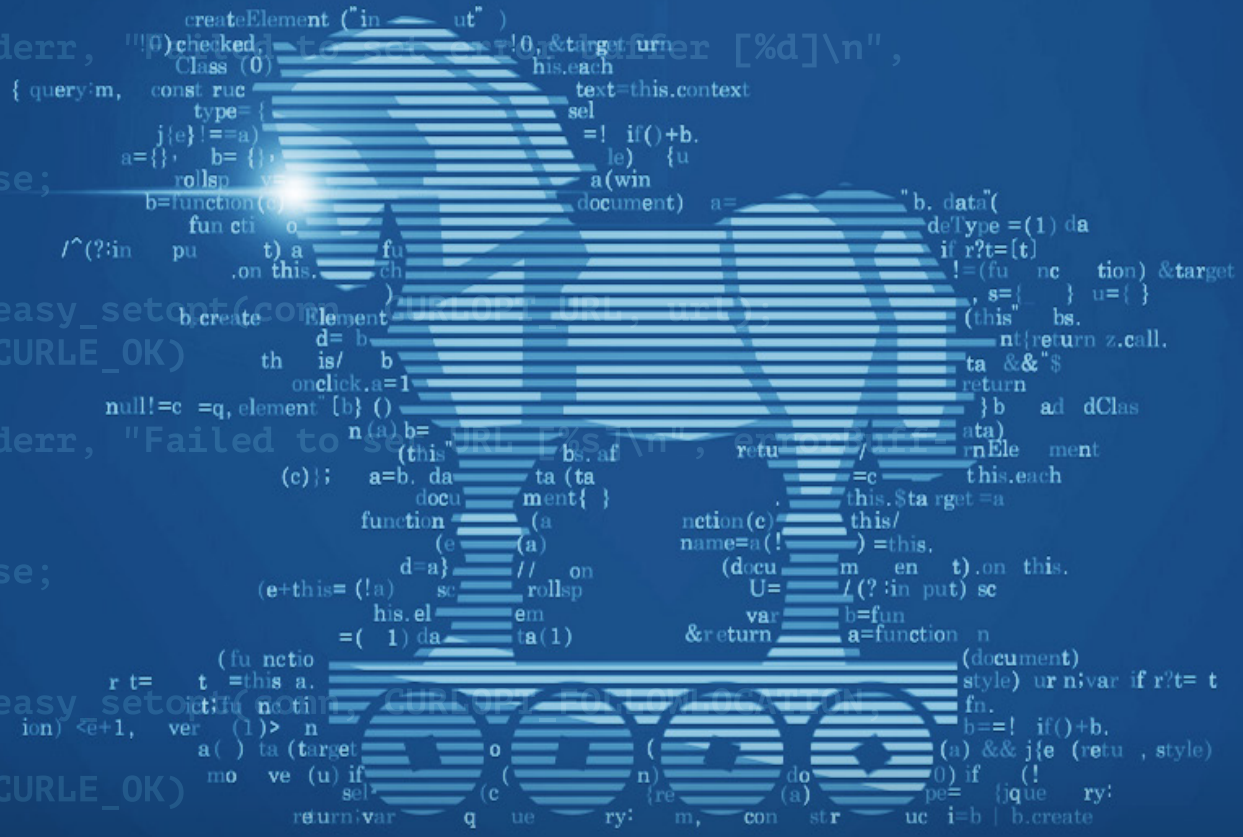
MHP
A PORSCHE COMPANY



CYBER SECURITY USE CASES

Beispiele aus der Praxis: Wie Sie Ihre Daten richtig schützen

Cyber Security in der Praxis: Darknet-Analyse und Kompetenz

Cyber Security hat viele Facetten. Es gibt nicht nur eine Vielzahl von Angriffsvektoren, die sich Kriminelle mit unterschiedlichen Motiven zunutze machen. Es gibt zahlreiche Ansätze für die präventive Risikobehandlung und die reaktive Vorfallsbehandlung. Den Status quo in Deutschland skizzieren wir in unserem Cyber-Security-Risk-Report, den wir gemeinsam mit dem Landeskriminalamt Baden-Württemberg erstellt haben.

Darin formulieren wir auch acht grundsätzliche Handlungsempfehlungen. Wie Unternehmen diese Empfehlungen umsetzen können, illustrieren wir anhand von zwei Use Cases. Diese können zum einen in dieser Form im eigenen Unternehmen etabliert werden. Zum anderen dienen sie als Blueprints für Aktivitäten zu anderen Cyber-Security-Aspekten.

