

Special

NIS-2:
Risiko- und
Incident-Management meistern

S.10

**Notfall-
übungen:**
Unverhofft
kommt oft ...

S.18

it-sa 2023
*Trends,
Produkte
und Lösungen*

**Mehr Wert.
Mehr Vertrauen.**



NIS2 – Die IT-Aufrüstung der KRITIS-Betreiber

Die Europäischen Institutionen haben mit der NIS2-Richtlinie die EU-weite Gesetzgebung für die IT-Sicherheit aktualisiert. Bis Oktober 2024 muss sie in nationales Recht überführt werden, hierzu gibt es bereits Entwürfe.

Der Referenten-Entwurf zur Umsetzung der NIS2-Richtlinie macht deutlich, dass sich KRITIS-Betreiber frühzeitig mit NIS2 auseinandersetzen und die derzeit noch freiwilligen Audits als Chance begreifen sollten, um ihre eigenen IT-Defensivmaßnahmen bereits vor Fristende im Oktober 2024 von unabhängiger Experten-Seite prüfen und zertifizieren zu lassen.

Mit Zertifizierungen sind KRITIS-Betreiber auf der sicheren Seite. Wir prüfen Ihre IT-Infrastruktur und sorgen gemeinsam mit Ihnen dafür, Ihre IT-Sicherheit zu verbessern. Sprechen Sie uns an!

tuvsud.com/ms-kritis

Mehr Info





Der „Stand der Technik“ befeuert die Renaissance des Patchmanagements *Seite 4*

Schwachstelle „Zertifikate“ endlich schließen *Seite 9*

Risikomanagement und Incident-Management effizient meistern *Seite 10*

Ganzheitliches Risikomanagement: Herausforderungen integriert managen und Kosten senken *Seite 12*

Zero Trust – zentrale Antwort auf Bedrohungsszenarien *Seite 14*

G DATA CyberDefense setzt auf Managed EDR *Seite 16*

Unverhofft kommt öfter als erwartet ... *Seite 18*

Schritt für Schritt zu einem höheren Sicherheitsniveau *Seite 21*

Die größten Vorteile verhaltenspsychologischer Elemente in Security-Awareness-Trainings *Seite 24*

Warum Unternehmen No-Code IAM brauchen *Seite 26*

NIS-2: Das nötige Update der KRITIS-Sicherheit *Seite 29*

Wire integriert Federation *Seite 32*

In AI we Trust – secure it anyway we must *Seite 35*

News und Produkte *Seite 37*

Impressum



Augustinusstraße 11 A, 50226 Frechen (DE)
Tel.: +49 2234 98949-30,
Fax: +49 2234 98949-32
redaktion@datakontext.com,
www.datakontext.com

Geschäftsführer: Dr. Karl Ulrich

Handelsregister:
Amtsgericht Köln, HRB 82299

Bankverbindung: UniCredit Bank AG, München,
IBAN: DE34 7002 0270 0015 7644 54

Alle Rechte vorbehalten, auch die des aus-
zugsweisen Nachdrucks, der Reproduktion
durch Fotokopie, Mikrofilm und andere Ver-
fahren, der Speicherung und Auswertung
für Datenbanken und ähnliche Einrichtungen.

Zurzeit gültige Anzeigenpreisliste:
Nr. 41 vom 01. Januar 2023

Anzeigenleitung: Birgit Eckert
(verantwortlich für den Anzeigenteil)
Tel.: +49 6728 289003, anzeigen@kes.de

Media-Daten: Unsere Media-Daten finden
Sie online auf www.kes.info/media/.

Herstellungsleitung und Vertrieb:
Dieter Schulz, dieter.schulz@datakontext.com,
Tel.: +49 2334 98949-99

Satz: BLACK ART Werbestudio
Stromberger Straße 43a, 55413 Weiler

Druck: QUBUS media GmbH,
Beckstraße 10, 30457 Hannover

Titelbild: NürnbergMesse / Thomas Geiger



Der „Stand der Technik“ befeuert die Renaissance des Patchmanagements

Wer dem Stand der Technik in der sensiblen IT-Sicherheitsbranche entsprechen möchte, darf sich nicht nur auf die „großen“ Themen wie Ransomware, DDoS-Attacken und EDR konzentrieren. In einer umfassenden Security-Architektur spielen auch vermeintlich „kleine“ Themen eine große Rolle.

