Serious Games für wirksame Awareness im ISMS

David Bothe[1], Marcus Schaper[2], Prof. Dr. (TU NN) Norbert Pohlmann[3]

Abstract:
Serious Games schließen die Lücke zwischen Wissen und Verhalten, indem sie sicherheitsrelevante Entscheidungen erlebbar machen.Der Beitrag zeigt, wie sie entlang des A.C.T.I.O.N.-Modells wirksam gestaltet und systematisch in Awareness-Kampagnen integriert werden können. Ziel ist es, Awareness von punktuellen Maßnahmen zu nachhaltiger Sicherheitskultur zu entwickeln.

1 Einleitung

Deutschland investiert zunehmend in IT Sicherheit: Ausgaben steigen bis 2026 auf geschätzt rund 12,2 Milliarden Euro, bei gleichzeitig jährlichen Schäden von etwa 202,4 Milliarden Euro durch Cyberangriffe [1]. Parallel erhöhen regulatorische Vorgaben wie NIS2 und der Cyber Resilience Act den Druck, IT- und Informationssicherheit nicht nur formal umzusetzen, sondern tatsächlich zu leben. Die Bedrohungslage verschärft sich zusätzlich durch generative und agentische KI, die Angriffsflächen erweitert und neue Risiken beschleunigt, etwa durch täuschend echte Pretexting-Angriffe via E-Mail, Profilen oder Stimmen.

Gleichzeitig verändern Social Media, Informationsüberflutung und Echokammern die Informationsumgebung und fördern Desinformation. Im Zentrum steht der Mensch: Trotz Awareness-Maßnahmen bleibt die Wirkung oft begrenzt, da Wissen im Alltag nicht konsequent angewendet wird. Informationssicherheit entsteht daher nur im Zusammenspiel von Technologie, Organisation und Verhalten.

1.1 Zielsetzung

Ziel dieses Beitrags ist es zu zeigen, wie Serious Games als Bestandteil von Awareness-Kampagnen in ein ISMS integriert werden können, um Wissen gezielt in handlungsrelevante Kompetenz zu überführen. Hierzu wird mit dem A.C.T.I.O.N.-Modell ein Gestaltungsrahmen für wirksame Cybersecurity Awareness vorgestellt und der Einsatz von Serious Games als praxisnahes Instrument im Kontext des IT-Grundschutzes eingeordnet.

[1] Cyberbüro Bothe, Gelsenkirchen
[2] SBG Serious Business Gaming GmbH, Düsseldorf
[3] Institut für Internet-Sicherheit - if(is), Westfälische Hochschule Gelsenkirchen

1.2 Fragestellung

Dieser Beitrag untersucht, wie Serious Games sinnvoll in Awareness-Kampagnen integriert werden, welche Gestaltungsprinzipien nachhaltige Verhaltensänderung unterstützen und an welchen Stellen sich konkrete Andockpunkte zu ISMS- und IT-Grundschutzprozessen ergeben.

2 Lernen, Verhalten und Resilienz

Der aktuelle Stand der Wissenschaft zeigt, dass nachhaltiges Lernen und Verhaltensänderung nicht durch reine Informationsvermittlung entstehen. Erkenntnisse aus Neurowissenschaft, Psychologie und Pädagogik erklären, wie Menschen Informationen verarbeiten, Entscheidungen treffen und Verhalten anpassen. Wirtschaftswissenschaftliche Perspektiven ordnen den Nutzen auf organisationaler und gesamtwirtschaftlicher Ebene ein.

2.1 Neurowissenschaftliche Erkenntnisse

Lernen findet im Gehirn durch den Aufbau und die Festigung neuronaler Verbindungen statt [2]. Dabei werden synaptische Verbindungen durch wiederholte Aktivierung verstärkt und stabilisiert, während ungenutzte Verbindungen abgeschwächt werden. Das limbische System bewertet eingehende Informationen kontinuierlich hinsichtlich ihrer Relevanz und beeinflusst damit, ob Inhalte weiterverarbeitet und gespeichert werden. Aufmerksamkeit, Motivation und Gedächtnisbildung werden maßgeblich durch das Belohnungssystem gesteuert. Insbesondere positive Abweichungen zwischen Erwartung und Ergebnis, beschrieben als Reward Prediction Error [3], führen zur Ausschüttung von Dopamin und begünstigen somit die Verarbeitung und Konsolidierung von Lerninhalten [4]. Dieser „Fehler“ dient als Lernsignal, das Anpassungen im Gehirn auslöst. Das Gehirn ist jedoch nicht auf dauerhafte Maximalleistung ausgelegt, sondern auf adaptive Stabilität unter wechselnden Bedingungen [5]. Es investiert zusätzliche kognitive Ressourcen vor allem dann, wenn Reize oder Aufgaben als relevant, bedeutsam oder lohnend erscheinen.

2.2 Psychologische Erkenntnisse

Lernen ist ein individueller und motivational regulierter Prozess. Die Aufnahme von Inhalten hängt maßgeblich von erfüllten Grundbedürfnissen ab: Autonomie, Kompetenz und soziale Eingebundenheit [6]. Werden diese erfüllt, entsteht intrinsische Motivation sowie Selbstwirksamkeit, also die Überzeugung, durch eigenes Handeln wirksam Einfluss nehmen zu können [7]. Dieses Erleben ist zentral für nachhaltige Verhaltensänderungen. Fehlt es, bleibt Motivation oft auf deklaratives Wissen beschränkt.