Wir wünschen eine interessante Lektüre!

USE CASE 1

DARKNET-ANALYSE

Zu den problematischsten Cyber-Security-Risiken gehören gestohlene unternehmensinterne Daten, die über das Darknet angeboten werden. Diese Daten sind nicht selten Grundlage für eine Reihe weiterer krimineller Aktivitäten. Dritte können sich beispielsweise mithilfe von ausgespähten Nutzernamen und Passwörtern jederzeit Zugriff auf IT-Systeme verschaffen und entwendete Kundendaten beispielsweise für Erpressung nutzen.

Ein wirksamer Schutz gegen die Bedrohung aus dem Netz stellen präventive Maßnahmen dar. Angesichts des rasant zunehmenden digitalen Datenaustauschs wird das aber immer schwieriger. Allein die Tatsache, dass während der Corona-Pandemie die Menge an Fernzugriffen vom Homeoffice aus förmlich explodiert ist, hat kriminellen Hacker*innen unendliche viele Türen geöffnet. Aus diesem Grund empfiehlt es sich ergänzend zum Schutz der Daten, das Darknet kontinuierlich nach eigenen Daten zu durchsuchen, diese einwandfrei als illegal zu identifizieren und dann Gegenmaßnahmen zu treffen. MHP führt gemeinsam mit einem Partner Darknet-Analysen bei Unternehmen durch und hilft so dabei, dass kriminelle Aktivitäten möglichst frühzeitig erkannt werden.

Was ist das Darknet?

Metaphorisch gesprochen ist das Darknet das Sin City des Internets. Aus technologischer Sicht gibt es nicht das eine Darknet, sondern etliche Darknets. Diese sind als Peer-to-Peer-Overlay-Netzwerk realisiert, bei dem die Teilnehmenden die Verbindungen manuell herstellen. Die Webseiten dieser Peer-to-Peer-Overlay-Netzwerke werden nicht von Suchmaschinen indiziert. Zudem werden meist nicht standardisierte Kommunikationsprotokolle verwendet. Der Zugriff ist nicht mit herkömmlichen Browsern möglich, sondern nur mit spezieller Software. Der Zugang erfolgt zum Beispiel über das Tor-Netzwerk mit dem Tor-Browser.

All das bedeutet: Wer sich im Darknet bewegt, bewegt sich tatsächlich anonym. Vorteilhaft ist das für Nutzer*innen aus Ländern, in denen das Internet eingeschränkt ist oder überwacht wird, weil sie auf diesem Weg leichter an Informationen aus anderen Ländern kommen und ihre Meinung äußern können, ohne Repressalien befürchten zu müssen. Gleichzeitig zieht die Anonymität auch Kriminelle an, da diese im Darknet schwerer auffindbar und damit sicherer vor Strafverfolgungen sind.

Vorgehensweise von MHP

Im Zuge der Darknet-Analyse werden im ersten Schritt Interviews mit Verantwortlichen der betroffenen Fachbereiche geführt und Workshops mit ihnen veranstaltet, um so die relevanten Assets zu definieren. Die Relevanz ergibt sich dabei aus der Kritikalität eines Assets für den einen Fachbereich beziehungsweise für das gesamte Unternehmen. Anschließend werden im zweiten Schritt repräsentative Schlüsselbegriffe für jedes definierte Asset festgelegt. Diese Schlüsselbegriffe bilden die Basis für die Suche nach gestohlenen Daten im Darknet, die als dritter Schritt durchgeführt wird. Das Ergebnis der Suche zeigt Daten, die im Darknet kostenlos zur Verfügung stehen oder zum Kauf angeboten werden, obwohl sie schützenswerte Informationen enthalten.

Aus den Resultaten zieht MHP im vierten Schritt Rückschlüsse auf konkrete Bedrohungsszenarien für das Unternehmen. Beispielsweise bedeutet eine zum Kauf angebotene Liste mit Passwörtern zu Unternehmens-E-Mail-Adressen, dass sich Akteure bereits Zugriff zum Unternehmensnetzwerk verschafft haben. Aufgrund einer zeitlichen Einordnung, ermittelbar durch Indikatoren wie die Aktualität der Passwortliste oder das Datum des ersten Erscheinens im Darknet, lässt sich wiederum ableiten, wann der Zugriff stattgefunden haben könnte. Ein solches und weitere Bedrohungsszenarien werden auf einer Skala hinsichtlich der Schadenshöhe und Eintrittswahrscheinlichkeit für das jeweilige Unternehmen eingeordnet. Für alle Bedrohungsszenarien werden schließlich im fünften Schritt kurzfristige operative und strategisch langfristige Maßnahmen für die präventive Risikobehandlung und die reaktive Vorfallsbehandlung entwickelt.

