

SERIOUS BUSINESS GAMING QUARTERLY



MANAGEMENT



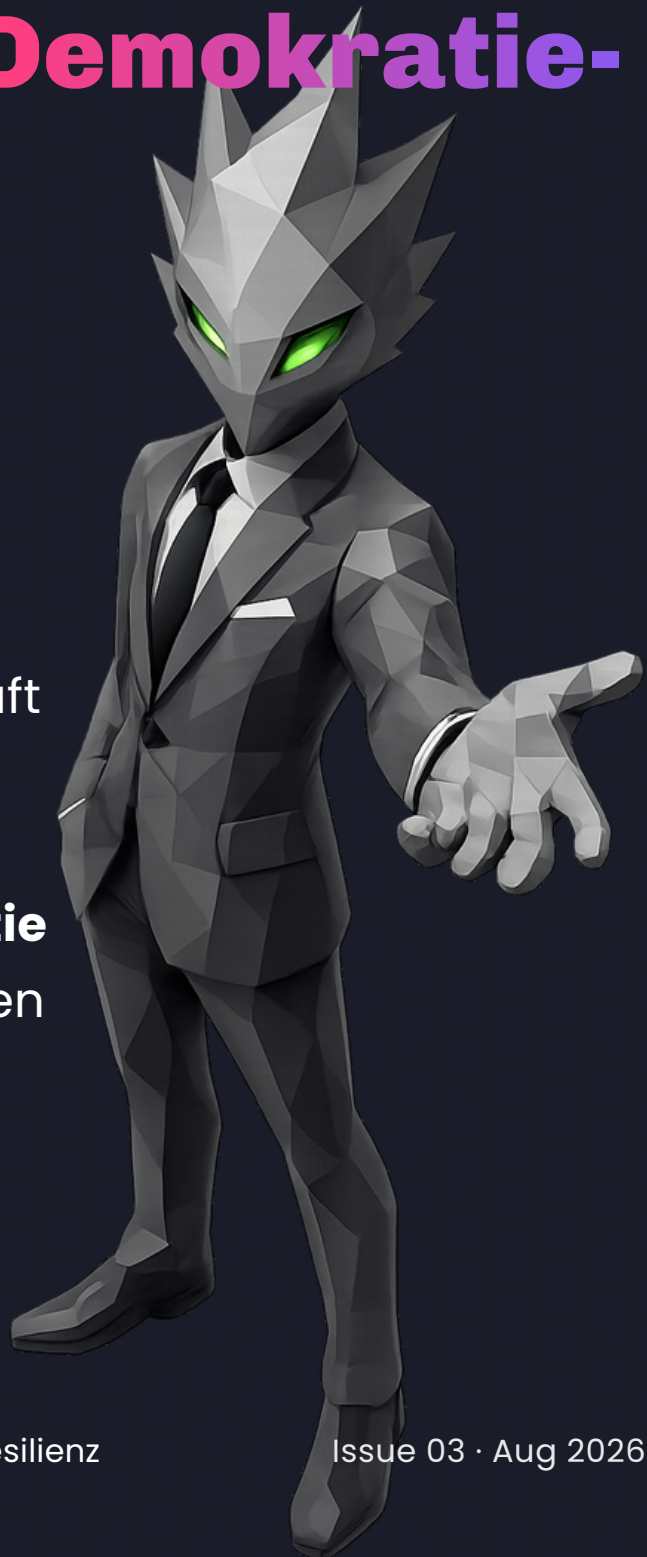
SCIENCE



TECHNOLOGY

Mit Engagement zur Cyber- und Demokratie- Resilienz

Wie wir als Zivilgesellschaft
den Bedrohungen und
Angriffen im **Cyberraum**
und gegen die **Demokratie**
wirksam begegnen können



Editorial

Liebe Leserinnen, liebe Leser,

Deutschland lebt vom Engagement seiner Bürger:innen. In Vereinen investieren Menschen freiwillig ein besonders knappes Gut: ihre Zeit. Sie tun das für den Sport, für Kultur, Bildung, Nachbarschaftshilfe, Opferhilfe oder viele andere Aufgaben, ohne die unser Gemeinwesen kaum funktionieren würde.

