Serious Business Gaming im Bereich Unternehmenssicherheit
April 2025

Einleitung

In der heutigen digitalen Welt sind Unternehmen zunehmend mit Cyberbedrohungen konfrontiert. Laut dem Kaspersky Human Factor 360° Report 2023 hatten 77 % aller Unternehmen innerhalb von zwei Jahren mindestens einen größeren Cybervorfall, wobei 40 % dieser Vorfälle durch internes Personal verursacht wurden (Kaspersky 2023).

Das Bundesamt für Sicherheit in der Informationstechnik betont daher, dass der Mensch als eine der größten Schwachstellen in der Informationssicherheit gilt und dass Sicherheitsmaßnahmen nur dann wirksam sind, wenn die Mitarbeiter entsprechend geschult werden (BSI 2024).

Auch wenn dieser Umstand hinreichend bekannt ist, investieren Chief Information Security Officers (CISOs) noch immer einen Großteil ihres Sicherheitsbudgets in Software, aber im Verhältnis dazu nur rund ein Achtel in das Wissen, die Motivation und das Bewusstsein ihrer Mitarbeiter, um ihren individuellen Beitrag zur Cybersicherheit zu leisten. Lediglich 4% des Sicherheitsbudgets investieren CISOs im Durchschnitt für Training und Sensibilisierung (IANS 2024).

Herausforderungen traditioneller Schulungsformate

Traditionelle E-Learnings und Web-based Trainings (WBT) erfüllen zwar formale Anforderungen, sind jedoch oft nicht effektiv, da sie als langweilig empfunden werden, keine echte Kontrolle durch den Arbeitgeber bieten (Mitarbeiter klicken sich durch), statischen Inhalt haben, schnell veralten und kognitive Überlastung verursachen. Diese Formate fördern oft einen passiven Konsum ohne Interaktivität, was die Lernmotivation der Mitarbeiter beeinträchtigt.

Die Lösung: Serious Business Gaming

Serious Business Gaming bietet innovative Ansätze, um Schulungen und Sensibilisierungsmaßnahmen im Bereich Unternehmenssicherheit effektiver und unterhaltsamer zu gestalten. Dabei geht es nicht nur darum, Gamification-Ansätze wie Highscores und Erfolg Badges als “Add-on” auf die üblichen Trainings aufzusetzen, sondern von vornherein eine

eigenständige Spielsituation zu schaffen, in die die Spieler interaktiv eingreifen können und gefordert werden.

Serious Business Gaming ist eine effektive Methode, um Mitarbeiter aktiv in Lernprozesse einzubinden. Die Teilnehmer werden in interaktive Szenarien integriert, die reale Sicherheitsbedrohungen simulieren und ihnen die Anwendung von Wissen in einem sicheren Umfeld ermöglichen. Durch diese spielerische Herangehensweise erhalten die Mitarbeiter ein nachhaltigeres, intensiveres und ansprechenderes Lernerlebnis. Darüber hinaus wird die Zusammenarbeit unter den Teammitgliedern gefördert, was das gemeinsame Verantwortungsbewusstsein für die Schaffung und Aufrechterhaltung eines sicheren Umfelds innerhalb der Organisation stärkt.

Ein Beispiel für ein solches Spiel ist „What the Hack!“ der SBG Serious Business Gaming GmbH, das Mitarbeiter trainiert, um auf unterhaltsame und interaktive Weise mit Sicherheitsbedrohungen umzugehen.

Die Story von “What the Hack!” ist, dass ein Hacker in das Netzwerk der Organisation eingedrungen ist und versucht, möglichst großen Schaden anzurichten. Das Ziel für die Spieler ist es, die Attacken abzuwehren und den Hacker dingfest zu machen.

Das Spiel wird in Runden gespielt, die jeweils aus drei Phasen bestehen:

1. **Mini Quest:** Die Spieler beantworten Fragen und lösen kleine Aufgaben, um Tokens zu erhalten.
2. **Angriff abwehren:** Der Hacker führt einen Angriff durch, den die Spieler mit ihren Tokens abwehren können.
3. **Hacker fangen:** Die Spieler bewegen ihre Figur im Netzwerk, um den Hacker zu fangen, bevor er größeren Schaden anrichten kann oder die Zeit von 30 Min. abläuft.

Der Sicherheitsbereich hat den „Steuerknüppel“ in der Hand, denn Fragen können flexibel an die Bedrohungssituation des Unternehmens angepasst werden. Außerdem werden durch den gezielten Einsatz von Gen-AI fortwährend relevante Datenbanken und Internetseiten analysiert und automatisiert neue Inhalte generiert.

Das Spiel „What the Hack!“ ist bereits in Großunternehmen erfolgreich erprobt worden und bringt alle Eigenschaften mit, um zum etablierten Bestandteil der Sicherheitskultur des Unternehmens zu werden. Das Resultat von „What the Hack!“ geht erfahrungsgemäß über die bloße Verhaltensänderung hinaus. Denn das Spiel beeinflusst in positiver Weise

grundlegend die Überzeugungen, Einstellungen und Wahrnehmungen der Mitarbeiter in Bezug auf (Cyber-)Sicherheit. Dies sind entscheidende Faktoren, um den Reifegrad für Security Awareness nachhaltig auf einem hohen Niveau zu halten (SANS 2025).

Fazit

Die Implementierung spielerischer Methoden zur Wissensvermittlung und Sensibilisierung ist entscheidend, um aktuellen Sicherheitsbedrohungen erfolgreich zu begegnen. Serious Business Gaming, wie beispielsweise das Spiel „What the Hack!“ ist dabei der Erfolgsgarant zur nachhaltigen Verbesserung der Sicherheitskultur in Unternehmen. Durch die aktive Einbindung der Mitarbeiter in Lernprozesse und die Förderung eines gemeinsamen Verantwortungsbewusstseins können Organisationen ihre Resilienz gegenüber Sicherheitsbedrohungen erheblich steigern.

Quellen

Kaspersky (2023): Kaspersky Human Factor 360° Report 2023. Redefining the Human Factor in Cybersecurity. URL: https://media.kasperskydaily.com/wp-content/uploads/sites/92/2023/11/22070742/KasperskyHumanFactor360Report2023.pdf

BSI (2024): Awareness stärken – Risiken minimieren. URL: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Broschueren/Management_Blitzlicht/Management_Blitzlicht_Awareness.pdf?__blob=publicationFile&v=3

IANS (2024): 2024 Security Budget Benchmark Summary Report. URL: https://sf-cdn.iansresearch.com/sitefinity/docs/default-source/reports/ians-2024-security-budget-benchmark-summary-report.pdf?sfvrsn=6ac1b09a_1

SANS (2025): Maturity Model. URL: https://www.sans.org/security-awareness-training/resources/maturity-model/