Beim Passwortlisten-Beispiel wären das die sofortige Änderung aller Passwörter, eine Netzwerkanalyse, um Schadsoftware zu identifizieren und zu isolieren und in langfristiger Sicht die Planung und Durchführung regelmäßige Aktivitäten zur Steigerung der Kompetenz der Mitarbeiter*innen.

Grundsätzlich sollte eine Darknet-Analyse nicht als singuläres Ereignis aufgefasst werden, sondern im Rahmen einer übergreifenden Cyber-Security-Strategie jährlich, halbjährlich, quartalsweise oder monatliche durchgeführt werden – abhängig von der Unternehmensgröße und der Kritikalität der Assets. Auf diese Weise wird nicht nur sichergestellt, dass eventuell gestohlene Daten rasch aus dem Darknet entfernt oder geeignete Gegenmaßnahmen ergriffen werden können. Die Darknet-Analyse hilft außerdem, die Wirksamkeit der Maßnahmen zu präventiven Risikobehandlung zu beurteilen und kontinuierlich weiterzuentwickeln.

Darknet-Analyse
VORGEHEN

SCOPE DARKNET-ANALYSE

- Festlegung Scope Darknet-Analyse
- Aufnahme & Clusterung von unternehmensspezifischen Assets
- Bewertung der Assets
- Definition der unternehmensspezifischen Keywords

→ **Definierter Scope, Assets & Keywords**

DARKNET RESEARCH

- Erstellung eines detaillierten Berichts zu den Findings
- Auswertung der Findings in einem Dashboard

→ **Identifizierte & strukturierte Findings**

BEDROHUNGS-SZENARIEN

- Definition von Bedrohungsszenarien entsprechend der Findings, unter Beachtung der Eintrittstiefe
- Priorisieren der bewerteten Bedrohungsszenarien gewichtet nach Eintrittswahrscheinlichkeit und Schadenspotential

→ **Bewertete & priorisierte Bedrohungsszenarien**

REAKTIONS-SZENARIEN

- Ableitung von kurzfristigen Reaktionsszenarien

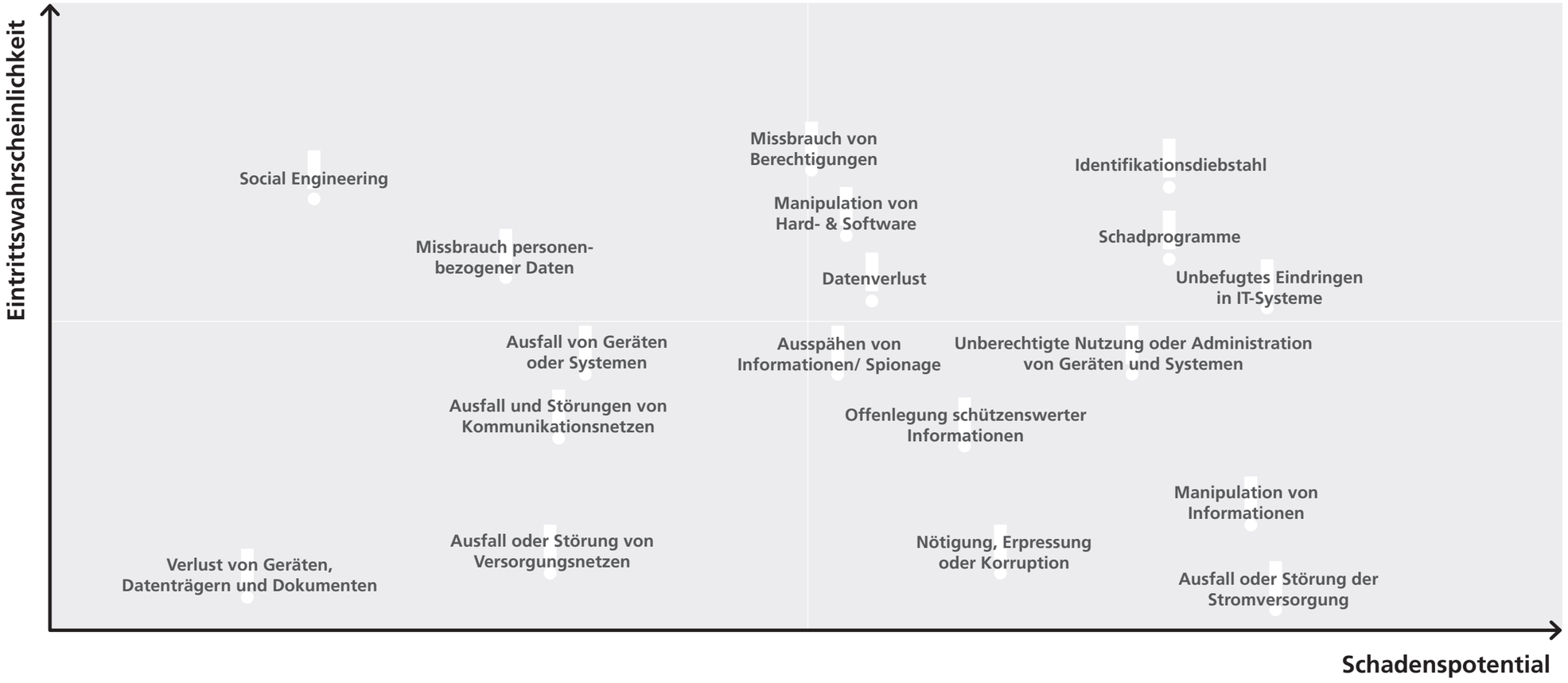
→ **Bewertete & priorisierte Reaktionsszenarien**