Gerade darin liegt die Stärke des Ehrenamts – und zugleich seine Verletzlichkeit. Denn Sicherheitsfragen stehen verständlicherweise selten im Mittelpunkt. Der Chor möchte singen, die Jugendmannschaft trainieren, die Opferhilfe Betroffene unterstützen. Niemand engagiert sich, weil er sich für Passwortregeln, Krisenpläne oder Desinformation interessiert.

Viele Vereine halten sich deshalb für kein attraktives Ziel. Doch automatisierte Cyberangriffe suchen nicht nach Größe oder Bekanntheit, sondern nach Gelegenheiten: schwachen Passwörtern, ungeschützten Webseiten oder kompromittierten E-Mail-Konten. Und auch Desinformation und Rufmord können genau das beschädigen, worauf Vereinsarbeit beruht: Vertrauen.

Gerade weil Vereine ein so wertvoller Teil unserer Gesellschaft sind, tragen ihre Mandatsträger eine besondere Verantwortung. Die größte Stärke eines Vereins ist seine Gemeinschaft. Sie zu schützen, gehört deshalb heute zu den zentralen Führungsaufgaben im Ehrenamt.

Ihr Marcus Schaper



Cyber- und Demokratie-Resilienz schützt auch Vereine

Executive Navigator

In dieser Sonderausgabe zu Engagement und Ehrenamt zeigt ab Seite **03** zeigt der wissenschaftliche Leitartikel, **warum Hacker und Demokratiesaboteure auf dieselben psychologischen Mechanismen setzen** – und weshalb Resilienz bei unserer eigenen Urteilsfähigkeit beginnt.

Daraus leiten wir zwei konkrete Angebote ab: Ab Seite **07** finden Vereinsvorstände einen **Resilienz-Check** samt Impulsen für direkt einsetzbare **Formate für Vereine**. Wer Manipulation mit Hilfe von Serious Gaming verstehen und in kniffligen Situationen selbst entscheiden möchte, lernt auf Seite **10** die neue **Kampagne Hack My Mind!** kennen.

Die Horizonte2030-Gründerin und Initiatorin der Catch the Hacker-Kampagne **Maren Schoening** setzt auf Seite **09** ihren persönlichen Akzent zum Thema Serious Gaming.

Den Abschluss bilden auf Seite **11 Mitmach-Möglichkeiten**, mehr über Serious Gaming und What the Hack! zu erfahren und gemeinsam mit uns weiterzuarbeiten.



Was Hacker und Demokratie-Saboteure gemeinsam haben

Wie unser Gehirn zur wichtigsten Angriffsfläche moderner Demokratien geworden ist und wie wir dem begegnen können

Warum fallen Menschen auch heute noch auf Phishing-Mails herein, obwohl die Maschen seit Jahren bekannt sind? Weshalb verbreiten sich Falschinformationen in sozialen Medien häufig schneller als ihre Richtigstellungen? Und warum gelingt es Demokratie-Saboteuren immer wieder, Misstrauen zu säen, gesellschaftliche Gruppen gegeneinander auszuspielen und demokratische Prozesse zu destabilisieren?