Von Michael Schröder, ESET Deutschland GmbH

Organisationen weltweit investieren so viel Geld in IT-Sicherheit wie noch nie. Die internationalen Ausgaben für Cybersicherheit sollen sich im laufenden Jahr auf rund 223,8 Milliarden US-Dollar summieren, prognostiziert das Marktforschungsunternehmen Canalis. Neue Sicherheitslösungen, moderne Security-Information-and-Event-Management-(SIEM)-Systeme oder professionelle Security-Operations-Center (SOC): Die Wunschliste der IT-Verantwortlichen ist lang und teuer. Wer seine Security auf den aktuellen Stand der Technik bringen

möchte, denkt fast automatisch in diese Richtung. Doch sinkt dadurch das Risiko, Opfer eines Angriffs zu werden? Oftmals sind es nämlich die vermeintlich kleinen, aber unterschätzten Gefahren, die Kriminellen Tür und Tor öffnen. Dazu zählen in allererster Linie auch Schwachstellen in Betriebssystemen und Software.

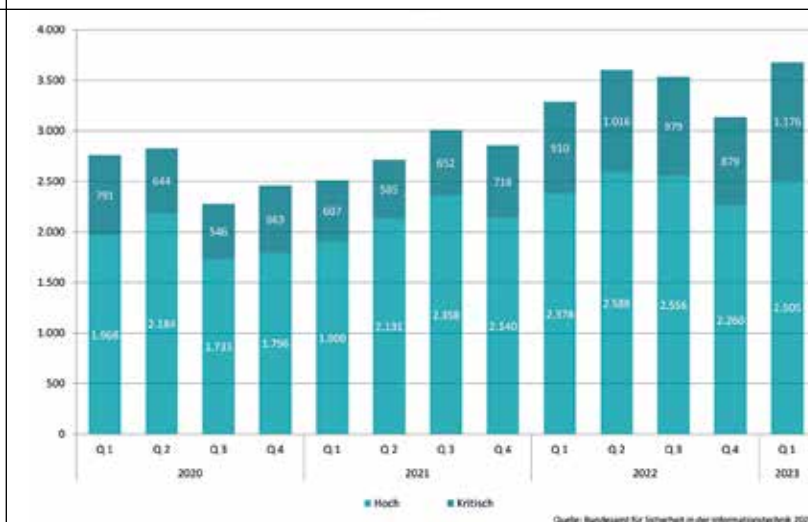
Sicherheitsvorfälle als Mahnung

Neu ist diese Erkenntnis beileibe nicht. In der Vergangenheit erfreute sich das Thema Vulnera-

bility- und Patchmanagement immer wieder großer Beliebtheit, um dann aus dem Rampenlicht zu verschwinden. Erst durch vermeidbare Sicherheitsverletzungen, als Unternehmen nicht oder zu spät auf bekannte Schwachstellen reagierte, horchten Verantwortliche erneut auf. Log4Shell, ProxyShell oder der berühmt-berüchtigte WannaCry-Ransomware-Angriff von 2017 sind nur einige Beispiele. Bei WannaCry wurden Systeme durch die Ausnutzung einer Microsoft-Sicherheitslücke infiziert, für die bereits ein Patch verfügbar war. Die Schadsoftware legte Tausende von Systemen weltweit lahm – auch noch viele Jahre später. Und die betroffenen Unternehmen erlitten massive finanzielle Verluste und Reputationschäden.

Aktuell vermelden nicht nur die Telemetriedaten von Security-Spezialisten wie ESET eine stark steigende Zunahme von Angriffen auf unzureichend gesicherte Systeme. Internationale Sicherheitsbehörden bestätigen den Eindruck mit der Veröffentlichung einer Liste der am häufigsten ausgenutzten Schwachstellen. Überraschenderweise zeigte

Abbildung 1: Bekannt gewordene Schwachstellen nach CVSS Score Anzahl (Bilder: ESET)



sich, dass Hacker gar nicht auf kürzlich bekannt gewordene Sicherheitslücken setzen. Stattdessen nahmen sie lieber ungepatchte und über das Internet erreichbare Systeme ins Visier. Grund dafür seien nicht zuletzt die für alte Schwachstellen längst verfügbaren Proof-of-Concept-Exploits, mit denen böswillige Akteure fremde Systeme leicht infiltrieren können.

Zahlen des Bundesamts für Sicherheit in der Informationstechnologie (BSI) unterstreichen den unschönen Trend: Die Anzahl der Schwachstellen wächst insgesamt und vor allem mit hohem oder sogar kritischem Level. Ins gleiche Horn stößt die amerikanische Organisation MITRE ATT&CK. Sie beziffert die Anzahl der sogenannten Common Vulnerabilities and Exposures (CVE) für das erste Quartal 2023 mit 7015: absoluter, jemals verzeichneter Rekord und vor allem um 15 Prozent höher als im Vorjahresquartal.

