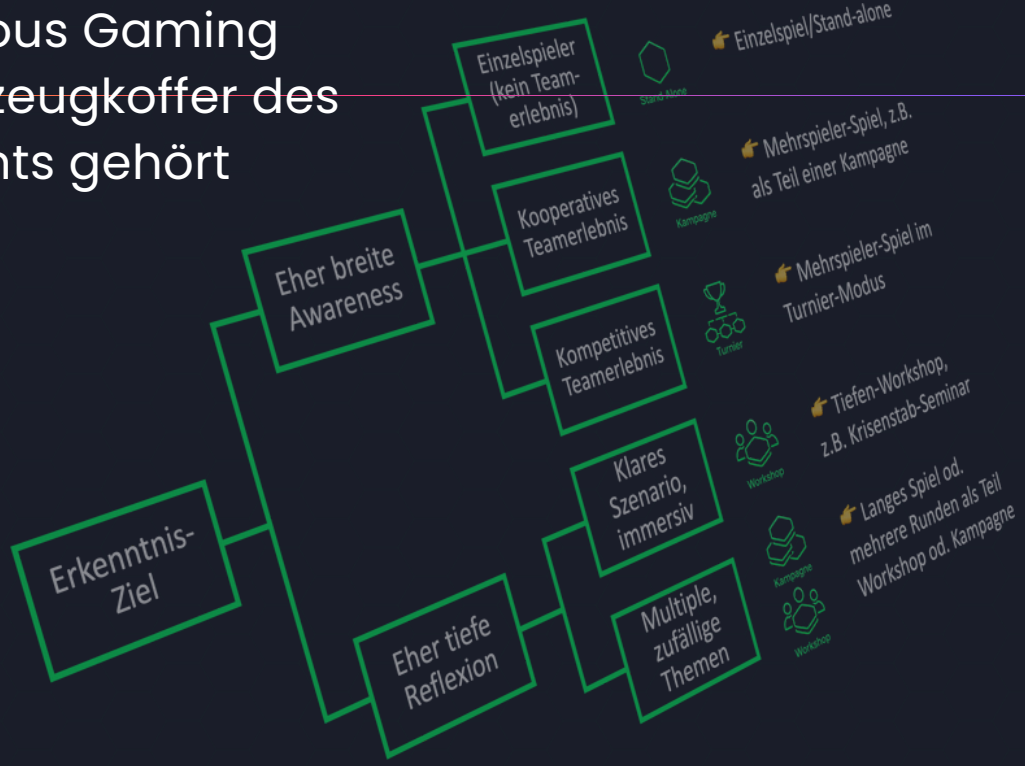
SBG
Serious Business Gaming

SERIOUS BUSINESS GAMING QUARTERLY

MANAGEMENT · SCIENCE · TECHNOLOGY

# Die perfekte [Compliance-Schulung] [Awareness-Kampagne] [Strategie-Simulation] mit Serious Gaming

Warum Serious Gaming in den Werkzeugkoffer des Managements gehört




SPECIAL zu Serious Games als Management-Instrument Issue 02 · May 2026

## Editorial

Liebe Leserinnen, liebe Leser,

geopolitische Unsicherheiten, KI und wirtschaftliche Transformationen erhöhen den Druck auf Unternehmen, ihre Mitarbeitenden gezielt weiterzuentwickeln. Ob Schutz vor Cyberrisiken, Verständnis neuer Technologien oder das Gelingen von Transformationen – Weiterbildung ist heute ein zentraler Erfolgsfaktor.

Dennoch wird sie häufig delegiert. Dabei ist sie eine Führungsaufgabe. Strategie, Organisation und Fähigkeiten lassen sich nur gemeinsam entwickeln. Wer wirksam führen will, muss auch Lernen aktiv gestalten.

***Wer wirksam führen will, muss auch das Lernen aktiv gestalten***

Gerade bei Awareness-Themen zeigt die Forschung: Lernen wirkt dann, wenn es erfahrbar ist und Entscheidungen erfordert. Genau hier setzen Serious Games an. Richtig eingesetzt sind sie kein Zusatz, sondern ein Management-Instrument.

In dieser Ausgabe zeigen wir, welche Instrumente in keinem Management-Werkzeugkasten fehlen dürfen, wie sich diese Instrumente konkret nutzen lassen. Wer sie einsetzt, wird Awareness- und Transformationsprogramme anders führen: klarer, wirksamer und näher an der Realität. Wir wünschen Ihnen eine anregende Lektüre.

