Serious business gaming in the field of corporate security
April 2025

Introduction

In today's digital world, companies are increasingly confronted with cyber threats. According to the Kaspersky Human Factor 360° Report 2023, 77% of all organizations have had at least one major cyber incident within two years, with 40% of these incidents caused by internal personnel (Kaspersky 2023).

The German Federal Office for Information Security therefore emphasizes that humans are considered one of the greatest vulnerabilities in information security and that security measures are only effective if employees are trained accordingly (BSI 2024).

While this is well known, Chief Information Security Officers (CISOs) still invest a large portion of their security budgets in software, but only about one-eighth of the knowledge and awareness of their employees to make their individual contribution to cybersecurity. On average, CISOs invest only 4% of their security budget in training and awareness (IANS 2024).

Challenges of traditional training formats

Traditional e-learning and web-based training (WBT) meet formal requirements, but are often not effective because they are perceived as boring, offer no real employer control (employees click through), have static content, quickly become obsolete and cause cognitive overload. These formats often encourage passive consumption without interactivity, which affects employees' motivation to learn.

The solution: Serious Business Gaming

Serious business gaming offers innovative approaches to make corporate security training and awareness more effective and fun. It's not just about using gamification approaches such as high scores and success Badges as an "add-on" to the usual trainings, but from the outset a to create an independent game situation in which the players can interactively intervene and are challenged.

Serious business gaming is an effective method of actively involving employees in learning processes. Participants are integrated into interactive scenarios that simulate real-world security threats and allow

them to apply knowledge in a secure environment. This playful approach gives employees a more sustainable, immersive and engaging learning experience. In addition, collaboration among team members is encouraged, which strengthens the shared sense of responsibility for creating and maintaining a safe environment within the organization.

An example of such a game is "What the Hack!" from SBG Serious Business Gaming GmbH, which trains employees to deal with security threats in a fun and interactive way.

The story of "What the Hack!" is that a hacker has penetrated the organization's network and is trying to cause as much damage as possible. The goal for the players is to fend off the attacks and arrest the hacker.

The game is played in rounds, each consisting of three phases :

1. **Mini Quest:** Players answer questions to earn tokens and solve small tasks.
2. **Defend against attack:** The hacker carries out an attack that players can fend off with their tokens.
3. **Catch Hacker:** Players move their character around the network to catch the hacker before he can do more damage or time runs out.

The security area has the "controller" in its hand, because questions can be flexibly adapted to the threat situation of the company. In addition, the targeted use of Gen-AI continuously analyzes relevant databases and websites and automatically generates new content.

The game "What the Hack!" has already been successfully tested in large companies and has all the characteristics to become an established part of the company's security culture. Experience has shown that the result of "What the Hack!" goes beyond a mere change in behavior. This is because the game has a fundamental influence on employees' beliefs, attitudes and perceptions of security in a positive way. These are crucial factors to keep the maturity level for security awareness at a high level in the long term (SANS 2025).

Result

The implementation of knowledge transfer and awareness methods is crucial to successfully counter current security threats. Serious business gaming, such as the playful game "What the Hack!", is the guarantee of success for the sustainable improvement of the security culture in companies. By actively engaging employees in learning and fostering a

shared sense of responsibility, organizations can significantly increase their resilience to security threats.

Sources

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): Strengthening awareness – minimizing risks. 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/