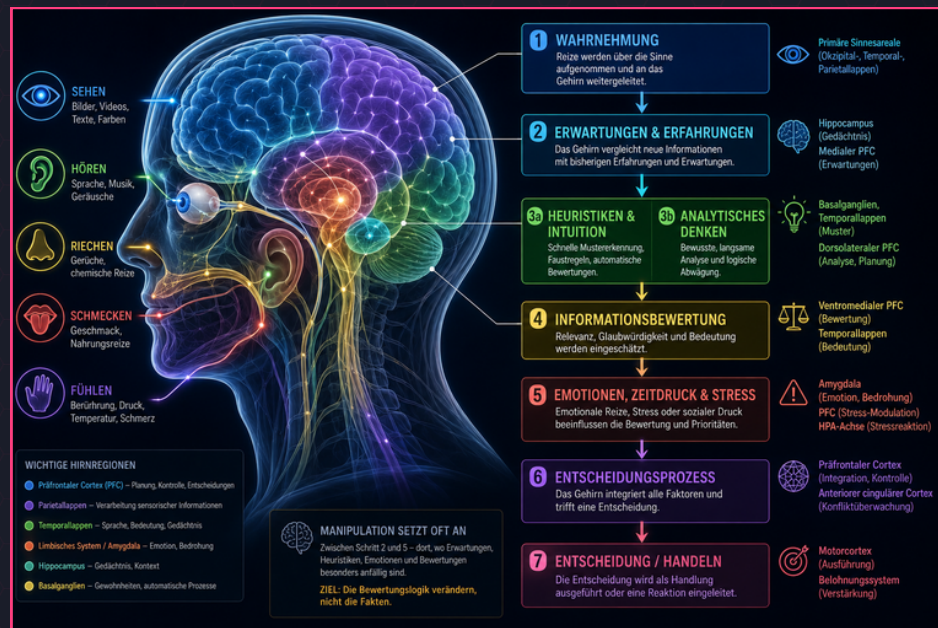
Auf den ersten Blick scheinen diese Phänomene wenig miteinander zu tun zu haben. Cyberkriminalität verfolgt andere Ziele als politische Manipulation. Die einen wollen Zugang zu Daten oder Geld erlangen, die anderen Vertrauen untergraben oder öffentliche Meinungsbildung beeinflussen. Betrachtet man jedoch ihre Methoden,

zeigt sich eine überraschende Gemeinsamkeit: Beide greifen nur selten zuerst technische Schwachstellen oder institutionelle Strukturen an. Sie nutzen dieselbe Angriffsfläche – den Menschen und seine Art, Informationen zu bewerten und Entscheidungen zu treffen.

Die Angriffsfläche moderner Gesellschaften ist deshalb weder der Computer noch die Demokratie. Es ist unser Gehirn.

Jeden Tag treffen wir tausende Entscheidungen. Welche Nachricht verdient Aufmerksamkeit? Wem können wir vertrauen? Welche Quelle erscheint glaubwürdig? Muss ich sofort handeln oder lohnt es sich, zunächst genauer hinzusehen?

Eine vollständige Analyse jeder Situation wäre unmöglich. Unser Gehirn verarbeitet weit mehr Informationen, als wir bewusst erfassen können. Um dennoch handlungs-



fähig zu bleiben, reduziert es Komplexität. Es erkennt Muster, greift auf Erfahrungen zurück und nutzt Heuristiken – mentale Faustregeln, die schnelle Entscheidungen auch dann ermöglichen, wenn Informationen unvollständig oder widersprüchlich sind.

Die Kognitionspsychologie beschreibt dieses Zusammenspiel seit Jahrzehnten. Modelle wie die **Dual-Process-Theorie**

unterscheiden zwischen schnellen, intuitiven und langsameren, analytischen Entscheidungsprozessen. Beide sind unverzichtbar. Ohne unsere Intuition könnten wir den Alltag kaum bewältigen. Analytisches Denken wiederum hilft dort, wo Entscheidungen neu, komplex oder besonders folgenreich sind.

Heuristiken sind deshalb keine Schwäche unseres Denkens. Sie sind eine bemerkenswert erfolgreiche Anpassung an eine komplexe Welt.

Gerade weil sie so gut funktionieren, verlassen wir uns meist unbewusst auf sie. Vertraute Absender wirken glaubwürdiger als unbekannte. Wiederholte Aussagen erscheinen plausibler als neue Informationen. Autoritäten genießen einen Vertrauensvorschuss.

Aussagen aus der eigenen sozialen Gruppe fühlen sich häufig überzeugender an als widersprechende Argumente.

