SERIOUS GAMES

Spielerisch zu mehr IT-Sicherheit

Sie möchten eines der Spiele in Ihrem Unternehmen durchführen?
Nehmen Sie gerne Kontakt mit uns auf:

seriousgames@unibw.de

Vorwort

Liebe Leserinnen und Leser,

Cyberangriffe gehören heute zum Alltag – ob in Behörden, Unternehmen oder im privaten Umfeld. Doch wie bereiten wir uns darauf vor? Wie gelingt es, Mitarbeitende für komplexe IT-Sicherheitsfragen zu sensibilisieren, ohne sie mit Fachbegriffen zu überfordern? Und wie können wir gemeinsam lernen, in kritischen Situationen sicher zu handeln?

Eine Antwort darauf liegt im Spiel. Genauer gesagt: im Serious Game.

Serious Games verbinden spielerische Elemente mit ernsten Lern- und Reflexionszielen. Sie ermöglichen es, Cybersicherheit nicht nur zu verstehen, sondern aktiv zu erleben. In realitätsnahen Szenarien treffen Spielteilnehmer Entscheidungen, übernehmen Verantwortung, reagieren auf Angriffe – und lernen dabei mit- und voneinander.

In dieser Broschüre stellen wir Ihnen eine Auswahl an Serious Games vor, die gezielt für den Einsatz im Bereich IT-Sicherheit entwickelt wurden. Ob beim Schutz digitaler Lieferketten, im Umgang mit Ransomware, beim Trainieren von Incident-Response-Prozessen oder zur Stärkung der persönlichen Awareness. Jedes Spiel verfolgt konkrete Lernziele und bringt dabei auf seine besondere Art Spaß, Interaktion und Erkenntnis zusammen.

Sie finden Informationen zu Spielabläufen, Zielgruppen, Einsatzmöglichkeiten – aber auch Hinweise zu Chancen und Grenzen dieser Methode. Denn so wirkungsvoll Serious Games sein können, sie sind kein Allheilmittel. Sie brauchen klare Ziele, eine sinnvolle Einbettung und den Mut, Neues zuzulassen.

Diese Broschüre lädt Sie ein, Serious Games als Impulsgeber zu entdecken: für Ihre Organisation, für Ihre Teams, für sich selbst. Denn wer spielt, lernt anders und oft nachhaltiger.

Wir wünschen Ihnen dabei Neugier, Inspiration und Spielfreude.

Prof. Dr. Ulrike Lechner
Professorin an der Universität der Bundeswehr München

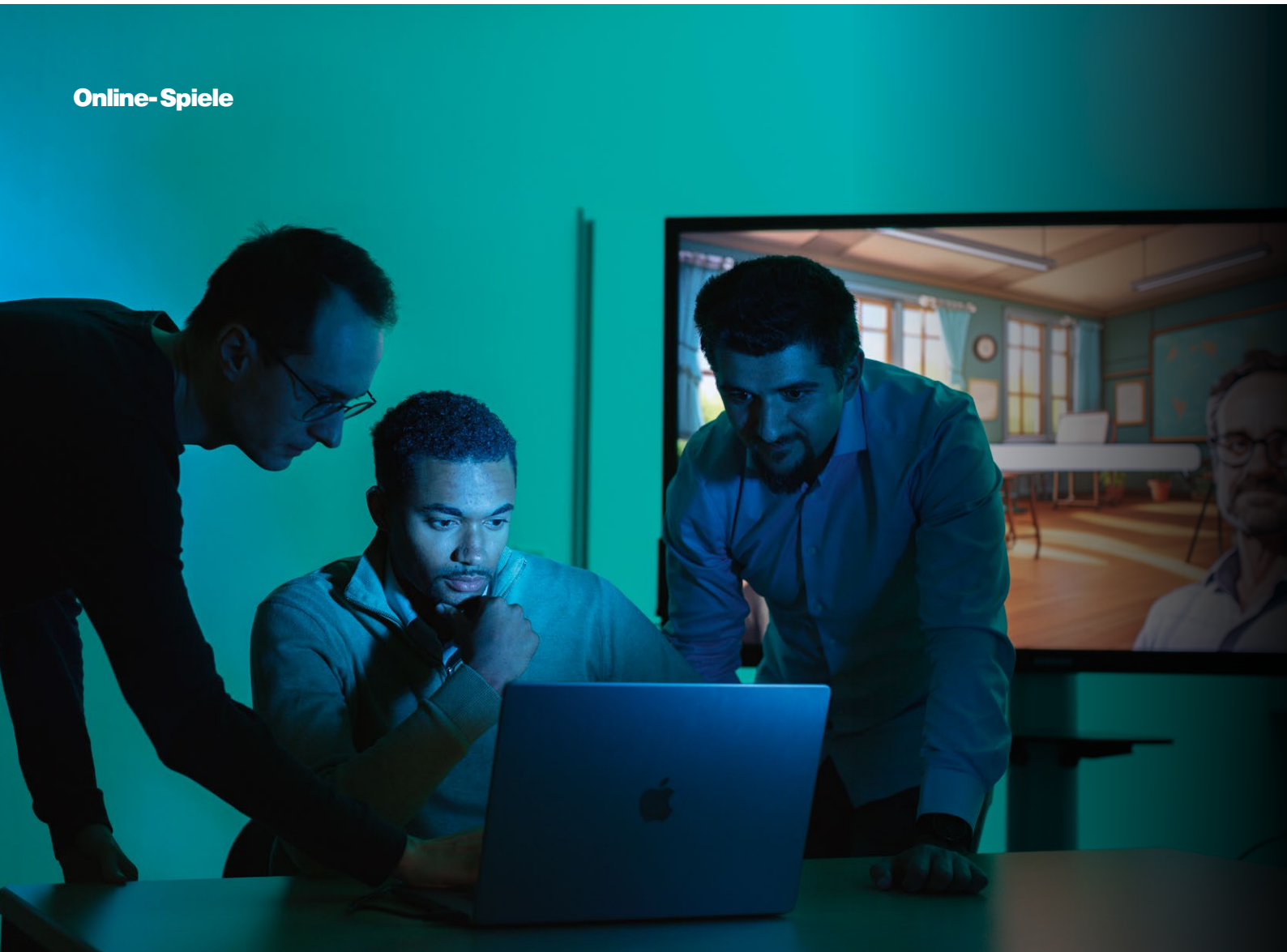
Warum Serious Games?

Chancen und Grenzen eines spielerischen Ansatzes

Serious Games – also Spiele mit ernstem Hintergrund wie einem Lern- oder Trainingszweck – haben sich im Bereich der IT-Sicherheit als erfolgreiche Methode etabliert, um komplexe Inhalte erlebbar zu machen, Kompetenzen wie Teamarbeit und Problemlösung zu fördern und das Interesse zu steigern. Sie finden Anwendung in der Schulung von Fachkräften, der Sensibilisierung von Mitarbeitenden sowie in der Identifikation von Schwachstellen, Bedrohungen und strategischen Handlungsfeldern innerhalb von Organisationen.