Der Intention Behavior Gap beschreibt dabei die Diskrepanz zwischen Wissen und tatsächlichem Verhalten [8]. Menschen wissen was zu tun ist, handeln jedoch nicht. Lernen ist sozial eingebettet und Verhalten wird in gemeinsamen Kontexten durch Beobachtung anderer übernommen [9].

Glaubwürdige und nahbare Vorbilder sind dabei wirksamer als abstrakte Anweisungen. Gruppendynamische Effekte wie soziale Resonanz, Konformität und "Fear of Missing Out" verstärken die Bereitschaft zur Verhaltensanpassung [10]. Die Vergessenskurve nach Ebbinghaus in Abbildung 1 zeigt, wie schnell Wissen ohne Aktivierung verloren geht [11]. Erst durch wiederholtes Abrufen und praktisches Anwenden werden Inhalte stabil verankert. Auch imaginierte Erfahrungen, etwa in simulierten oder nachempfundenen Szenarien beschrieben, lösen Lernprozesse aus. Abweichungen zwischen Erwartung und Ergebnis führen dabei durch den in Abschnitt 2.1 beschriebenen Effekt zu Bewertungsprozessen [12].

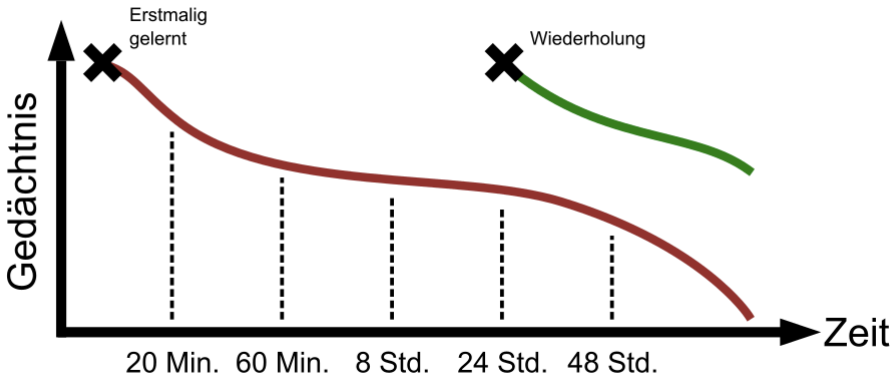

Abbildung 1: Vergessenskurve nach Ebbinghaus

2.3 Pädagogische Erkenntnisse

Positive Rückmeldungen stärken das Kompetenzerleben und fördern die Motivation. Wahrgenommene Fortschritte werden sichtbar und Handlungen werden als wirksam bestätigt. Reflexion fungiert dabei als zentraler Mechanismus, um Abweichungen zwischen Ziel und Ergebnis zu erkennen, Denkfehler aufzudecken und Verhalten gezielt anzupassen [13, 14]. Erst durch wiederholte Anwendung in realitätsnahen Kontexten sowie durch gezielte Rückmeldung wird Wissen in handlungsleitende Routinen überführt [15]. Lernen entwickelt sich dabei iterativ über Ausprobieren, Scheitern, Korrigieren und erneutes Versuchen. Aktive Lernprozesse erhöhen nachweislich die Leistung und fördern ein tieferes Verständnis der Inhalte[16].

2.4 Wirtschaftswissenschaftliche Erkenntnisse

Cybersecurity Awareness ist ein zentrales Element nationaler und organisationaler Sicherheitsstrategien. Investitionen in Wissen und Sicherheitsbewusstsein stärken die organisationale Resilienz und tragen zur Stabilität wirtschaftlicher Systeme bei [17]. Informationssicherheit wird damit vom technischen Thema zum Bestandteil unternehmerischer Wertschöpfung. Aus betriebswirtschaftlicher Sicht ist die Schulung von Mitarbeitenden eine Investition: Sie reduziert Risiken, minimiert Fehlverhalten und senkt die Wahrscheinlichkeit von Vorfällen. Präventive Maßnahmen sind dabei deutlich kosteneffizienter als die Bewältigung eingetretener Schäden, wie jährliche Berichte zeigen [18]. Auf volkswirtschaftlicher Ebene trägt Awareness zur Resilienz von Wertschöpfungsketten bei, indem sie die Häufigkeit und Auswirkungen von Sicherheitsvorfällen reduziert [19]. Dies senkt indirekte Kosten wie Produktionsausfälle, Betriebsunterbrechungen oder Reputationsverluste und stabilisiert damit gesamtwirtschaftliche Strukturen. Ein wesentlicher Erfolgsfaktor liegt dabei in der Skalierbarkeit moderner Lernformate. Digitale Awareness-Maßnahmen ermöglichen es, große Zielgruppen effizient zu erreichen, Inhalte kontinuierlich zu aktualisieren und flexibel an neue Bedrohungslagen anzupassen [20].

3 Awareness gestalten und Serious Games im ISMS verankern

Awareness entfaltet ihre Wirkung, wenn sie als integraler Bestandteil des Informationssicherheitsmanagements verstanden und systematisch in Zieldefinition, Umsetzung, Wirksamkeitsmessung und kontinuierliche Verbesserung eingebettet wird. Entsprechende Anforderungen formulieren etablierte Standards, insbesondere hinsichtlich risikobasierter, zielgruppenspezifischer Maßnahmen und deren Evaluation [21, 22].

