CYBERSECURITY & RESILIENCE

CII WHITE PAPER

Human Based Cybersecurity

Erfolgsfaktor Augmented Reality am Beispiel der Krisenstabsübung

Prof. Dr. Dennis-Kenji Kipker

Prof. Dr. Sachar Paulus

CYBER|INTELLIGENCE
.Institute

Inhalt

I.
Schulung und Weiterbildung als integraler Bestandteil der betrieblichen Cybersecurity Governance 3

II.
Bestehende Angebote und Defizite in der betrieblichen Wissensvermittlung zur Cybersicherheit 4

III.
Die bisherige und zukünftige Rolle virtueller Realitäten in der praktischen Cybersecurity Aus- und Weiterbildung 6

IV.
Cyber-Krisenstabsübungen als Fallbeispiel für die Notwendigkeit immersiver betrieblicher Aus- und Weiterbildungserfahrungen 7

V.
Fazit und Ausblick 9

I. Schulung und Weiterbildung als integraler Bestandteil der betrieblichen Cybersecurity Governance

Die an das betriebliche Personal gestellten Erwartungen an Kenntnisse in der Cybersicherheit wachsen stetig – und zwar abteilungsübergreifend. Bestes Beispiel hierfür sind aktuell die Schulungspflichten, die durch die zweite europäische Netz- und Informationssicherheitsrichtlinie (NIS-2-Richtlinie) vorausgesetzt werden.

So fällt die Durchführung von Schulungen einerseits in das Risikomanagement zur Cybersicherheit nach Art. 21, indem hier „grundlegende Verfahren im Bereich der Cyberhygiene und Schulungen im Bereich der Cybersicherheit“ als Mittel der Wahl bezeichnet werden, um die Netz- und Informationssysteme vor Sicherheitsvorfällen zu schützen. Andererseits sind die Schulungen kehrseitig als notwendige Maßnahmen zur Implementierung geeigneter Governance-Strukturen zu sehen, um Cybersicherheit nicht nur möglichst effektiv umzusetzen, sondern auch zu überwachen. Nicht umsonst bestimmt in diesem Zusammenhang der Art. 20 NIS-2-Richtlinie deshalb, dass nicht nur die Leitungsorgane wesentlicher und wichtiger Einrichtungen an Schulungen teilnehmen müssen, sondern die Geschäftsleitung vielmehr sicherzustellen hat, dass allen Mitarbeiter:innen regelmäßig entsprechende Schulungen anzubieten sind, um „ausreichende Kenntnisse und Fähigkeiten zur Erkennung und Bewertung von Risiken sowie Managementpraktiken im Bereich der Cybersicherheit und deren Auswirkungen auf die von der Einrichtung erbrachten Dienste zu erwerben“.

Obwohl die NIS-2-Richtlinie zum gegenwärtigen Stand noch nicht in das nationale Recht umgesetzt wurde, sind die auf dem Markt verfügbaren Schulungsangebote bereits jetzt umfassend und reichen von wenigen Stunden dauernden Webinaren bis hin zu mehrtätigen Systemschulungen vor Ort. Dies erklärt sich unter anderem auch damit, dass die NIS-2-Richtlinie selbst nicht bestimmt, auf welche Art und Weise und in welcher Form die nachweispflichtige Schulung abzuhalten ist.

Neue Pflichten für Geschäftsleiter im Bereich Cybersicherheit

Doch auch jenseits der NIS-2-Richtlinie und den neuen Pflichten für Geschäftsleiter spielt die Weiterbildung im Bereich der Cybersicherheit eine erhebliche Rolle.

- So setzt nach wie vor eine erhebliche Zahl erfolgreicher Cyberangriffe eine menschliche Interaktion voraus, um zum Erfolg zu gelangen, sei es durch Phishing-Angriffe, die Verbreitung von Malware oder im Bereich des Social Engineerings.
- Die subjektive Cybersecurity-Prävention umfasst nicht nur Maßnahmen in der unmittelbaren Abwehr von Cyberangriffen, sondern ebenso die Verwendung richtig konfigurierter Authentisierungsmechanismen sowie den erfahrenen Umgang mit der Unternehmens-IT unter verschiedenen Bedingungen, beispielsweise bei bekannt gewordenen Sicherheitslücken.

