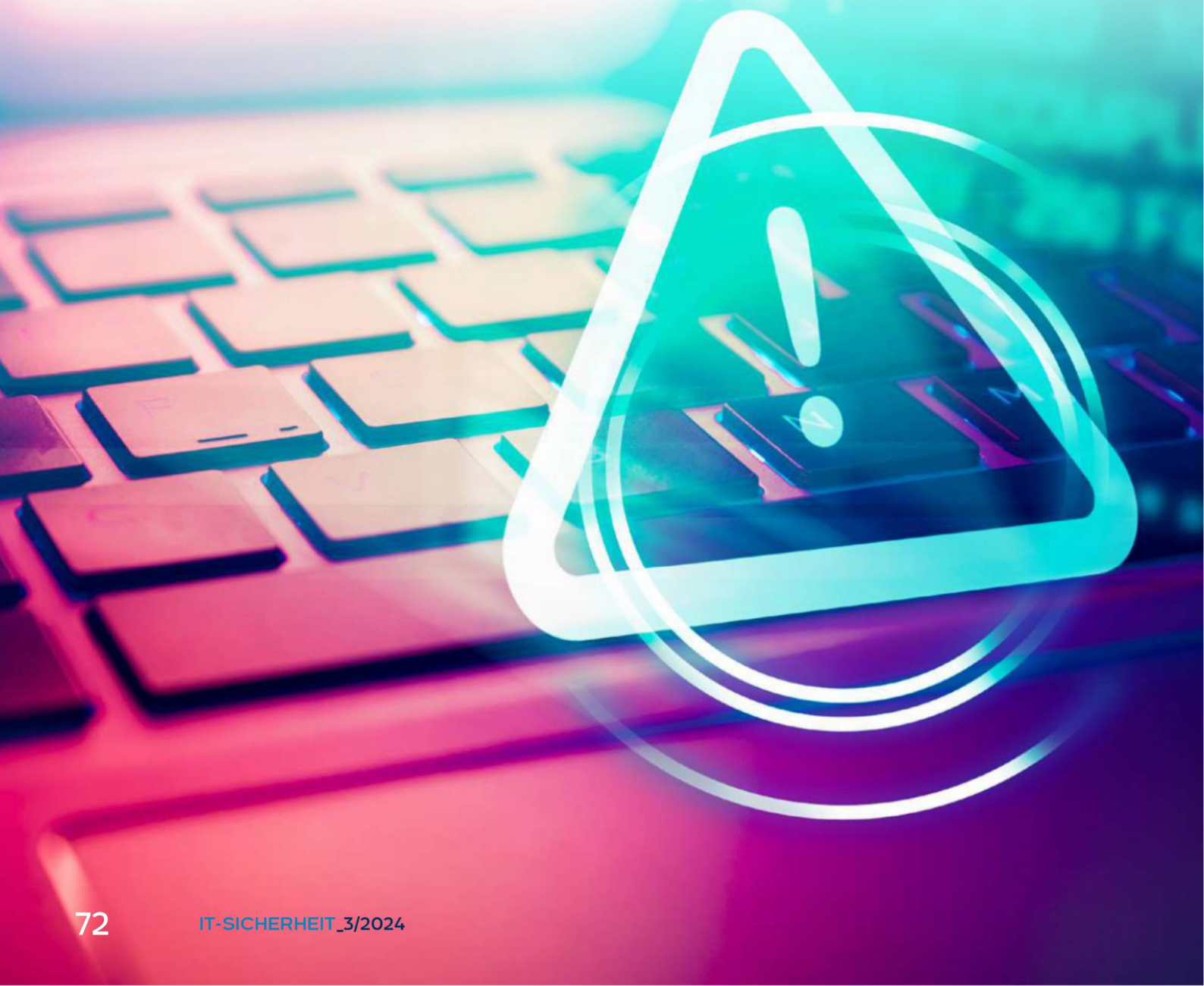
SecAware.nrw –
das kostenlose Selbstlernangebot,
nicht nur für Hochschulen

