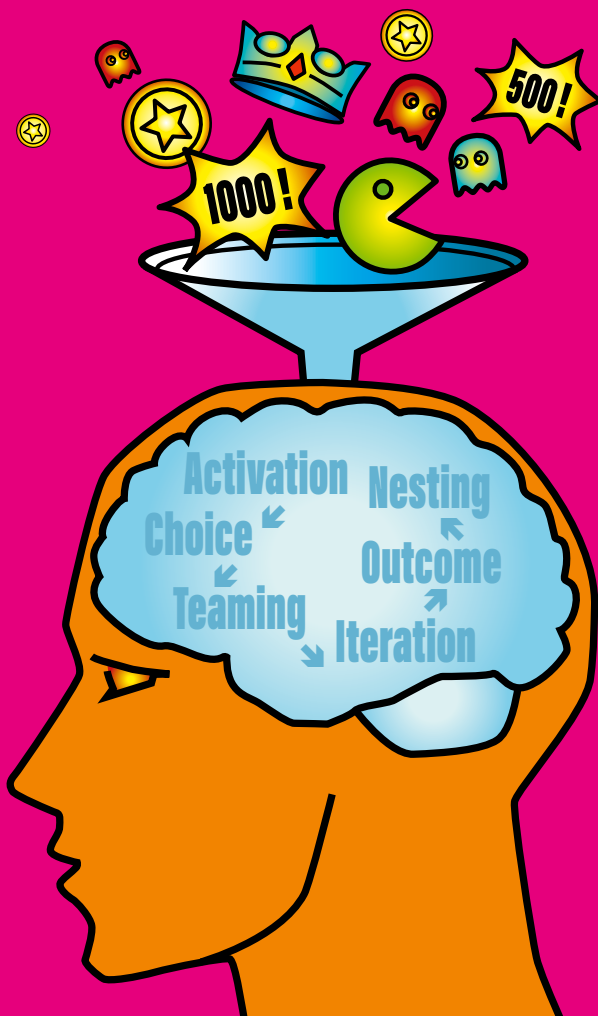




Spielend lernen für mehr Resilienz (1)

Serious Games als Lernmotor der Informations-Sicherheit – Teil 1: Vom Wissen zum Handeln

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 erste Teil richtet den Blick auf Erkenntnisse aus Neurowissenschaft, Psychologie, Pädagogik und Wirtschaftswissenschaften und fragt: Warum reicht Wissen allein nicht aus, um Verhalten zu verändern? Und wie können Serious Games dabei helfen, Awareness neu zu denken?

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

In den letzten Jahren hat die Gefahr der Destabilisierung von Unternehmen und Gesellschaften spürbar zugenommen – zahlreiche Cyberangriffe haben gezeigt, wie verletzlich unsere Institutionen sind. Cybersecurity und das Wissen darum sind damit längst nicht mehr nur technisches Thema, sondern eine zentrale Voraussetzung für die Funktionsfähigkeit von Wirtschaft, Verwaltung und Gesellschaft.

Die Dynamik neuer Technologie verschärft die Bedrohungslage weiter: Generative künstliche Intelligenz (KI) und Agent AI, Quantencomputing und maschinelles Lernen vergrößern nicht nur die Angriffsflächen, sondern erhöhen auch die Geschwindigkeit, mit der neue Risiken entstehen. Besonders sichtbar wird das beim Pretexting: KI erzeugt täuschend echte E-Mails, Profile oder Stimmen, die gezielt Vertrauen ausnutzen – umso wichtiger

bleiben Awareness und die Fähigkeit zur kritischen Bewertung von Kommunikation.

Parallel verändern gesellschaftliche Entwicklungen die Informationsumgebung: Social Media prägt Wahrnehmung und Kommunikation, Einsamkeit und Informationsüberflutung nehmen zu, Echokammern und Verschwörungserzählungen gewinnen an Einfluss – ein Umfeld, in dem Desinformation und Manipulation besonders leicht gedeihen.