Zentrale Ziele beim Einsatz sind u. a. die Förderung von IT-Sicherheitskompetenzen, die realitätsnahe Vorbereitung auf Vorfälle (Incident Response), das Trainieren von Kommunikations- und Entscheidungsprozessen in Krisensituationen sowie die Entwicklung und Erprobung von Schutzstrategien. Serious Games lassen sich auch zur Simulation von Angriffsszenarien, zur Risikoanalyse oder zur Auswertung organisationaler Resilienz einsetzen.

Vorteile gegenüber klassischen Lernformaten liegen in der hohen Motivation, dem aktiven Involvement und der positiven emotionalen Einbindung der Spielenden. Studien zeigen, dass Spiele nicht nur den Lernerfolg steigern, sondern auch den Wissenstransfer in den Berufsalltag erleichtern. Die spielerische Auseinandersetzung mit Cyberbedrohungen stärkt zudem die Risikowahrnehmung und das Verantwortungsbewusstsein – auch bei Zielgruppen ohne technischen Hintergrund.



Brettspiele

Den Vorteilen stehen jedoch auch Herausforderungen gegenüber: Serious Games erfordern häufig organisatorischen Aufwand, insbesondere bei analogen Formaten mit begrenzter Teilnehmendenzahl. Auch die Entwicklung professioneller Spielmaterialien kann mit hohen Kosten verbunden sein. Zudem existieren nach wie vor Vorurteile gegenüber dem Einsatz spielerischer Methoden in sicherheitskritischen Kontexten – etwa die Annahme, Spiele seien „nicht ernst genug".

Trotz dieser Hürden belegen zahlreiche Studien das Potenzial von Serious Games als wirksames und zukunftsorientiertes Instrument in der IT-Sicherheitsbildung – vorausgesetzt, sie sind didaktisch fundiert, realitätsnah gestaltet und in bestehende Sicherheitsstrategien eingebettet.

Escape Room

Inhaltsverzeichnis

DuckDebugger Seite 08
Online Spiel

COPYCAT Seite 10
Escape Room

Digital Detectives Seite 12
Online Spiel

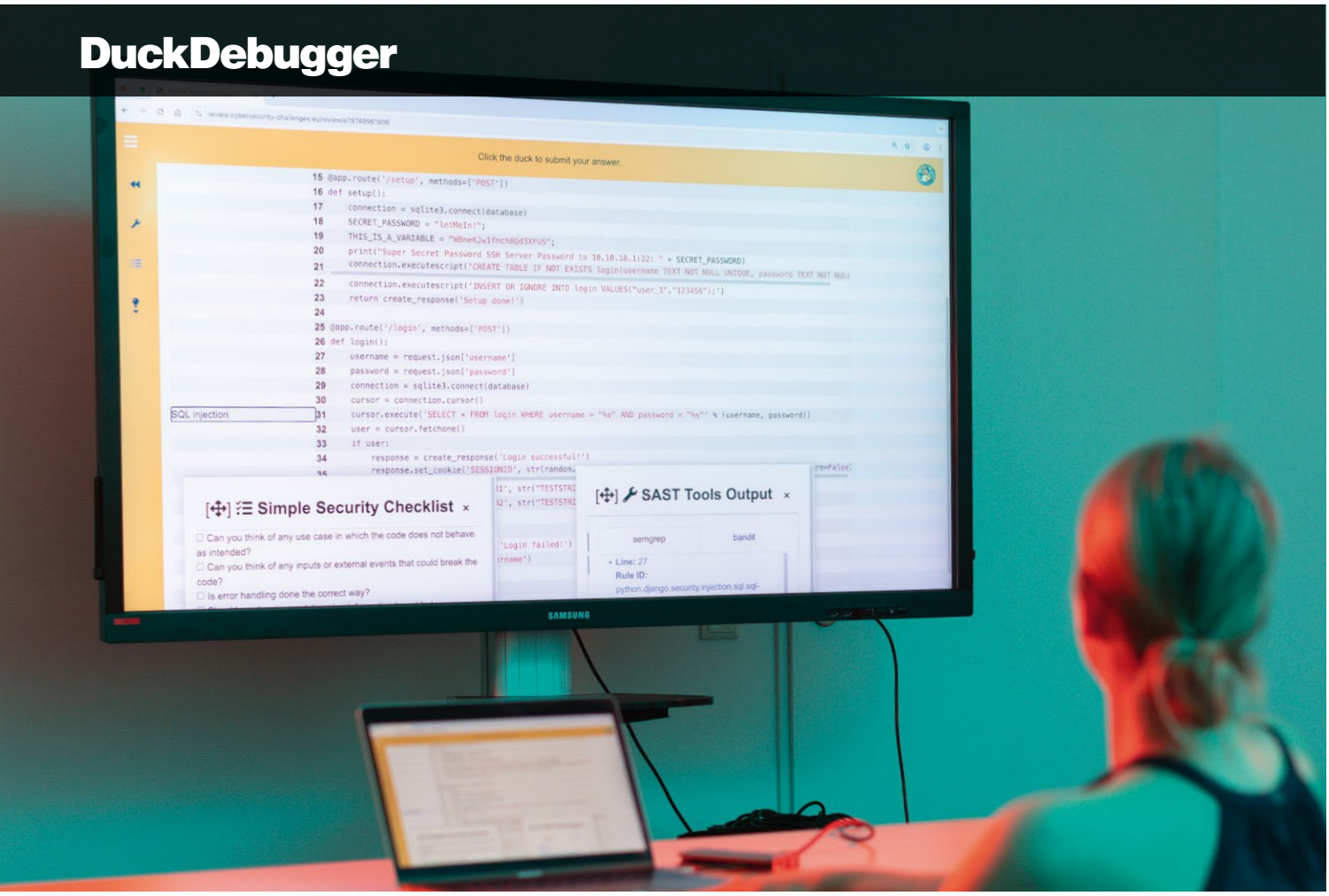
Operation Raven Seite 14
Brettspiel

Eine Frage der Sicherheit Seite 16
Brettspiel

Hack dich nicht! Seite 18
Brettspiel

Count2zero Seite 20
Escape Room

DuckDebugger



Code verstehen, Schwachstellen erkennen – spielerisch zur sicheren Software

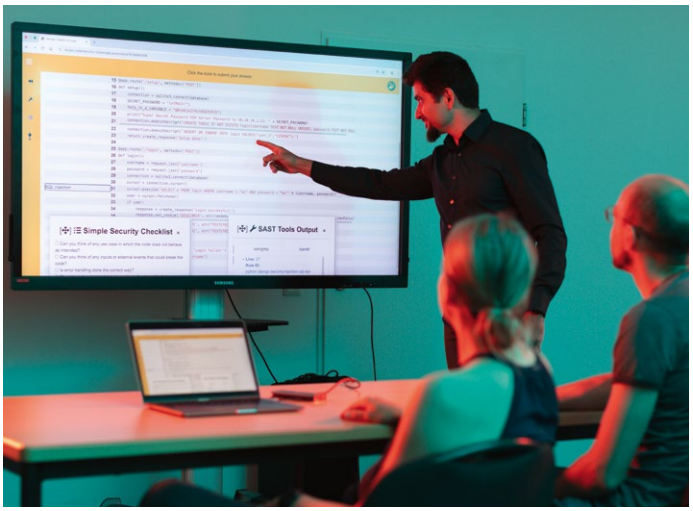
Sicherer Code beginnt im Kopf – und manchmal beim lauten Denken. In „DuckDebugger“ erleben Sie, wie aus Code-Reviews ein interaktives Spiel wird. Überraschend lehrreich. Unerwartet motivierend. Und verblüffend wirksam.

