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.

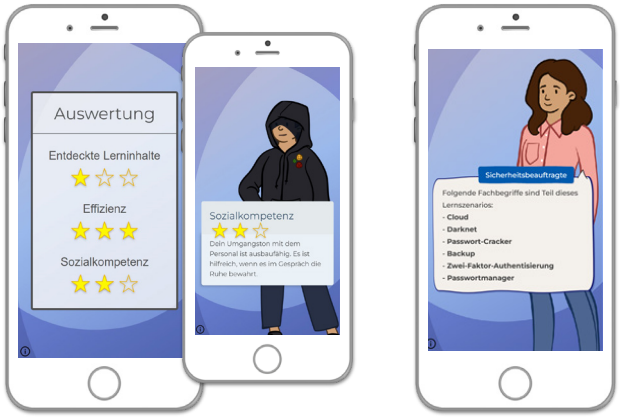

Hacker*in


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.



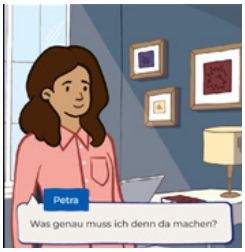
Am Ende eines Spiels erhalten die Teilnehmenden Feedback zu den erzielten Punkten. Dies beinhaltet Vorschläge und Aufforderungen an die Spielenden sowie eine kurze Zusammenfassung über die im konkreten Spiel gewonnenen Erkenntnisse (lessons learned). Auch bereits im Laufe des Spiels werden Nachrichten 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.

Mittelstand-Digital

Gefördert durch:
Bundesministerium für Wirtschaft und Klimaschutz
aufgrund eines Beschlusses des Deutschen Bundestages

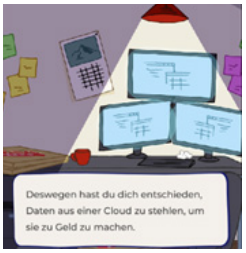
Testen Sie die 7 digitalen Serious Games

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



Der erste Tag

Social Engineering, sicheres Verhalten in Sozialen Netzwerken, Passwortschutz, Clean Desk, sicherer Umgang mit externen Speichermedien (z. B. USB-Sticks)



Alles nur geCLOUD

Passwort-Hacking-Methoden, Passwortschutz (z. B. Zwei-Faktor-Authentisierung) und sichere Cloud-Nutzung

Der Hackerangriff

Social Engineering Methoden und Werkzeuge (z. B. Soziale Netzwerke, USB-Sticks, Spyware, Vor-Ort-Besuche, Telefonanrufe)

Eine Klassifizierung für sich

Informationsklassifizierung und sicherer Umgang mit ausgedruckten und digitalen Informationen sowie Terminen

Die Spurensuche

CEO-Fraud Methoden (z. B. Phishing, Deepfakes, Rechnungsbetrug) und entsprechende Schutzmaßnahmen (z. B. Zahlungsmanagement, Firmenkultur)

Der Ransomware-Angriff

Ransomware, Verschlüsselung, sichere Nutzung von Messenger-Diensten

KI im Homeoffice

Schutzmaßnahmen im Homeoffice und Smarthome (z. B. VPN, Passwörter-Vergabe, sichere Videotelefonie)

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