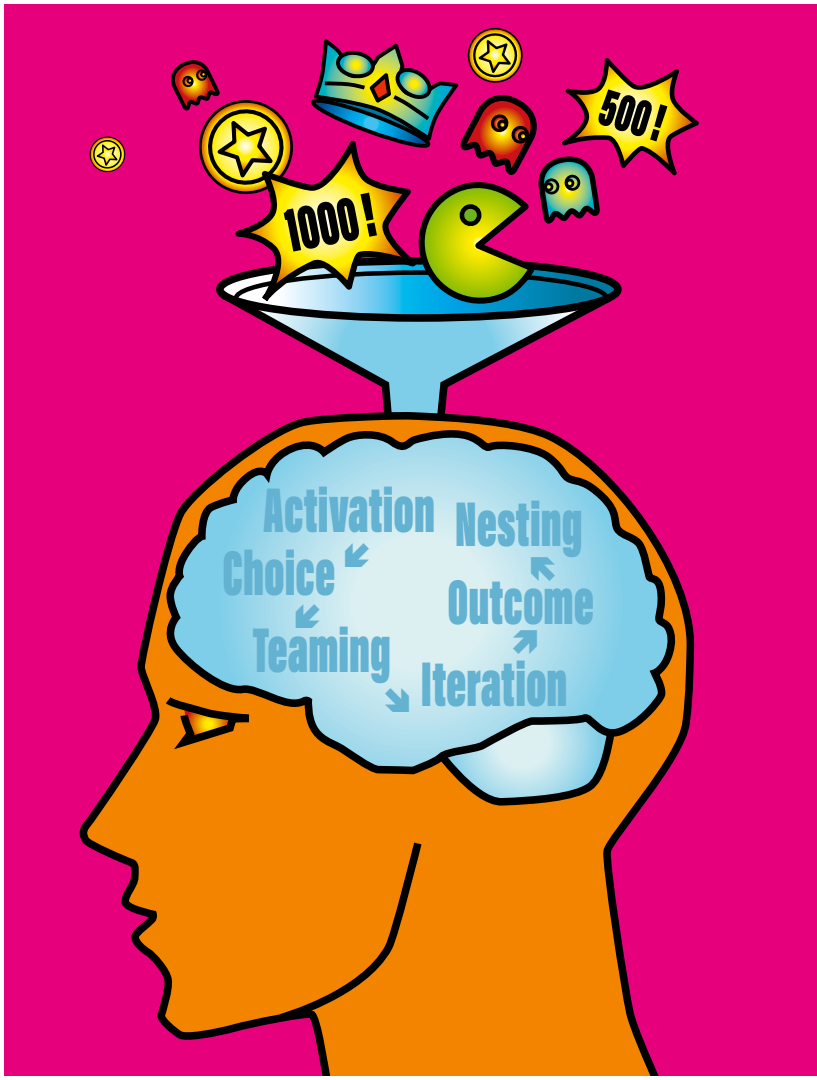
Spielend lernen für mehr Resilienz (2)

Serious Games als Lernmotor der Informations-Sicherheit – Teil 2: Vom Handeln zur gelebten Kultur



In einer zweiteiligen Reihe betrachten die Autoren, wie Menschen in der Informationssicherheit tatsächlich lernen – und weshalb spielerische Formate wie Serious Games ein ernstzunehmender Baustein wirksamer Awareness sein können. Der zweite Teil behandelt, wie sich Serious Games unter den sechs in Teil 1 eingeführten A.C.T.I.O.N.-Prinzipien bewähren, wie man sie in den Organisationsalltag integrieren kann und warum aus individuellem Handeln erst durch eine umgebende Kultur echte Sicherheit entsteht.

Von David Bothe, Gelsenkirchen, Marcus Schaper, Buchholz, und Norbert Pohlmann, Gelsenkirchen

Im ersten Teil dieser Reihe wurde deutlich: Wissen verändert kein Verhalten – Awareness entsteht erst, wenn Mitarbeiter* Informationen anwenden und sich im Arbeitsalltag sicher fühlen. Doch dieser Schritt vom Wissen zum Handeln ist nur ein Zwischenziel: Wer Informationssicherheit dauerhaft verankern will, muss weitergehen – vom Handeln zur täglich gelebten Kultur.