Daher betrachtet der IT-Grundschutz des BSI die Themen Sensibilisierung und Schulung umfassend innerhalb des Bausteins „Organisation und Personal“. Ziel ist, die Mitarbeitenden zu einem verantwortungsbewussten Umgang mit den Informationen einer Institution zu befähigen und ihre Qualifikation auf diese Weise nachhaltig zu verbessern.

ZITAT aus dem BSI IT-Grundschutz-Kompendium Edition 2023, Baustein ORP.2 Personal:

„Im täglichen IT-Betrieb einer Institution können viele Störungen und Fehler auftreten. Sind die verantwortlichen Mitarbeitenden nicht ausreichend qualifiziert, sensibilisiert und geschult, haben sie z. B. einen veralteten Wissensstand für ihre Aufgabenerfüllung, könnten sie sicherheitsrelevante Ereignisse nicht als solche identifizieren und so Angriffe unerkannt bleiben. Auch wenn die Mitarbeitenden ausreichend für die Belange der Informationssicherheit qualifiziert, sensibilisiert bzw. geschult sind, kann trotzdem nicht ausgeschlossen werden, dass sie Sicherheitsvorfälle nicht erkennen.“

Der Bedarf für fachliche Qualifikation und Weiterbildung im Bereich der Cybersecurity ergibt sich aber nicht nur für die Prävention und die rechtzeitige Erkennung von Angriffen, sondern bezieht sich ebenso auf eine angemessene, zeitnahe und richtige Vorfallsreaktion, um das Eintreten von Cyberschäden zu verhindern oder ihre Auswirkungen weitestgehend möglich zu reduzieren. Insbesondere für den letztgenannten Bereich ist es notwendig, über abstrakt vermitteltes Wissen hinaus konkrete Handlungs- und Umsetzungspläne im Sinne von Best Practices zu definieren und einzuüben, damit Mitarbeiter:innen in Notsituationen von Anfang an die richtigen Entscheidungen treffen.

Vorbereitung auf den Krisenfall

Teils wird daher vorgeschlagen, basierend auf der individuellen unternehmerischen Risikoanalyse zur Cybersicherheit verschiedene Krisenszenarien zu entwickeln und zu erproben, um über die theoretische Wissensvermittlung zur Cybersecurity Governance hinaus Erfahrung in ihrer konkreten Umsetzung zu sammeln. Dies kann beispielsweise im Rahmen von Krisenstabsübungen geschehen.

- Solche Übungen verfolgen den Zweck, die Mitglieder des Krisenstabs eines Unternehmens auf ihre Krisenarbeit vorzubereiten.
- Diese Krisenarbeit ist vor allem durch Unplanbarkeit, neuartige Situationen und in der Regel erhebliche Auswirkungen auf Menschen, Ressourcen, Infrastruktur und Geschäftsprozesse gekennzeichnet.

Entsprechend kommt der Entwicklung persönlicher Kompetenzen im Dialog mit anderen (Entscheidungsfindung unter Unsicherheit, gemeinsames Abwägen des „geringsten Übels“, aktive Kommunikation von negativen Entwicklungen und Folgen) bei der Konzeption von Schulungs- und Übungsmaßnahmen zur Stärkung der digitalen unternehmerischen Resilienz eine erhebliche Bedeutung zu.

Zusammenfassend lässt sich folglich feststellen, dass sich die gestiegene Relevanz und damit Notwendigkeit zur Durchführung von betrieblichen Weiterbildungsmaßnahmen nicht nur aus abstrakten gesetzlichen Vorschriften ergibt, sondern als Bestandteil digitalisierter betrieblicher Prozesse ein zwingendes Erfordernis ist. Die Notwendigkeit praktischer betrieblicher Aus- und Weiterbildung in der Cybersicherheit ist hierbei abteilungsübergreifend zu denken und betrifft nicht nur die Geschäftsleitung, sondern verfügt über Anknüpfungspunkte in sämtliche Bereiche vom Einkauf über die Entwicklung und Fertigung bis hin zum Vertrieb und der Außenkommunikation. Die an die Fortbildungsmaßnahmen anzulegenden Anforderungen sind vielfältig, denn nicht allein die abstrakte Wissensvermittlung ist notwendig, sondern ebenso die praktische Bewährung erlernter Fertigkeiten – und das auch in Notsituationen.