3.1 Serious Games

Klassische Schulungsformate sind überwiegend auf die Vermittlung von Wissen ausgerichtet. Sie adressieren jedoch nur begrenzt die Mechanismen, die für nachhaltiges Lernen und Verhaltensänderung entscheidend sind. Serious Games sind Spiele mit einem definierten Lern- oder Trainingsziel, die Inhalte in interaktive, erfahrungsbasierte Szenarien überführen [23]. Im Gegensatz zu rein instruktionalen Formaten ermöglichen sie es, Entscheidungen zu treffen, Konsequenzen zu erleben und Handlungsoptionen zu erproben. Lernende bewegen sich dabei in einem geschützten Raum, in dem auch Fehlentscheidungen Teil des Lernprozesses sind. Wissen wird damit schrittweise in Routinen überführt [24].

Sie sind insbesondere dann wirksam, wenn sie Lern- und Spielziele konsequent miteinander verknüpfen. Sie erhöhen die Aufmerksamkeit und Beteiligung, fördern das Kompetenzerleben und ermöglichen es, komplexe Zusammenhänge in einem anwendungsnahen Kontext zu erfassen [25]. Gleichzeitig adressieren sie zentrale Herausforderungen klassischer Awareness-Maßnahmen, insbesondere die Diskrepanz zwischen Wissen und tatsächlichem Verhalten. Realitätsnahe Szenarien bilden gezielt typische Entscheidungssituationen ab, etwa bei Phishing, Meldewegen oder der Priorisierung im Incident-Fall [27].

4 Das A.C.T.I.O.N.-Modell zur Gestaltung wirksamer Awareness im ISMS

Das A.C.T.I.O.N.-Modell überführt die wissenschaftlichen Erkenntnisse in eine anwendbare Struktur und leitet daraus konkrete Fragen für die Auswahl und Gestaltung wirksamer Maßnahmen ab. Awareness reift von punktuellen Maßnahmen über wiederkehrende Routinen bis hin zu einer stabilen Sicherheitskultur. Ziel ist es daher, Awareness so zu gestalten, dass sie nicht beim Wissen stehen bleibt, sondern in handlungsrelevante Kompetenz übergeht und langfristig das Verhalten prägt. Eine Übersicht über die Dimensionen und Reifegrade des Modells liefert Abbildung 2.

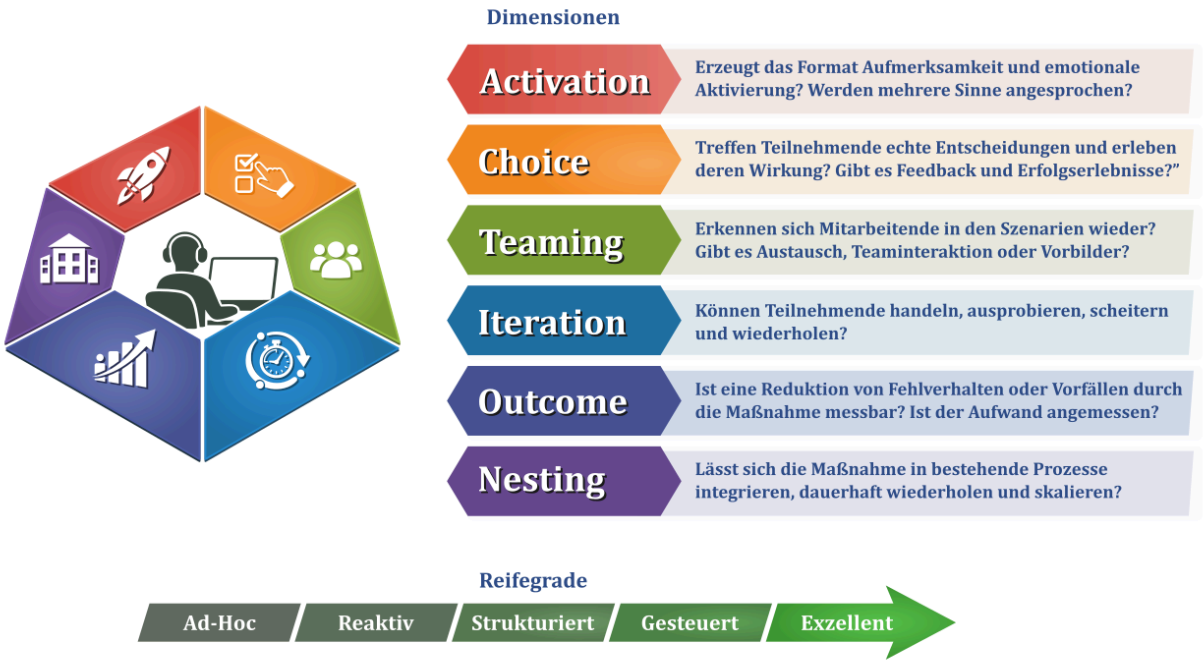

Abbildung 2: A.C.T.I.O.N. Modell

4.1 Dimensionen

Die sechs Dimensionen leiten sich aus Kapitel 2 ab und adressieren zentrale Wirkmechanismen. Leitfragen ermöglichen die Einordnung des Reifegrads in fünf Stufen (Tabellen 1-6) und zeigen Anpassungsbedarf auf.

Activation: Emotionale, multisensorische und überraschende Reize erhöhen Aufmerksamkeit, Verarbeitung und Speicherung.