Unter emotionalem Druck verstärken sich diese Effekte. Neurobiologische Forschung zeigt, dass Stress die Verarbeitung von Informationen verändert. Emotionale Reize gewinnen an Bedeutung, während Hirnregionen des präfrontalen Cortex, die stärker mit reflektierter Abwägung verbunden sind, weniger wirksam arbeiten. Was evolutionsbiologisch sinnvoll war – in Gefahr schnell zu handeln –, eröffnet in modernen Informationsgesellschaften neue Möglichkeiten für gezielte Manipulation.

Genau hier liegt die Gemeinsamkeit von Phishing, Desinformation und demokratischer Manipulation.

Manipulation beginnt nicht damit, unsere Meinung zu verändern; sondern damit, unsere Informationsbewertung zu ändern

Eine Phishing-Mail muss ihr Opfer nicht davon überzeugen, grundsätzlich leichtsinnig zu werden. Es genügt, den Eindruck zu erzeugen, sofort handeln zu müssen. Eine Falschinformation muss nicht sämtliche Fakten widerlegen. Oft reicht es aus, Unsicherheit zu erzeugen oder das Vertrauen in verlässliche Quellen zu erschüttern. Demokratie-Saboteure müssen Menschen nicht vollständig von ihrer Weltanschauung abbringen. Häufig genügt es, Emotionen stärker zu gewichten als Fakten oder Gruppenzugehörigkeit wichtiger erscheinen zu lassen als eine differenzierte Betrachtung.



Manipulation verändert deshalb häufig nicht zuerst unsere Überzeugungen. Sie verändert den Bewertungsmaßstab, nach dem neue Informationen eingeordnet werden.

Eine weitere Erkenntnis aus der Neurowissenschaft hilft, dieses Phänomen besser zu verstehen. Nach dem Konzept des **Predictive Processing** bildet das Gehirn die Wirklichkeit nicht einfach passiv ab. Es entwickelt fortlaufend Erwartungen darüber, was wahrscheinlich geschieht, und gleicht



diese mit neuen Sinneseindrücken ab. Wahrnehmung entsteht somit aus dem Zusammenspiel von Erfahrung, Erwartungen und Beobachtung.

Wir sehen die Welt nicht, wie sie ist. Wir sehen sie immer so, wie unser Gehirn erwartet, dass sie ist

Diese Fähigkeit macht menschliches Denken außerordentlich effizient. Gleichzeitig erklärt sie, warum Vorurteile, Wiederholungen oder emotional aufgeladene Erzählungen einen so großen Einfluss entfalten können. Wer Erwartungen gezielt beeinflusst, verändert auch die Art und Weise, wie neue Informationen bewertet werden.

Deshalb ähneln sich die Methoden von Hackern und Demokratie-Saboteuren stärker, als ihre unterschiedlichen Ziele vermuten lassen. Beide nutzen Zeitdruck, Unsicherheit, Autorität, Gruppenzugehörigkeit oder starke Emotionen, um menschliche Urteilsprozesse zu beeinflussen. Der eigentliche Angriff richtet sich nicht gegen Computer oder demokratische Institutionen, sondern gegen die Mechanismen menschlicher Entscheidungsfindung.

Die gute Nachricht lautet jedoch: Dieselben Mechanismen, die Manipulation ermöglichen, lassen sich auch trainieren. Wer seine eigene Urteilsfähigkeit stärken möchte, muss nicht jede neue Betrugsmasche oder jede Form von Desinformation kennen. Entscheidend ist vielmehr, die eigenen Denkprozesse regelmäßig herauszufordern. Wie das funktioniert, können Sie in der Infobox "Mind-Hacks" sehen.

Diese kleinen Gehirn-Interventionen stärken genau jene Fähigkeiten, auf die Manipulation abzielt: kritisches Denken, Perspektivwechsel, Selbstreflexion und den bewussten Umgang mit Unsicherheit. Sie helfen nicht nur dabei, Phishing-Mails oder Falsch-

informationen besser zu erkennen. Sie fördern zugleich die Fähigkeit, auch in gesellschaftlichen Debatten oder bei unternehmerischen Entscheidungen differenziert zu urteilen und sich nicht vorschnell von Emotionen oder Gruppendruck leiten zu lassen.