MASSNAHMEN-UMSETZUNG

- Gemeinsame Ableitung konkreter Handlungsfelder & Maßnahmen zur zukünftigen Cyber-Fitness

→ **Kurz- und langfristige Handlungsfelder**

Ergebnis Darknet-Analyse
BEDROHUNGSSZENARIEN



Beispielhafte Bewertung
Bewertung wird nach Analyse der
Findings angepasst

USE CASE 2

MASSNAHMEN ZUR VERBESSERUNG DER CYBER-SECURITY-KOMPETENZ

Viele Cyber-Attacken sind nicht deshalb erfolgreich, weil die angegriffene Technologie eine eklatante Schwachstelle aufweist, sondern weil das Verhalten der Nutzer*innen durch Hacker*innen ausgenutzt wird. Das Gute daran: Das Verhalten lässt sich ohne hohe Kosten beeinflussen. Dafür ist der Dreiklang von Sensibilisierung, Information und Befähigung erforderlich. Für Unternehmen, die eine Zertifizierung nach der Norm ISO 27001 anstreben, ist eine auf diesem Weg erreichte Steigerung der Cyber-Security-Kompetenz obligatorisch. Für alle anderen Unternehmen sollte sie selbstverständlich sein. MHP unterstützt Unternehmen dabei, einen Kompetenz-Ansatz zu entwickeln und zu implementieren, der zur spezifischen Bedrohungssituation und der Disposition der Mitarbeiter*innen passt.

Vorgehensweise von MHP

Fundament für unsere Arbeit in Unternehmen ist die Überzeugung, dass die richtige Kommunikation zur richtigen Zeit für die richtige Zielgruppe die Aufmerksamkeit erhöht, für Informationen empfänglich macht und das richtige Verhalten trainiert. Dabei soll die Kommunikation nicht nur Wissen vermitteln, sondern gleichzeitig engagieren, aktivieren und inspirieren. Konkret folgen wir dabei fünf Schritten:

- Im ersten Schritt geht es darum, die Ist-Situation zu erfassen, die Soll-Situation als klares Ziel zu formulieren, und daraus den Veränderungsbedarf abzuleiten.
- Der erforderliche Change wird dann im zweiten Schritt mithilfe des Why-How-What-Prinzips operationalisiert. Dieser Schritt ist elementar, um bei den Mitarbeiter*innen eine hohe Akzeptanz zu erreichen.
- Die betroffenen Personen im Unternehmen werden im dritten Schritt in Zielgruppen segmentiert, die genauer analysiert und für die passenden Kommunikationskanäle festgelegt werden.
- Außerdem werden für die Zielgruppen im vierten Schritt geeignete Formate und Inhalte umgesetzt.
- Diese werden schließlich im fünften Schritt ausgeführt.