Ihr Marcus Schaper

MANAGEMENT · SCIENCE · TECHNOLOGY

### Executive Navigator

In dieser Ausgabe zu **Serious Gaming als Management-Werkzeug** beginnen wir mit einem Review der wichtigsten wissenschaftlichen Erkenntnisse zum Serious Gaming auf Seite **03**. Der Fokus liegt diesmal auf den Management-Werkzeugen ab Seite **04**: dem Closed-Management-Loop, der nicht zur bei Awareness-Strategien eine exzellente Figur abgibt; dem Entscheidungsbaum, welches Spiel zu welchem Zweck passt und schließlich ein feines Portfolio an Serious Games, das man immer parat haben sollte. Abgerundet wird der Teil durch einen Standpunkt von **Florian Haacke**.

Wenn Sie glauben, Spionage wäre nur etwas für James Bond, lesen Sie Seite **07** – dort können Sie auch die neue Kampagne dazu kennenlernen. Es ist eine von fünf neuen Kampagnen von **What the Hack!**, für das auch neue Features wie KI-gesteuerte Hacker auf Seite **08** für mehr Freiraum für Teams sorgen.

Unsere Angebote diesmal beinhalten Open Game Sessions und individuelle Demorunden. Falls Sie im Automobilbereich oder in der Chemiebranche arbeiten, laden wir Sie herzlich ein, bei einer neuen Branchen-Kampagne mitzuwirken. Alle Mitmach-Angebote finden Sie auf Seite **09**.

# Was die Wissenschaft zu Serious Games sagt

## Vier empirische Erkenntnisse für den Unternehmensalltag

Spielen im Büro - passt das zusammen? Diese Frage stellen sich viele Manager, und lassen es im Zweifel lieber bleiben. Zu unrecht, wie uns seit vielen Jahren wissenschaftliche Erkenntnisse zeigen.*

***Wissenschaft ist sich einig: Serious Gaming ein wichtiger Baustein im Betrieb***

Seit vielen Jahren gibt es Untersuchungen dazu, wie Spielen im Vergleich zu anderen Formaten bei Themen wie Schulung, aber auch Strategiedefinition oder Krisenstab-Simulation funktioniert. Die Ergebnisse sind eindeutig. Das neue A.C.T.I.O.N. Framework (siehe Box) hilft dabei, die wichtigen Bedingungen erfolgreichen Awareness-Trainings einzuhalten.

**1 Spielen ändert Verhalten effektiv**
Durch das höhere A.C.T.I.O.N.-Level von Serious Games werden mehr Gehirnregionen intensiver angeregt, was zu höherer Gedächtnisleistung führt. Bei Auftreten der Triggerpunkte ("das habe ich schon mal gehört") kommen Denkprozesse in Gang, die zu verändertem Handeln führen können.

**2 Spielen macht "langweilige" Themen "spannend"**
Etwa 90% der Erwachsenen empfinden Gaming als produktivitätssteigernd beim Lernen, und 70% berichten über höhere Motivation.

**3 Spielen im Team stärkt Lernleistung und Problemlösungskompetenz**
Meta-Analysen des *cooperative learnings* zeigen 15-25% besseres Abschneiden in Leistungstests. Die PISA-Studie vermeldet "signifikant bessere Ergebnisse" beim Problemlösen komplexer Aufgaben.

**4 Spielen hat einen exzellenten Lern-ROI**
Stellt man die positiven Effekte von weniger Cybervorfälle in Verhältnis zu Spiel- und Organisationsaufwand, so ergeben sind positive ROI (*return on investment*) von 2:1 bis 5:1, je nach Thema und Spielkonzept.

Serious Gaming ist kein kurzer Hype, sondern ein nachhaltiges Konzept für Awareness-Aufbau und Verhaltensänderung. Von Cybersicherheits-Trainings bis hin zu Transformationsbegleitung gehört es in den Werkzeugkasten jedes Managers. Wie Sie es nutzen können, verrät der nächste Artikel.