Bei alledem steht der Mensch noch immer im Zentrum. Der menschliche Faktor (Human Factor) beschreibt die Wahrnehmungs-, Entscheidungs- und Handlungsmuster, die unser Verhalten im digitalen Alltag prägen. Und auch Informationssicherheit lässt sich nicht auf Firewalls oder Richtlinien reduzieren: Informationssicherheit

wird vielmehr im Zusammenspiel aus Technik, Organisation und menschlichem Verhalten verwirklicht.

Stand der Wissenschaft

Neurowissenschaft, Psychologie, Pädagogik und Wirtschaftswissenschaft zeigen heute deutlich, wie Menschen Informationen verarbeiten, Entscheidungen treffen und Verhalten verändern. Diese Perspektiven liefern konkrete Ansatzpunkte, um Awareness wirksamer zu gestalten – von den biologischen Grundlagen des Lernens über kognitive und emotionale Einflussfaktoren bis hin zu didaktischen Prinzipien und wirtschaftlichem Nutzen. Im Folgenden werden zentrale Erkenntnisse vorgestellt und Impulse untersucht, die für die Entwicklung wirksamer Awareness-Strategien vielversprechend sind.

Lernen beginnt im Gehirn (Neurologie)

Lernen findet dort statt, wo neue Verbindungen entstehen: im Gehirn. Wenn Menschen Neues aufnehmen, werden Signale zwischen Milliarden von Nervenzellen ausgetauscht und synaptische Netzwerke umgebaut. Neurowissenschaftliche Studien zeigen, dass die Art des Lernens beeinflusst, welche Hirnregionen aktiviert und wie stabil neue Gedächtnisspuren gebildet werden.

Lernen ist kein rein kognitiver, sondern ein multisensorischer Prozess. Je mehr Sinne beteiligt sind, desto stärker werden neuronale Verbindungen gebildet und gefestigt. Wenn wir etwas sehen, hören, bewegen oder selbst tun, werden gleichzeitig Wahrnehmung, Motorik, Emotion und das Belohnungssystem aktiv. Durch diese parallele Aktivierung entsteht ein dichtes Netz an Verknüpfungen, das Wissen stabiler und leichter abrufbar macht. Synapsen entstehen zudem nicht beim ersten Kontakt mit Information,

sondern erst, wenn das Gehirn Inhalte wiederholt verarbeitet und festigt.

Eine zentrale Rolle spielt das Belohnungssystem: Immer dann, wenn das Gehirn eine positive Abweichung zwischen Erwartung und Ergebnis erlebt, zum Beispiel wenn etwas besser gelingt oder interessanter ist als gedacht, wird Dopamin ausgeschüttet. Dieser Botenstoff verstärkt Aufmerksamkeit, Motivation und Gedächtnisbildung. In der Forschung wird dieser Mechanismus als Reward-Prediction-Error bezeichnet. Abbildung 1 versinnbildlicht, wie Dopamin das Lernen positiv beeinflusst.

Das Gehirn zielt übrigens nicht auf maximale Leistung, sondern auf Resilienz – also darauf, Energie zu sparen, Belastung zu vermeiden und unter wechselnden Bedingungen funktionsfähig zu bleiben. Lernen fordert das Gehirn heraus, diesen Energiesparmodus zu verlassen. Aber erst wenn etwas als relevant, bedeutsam oder lohnend erlebt wird, investiert das Gehirn zusätzliche Energie, um neue Verbindungen aufzubauen.

Motivation und Verhalten (Psychologie und Soziologie)

Lernen beginnt im Individuum. Ob wir uns auf etwas einlassen, hängt von drei psychologischen Grundbedürfnissen ab: Autonomie, Kompetenz und Zugehörigkeit. Wenn Menschen selbst entscheiden können und erleben, dass ihr Handeln Wirkung hat, entsteht Selbstwirksamkeit – der Kern jeder Verhaltensänderung. Ohne dieses Erleben bleibt Motivation theoretisch. Genau hier zeigt sich der „Intention-Action-Gap“: Menschen wissen zwar, was richtig wäre, tun es aber nicht.