II. Bestehende Angebote und Defizite in der betrieblichen Wissensvermittlung zur Cybersicherheit

Betriebliche Weiterbildungen zur Cybersicherheit werden gegenwärtig in den unterschiedlichsten didaktischen Formaten angeboten. Diese reichen von klassischen Präsenzschulungen in der Form von Classroom Trainings (Seminare, Workshops, Fachkonferenzen, Intensivkurse und Bootcamps) über Online-Schulungen in der Form von E-Learnings (Webinare, professionelle webbasierte Trainingsmodule oder „Massive Open Online Courses“ (MOOCs)) bis hin zu modernen Blended-Learning-Konzepten, die Präsenz- und Online-Phasen im Lehren und Lernen miteinander verbinden, um eine bestmögliche Anwendung in der Wissensgenerierung zu gewährleisten. Ein Beispiel in diesem Kontext ist das Vermitteln der theoretischen Grundlagen innerhalb eines Fernkurses, wohingegen praktische Übungen im Präsenzunterricht abgehalten werden, um das erlernte Wissen zu erproben. Auch in der universitären Weiterbildung erfreut sich dieses Format einer zunehmenden Beliebtheit.

Trend zu rollenspezifische Formaten der Kompetenztrainings

Speziell für die Weiterbildungsangebote in der Cybersecurity ist in den letzten Jahren mit dem Anwachsen der Compliance-Anforderungen jedoch auch eine zunehmende Diversifizierung in praxisorientierte Formate und rollenspezifische Schulungen einhergegangen. Diese reichen von Social Engineering-Übungen über Phishing-Simulationen, klassische Capture The Flag (CTF)-Wettbewerbe bis hin zu technisch anspruchsvollen Cyber Range Trainings, bei denen realistische Simulationen von Cyberangriffen in einer sicheren Umgebung durchgeführt werden, damit Teams lernen, Cyberbedrohungen zu erkennen, abzuwehren und darauf richtig zu reagieren. Ergänzt werden die verschiedenen Formate in Teilen und soweit didaktisch möglich durch rollenspezifische Besonderheiten beispielsweise für technische Mitarbeiter:innen, Führungskräfte, Krisenstäbe, die Kommunikationsabteilung oder Enduser.

Insbesondere seit einigen Jahren treten zunehmend auch Anbieter des „spielerischen Lernens“ in der Form von „Serious Games“ auf dem Cybersecurity-Weiterbildungsmarkt in Erscheinung und übertragen die Prinzipien und Mechanismen zum Beispiel von Videospielen, Brettspielen (Tabletop Exercise) oder gar kompletten Escape Rooms auf die Vermittlung von Kenntnissen zur digitalen Resilienz.

Defizite klassischer Awarness-Übungen für Cybersecurity

Das nicht ohne Grund, denn viele der vorangehend genannten Verfahren zur Wissensvermittlung in der Cybersecurity sind problembehaftet:

- Teils sind sie zu aufwändig und kostenintensiv, um regelmäßig oder durch alle Betriebstypen abgehalten zu werden.
- Da die Inhalte gängiger Schulungen zur Cybersicherheit teils nach wie vor abstrakt-theoretisch und wenig praxisorientiert sind, fehlt es für die User nicht selten an konkreten Anwendungsszenarien – die größten Fortschritte werden hier aktuell noch im Bereich von Phishing-Simulationen erzielt, da die persönliche Betroffenheit hier einfacher darstellbar ist als bei komplexen technischen Angriffsvektoren, deren Relevanz sich nicht für sämtliche Anwenderkreise auf der Stelle erschließt.
- Oft sind die Inhalte standardisierter Schulungen nur schwer aufnehmbar, da es zumeist um generische Probleme ohne einen Bezug zum konkreten Arbeitsalltag geht.
- Überdies zeichnen sich gängige Schulungsmodelle trotz ihrer Vielfalt durch ein ganz entscheidendes Problem aus: Mangelnde Interaktivität und Engagement führen zu einer rein passiven Wissensaufnahme.