„DuckDebugger“ bringt Bewegung in den Code – und in den Kopf. Das Serious Game überträgt das Prinzip des „Rubber Duck Debugging“ in eine kollaborative Spielform, bei der Softwareentwickelnde gemeinsam Code analysieren, Probleme formulieren und Sicherheitsrisiken sichtbar machen.

In realitätsnahen Szenarien werden Codeausschnitte untersucht, potenzielle Schwachstellen identifiziert und Lösungen diskutiert. Dabei geht es nicht nur um Technik, sondern auch um Verständlichkeit, Verantwortung und Zusammenarbeit. Denn gute Software entsteht nicht im stillen Kämmerlein – sondern im Dialog.

Das Spiel lebt vom Perspektivwechsel: Durch das Aussprechen eigener Gedanken entstehen neue Einsichten, blinde Flecken werden erkannt, versteckte Lücken aufgedeckt. Genau das macht „DuckDebugger“ so besonders – es trainiert nicht nur Wissen, sondern Denkprozesse.

Erprobt wurde das Spiel bereits mit über 300 Entwickelnden in Unternehmen – mit durchweg positiver Resonanz. Die Verbindung aus spielerischer Reflexion, direktem Feedback und Teaminteraktion macht aus einer abstrakten Aufgabe ein echtes Lernerlebnis.



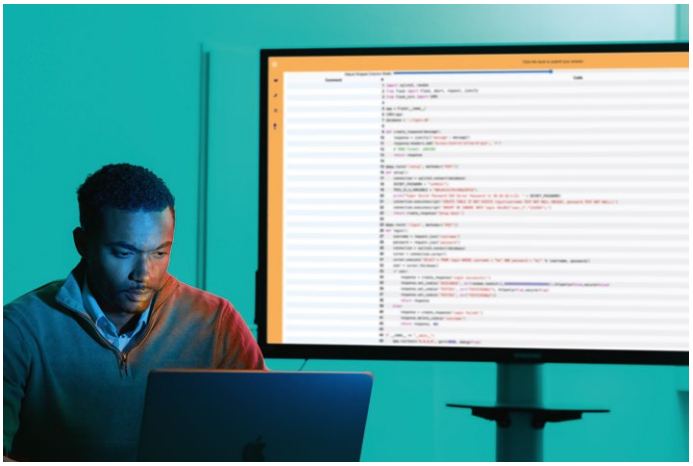
Ob als Teil eines Sicherheitstrainings, beim Onboarding oder zur Teamentwicklung – „DuckDebugger“ bringt neue Impulse in bestehende Entwicklungsprozesse. Und zeigt: Auch komplexe Themen dürfen Spaß machen – wenn man sie gut erklärt. Oder einfach laut darüber nachdenkt.

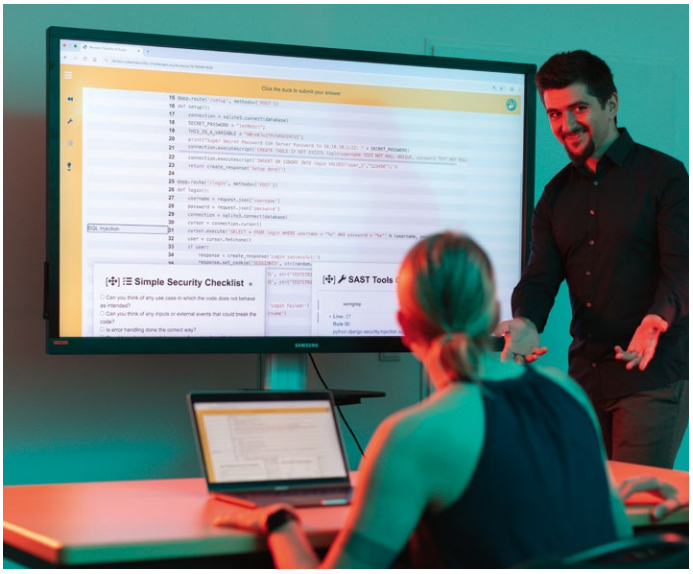
Motivation

„DuckDebugger“ eignet sich sowohl für Einsteiger als auch für erfahrene Entwicklerinnen und Entwickler, die ihre Fähigkeiten im Bereich der sicheren Softwareentwicklung vertiefen möchten.

In einer Zeit, in der Software-Sicherheit zunehmend an Bedeutung gewinnt, bietet „DuckDebugger“ einen innovativen Ansatz, um Entwicklerinnen und Entwickler für sicherheitsrelevante Aspekte zu sensibilisieren. Das Spiel fördert nicht nur das technische Verständnis, sondern auch die Kommunikation und Zusammenarbeit im Team – essenzielle Faktoren für erfolgreiche Code-Reviews.

Durch das spielerische Erleben von Sicherheitsherausforderungen werden abstrakte Konzepte greifbar und das Lernen nachhaltig gestaltet. „DuckDebugger“ zeigt, dass Sicherheit nicht trocken und theoretisch sein muss, sondern auch Spaß machen kann.





DuckDebugger

Projekt: DuckDebugger

Spielthema: Sicherheitsbewusste Code-Reviews durch spielerisches Reflektieren und Teamarbeit.

Zielgruppe: Softwareentwicklerinnen und -entwickler, IT-Sicherheitsbeauftragte, DevOps-Teams und alle, die sichere Software entwickeln möchten.

Format: Online – webbasiert und ohne zusätzliche Installation spielbar

Zahl der Spielenden pro Spielrunde: Flexibel – geeignet für Einzelspieler:innen und Teams

Spielrunden können angefragt werden: Ja – ideal für Workshops, Schulungen und Awareness-Kampagnen

Besonderheiten: „DuckDebugger“ verbindet bewährte Methoden des Code-Reviews mit spielerischen Elementen, um das Sicherheitsbewusstsein zu stärken. Durch interaktive Szenarien und unmittelbares Feedback wird das Lernen effektiv und nachhaltig gestaltet.

