

SERIOUS BUSINESS GAMING QUARTERLY

 **MANAGEMENT**

 **SCIENCE**

 **TECHNOLOGY**

Issue 01 · Feb 2026

Mehr **A.C.T.I.O.N.** für Ihre Awareness- Strategie

Wie Serious Business Gaming
Lernen, Verhalten und Resilienz
wirksam verbessert



SPECIAL zu Cybersecurity-Awareness

Mehr A.C.T.I.O.N. für Ihre Awareness-Strategie

Was Verhalten beeinflusst und wie Serious Gaming hilft

Cybersecurity ist heute Voraussetzung für die Funktionsfähigkeit von Wirtschaft, Verwaltung und Gesellschaft. Gleichzeitig wachsen Angriffsfläche und Tempo – etwa durch generative KI, die Pretexting mit täuschend echten Mails, Profilen oder Stimmen skaliert. In diesem Umfeld entscheidet der Humanfaktor: Informationssicherheit entsteht im Zusammenspiel von Technik und menschlichem Verhalten.

Was sagt die Forschung – vom kleinen Beobachtungsgegenstand (Gehirn, Kognitionswissenschaften) zum großen (Organisation, Betriebs- und Volkswirtschaft)? Vier Perspektiven ergeben ein klares Bild.

Was Verhalten tatsächlich beeinflusst

Neurowissenschaft: Lernen wird stabil, wenn mehrere Sinne beteiligt sind und Inhalte wiederholt aktiviert werden. Motivation steigt, wenn Lernen als relevant und „lohnend“ erlebt wird.

Psychologie/Soziologie: Autonomie, Kompetenz und Zugehörigkeit fördern Selbstwirksamkeit. Ohne sie bleibt der Intention-Action-Gap: Menschen wissen, was richtig wäre, handeln aber nicht entsprechend. Teamdynamik und Vorbilder verstärken ebenfalls gewünschtes Verhalten.

Pädagogik: Übung und Feedback sind entscheidend. Verhalten entsteht durch Ausprobieren, Scheitern, Korrigieren und erneutes Versuchen – nicht durch Informationskonsum.



Wirtschaftswissenschaften: Awareness ist eine Investition. Prävention kostet nur einen Bruchteil dessen, was Incidents und Folgeschäden verursachen; Skalierbarkeit und Aktualisierbarkeit entscheiden über Wirkung.

Warum greifen Standardformate oft zu kurz? E-Learnings informieren, aber aktivieren selten. Phishing-Simulationen erzeugen Aufmerksamkeit, können jedoch Stress oder Misstrauen auslösen – und die Wirkung bleibt begrenzt. →

Selbst umfangreiche Phishing-Simulationen senken die Klickrate im Durchschnitt um gerade einmal 1,7%. [Grant Ho et al, 2025]

Mehr Wirkung entsteht, wenn Awareness als Erfahrungsraum gestaltet wird. Dafür haben wir das **A.C.T.I.O.N.-Framework** entwickelt – sechs Prinzipien, die Wissenschaft und Praxis verbinden:

Activation – Awareness beginnt mit Aufmerksamkeit: Lernen wirkt nur, wenn Menschen emotional aktiviert sind und Relevanz erleben.

Choice – Verhalten ändert sich, wenn Entscheidungen echte Konsequenzen haben – Selbstwirksamkeit wirkt.

Teaming – Menschen lernen sozial: Austausch, Vorbilder und gemeinsame Entscheidungen stärken Wirkung und Verankerung.

Iteration – Nachhaltiges Lernen entsteht durch Wiederholung, Ausprobieren und Korrigieren – nicht durch Einmal-Infos.

Outcome – Awareness muss messbaren Nutzen stiften: weniger Fehlverhalten, geringere Risiken und höhere Resilienz.

Nesting – Erst die Integration in Routinen und Unternehmenskultur macht Awareness dauerhaft wirksam und skalierbar.

Wendet man diese Kriterien auf die klassischen Trainingsformate an, ergeben sich deutliche Unterschiede bei der Erfüllung der obigen Kriterien.