Nach wie vor werden eigentlich akute betriebliche Cyberbedrohungen deshalb nicht als realistisch, sondern als bloße hypothetische Möglichkeit wahrgenommen und deshalb nicht aktiv in den Betriebsabläufen verinnerlicht, was insbesondere für den Fall der bei akuten Cyberangriffen bestehenden Notsituationen problematisch ist. Zusammen mit einer fehlenden Integration in den Arbeitsalltag sinkt hierdurch nicht nur die kognitive Behaltensleistung, sondern es können im Gegenteil mit dem erlernten Wissen keine persönlichen Erfolgserlebnisse erzielt werden und ebenso wenig die bei Cybervorfällen entstehende Gruppendynamik in der Praxis erprobt werden.

Betriebliche Cybersecurity Awareness wird damit trotz der Vielfalt an unterschiedlichen Weiterbildungsangeboten auf dem Markt im Wesentlichen bislang auf eine negative bis bestenfalls neutrale Erfahrung reduziert, die in den meisten Fällen losgelöst neben dem betrieblichen Kontext steht. Reale Erfolgserlebnisse sind kaum generierbar, soweit zumeist die passive Wissensvermittlung im Vordergrund steht. Hieran vermögen auch abstrakte Wissenstests oder Quizaufgaben im Anschluss an ein Schulungsformat nicht viel zu ändern, da das Erfolgserlebnis in der Gruppe und damit auch die Anerkennung von Team-Mitgliedern und Kolleg:innen fehlen.

Vorteile verstärken die Verbreitung proaktiver Formate

Vor diesem Hintergrund überrascht der zunehmende Erfolg von Serious Gaming-Formaten nicht, bieten sie doch die Möglichkeit, ein klar fokussiertes Lernziel zu vertiefen und dieses anhand fest vorgegebener Spielmechaniken durch den richtigen Einsatz des erlernten Wissens optimalerweise proaktiv zu erreichen, in der Gruppe zusammenzuarbeiten und gedanklich bestenfalls mit einem Erfolgserlebnis zu verknüpfen.

> **Serious Gaming stößt in der Cybersecurity-Weiterbildung an didaktische Grenzen**

Doch auch das Serious Gaming stößt in der Cybersecurity-Weiterbildung immer wieder an didaktische Gren-

zen: Trotz aller Identifikation der Spieler mit ihrer Rolle ist das eigentliche betriebliche Szenario, das durch das Spiel abgebildet wird, nach wie vor theoretischer Natur, denn es handelt sich, wie es der Name bereits aussagt, lediglich um ein „Spiel“, dessen sich auch der User bewusst ist. Akute physische und psychologische Drucksituationen, wie sie sich beispielsweise im Falle einer gerade stattfindenden Ransomware-Verschlüsselung des Betriebs ergeben, können auf diese Weise kaum abgebildet werden. Überdies wird die fachliche Operationalisierung von Cybersecurity-Handlungsweisen erschwert, indem alle Spieler:innen im Wesentlichen aus einer strategischen Rolle heraus handeln, die ihrer tatsächlichen Funktion im betrieblichen Cybersecurity-Gefüge nicht unbedingt gerecht wird.

III. Die bisherige und zukünftige Rolle virtueller Realitäten in der praktischen Cybersecurity Aus- und Weiterbildung

In der praktischen Anwendung zu Aus- und Weiterbildungszwecken in der Cybersicherheit bislang weitestgehend unberücksichtigt sind technische Methoden, die Virtual Reality (VR) und Augmented Reality (AR) zur Grundlage nehmen. VR-Umgebungen erzeugen eine vollständig immersive und computergenerierte Umgebung, die die reale Welt des Users bewusst komplett ausblendet, sodass dieser vollständig in eine digital simulierte Erfahrung eintaucht und mit dieser interagiert. AR hingegen ergänzt und erweitert die reale Welt mit computergenerierten Informationen und Objekten, die in die reale Ansicht des Nutzers eingeblendet werden. Auf diese Weise werden digitale Inhalte auf die reale Welt überlagert, sodass sich der User seiner physischen Umgebung bewusst bleibt, diese aber um zusätzliche virtuelle Elemente bereichert wird.