Dieser zweite Teil zeigt daher, wie aus Verhalten Routine und schließlich Kultur entstehen kann – nicht durch Richtlinien, sondern durch wiederholte Erfahrungen, die Bedeutung schaffen. Bereits in Teil 1 haben die Autoren dargelegt, dass Lernen erst dann Verhalten verändert, wenn bestimmte Bedingungen erfüllt sind und dies im A.C.T.I.O.N.-Modell zusammengefasst: Menschen müssen aktiviert *(Activation)* werden, Wahlmöglichkeiten haben *(Choice)*, soziale Resonanz und *Teaming* erleben, durch *Iteration* ausprobieren dürfen, Ergebnisse sehen *(Outcome)* und diese Erfahrungen schließlich im Alltag verankern *(Nesting)*. Tabelle 1 zeigt, wie bekannte Schulungsformate dabei abschneiden.

Lernen für Resilienz

Das Ziel von Awareness liegt darin Menschen zu befähigen, mit Unsicherheit, Stress und Abweichungen souverän umzugehen – es liegt nicht in der Fehlervermeidung. Genau das beschreibt Resilienz: die Fähigkeit, Störungen zu absorbieren, sich anzupassen und aus Erfahrungen zu lernen.

Tabelle 1: Einordnung klassischer Awareness-Maßnahmen in das A.C.T.I.O.N.-Modell

Format	Activation	Choice	Teaming	Iteration	Outcome	Nesting
Phishing-Simulation	erfüllt	teilweise erfüllt	nicht erfüllt	nicht erfüllt	teilweise erfüllt	nicht erfüllt
E-Learning	teilweise erfüllt	nicht erfüllt	nicht erfüllt	erfüllt	erfüllt	erfüllt
Präsenzschulung (klassisch)	teilweise erfüllt	nicht erfüllt	erfüllt	nicht erfüllt	nicht erfüllt	teilweise erfüllt

In der Cybersicherheit bedeutet das, auch unter Druck handlungsfähig zu bleiben und dazu ruhig, lösungsorientiert und als Team abgestimmt zu reagieren. Resilienz ist keine angeborene Eigenschaft, sondern erlernbar. Wiederholung und Reflexion festigen Muster, die dann im Ernstfall automatisch greifen. In Krisen zeigt sich nicht, wer das meiste Wissen hat, sondern wer handlungsfähig bleibt.

Verankerung in der Unternehmenskultur

Awareness wirkt jedoch nicht, wenn sie als einzelne Maßnahme für sich steht – wirksam wird sie erst, wenn Lernimpulse Teil der täglichen Abläufe werden. Organisationen, die Awareness in bestehende Routinen integrieren, verändern das Verhalten ihrer Mitarbeiter nachhaltig.

Awareness braucht Routinen – verschiedene Formate ergänzen sich dabei: Webtrainings für Grundlagen, Impulse für Präsenz, Serious Games für Erlebnis und Selbstwirksamkeit. Awareness entwickelt sich dabei als Reifeprozess: von Ad-hoc über Routine hin zu einer Kultur – erst auf dieser Stufe läuft sicheres Verhalten „auf Autopilot“ (vgl. Abb. 1).

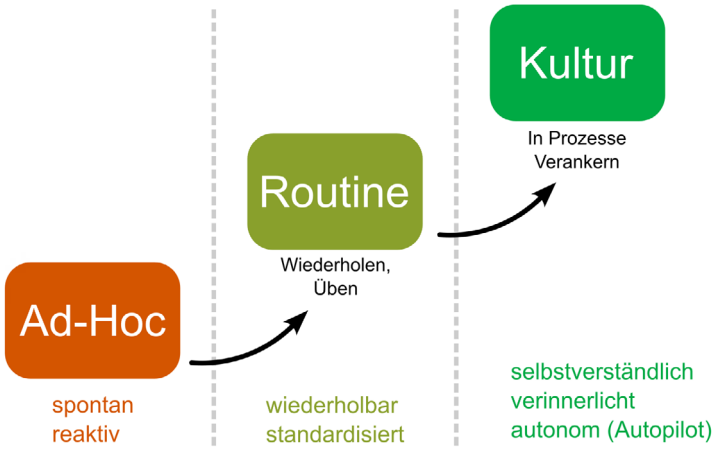


Abbildung 1: Awareness entwickelt sich vom Ad-hoc-Handeln über eine Routine bis hin zur verinnerlichten Kultur (Autopilot).

Serious Games in A.C.T.I.O.N.

Serious Games besitzen eine didaktische Stärke, die klassische Lernformate selten erreichen: Sie erzeugen Lernen durch reale Entscheidungssituationen unter Unsicherheit und Zeitdruck – so erfüllen Serious Games alle sechs Dimensionen des A.C.T.I.O.N.-Modells (vgl. Tab. 2):

Activation: Ein Serious Game führt Teilnehmer schnell in eine Entscheidung hinein. Eine kurze Einführung oder Moderation kann den Kontext setzen, doch der entscheidende Impuls entsteht durch das Spiel selbst: Die Situation verlangt eine Reaktion. Die Teilnehmer agieren innerhalb eines Szenarios, treffen Entscheidungen und erleben deren Konsequenzen. Dabei ist es wichtig, zu erklären, dass auch Spielen als solches einen unternehmerischen Wert hat, um Resilienz zu trainieren und letztlich das Unternehmen vor Gefahren und Risiken zu schützen.