Klassische Formate wie Web-Based-Trainings oder Frontalunterricht vermitteln Wissen – sie verändern jedoch selten Verhalten. Sie bleiben abstrakt und passiv.

Hohe Wirksamkeit von Serious Gaming

Serious Games setzen genau dort an, wo Lernen wirksam wird: in Entscheidungs-

situationen unter Zeitdruck und Unsicherheit. Sie aktivieren Emotionen, erzwingen Wahlmöglichkeiten, machen Konsequenzen erlebbar und ermöglichen Lernen im Team. Fehler sind Teil des Prozesses, nicht Anlass zur Sanktion. So entsteht Selbstwirksamkeit statt Pflichterfüllung – und Awareness wird von Information zu gelebter Handlung.



In wissenschaftlichen Experimenten konnte effektive Wissensvermittlung, kombiniert mit hoher Lern- und Spielmotivation nachgewiesen werden:

Studierende erzielten nach dem Lernen mit einem Serious Game (60,1 Punkte) bessere Ergebnisse als die Kontrollgruppe (52,6 P.). Das Serious Game wurde als deutlich motivierender bewertet und führte zu einer dreimal längeren freiwilligen Lernzeit (3h statt 1h). [Dankbaar et al, 2017]

Was aber auch klar ist: Serious Games können nur ein Baustein einer wirkstarken Awareness-Strategie sein; es bedarf der Verankerung in Unternehmensstrategie und -kultur. Sofern das gelingt, kann sich Cybersecurity-Resilienz von einem Kostenfaktor zu einem strategischen Wettbewerbsvorteil entwickeln.

Management-Praxis

So verbessern Sie Ihren Awareness-Reifegrad

Sie wollen wissen, wie viel **A.C.T.I.O.N.** Ihre Awareness-Strategie enthält und wo sich noch etwas herausholen lässt? So funktioniert's: Markieren Sie, wo Sie sich am ehesten wiederfinden und vergleichen Sie es mit den Sollprofilen für Ihre Branche.

	Level 1 Ad-hoc	Level 2 Reaktiv	Level 3 Strukturiert	Level 4 Gesteuert	Level 5 Exzellent
Activation	Reine Pflichtkommunikation; informativ, aber emotionslos	...	Punktuelle Aktivierung durch Zielgruppen-Formate	...	Kontinuierliche Relevanz; tief im Geschäftsalltag verankert
Choice	Starre Regeln ohne Handlungsspielraum	...	Entscheidungs-Szenarien mit Feedback-Schleifen	...	Freiräume für sicheres Handeln; klare Zielorientierung
Teaming	Lernen ist individuell und isoliert	...	Teamformate existieren, aber ohne feste Logik	...	Soziale Verankerung; Awareness ist Team-Kultur
Iteration	Einmal-Maßnahmen; kein Lerneffekt	...	Wiederholung erfolgt, aber ohne Anpassung	...	Festes Trainingselement; stetige Weiterentwickl.
Outcome	Erfolg wird nicht gemessen	...	Messung via Kennzahlen und Indikatoren	...	Direkter Impact auf Resilienz und Unternehmensziele
Nesting	Isoliertes Inselthema im Tagesgeschäft	...	Teilweise Einbettung in Kampagnen	...	Volle Integration in Strategie, Prozesse und Führung

In welcher Branche ist Ihr Unternehmen tätig? Bei mehreren Tätigkeitsfeldern wählen Sie die Branche mit der höchsten Sicherheitsstufe (S).