In der Umsetzung kann das sehr unterschiedliche Formen annehmen: In den drei Kästen haben wir Beispiele für die Bereiche **„Sensibilisierung und Aufmerksamkeit“**, **„Information und Austausch“** sowie **„Befähigung“** zusammengestellt.

Sensibilisierung und Aufmerksamkeit

- **Thematische Kampagne:** E-Mail-Kampagne zur Schärfung der Aufmerksamkeit für ein bestimmtes Thema
- **Escape Truck**: Gamification-Ansatz, der Cybercrime erfahrbar macht
- **Erklärvideos**: Darknet-Monitoring, Passwort-Diebstahl und andere Themen anschaulich erklärt
- **Standortkampagne**: Sticker, Aufsteller, Give-Aways als Hingucker und Aufmerksamkeits-Trigger

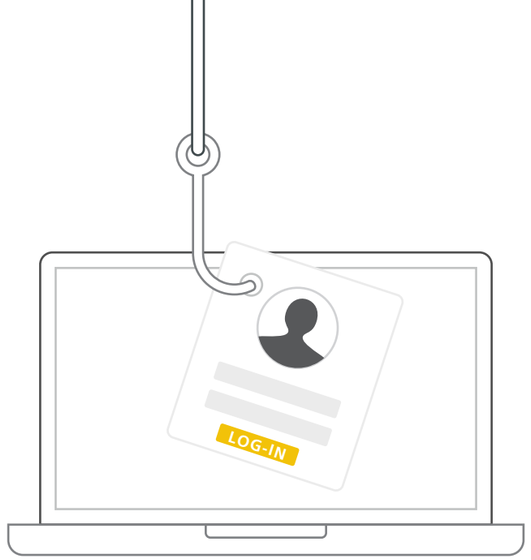
Information und Austausch

- **Newsletter**: Fachspezifische Updates für die Information Security Officers – als E-Mail-Newsletter oder als Blog mit RSS-Feed
- **Cyber Monday**: Monatlich gebrandete Content-Reihe zu aktuellen Security-Themen wie Passwortmanagement, Sicherheit am digitalen Arbeitsplatz oder Phishing
- **Newsroom**: Zentrale Plattform mit allen relevanten Inhalten auf einen Blick – Blogbeiträge, Leitfäden, FAQs, Ansprechpartner*innen etc.
- **Security Community**: Community für den regelmäßigen Erfahrungsaustausch unter Expert*innen und Security-Interessierten sowie regelmäßige Themen-Events – zum Beispiel in Microsoft Teams

Befähigung

- **Web-basierte Trainings**: Schulung zu den Grundlagen der Informationssicherheit im Arbeitsalltag
- **Vor Ort/Remote-Trainings:** Zielgruppenspezifische Vermittlung von Wissen
- **Digital Experience Room**: Erfahrbare Aufbereitung von Cyber-Security-Themen
- **How-to-Quick-Guide**: Security-Themen kompakt und verständlich auf wenigen Seiten erklärt
- **Storytelling**: Geschichten, die komplexe Richtlinien für die Anwender*innen nachvollziehbar machen
- **Cyber-Awareness-Monat**: Ein ganzer Monat mit Vorträgen, Artikeln, einem Digital-Goodie-Bag, einem Cyber-Security-Quiz und Events

Beispiel 1: Phishing-Kampagne



Ziel

Eine Phishing-Kampagne soll sensibilisieren und das Bewusstsein für Cyber-Angriffe steigern.

Umsetzung

Dafür wird eine fiktive Phishing-E-Mail an die Mitarbeiter*innen gesendet. Vor, während und nach dem Versand findet eine begleitende Kommunikation statt.

Vor der Phishing-Kampagne

Vorab wird intensiv kommuniziert und zum Thema Phishing aufgeklärt: Wie erkenne ich Phishing-E-Mails? Wie gehe ich richtig mit einer Phishing-E-Mail um? Inhalte dazu erscheinen in den internen Medien einige Wochen vor dem Versand der fiktiven E-Mail.