Choice: Im Spiel stehen reale Handlungsoptionen zur Verfügung. Jede Entscheidung verändert den Verlauf – unmittelbar und nachvollziehbar. Daraus entsteht Selbstwirksamkeit: Das eigene Handeln hat Einfluss. Lernen findet nicht auf der Ebene von Information statt, sondern im Durchlaufen von Konsequenzen. Diese Autonomie schüttet Dopamin aus und verankert den Spieler emotional in der Spielsituation.

Teaming: Serious Games machen Verhalten sichtbar. In Mehrspieler-Formaten entsteht Resonanz durch Zusammenarbeit – Entscheidungen werden abgestimmt, Rollen greifen ineinander. Auch Einzelspiele erzeugen allerdings soziale Orientierung, etwa über Rollen oder narrative Vorbilder.

Iteration: Fehler sind kein Misserfolg, sondern Teil des Lernprozesses. Serious Games ermöglichen Wiederholung ohne Risiko – Strategien lassen sich anpassen, bis ein besseres Ergebnis entsteht. Lernen entsteht durch das Erleben von Alternativen, nicht durch die richtige Lösung.

Outcome: Entscheidungen und Reaktionswege werden dokumentiert und liefern messbare Daten zum Lernfortschritt. Ein Serious Game ist beliebig oft einsetzbar – mit verschiedenen Teams, in unterschiedlichen Kontexten und über längere Zeiträume hinweg.

Nesting: Nach dem Spiel entsteht die Verhaltensänderung – im Debriefing wird die Erfahrung

mit realen Prozessen verknüpft. Digitale Serious Games sind überdies skalierbar und wiederholt einsetzbar – ohne zusätzlichen Moderationsaufwand, in Teamsitzungen, remote oder standortübergreifend.

Transfer in die Praxis

Awareness wird wirksam, wenn Lernimpulse echte Situationen abbilden. Verhalten ändert sich nicht durch abstrakte Hinweise, sondern wenn Mitarbeiter Entscheidungen unter realem Druck treffen müssen – wie bei einer scheinbar dringenden Anfrage eines Lieferanten. Ob Rollenspiel oder digitales Szenario: Wichtig ist nicht das Format, sondern die Entscheidungssituation und das Erleben der eigenen Wirksamkeit.

Serious Games als zentrales Kampagnenelement

Awareness-Kampagnen bestehen häufig aus einem Bündel einzelner Maßnahmen, die parallel laufen: E-Learnings vermitteln Wissen, Phishing-Tests erzeugen Aufmerksamkeit, Poster und Newsletter sorgen für Sichtbarkeit. Was dabei jedoch fehlt, ist ein gemeinsamer Erfahrungspunkt. So werden Informationen zwar gesendet, aber nicht verankert. Serious Games schließen diese Lücke: Sie schaffen ein gemeinsames Erlebnis, über das Teams sprechen und reflektieren können. Statt „Ich habe die Schulung gemacht" entsteht „Wir haben entschieden – und gesehen, was daraus wurde."

Serious Games lassen sich in Kampagnen flexibel einsetzen: als Auftakt, um Aufmerksamkeit zu erzeugen – als Interaktionsanker in Workshops oder Teammeetings – am Ende zur Reflexion, um das Erlebte mit realen Sicherheitsprozessen zu verknüpfen. Entscheidend ist dabei nicht das einzelne Format, sondern der richtige Trainingsmix: Inhalte, die in Schulungen vermittelt wurden, müssen im Erleben aktiviert werden.

Beispiele aus der Praxis

Was in der Theorie überzeugend klingt, entfaltet seine Wirkung erst im Erleben. Die drei folgenden Beispiele belegen, wie Serious Games aus Wissen Bedeutung machen.

