ALARM
Awareness Labor KMU
Informationssicherheit

Technische Hochschule Wildau
Technical University of Applied Sciences

» Forschung in Wildau – innovativ und praxisnah «

Neue Wege für mehr **Informationssicherheit** in KMU

Reden Sie über das Thema Sicherheit bevor der Notfall eintritt. Unsere 7 analogen Spiele unterstützen Sie dabei.

Manövrieren Sie sich durch 7 digitale Stories, jede eine Herausforderung für Wissen und Handeln.

Jedes Serious Game behandelt schwerpunktmäßig ein anderes Thema der Informationssicherheit, das für KMU relevant ist. (z. B. Social Engineering, CEO-Fraud, Passwort-schutz). Die digitalen Serious Games können unabhängig voneinander und in beliebiger Reihenfolge gespielt werden.

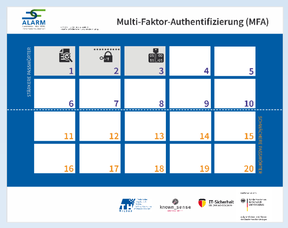
Gleichwohl sind die einzelnen Geschichten durch eine übergreifende Gesamtstory, die in einem fiktiven KMU spielt, miteinander verknüpft.

Einsatzmöglichkeiten der einzelnen Serious Games

- Teil eines ganzheitlichen Awareness-Konzepts
- Kombination mit anderen Serious Games dieses Formats als Awareness-Training (Stationenlernen-Methode)
- Als Einstieg oder Auflockerung einer Schulung zum Thema des Serious Games (z. B. CEO Fraud)
- Zeitrahmen: 15–45 Minuten (je nach gewünschter Intensität)
  Durchführung: 1 moderierende Person & ca. 10 teilnehmende Mitarbeitende

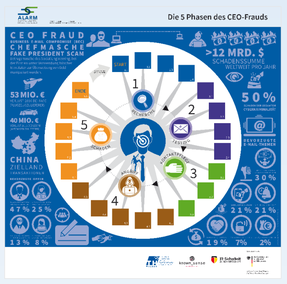
Sicher zuhause wohnen & arbeiten

Dieses Serious Game gibt einen Überblick über die wichtigsten betrieblichen und privaten Informationssicherheits- und Datenschutz-risiken in der eigenen Wohnung bzw. im eigenen Haus sowie über zugehörige Präventionsmaßnahmen, um Risiken zu minimieren.



Multi-Faktor-Authentifizierung (MFA)

Dieses Serious Game vereint Aspekte von Passwortschutz und der Multi-Faktor-Authentifizierung (MFA) und demonstriert, dass der Schutz von Informationen in einem großen Maße von einer sicheren Authentifizierung abhängt. Es zeigt, wie ein „starkes“, weil sicheres, Passwort gebildet wird und dass ein (1!) Faktor zum Schutz sehr sensibler Informationen nicht ausreichend ist.



Die fünf Phasen des CEO Frauds

Hier wird ein Überblick über den Gesamtprozess von CEO Fraud und über Präventionsmaßnahmen gegeben – insbesondere auch für das oft übersehene „Vorspiel“ der Vorbereitungen. Wir gehen von den folgenden fünf Phasen aus: Recherche, Testing, Kontaktpflege, Angriff und Schaden.

Cyber Pairs

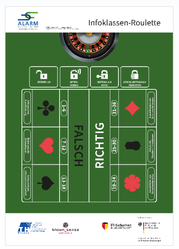
Dieses Serious Game bricht mögliche Barrieren auf und führt zu mehr Sicherheit im Umgang mit Begriffen bzw. Bezeichnungen von gängigen bzw. neuartigen Cybercrime-Angriffen, indem es dabei unterstützt, diese auch im Detail zu verstehen und in Bezug auf mögliche Präventionsmaßnahmen unterscheiden zu können – stets verbunden mit der Fragestellung, was jede/r Einzelne von uns tun kann, um Risiken zu minimieren.

Mobile Kommunikation, Apps & Co.

Dieses Serious Game sensibilisiert in Bezug auf Risiken und Präventionsmaßnahmen, die die potenziellen Gefahren mobiler Kommunikation bzw. bei Nutzung von Apps verringern.

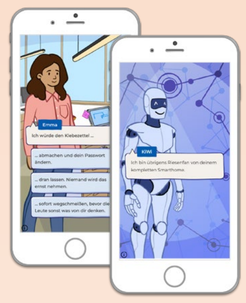
Daten- und Informationsschutz

Der Schutz von Informationen und Daten von Kund/innen, Mitarbeitenden und anderen Parteien ist Teil des Geschäftes jedes Unternehmens. Dieses Serious Game unterstützt dabei, Daten- und Informationsschutz zu gewährleisten, indem der Umgang mit den wichtigsten Schutzstrategien rekapituliert und eingeübt wird.



Infoklassen-Roulette

Der Zweck von Informationsklassifizierung ist der Schutz von wertvollen Informationen jeder Organisation. Die „richtigen“ Klassen hängen von den potenziellen Auswirkungen auf Verfügbarkeit, Beschädigung oder Verlust von Informationen ab. Dieses Serious Game unterstützt beim Verständnis von Informationsklassifizierung und deren Notwendigkeit.



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

7 Praxistipps – Konzepte die sie kennen sollten!

CEO-Fraud: Betrugsmethode über E-Mail als Kommunikationsmittel, bei der sich der Angreifer als Geschäftsführer, Manager oder Chef eines Unternehmens ausgibt.

Passwort Breach Service: Mithilfe der geschäftlichen E-Mailadressen wird geprüft, ob persönliche Identitätsdaten bereits im Internet veröffentlicht wurden und miss-braucht werden könnte.

Live-Hacking: Bildungs- und Informationsveranstaltung zur Entwicklung von persönlichem Risikobewusstsein und zur Sensibilisierung der Durchführung von Sicherheitschecks der IT-Infrastruktur auf organisatinaler Ebene.

Phishing: Beschaffung persönlicher Daten anderer Personen mit gefälschten E-Mails.

Smishing: Unter Smishing versteht man das betrügerische Ausspieonieren von sensiblen Daten per SMS.

Tailgating: Physischer „Einbruch“ in das Unternehmen, um sensible Daten zu stehlen.

Vorfallsmeldung: Simulierter Ransomeware-Angriff mit dem Ziel den Incident Response Prozess in den Unternehmen zu aktivieren.

Sie wissen Bescheid?
Unser Security Self Check könnte Ihnen helfen und/oder Wissenslücken aufdecken.

Sie können Ihr Wissen in allen Kategorien auf die Probe stellen und an den Ergebnissen anderer Anwender messen, die den gleichen Test ebenfalls absolviert haben.

https://sesec.wildau.biz

IT-Sicherheit IN DER WIRTSCHAFT

Gefördert durch:
Bundesministerium für Wirtschaft und Klimaschutz

aufgrund eines Beschlusses des Deutschen Bundestages

Homepage: https://alarm.wildau.biz

Prof. Dr. Margit Scholl (Projektmanagement):
margit.scholl@th-wildau.de