In der Aus- und Weiterbildung können sowohl VR- wie auch AR-Anwendungen genutzt werden, wobei dies in der Vergangenheit nur unzureichend geschah, insbesondere gemessen am dargestellten Bedarf für praxisorientierte Fortbildungsformate insbesondere im Bereich der Cybersicherheit. Das lag vor allem an fehlender Rechenleistung und unzureichenden Netzwerkverbindungen, aber vor allem auch an der fehlenden Technologie zur Vermittlung von Sinneseindrücken sowie überkomplexer Sensortechnologie zur Navigation im virtuellen und augmentierten Raum. Mit den erheblichen technischen Fortschritten, die in diesen Bereichen in den vergangenen Jahren erzielt wurden, können VR und AR schon jetzt aktiv in Lernerfahrungen, Bildung und Ausbildung integriert werden. Mehr und mehr im Alltag setzen sich insbesondere auch AR-Endgeräte durch, die durch mobile Datenverbindungen nicht nur preisgünstiger werden, sondern auch leichter handhabbar sind und längere Akkulaufzeiten vorweisen können.

Die entsprechenden Szenarien für den VR- und AR-Einsatz im Kontext betrieblicher Weiterbildung sind – wie eingangs angemerkt vor allem jenseits der Cybersecurity – bereits jetzt mannigfaltig.

- So existieren virtuelle **Klassenräume**, Webinare werden in digitalisierten Präsentationsumgebungen durchgeführt oder eLearnings werden zu virtuellen Begegnungsstätten umfunktioniert, in denen sich die Charaktere der User („Avatare“) treffen und austauschen können.
- Maßnahmen der betrieblichen Fortbildung können teils schon jetzt in VR-Umgebungen durchgeführt werden, so zum Beispiel **Brandschutzseminare**, bei denen Beschäftigte den Einsatz des Feuerlöschers gegen ein virtuelles Feuer üben.
- In der **medizinischen Ausbildung** werden VR- und AR-Umgebungen zur simulierten Durchführung von Operationen bereitgestellt.
- In der **Personenbeförderungs- und Logistikbranche** werden VR-Anwendungen bereits seit Längerem

eingesetzt, um Zugführer, Bus- und LKW-Fahrer auszubilden, indem ein realitätsnahes Training zu allen Tages- und Nachtzeiten ermöglicht wird.

Gegenwärtig experimentieren zahlreiche weitere Branchen und Einrichtungen mit der aktiven Einbindung von VR und AR in Aus- und Weiterbildungsprozesse, darunter Fluggesellschaften, Automobilhersteller, Chemiekonzerne, Versicherungen, Softwareentwickler bis hin zu Fußballvereinen und der Raumfahrtindustrie. Vielfach erfolgt die Einbindung von augmentierter und virtueller Realität aber noch nicht im Rahmen extern bereitgestellter Formate, sondern in internen betrieblichen Erprobungsprozessen der Technologie.

VR- und AR-Konzepte können dabei im betrieblichen Kontext aufgrund ihrer Immersivität geeignet sein, Lernprozesse zu verbessern, indem sie einerseits interaktive Lernumgebungen schaffen, andererseits aber aufgrund der räumlichen Wahrnehmung gleichzeitig eine intensive Bezugherstellung zum einsetzenden Betrieb und seinem realen Personal ermöglicht wird. Dies gilt insbesondere für AR-Weiterbildungskonzepte: Indem nicht der vollständige berufliche räumliche Kontext ausgeblendet wird, können Interaktionen mit den bestehenden Räumlichkeiten und betrieblichen Bezugspersonen stattfinden.