Wir haben fünf "Mind-Hacks" für Sie vorbereitet - der sechste ist Ihre ganz persönliche Selbst-Intervention, die Sie sich im Alltag immer wieder vor Augen führen können - als Ausdruck auf dem Schreibtisch oder kleine Merkkärtchen für unterwegs.

Cyberresilienz und Demokratieresilienz beginnen damit, auch unter Unsicherheit gute Entscheidungen zu treffen

Cyberkriminelle und Demokratie-Saboteure werden ihre Methoden weiterentwickeln. Die gemeinsame Angriffsfläche bleibt jedoch dieselbe. Wer versteht, wie menschliche Entscheidungen entstehen, erkennt auch besser, wie sie beeinflusst werden können. Die wirksamste Form der Resilienz beginnt deshalb nicht erst bei technischen Schutzmaßnahmen oder politischen Institutionen. Sie beginnt dort, wo Menschen lernen, ihre eigene Urteilsfähigkeit bewusst zu stärken.

Literatur (Auswahl):

- Kahneman, D. (2011): Thinking, Fast and Slow. Farrar, Straus and Giroux.
- Friston, K. (2010): The Free-Energy Principle: A Unified Brain Theory? Nature Reviews Neuroscience, 11(2), 127–138.
- Gigerenzer, G. (2007): Gut Feelings: The Intelligence of the Unconscious. Viking.
- Cialdini, R. B. (2021): Influence – New and Expanded: The Psychology of Persuasion. Harper Business.
- Kahneman, D., Sibony, O. & Sunstein, C. R. (2021): Noise – A Flaw in Human Judgment. Little, Brown Spark.



Sechs “Mind-Hacks” für jeden Tag

Zum Mitnehmen, Weitergeben oder An-den-Bildschirm-Hängen

Suche und schätze den Widerspruch

Lies bewusst eine seriöse Quelle, die eine andere Position als Du vertrittst. Sage Dir: “Es ist wertvoll, dass ich diese Position kenne, denn sie hilft mir, eine bessere eigene aufzubauen”.

Erkenne den emotionalen Druck

Wenn Du Dich unwohl mit einer Entscheidung fühlst, weil Du Zeitdruck oder Gruppendruck spürst, mache Dir bewusst, dass so etwas Manipulationstechniken sind. Entscheide erst dann die Dringlichkeit.

Hinterfrage Deine Sicherheit

Je sicherer Du bist, desto eher lohnt sich ein zweiter Blick: Bin ich mir sicher, weil ich ein bewährtes Muster wiederhole, oder ist diese spezifische Situation vielleicht anders?

Nutze Gefühl und Verstand

Emotionen sind wichtig, sie sollten aber nicht allein das Urteil lenken. Überlege Dir, welchen Anteil Fakten und analytisches Denken an Deinem Urteil hatten und nutze beides gleich stark.

Checke Deine Annahmen

Jede Entscheidung unter Unsicherheit beruht auf Annahmen. Welches sind diejenigen, ohne die Du eine andere Entscheidung getroffen hättest – überlege, ob sich höchstwahrscheinlich zutreffen und was passiert, wenn nicht?



Vereine müssen schützen, was sie stark macht

Cyber- und Demokratieresilienz gehören im Ehrenamt dazu

Menschen engagieren sich freiwillig, weil ihnen etwas wichtig ist. Sie investieren Zeit, Energie und Herzblut – nicht für einen Arbeitgeber, sondern für eine **gute, gemeinsame Sache**. Für den Sportverein, den Chor, die Freiwillige Feuerwehr, den Tiererschutz, die Opferhilfe oder den Kleingartenverein.