S5 Hochkritisch: Militär, Nachrichtendienste, nationale Sicherheit → L5

S4 Kritisch: KRITIS (Versorger, Verkehr, HealthCare, Finanzinfrastruktur) → L4/5

S3 Reguliert: Finanzdienstleistungen, Chemie & Pharma, Luftfahrt, Hightech → L4

S2 Relevant: Maschinenbau, Dienstleister, Handel, Technologie (sonstige) → L3

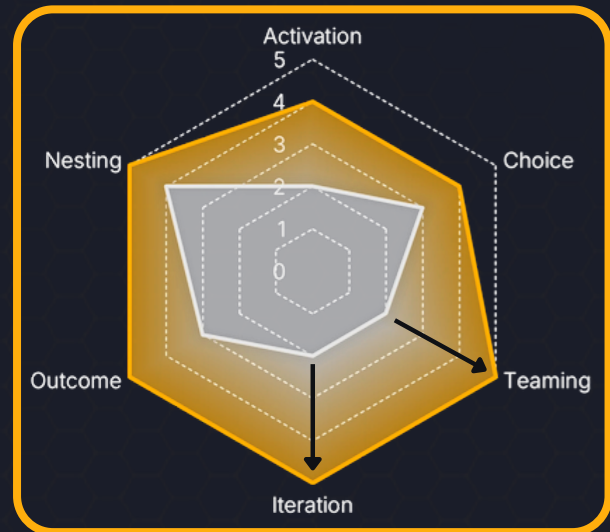
S1 Andere: Bildung, Kommunen, NGO → L2/3

Nun können Sie den Reifegrad Ihres Unternehmens mit dem Branchen-Sollwerten vergleichen und die Handlungsfelder ableiten. →

In diesem Beispiel ist ein hohes Sicherheitsniveau gefragt, um die Anforderungen an die kritische Infrastruktur (KRITIS) zu erfüllen.

Man sieht deutlich, dass in den Bereichen Iteration und Teaming die größten Handlungsbedarfe bestehen (siehe Pfeile rechts), da die Pflichtschulungen nur jährlich und individuell statt im Team stattfinden.

Es empfiehlt sich daher, die bestehende Awareness-Strategie um Elemente zu erweitern, die mehr Teamdynamik nutzen und auch gut unterjährig durchgeführt werden können. **Serious Gaming** ist hier nur eine Möglichkeit von vielen. Auch Treffen von Nutzergruppen, in denen Krisensimula-



tionen oder Rollenspiele genutzt werden, können sehr wirksam sein. Wichtig ist, eine gute Balance aller Dimensionen zu finden.

Management-Playbook für die Umsetzung

Sobald die Prioritäten feststehen, kann es ohne Umschweife an die Umsetzung gehen. Worauf es dabei wirklich ankommt, sagt dieses **Management-Playbook**, damit aus

den Handlungsfeldern wirksame Veränderung und eine spürbare und nachhaltige Verbesserung der Resilienz entstehen kann.

01 Sinn stiften

Hinter jedem Projekt muss ein wirkketten-gestützter Zweck stehen, den nicht nur das Management, sondern jeder versteht.

03 Kultur nutzen

Nutzen Sie Strategemaßnahmen, die die Awareness unterstützen, und kulturelle Eigenschaften Ihrer Organisation, um die Awareness auf Teamebene wirken zu lassen.

02 Vorbild sein

Leben Sie A.C.T.I.O.N. vor – z.B. Teaming, indem Sie eine Handvoll Meinungsführer aus der Organisation in ein Team „Awareness-Booster“ holen.

04 Fokus halten

Wählen Sie maximal zwei Hebel aus. Mehr Fokus bringt auch mehr nachhaltige Veränderung. Ausnahme: Falls Sie noch keine Awareness-Strategie haben.

Sie möchten das Tool nutzen oder Ihre Awareness-Strategie mit Experten diskutie-

ren? Sprechen Sie mit uns auf LinkedIn oder über info@sbg-gaming.com.