Durch den Bezugspunkt zum konkreten betrieblichen Alltag wird ein höherer Grad der Wissensretention ermöglicht, indem Lernende durch regelmäßige Übung wiederkehrende und einprägsame Erlebnisse aufbauen können, die auf visuellen und damit selbst erlebten Informationen basieren. Überdies werden Kollaborationsfertigkeiten und soziale Fähigkeiten gestärkt, indem die Zusammenarbeit mit echten Kolleg:innen anstelle von virtuellen Abbildern ermöglicht wird.

Gerade im **Bereich der Cybersecurity** spielt eine derartige Personalisierung der Lernerfahrung eine größere Rolle als in anderen Bereichen, denn in betrieblichen Notsituationen kommt es für ein erfolgreiches Krisenmanagement nicht nur auf das Know-how einer Einzelperson, sondern auf das effektive und effiziente Zusammenwirken in der Gruppe an, um die richtigen Entscheidungen innerhalb von begrenzten Zeitspannen zu treffen und zur erfolgreichen Umsetzung zu bringen, so beispielsweise im Rahmen von Übungen des Krisenstabs.

An dieser Stelle zeigt sich somit bei der Verwendung von virtuellen Realitäten auch ein entscheidender Unterschied zu bestehenden Serious Gaming-Ansätzen in der Cybersicherheit:

- Wo letztere nach wie vor als abstraktes Spiel wahrgenommen werden, lassen sich beispielsweise AR Cybersecurity-Erfahrungen unmittelbar in einen betrieblichen Kontext einbinden, anstelle dem Einzelnen durch die strategische Kollektivität eines Serious Games die Letztverantwortung für seine eigene Entscheidung abzusprechen.
- Erlebte betriebliche Notsituationen wie bei einem aktiven Ransomware-Vorfall können so zum Beispiel individuell erfahrbar gemacht werden, anstelle sie ausschließlich als gemeinsame und vom betrieblichen Alltag losgelöste Ausbildungserfahrung oder gar nur als „harmloses Spiel“ und nicht als realistisches Szenario zu begreifen, das sich jederzeit ereignen kann.

IV. Fallbeispiel Cyber-Krisenstabsübungen: Notwendigkeit immersiver betrieblicher Aus- und Weiterbildungserfahrungen

Veranschaulicht wurde, dass insbesondere in der Cybersecurity die Notwendigkeit für ein Umdenken bei den gängigen Weiterbildungsformaten besteht: In einem Bereich, in dem es mehr denn je auf schnelles Entscheiden und strategisch richtiges Handeln ankommt, können passive Lernformate kaum eine sinnvolle Hilfestellung bieten, um den betrieblichen Notfall ernsthaft unter realistischen Bedingungen zu verinnerli-

chen und Defizite und Gruppendynamiken zu erkennen und zu bewerten.

Hinzu kommt, dass die Anforderungen an die erforderliche Cybersecurity-Kompetenz in Unternehmen einerseits und die zunehmende Digitalisierung des allgemeinen Arbeitskontexts andererseits es erforderlich machen, schon jetzt verfügbare neue Technologien einzusetzen, um die Arbeitsrealität moderner Unternehmen abzubilden. Diese setzt sich regelmäßig zusammen aus deutlich verteilteren Standorten und zahllosen Online-Zusammenarbeitsmodellen, was wiederum zu entsprechend weniger gemeinsamer verfügbarer Zeit in bestimmten betrieblichen Lokationen führt. Wie diesen Herausforderungen insbesondere durch den Einsatz AR-gestützter Aus- und Weiterbildungsmodelle begegnet werden kann, wird nachfolgend am Beispiel von Cyber-Krisenstabsübungen demonstriert.

(Cyber-)Krisenstabsübungen dienen dazu, die Mitglieder des Krisenstabs eines Unternehmens auf ihre Krisenarbeit vorzubereiten. Diese Krisenarbeit ist vor allem durch Unplanbarkeit, neuartige Situationen und in der Regel erhebliche Auswirkungen auf Menschen, Ressourcen, Infrastruktur und Geschäftsprozesse gekennzeichnet. Entsprechend kommt der Entwicklung persönlicher Kompetenzen im Dialog mit anderen bei der Konzeption von Schulungs- und Übungsmaßnahmen für den Krisenstab eine wesentliche Bedeutung zu.

