IT-Sicherheitstrainings mit Serious Games

SPIELERISCH GEGEN CYBERBEDROHUNGEN

Klassische Schulungsmethoden vermitteln zwar theoretisches Wissen, stoßen jedoch oft an ihre Grenzen, wenn es darum geht, auf komplexe und dynamische Bedrohungsszenarien zu reagieren. Hier setzen Serious Games an: Sie bieten eine interaktive Möglichkeit, IT-Sicherheit praxisnah zu erlernen, Entscheidungsprozesse unter realistischen Bedingungen zu simulieren und direkt zu erleben.

Serious Games bringen eine Reihe von Vorteilen für Cybersecurity-Awareness mit sich. Die spielerischen Elemente erhöhen die Motivation der Teilnehmer und fördern eine aktivere Auseinandersetzung mit Bedrohungsszenarien, denn Simulationen ermöglichen es, Krisensituationen realitätsnah zu erleben und effektive Reaktionsstrategien zu entwickeln.

Rollenspiele als didaktische Methode basieren auf dem Konzept des erfahrungsbasierten Lernens. Schon in den 1980er-Jahren wurde betont, dass Menschen Wissen durch aktives Handeln und Reflexion erwerben. [1] Besonders in sicherheitskritischen Bereichen sind solche praxisorientierten Lernmethoden von großer Bedeutung. Studien zeigen, dass Simulationen dabei helfen, kognitive Überlastung zu reduzieren und eingeübte Muster in Notfällen schneller abrufen zu können.[2] Während diese Erkenntnisse bereits seit Jahrzehnten bekannt sind, werden sie in der IT-Sicherheitsausbildung bisher nicht konsequent genutzt.

Neben der individuellen Entscheidungsfindung spielt auch die Teamdynamik eine große Rolle. Der Sozialpsychologe Irving Janis beschrieb in seiner „Groupthink"-Theorie[3], wie Gruppendruck und Machtverhältnisse zu suboptimalen Entscheidungen führen können. Gleichzeitig beeinflusst die hierarchische Struktur von Teams sowohl die Effizienz als auch die Nutzung kollektiver Expertise. Während Hierarchien Stabilität und klare Verantwortlichkeiten schaffen, können sie auch zu Konflikten und einer geringeren Berücksichtigung alternativer Perspektiven führen.[4] Studien unterstreichen zudem, dass Serious Games in der Cybersecurity-Ausbildung die Fähigkeit verbessern, mit unklaren Situationen und Zeitdruck umzugehen.[5]

Aktuelle Studien belegen, dass Lernspiele das Cybersecurity-Bewusstsein stärken und die Lösungsfindung unter Druck verbessern. Der Einsatz solcher Spiele erhöht nicht nur das Sicherheitsbewusstsein, sondern sie ermöglichen auch spielerische Lernformate, die klassische Schulungsmaßnahmen ergänzen.[6]

TEAMDYNAMIK UND MACHTVERHÄLTNISSE

In Krisensituationen stehen Teams unter erheblichem Druck. Rollenverteilung, Kommunikation und Entscheidungsprozesse sind oft unklar, was zu Missverständnissen und ineffektiven Maßnahmen führen kann. Forschungen zeigen, dass Teams, die regelmäßig unter simulierten Krisenbedingungen trainieren, in realen Notfällen schneller und koordinierter reagieren.[7] Serious Games bieten hier eine Möglichkeit, Teaminteraktionen in einer sicheren Umgebung zu erproben.

Machtverhältnisse innerhalb eines Teams beeinflussen maßgeblich, wie Entscheidungen getroffen werden. Dominante Persönlichkeiten oder hierarchische Unterschiede können dazu führen, dass kritische Meinungen nicht ausreichend gehört werden. Der Wunsch nach Harmonie kann bewirken, dass Risiken unterschätzt und abweichende Meinungen unterdrückt werden, was in kritischen Situationen fatale Folgen haben kann. In diesem Kontext ermöglicht das Rollenspiel „Data & Disasters", verschiedene Perspektiven erfahrbar zu machen, indem es Teilnehmer in unterschiedliche Rollen versetzt.