Sobald Menschen gemeinsam lernen, wirken soziale Prozesse: Wir beobachten, spiegeln und übernehmen Verhalten. Die Lerntheo-

rie zeigt, dass bereits das Beobachten von Handlungen eine neuronale Aktivierung auslöst. Glaubwürdige und nahbare Vorbilder wirken deshalb stärker als abstrakte Anweisungen. Und Gruppendynamik schafft Resonanz: Häufig entsteht ein Impuls, sich anzuschließen – auch bekannt als „Fear of Missing Out“ (FOMO).

Damit Lernen nachhaltig wirkt, braucht es Wiederholung und Anwendung. Die Vergessenskurve nach Ebbinghaus [1] verdeutlicht, dass Wissen schnell verblasst, wenn es nicht aktiviert wird (siehe Abb. 2). Erst durch Tun und erneutes Abrufen werden neuronale Verbindungen stabil. Erfolgserlebnisse verstärken diesen Prozess: Sie lösen Freude aus, stärken das Kompetenzgefühl und erhöhen die Bereitschaft, weiterzugehen. Ebenso wichtig ist Reflexion: Das Erkennen und Korrigieren von Denkfehlern (Debiasing) ermöglicht es, Verhalten gezielt anzupassen.

Lernen gestalten und steuern (Pädagogik)

Wie lässt sich Lernen so gestalten, dass es nicht nur Wissen vermittelt, sondern Verhalten verändert? Die pädagogische Forschung betont zwei zentrale Elemente wirksamer Lernprozesse: Übung und Feedback. Erst durch wiederholtes Anwenden und gezielte Rückmeldung wird Wissen in Handlung übersetzt. Menschen lernen nicht al-

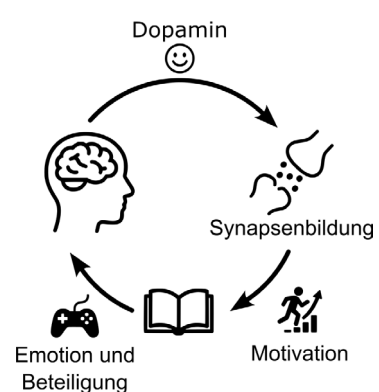


Abbildung 1: Wird der Lernstoff interessant, bilden sich dank Dopamin neue Synapsen – das Lernen macht Spaß, die Motivation steigt.

lein durch Informationen, sondern durch Erfahrung – durch Ausprobieren, Scheitern, Korrigieren und erneutes Versuchen.

Lernziele müssen dabei realistisch bleiben! Awareness-Trainings sollen keine Sicherheitsexperten* ausbilden, sondern alltägliches Verhalten prägen. Ziel ist es, Risiken bewusst wahrzunehmen, Bedrohungen zu erkennen und angemessen zu reagieren. Formate, die diese Kompetenzentwicklung fördern, sind praxisnah, szenisch und handlungsorientiert aufgebaut.

Entscheidend ist, dass Teilnehmer Situationen erleben, die sie selbst betreffen, dass sie eigenes Verhalten erproben und unmittelbares Feedback erhalten. Lernen wird dann nicht gesteuert, sondern angeregt – als Prozess, der Einsicht, Motivation und Erfahrung miteinander verbindet.

Der Wert des Lernens (Wirtschaftswissenschaften)

Unternehmen, die in Wissen und Sicherheitsbewusstsein investieren, erhöhen ihre Stabilität und tragen zugleich zu einer widerstandsfähigeren Wirtschaft bei. Informationssicherheit wird dann nicht als isoliertes Ziel verstanden, sondern als gemeinsame Verantwortung.

Aus betriebswirtschaftlicher Sicht ist Awareness eine Investition: Sie reduziert Risiken, verhindert Fehlhandlungen und spart Kosten. Prävention kostet schließlich nur ei-

nen Bruchteil dessen, was ein Sicherheitsvorfall verursacht.

Volkswirtschaftlich stärkt Awareness die Resilienz ganzer Wertschöpfungsketten und senkt Folgekosten aufgrund von Produktionsausfällen oder Reputationschäden. Unternehmen reduzieren Vorfälle – die Volkswirtschaft profitiert.