Klassische Fälle betreffen in diesem Kontext die Entscheidungsfindung unter Unsicherheit, das gemeinsame Abwägen des „geringsten Übels“ und die aktive Kommunikation von negativen Entwicklungen und Folgen. Um dieser Dynamik gerecht werden zu können, werden solche Krisenstabsübungen regelmäßig in Präsenz mit Stift und Papier als so genannte „Tabletop Exercises“ (TTX) durchgeführt.

- Ein Moderator erläutert dabei die Veränderung der Situation – meist durch eine Nachricht einer Abteilung oder der Presse – und lässt dann den Krisenstab selbständig agieren. Im weiteren Verlauf der TTX werden zusätzliche Informationen zugestellt, die die Situation verschärfen, verändern oder erleichtern können. Dies erfolgt dynamisch auf der Grundlage des bisherigen Handelns oder auch Nicht-Handelns des Krisenstabs.
- Nach einer vorab festgelegten Zeitspanne oder einem geplanten „Zustand“ der Krise wird die Übung beendet. Je nach Realitätsnähe der Übung kann auch die Alarmierung und das Zusammenkommen des Krisenstabs Teil der Übung sein. Die Arbeit des Krisenstabs, vor allem seine Entscheidungsfindung und die eingesetzte Kommunikation nach innen wie nach außen wird dabei durch einen (meist externen) Beobachter dokumentiert.
- Im Nachgang zur eigentlichen Übung wird sodann das Verhalten der Krisenstabsmitglieder gemeinsam diskutiert, um bei den Mitgliedern eventuelle Einsichten und – im Sinne der Krisenstabsarbeit – positive Verhaltensänderungen zu initiieren.

Diese Vorgehensweise ist jedoch unter Zugrundlegung konventioneller Ausbildungsmethoden mit verschiedenen Nachteilen verbunden, die mit zunehmender Digitalisierung und Dezentralisierung von Personal und betrieblichen Standorten noch größer erscheinen. So müssen für eine Krisenstabsübung die Mitglieder des Stabs physisch zusammenkommen, sollte ihr Dienstort nicht am selben Standort liegen, die Durchführung von Übungen ist stets individuell und auch von der Persönlichkeit des Moderators abhängig, zudem knüpfen die Ergebnisse der Stabsübungen erheblich an die Erfahrung und Beurteilung durch den jeweiligen Beobachter an.

> **In einem Bereich, in dem es mehr denn je auf schnelles Entscheiden und strategisch richtiges Handeln ankommt, können passive Lernformate kaum eine sinnvolle Hilfestellung bieten.**

Diesen Herausforderungen kann durch die Verwendung zeitgemäßer Digitalisierungs- und AR-Technologie begegnet werden. Dabei ist es aufgrund des großen Anteils an nonverbaler Kommunikation, welche bei der gemeinsamen Entscheidungsfindung in Stresssituationen auftritt, entscheidend, nicht ausschließlich eine Web-Konferenzlösung einzusetzen, weil hierdurch das akute Geschehen nicht immersiv, sondern vor allem wie im Regelfall nur als passiver Beobachter und Kommentator erlebt werden kann.

- Die digitale Virtualisierung des Fortbildungsgeschehens bietet hier die Möglichkeit, Bewegungen im Raum, Diskussionen in Kleingruppen sowie ein gemeinsames Erarbeiten von Konzepten und Plänen an virtuellen Pinnwänden zu ermöglichen, um den

Entscheidungsprozess möglichst optimal zu unterstützen, indem ein realistisches Erlebnis „vor Ort“ gewährleistet wird.