RÜSTZEUG FÜR MEHR SECURITY-AWARENESS



Security-Awareness ist eine zentrale Säule der IT-Sicherheit in der modernen Hochschullandschaft. Vor diesem Hintergrund wurde SecAware.nrw entwickelt, ein maßgeschneidertes Online-Selbstlernangebot, das rund 750.000 Studierenden und rund 50.000 Hochschulangehörigen in Nordrhein-Westfalen wesentliche Kenntnisse und Kompetenzen im Bereich der Cyber- und Informationssicherheit vermitteln soll. Geeignet ist das Tool aber nicht nur für Hochschulen.

Die Welt der Hochschulbildung steht vor einer sich stetig wandelnden Bedrohungslage im digitalen Raum. Universitäten und Forschungseinrichtungen entwickeln sich zu bevorzugten Zielen für Cyberkriminelle, angezogen von einem Reichtum an sensiblen Daten. Bezeichnende Beispiele hierfür liefern die Berichte „Die Lage der IT-Sicherheit in Deutschland 2022 & 2023" des Bundesamtes für Sicherheit in der Informationstechnik (BSI): Von 23 registrierten Ransomware-Attacken im Bildungssektor zielten im Jahr 2023 13 auf Universitäten und Forschungseinrichtungen.[1] Die Konsequenzen dieser Angriffe reichen von Datenschutzverletzungen bis hin zu empfindlichen Betriebsstörungen, welche Präsidien, Rektorate und IT-Abteilungen von Hochschulen Sorge bereiten.

So wurde beispielsweise die Universität Duisburg-Essen Ende 2022 durch einen schweren Cyberangriff lahmgelegt, der die gesamte IT-Infrastruktur und das Telefonsystem außer Betrieb setzte. Die Angreifer verschafften sich Zugang zu essenziellen internen Systemen und legten durch Verschlüsselung wichtige Dienste wie Office-Anwendungen, Verwaltungssysteme sowie den E-Mail- und Telefonverkehr lahm (siehe Abbildung 1). Die Universitätsverwaltung sah sich mit erheblichen organisatorischen und rechtlichen Schwierigkeiten konfrontiert: Studierende erwarteten ihre Abschlusszeugnisse, befristete Verträge standen still und die Prüfungsplanung war blockiert. Lehre und Forschung litten unter dem Ausfall der Lernplattformen, da weder Studierende noch Dozierende auf Materialien und Inhalte zugreifen konnten. Der universitäre Betrieb war somit für einige Zeit auf analoge Prozesse angewiesen.[2]

GEFAHR VOR CYBERANGRIFFEN: „HOCH WIE NIE"

Es verstrichen Monate, in denen nur schrittweise und mit erheblichen Anstrengungen einige digitale Services wiederhergestellt oder ersetzt werden konnten. Selbst nach einem Vierteljahr waren noch nicht alle IT-Systeme der Hochschulen voll funktionsfähig. Dieser Vorfall, bei dem Hacker mit der Veröffentlichung der Daten im Darknet drohen und Lösegeld forderten, ist nur einer in einer Reihe von Angriffen auf Hochschulen in Nordrhein-Westfalen. Weitere Vorfälle sind an der Bergischen Universität Wuppertal, der Heinrich-Heine-Universität Düsseldorf sowie auch an der Fachhochschule Münster oder der Hochschule Ruhr West (HRW) zu verzeichnen.[2] In den letzten fünf Jahren sahen sich sämtliche Hochschulen in NRW mit Cyberangriffen konfrontiert, die Intensität variierte dabei. Dies wurde durch die NRW-Wissenschaftsministerin Ina Brandes von der CDU bestätigt, als Reaktion auf eine Anfrage der SPD im Landtag. Die SPD hob hervor, dass das Bundesamt für Sicherheit in der Informationstechnik die aktuelle Bedrohungslage seit Beginn des russischen Angriffskriegs auf die Ukraine als so „hoch wie nie" einstuft.[4]