Genau darin liegt die größte Stärke des Ehrenamts. Und zugleich seine größte Verletzlichkeit. Denn das Fundament jedes Vereins ist **Vertrauen**. Vertrauen darauf, dass Mitgliederdaten sicher sind. Dass Spenden dort ankommen, wo sie gebraucht werden. Dass Informationen stimmen. Dass unterschiedliche Meinungen respektvoll ausgetauscht werden können. Und dass sich Menschen unabhängig von Herkunft, Alter oder Weltanschauung gemeinsam für ein Ziel engagieren.

Dieses Vertrauen entsteht nicht von selbst. Es muss geschützt werden. Dabei denken viele Vereine zunächst: **Warum sollten Hacker ausgerechnet uns angreifen? Wir verwalten ein paar Mitgliedsdaten, organisieren Veranstaltungen und arbeiten überwiegend ehrenamtlich. Für Kriminelle gibt es doch deutlich attraktivere Ziele.** Diese Einschätzung ist nachvollziehbar. Heute trifft sie jedoch immer seltener zu.

Cyberangriffe werden längst nicht mehr ausschließlich gegen einzelne Organisationen geführt. Die meisten Angriffe erfolgen automatisiert. Programme durchsuchen das Internet nach ungeschützten Webseiten, schwachen Passwörtern oder kompromittierten E-Mail-Konten – unabhängig davon, ob dahinter ein internationaler Konzern, ein

Handwerksbetrieb oder ein kleiner Sportverein steht. **Entscheidend ist nicht, wer angegriffen wird, sondern wer sich leicht angreifen lässt.**

Gerade heute [wird] die freiheitliche Demokratie im Innern wie von außen angegriffen. [F.W.Steinmeier, 2025]

Für Vereine können die **Folgen existenziell sein**. Mitgliederdaten können verloren gehen, Spendenkonten missbraucht, Veranstaltungen abgesagt oder Kommunikationskanäle übernommen werden. Noch schwerer wiegt häufig der Vertrauensverlust.

Ehrenamt lebt davon, dass Menschen Verantwortung übernehmen und darauf vertrauen können, dass ihre Daten, ihre Spenden und ihr Engagement in guten Händen sind. Geht dieses Vertrauen verloren, ist der eigentliche Schaden oft deutlich größer als der finanzielle Verlust.

Hinzu kommt eine zweite Entwicklung. Vereine sind Orte, an denen Menschen offen miteinander diskutieren und gesellschaftlichen Zusammenhalt leben. Gerade deshalb können auch Desinformation, gezielte Provokationen oder manipulative Inhalte **Gemeinschaften belasten**. Denn dieselben psychologischen Mechanismen, die Cyberkriminelle ausnutzen, spielen auch dort eine Rolle.

Die gute Nachricht lautet: Vereine müssen dafür keine Sicherheitsexperten anheuern oder langatmige Schulungen durchkauen. Viel wichtiger ist eine **Kultur der Aufmerksamkeit**. Wer lernt, Manipulationsversuche zu erkennen, Informationen kritisch zu



hinterfragen und gemeinsam gute Entscheidungen zu treffen, stärkt zugleich die Cyberresilienz und die Widerstandsfähigkeit der Gemeinschaft.

Serious Games bieten hierfür einen ungewöhnlichen, aber wirkungsvollen Ansatz. Statt abstrakte Regeln zu vermitteln, bringen sie Menschen miteinander ins Gespräch. Sie schaffen gemeinsame Erlebnisse, machen Manipulationsversuche greifbar und stärken genau das, was Vereine ohnehin auszeichnet: Zusammenarbeit, gegenseitiges Vertrauen und die Freude, gemeinsam Herausforderungen zu meistern. Das Ganze mit wenig Zeiteinsatz und hohem Spaßfaktor.

Machen Sie den **Resilienz-Test** unten, ob Ihr Verein einfach anzugreifen ist. Wenn ja – und das dürfte für die deutliche Mehrheit der Vereine zutreffen – sollten Sie Resilienz in ihre Vereinsarbeit aufnehmen, zumindest intern für Ihre Mitglieder.