DAS ROLLENSPIEL

Das Spiel „Data & Disasters" richtet sich an IT-Sicherheitsteams, Entscheidungsträger in Unternehmen, IT-Administrationen sowie alle, die mit Krisenkommunikation und Notfallmanagement betraut sind. Es bietet eine praxisnahe Methode, um sich in einer geschützten Umgebung mit den Herausforderungen eines Cybervorfalls auseinanderzusetzen. Das Hauptziel besteht darin, die Entscheidungsfähigkeit unter Druck zu verbessern, sowohl die interne als auch externe Kommunikation in einer Krisensituation zu optimieren, teaminterne Kommunikationswege zu stärken und die Dynamik einer eskalierenden Cyberkrise realistisch zu simulieren. Dabei werden nicht nur technische Aspekte der IT-Sicherheit behandelt, sondern auch die oft unterschätzten interpersonellen und strategischen Herausforderungen berücksichtigt.

Es basiert auf bekannten Prinzipien aus Freizeitrollenspielen, wurde jedoch speziell für die Schulung von Cybersicherheit und Krisenmanagement konzipiert. Das Spiel kombiniert szenariobasierte Entscheidungen, Würfelmechaniken

und Charakterinteraktionen mit technischen, kommunikativen und strategischen Herausforderungen. Ziel ist es, die Dynamik einer Cyberkrise realistisch abzubilden und Entscheidungsprozesse unter Druck zu simulieren. Dabei sind die Elemente bewusst weniger komplex als in traditionellen Rollenspielen gestaltet, um alle Spieler unabhängig von ihrem Vorwissen einzubeziehen.

„Data & Disasters" funktioniert also wie eine Tabletop-Übung, benötigt jedoch keine umfangreiche Vorbereitung. Stattdessen wird das Szenario anhand eines Beispielunternehmens durchgespielt, sodass die Teilnehmer direkt in die Übung einsteigen können. Dies erleichtert den Zugang zum Spiel und ermöglicht es, sich schrittweise mit den Herausforderungen eines Cybervorfalls vertraut zu machen. Abbildung 1 zeigt das Logo, das die zwei Seiten einer Krise verdeutlicht: Daten und das drohende Desaster.

Abbildung 1: Data & Disasters (Bild: if(is))

AUFBAU DES ROLLENSPIELS

Jeder Teilnehmer erhält eine Personenkarte, die eine spezifische Rolle innerhalb eines fiktiven Unternehmens beschreibt. Die Rollen decken verschiedene Bereiche ab, darunter IT-Sicherheit, Geschäftsführung, PR und Finanzen und andere eher operative Rollen, wie etwa aus dem Bereich der Produktion. Neben einer öffentlichen Beschreibung der Figur, die allen anderen bekannt gemacht wird, enthält die Karte auch private Informationen wie persönliche Motive, Karriereziele bis hin zu negativen charakterlichen Eigenheiten, die das Gruppengeschehen beeinflussen können. Mithilfe dieser Personenkarten haben die Spieler eine Möglichkeit, sich in ihre Rolle hineinzufinden.

Ein Spannungselement ist die mögliche Existenz eines Innentäters. Per Zufall kann einer der Teilnehmer die geheime Information erhalten, dass er oder sie mit einem fiktiven Hacker kooperiert und versucht, das Krisenmanagement der Gruppe zu sabotieren. Dieses Element erhöht die Komplexität der Entscheidungsprozesse und spiegelt reale Bedrohungen durch Insider wider.

Das Spiel verläuft in Echtzeit, wobei in regelmäßigen Abständen neue Ereigniskarten ins Spiel gebracht werden. Diese Ereignisse reichen von harmlosen Zwischenfällen bis hin zu gravierenden Krisen, auf die die Gruppe gemeinsam reagieren muss. Der Spielstand wird anhand dreier Unternehmenswerte – Produktion, Wirtschaftlichkeit und Reputation – visualisiert. Diese starten bei 100 Prozent und können durch die Entscheidungen der Teilnehmer positiv oder negativ beeinflusst werden. Sinkt einer dieser Werte auf 0 Prozent, gilt das als Totalschaden in diesem Bereich.

EIGENSCHAFTEN UND ENTSCHEIDUNGSMECHANIKEN

Jede Rolle besitzt vier Kernwerte: Kommunikation, Fachwissen, Aufmerksamkeit und Geduld. Diese Werte bestimmen, wie erfolgreich bestimmte Aktionen im Spiel ausgeführt werden können. Würfelmechaniken kommen ins Spiel, wenn es um riskante oder unsichere Entscheidungen geht. Der Zufallseffekt sorgt für zusätzliche Unvorhersehbarkeit, ähnlich wie in einer echten Krisensituation.

Dabei sind die Entscheidungen nicht immer rein technischer Natur – oft spielen zudem soziale Dynamiken, Überzeugungskraft oder Teamabsprachen eine Rolle. Dies trägt dazu bei, dass nicht nur technische Expertise, sondern auch strategisches Denken und Verhandlungsgeschick gefragt sind.