Für die betroffenen Hochschulen bleibt in solchen Szenarien kaum mehr als die Erstattung einer Anzeige. Diese Vorfälle unterstreichen drastisch die Notwendigkeit einer ständigen Weiterentwicklung und Anpassung der IT-Governance- und

Abbildung 1: 2022 verschlüsselte ein Ransomware-Angriff wesentliche Systeme der Universität Duisburg-Essen. (Bild: (if(is))

Bild: janews094 - stock.adobe.com

-Sicherheitsstrategien an Hochschulen, um gegen die immer raffinierter werdenden Cyberbedrohungen gewappnet zu sein.

DER RISIKOFAKTOR MENSCH – UND WIE SECURITY-AWARENESS SCHÜTZT

Aufgrund des technischen Fortschritts legen Angreifende ihren Schwerpunkt jedoch nicht mehr nur auf technische, sondern vermehrt auf menschliche Schwachpunkte – insbesondere der „Faktor Mensch" macht den kritischsten Risikofaktor in der IT-Sicherheit aus.[5] Vor dem Hintergrund, dass täglich Hunderttausende in den nordrhein-westfälischen Hochschulen auf das Internet zugreifen, die potenzielle Einfallstore für Cyberangriffe schaffen, wird die Notwendigkeit einer robusten Security-Awareness von Hochschulen mehr als deutlich unterstrichen.

Dabei umfassen die Kernziele von Security-Awareness den Schutz vor den Gefahren, die durch unachtsame oder unwissende Mitarbeitende entstehen könnten, sowie den Schutz vor den Fallen des Social Hacking. In Security-Awareness-Schulungen werden elementare Verhaltensregeln vermittelt, die das alltägliche Fehlverhalten präventiv adressieren. Inhalte solcher Schulungen umfassen Themen wie grundlegende Cybersicherheit, den Umgang mit Social-Engineering, sichere E-Mail- und Passwortpraktiken, sicheres Surfen, die Risiken von Malware und die Nutzung mobiler Geräte sowie die Herausforderungen durch Soziale- und Berufsnetzwerke.[6]

Im Kontext der digitalen Transformation von Hochschulen wird jedoch deutlich, dass ein akuter Mangel an leicht zugänglichen, qualitativ hochwertigen und zielgruppenorientierten Schulungs- und Selbstlernangeboten vorliegt. Obendrein ist der akademische Sektor nicht nur geprägt von begrenzten Lernmöglichkeiten oder unzureichendem Fachwissen, sondern auch von Zeitmangel und fehlenden Anreizen, die unbeabsichtigtes, riskantes Verhalten begünstigen und die so die Sicherheitsproblematik verstärken.

DIE ONLINE-SELBSTLERN-AKADEMIE

Das Projekt *SecAware.nrw* hat es sich zur Aufgabe gemacht, genau diese Herausforderungen anzugehen. Es bietet ein spezifisches, auf die Bedürfnisse der akademischen Gemeinschaft zugeschnittenes Selbstlernangebot, das sowohl in deutscher als auch in englischer Sprache zur Verfügung steht. Ein modularer Aufbau des Lernangebots ermöglicht eine präzise Anpassung an individuelle Bedürfnisse, wobei der inhaltliche Schwerpunkt je nach Zielgruppe – wozu vorrangig Studierende, wissenschaftliche Mitarbeitende oder die Professorenschaft zählen – variieren kann. Unter Berücksichtigung der besonderen Anforderungen und der spezifischen Risiken, die innerhalb des Hochschulkontextes bestehen, zielt *SecAware.nrw* darauf ab, nicht nur aufzuklären, sondern die Nutzenden nachhaltig zum Thema Cyber- und Informationssicherheit zu sensibilisieren.