Ob Sie das Spiel Catch the Hacker in einer launigen Spielesession nutzen, eine Krisensimulation durchführen oder regelmäßig in den Vereinssitzungen über einzelne Themen sprechen, ist nicht entscheidend. Wichtig ist, dass Resilienz regelmäßig Auffrischung braucht, damit Sie sich weiter auf das konzentrieren können, dass Ihnen am Herzen liegt.

Wie funktioniert's?

1. Beantworten Sie die Fragen ehrlich
2. Ist eine rote oder zwei gelbe Ampeln dabei? Dann sollten Sie aktiv werden



Spion:

Welche Informationen über Euren Verein und die Mitglieder wären für andere interessant?



Hacker:

Wie lange könnte Euer Verein ohne IT oder E-Mail/Social Media funktionieren?



Betrüger:

Wie gut sind Eure Konten und Einkaufsprozesse abgesichert?



Saboteur:

Wodurch würde Eure Vereinsarbeit für mehrere Wochen stillstehen?



Agitator:

Was könnte Euren Zusammenhalt zerstören oder Mitglieder gegeneinander aufbringen?



Wir speichern gar keine Informationen

Namen von Mitgliedern u. Spendern

Viel: Namen, Adressen, Telefonnr.

Dauerhaft

bis zu 3 Monaten

weniger als einen Monat

wie rechts + Cyberversich. u. digital sign. Verträge

Mind. MFA u. Vieraugenprinzip

Weniger als links

Nichts

Profi-Werkzeuge nötig

Ernsthafter Amateur

Lange, breit angelegte Kampagne

Organisierte Kampagne/ Desinformat.

Weniger

Standpunkt

Maren Schoening

Gründerin und Vorstand der gemeinnützigen Gesellschaft Horizonte 2030 – Forum für den interkulturellen Dialog.



SBGQ: Maren, etwas Persönliches zum Start: Was spielst Du am liebsten und was reizt Dich daran?

Schoening: Spiele habe ich eher auf dem Sportfeld ausgetragen. Vor einiger Zeit habe ich die Möglichkeiten von Serious Games kennengelernt und bin begeistert.

SBGQ: Viele verbinden Spielen mit Leichtigkeit. Wann hast du zum ersten Mal erlebt, dass Spielen auch Tiefe haben kann?

Schoening: Mit zahlreichen Spiel lernt man strategisches Denken auf die leichte Art. Daher ist spielen für uns alle so wichtig.

SBGQ: Was ist die Idee hinter Horizonte 2030 – und warum braucht unsere Gesellschaft genau jetzt solche Formate?

Schoening: Wenn Zeitzeugen des Holocaust sterben, dann müssen wir ihr Erbe als Erinnerungsbotschafter weitertragen und uns konsequent gegen Antisemitismus, Rassismus und Ausgrenzung einsetzen. Der aufkommende Rechtsextremismus fordert uns alle, für unser Land, unsere Vielfalt und unsere universellen Werte einzustehen.

SBGQ: In deinen Projekten geht es um sensible Themen. Warum kann gerade ein Serious Game hier wirksamer sein als klassische Bildungsformate?

Schoening: Serious Games sind natürlich kein Ersatz für Unterricht. Sie können aber das Lernen bereichern und Jung und Alt spielerisch Themen näherbringen. Mit SBG entwickeln wir gerade das Spiel "Catch the Hacker" zum Thema Cybersicherheit, Fake News und Mobbing. Wir wollen mit dem Spiel gemeinsames Lernen und Spielfreude schaffen und gleichzeitig Wissen vermitteln. Im Herbst kommt es auf den Markt und kann über Horizonte 2030 bezogen werden.

SBGQ: Stell dir vor, ein Serious Game könnte eine Fähigkeit in unserer Gesellschaft stärken. Welche wäre das?

Schoening: Da kann ich mir viele Dinge vorstellen. Neben dem Spiel zur Cybersicherheit haben wir auch gerade ein Spielkonzept mit historischen und aktuellen Szenarien zur Einschränkung von Menschen- und Bürgerrechten in Deutschland entwickelt. Mit SBG gehen uns aber die Ideen nicht aus.

SBGQ: Wir danken für das Gespräch.

