Cyber Krimi Dinner

PwC Cyber Awareness Training

August 2026

Kurzbeschreibung

Das Cyber Krimi Dinner „Diagnose: Erpressung – Spurensuche zwischen Servern und Skalpell" ist ein interaktives Krimi-Dinner-Spiel, das darauf ausgelegt ist, Cyber-Security-Awareness auf eine spannende und einprägsame Weise zu fördern.

Handlung & Szenario

Das Szenario spielt im fiktiven Krankenhaus Lichtenwald, das Opfer eines verheerenden Cyberangriffs geworden ist. Sämtliche Systeme wurden durch Ransomware verschlüsselt und der Betrieb ist zum Stillstand gekommen. Die Spieler:innen schlüpfen in verschiedene Rollen – von der Geschäftsführung, dem Oberarzt bis hin zur IT-Leitung und einer aufmerksamen Patientin – und müssen gemeinsam rekonstruieren, was passiert ist, das Motiv des Angreifers aufdecken und herausfinden, ob ein Insider oder der Angreifer unter ihnen ist. Die Handlung basiert auf realen Cyber-Vorfällen und greift authentische Angriffsmethoden wie Social Engineering, Phishing, Ransomware und KI-gestützte Techniken auf.

Lernziele

Durch das Cyber Krimi Dinner entwickeln Teilnehmende ein umfassendes Verständnis für moderne Cyberbedrohungen, den Einfluss interner Reibungspunkte in Bezug auf IT-Sicherheit und wirksame Schutzmaßnahmen. Es werden die folgenden Aspekte thematisiert:

- Physische Sicherheit: Tailgating
- Prinzip „Least Privilege“
- Gefahren durch öffentlich zugängliche sensible Informationen
- Psychologische Trigger / Social Engineering
- Erkennen von Phishing-E-Mails
- Bedeutung einer guten Fehlerkultur
- Ransomware-Angriffe
- Backups und Wiederherstellungsverfahren
- Wichtigkeit von guter Vorbereitung und Notfallübungen

Die einzelnen Themen können nach dem Spiel in einem Workshop vertieft werden. Über eine inhaltliche Reflexion kann gezieltes Wissen eingebracht und gezielt auf Ankerpunkte aus dem Spiel eingegangen werden.

Materialien

Das Spiel besteht aus den folgenden Materialien (je nach ausgewählter Variante in bereits gedruckter Form oder digital als PDF vorliegend):

- 9 Charakter-Hefte — ein Heft je Teilnehmenden, jeweils mit einer individuellen Rollenbeschreibung, persönlichem Hintergrund, Beziehungen zu anderen Charakteren sowie versiegelten Abschnitten mit Hinweisen, die im Spielverlauf schrittweise aufgedeckt werden.
- Ereignisheft / Moderationsleitfaden — enthält den Prolog, rundenweise Ereignis-Erzählungen, Moderationsanweisungen mit Zeitvorgaben sowie die vollständige Auflösung des Falls.
- Zusatzinformationen-Dokument — mit Hintergrundinformationen und technischen Erklärungen zu Cyber-Security-Konzepten (Social Engineering, Ransomware, Phishing, Deepfakes), Glossar wichtiger Begriffe.
- Ergänzende Materialien — wie E-Mails, System-Log-Auszüge und weitere spielinterne Dokumente, die als Hinweise dienen.
- Namensschilder, Abstimmungszettel.

Security Awareness – Immersives Lernerlebnis mit nachhaltiger Wirkung

Das Spiel bietet Kunden und deren Mitarbeitenden einen immersiven, szenariobasierten Einstieg in reale Cyberbedrohungen wie Social Engineering, Phishing und Ransomware. Indem die Teilnehmenden ein Angriffsszenario aus erster Hand erleben, entwickeln sie ein tieferes Verständnis für Cyberrisiken und Schutzmaßnahmen.

- **Aktives Erleben:** Durch das aktive Erleben eines realistischen Angriffsszenarios lernen Mitarbeitende intuitiv und emotional – das führt zu besserem Risikobewusstsein als eine Standard-Schulung
- **Breite Zielgruppe:** Von Mitarbeitenden bis zur Führungsebene – das Spiel macht Cyber-Bedrohungen für jede Position verständlich und verdeutlicht zudem Herausforderungen auf den verschiedenen Ebenen
- **Authentische Szenarien:** Basierend auf realen Angriffsmethoden (Social Engineering, Phishing, KI-gestützte Attacken) – anstelle theoretischer Beispiele
- **Organisationale Resilience:** Teams entwickeln gemeinsam ein tieferes Verständnis für Cyberrisiken und lernen krisenhafte Situationen besser zu bewältigen und zu vermeiden
- **Compliance & Governance:** Dokumentierbare Awareness-Schulungen, welche die steigenden regulatorischen Anforderungen direkt adressieren, die eine regelmäßige Sensibilisierung der Mitarbeitenden fordern (z.B. NIS-2, ISO 27001 & BSI IT-Grundschutz)

Warum das Cyber Krimi Dinner?