COPYCAT

Digitale Bedrohungen verstehen – Verteidigung aktiv trainieren

Ein Cyberangriff rollt heran – sind Sie vorbereitet? In „COPYCAT“ wird Cybersicherheit zur Teamsache. Interaktiv und herausfordernd – ein digitales Spiel, das Wissen und Intuition auf die Probe stellt.

Im digitalen Serious Game „COPYCAT“ stellen realistische Angriffsszenarien das strategische Denken und die Koordination der Spielenden auf die Probe. Wer hier als Gewinner hervorgehen will, muss im online verfügbaren Spiel umsichtig agieren und technische sowie organisatorische Maßnahmen zu einer klugen Verteidigungsstrategie kombinieren.

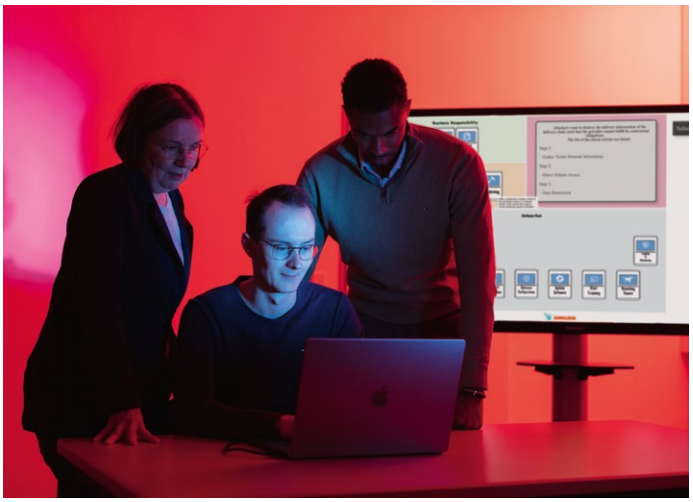
Ob als Einzelspiel oder im Team, die Teilnehmenden begegnen realen Angriffsszenarien auf die Software-Lieferkette – von manipulierten Updates bis zu kompromittierten Zulieferern nutzt das Spiel die Erkenntnisse des MITRE ATT&CK®-Frameworks. Mit Hilfe von Verteidigungskarten kombinieren Sie technische und organisatorische Maßnahmen, delegieren Aufgaben und treffen Entscheidungen mit Gewicht.

Das Spiel bringt Struktur und Dynamik zusammen: Angriff erkennen, passende Maßnahme finden, sinnvoll im Team verteilen – all das unter Druck und mit begrenzten Ressourcen. Wer zögert, verliert wertvolle Zeit. Wer gut plant, schützt Systeme, Daten und Reputationen.

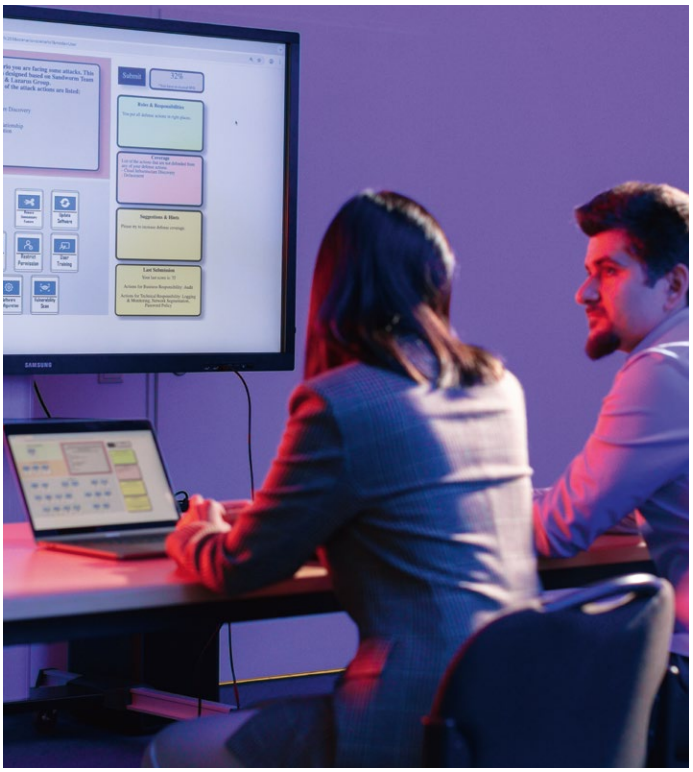
Motivation

COPYCAT lässt sich überall dort einsetzen, wo Cybersicherheit relevant ist – ob als Training für IT-Fachleute, Awareness-Spiel für gemischte Teams oder interaktives Element in Workshops.

Das Spiel vermittelt strategisches Denken, sensibilisiert für Angriffstechniken und stärkt das Verständnis für Rollen, Zuständigkeiten und Prozesse innerhalb sicherheitsrelevanter Organisationen. Es macht deutlich: Cybersicherheit ist Teamarbeit – und jede Entscheidung zählt.



COPYCAT



Projekt: COPYCAT

Spielthema: Verteidigungsstrategien in der Lieferkettensicherheit üben, Rollen und Verantwortlichkeiten kennenlernen.

Zielgruppe: Anwender/ Technische Experten/ Produktinhaber/ Produktmanager

Format: Online-Spiel

Zahl der Spielenden pro Spielrunde: Keine Begrenzung

Spielrunden können angefragt werden: Ja

Besonderheiten: Die Teilnehmenden benötigen einen Laptop mit Browser, um „COPYCAT“ zu spielen.

Digitale Spuren lesen, Angreifer entlarven – Forensik spielerisch erleben

Ein Cyberangriff erschüttert ein Unternehmen – Daten sind verschwunden, Systeme kompromittiert. In „Digital Detectives“ schlüpfen Sie in die Rolle eines digitalen Ermittlers und begeben sich auf die spannende Suche nach den Tätern.

„Digital Detectives“ ist ein Serious Game im Point-and-Click-Stil, das Sie in die Welt der digitalen Forensik entführt. Als Ermittler in einem fiktiven Unternehmen analysieren Sie einen realitätsnahen Cyberangriff: Sie durchsuchen virtuelle Räume, sammeln Beweise, identifizieren Schwachstellen und rekonstruieren den Tathergang.

Das Spiel kombiniert interaktive Szenarien mit Mini-Games, in denen Sie beispielsweise Netzwerkaktivitäten analysieren oder verschlüsselte Daten wiederherstellen. Dabei lernen Sie die vier Phasen der digitalen Forensik kennen: Identifikation, Sammlung, Analyse und Präsentation von Beweismitteln.

Die visuell ansprechende Gestaltung und die intuitive Benutzerführung machen „Digital Detectives“ sowohl für Einsteiger als auch für Fortgeschrittene zugänglich. Entwickelt wurde das Spiel auf Basis des Experiential-Gaming-Modells und des Event-Based-Learning-Modells, um ein effektives und motivierendes Lernerlebnis zu gewährleisten.