- Mittels eines Cloud-Backends können die für die Übungen zugrundeliegenden Szenarien modelliert und in Abläufe strukturiert werden, um die Informationsversorgung an den Krisenstab sicherzustellen und die Aktivitäten und Entscheidungen des Krisenstabs zu protokollieren.
- Soweit Anwendungen der augmentierten Realität und der Einsatz von Künstlicher Intelligenz (KI) zur Durchführung von Cyber-Krisenstabsübungen miteinander kombiniert werden, kann eine möglichst neutrale automatisierte Auswertung der Übungsdokumentation dabei unterstützen, Empfehlungen für eine Optimierung sowohl von gemeinsamen Abläufen als auch von individuellen Verhaltensweisen der Krisenstabsmitglieder vorzuschlagen.

V. Fazit und Ausblick

Gezeigt wurde einerseits, dass der Bereich der betrieblichen Cybersecurity Compliance in den letzten Jahren verstärkt an Bedeutung gewonnen hat und auch zukünftig weiter an Bedeutung gewinnen wird, welches sich kehrseitig verstärkt in der Einführung von unternehmensinternen Governance-Strukturen zur Verbesserung der Cybersicherheit widerspiegelt.

Andererseits wurde verdeutlicht, dass die betriebliche Aus- und Weiterbildung zur Optimierung von unternehmerischen Cybersecurity-Prozessen zwar vielfältige Möglichkeiten bietet, bisherige Maßnahmen jedoch zu großen Teilen nur wenig bis begrenzt immersiv sind, sodass nur ein verhältnismäßig geringer Grad an Wissensretention vorhanden ist, da es an der aktiven Wahrnehmung und Einbindung der Mitarbeiter:innen in das Geschehen fehlt. Insbesondere für den richtigen Umgang mit Cyber-Krisenfällen kann dies problematisch sein, da es nicht nur auf die abstrakte Wissensvermittlung, sondern mindestens genauso auf das richtige Agieren und Entscheiden in (zeitlichen) Zwangssituationen ankommt, wobei auch eventuelle Gruppendynamiken zu berücksichtigen sind.

Hilfe bieten können hierbei VR- und AR-gestützte Ausbildungsmodelle, die die Szenarien und Besonderheiten des betrieblichen Alltags unmittelbar in eine (teil)virtuelle Umgebung integrieren und somit erlebbar machen. Die entsprechende Technologie zur Umsetzung ist bereits vorhanden, wird in diesem Kontext zurzeit aber noch nicht ausreichend genutzt.

Am Beispiel von Cyber-Krisenstabsübungen wurde gezeigt, wie ein solches modelliertes Szenario in der Cybersicherheit augmentiert werden kann und welche Möglichkeiten zur Verbesserung der betrieblichen Weiterbildung sich dabei ergeben können. Letztlich handelt es sich hierbei aber nur um ein Anwendungsfeld, welches verdeutlicht, wie den steigenden Kompetenzanforderungen an Sicherheit und sicheres Verhalten in modernen Unternehmensstrukturen effektiv begegnet werden kann. Weitere denkbare Szenarien im Kontext der Cybersecurity sind etwa Schulungen, Vorbereitungskurse auf Zertifizierungen oder die Durchführung von Audits.

Impressum

Die Autoren
Der Verfasser Prof. Dr. Dennis-Kenji Kipker ist wissenschaftlicher Direktor am cyberintelligence.institute und Professor für IT-Sicherheitsrecht an der Hochschule Bremen.

Der Verfasser Prof. Dr. Sachar Paulus ist Mitglied im Scientific Advisory Board des cyberintelligence.institute und Professor für IT-Sicherheit an der Technischen Hochschule Mannheim.

Diese Studie wurde erstellt mit Unterstützung des CII-Fördermitglieds: MACONIA GmbH

---

cyberintelligence.institute (Herausgeberin)
MesseTurm
Friedrich-Ebert-Anlage 49
60308 Frankfurt a.M.

T +69 5050 34-602

www.cyberintelligence.institute
info@cyberintelligence.institute

Der Text dieses Werkes ist lizenziert unter den Bedingungen von „Creative Commons Namensnennung-Weitergabe unter gleichen Bedingungen 4.0 international", CC BY-SA 4.0 (abrufbar unter: https://creativecommons.org/licenses/by-sa/4.0/legalcode.de)