ESKALATION UND ENTSCHEIDUNGSFINDUNG

Das Szenario beginnt mit einem initialen Cyberangriff, beispielsweise durch eine Ransomware-Infektion. Zunächst scheinen die Vorfälle harmlos, eskalieren aber im Laufe des Spiels durch aufeinander aufbauende Ereigniskarten. Beispielsweise kann ein unbedachtes Posting eines Mitarbeiters auf Social Media die Reputation des Unternehmens schädigen, was wiederum eine Krisenkommunikation erforderlich macht. Die Gruppe muss Entscheidungen treffen, deren Konsequenzen in den Unternehmenswerten sichtbar werden.

Spannungen innerhalb der Gruppe sind notwendig, um die Realität einer Krisensituation widerzuspiegeln. Machtgefälle, Konflikte und verschiedene Interessen der Rollen sollen dafür sorgen, dass die Teilnehmer nicht nur technische, sondern auch kommunikative Herausforderungen meistern müssen. Da nicht immer alle relevanten Charaktere in jeder Runde vertreten sind, kann es passieren, dass beispielsweise die Sicherheitsverantwortlichen nicht verfügbar sind und eine andere Rolle die Krise bewältigen muss. Wie es in der Realität auch vorkommen kann.

PERSONENKARTEN – STRUKTUR UND INHALTE

Ein zentrales Element des Spiels sind die Personenkarten, die den Teilnehmern helfen, sich in ihre Rollen einzufinden. Die in Abbildung 2 dargestellte Karte zeigt die wesentlichen Elemente dieser Rollenbeschreibungen. Jede Karte enthält den Namen der Rolle sowie die zugehörige Abteilung (1), die durch ein Symbol gekennzeichnet ist, um eine leichtere Zuordnung im Spiel zu ermöglichen. Zudem gibt es öffentliche Informationen (2), die beschreiben, wie die Person von anderen wahrgenommen wird. Diese können zu Beginn des Spiels vorgelesen werden, um den anderen Teilnehmern einen ersten Eindruck zu vermitteln.

Die geheimen Informationen (3), die nur den jeweiligen Spielern bekannt sind, finden sich direkt darunter. Ergänzend dazu besitzt jede Person spezifische Eigenschaften und Werte (4) in den Kategorien Kommunikation, Fachwissen, Aufmerksamkeit und Geduld. Diese beeinflussen, wie erfolgreich bestimmte Aktionen im Spiel ausgeführt werden können.

Ein weiterer wichtiger Bestandteil der Personenkarten sind die Spannungen zwischen den Charakteren (5). Jede Person hat eine spezifische Spannung zu einer anderen Figur im Spiel, die sich auf das Verhalten und die Entscheidungsfindung auswirken kann. Diese Spannungen spiegeln realistische Herausforderungen in Krisensituationen wider und fordern die Teilnehmer heraus, auch interpersonelle Konflikte zu berücksichtigen.

MODERATION, BRIEFING UND DEBRIEFING

Das Rollenspiel sollte idealerweise in einem Unternehmen oder einer Organisation durchgeführt werden, die von Cyberrisiken betroffen ist. Es eignet sich für IT-Sicherheitsabteilungen, Krisenteams und alle relevanten Entscheidungsträger. Die Umgebung sollte so gestaltet sein, dass eine konzentrierte und realitätsnahe Simulation möglich ist, etwa in einem Besprechungsraum oder einem speziell eingerichteten Schulungsbereich.

Das Spiel dauert inklusive Briefing, Simulation und Debriefing in der Regel drei bis vier Stunden, abhängig von der Gruppengröße. Kleinere Gruppen erlauben eine intensivere Betrachtung einzelner Aspekte und eine detaillierte Analyse, während größere Gruppen durch die Dynamik und das entstehende Chaos schneller zu Entscheidungen kommen. Bei besonders großen Gruppen, wie unserer bisherigen Rekordgröße von etwa 25 Teilnehmern, nimmt nach etwa zweieinhalb Stunden die Konzentration spürbar ab, ein guter Zeitpunkt, um das Debriefing einzuleiten.