Beispiel 1: Leons Identität

Das vom Land NRW entwickelte Adventure „Leons Identität" nutzt Storytelling und Empathie als Lernwerkzeug. Spieler schlüpfen in die Rolle von Jonas, der digitale Spuren seines verschwundenen Bruders verfolgt und dabei eine schleichende Radikalisierung entdeckt (https://leon.nrw.de, Abb. 2). Statt Fakten zu erklären, lässt das Spiel erleben, wie Vertrauen bröckelt und digitale Kommunikation manipulativ wirken

A.C.T.I.O.N.	Leitfragen	Serious Games	Erfüllung
Activation	Erzeugt das Format Aufmerksamkeit und emotionale Aktivierung? Werden mehrere Sinne angesprochen?	Einstieg über eine echte Entscheidungssituation keine lange Einführung – sofortiges Handeln Aktivierung entsteht durch Bedeutung im Spiel	ja
Choice	Treffen Teilnehmer echte Entscheidungen und erleben deren Wirkung? Gibt es Feedback und Erfolgserlebnisse?	Entscheidungen verändern den Verlauf unmittelbares Feedback erzeugt Selbstwirksamkeit	ja
Teaming	Erkennen sich Mitarbeiter in den Szenarien wieder? Gibt es Austausch, Teaminteraktion oder Vorbilder?	Zusammenarbeit erzeugt Resonanz soziale Dynamiken werden sichtbar – auch in Einzelspielen durch Rollen/Narrativ	ja
Iteration	Können Teilnehmer handeln, ausprobieren, scheitern und wiederholen?	Fehler sind vorgesehen Szenarien sind wiederholbar Lernen durch Alternativen ist möglich	ja
Outcome	Trägt das Format messbar zur Reduktion von Fehlverhalten oder Vorfällen bei? Ist der Aufwand angemessen? Lässt sich das Format skalieren?	Daten zu Entscheidungen werden sichtbar Format ist digital skalierbar Format ist mehrfach einsetzbar	ja
Nesting	Lässt sich die Maßnahme in bestehende Prozesse integrieren und dauerhaft wiederholen? Kann sie auf einer Plattform betrieben oder auf andere Weise multipliziert werden?	Debriefing verknüpft Spiel mit realen Prozessen Spiele sind in Routinen integrierbar	ja

Tabelle 2: A.C.T.I.O.N.-Erfüllungsgrad von Serious Games

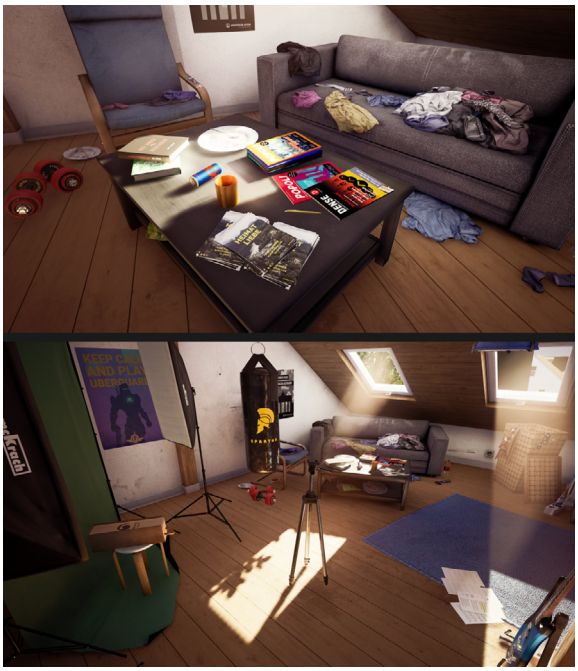


Abbildung 2: Leons Identität

kann. Dieser Perspektivwechsel erzeugt emotionale Beteiligung und Reflexion.

Beispiel 2:
What the Hack!

Ein vielschichtiges Beispiel aus dem Bereich der Cybersicherheit ist „What The Hack!" der SBG Serious Business Gaming GmbH (https://whatthehack.ai). Das Spiel wurde speziell dafür entwickelt, Cybersicherheit und benachbarte Gebiete in ein lebendiges, gruppenbasiertes Erlebnis zu verwandeln. Ziel ist es nicht, Wissen abzufragen, sondern das Bewusstsein für Risiken, Entscheidungslogik und Verantwortung zu schärfen. Man spielt kooperativ als Team gegen einen imaginären Angreifer, den es aufzuhalten gilt – dafür gibt es ein striktes Zeitkontingent von üblicherweise 30 Minuten.

Das Konzept folgt einem klaren Aufbau: Die Spieler sammeln auf dem digitalen Spielfeld (Abb. 3) durch kleine Rätsel und Wissensfragen sowie Aufgaben Tokens, die in späteren Runden zur Abwehr realitätsnaher Angriffsszenarien genutzt werden und für das finale Ziel – das Fangen des Angreifers – notwendig sind.

Während des Spiels sieht jeder Player die Aufgaben auf dem eigenen Mobilgerät und kann zunächst selbstständig abstimmen, bevor eine moderierte Teamentscheidung herbeigeführt wird. Je nach Erfolg können Player und Angreifer auf dem Spielbrett unterschiedlich weit vorangehen. Im Finale müssen die Teams unter zunehmendem Zeitdruck reagieren, Attacken erkennen, priorisieren und im richtigen Moment die gesammelten Ressourcen einsetzen, um den Angreifer zu stoppen. Nur wer strategisch denkt, kommuniziert und gemeinsam Entscheidungen trifft, kann das Spiel gewinnen.