In einer zunehmend digitalisierten Welt sind Kenntnisse in der digitalen Forensik unerlässlich. „Digital Detectives“

vermittelt spielerisch, wie Cyberangriffe analysiert und aufgeklärt werden können. Das Spiel fördert nicht nur technisches Verständnis, sondern auch kritisches Denken und Problemlösungskompetenz.

Motivation

„Digital Detectives“ macht digitale Forensik greifbar und zeigt, wie aus technischen Details verwertbare Erkenntnisse werden. Besonders geeignet ist es für alle, die Cybersicherheit nicht nur verstehen, sondern selbst erleben wollen: für Studierende, IT-Nachwuchskräfte, Awareness-Programme, aber auch für Fachabteilungen ohne technischen Fokus. Wer mitspielt, entwickelt ein geschärftes Auge für digitale Spuren – und ein besseres Verständnis dafür, was Cyberaufklärung wirklich bedeutet.

Digital Detectives

Projekt: Digital Detectives

Spielthema: Erforschen Sie einen Cyberangriff auf ein fiktives Unternehmen und lernen Sie die Methoden der digitalen Forensik kennen – von der Beweissicherung bis zur Täteridentifikation.

Zielgruppe: Studierende, IT-Fachkräfte, Sicherheitsbeauftragte und alle, die ein Verständnis für digitale Forensik und Cybersicherheit entwickeln möchten.

Format: Online – spielbar im Webbrowser ohne zusätzliche Installation

Zahl der Spielenden pro Spielrunde: Einzelspieler

Spielrunden können angefragt werden: Ja – ideal für Workshops, Schulungen und Awareness-Kampagnen

Besonderheiten: Digital Detectives basiert auf realen Angriffsszenarien und vermittelt praxisrelevantes Wissen durch interaktive Elemente und Mini-Games. Die Kombination aus spielerischem Lernen und fachlicher Tiefe macht das Spiel zu einem effektiven Tool für die Aus- und Weiterbildung im Bereich der digitalen Forensik.

Operation Raven

Unter Strom: Ransomware in der Kritischen Infrastruktur!

Ein Cyberangriff trifft die Nerven eines Unternehmens – Systeme brechen weg, Entscheidungen müssen schnell getroffen werden. In „Operation Raven" erleben Sie genau diesen Moment. Und lernen dabei, was wirklich zählt.

„Operation Raven" bringt Sie an den Punkt, an dem aus IT-Theorie plötzlich Realität wird. Das analoge Planspiel simuliert einen gezielten Ransomware-Angriff auf ein Unternehmen der kritischen Infrastruktur. Sie übernehmen gemeinsam mit anderen die Rollen im Incident-Response-Team – vom technischen Betrieb bis zur Kommunikation mit Behörden und Öffentlichkeit.

In mehreren Spielrunden konfrontiert Sie der Spielleiter mit Herausforderungen die auf realen Frameworks wie MITRE ATT&CK®- und den NIST-Phasen basieren: kompromittierte Netzwerke, verschlüsselte Daten, kritische Entscheidungen. Ihr Ziel: Angriffe erkennen, eindämmen, beseitigen – und dabei den Betrieb wieder auf Kurs bringen.

Das Besondere: Die Rollen sind nicht rein technisch gedacht. Auch Management, Datenschutz, Recht und Kommunikation sind Teil des Spiels – denn im Ernstfall zählt jeder Kontaktpunkt. Auf dem Response-Board entwickeln Sie gemeinsam einen Aktionsplan. Sie erleben, wie wertvoll abgestimmte Kommunikation, klares Handeln und strategisches Denken unter Druck sind – ganz ohne reales Risiko, aber mit vollem Lerneffekt.

Motivation

„Operation Raven" ist ein Training, das sich anfühlt wie ein echter Krisenmoment – nur ohne die negativen Folgen. Es macht spürbar, wie Cyberangriffe ablaufen, wie komplex die Zusammenarbeit wird – und wie entscheidend gute Vorbereitung ist.

Besonders geeignet ist das Spiel für Teams aus kritischen Infrastrukturen und sensiblen Unternehmen, die bei einem echten Vorfall zusammenarbeiten müssen: CERTs, SOCs, IT-Sicherheit, aber auch Leitungsebenen. Wer spielt, erkennt nicht nur technische Schwachstellen, sondern auch Lücken in Kommunikation und Strategie. Und vor allem: wie sie sich schließen lassen.

Operation Raven

Projekt: Operation Raven

Spielthema: Die Bewältigung eines Ransomware-Angriffs auf die IT-Systeme einer Kritischen Infrastruktur. Spieler übernehmen die Rollen eines Incident-Response-Teams und trainieren Erkennung, Eindämmung und Beseitigung von Cyberbedrohungen.

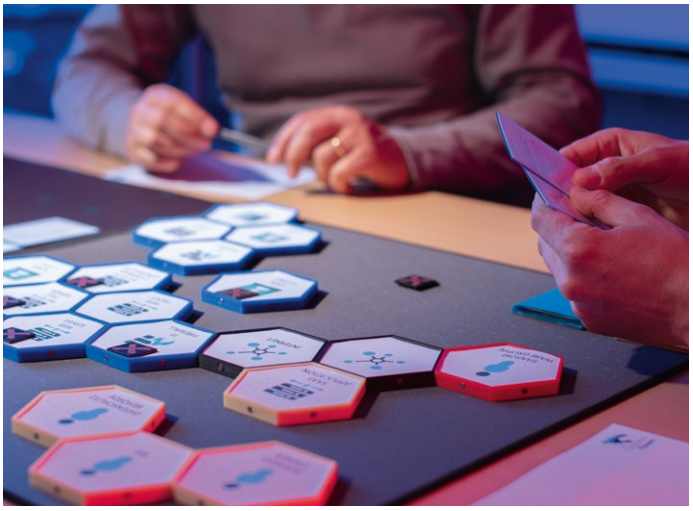
Zielgruppe: Fach- und Führungskräfte aus CERTs/ SOCs/ IT-Abteilungen/ Krisenstäben und sicherheitsrelevanten Bereichen – besonders geeignet für Organisationen mit kritischer Infrastruktur.