Denn ein essenzieller Bestandteil des Spiels ist die Rolle des Moderators. Er stellt sicher, dass das Szenario realistisch, aber steuerbar bleibt, und sorgt für eine strukturierte Durchführung. Der Moderator überwacht den Spielverlauf, führt neue Ereignisse ein und stellt sicher, dass die Teilnehmer sich an die vorgegebenen Regeln halten. Besonders wichtig ist dabei das Briefing. Zu Beginn der Simulation erhalten die Spieler eine Einführung in das Szenario, ihre Rollen und die grundlegenden Mechaniken des Spiels. Hier werden auch Fragen geklärt, damit alle auf demselben Wissensstand sind und sich besser in ihre Charaktere hineinversetzen können.

Am Ende des Spiels erfolgt das Debriefing, eine strukturierte Nachbesprechung, in der die getroffenen Entscheidungen reflektiert und analysiert werden. Die Teilnehmer diskutieren alternative Handlungsoptionen, erörtern Herausforderungen und ziehen Schlüsse für reale Krisensituationen. Der Moderator spielt dabei eine Schlüsselrolle, indem er gezielte Fragen stellt, die Reflexion anregt und darauf achtet, dass konstruktives Feedback gegeben wird. Gerade der Transfer in den realen Arbeitsalltag ist ein zentraler Punkt – welche Erkenntnisse lassen sich auf echte IT-Notfälle übertragen? Welche Prozesse könnten im Unternehmen verbessert werden?

FOKUS- UND GRUPPEN-ROLLENSPIEL

Wir unterscheiden zwei Varianten des Rollenspiels: das Fokus-Rollenspiel für kleinere Gruppen mit maximal zehn Teilnehmern und eine vereinfachte Version für größere Gruppen. Im Fokus-Rollenspiel kommen alle vorgestellten Mechaniken zum Einsatz, darunter detaillierte Personenkarten, Würfelmechaniken und tiefgehende Charakterinteraktionen. Diese Variante erlaubt eine besonders immersive Simulation mit vielen individuellen Entscheidungen.
Für größere Gruppen, die ebenfalls sinnvoll sind, gibt es eine vereinfachte Variante mit weniger Detailtiefe. Hier sind die Personalkarten weniger umfangreich, enthalten aber weiterhin private

Abbildung 2: Personakarte von Anna Müller als Beispiel. (Bild: if(is))

und öffentliche Informationen. Auf Würfelmechaniken wird verzichtet, da das entstehende Chaos bereits ausreichend Dynamik schafft. Die drei Unternehmenswerte bleiben jedoch erhalten, sodass auch hier deren Veränderung durch Entscheidungen sichtbar wird. Während im Fokus-Rollenspiel einzelne Charaktere agieren, müssen sich die Teilnehmer in der größeren Version eher als Teil fiktiver Abteilungen organisieren. Trotz der Anpassungen bleibt der Lerneffekt hoch – die Gruppen müssen unter Druck zusammenarbeiten, um den Schaden für das Unternehmen zu begrenzen.

WISSENSCHAFTLICHER HINTERGRUND UND WEITERENTWICKLUNG

Das Rollenspiel basiert auf konstruktivistischen Lernansätzen, nach denen Wissen durch aktives Handeln und Reflexion aufgebaut wird. Besonders in sicherheitskritischen Bereichen sind erfahrungsbasierte Lernmethoden von hoher Bedeutung, da sie nicht nur Faktenwissen vermitteln, sondern auch unter Stress abrufbare Entscheidungsprozesse trainieren. Psychologische Untersuchungen zeigen, dass Simulationen helfen, die kognitive Belastung zu reduzieren und erlernte Muster für Notfälle abrufbar zu machen. Zudem verbessert die Kombination aus technischen, analytischen und kommunikativen Elementen die interdisziplinäre Zusammenarbeit innerhalb von Incident-Response-Teams.

Das Spiel wird nun wissenschaftlich durch das Institut für Internet-Sicherheit an der Westfälischen Hochschule Gelsenkirchen sowie durch das „Voice of Wisdom"-Projekt begleitet. Voice of Wisdom ist ein Forschungsprojekt, das vom Zentrum für Digitalisierungs- und Technologieforschung der Bundeswehr (dtec.bw) sowie dem Lehrstuhl für Human-Centred Security an der Ruhr-Universität Bochum mitgetragen wird. Während sich Voice of Wisdom vorrangig mit neuen Ansätzen zur Erkennung menschenzentrierter Cyberangriffe und der Analyse physiologischer Reaktionen in sicherheitskritischen Situationen befasst, bietet das Rollenspiel eine Gelegenheit, Social-Engineering-Aspekte und Gruppenverhalten in Krisensituationen zu untersuchen. Hierbei liegt der Fokus besonders auf der Frage, welche manipulativen Techniken in simulierten Krisen funktionieren und wie sich Gruppenmechanismen auf Entscheidungsprozesse auswirken. Die Kooperation mit der AWARE7 GmbH ermöglicht zudem eine praxisnahe Weiterentwicklung des Spiels.