Beispiel 3:
Little Impacts

Ein weiteres Beispiel liefert das Mobile Game „Little Impacts"des Umweltbundesamts (https://littleimpacts.de, Abb. 4). Spieler begleiten eine junge Protagonistin durch alltägliche Entscheidungen – beim Einkaufen, Wohnen oder Reisen – und erleben deren direkte Auswirkungen auf Umwelt und Mitmenschen. Little Impacts zeigt, wie sich auch komplexe Themen durch eine narrative Struktur, Entscheidungsfreiheit und unmittelbares Feedback emotional verständlich und nachhaltig vermitteln lassen.

Der Weg zur Sicherheitskultur

Wie die Beispiele verdeutlichen, vermitteln Serious Games nicht einfach Inhalte – sie verändern Perspektiven und Haltungen. Menschen lernen nachhaltiger, wenn sie selbst handeln, Entscheidungen treffen und unmittelbar erleben, welche Folgen ihr Verhalten hat. Das erzeugt ein Gefühl von Beteiligung statt Belehrung und führt zu einem Verständnis, das nicht rein kognitiv bleibt, sondern erfahrungsbasiert ist. Serious Games schaffen Situationen, in denen das Sicherheitsverhalten sichtbar wird: Kommunikation unter Zeitdruck, Priorisierung von Risiken, Umgang mit Unsicherheit.

Die Bedeutung einer starken Sicherheitskultur wird dabei oft unterschätzt. Technologie und Prozesse können noch so gut gestaltet sein: Wenn Entscheidungen getroffen werden, setzt sich nicht das „richtige Wissen", sondern das gelebte Muster durch! IT-Sicherheit entscheidet sich nicht im Meeting, sondern zwischen zwei Mikropausen im Tagesgeschäft: „Schicke ich die Datei raus oder frage ich nach?" Eine robuste Sicherheitskultur sorgt dafür, dass Menschen in solchen Momenten automatisch das korrekte Verhalten abrufen − ohne Druck, ohne Kontrolle, ohne Reminder.

Rezept für die Praxis

Wie aber lässt sich gewünschtes Verhalten dauerhaft im Unternehmen etablieren, sodass daraus eine echte Sicherheitskultur entsteht? Eine nachhaltige Verhaltensänderung entsteht nur dann, wenn Menschen wiederholt Erfahrungen machen, die im Arbeitsalltag anschlussfähig sind − und in denen sie sich selbst, ihre Umgebung, ihre Arbeit und ihr Unternehmen wiedererkennen. Sicherheitskultur bedeutet nicht, dass Mitarbeiter „wissen, wie es richtig wäre", sondern dass sie in echten Entscheidungssituationen Resilienz zeigen und handlungsfähig bleiben.

Dabei ist es entscheidend, Awareness strategisch in die Unternehmensziele einzubetten, anschließend in Kampagnen detailliert auszugestalten und schließlich konsequent umzusetzen. Nachfolgend sind Kontrollen und Feedbackloops wichtig, um die Ziele und deren Umsetzung regelmäßig zu hinterfragen. Als Endergebnis entsteht in fünf Schritten der im Folgenden erläuterte Closed-Management-Loop der Sicherheitsawareness (Abb. 5).

Schritt 1: Awareness-Strategie definieren

Um eine kontinuierliche Verbesserung entlang eines Closed-Management-Loops zu erreichen, ist es wichtig, jede Kampagne strategisch auf die Ziele des Unternehmens auszurichten: Was ist die Rolle von Sicherheitsawareness in der eigenen Organisation? Geht es um eine produktseitige Notwendigkeit, eine wirtschaftliche und reputatorische Risikominimierung oder eine rechtliche Verpflichtung?

Wenn die strategischen Treiber bekannt sind, sollte man die Ist- und die Ziel-Situation definieren. Dabei hilft es, wenn man sich Key-Performance-Indicators (KPIs) anschaut, welche die Situation mess- und damit managebar machen. Beispiele sind Phishingquoten in Simulationen, die Anzahl der erfolgreich geschulten Mitarbeiter sowie ein gewichtetes Schadensrisiko durch Cyberangriffe.

Als nächstes lassen sich Ziele auf die sie beeinflussenden Gruppen von Mitarbeitern herunterbrechen, die dann wiederum zur Zielgruppe von Kampagnen werden. Die Kampagnen selbst kann man sich als schrittweise Umsetzung der Ziele entlang kleiner „Impact-Häppchen“ vorstellen – beispielsweise nach Unternehmensbereichen oder Themenfeldern unterteilt.