Ein zentraler Schwerpunkt liegt auf der partizipativen Entwicklung des Lernangebots („User Centered Design") mit der Absicht, die IT-Kompetenzen im Kontext Cyberattacken gezielt aufzubauen und zu stärken. Durch fortlaufende qualitative Evaluationen sichert das Projekt die Relevanz und verbessert kontinuierlich die Effektivität der Lehrinhalte. Dieser Ansatz dient nicht nur der Wirksamkeit des Bildungsangebots, sondern leistet auch einen entscheidenden Beitrag zur Steigerung des Sicherheitsbewusstseins im akademischen Umfeld. Aufgrund dessen sind Informationssicherheitsbeauftragte (CISOs) der Hochschulen in Nordrhein-Westfalen laut der „Vereinbarung zur Informationssicherheit an den Hochschulen (Vzl)" § 2 (10) nun mehr auch verpflichtet, auf *SecAware.nrw* zurückzugreifen und es an der jeweiligen Hochschule zu implementieren.[7]

Entwickelt wurde das Tool vom Institut für Internet-Sicherheit – if(is) der Westfälischen Hochschule Gelsenkirchen in Zusammenarbeit mit dem Institut für die Digitalisierung von Arbeits- und Lebenswelten – IDiAL der Fachhochschule Dortmund. Das if(is) verfügt über jahrzehntelange Expertise in der anwendungsorientierten IT-Sicherheit und legt seit Gründung seinen Schwerpunkt auf die Ausbildung von IT-Security-Experten sowie die Steigerung der Internetsicherheit für Verbraucher und Unternehmen. Gemeinsam mit dem IDiAL, das für die Entwicklung und Optimierung des didaktischen Konzepts verantwortlich ist, steht das Projektteam für Qualität und Fachkompetenz im Bereich der Internetsicherheit.

PROJEKTAUFBAU UND STRUKTUR

Das Projekt *SecAware.nrw* zeichnet sich durch einen strukturierten Projektaufbau und Herangehensweise aus, die das Fundament für eine effektive Cybersicherheitsschulung bilden. Der Produktionsprozess umfasst mehrere Schlüsselschritte: Konzeption, Skripterstellung, Videoproduktion, Vertonung sowie die Erstellung interaktiver Elemente. Jeder dieser Schritte folgt einem iterativen Ansatz, der es ermöglicht, Feedbackversionen systematisch zu integrieren und die Qualität des Endprodukts kontinuierlich zu verbessern.

DER PRODUKTIONS-PROZESS

Die initiale Phase, die Konzeption, basiert auf der Identifizierung aktueller, relevanter Cybersicherheitsthemen und der Zusammenarbeit mit Informationssicherheitsbeauftragten. Daraus entsteht ein Curriculum, das spezifisch auf die Bedürfnisse der Zielgruppe zugeschnitten ist. Im nächsten Schritt folgt die Skripterstellung durch eine journalistisch ausgebildete Redaktion. Jedes Skript, erstellt auf Basis verifizierter Quellen und eingehender Recherchen, durchläuft einen mehrstufigen Feedbackzyklus durch Fachex-

Abbildung 2: Schulungen sind ein Grundpfeiler für mehr Security-Awareness in Organisation. (Bild: if(is))

perten, um die Korrektheit und Vollständigkeit zu sichern. Das Skript bildet ein relevantes Fundament für weitere Ausarbeitungsschritte: gemünzt auf die Anforderungen der Videoproduktion, für die professionelle Vertonung und die Erstellung begleitender Fachtexte.

Bei der Videoproduktion durchläuft das vorläufige Voice-Over, generiert durch KI-gestützte Text-zu-Sprache-Technologie, einen Transformationsprozess, der mit der Erstellung von Vektorgrafiken und deren Animation beginnt und mit der Vertonung durch professionelle Sprecher endet. Hierbei wird besonderer Wert auf die Synchronisation des auditiven und visuellen Materials gelegt, inklusive der Integration von Untertiteln in Englisch und Deutsch zur Förderung der Zugänglichkeit. Im letzten Schritt erfolgt die Ausarbeitung interaktiver Elemente in gemeinsamen Workshops, um Selbstüberprüfungsaufgaben und interaktive Darstellungen zu entwerfen. Diese werden zu Prototypen mithilfe der Software „Articulate Storyline 360" entwickelt und abschließend in das Selbstlernangebot eingebettet, bevor die vollständigen Informationen an ein Lernmanagementsystem (LMS) übermittelt werden.