State of the Art Cyber-Security-Awareness: Die Handlung des Spiels basiert auf authentischen, realen Angriffsmethoden – darunter KI-gestützte Angriffe oder Social-Engineering-Techniken – und spiegelt damit die aktuelle Cyberbedrohungslandschaft wider.

Einfache Handhabung und niedrigschwellige Themeneinführung: Das Cyber Krimi Dinner erfordert wenig technisches Vorwissen der Teilnehmenden. Das Spielformat führt komplexe Cyber-Security-Themen auf natürliche Weise durch Storytelling und Rollenspiel ein und macht sie so für jede Zielgruppe zugänglich und ansprechend. Die Durchführung ist unkompliziert dank einsatzbereiter Spielmaterialien und eines klar strukturierten Moderationsleitfadens.

Event-basierte Awareness: Security-Awareness-Simulation werden zumeist mithilfe von Technologie (iPad/Computer) umgesetzt, die Teilnehmenden in Cyberangriffs- und Verteidigungsszenarien eintauchen lassen. Während PwC Produkte wie das „Game of Threats[1]“ oder der „Cyber Escape Room[2]“, technologiegetrieben sind und den Fokus auf Entscheidungsfindung in einer digitalen Oberfläche legen, differenziert sich das Cyber Krimi Dinner hiervon durch sein analoges, soziales und narrativ geprägtes Format – mit dem Schwerpunkt auf persönlicher Interaktion, Teamdiskussion und einem immersiven (Dinner-)Erlebnis. Die beiden Produkte ergänzen sich gegenseitig: Game of Threats bedient den Bereich der digitalen Simulation, während das Cyber Krimi Dinner die Lücke für persönliche, eventbasierte Awareness-Erlebnisse schließt.

Produktvarianten & Pricing

Variante	Beschreibung	Preis
Digitale Materialien (DE/EN)	Ein vollständiges Spielset, wird in digitaler Form versendet. Mehrmalige Nutzung möglich. Sofort einsatzbereit.	2.500 €
Print-Materialien (DE/EN)	Ein vollständiges Spielset, wird in gedruckter Form versendet (inkl. Verpackung). Sofort einsatzbereit. Ab 5+ Sets: Mengenrabatt (10%).	250 € / Set Inkl. Versandkosten

[1] https://www.pwc.de/de/cyber-security/game-of-threats.html
[2] https://www.pwc.de/de/cyber-security/information-security-management/innovatives-trainingstool-der-cyber-escape-room.html

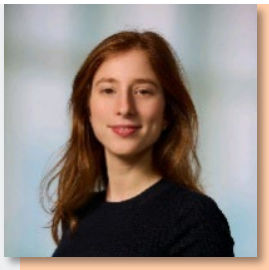
Veranstaltung – Bei PwC	Moderation & Durchführung des Cyber Krimi Dinner im PwC Office/Restaurant, 5-36 Personen pro Event Print-Materialien sind enthalten.	4.000 - 9.500 € / Event
Veranstaltung – Bei Ihnen	Moderation vor Ort, Vorbereitung, Durchführung, Nachbereitung (Spiel + anschließendem Workshop/Reflexion), 5-36 Personen pro Event Print-Materialien sind enthalten.	6.000 – 11.500 € / Event
Virtuelles Event	Moderation in einer Online-Session (z.B. über Teams), Vorbereitung, Durchführung, Nachbereitung, 5-36 Personen pro Event Digitale Materialien sind enthalten.	3.500 – 8.000 € / Event
Individualisierung	Szenario angepasst auf Kundenbranche oder spezifische Themen	Auf Anfrage

Ihre Ansprechpartner

Kommen Sie gerne auf uns zu!

Thomas Klir

+49 (0) 171 2852714
thomas.klir@pwc.com



Lena T. Schramm

+49 (0) 171 6422902
lena.theodora.schramm@pwc.com