Schritt 2: Kampagnen gestalten

Bevor man eine Kampagne plant, muss klar sein, was das messbare Ziel (KPI) ist, wen sie erreichen soll und in welchen Situationen sicherheitsrelevante Entscheidungen tatsächlich entstehen. Nicht alle Mitarbeiter haben die gleichen Berührungspunkte mit Risiken. Entscheidend ist: Welche Rolle entscheidet über was – und unter welchen Bedingungen?

Kampagnen sind zeitlich beschränkte und auf bestimmte Felder zugespitzte Bündel aus verschiedenen Maßnahmen, die Mitarbeiter im Unternehmen in ihren täglichen Entscheidungssituationen abholen sollen, um

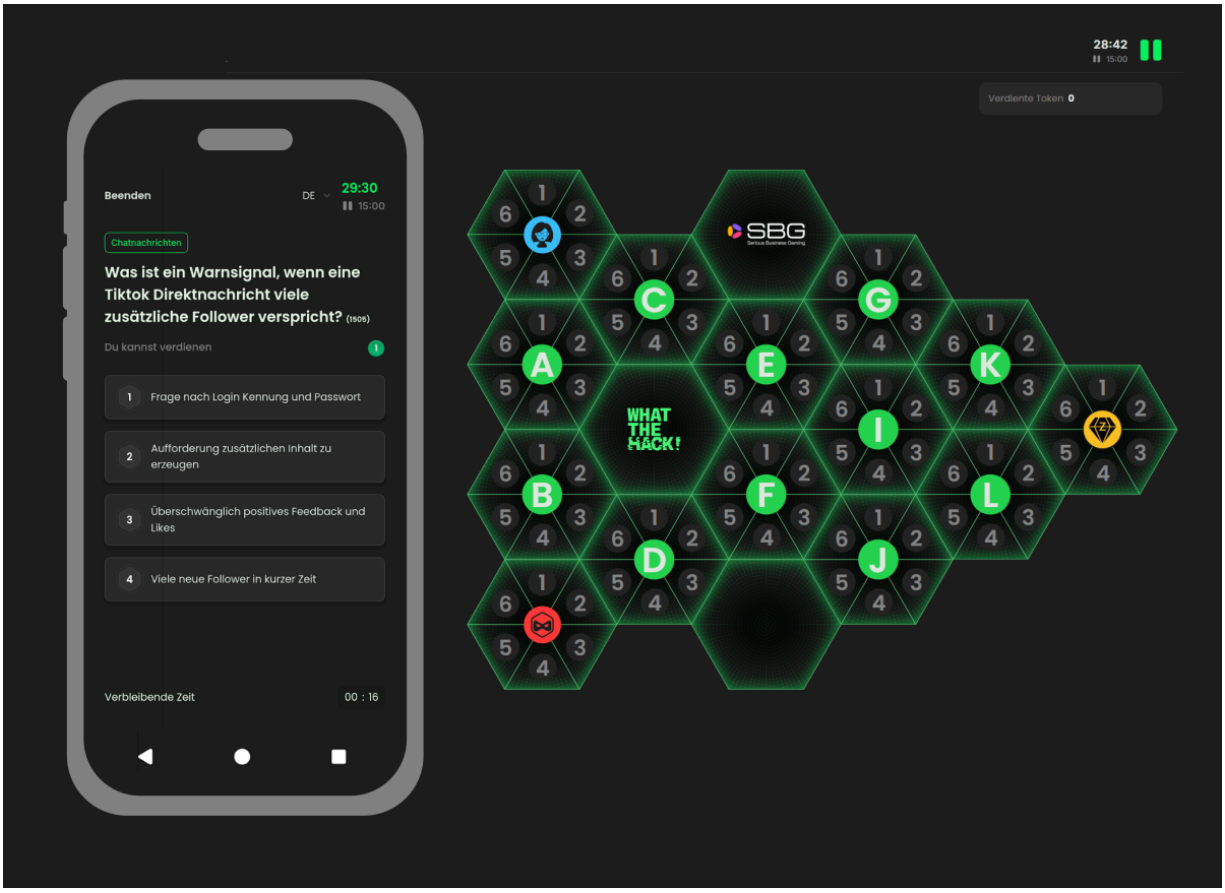


Abbildung 3: In „What the Hack!“ wird das eigene Smartphone benutzt und der gemeinsame Fortschritt auf dem Spielfeld verfolgt.

ihr Verhalten und ihre Haltung zu verändern. Eine gute Mischung besteht aus folgenden Komponenten:

_____ messbares Ziel und klare Zielgruppe – beispielsweise „Phishingquoten unter 5 % bei allen Büroangestellten“
_____ klare Botschaft – etwa „Wir sind die Human Firewall!“
_____ Mix aus Medien und Kanälen: Neben unidirektionalen Videos und Printmedien eignen sich interaktive Formate wie Serious Games besonders gut.
_____ Motivation durch Wettbewerb und Wertschätzung – zum Beispiel „Wir ermitteln die Cybersecurity-Champions der Firma – die Sieger bekommen ein Teamevent gesponsert“
_____ Vorleben durch Führungskräfte – etwa durch sichtbare Nutzung von Passwortmanagern und dem offenkundigen Einhalten von Richtlinien
_____ Überprüfung durch Simulationen – beispielsweise durch wöchentliches Versenden von 100 „Phishing-Attacken“ auf verschiedenen Kanälen und das Messen der Rücklaufquoten

Schritt 3: Maßnahmen in der Breite durchführen

Sicherheitsmaßnahmen entfalten ihre Wirkung erst, wenn man sie als selbstverständlicher Bestandteil der Zusammenarbeit im operativen Alltag wahrnimmt. Awareness wird dann akzeptiert, wenn sie nicht „von oben verordnet“ wirkt, sondern als „unsere“ Maßnahme verstanden wird: nah an echten Aufgaben, mit klaren Zuständigkeiten und sichtbarem Nutzen.

Gleichzeitig braucht es die Beteiligung aller Ebenen – vom Vorstand über Fachabteilungen bis zu Experten: Führungskräfte setzen den Rahmen, operative Teams machen Sicherheit sichtbar et cetera. Nur wenn alle Gruppen eingebunden und die Maßnahmen im Tagesgeschäft verankert sind, entsteht ein gemeinsames Verständnis von Verantwortung.

Schritt 4: Kampagnenerfolg messen und Maßnahmen adaptieren

Eine Kampagne wirkt nur dann nachhaltig, wenn man ihre Wirkung nicht nur vermutet, sondern gemessen hat. Daher sollte kontinuierlich Feedback eingeholt werden – bereits während der Durchführung, nicht erst am Ende. Rückmeldungen aus verschiedenen Bereichen ermöglichen dann ein frühzeitiges Nachsteuern: Welche Inhalte greifen? Wo entstehen Hürden? Besonders wertvoll ist das Einbeziehen von Meinungsführern aller Ebenen – von Mitarbeitern im operativen Alltag bis zu Führungskräften: Sie spiegeln, wie die Maßnahmen tatsächlich ankommen.

Mögliche Messzahlen sind dabei etwa:

_____ Teilnahmequote: Wie viele Personen werden tatsächlich erreicht?

Abbildung 4: Little Impacts (verfügbar via Google Play und App Store)

Aktive Beteiligung: Wie oft wird interagiert? (z. B. Entscheidungen im Game, Rückmeldungen im Workshop)

Verhaltensindikatoren: Verändern sich Entscheidungen in realen Situationen? (z. B. weniger impulsives Klicken, mehr Rückfragen)

Qualitatives Feedback: Was sagen Mitarbeiter über Nutzen, Relevanz und Alltagstauglichkeit der Maßnahme?

Schritt 5: Strategieanpassung

Auf Basis solcher Messergebnisse sollte man die eigene Strategie weiterentwickeln: Was funktioniert, wird verstärkt – was nicht wirkt, wird angepasst oder ersetzt. Je nach Unternehmenskultur können Formate, Frequenz oder Kommunikationswege variieren – vom kurzen Impuls im Teammeeting bis hin zum Serious Game als zentralem Baustein.