Das Resultat ist ein modulares Lernkonzept, das durch eine durchdachte Didaktik den Nutzenden die komplexen Themen der Cybersicherheit verständlich macht. Durch den umfassenden Produktionsprozess, der in *SecAware.nrw* implementiert wurde, wird ein bedeutendes Engagement in der Vermittlung von Cybersicherheitsbewusstsein deutlich. Mit über zwei Jahren und fast 10.000 Arbeitsstunden, die in die Produktion des Materials geflossen sind, setzt das Projekt neue Maßstäbe in der Qualität und Intensität der E-Learning-Entwicklung.

WIE KANN MAN TEILNEHMEN?

SecAware.nrw kann für die Integration in ein LMS wie Moodle oder ILIAS heruntergeladen werden, steht aber ebenso über die Plattform *https://SecAware.nrw/* im Open Access für alle Interessierten kostenfrei zur Verfügung. Der Inhalt ist auf den Hochschulbereich ausgerichtet, aber dennoch so universell gestaltet, dass es auch für die Allgemeinbevölkerung nützlich ist. Studierende, die zukünftigen Fachkräfte in Unternehmen, profitieren besonders von der Ausrichtung auf kritisches Denken und Handlungskompetenzen. Somit stärkt *SecAware.nrw* nicht nur akademische Institutionen, sondern bietet auch Unternehmen und Einzelpersonen wertvolles Wissen. Ein motivierendes Lernumfeld mit interaktiven Elementen wie Quiz und Anwendungsaufgaben lädt jeden ein, sich aktiv mit den Materialien auseinanderzusetzen und die eigene Cyber-Sicherheitskompetenz zu erhöhen.

Besonders kleinere Unternehmen, für die individuelle Awareness-Schulungsprogramme oft nicht finanzierbar sind, können das Selbstlernangebot kostenlos nutzen. Zudem werden auf dem Marktplatz IT-Sicherheit des Instituts für Internet-Sicherheit (*https://it-sicherheit.de/selbstlernangebot-it-sicherheit/*) weitere Informationen bereitgestellt.

DIE MODULE DER SELBSTLERNPLATTFORM

Das Projektteam von *SecAware.nrw* hat sich im Rahmen seiner Vorrecherchen mit vielen IT-Security-Verantwortlichen zusammengetan, um die drängendsten Themen zu identifizieren. Neben dem Schwerpunkt der Aktualität, floss aber auch die Relevanz des täglichen Bedarfs in die Entscheidungsfindung mit ein.

Finalisiert wurden schließlich die folgenden Module: Passwörter und Authentifizierung sowie der Bereich Onlinebetrug mit Input zu Phishing, Spear Phishing, Social Engineering und Fake-Websites. Das Thema IT-Infrastruktur mit Lernmaterialien zu Netzwerken, Backups, Updates und Sicherheit am Arbeitsplatz, der Sektor Datenaustausch mit Videos zu Cloud-Diensten, physischen Datenträgern und Verschlüsselung. Das Feld von Kommunikation und Social Media mit Material zu Social Media, Messengern und Fake News, das Thema Datenschutz und DSGVO sowie der Bereich Urheberrecht und Lizenzen mit Inhalten zu Creative Commons und Urheberrecht.

Die Themen wurden hinsichtlich ihrer Brisanz und ihres Vorkommens im Arbeitsalltag der adressierten Zielgruppen beleuchtet. Da das Lernmaterial jedoch einen breiten Zuschnitt hat, sind die Videos, die Quiz und sämtliche Materialien für alle IT-Sicherheitsinteressierten hilfreich – der Output der Module erlaubt eine Awareness-Steigerung quer durch alle Zielgruppen, die online unterwegs sind. Insgesamt zielt die Lernplattform auf die Sensibilisierung der Nutzenden ab und möchte ein Paket zur proaktiven Selbsthilfe schnüren.