Ein wichtiger Faktor ist dabei die Skalierbarkeit: Digitale Formate erreichen große Zielgruppen, lassen sich aktualisieren und an neue Bedrohungen anpassen. Lernen wird damit doppelt wirksam: Es stärkt individuelle Kompetenz und erhöht den wirtschaftlichen Nutzen von Sicherheit.

Awareness ist damit keine Pflicht, sondern wird zur strategischen Wertschöpfung.

Zwischenfazit: Die drei Triebfedern des Lernens

Aus der wissenschaftlichen Betrachtung wird deutlich, dass nachhaltiges Lernen nicht durch Information entsteht, sondern durch Wiederholung, Emotion und soziale Bestätigung. Diese drei Elemente wirken wie Verstärker – sie entscheiden, ob Wissen im Gehirn ankommt, verankert wird und später zu (verändertem) Verhalten führt.

Wiederholung: Durch wiederholtes Anwenden entstehen stabile neuronale Verbindungen – Wissen

wird langfristig abrufbar. Entscheidend ist, dass Wiederholung nicht eintönig wird. Daher muss man sie mit Variation und Überraschung kombinieren. Auch Spaß ist wichtig: Wenn Lernen Freude macht, wird Dopamin ausgeschüttet – der biochemische Antrieb für Aufmerksamkeit, Motivation und Gedächtnisbildung.

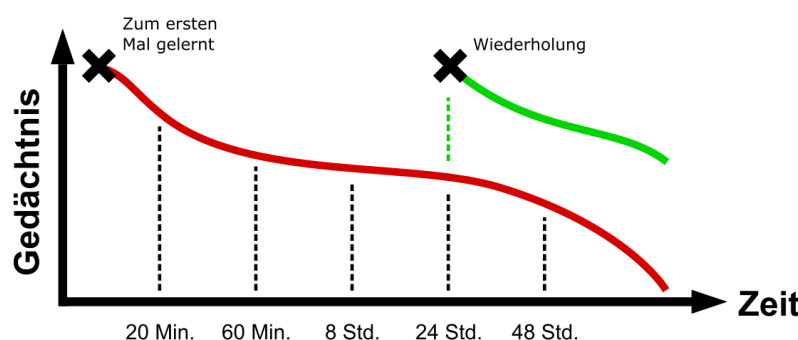
Emotion: Erlebte Emotionen markieren Inhalte als „wichtig“. Positive Anspannung, kleine Erfolgserlebnisse und Überraschungen fördern die Gedächtnisbildung – Angst oder Druck blockieren hingegen die kognitive Verarbeitung.

Soziale Bestätigung: Menschen lernen im sozialen Kontext. Verhalten wird stabil, wenn es im Team sichtbar, bestätigt oder nachgeahmt wird. Sogenannte Spiegelneuronen sorgen dafür, dass allein das Beobachten von Verhalten schon Lernprozesse auslöst: „Monkey see, monkey do.“ Gemeinsames Gelingen stärkt überdies nicht nur das Lernen, sondern auch die Resilienz eines Teams.

Die erste Hälfte dieses Beitrags hat den wissenschaftlichen Blick Schritt für Schritt erweitert: vom Gehirn des Einzelnen und der Frage, wie Wissen verankert wird, über selbstwirksames Verhalten und gruppenspezifische Prozesse bis hin zu pädagogischen Erkenntnissen, die zeigen, wie Lernen gestaltet sein muss, um Verhalten tatsächlich zu verändern. Dabei wurde deutlich, dass wirksame Awareness nicht nur dem einzelnen Unternehmen nutzt, sondern auch gesamtwirtschaftliche Resilienz stärkt.

Mehr A.C.T.I.O.N.

Auf Basis dieser wissenschaftlichen Erkenntnisse lassen sich die nachfolgend erläuterten Gestaltungsprinzipien für wirksame Awareness formulieren (siehe auch



Tab. 1). Überdies erfolgt eine kritische Würdigung, wie gut klassische Formate aus Schule, Unternehmen und Behörden diesen Prinzipien gerecht werden.