Während der Phishing-Kampagne

Die fiktive Phishing-E-Mail wird inhaltlich und hinsichtlich ihres Designs so professionell wie möglich aufbereitet. Schließlich sind Angriffe heute meist professionell durchgeführt und ahmen den üblichen E-Mail-Austausch fast perfekt nach – inklusiver beruflicher und privater Informationen über das Angriffsziel, die im Internet verfügbar sind. Die fiktive Phishing-E-Mail wird im Unternehmen gestreut. Sofern ein Adressat richtig reagiert hat, erhält er eine digitale Dankespostkarte. Klickt der Adressat auf den Phishing-Link, wird er automatisch auf eine eigens erstellte Webseite weitergeleitet, auf der ihm erklärt wird, dass dies glücklicherweise ein Test war und wie er sich beim nächsten Mal verhalten sollte.

Nach der Phishing-Kampagne

Zwei Wochen nach Versand der Phishing-E-Mail wird wieder in den internen Medien kommuniziert – in diesem Fall mit Fokus auf die Kampagne und ihren Zweck. Dazu kann beispielsweise der Chief Information Security Officer (CISO) in einem Interview über die Hintergründe und die Auswertung der Kampagne berichten.

Ergebnis einer Phishing-Kampagne eines Kundens

Der Vergleich der Klickraten eines Kunden zeigt, dass im zweiten Jahr deutlich weniger Mitarbeitende durch die Phishing-E-Mail getäuscht wurden. Außerdem verzeichnete der Cyber-Security-Informationsbereich im Intranet im Monat der Kampagne eine um 30 Prozent erhöhte Klickrate.

Beispiel 2: Digital Experience Room

Ziel

Ein digitaler Experience Room ist vergleichbar mit einem Escape Room und dient der zeit- und ortsunabhängigen Sensibilisierung der Teilnehmenden. Im Fokus stehen Teamfähigkeit, logisches Denken, nachhaltige Anwendung und Spaß bei der Lösung der Aufgaben. Das Konzept und die Inhalte hat MHP konzipiert, die technische Umsetzung hat ein auf Escape Games spezialisierter Dienstleister übernommen. Eine physische Variante wäre beispielsweise ein Escape Truck, der bei Events vor Ort eingesetzt werden kann.

Einsatz

Der digitale Experience Room kann als dauerhafter Lernraum über zentrale Lernplattformen angeboten werden. Teams aus unterschiedlichen Abteilungen können hier miteinander spielen, sich vernetzen und ihre spezifischen Fähigkeiten zur Lösung des Experience Rooms einsetzen. Für eine Spielrunde ist eine Dauer von 30 bis 60 Minuten ideal.

Ergebnis

Durch die digitalisierte Variante des Experience Rooms werden mehrere tausend Mitarbeitende gleichzeitig erreicht. Bei ihnen werden Cyber-Security-Themen wegen der Gamification- und Storytelling-Elemente nachhaltig im Bewusstsein verankert. Neben dem Sprachzentrum werden weitere Bereiche des Gehirns, wie das assoziative Denken (Sinneseindrücke) oder das episodische Langzeitgedächtnis, angeregt. Dabei werden emotionale Ereignisse zu Erinnerungen abgespeichert und bleiben länger im Gedächtnis.

ANSPRECHPARTNER

Dr. Christoph Schlude
Senior Manager
Focus Topic Lead Cyber Security
+49 151 20 30 12 35
christoph.schlude@mhp.com

AUTORINNEN

Kitty Wanke
Senior Management Consultant
Operations Performance & Strategy
MHP – A Porsche Company

Kim Großmann
Senior Consultant
Governance & Communication
MHP – A Porsche Company

Laura Krause
Consultant
Governance & Communication
MHP – A Porsche Company

Sabrina Cornelius
Senior Manager
Governance & Communication
MHP – A Porsche Company

Carolin Schmitt
Consultant
Governance & Communication
MHP – A Porsche Company

Sarah Groh
Senior Consultant
Governance & Communication
MHP – A Porsche Company

Bildrechte ©by Adobe Stock
Cover Jackie Niam // Seite 2/3 metamorworks

Layout
Freiland Design

MHP: DRIVEN BY EXCELLENCE

20 **MHP**Offices in Germany, England, USA, China,
Romania, Czech Republic, Austria, Israel, and Hungary.

Germany

Ludwigsburg
(Headquarters)
Berlin
Düsseldorf
Frankfurt a. M.
Ingolstadt
Munich
Nuremberg
Wolfsburg

International

Atlanta (USA)
Reading (England)
Cluj-Napoca (Romania)
Timișoara (Romania)
Prague (Czech Republic)
Shanghai (China)
Zell am See (Austria)
Tel Aviv (Israel)
Budapest (Hungary)

www.mhp.com