Das Rollenspiel war bereits bei einigen zufriedenen Unternehmen im Einsatz. Nun soll die wissenschaftliche Begleitung dazu beitragen, die bisherigen positiven Ergebnisse zu bestätigen und weiter zu optimieren.

Ein weiteres Untersuchungsfeld betrifft den Einfluss von Storytelling. Bevorzugen Teilnehmer eine freie, dynamische Entwicklung der Geschichte oder sind vorgefertigte Szenarien mit mehr Struktur effektiver? Auch die Messbarkeit des Lernerfolgs steht zur Debatte – etwa die Frage, ob durch das Rollenspiel tatsächlich die Entscheidungsqualität in realen Krisensituationen verbessert wird. Zudem soll untersucht werden, ob heterogene Gruppen mit unterschiedlichem Fachwissen besser abschneiden als homogene Teams. Ein besonderer Fokus liegt auf der Rolle des Innentäters: Steigert er den Realismus oder führt er zu einer übermäßigen Störung der Simulation?

FAZIT

Serious Games haben das Potenzial, klassische IT-Sicherheitsschulungen nicht nur zu ergänzen, sondern auch weiterzuentwickeln. Durch den interaktiven und praxisnahen Ansatz lernen Teilnehmer, mit komplexen Cyberbedrohungen umzugehen und ihre Entscheidungsfähigkeit unter Druck zu verbessern. Das hier vorgestellte Cybersecurity-Rollenspiel verbindet spielerische Elemente mit realitätsnahen Krisenszenarien und bietet eine gute Methode, um IT-Sicherheit und Teamarbeit gleichzeitig zu trainieren. ■

DAVID BOTHE
Wissenschaftlicher Mitarbeiter mit dem Forschungsschwerpunkt Cybersecurity Awareness im Institut für Internet-Sicherheit – if(is) an der Westfälischen Hochschule in Gelsenkirchen sowie IT-Sicherheitsberater bei der AWARE7 GmbH

JAN HÖRNEMANN
ist Doktorand im Institut für Internet-Sicherheit - if(is) an der Westfälischen Hochschule in Gelsenkirchen sowie COO & Prokurist bei der AWARE7 GmbH

NORBERT POHLMANN
ist Professor für Cybersicherheit und Leiter des Instituts für Internet-Sicherheit – if(is) an der Westfälischen Hochschule in Gelsenkirchen sowie Vorstandsvorsitzender des Bundesverbands IT-Sicherheit – TeleTrusT und im Vorstand des Internetverbandes – eco.

Quellen

[1] *Kolb, D. A. (1984). Experiential Learning: Experience as the Source of Learning and Development. Englewood Cliffs, NJ: Prentice Hall http://academic.regis.edu/ed205/Kolb.pdf*

[2] *Endsley, M. R. (1995). Toward a theory of situation awareness in dynamic systems. Human Factors: The Journal of the Human Factors and Ergonomics Society, 37(1), 32–64. https://doi.org/10.1518/001872095779049543*

[3] *Janis, I. L. (1982). Groupthink: Psychological Studies of Policy Decisions and Fiascos. Boston: Houghton Mifflin.*

[4] *Bunderson, Stuart & Reagans, Ray. (2011). Power, Status, and Learning in Organizations. Organization Science. 22. 1182-1194. 10.1287/orsc.1100.0590.*

[5] *Salas, E., Tannenbaum, S. I., Kraiger, K., & Smith-Jentsch, K. A. (2012). The science of training and development in organizations: What matters in practice. Psychological Science in the Public Interest, 13(2), 74–101. https://doi.org/10.1177/1529100612436661*

[6] *Moumouh, C., Chkouri, M.Y., Fernández-Alemán, J.L. (2023). Cybersecurity Awareness Through Serious Games: A Systematic Literature Review. In: Ben Ahmed, M., Abdelhakim, B.A., Ane, B.K., Rosiyadi, D. (eds) Emerging Trends in Intelligent Systems & Network Security. NISS 2022. Lecture Notes on Data Engineering and Communications Technologies, vol 147. Springer, Cham. https://doi.org/10.1007/978-3-031-15191-0_18*

[7] *Schulte-Seitz, Eva & Kauffeld, Simone. (2017). Krisen in Teams: Teamresilienz als Präventions- und Bewältigungsstrategie. 10.1007/978-3-662-54632-1_11.*