Wissen allein verändert kein Verhalten

Das Schlüsselproblem ist bekannt: Menschen wissen oft, was sie tun sollten, handeln aber nicht danach. Sie verwenden etwa unsichere Passwörter, klicken auf verdächtige Links oder ignorieren Sicherheitsrichtlinien, obwohl ihnen die Risiken bewusst sind. Dieser Abstand zwischen Einsicht und Handlung ist kein Zeichen von Unwissenheit, sondern ein typisches Merkmal menschlichen Verhaltens.

In der Praxis dominieren nach wie vor Lernformate, die Wissen prüfen, statt Verhalten zu fördern. E-Learnings oder standardisierte Präsenzs Schulungen sind leicht umzusetzen und erfüllen organisatorische Anforderungen, bleiben jedoch oberflächlich: Sie adressieren das Was, aber nicht das Wie.

Auch Phishing-Simulationen, ursprünglich als praxisnahe Tests gedacht, haben daher nur begrenzten Nutzen: Sie erzeugen kurzfristige Aufmerksamkeit, führen aber häufig auch zu Stress, Scham oder Misstrauen. Der Fokus auf Kontrolle statt Befähigung schwächt das Vertrauen und mindert die intrinsische Motivation. Eine aktuelle Studie in einem US-Gesundheitsunternehmen hat gezeigt, dass selbst umfangreiche Phishing-Simulationen nur minimal dazu beitragen, Menschen von heiklen Aktivitäten abzuhalten (siehe [9]): „Selbst umfangreiche Phishing-Simulationen senken die Klickrate im Durchschnitt um gerade einmal 1,7 %.“

Wirksame Awareness entsteht nur, wenn entsprechende Maßnahmen Erkenntnisse aus Neurowissenschaft, Psychologie, Pädagogik und Wirtschaft berücksichtigen. Daraus leiten die Autoren sechs Gestaltungsprinzipien ab (Tab. 1), die sie als A.C.T.I.O.N.-Modell bezeichnen: Lernen entfaltet erst dann sein Potenzial, wenn *Activation*, *Choice*, *Teaming*, *Iteration*, *Outcome* und *Nesting* zusammenwirken.

Klassische Awareness auf dem Prüfstand

Viele Organisationen setzen auf Standardformate wie Phishing-Simulationen, E-Learnings und Präsenzs Schulungen. Doch inwiefern erfüllen diese die Anforderungen wirksamen Lernens – und damit die sechs Prinzipien des A.C.T.I.O.N.-Modells?

Phishing-Simulationen erzeugen kurzfristige Aktivierung: Sie überraschen und erzeugen Aufmerksamkeit.

Doch sie tragen kaum zur Selbstwirksamkeit (*Choice*) bei: Mitarbeiter treffen zwar eine Entscheidung (klicken oder nicht), erhalten aber selten konstruktives Feedback oder die Möglichkeit, ihr Verhalten zu üben. Resonanz (*Teaming*) fehlt ebenfalls häufig – das Szenario bleibt isoliert, ohne Austausch oder Vorbilder. So entsteht kaum Lernwirkung (*Outcome*) und ohne zusätzliche Verankerung (*Nesting*) verpufft der Effekt nach der Kampagne sehr schnell.

E-Learnings sind zwar skalierbar und effizient, doch aus Sicht von A.C.T.I.O.N. bleiben sie an der Oberfläche: Sie informieren, aber sie aktivieren nicht. Teilnehmer konsumieren Inhalte, ohne *Choice* oder *Iteration* – keine Entscheidungen, kein echtes Ausprobieren. Resonanz fehlt, weil Lernen nicht gemeinsam stattfindet. Zusammengefasst sind E-Learnings womöglich wirtschaftlich sinnvoll, aber pädagogisch unzureichend.

Präsenzs Schulungen schaffen immerhin *Teaming*: Menschen begegnen sich, diskutieren Fälle und entwickeln gemeinsames Verständnis. Doch es bleibt meist bei Worten: Es fehlt an Aktivierung, *Iteration* und *Outcome*. Ohne Übungssituation entsteht keine Selbstwirksamkeit und ohne Verankerung hat das Gelernte im Alltag keinen Bestand.