Das **A.C.T.I.O.N.-Modell** beschreibt sechs Wirkprinzipien für nachhaltige Awareness- und Lernprogramme: **Activation** sorgt für Aufmerksamkeit und Relevanz. **Choice** macht Entscheidungen und Konsequenzen erlebbar. **Teaming** nutzt soziale Dynamik, Austausch und Vorbilder. **Iteration** verankert Lernen durch Wiederholung, Feedback und Ausprobieren. **Outcome** richtet Maßnahmen auf messbare Wirkung aus – etwa weniger Fehlverhalten, bessere Entscheidungen oder höhere Resilienz. **Nesting** sorgt dafür, dass Lernen nicht isoliert bleibt, sondern in Routinen, Führung, Kultur und Strategie eingebettet wird. So wird aus Information nicht nur Wissen, sondern handlungsfähiges Verhalten im Alltag.

* Wouters et al., 2013; Clark et al., 2016; Jayakrishnan et al., 2022; Ninaus et al., 2014; Wen et al., 2019.

# Drei Tools für den Management-Werkzeugkasten

Beeindrucken Sie Ihre Kolleg:innen und Mitarbeitende mit innovativen Management-Tools, die wirken. Hier sind sie:

1. Der **Closed-Management-Loop** für Cybersicherheit (und andere Compliance-Themen) ist das Universalwerkzeug für nachhaltige Wirksamkeit von der Strategie bis zur Umsetzung
2. Der **Gamification-Entscheidungsbaum** hilft bei der Auswahl der passenden Spiele für den richtigen Zweck
3. Ein (feines) **Portfolio von Serious Games** sollte jeder im Köcher haben, um im entscheidenden Moment schnell einsatzbereit zu sein

---

Der **Closed-Management-Loop** - nicht nur für Cybersicherheit - definiert das Thema mit strategischer Einbettung. Warum brauchen wir Cybersicherheit? Gibt es eine produktseitige Notwendigkeit, operative Verpflichtungen oder reputatives Risiko?

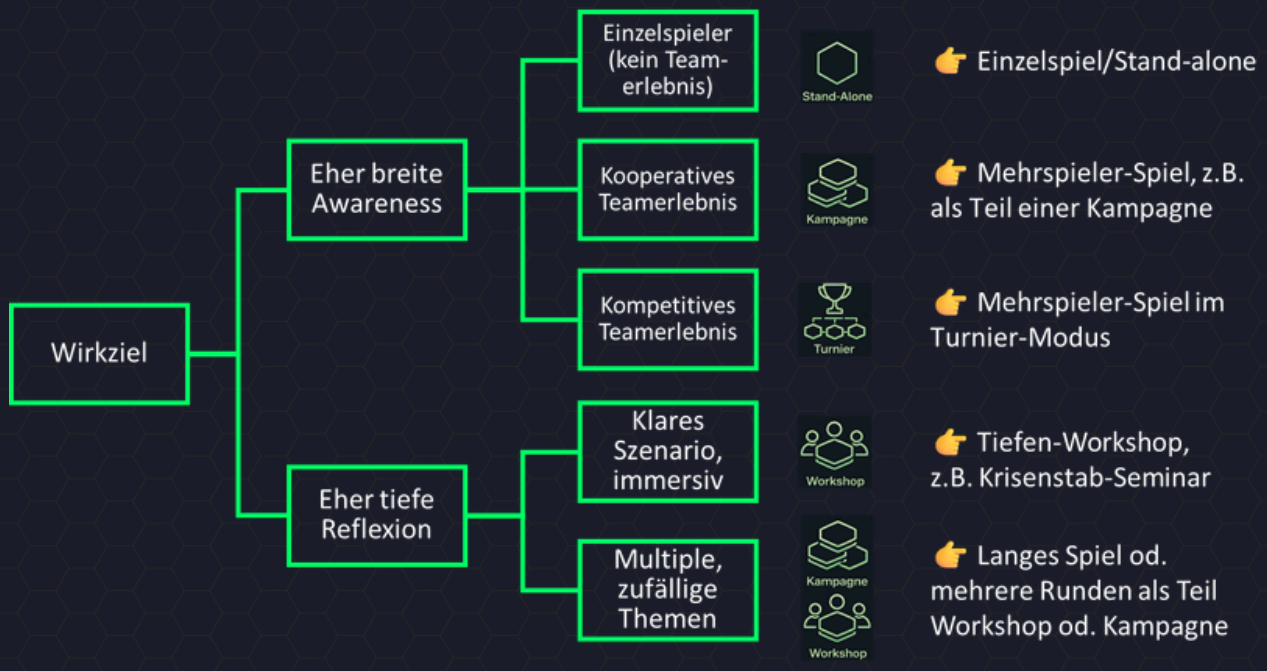
Daraus wird im ersten Schritt die **Strategie** abgeleitet: Welche langfristigen Änderungen an Produkten, Prozessen oder Skills werden durch wen, wann und wo gebraucht? Welche KPIs zeigen, ob die Strategie ihre gewünschte Wirkung entfaltet? Weiter geht die **Ableitung** in "absteigender" Richtung durch Programme, Projekte, Sprints bis zu einzelnen Handlungen, die dann umgesetzt werden. Hier beginnt der wesentliche Teil: der Review und die Adaption.