SICHERHEIT FÄNGT BEIM NUTZER AN

Im Modul Passwörter und Authentifizierung werden daher die Schwerpunkte auf die Themen „Starke Passwörter", „Passwort-Manager" und „Multi-Faktor-Authentifizierung" gelegt. So bietet das Video zum Thema Passwörter kurzweiliges Hintergrundwissen über die Notwendigkeit starker Passwörter für unterschiedliche Dienste und gibt praktische Tipps zur Erstellung dieser. Ein weiteres Video erklärt den Usern die Vorteile

des Passwort-Managers, während das Material zur Multi-Faktor-Authentifizierung (MFA) anwendungsorientiert darstellt, warum die MFA bei der Anmeldung eine zusätzliche Schutzebene ist. Der Vierklang aus Videos, Quiz, interaktiven Elementen und Zusatzmaterial bedient dabei konsequent die unterschiedlichen Lerntypen und geht auf die Präferenzen der Lernenden ein.

SENSIBLER UMGANG MIT E-MAILS UND ONLINEDIENSTEN

Aufgrund der zahlreichen Vorfälle mit betrügerischen E-Mails an Hochschulen widmet sich das Modul Onlinebetrug vor allem den Fallstricken von Phishing, Spear Phishing, Social Engineering und gefälschten Webseiten. Erklärtes Ziel des Moduls ist es, die Sensibilität der Mitarbeitenden und Studierenden im täglichen Umgang mit E-Mails und Onlinediensten zu steigern. *SecAware.nrw* zielt besonders in diesem Modul auf die Erweckung einer „Habachtstellung" der Nutzenden ab, ohne jedoch Angst zu schüren oder den belehrenden Zeigefinger zu erheben. Vielmehr erschaffen die Videos des Moduls ein fundiertes Wissen, das eine gesunde Beurteilung von potenziellen Gefahren aufkommender Situationen erlaubt: Der Nutzer ist gewarnt, hinterfragt E-Mails und Korrespondenz und kennt nun Mechanismen, um Quellen zu verifizieren. Auch komplexe Betrugsszenarien, wie sie häufig bei Social Engineering vorkommen, werden in den Videos und interaktiven Elementen dargestellt und lösungsorientiert behandelt.

Nach Abschluss des Selbstlernangebots von *SecAware.nrw* können die Nutzenden den Tücken des digitalen Alltags deutlich sensibler, informierter und selbstsicherer entgegentreten.

SECAWARE 2.0

Der Bereich der IT-Sicherheit verlangt nach einem agilen Ansatz, der es nötig macht, die Selbstlernakademie kontinuierlich zu aktualisieren und in den nächsten drei Jahren um neue Module zu erweitern. Diese setzen sich mit vordergründigen Themen wie künstliche Intelligenz (KI) und speziell deren Anwendungen wie ChatGPT oder aber auch mit Thematiken wie modernen Angriffsvektoren auseinander. Diese Erweiterungen zielen darauf ab, das Angebot aktuell zu halten und den Nutzenden eine tiefere und breitere Kenntnisbasis zu bieten. Ein integraler Teil von SecAware 2.0 wird ein vertiefter Austausch mit CISOs der Hochschulen sein, um praxisnahe Erkenntnisse und Erfahrungen zu integrieren und das Lernangebot damit präziser an den realen Bedürfnissen auszurichten. Gleichzeitig schärft eine stetige Evaluation des Angebots die Effizienz und die Benutzerfreundlichkeit, um eine optimierte Nutzungserfahrung zu garantieren. Die Dynamik in der IT-Sicherheit – gekennzeichnet durch eine kontinuierliche Entwicklung neuer Bedrohungen und Schutzmechanismen – erfordert ein Selbstlernangebot, das gleichermaßen dynamisch ist, um auf diese Weise einen sicheren Umgang im Internet und mit neuen Technologien zu vermitteln.