Prinzip	Ursprung	Leitfragen
Activation (Aktivierung)	Neurowissenschaft, Psychologie	Erzeugt das Format Aufmerksamkeit und emotionale Aktivierung? Werden mehrere Sinne angesprochen?
Choice (Selbstwirksamkeit)	Psychologie	Treffen Teilnehmer echte Entscheidungen und erleben deren Wirkung? Gibt es Feedback und Erfolgserlebnisse?
Teaming (Resonanz)	Psychologie, Soziologie	Erkennen sich Mitarbeiter in den Szenarien wieder? Gibt es Austausch, Teaminteraktion oder Vorbilder?
Iteration (Erfahrung)	Pädagogik, Didaktik	Können Teilnehmer handeln, ausprobieren, scheitern und wiederholen?
Outcome (Nutzen)	Wirtschaftswissenschaft, Betriebswirtschaft	Trägt das Format messbar zur Reduktion von Fehlverhalten oder Vorfällen bei? Ist der Aufwand angemessen? Lässt sich das Format skalieren?
Nesting (Verankerung, Nachhaltigkeit)	Psychologie, Pädagogik, Wirtschaftswissenschaft, Volkswirtschaft	Lässt sich die Maßnahme in bestehende Prozesse integrieren und dauerhaft wiederholen? Kann sie auf einer Plattform betrieben oder auf andere Weise multipliziert werden?

Tabelle 1:
A.C.T.I.O.N.-Grundprinzipien wirksamer Awareness

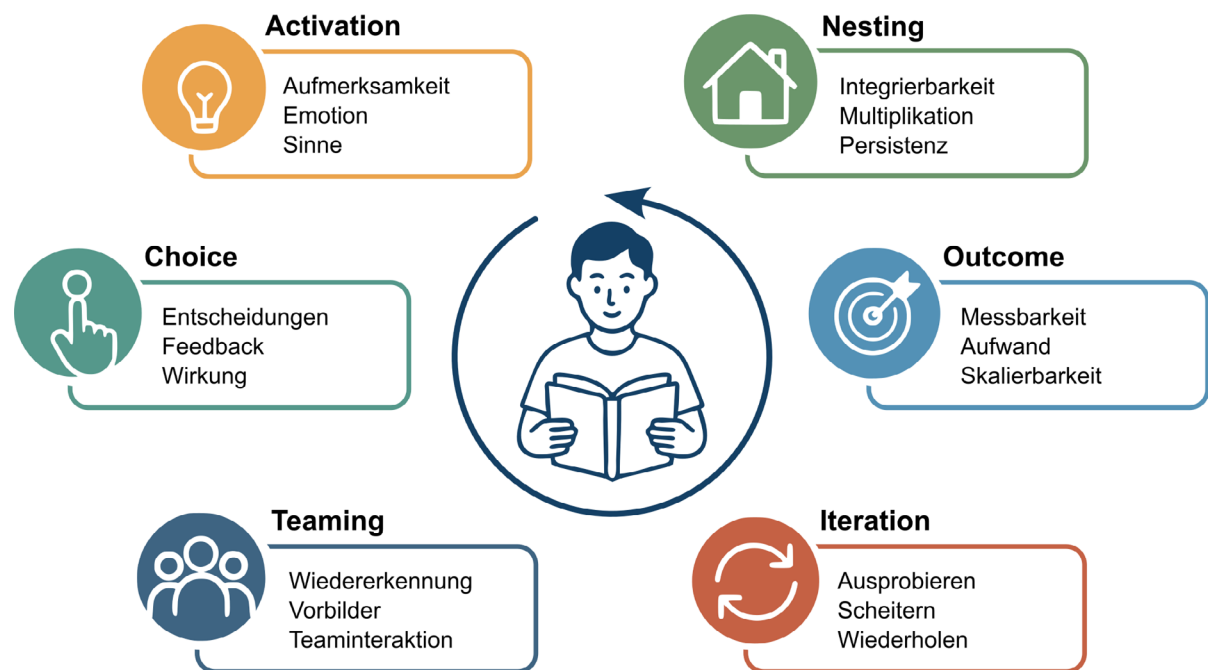


Abbildung 3: Nur wenn Leitmotive ausreichend bedient werden, kann Awareness langfristig Verhalten ändern.