Format: Analog

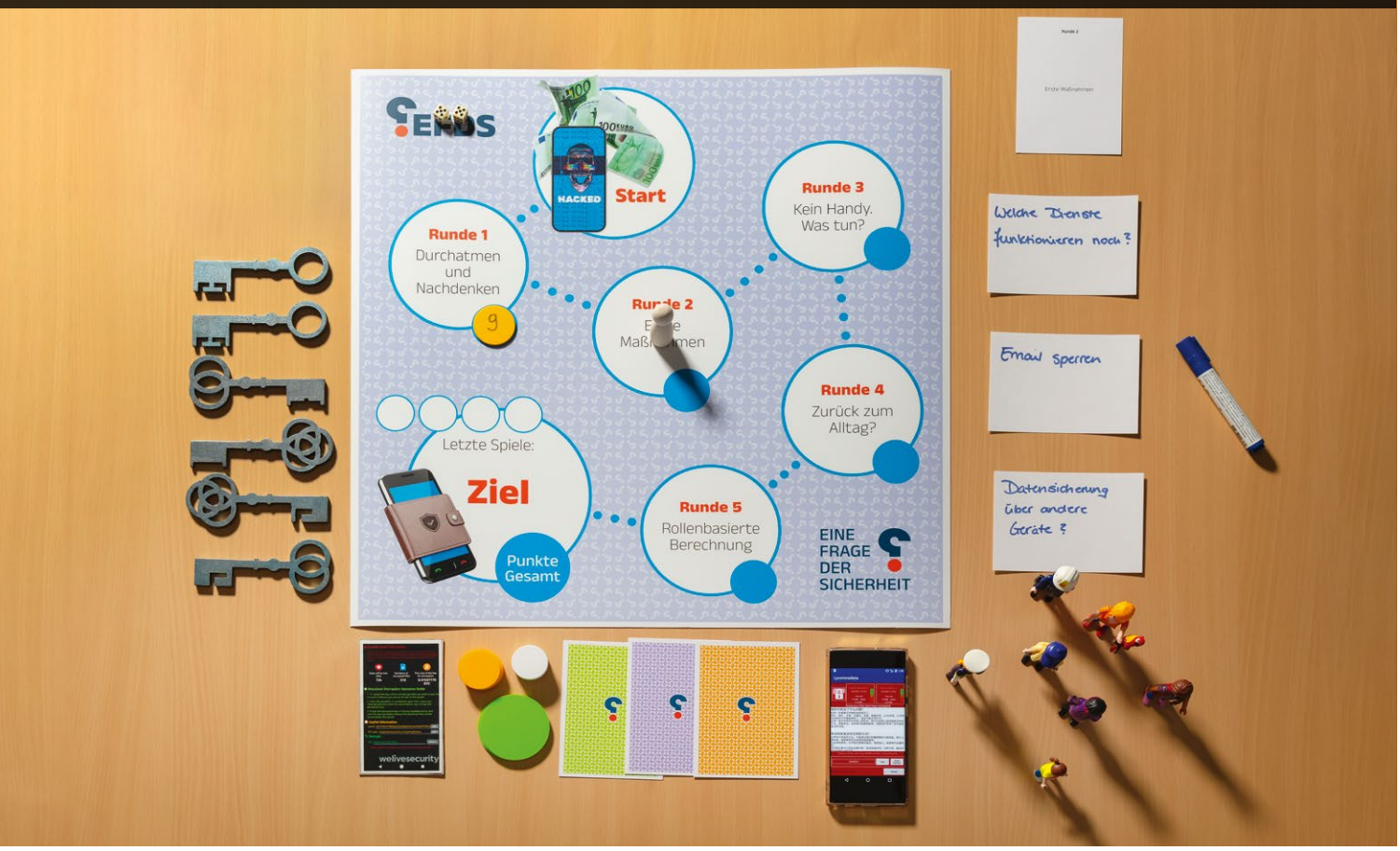
Zahl der Spielenden pro Spielrunde: Von 2 bis 5 Spielern pro Gruppe (mehrere Gruppen parallel möglich)

Spielrunden können angefragt werden: Ja

Besonderheiten: Realitätsnahe Spielinhalte basieren auf echten Bedrohungsszenarien, MITRE ATT&CK®-Framework und NIST-Standards. Anpassbar an verschiedene Infrastrukturen, sehr gut geeignet zur Erstellung konkreter Playbooks. Ein Spielleiter führt durch das Szenario.



Eine Frage der Sicherheit



Ransomware auf dem Smartphone – was nun? Entscheide klug, denn die Uhr läuft

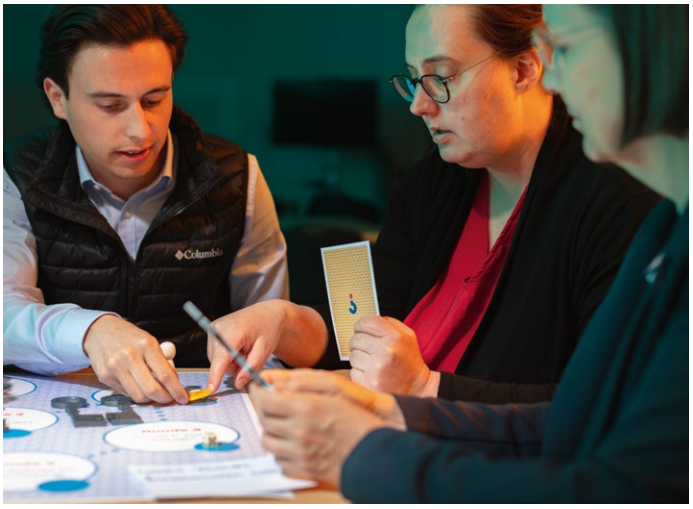
„Eine Frage der Sicherheit“ ist ein analoges Serious Game, das sich einem sehr realen Albtraum widmet: Ein Ransomware-Angriff auf das eigene Smartphone – und das mitten im Arbeitsalltag. Spielende schlüpfen in die Rolle betroffener Mitarbeitender in einem KMU und entwickeln Schritt für Schritt ihre Strategie zur Bewältigung der Krise.

Das Spiel folgt einem klar strukturierten Ablauf über fünf Runden – von der ersten Schockreaktion über konkrete Maßnahmen bis zur Nachbereitung und Bewertung. Die Spielenden stellen sich Fragen wie: „Wen muss ich informieren?“, „Was darf ich tun?“, „Welche Daten sind gefährdet?“ und „Wie komme ich wieder arbeitsfähig zurück?“ – stets begleitet von einem Spielleitenden, der als Sicherheitsinstanz die passenden Antworten liefert.

Ein besonderes Highlight: In der letzten Runde schlüpfen die Spielenden in die Perspektive von Betroffenen wie Kolleg:innen, Familie, Datenschutz oder Management und bewerten gemeinsam den Krisenverlauf. Zusätzliche Rätsel und Spielmaterialien wie Spielfiguren, Würfel, Punktetafeln und Karten machen das Spiel zu einem immersiven Erlebnis, das sowohl zum Nachdenken als auch zum Diskutieren einlädt.

„Eine Frage der Sicherheit“ hilft Menschen ohne technischen Hintergrund, das komplexe Thema Ransomware greifbar zu machen. Durch die Verbindung aus Storytelling, Teamarbeit und Escape-Game Rätseln lernen die Spielenden, wie man in einem echten Vorfall besonnen und zielgerichtet handelt.

Dabei geht es nicht nur um Technik – sondern um Verantwortung, Kommunikation und die richtigen Fragen zur richtigen Zeit. Das Spiel stärkt das Sicherheitsbewusstsein und schafft Raum für neue Perspektiven – ein echter Mehrwert für Organisationen und Teams, die sich gegen digitale Risiken wappnen wollen.