Zusammenfassend lässt sich sagen, dass *SecAware.nrw* zwar in erster Linie für den akademischen Bereich entwickelt wurde, aber auch für Unternehmen eine wertvolle Ressource darstellt, um das Bewusstsein für Cybersicherheit in der Belegschaft zu schärfen. Die Inhalte sind modular und flexibel gestaltet, was eine leichte Integration in den Arbeitsalltag und eine schnelle sowie effektive Schulung der Mitarbeitenden ermöglicht. Mit interaktiven Elementen wie Quiz und praxisnahen Aufgaben fördert die Plattform die aktive Auseinandersetzung mit dem relevanten Themenbereich der Cybersicherheit. Als wissenschaftlich fundiertes und von Experten validiertes Tool steht *SecAware.nrw (https://SecAware.nrw/)* kostenfrei zur Verfügung, ist stets aktuell und passt sich kontinuierlich den neuesten Entwicklungen im Bereich IT-Sicherheit an. ■

Literatur

[1] *Bundesamt für Sicherheit in der Informationstechnik (BSI), Die Lage der IT-Sicherheit in Deutschland 2023, https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/Lagebericht2023.html?nn=129410, 2023*

[2] *Weidlich, L., Hackerangriffe: Die digitale Universität braucht eine Brandmauer, FAZ.NET, https://www.faz.net/aktuell/karriere-hochschule/hackerangriffe-die-digitale-universitaet-braucht-eine-brandmauer-18529880.html, 14. Dezember 2022*

[3] *Westdeutscher Rundfunk (WDR), Hackerangriff auf Fachhochschule Münster, Westdeutscher Rundfunk Köln, https://www1.wdr.de/nachrichten/westfalen-lippe/hackerangriff-fachhochschule-muenster-fh-100.html, 24. Juni 2022*

[4] *Der Spiegel, Alle Hochschulen in NRW Ziel von Cyberattacken, DER SPIEGEL, Hamburg, Germany, https://www.spiegel.de/start/hacker-greifen-unis-an-alle-hochschulen-in-nrw-ziel-von-cyber-kriminellen-a-85fe2a58-c389-4a69-924f-b79e85ecbd7d, 1. April 2023*

[5] *Beissel, S.: Security Awareness: Grundlagen, Maßnahmen und Programme für die Informationssicherheit, De Gruyter, 2019*

[6] *Pohlmann, Norbert, Security Awareness (Sicherheitsbewusstsein), Prof. Dr. Norbert Pohlmann Glossar, https://norbert-pohlmann.com/glossar-cyber-sicherheit/security-awareness-sicherheitsbewusstsein/, 2023*

[7] *Ministerium für Kultur und Wissenschaft des Landes Nordrhein-Westfalen, Vereinbarung zur Informationssicherheit an den Hochschulen (VzI), https://www.mkw.nrw/hochschule-und-forschung/digitalisierung-hochschule-und-wissenschaft/cybersicherheit#:~:text=Mit%20der%20zum%201,die%20Cybersicherheit%20zur%20Verf%C3%BCgung%20gestellt, 1. Juli 2023)*

MIRIAM NAß
Projekt- und Teamleiterin von SecAware.nrw sowie Doktorandin im Institut für Internet-Sicherheit – if(is) an der Westfälischen Hochschule Gelsenkirchen.

SILVANA REMMERS
Wissenschaftliche Mitarbeiterin im Projekt SecAware.NRW im Institut für Internet-Sicherheit – if(is) an der Westfälischen Hochschule Gelsenkirchen.

NORBERT POHLMANN
ist Professor für Cybersicherheit und Leiter des Instituts für Internet-Sicherheit – if(is) an der Westfälischen Hochschule in Gelsenkirchen sowie Vorstandsvorsitzender des Bundesverbands IT-Sicherheit – TeleTrusT und im Vorstand des Internetverbandes – eco.