Gemeinsam ist allen drei Formaten: Sie schaffen – zumindest eine Zeit lang – Wissen, ändern aber kaum Verhaltensweisen. Sie erfüllen organisatorische Anforderungen, aber nicht die Prinzipien wirksamen Lernens.

Spielerische Wege – Serious Games

Wenn Wissen allein Verhalten nicht verändert, braucht es ergo andere Lernformen, die Menschen aktiv einbeziehen: Wirksam wird Lernen dort, wo Menschen handeln – nicht nur verstehen. Formate, die Emotion auslösen, Entscheidungen ermöglichen und soziale Bestätigung erzeugen, schaffen Erlebnisse, die im Gedächtnis bleiben.

Klassische Schulungen vermitteln Informationen, erzeugen aber weder Beteiligung noch Selbstwirksamkeit – sie prüfen Wissen, anstatt Verhalten zu verändern. Das Ergebnis: Risiken bleiben bestehen, obwohl Wissen vorhanden ist.

Erfahrungsorientiertes Lernen setzt genau hier an: Menschen treffen Entscheidungen, erleben deren Wirkung und reflektieren ihr Vorgehen. Überraschung, Herausforderung und unmittelbares Feedback aktivieren das Belohnungssystem – Lernen wird wirksam verankert statt einfach nur „abgelegt“.

„79 % lernten durch das Spiel Neues, 84 % fühlten sich durch die Story engagiert, 68 % hatten Spaß – und 84 % würden es weiterempfehlen“, hat etwa eine

Studie ermittelt, für die das Lernspiel „CyberHero“ entwickelt wurde [10].

Serious Games sind Spiele mit einem klar definierten Lern- oder Trainingsziel. Sie verbinden Wahrnehmung, Emotion und Handlung zu einem gemeinsamen Lernraum: Teams probieren aus, scheitern und lernen gemeinsam – ohne reale Konsequenzen. Dadurch entsteht Kompetenz, die sich messbar auf den Arbeitsalltag übertragen lässt.

Wie Serious Games die Elemente des A.C.T.I.O.N.-Modells abbilden, ist Inhalt des zweiten Teils dieser Artikelserie, der in der nächsten Ausgabe der <kes> erscheint.

Fazit

Awareness ist kein Format, sondern ein Prozess: Wirksam wird sie nicht durch einmalige Schulungen, sondern durch die Verbindung von Wissen, Erfahrung und gelebten Strukturen. Forschungsergebnisse aus Neurowissenschaft, Psychologie, Pädagogik und Wirtschaft zeigen: Nachhaltiges Lernen entsteht dort, wo Menschen handeln, reflektieren und Rückmeldung erhalten – dort, wo Sicherheit *erlebt*, statt nur „verstanden“ wird.

Serious Games schaffen genau solche Lernräume. Sie übersetzen Regeln in Entscheidungen, ermöglichen Fehler ohne Risiko und stärken Selbstwirksamkeit. Doch ohne strukturelle Verankerung bleiben auch sie Moment-

aufnahmen. **Sicherheitskultur** entsteht erst dann, wenn Lernerlebnisse in Prozesse und Routinen übergehen. Informationssicherheit wandelt sich dann von einer Pflicht zum gemeinsamen Lern- und Verbesserungsprozess. ■

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

Der zweite Teil dieser Reihe erscheint in <kes> 2026^{#1} und zeigt, wie sich Serious Games unter den sechs A.C.T.I.O.N.-Prinzipien bewähren, wie sie sich in den Alltag von Organisationen integrieren lassen und warum aus individuellem Handeln erst durch Kultur echte Sicherheit entsteht.