Selten funktionieren Strategien auf Anhieb, häufig muss adjustiert und korrigiert werden. Dazu sind die **Reviews und Adaptionen** in "aufsteigender" Richtung wichtig – und oft dem Imperativ neuer Initiativen geopfert. Aber gerade hier zeigt sich, ob die "nächste Sau durchs Dorf getrieben" wird, ober eine nachhaltige Verhaltens- und Strukturtransformation erreicht wird.

Nicht nur die saubere Ableitung und der rigorose Review sind wichtig, auch die enge **Verzahnung** von Produkt, Prozess und Personal. So kann die beste Awareness-Strategie nicht greifen, wenn die Patching-Prozesse zu lange Schwachstellen offen lassen, oder wenn die Firewall-Einstellungen zu durchlässig sind.

Prüfen Sie für Ihre Organisation, wie vollständig (vor allem der aufsteigende Ast) und wie verzahnt Ihre Cybersicherheits-Strategie ist und ergänzen Sie Lücken zügig. Besser schnell starten und durch kontinuierliche Verbesserungsprozesse sich an das Optimum annähern, als einen Totalausfall durch Ransomware zu riskieren.

Der **Gamification-Entscheidungsbaum** hilft dabei, den richtigen Mix verschiedener Formate zu finden. Beginnen Sie mit der Wurzel und entscheiden Sie sich von links nach rechts durch. Am Ende sehen Sie konkrete Beispiele, wie Serious Games für die verschiedenen Ziele eingesetzt werden können. Sie können den Baum aber auch für Phishing Kampagnen, Krisen-Simulationen oder andere Themen nutzen.




Ein kleines, aber feines und schnell einsetzbares **Portfolio an Serious Games** schließlich runden die *Must-Haves* an Management-Werkzeugen ab.

**1 Wissens- und Entscheidungsspiel**
wie **What the Hack!** Schnell erklärt, in 30 Minuten gespielt, hohe Intensität an Fragen pro Minute, als Teamaktivität gut geeignet.

**2 Simulationsplanspiel**
zur Überprüfung von Strategien. Möglichst genaue Abbildung von Marktverhältnissen und Kundenbedürfnissen sowie Wettbewerbsszenarien. Erfordert Vorbereitung.

**3 Krisen(stabs)simulation**
um eine Krise in allen Stadien nachzuspielen: von der Prävention (sind wir auf den Ernstfall vorbereitet) über die Reaktion (was tun wir im Ernstfall) bis hin zur Reflexion (wie verarbeiten wir den Ernstfall, wenn er vorüber ist).

**4 Escape-Game**
bringt Immersion und Spannung ins Team. Gute Logik- und Kombinationsrätsel trainieren die Problemlösungsfähigkeiten des Teams.

**5 Mindfulness-Spiel**
damit wir auch mal innehalten im hektischen Management-Alltag. *Cues* und *Biases* erkennen und *Nudges* geben. Stärkt das Verständnis und den Zusammenhalt im Team.

**6 Unternehmensfluss-Simulation**
"Ich bin eine Bestellung oder eine Anforderung" - wie ist der Weg durch die Unternehmung, welche Abteilungen sind involviert, wer entscheidet, wie oft muss nachgearbeitet werden, wie lange dauern die einzelnen Stufen, wie lange liegt die Bestellung ohne aktive Weiterarbeit? Öffnet vor allem als physische Übung die Augen für Optimierungspotenziale und -hebel.

# Standpunkt

## Florian Haacke

Seit über 25 Jahren im Dienste der (Cyber)Sicherheit unterwegs bei DHL, Metro, RWE, innogy und Porsche. Co-Founder der SBG Serious Business Gaming GmbH.

*SBGQ: Wo liegt die größte Bedrohung der Cybersicherheit für Deutschland und Europa?*

**Haacke:** Die geopolitische Lage und neue technische Fähigkeiten durch Künstliche Intelligenz machen Cyberangriffe zu einem dauerhaften strategischen Risiko. Gleichzeitig erlebe ich in der Praxis: Unsere größte Schwäche liegt oft bei uns selbst – beim Faktor Mensch in der Resilienzkette.