Motivation

„Eine Frage der Sicherheit“ hilft Menschen ohne technischen Hintergrund, das komplexe Thema Ransomware zu verstehen und ihren persönlichen Notfallplan zu erarbeiten. Auch Informationssicherheits-Experten profitieren von den Spielrunden, weil sie spielerisch eigene Prozesse durchgehen und überprüfen können. Durch die Verbindung aus Storytelling, Teamarbeit und Escape-Game Rätseln lernen die Spielenden, in einem echten Vorfall besonnen und zielgerichtet zu handeln.

Dabei geht es längst nicht nur um Technik, entscheidend sind Teamarbeit und die richtigen Fragen zur richtigen Zeit. Das Spiel stärkt das Sicherheitsbewusstsein und schafft Raum für neue Perspektiven – ein echter Mehrwert für Organisationen und Teams, die sich gegen digitale Risiken wappnen wollen.

Projekt: EFDS – Eine Frage der Sicherheit

Spielthema: Ransomware auf dem Smartphone – ein Szenario, das viele betrifft. Das Spiel zeigt, wie man sich Schritt für Schritt zurück in den Normalbetrieb kämpft – mit klaren Fragen, guten Entscheidungen und Teamgeist.

Zielgruppe: Mitarbeitende ohne vertiefte IT-Kenntnisse, Sicherheitsbeauftragte, Awareness-Teams – ideal für Teams, die gemeinsam lernen wollen.

Format: Analog – Tischspiel mit Karten, Spielfiguren und moderierter Spielleitung

Zahl der Spielenden pro Spielrunde: Von 3 bis 8

Spielrunden können angefragt werden: Ja – besonders geeignet für Awareness-Workshops, Schulungen oder Teamevents

Besonderheiten: „Eine Frage der Sicherheit“ kombiniert spielerisches Lernen mit tiefgehender Reflexion. Es eignet sich besonders für Organisationen, die praxisnah für Cybervorfälle sensibilisieren wollen – ohne Fachjargon, aber mit Substanz.

Hack dich nicht!

Cyberangriff auf die Logistik? Reagieren, verteidigen, weiterfahren!

Ein Cyberangriff trifft die Lieferkette – Stillstand droht. In „Hack dich nicht" navigieren Sie Ihr Logistikunternehmen durch ein digitales Krisenszenario – mit Taktik, Teamgeist und einem kühlen Kopf.

„Hack dich nicht" ist ein analoges Serious Game, das Cybersicherheit mit logistischer Krisenresilienz verknüpft. Das Spiel versetzt die Teilnehmenden in die Rolle eines Spediteurs, dessen Unternehmen von einem Ransomware-Angriff betroffen ist. Das Ziel: trotz der Angriffe den Betrieb aufrechterhalten und die eigenen Spielfiguren – also das Unternehmen – sicher ins Ziel bringen.

Der Spielverlauf konfrontiert die Gruppe mit realitätsnahen Bedrohungen. Durch das Aufdecken von Angriffskarten entstehen unvorhersehbare Szenarien, auf die mit Verteidigungs- und Ressourcenkarten reagiert werden muss. Die Entscheidungen betreffen nicht nur technische Maßnahmen, sondern auch die Priorisierung von Kommunikation, Datenschutz und finanzielle Entscheidungen.

Die Spielmechanik fördert spontanes Handeln, vorausschauende Planung und gemeinsames Taktieren. Die Spielenden lernen nicht nur mehr über Angriffsarten und Sicherheitsmaßnahmen, sondern reflektieren auch ihre eigenen Reaktionsmuster – im Vergleich mit den Strategien anderer. Das Ergebnis: ein dynamisches und lehrreiches Erlebnis, das Sicherheit nicht als Hürde, sondern als Erfolgsfaktor vermittelt.

Ob im Rahmen einer Awareness-Schulung oder als Planspiel – „Hack dich nicht“ zeigt: Wer vorbereitet ist, kommt sicher an.

Motivation

„Hack dich nicht“ macht spürbar, was digitale Angriffe in der realen Welt bedeuten – nämlich Chaos in der Logistik, unterbrochene Lieferketten und plötzlich drängende Entscheidungen. Wer mitspielt, erlebt, wie rasch sich ein Cybervorfall auf Betriebsabläufe auswirkt und wie wichtig kluge, koordinierte Reaktionen sind.
Besonders geeignet ist das Spiel für Mitarbeitende aus Logistik, IT, Krisenstab, Supply Chain Management sowie für interdisziplinäre Teams, die gemeinsam lernen wollen, unter Druck handlungsfähig zu bleiben. Das Spiel stärkt das Verständnis für Zusammenhänge, fördert das Sicherheitsbewusstsein und eröffnet wertvolle Einblicke in die eigenen Reaktionsmuster. So entsteht nicht nur Wissen, sondern Widerstandsfähigkeit.

Hack dich nicht!

Projekt: Hack dich nicht!

Spielthema: Ein Ransomware-Angriff bedroht die Lieferkette. Wer führt sein Logistikunternehmen trotz massiver Störungen sicher ins Ziel? Ein Spiel über digitale Bedrohungen – und den richtigen Umgang damit.

Zielgruppe: Teams aus Logistik, Transport, IT, Management oder Sicherheit – sowie alle, die Lieferketten verstehen und schützen wollen.

Format: Analoges Planspiel mit Karten, Spielfeld und moderierter Anleitung

Zahl der Spielenden pro Spielrunde: Von 2 bis 6

Spielrunden können angefragt werden: Ja – geeignet für Trainings, Workshops oder Awareness-Maßnahmen

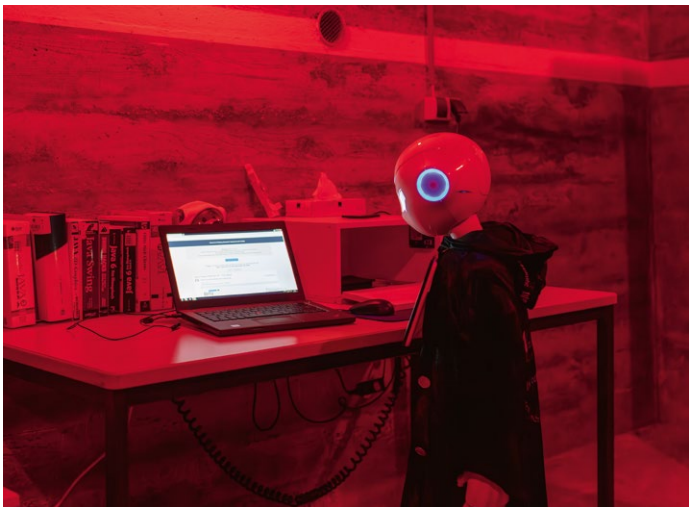
Besonderheiten: Das Spiel vermittelt Cybersicherheit praxisnah durch Spielmechanik, Reflexion und Teaminteraktion. Spontane Ereignisse, taktische Entscheidungen und echte Aha-Momente machen „Hack dich nicht“ zu einem Erlebnis mit echtem Mehrwert.