Literatur

[1] Hermann Ebbinghaus, Über das Gedächtnis, Untersuchungen zur experimentellen Psychologie, Dunker & Humblot, 1885, online verfügbar auf www.deutschestextarchiv.de/book/show/ebbinghaus_gedaechtnis_1885

[2] Albert Bandura, Social learning theory, Prentice-Hall, September 1977, ISBN 978-0-13-816744-8

[3] David A. Kolb, Experiential learning, Experience as the source of learning and development, Prentice-Hall, 1984, ISBN 978-0-13-295261-3, online verfügbar auf www.researchgate.net/publication/235701029_Experiential_Learning_Experience_As_The_Source_Of_Learning_And_Development

[4] Edward L. Deci, Richard M. Ryan, Intrinsic Motivation and Self-Determination in Human Behavior, Plenum Press, August 1985, ISBN 978-0-306-42022-1, <https://doi.org/10.1007/978-1-4899-2271-7> (kostenpflichtig)

[5] Paschal Sheeran, Intention–Behavior Relations: A Conceptual and Empirical Review, European Review of Social Psychology Vol. 12 (1), 2002, S. 1, <https://doi.org/10.1080/14792772143000003> (kostenpflichtig), Alternativversion online verfügbar auf www.researchgate.net/publication/279613604_Intention-Behavior_Relations_A_Conceptual_and_Empirical_Review

[6] Paul Howard-Jones, Tim Jay, Reward, learning and games, Current Opinion in Behavioral Sciences Vol. 10 (1), S. 65, <https://doi.org/10.1016/j.cobeha.2016.04.015> (kostenpflichtig), Peer-Review-Version online verfügbar auf [https://research-information.bris.](https://research-information.bris.ac.uk/ws/portalfiles/portal/102521125/Games_DA_Education_Revise_v7_.pdf)

[ac.uk/ws/portalfiles/portal/102521125/Games_DA_Education_Revise_v7_.pdf](https://research-information.bris.ac.uk/ws/portalfiles/portal/102521125/Games_DA_Education_Revise_v7_.pdf)

[7] Wolfram Schultz, Dopamine reward prediction error coding, Dialogues in Clinical Neuroscience Vol. 18 (1), März 2016, S. 23, <https://doi.org/10.31887/DCNS.2016.18.1/wschultz> (kostenpflichtig), online verfügbar auf www.researchgate.net/publication/302578615_Dopamine_reward_prediction_error_coding

[8] Lina Brunken, Annalina Buckmann, Jonas Hiel-scher, and M. Angela Sasse, „To do this properly, you need more resources“: The Hidden Costs of Introducing Simulated Phishing Campaigns, in: Proceedings of the 32nd USENIX Conference on Security Symposium, 2023, ISBN 978-1-939133-37-3, online verfügbar auf www.usenix.org/conference/usenixsecurity23/presentation/brunken

[9] Grant Ho, Ariana Mirian, Elisa Luo, Khang Tong, Euyhyun Lee, Lin Liu, Christopher A. Longhurst, Christian Dameff, Stefan Savage, Geoffrey M. Voelker, Understanding the Efficacy of Phishing Training in Practice, in: Proceedings of the 2025 IEEE Symposium on Security and Privacy, Mai 2025, ISBN 979-8-3315-2237-7, online verfügbar auf www.researchgate.net/publication/392739544_Understanding_the_Efficacy_of_Phishing_Training_in_Practice

[10] Rania Hodhod, Harlie Hardage, Safia Abbas, Eman Abdullah Aldakheel, CyberHero: An Adaptive Serious Game to Promote Cybersecurity Awareness, Electronics Vol. 12 (17), August 2023, S. 3544, <https://doi.org/10.3390/electronics12173544>



Die Zeitschrift für
Informations-Sicherheit

Mehr wissen mit <kes>+

Sichern Sie sich Ihren Wissensvorsprung
in der Informationssicherheit!

- Fachzeitschrift <kes> inkl. Specials 6x jährlich per Post und digital.
- Zugang zu aktuellen Online-Fachartikeln und Studien sowie zu dem kompletten Online-Archiv.
- Exklusiver Zugriff auf über zwanzig neue Online-Premium-Artikel pro Monat sowie auf aktuelle Videos und Webinaraufzeichnungen.
- 10 % Rabatt auf DATAKONTEXT-Online-Schulungen im Bereich Informationssicherheit.
- nur 207,- € im Jahr (inkl. Mwst. und Inlandsversand)



Jetzt 30 Tage kostenfrei testen:
www.kes-informationssicherheit.de