Gründe für verzögertes Patchen

Warum zögern Unternehmen oft, Patches zeitnah zu installieren? Ein Hauptgrund ist die Komplexität der IT-Infrastrukturen. Unternehmen verfügen über eine Vielzahl von Systemen, Anwendungen und Geräten, die alle aktualisiert werden müssen. Dies kann zeitaufwendig sein und den normalen Betrieb stören. Die Angst vor unerwünschten Nebenwirkungen oder Systemausfällen kann ebenfalls dazu führen, dass Unternehmen zögern, Patches einzuspielen. Darüber hinaus kann es schwierig und zeitaufwendig sein, Schwachstellen zu identifizieren und nach ihrem Schweregrad zu priorisieren, was zu einer ineffizienten Zuweisung von Ressourcen und einem erhöhten Risiko führt. Ressourcenknappheit und die Notwendigkeit, Patches vor der Implementierung gründlich zu testen, sind weitere Faktoren.

Vorteile eines effektiven Vulnerability- und Patchmanagements

Dabei liegen die Vorteile eines durchdachten Vulnerability- und Patchmanagements klar auf der Hand:

_____ Minimierung von Angriffsvektoren: Durch regelmäßige Aktualisierungen und die Schließung von Sicherheitslücken wird die Angriffsfläche für Cyberkriminelle erheblich reduziert.

_____ Einhaltung von Vorschriften: Viele Branchen unterliegen strengen Compliance-Anforderungen. Ein gutes Patchmanagement hilft, diese Vorschriften einzuhalten und hohe Geldstrafen zu vermeiden.

_____ Vermeidung von Datenverlust: Patches helfen dabei, Datenverluste und Datenschutzverletzungen zu verhindern, indem sie potenzielle Eintrittspunkte für Angreifer blockieren.

_____ Sicherung von Reputation: Effizientes Patchmanagement verhindert Sicherheitsverletzungen, die das Vertrauen der Kunden beeinträchtigen könnten. Der Schutz des Unternehmensrufs ist von unschätzbarem Wert.

_____ Kostenersparnis: Die finanziellen Auswirkungen von Sicherheitsverletzungen, die durch Patchen hätten verhindert werden können, sind oft deutlich höher als die Kosten und die Zeit, die für regelmäßiges Patchen aufgewendet werden.

NIS-2 patcht die Organisations-Security

Vielleicht muss man IT-Verantwortliche manchmal „zu ihrem Glück zwingen“, sagen immer mehr Sicherheitsexperten. Denn die Europäische Union hat mit der NIS-2-Richtlinie das Security-Level von KRITIS-Unternehmen deutlich angehoben. Spätestens am 17. Oktober 2024 müssen Organisationen das aus NIS-2 abgeleitete nationale Recht umgesetzt haben. Zentraler



Abbildung 2: Schritte des Vulnerability- und Patchmanagement-Prozesses

Inhalt ist die Aufforderung, die Resilienz der Systeme im Hinblick auf die Cybersicherheit zu stärken. Konkret müssen KRITIS-Betreiber die Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit ihrer informationstechnischen Systeme, Komponenten oder Prozesse sicherstellen, die für die Funktionsfähigkeit der von ihnen betriebenen kritischen Infrastrukturen maßgeblich sind. Und genau dazu gehört auch das Vulnerability- und Patchmanagement. Mit der NIS-2-Richtlinie werden über die bislang regulierten wesentlichen Organisationen hinaus demnächst weitere wichtige (ab einer Größe von 50 Mitarbeitern) als Adressaten des Gesetzes in den Fokus geraten. Der Anwendungsbereich der gesetzlichen Pflichten steigert sich damit um eine enorme Anzahl von Organisationen.

Auf dem Markt gibt es eine Vielzahl von Softwarelösungen, mit denen Organisationen das Problem in den Griff bekommen

Abbildung 3:
Mit der ESET
PROTECT Cloud-
Konsole lassen sich
Sicherheitslücken
bewerten und
Patches für das
gesamte Netzwerk
steuern.



können. Manche Hersteller wie ESET verzahnen sie direkt mit anderen Techniken. IT-Sicherheitsverantwortliche können so über eine zentrale Managementkonsole die Informationen aus dem Vulnerability- und Patchmanagement als eine von mehreren Datenquellen nutzen, um mögliche Bedrohungen zu verstehen.

ESET Vulnerability & Patch Management

ESET Vulnerability & Patch Management unterstützt Organisationen dabei, Sicherheitslücken in ihren Systemen zuverlässig zu erkennen und zu beheben. Hat die Software Schwachstellen in Betriebssystemen oder gängigen Anwendungen identifiziert, können Administratoren automatisch benötigte Patches installieren lassen oder manuell agieren. Die mitgelieferten Richtlinien vereinfachen den Verantwortlichen die Arbeit und lassen sich individuell anpassen. Mithilfe zahlreicher Filteroptionen können Schwachstellen entsprechend ihres Schweregrads priorisiert werden.