Activation (Aktivierung, Aufmerksamkeit)	
Leitfragen: *"Erzeugt das Format Aufmerksamkeit und emotionale Aktivierung?" "Werden mehrere Sinne angesprochen?"*	
Reifegrad	**Beschreibung**
(1) Ad-Hoc	Reine Pflichtkommunikation, informativ aber ohne emotionale Wirkung
(2) Reaktiv	Anlassbezogene Kommunikation nach Vorfällen oder Audits, punktuell aufmerksamkeitsstark
(3) Strukturiert	Aktivierung durch zielgruppenspezifische Formate
(4) Gesteuert	Kontinuierliche Kampagnen mit abgestimmten Formaten
(5) Exzellent	Kontinuierliche Kampagnen mit abgestimmten Formaten zu konkretisierten Zielgruppen aus dem Geschäftsalltag

Tabelle 1: Activation Reifegrade

Choice: Verhalten verändert sich nachhaltig, wenn Menschen eigene Entscheidungen treffen und deren Wirkung erleben.

Choice (Auswahl, Selbstwirksamkeit)	
Leitfragen: *"Treffen Teilnehmende echte Entscheidungen und erleben deren Wirkung?" "Gibt es Feedback und Erfolgserlebnisse?"*	
Reifegrad	**Beschreibung**
(1) Ad-Hoc	Starre Regeln ohne Handlungsspielraum
(2) Reaktiv	Einzelne Entscheidungssituationen werden erklärt, aber nicht erlebt
(3) Strukturiert	Szenarien mit Entscheidungen und vereinzelt Feedback
(4) Gesteuert	Realitätsnahe Entscheidungssituationen und Feedback
(5) Exzellent	Realitätsnahe, prozessorentierte Entscheidungssituationen mit klarer Rückmeldung und Lernschleifen

Tabelle 2: Choice Reifegrade

Teaming: Soziale Einbettung prägt das Lernen. Beobachtungslernen, Resonanz und Gruppendynamik wirken stärker als Regeln. Orientierung erfolgt am Umfeld und an glaubwürdigen Vorbildern.

Teaming (Resonanz, Soziale Bestätigung)	
Leitfragen: *"Erkennen sich Mitarbeitende in den Szenarien wieder?" "Gibt es Austausch, Teaminteraktion oder Vorbilder?"*	
Reifegrad	**Beschreibung**
(1) Ad-Hoc	Lernen erfolgt individuell und isoliert
(2) Reaktiv	Gelegentlicher Austausch, aber ohne Struktur
(3) Strukturiert	Kooperative Formate vorhanden, jedoch nicht systematisch genutzt
(4) Gesteuert	Gezielte Nutzung von Teamdynamik, Austausch gefördert
(5) Exzellent	Awareness ist Teil der Teamkultur, soziale Normen und Vorbilder fördern sicheres Verhalten

Tabelle 3: Teaming Reifegrade

Iteration: Nachhaltige Verhaltenssicherheit entsteht durch wiederholtes Handeln, Feedback und Reflexion. Fehler beim Ausprobieren gehören dazu.

Iteration (Wiederholung, Erfahrung)	
Leitfrage: *"Können Teilnehmende handeln, ausprobieren, scheitern und wiederholen?"*	
Reifegrad	**Beschreibung**
(1) Ad-Hoc	Maßnahmen werden vereinzelt eingesetzt
(2) Reaktiv	Wiederholungen, jedoch unregelmäßig und ohne Systematik
(3) Strukturiert	Wiederholungen durch dieselben oder ähnliche Inhalte
(4) Gesteuert	Regelmäßige Wiederholungen mit unterschiedlichen Herausforderungen
(5) Exzellent	Regelmäßige Wiederholungen und kontinuierliche Weiterentwicklung der Formate, Lernen als fester Bestandteil der Organisation

Tabelle 4: Iteration Reifegrade

Outcome: Awareness muss einen messbaren Beitrag zur Risikoreduktion leisten. Wirksamkeit zeigt sich in verändertem Verhalten, reduzierten Vorfällen und einem angemessenen Verhältnis von Aufwand und Nutzen.

Outcome (Nutzen, Anpassung)	
Leitfragen: *"Ist eine Reduktion von Fehlverhalten oder Vorfällen durch die Maßnahme messbar? Ist der Aufwand angemessen?"*	
Reifegrad	**Beschreibung**
(1) Ad-Hoc	Wirkung wird nicht gemessen
(2) Reaktiv	Einzelne Kennzahlen, meist reaktiv erhoben
(3) Strukturiert	Strukturierte Messung über KPIs und Indikatoren
(4) Gesteuert	Systematische Auswertung und Steuerung von Maßnahmen
(5) Exzellent	Direkter Nachweis von Wirkung auf Verhalten, Risiken und Unternehmensziele

Tabelle 5: Outcome Reifegrade

Nesting: Awareness wird in Prozesse, Systeme und Abläufe integriert und dadurch nachhaltig verankert. Sie wird zur Kultur am Arbeitsplatz.

Nesting (Verankerung, Nachhaltigkeit)	
Leitfrage: *"Lässt sich die Maßnahme in bestehende Prozesse integrieren, dauerhaft wiederholen und skalieren?"*	
Reifegrad	**Beschreibung**
(1) Ad-Hoc	Isoliertes Thema ohne Bezug zum Tagesgeschäft
(2) Reaktiv	Teilweise Einbindung von einzelnen Prozessen
(3) Strukturiert	Integration in einigen Prozessen
(4) Gesteuert	Verankerung in Prozessen, Rollen und Steuerungssystemen
(5) Exzellent	Vollständige Integration in Strategie, Führung und Unternehmenskultur

Tabelle 6: Nesting Reifegrade

4.2 Reifegrade

Die sechs Dimensionen des A.C.T.I.O.N.-Modells bilden einen strukturierten Bewertungsrahmen für Maßnahmen und Sicherheitskultur und machen Lücken sichtbar. Daraus erfolgt die Einordnung in Reifegrade. Die Zielstufe

hängt vom Risikoprofil und der Branche ab. Höhere Kritikalität erfordert eine stärker verankerte Sicherheitskultur. Eine Übersicht empfohlener Zielreifegrade zeigt Tabelle 7.