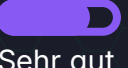


Hack my Mind!

Ein **Crashkurs** zu Denkfallen, Manipulation und KI-Gefahren – ohne Psychologie-Jargon

Geopolitische Spannungen, hochgradig personalisierte Betrugsmaschen und KI-gestützte Deepfakes verschärfen die Bedrohungslage rasant. Der kritischste Angriffsvektor ist längst nicht mehr nur die IT-Infrastruktur, sondern das menschliche Gehirn – egal ob am Arbeitsplatz oder im privaten Alltag.

Viele Menschen sind unsicher: „Wie erkenne ich kognitive Denkfallen, KI-Täuschungen und verdeckte Manipulationen im Alltag und Beruf rechtzeitig?“ Genau dafür haben wir diese Kampagne entwickelt, in der innerhalb von 30 Minuten die wichtigsten Wahrnehmungs- und Entscheidungsmuster spielerisch analysiert und reflektiert werden.

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

Zweck. Uns befähigen, kognitive Fehlschlüsse und Verzerrungen (Biases), Social-Engineering-Muster zu durchschauen: Wahrnehmen, Hinterfragen und entschärfen

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

Schwierigkeit.     

Kernthemen (Auswahl):

Kognitive Biases & Denkfallen: Wahrnehmungsverzerrungen (z. B. Authority Bias, Confirmation Bias, Sunk Cost Fallacy)

KI-Synthese & Medienkompetenz: Risiken durch KI-Voice-Cloning (z.B. Enkeltrick 2.0), Deepfakes, Uncanny Valley bewerten

Dark Patterns & Micro-Targeting: Manipulative Benutzeroberflächen, Abo-Fallen, verdecktes Nudging und personalisierte Impulskäufe durchschauen

Civic Resilience & Zivilcourage: Deeskalations-Strategien, Counterspeech, Überwindung von Scham-Lähmungen (Post-Scam-Apathy) nach Betrugsversuchen

Zielgruppe. Alle, die Spaß daran haben, mehr über sich und ihr Gehirn zu erfahren

Der dringende Notruf

Ein Hackerangriff erfolgt

Du erhältst eine Sprachnachricht von deiner Schwester, die um Geld bittet. Die Stimme klingt exakt wie sie, aber die Intonation wirkt minimal künstlich. Welcher Effekt verrät die KI-Fälschung und wie handelst du richtig?

1

Es handelt sich um den Uncanny Valley Effect; ich verlasse mich auf mein Störgefühl und rufe meine Schwester direkt auf ihrer gewohnten Nummer an

2

Es handelt sich um den Fear Appeal; ich beruhige mich bewusst und hinterfrage die behauptete Notlage auf ihre Plausibilität

3

Es handelt sich um den Social Proof; ich frage zuerst bei anderen Familienmitgliedern nach, ob ihnen dieser Notfall bekannt ist

4

Es handelt sich um den Default Effect; ich ignoriere die übermittelten Zahlungsdaten und nutze ausschließlich die mir bekannten Bankverbindungen

Antwort 1 ist korrekt: Das Uncanny Valley erzeugt das subtile Störgefühl bei synthetischen Stimmen. Die einzig handlungssichere Reaktion bei KI-Voice-Cloning ist der direkte Rückruf über die vertraute Primärnummer.



Ausblick

SBG auf Konferenzen und Events



07.09. Open Game Session (online)



24.09. EduCamp Summer Schwäbisch Gmünd



01.10. Cybersecurity Oktoberfest Stuttgart



05.10. Open Game Session (online)



27.-29.10. it-sa Congress Nürnberg

What the Hack! vor Ort erleben

Sie möchten selbst einmal gemeinsam im Verein oder der Firma 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 **HighTech** und **Software**

Compliance/Security-Trainings zu **Desinformation**

Schulungen zu **Scrum** und **Remote-Projekten**

Zum Abonnieren des SBG Quarterly hier scannen:



Die nächste Ausgabe des Quarterly erscheint am 5. November 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