Auf Spurensuche im Bunker

Alte Gemäuer, neue Technik und herausfordernde Rätsel: das Escape-Room Game „count2zero" führt tief hinunter in den Luftschutzbunker und lässt das Herz aller Escape-Room Fans höherschlagen. Der Wissenszuwachs in Sachen IT-Security ist garantiert.

Alte Gemäuer, neue Technik und herausfordernde Rätsel: das Escape-Room Game „count2zero" führt tief hinunter in einen Luftschutzbunker im oberbayerischen Erding und lässt das Herz aller Escape-Room Fans höherschlagen. Der Wissenszuwachs in Sachen IT-Security ist ebenso garantiert wie Spielspaß und ein Teamerlebnis, das im Gedächtnis bleibt.

Die schwere Metalltür des ehemaligen Luftschutzbunkers fällt ins Schloss und der Timer beginnt rückwärtszulaufen, „count2zero" eben. Doch wie schnell die Zeit wirklich vergeht, merkt man in diesem Escape Room gar nicht, denn schon halten einen die ersten Rätsel in Schach. Das Briefing, welches die Spielenden zu Beginn erhalten, weist auf eine unklare, aber ernste Bedrohungslage hin, es besteht dringender Handlungsbedarf. Gut, dass das Team aus bis zu fünf Spielenden schon vor Ort ist und gleich loslegen kann! Zum Ausruhen bleibt auch keine Zeit, denn viele Meter unter der Erde auf sich allein gestellt, werden die eigenen kombinatorischen Fähigkeiten ebenso auf eine harte Probe gestellt wie die Fingerfertigkeiten und der Umgang mit moderner Technik. Auf der fieberhaften Suche nach einer Möglichkeit, der Lage Herr zu werden, begegnen dem Team PCs, Sensorik, Robotik und IoT-Kom-



ponenten, alles was auch der Alltag in ähnlicher Weise zu bieten hat. Wie diese Puzzleteile zusammenspielen, ist dabei zunächst ein Rätsel für sich. Die Zusammenhänge werden erst nach und nach klar, während sich die Ziffern des Countdown-Timers unerbittlich immer weiter der Null annähern. Derweil gilt es, die richtigen Schlüsse zu ziehen, sicherheitsrelevante Probleme zu erkennen, Informationen korrekt zu interpretieren und als Team eine Lösung zu entwickeln. Ob es dem Team gelingt, das Rennen gegen die Uhr zu gewinnen? Denn auch wenn die Aufgaben zunächst spielerisch wirken, werden in der einzigartigen Atmosphäre des alten Bunkers reale und aktuelle Bedrohungen der IT-Sicherheit durchgespielt.

Motivation

Kompromittierte Systeme fehlerhafte Zugangskontrollen, verborgene Hackeraktionen, intelligenten Datenanalysen – „count2zero" fördert technisches Verständnis, Teamkommunikation und ein geschärftes Verantwortungsbewusstsein im digitalen Raum. Durch intensive Erleben im Team werden Inhalte nachhaltig verankert.
Das Escape Game stärkt das Bewusstsein für IT-Sicherheit und sensibilisiert praxisnah für digitale Risiken. Es vermittelt grundlegende Prinzipien der Cyber-Sicherheit, wie den sicheren Umgang mit Passwörtern, die Risiken unbekannter USB-Geräte oder das Erkennen von Phishing-Versuchen. Gleichzeitig fördert es den Teamgeist und zeigt, wie wichtig klare Kommunikation und koordiniertes Handeln im Ernstfall sind.
Durch die immersive Spielerfahrung im Escape Room lernen die Teilnehmenden nicht nur, technische Herausforderungen analytisch zu durchdringen und systematisch anzugehen, sondern diese auch gemeinsam im Team zu lösen. Dabei rücken neben Fachwissen auch Verantwortungsbewusstsein und die Fähigkeit zum entschlossenen Handeln in den Mittelpunkt – Kompetenzen, die für den Schutz unserer digitalen Welt unverzichtbar sind.

count2zero

Projekt: count2zero

Spielthema: Ausgestattet mit moderner Technik, vermittelt der Escape Room in einem Bunker grundlegende Prinzipien der Cyber-Sicherheit und stärkt die Zusammenarbeit unter den Spielenden.

Zielgruppe: Soldaten/ Anwender/ Führungsebene

Format: Analog

Zahl der Spielenden pro Spielrunde: Von 3 bis 5

Spielrunden können angefragt werden: Ja

Besonderheiten: Der Escape Room befindet sich am WIWeB in Erding und kann ausschließlich dort gespielt werden.

Spielentwicklung

DuckDebugger:	Andrei-Cristian Iosif
CopyCat:	Tiange Zhao
Digital Detectives:	Sabrina Meindl, Tobias Reittinger
Operation Raven:	Andreas Seiler
Eine Frage der Sicherheit:	Judith Strußenberg
Hack dich nicht!.	Michael Schuster, Sonja Marquart, Jakob Kroen, Jason Schwabe, Linus Rau, Damian Stano, Florian Hermann, Julian Zengler, Lukas Sehorz
count2zero:	Markus Rebhan

Impressum

1. Auflage, 2025
© Alle Rechte vorbehalten.

Herausgeberin: Prof. Dr. Ulrike Lechner

Die Broschüre ist erstellt vom deutsch-österreichischen Forschungsprojekt „Effiziente Reaktion auf IT-Sicherheitsvorfälle in transnationalen Lieferketten (CONTAIN)“.

Auf deutscher Seite wird das Projekt CONTAIN innerhalb des Programms Forschung für die zivile Sicherheit vom Bundesministerium für Forschung, Technologie und Raumfahrt (BMFTR) gefördert (FKZ 13N16581-13N16587); auf Österreichischer Seite wird CONTAIN innerhalb des Sicherheitsforschungs-Förderprogramms KIRAS gefördert (FO999902707).

Sprecherin des Gesamtprojekts:
Prof. Dr. Ulrike Lechner

Projektleitung CONTAIN Deutschland:
Dr. Steffi Rudel (Universität der Bundeswehr München)

Projektleitung CONTAIN Österreich:
Dr. Stefan Schauer (Austrian Institute of Technology AIT)

Projektleitung und Autorenschaft der Broschüre:
Judith Strußenberg

Mitwirkende:
Fotograf: Martin Bolle - https://martinbolle.de
Lektorat: Prof. Dr. Ulrike Lechner und Maximilian Greiner
Design: Artes Advertising GmbH, München
Druck und buchbinderische Verarbeitung:
Rechenzentrum der Universität der Bundeswehr München

contain

Gefördert von

Bundesministerium für Forschung, Technologie und Raumfahrt

SIFO.de

FFG Forschung wirkt.

KIRAS Sicherheitsforschung

Bundesministerium Finanzen