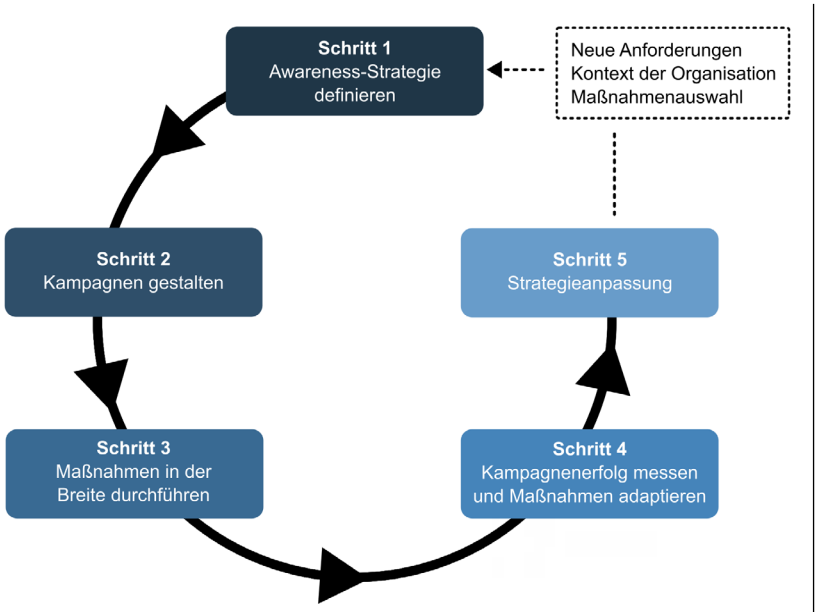


Abbildung 5: Awareness-Kampagnen gestalten

Nach der Auswertung beginnt der nächste Loop: anpassen, ausprobieren, verbessern. So wird aus einer Kampagne ein systematischer Bestandteil der Sicherheitskultur.

Fazit

Im ersten Teil dieser Reihe haben die Autoren erläutert, warum Wissen allein kein Verhalten

verändert. Neurowissenschaftliche, psychologische, pädagogische und wirtschaftswissenschaftliche Erkenntnisse zeigen übereinstimmend: Menschen lernen nicht, weil sie Informationen besitzen, sondern weil sie Erfahrungen machen. Verhalten entsteht nicht im Kopf, sondern im Kontext – durch Emotion, Handlung, Rückmeldung und den sichtbaren Nutzen für den Einzelnen und die Organisation.

Der jetzige zweite Teil zeigt, wie dieser Transfer gelingen kann: Awareness wird dann wirksam, wenn sie Teil der täglichen Routinen ist. Serious Games spielen dabei eine besondere Rolle: Sie schaffen Erlebnisse, in denen Menschen Entscheidungen treffen, Konsequenzen erfahren und ihr eigenes Verhalten reflektieren. Sie erzeugen Selbstwirksamkeit – und genau diese Erfahrung verändert Kultur.

Wenn Lernimpulse an reale Situationen andocken und durch Wiederholung, Dialog und Reflexion verstärkt werden, entsteht gelebte Sicherheitskultur: Sicherheit wird dann nicht erklärt, sondern selbstverständlich. ■

David Bothe war wissenschaftlicher Mitarbeiter mit dem Forschungsschwerpunkt Cybersecurity-Awareness und Serious Games am Institut für Internet-Sicherheit – if(is) der Westfälischen Hochschule in Gelsenkirchen und ist selbstständiger Berater für Security-Awareness und Serious Games sowie Inhabert des Cyberbüro Bothe.

Marcus Schaper ist Serious-Gaming-Enthusiast und Co-Founder der SBG Serious Business Gaming GmbH – er hat über 25 Jahre IT-Erfahrung als Programmierer bei Accenture, Strategieberater bei McKinsey sowie CIO bei RWE, innogy und E.ON gesammelt.

Norbert Pohlmann ist Professor für Cyber-Sicherheit und Leiter des if(is) an der Westfälischen Hochschule in Gelsenkirchen sowie Vorstandsvorsitzender des Bundesverbands IT-Sicherheit – TeleTrusT und im Vorstand des eco – Verband der Internetwirtschaft.

Literatur

[1] Marktplatz IT-Sicherheit, Serious Games – spielerisch Cybersicherheit vermitteln, Anbieterübersicht, fortlaufend, https://it-sicherheit.de/ratgeber/serious-games

[2] Jan Hense, Heinz Mandl, Learning in or with Games? Quality Criteria for Digital Learning Games from the Perspective of Learning, Emotion, and Motivation Theory, Januar 2012, www.researchgate.net/publication/303863429_Learning_in_or_with_games_Quality_criteria_for_digital_learning_games_from_the_perspectives_of_learning_emotion_and_motivation_theory

[3] European Union Agency for Cybersecurity – ENISA , Cybersecurity Culture Guidelines: Behavioural Aspects of Cybersecurity, Dezember 2018, ISBN 978-92-9204-267-7, online verfügbar via www.enisa.europa.eu/publications/cybersecurity-culture-guidelines-behavioural-aspects-of-cybersecurity

[4] Tienhua Wu, Kuang-You Tien, Wei-Chih Hsu, Fu-Hsiang Wen, Assessing the Effects of Gamification on Enhancing Information Security Awareness Knowledge, Applied Sciences Vol. 11(19), S. 9266, Oktober 2021, https://doi.org/10.3390/app11199266

[5] Georgia Zempila, Stelios Xinogalos, Investigating the role of serious games on raising students' awareness on safety and data protection on the Internet, Discover Education Vol. 4, Art. 268, August 2025, https://doi.org/10.1007/s44217-025-00722-0