*SBGQ: Warum sind wir Menschen immer noch wenig begeistert, wenn wir etwas über Cybersecurity lernen sollen?*

**Haacke:** Weil das Thema häufig als Pflichtübung daherkommt und nicht als Teil guter Führung und Zusammenarbeit. Und weil viele Formate nicht emotional ansprechen – sie erklären, aber sie erreichen die Menschen nicht.

*SBGQ: Welche neuen Konzepte können bei Awareness-Kampagnen helfen?*

**Haacke:** Alles, was Menschen ins Handeln bringt, ist wirksam. Formate wie Serious Business Gaming funktionieren, weil sie Entscheidungen unter realistischen Bedingungen erlebbar machen – ergänzt durch einen durchdachten Format-Mix.

*SBGQ: Was macht überhaupt eine gute Awareness (Cyberresilienz)-Strategie aus?*

**Haacke:** Sie beginnt nicht bei Richtlinien, sondern bei den Arbeitsrealitäten der Menschen. Wenn Sicherheitsanforderungen in den Alltag integrierbar sind, verändert sich Verhalten – nicht nur Wissen.

*SBGQ: Wenn Du einen Wunsch frei hättest, was wäre das?*

**Haacke:** Dass wir Cyberresilienz konsequent als Teil guter Unternehmensführung verstehen. Dann sprechen wir nicht mehr über Awareness-Maßnahmen, sondern über verantwortungsvolle Entscheidungen im Alltag aller Mitarbeitenden.

*SBGQ: Wir danken für das Gespräch.*

# Spionage & Sabotage begegnen

## Ein Awareness-Crashkurs zu Industriespionage, Insider-Risiken und physischer Sicherheit

Geopolitische Spannungen, technologische Abhängigkeiten und zunehmender Wettbewerbsdruck machen Unternehmen anfälliger für Spionage und Sabotage. Angriffe beginnen dabei selten spektakulär. Oft reichen ein beiläufiges Gespräch, ein fremdes USB-Kabel, ein offener Drucker oder eine harmlose Frage in einem Business-Netzwerk wie LinkedIn oder Xing.

Viele Mitarbeitende unterschätzen diese Risiken, weil sie nicht wie klassische Cyberangriffe aussehen. Genau dafür wurde diese Kampagne entwickelt: wie funktioniert Spionage im Alltag, wie kann man verdächtige Situationen erkennen und professionell reagieren. Das Modul kann sehr gut als Teil einer größeren Kampagne eingesetzt werden. Oder Stand-Alone.

| Stand-Alone | Kampagne | Turnier | Workshop |
|---|---|---|---|
| Sehr gut | Exzellent | Gut | Gut |
| Standortbestimmung und erste Awareness | Vertiefte Awareness, gut kombinierbar | Einmaliger Aufmerksamkeits-Booster | Tiefe Reflexion, gut für Experten |

**Zweck.** Mitarbeitende befähigen, Spionage- und Sabotagerisiken im Arbeitsalltag zu begegnen und somit kritische Infrastrukturen und Daten besser zu schützen

**Schwierigkeit.**

**Kernthemen (Auswahl):**
**Social Engineering & Elicitation**: Erkennen manipulativer Gesprächstechniken, Fake-Profile, Honeypots und scheinbar harmloser Informationsabfragen
**Physische Sicherheit & Sabotage**: Schutz vor Tailgating, manipulierten Geräten, Hardware-Angriffen, Infrastruktur-Sabotage und Visual Hacking
**Insider Threats & MICE**: Verständnis für typische Anwerbemotive, Unzufriedenheit, Erpressbarkeit und Warnsignale
**Know-how-Schutz & Exfiltration**: Sicherer Umgang mit Cloud-Diensten, KI, mobilen Geräten, Offboarding und Datenabfluss

**Zielgruppe.** Alle Mitarbeitenden, insbes. mit Kontakt zu vertraulichen Informationen

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

Business-Netzwerke

Ein Hackerangriff erfolgt

**Im Profil eines neuen Kontakts finden Sie ein makelloses Foto, im CV renommierte Firmen, aber keine gemeinsamen Kontakte. Was könnte dies bedeuten?** (6870)