Stufe	Branchenbeispiele	Ziel
S1	Bildung, Kommunen, NGOs	Level 2–3
S2	Maschinenbau, Dienstleister, Handel, allgemeine IT	Level 3
S3	Finanzdienstleister, Chemie, Pharma, Luftfahrt, Hightech	Level 4
S4	Kritische Infrastrukturen wie Energie, Verkehr, Gesundheit, Finanzsysteme	Level 4–5
S5	Militär, Nachrichtendienste, nationale Sicherheitsorganisationen	Level 5

Tabelle 7: Nesting Reifegrade

Auf dieser Grundlage werden Ist- und Zielzustand definiert und über Key Performance Indicators wie Phishingquoten, Schulungsgrad oder gewichtete Schadensrisiken messbar gemacht. Für nachhaltige Wirkung braucht es einen geschlossenen, zum PDCA-Zyklus kompatiblen Managementkreislauf [28]. In der Plan-Phase werden Ziele, Zielgruppen und typische Entscheidungssituationen festgelegt und in fokussierte Kampagnen überführt. In der Do-Phase erfolgt die Umsetzung, etwa durch Workshops, Serious Games oder andere Formate, die konkrete Verhaltensimpulse setzen und gezielt Teamdynamiken aktivieren. Ergänzend bieten sich regelmäßige, unterjährige Formate wie Nutzergruppentreffen, Krisensimulationen oder Rollenspiele an, um sicherheitsrelevante Entscheidungen im Team zu trainieren. In der Check-Phase werden Teilnahme, Interaktion, Verhaltensänderungen und Feedback systematisch erfasst. In der Act-Phase werden die Maßnahmen entsprechend angepasst und weiterentwickelt, mit dem Ziel, eine ausgewogene Balance der Dimensionen zu erreichen und die Awareness-Strategie iterativ zu stärken.

Abbildung 3 zeigt ein Beispiel mit hohem Zielniveau zur Erfüllung der Anforderungen an kritische Infrastrukturen. Dabei wird deutlich, dass insbesondere in den Dimensionen Iteration und Choice die größten

Handlungsbedarfe bestehen, da Maßnahmen bislang vor allem als jährliche Pflichtschulungen und überwiegend individuell durchgeführt werden.

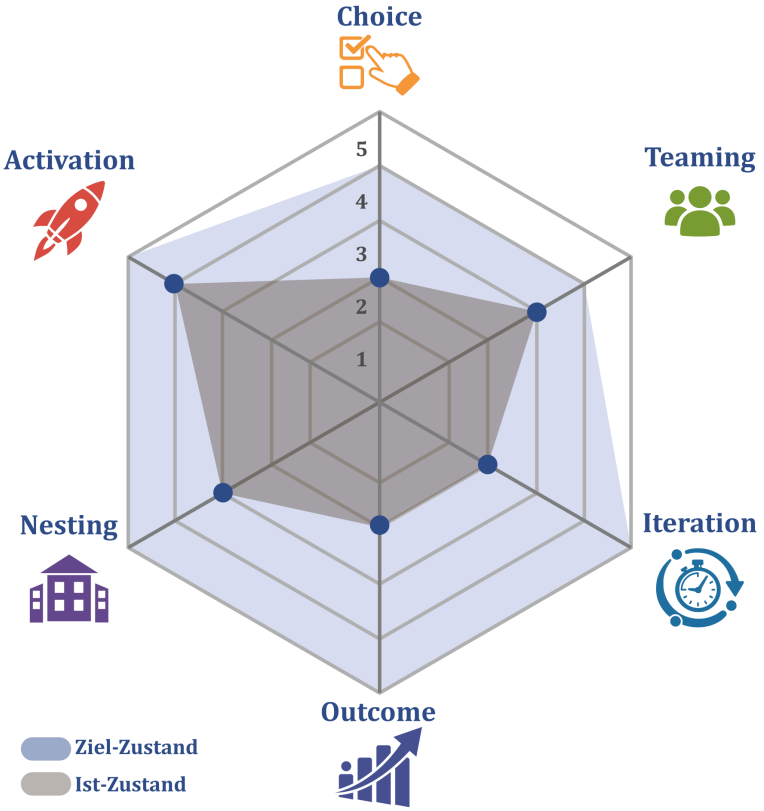

Abbildung 3: Mögliche Bewertung einer Maßnahme

5 Vom Gestaltungsmodell zu konkreten Lernformaten

Serious Games übersetzen die Gestaltungsprinzipien in unterschiedliche Lernformen, von digitalen Simulationen bis hin zu analogen Brett-, Karten- oder Rollenspielen sowie hybriden Ansätzen mit App- und Storytelling-Elementen. Entscheidend ist dabei nicht die Form, sondern ihre Passung zu Lernziel, Zielgruppe und organisatorischem Kontext. Besonders wirksam sind narrative Ansätze, die Perspektiven, Entscheidungsdilemmata und emotionale Reaktionen erlebbar machen. Beispiele für Serious Games sind „What the Hack!“[4], „Leons Identität“[5] und „Data & Disasters“[6]. Eine Übersicht weiterer Serious Games bietet der Ratgeber des Marktplatz IT-Sicherheit [29].