Neues von **What the Hack!**

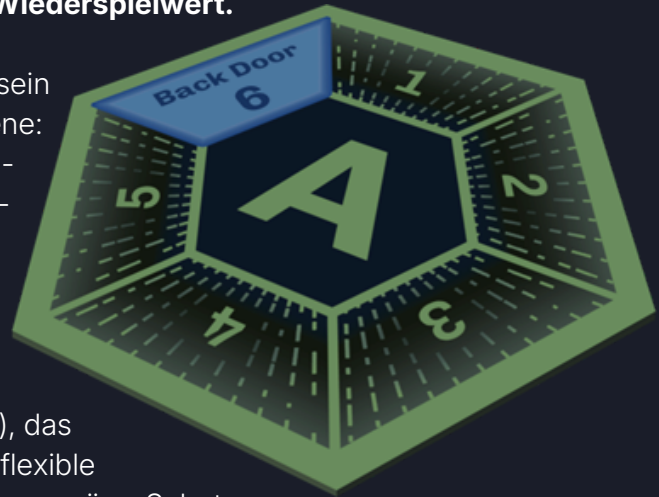
Was sich lohnt auszuprobieren

Token Actions. Mehr taktische Tiefe. Mehr Wiederspielwert.

Mit **Token Actions** erweitert **What the Hack!** sein Spielprinzip um eine zusätzliche taktische Ebene: Teams können gesammelte Tokens gezielt einsetzen, um den Spielverlauf aktiv zu beeinflussen. Bestimmte Felder auf dem Spielbrett ermöglichen spezielle Aktionen, die sofort wirksam werden – bewusst gewählt, situativ eingesetzt und gemeinsam entschieden.

Ob ein schneller Positionswechsel (Back Door), das Zurückdrängen des Hackers (Push Back), der flexible Tausch von Ressourcen (Exchange) oder ein temporärer Schutzraum (Safe Space): Token Actions machen Entscheidungen spürbar.

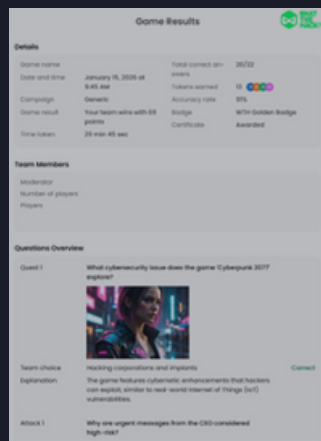
Warum das wichtig ist. Token Actions erhöhen den **Wiederspielwert** deutlich und stärken genau jene Lernmechanismen, die wirksame Awareness ausmachen: Selbstwirksamkeit, Iteration und Teamentscheidungen unter Unsicherheit.



Game Results

machen Lernwirkung messbar: Der neue Spielbericht zeigt Entscheidungen und Lernerfahrungen eines Teams. So entsteht aus dem Spielerlebnis die Basis für Reflexion, Steuerung und Reporting.

Jetzt nach jedem Spiel auf Deutsch und Englisch verfügbar.



Drei neue Kampagnen für neue

Lernimpulse.

Ideal geeignet für mehr Activation und Iteration.

Märchen-Hacks fordern Ihre Literaturkenntnisse heraus, Phishing zeigt die neuesten Tricks der Hacker, die auch bei den Neuen Hacks Q1 die Hauptrolle spielen.



+++ **News-Ticker** +++ ISO 27001 Kampagne für Experten und solche, die es werden wollen
 +++ Wer's wissen will: WTH-Erklärvideo in 90 Sekunden auf Vimeo +++ Einfachere Navigation für Moderatoren: Wechsel zwischen Admin und Game-Seite, Pause durch Leertaste steuern +++ Präzise Zeitsteuerung für Fragen bei eigenen Kampagnen +++

Führung trifft Risiko (aka NIS-2)

Ein Executive-Crashkurs zu Governance, Recht und Resilienz, aber ohne Technikwust

Geopolitische Spannungen und KI-gestützte Angriffe verschärfen die Bedrohungslage rasant, nicht nur für die IT, sondern ganze Geschäftsmodelle – bis hin zur Haftung des Managements. **NIS-2 macht Cybersicherheit zur Vorstandsaufgabe.**

Viele Führungskräfte sind allerdings unsicher: „Was muss ich jetzt wissen und tun?“ Genau dafür haben wir diese Kam-

pagne entwickelt, in der innerhalb von 30 Minuten alle wesentlichen Themen angesprochen werden

Wie Sie die neue Kampagne am wirkungsvollsten in Ihrem Unternehmen einsetzen, hängt stark von Strategie und Kultur ab. Hier eine kleine Einordnung. Unsere Empfehlung ist klar: organisieren Sie einen **Leadership-Workshop.**

 Sehr gut 	 Gut 	 Exzellent 	 Gut 
Schulung u. Standort-Bestimmung	Teil der Führungskräfte-Compliance	Auflockerung und Reflexion	Wettbewerb und Benchmark

Zweck. Führungskräfte befähigen, Cybersecurity als Geschäftstreiber zu steuern: Bewerten, entscheiden, priorisieren, und dadurch letztlich Haftung reduzieren

Schwierigkeit.     