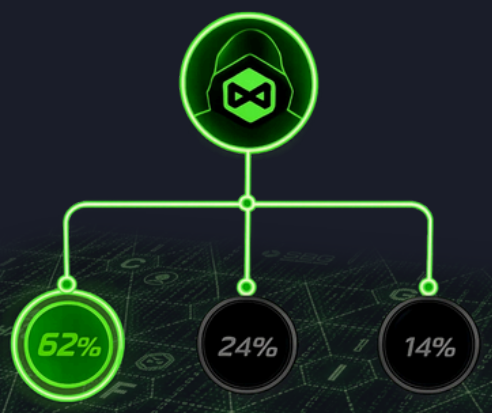
1. Der Kontakt legt besonderen Wert auf Privatsphäre und nutzt daher ein professionelles Fotografen-Bild statt einer privaten Aufnahme
2. Es handelt sich vermutlich um einen Honeypot, bei dem ein synthetisches Profil genutzt wird, um Vertrauen aufzubauen
3. Das Profil wurde von einem Headhunter-Algorithmus erstellt, der automatisch den bestmöglichen Lebenslauf zusammenstellt
4. Die Person ist ein Ghost-Worker, der im Auftrag verschiedener Firmen lediglich Marktforschung betreibt

Richtige Antwort: 2. Fehlende Interaktionen und zu perfekte Bilder sind Warnsignale für Fake-Profile. Spione nutzen diese, um Barrieren abzubauen und Informationen abzusaugen

# Neues von What the Hack!

**AI Hacker Moves. Hacker nutzen AI. Wir auch.**

Ab sofort kann sich die rote Hackerfigur bei **What the Hack!** autonom bewegen, gesteuert durch AI und angepasst auf das jeweilige Schwierigkeitsniveau. Das bedeutet, Teams und Moderator:innen können sich auf das konzentrieren, was am wichtigsten ist: gemeinsam Lösungen für die kniffeligen Rätsel und Entscheidungssituationen finden und die Hacker dingfest machen.




**Warum das wichtig ist.** Zum ersten Mal wird **What the Hack!** auch solo spielbar. Außerdem können sich Moderator:innen nun komplett auf ihr Team konzentrieren, das Spiel bleibt fair und neutral. Weniger Spielmechanik, mehr Fokus auf Diskussionen und Entscheidungen.

Gleichzeitig bleiben Teams flexibel: Für jedes Spiel kann weiterhin festgelegt werden, dass Moderator:innen die Hackerfigur steuern – etwa bei Spielen mit Kindern, Einsteigergruppen oder wenn bewusst mehr Einfluss auf den Spielverlauf gewünscht ist.

---

**Sounds. Mehr Immersion, mehr Emotion.**

Mit neuen Soundeffekten und einem eigens komponierten Soundtrack wird **What the Hack!** noch intensiver erlebbar.
Ein atmosphärisches „Willkommen zu What the Hack!“ zum Start, ein euphorisches „Glückwunsch, Ihr habt gewonnen!“ beim Sieg. Und dazwischen: ein subtiler Soundtrack, der Spannung aufbaut und die Atmosphäre der Hackerjagd unterstützt. Gibt’s zum Start auf Deutsch und Englisch (je nach Spielsprache).

Natürlich gilt auch hier: alle Sounds lassen sich abschalten, je nach Setting oder persönlicher Präferenz.

**Fünf neue Kampagnen** für mehr Relevanz in wichtigen Themenfeldern und Industrien. Die Industriekampagnen bringen verschiedene Perspektiven einer Industrie zusammen, während die Themenkampagnen zur gezielten Vertiefung dienen.

---

**News-Ticker** +++ Neue Demo-Kampagne für schnelle 15 Minuten-Games (Schwierigkeit “hoch” einstellen) +++ einfacher Wechsel zwischen Moderator- und Online-Brett-Screens +++ QR-Code auch auf dem Spielbrett für “Späteinsteiger” +++ Game-Statistiken abrufbar

# Ausblick

### SBG auf Konferenzen und Events

12./13.05. NIS-2 Kongress Frankfurt

20./21.05. Takeaware Düsseldorf

01.06. Open Game Session (online)

18./19.06. Transform_D Summit Berlin

15.07. Phish & Chips Bonn

### 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 **Automotive, Chemie & Pharma**

**Compliance/Security**-Trainings zu Sabotage & Spionage

Schulungen zu **New Work & Agile, Unternehmenstransformation**

**Zum Abonnieren des SBG Quarterly hier scannen:**

Die nächste Ausgabe des Quarterly erscheint am 4. August 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