[4] https://sbg-gaming.com/
[5] https://leon.nrw.de
[6] https://cyberbothe.de

5.1 What the Hack!

„What the Hack!“ ist ein hybrides Brettspiel, in dem Teams unter Zeitdruck kooperativ gegen einen simulierten Hacker antreten. Im Fokus stehen nicht Wissensabfragen, sondern Risikobewusstsein, Entscheidungslogik und Verantwortungsübernahme. Über Aufgaben und Entscheidungen sammeln die Teilnehmenden Ressourcen, die sie in realitätsnahen Angriffsszenarien gezielt einsetzen, um den Hacker zu stoppen. Teams nutzen Tokens, um situativ Einfluss zu nehmen und strategische Optionen zu eröffnen.

Bestimmte Spielfelder ermöglichen direkte Eingriffe, etwa Positionswechsel (Back Door), Zurückdrängen des Hackers (Push Back), Ressourcentausch (Exchange) oder temporäre Absicherung (Safe Space). Die Teilnahme erfolgt browserbasiert über die Endgeräte der Spielenden, während Moderatoren und Spielrunden zentral verwaltet, geplant und zugewiesen werden können. Abbildung 4 zeigt das Spiel in Aktion.

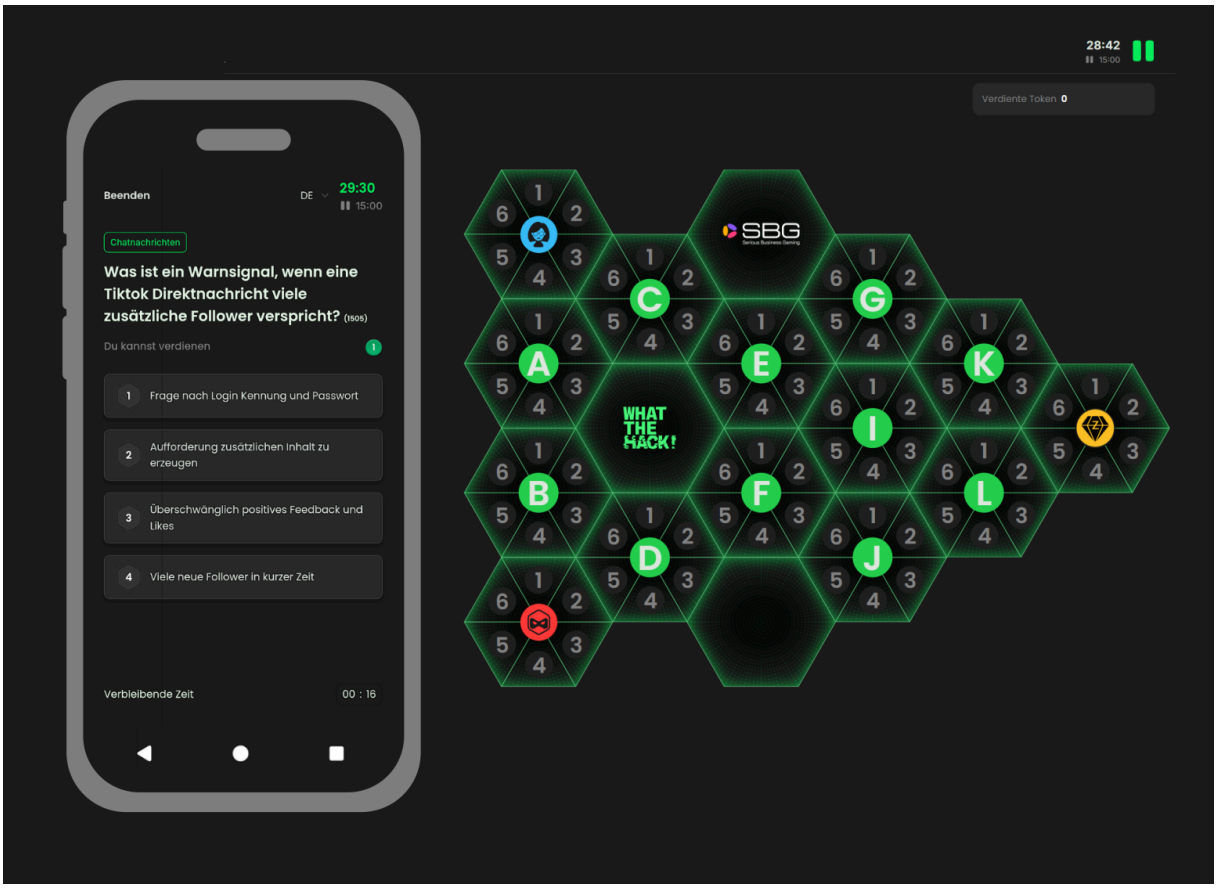

Abbildung 4: What the Hack!

5.2 Leons Identität

Das vom Land NRW entwickelte Adventure „Leons Identität“ (Abbildung 5) nutzt Storytelling und Empathie als Lernansatz. Spieler schlüpfen in die Rolle von Jonas, der die digitalen Spuren seines verschwundenen Bruders verfolgt und dabei eine schleichende Radikalisierung erkennt. Statt Wissen zu vermitteln, macht das Spiel anhand von Figuren erlebbar, wie Vertrauen bröckelt und digitale Kommunikation manipulativ wirkt. Zugleich sensibilisiert es für Mechanismen extremistischer Einflussnahme im Internet und stärkt die kritische Auseinandersetzung mit digitalen Inhalten.

