer Situationen rund um Social Engineering und Passwortschutz, die eine hohen Identifikation für alle Spielenden bieten. Bewertet werden dabei Sicherheitsverständnis und Sozialkompetenz.



Der Hackerangriff
Social-Engineering-Methoden & -Werkzeuge
Ziel des Spiels ist es, die gängigen von Hackenden benutzten Strategien in einer reellen Situation und aus der Perspektive der Hackenden kennenzulernen und dabei spielerisch zu erleben, wie schon kleinste Sicherheitslücken ausreichen, um Hackenden den Zugriff zu erlauben. Bewertet werden dabei Effizienz und die Variabilität an Angriffswegen, die die Spielenden ausprobieren.

Die Spurensuche
CEO-Fraud-Methoden & -Schutzmaßnahmen
Ziel des Spiels ist, gängige Praktiken von CEO Fraud aufzudecken und wirksame Schutzmaßnahmen zu ergreifen. Eine besondere Rolle spielt bei diesem Thema die Zeit – nur wenn die Spielenden die Attacke rechtzeitig auflösen, können sie größeren Schaden verhindern. Bewertet werden dabei Effizienz, entdeckte Lerninhalte und Sozialkompetenz.

KI im Homeoffice
Schutzmaßnahmen im Homeoffice & Smarthome
Ziel des Spiels ist es, nicht einen großen Aktionserfolg zu erzielen, sondern durch kleinere Aufgaben die beliebtesten Fehler im Homeoffice zu finden. Dabei wird in praktischen und witzigen Beispielen auf die Tücken des Homeoffice aufmerksam gemacht. Bewertet werden dabei Sicherheitsbewusstsein und Machine Learning.



Alles nur geCLOUD
Password-Hacking-Methoden & Passwortschutz
Ziel des Spiels ist es, das Thema Datenspeicherung in der Cloud und Passwortsicherheit aus zwei verschiedenen Perspektiven zu beleuchten: des Angreifenden und des Aufklärenden. Dabei stehen jeweils unterschiedliche Aspekte der Gefährdung im Mittelpunkt und erlauben ein ganzheitliches Erleben des Themas. Bewertet werden dabei Effizienz und Gründlichkeit.

Eine Klassifizierung für sich
Info-Klassen und Verwendungszweck
Ziel des Spiels ist es, ein System zu entwickeln, wie Informationen richtig klassifiziert werden können. Dabei gibt es drei Informationskategorien, denen bestimmte Eigenschaften zugeordnet werden. Bewertet werden dabei die Fähigkeit, Kategorien zu definieren, Informationen einzuordnen, Termine zu verwalten und Fehler zu identifizieren.

Der Ransomware-Angriff
Verschlüsselung und Messenger-Dienste
Ziel des Spiels ist es, die Sicherheitslücke im Messenger zu identifizieren und unter Zeitdruck ein verschlüsseltes Passwort zu entschlüsseln, um die gefährdeten Daten zu sichern. Bewertet werden dabei Codeknacker Kompetenz und Aufmerksamkeit.

Weitere Informationen zum Projekt finden Sie unter https://alarm.wildau.biz