Kernthemen (Auswahl):

Ganzheitliche Governance: Strategische Verankerung von Cybersicherheit als Geschäftsrisiko

Methodisches Risikomanagement:

Systematische Identifikation von Assets und Schwachstellen sowie Priorisierung von Maßnahmen

Betriebliche Resilienz: Fokus auf Business Continuity und Incident Management zur Sicherung kritischer Produkte, Dienstleistungen und Lieferketten

Strategische Trade-offs: Bewusste Abwägung zwischen Sicherheitsgewinn, Wirtschaftlichkeit und operativer Effizienz

Zielgruppe. Geschäftsleitung, Aufsichtsrat, Führungskräfte

Mini-Spiel. Lust auf eine Beispielfrage aus der Kampagne? Wie würden Sie sich entscheiden? Sie haben 60 Sekunden Zeit, die Antwort finden Sie unten.

Priorisierung von Schwachstellen

Ein Hackerangriff erfolgt

Die IT meldet zwei Lücken: A) Kritische Lücke in App X (wenig genutzt) und B) Mittlere Lücke in App Y (kernkritisch). Was priorisieren Sie, wenn beide sofort behoben werden können (48-49)

- Schwachstelle A, da der dort ein erfolgreicher Angriff am wahrscheinlichsten ist
- Schwachstelle B, da deren potenzieller Schaden am größten wäre
- Beide gleichzeitig, um Compliance zu zeigen
- Die Behebung, die am schnellsten umsetzbar ist

Richtige Antwort: 1. Die Priorisierung von Schwachstellen unterliegt einem Trade-off zwischen Eintrittswahrscheinlichkeit und Schadensausmaß. Bei sofortiger Behebbarkeit ist oft die höchste Eintrittswahrscheinlichkeit (kritische Lücke) die beste operative Priorität, um zu verhindern, dass sich Hacker im Netz einnisten und bewegen.

Ausblick

Konferenzen und Events



2. März online



3. März in Dortmund



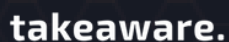
6. April online



28. April in Hamburg



4. Mai online



21. Mai in Düsseldorf

What the Hack! vor Ort erleben

Sie möchten selbst einmal gemeinsam mit Kolleg:innen erleben, wie **What the Hack!** funktioniert, wie es sich anfühlt, Teil der Human Firewall zu sein und Hacker zu fangen?

Dann buchen Sie einen Termin für ein Demospiel vor Ort oder Online unter

info@sbg-gaming.com

Call for Participation – wir suchen interessierte Unternehmen, Behörden und (Hoch) Schulen, die als Co-Creators an den folgenden Kampagnen mitwirken möchten:

Industrieperspektive auf **Healthcare, Finance**

Compliance-Trainings zu Arbeitssicherheit, Geldwäsche & Finanzkriminalität

Schulungen zu **Einführung in die KI, New Work & Agile**

Zum Abonnieren
des SBG Quarterly
hier scannen →



Die nächste Ausgabe des Quarterly
erscheint am 5. Mai 2026.



Impressum

Serious Business Gaming Quarterly ist eine unternehmensbezogene Publikation der

SBG Serious Business Gaming GmbH
Waagenstraße 20 in 40229 Düsseldorf
Vertreten durch: Marcus Schaper, CEO

Kontakt und Website:
info@sbg-gaming.com
www.sbg-gaming.com

Serious Business Gaming Quarterly ist kein journalistisch-redaktionelles Pressemedium

© 2026 SBG Serious Business Gaming