Abbildung 5: Leons Identität

5.3 Data & Disasters

„Data & Disasters“ ist ein rollenspielbasiertes Serious Game, das einen Cyberangriff als realitätsnahe Krisensituation simuliert. Teilnehmende übernehmen unterschiedliche Rollen und treffen unter Zeitdruck Entscheidungen zu eingehenden Ereignissen. Dabei werden technische, organisatorische und zwischenmenschliche Aspekte gleichermaßen adressiert. Hierarchiegrenzen werden aufgebrochen, unterschiedliche Organisationstypen abgebildet und potenzielle Rollenkonflikte bewusst erlebbar gemacht. Die Spielenden erhalten sowohl private als auch öffentliche Informationen, die ihre Perspektiven und Motive prägen. Einfache Würfelmechaniken kommen zum Einsatz und berücksichtigen die unterschiedliche Eignung der Rollen für bestimmte Handlungen. Im Spielverlauf wirken sich Entscheidungen unmittelbar auf drei zentrale Unternehmenswerte aus, deren Stabilität im Spielverlauf gesichert werden muss, um die Organisation handlungsfähig zu halten.

Das Format orientiert sich eng an klassischen Übungen, wie sie im BSI-Standard 200-4 [30] beschrieben sind, erweitert diesen Ansatz jedoch gezielt um spielerische Elemente. Abbildung 6 zeigt eine der Rollen im Spiel.

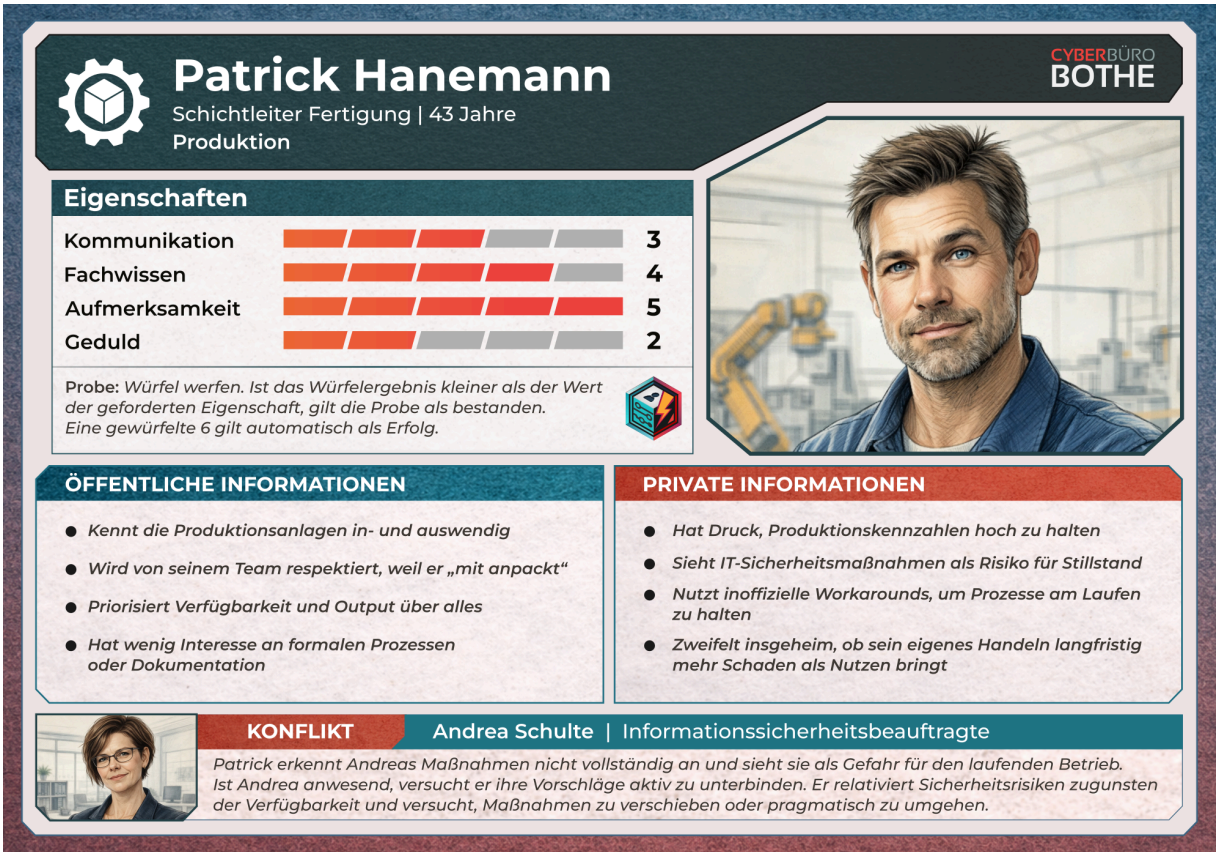

Abbildung 6: Data & Disasters Rollenkarte

6 Fazit

Serious Games schließen die Lücke zwischen Wissen und Verhalten, indem sie sicherheitsrelevantes Handeln erlebbar, reflektierbar und trainierbar machen. Im Kontext eines ISMS entfalten sie ihre Wirkung insbesondere dann, wenn sie systematisch in Awareness-Strategien integriert und entlang des A.C.T.I.O.N.-Modells gestaltet, bewertet und weiterentwickelt werden. Sie adressieren zentrale Wirkmechanismen des Lernens und ermöglichen es, Entscheidungen unter realitätsnahen Bedingungen zu üben. Eingebettet in einen kontinuierlichen Managementkreislauf tragen sie dazu bei, Maßnahmen iterativ zu verbessern und nachhaltig in Prozesse und Strukturen zu verankern. So entwickelt sich Awareness von punktuellen Maßnahmen hin zu einer stabilen Sicherheitskultur, in der sicheres Verhalten im Arbeitsalltag selbstverständlich wird.

Literaturhinweise

[1] Bitkom Research 2025

[2] Goldberg H. Growing Brains, Nurturing Minds-Neuroscience as an Educational Tool to Support Students' Development as Life-Long Learners. Brain Sci. 2022 Nov 26;12(12):1622. doi: 10.3390/brainsci12121622. PMID: 36552082; PMCID: PMC9775149.

[3] Wise RA. Dopamine, learning and motivation. Nat Rev Neurosci. 2004 Jun;5(6):483-94. doi: 10.1038/nrn1406. PMID: 15152198.

[4] Schultz W. Dopamine reward prediction error coding. Dialogues Clin Neurosci. 2016 Mar;18(1):23-32. doi: 10.31887/DCNS.2016.18.1/wschultz. PMID: 27069377; PMCID: PMC4826767.

[5] Schulkin J, Sterling P Allostasis: A Brain-Centered, Predictive Mode of Physiological Regulation, Trends in Neurosciences, 2019; 42, 740-752

[6] Deci, E. L., & Ryan, R. M. (2000). The “What” and “Why” of Goal Pursuits: Human Needs and the Self-Determination of Behavior. Psychological Inquiry, 11(4), 227–268. https://doi.org/10.1207/S15327965PLI1104_01

[7] Bandura, A. (1997). Self-efficacy: The exercise of control. W H Freeman/Times Books/ Henry Holt & Co.

[8] Sheeran, P., and Webb, T. L. (2016) The Intention–Behavior Gap. Social and Personality Psychology Compass, 10: 503–518. doi: 10.1111/spc3.12265.

[9] Bandura, A. (1977). Social learning theory. Englewood Cliffs, NJ: Prentice-Hall.

[10] Przybylski, A. K., Murayama, K., DeHaan, C. R., & Gladwell, V. (2013). Motivational, emotional, and behavioral correlates of fear of missing out. Computers in Human Behavior, 29(4), 1841–1848.

[11] Ebbinghaus, H. (1885). Über das Gedächtnis. Duncker & Humblot.

[12] Dabas, A., Bruckner, R., Schultz, H. et al. Learning from imagined experiences via an endogenous prediction error. Nat Commun 16, 10845 (2025). https://doi.org/10.1038/s41467-025-66396-2

[13] Hattie, J., & Timperley, H. (2007). The Power of Feedback. Review of Educational Research, 77(1), 81-112.

[14] Larrick, R. P. (2004). Debiasing. In D. J. Koehler & N. Harvey (Eds.), Blackwell handbook of judgment and decision making (pp. 316–337). Blackwell Publishing. https://doi.org/10.1002/9780470752937.ch16

[15] Kolb, D. A. (1984). Experiential learning: Experience as the source of learning and development. Prentice Hall.

[16] S. Freeman, S.L. Eddy, M. McDonough, M.K. Smith, N. Okoroafor, H. Jordt, & M.P. Wenderoth, Active learning increases student performance in science, engineering, and mathematics, Proc. Natl. Acad. Sci. U.S.A. 111 (23) 8410-8415, https://doi.org/10.1073/pnas.1319030111 (2014).

[17] ENISA – European Union Agency for Cybersecurity (2021). Raising Awareness of Cybersecurity

[18] IBM Security (2025). Cost of a Data Breach Report 2025

[19] World Economic Forum (2025). Global Cybersecurity Outlook 2025

[20] ENISA – European Union Agency for Cybersecurity, 2018: Cybersecurity Culture Guidelines: Behavioural Aspects of Cybersecurity

[21] ISO/IEC 27001:2022 – Information Security Management Systems

[22] Bundesamt für Sicherheit in der Informationstechnik (2022): IT-Grundschutz-Kompendium

[23] Tiange Zhao, Tiago Gasiba, Ulrike Lechner, Maria Pinto-Albuquerque, Thriving in the era of hybrid work: Raising cybersecurity awareness using serious games in industry trainings, Journal of Systems and Software, Volume 210, 2024

[24] Hodhod, R., Hardage, H., Abbas, S., & Aldakheel, E. A. (2023). CyberHero: An Adaptive Serious Game to Promote Cybersecurity Awareness. Electronics, 12(17), 3544. https://doi.org/10.3390/electronics12173544

[25] Zempila, G., Xinogalos, S. Investigating the role of serious games on raising students' awareness on safety and data protection on the Internet. Discov Educ 4, 268 (2025). https://doi.org/10.1007/s44217-025-00722-0

[26] Victor Legbo Yisa and Rita Orji. 2025. Who Wants to Be Cybersecure? Expert Evaluation of a Culturally Adaptive Gamified Cybersecurity Awareness App. In Proceedings of the 5th Biennial African Human Computer Interaction Conference (AfriCHI '25). Association for Computing Machinery, New York, NY, USA, 243–255. https://doi.org/10.1145/3757232.3757249

[27] Howard-Jones, P., & Jay, T. (2016). Reward, learning and games. Current Opinion in Behavioral Sciences, 10, 65-72. https://doi.org/10.1016/j.cobeha.2016.04.015

[28] Bundesamt für Sicherheit in der Informationstechnik (2017). BSI-Standard 200-2: IT-Grundschutz-Methodik

[29] https://it-sicherheit.de/ratgeber/it-sicherheitstools/serious-games/, zuletzt abgerufen am 23.03.2026

[30] Bundesamt für Sicherheit in der Informationstechnik (2023). BSI-Standard 200-4: Business Continuity Management