Die Lösung scannt Tausende gängiger Anwendungen wie Adobe Acrobat, Mozilla Firefox oder Zoom auf über 35.000 Sicherheitslücken und Gefährdungen (CVEs). Diese automatischen Überprüfungen sind in den Einstellungen flexibel konfi-

gurierbar und erlauben auch Ausnahmeregelungen. Schwachstellen können gefiltert und nach Gefährdungsgrad und zeitlichem Verlauf priorisiert werden. Über die cloudbasierte Konsole ESET PROTECT können Organisationen beispielsweise Reports über die am stärksten gefährdeten Anwendungen und betroffenen Geräte erstellen. Sie bietet mehrsprachige Unterstützung und stellt nur geringe Anforderungen an die IT-Infrastruktur.

Mit der zentralen Verwaltung über die ESET PROTECT Cloud-Konsole können Unternehmen auf einfache Weise Sicherheitslücken bewerten und Patches für das gesamte Netzwerk steuern, um die schnelle Erkennung und Behebung der neuesten Zero Day-Schwachstellen sicherzustellen. Darüber hinaus können Unternehmen mit automatischen und manuellen Patching-Optionen dafür sorgen, dass ihre Endpoints rechtzeitig mit den aktuellen Sicherheitsupdates versorgt werden. Zudem lässt sich der gesamte Prozess weiter vereinfachen, indem kritische Ressourcen vorgezogen und die restlichen Vorgänge auf Zeiten außerhalb der Geschäftszeiten gelegt werden. Das vermeidet Unterbrechungen im Arbeitsalltag. Organisationen können auch auf die Vorteile des mandantenfähigen Schwachstellen- und Patchmanagements zurückgreifen, um die volle

Transparenz über ihr Netzwerk zu erhalten und sich dennoch auf bestimmte Bereiche zu konzentrieren.

ESET Vulnerability & Patch Management ist elementarer Bestandteil folgender ESET Business Bundles:

_____ ESET PROTECT Complete beinhaltet neben Sicherheitslösungen für Endpoints, Mailserver und Cloud-Anwendungen auch Festplattenverschlüsselung sowie Cloud-Sandboxing.

_____ ESET PROTECT Elite bietet neben den Komponenten des Complete-Bundles natives Extended Detection and Response (XDR) sowie Multi-Faktor-Authentifizierung.

_____ ESET PROTECT MDR ist eine Lösung für Unternehmen, die ein umfassendes Cyber-Risikomanagement, Threat Hunting und ESET Expertise auf Abruf bietet. ESET PROTECT MDR kombiniert die Lösungen von ESET PROTECT Elite mit ESET Managed Detection and Response Services (MDR-Services).

Fazit

Vulnerability- und Patchmanagement ist ein Schlüsselfaktor für eine robuste IT-Sicherheitsstrategie und zählt zu den wichtigsten Maßnahmen im Hinblick auf den Stand der Technik in der Security. Indem Unternehmen kontinuierlich ihre Systeme und Anwendungen auf Schwachstellen überprüfen, können sie potenzielle Risiken minimieren und Angriffsvektoren einschränken. Die Investition in diese Prozesse ist unverzichtbar, um die Integrität, Vertraulichkeit und Verfügbarkeit von Unternehmensressourcen zu gewährleisten und den Anforderungen einer sich ständig verändernden Sicherheitslandschaft gerecht zu werden. ■

Messestand ESET
Halle 7, Stand 531
Kostenlose Tickets unter
www.eset.com/de/itsa-2023



Sicheres und datenschutzkonformes Messaging

Sie wollen mehr wissen?

Sprechen Sie mit uns auf der IT-SA. Termin buchen:
wire.com/de/it-sa



- Höchster Sicherheitsstandard unter Business-Messengern für individuelles und Gruppen-Messaging, Video- und Sprachkonferenzen
- IMMER Ende-zu-Ende verschlüsselt
- Selbstlöschende Nachrichten und viele weitere sicherheitsrelevante Funktionalitäten
- Management Konsole – Benutzermanagement und rollenbasierte Rechteverwaltung
- Federation ermöglicht datensouveräne Zusammenschaltung von Wire-Instanzen
- Gerüstet für NIS-2
- Operator- und Administrator-Shielding

wire.com/de/it-sa



NCP

Zero Trust

Cyberbedrohungen, Homeoffice und technologische Strategien wie SASE, Single Sign-On, SD-WAN oder Zero Trust stellen IT-Abteilungen vor Herausforderungen.

Schützen Sie Ihr Unternehmen mit der NCP Secure Enterprise Lösung und sichern Sie auch moderne Cloud-Technologien wie SD-WAN, SASE, SAML/SSO und Zero Trust durch zukunftssichere VPN-Technik ab.

Vertrauen Sie der richtigen Technologie?



Besuchen Sie uns:
Halle 7A-412



Automatisiertes Zertifikatsmanagement erhöht Schutz und Verfügbarkeit

Schwachstelle „Zertifikate“ endlich schließen

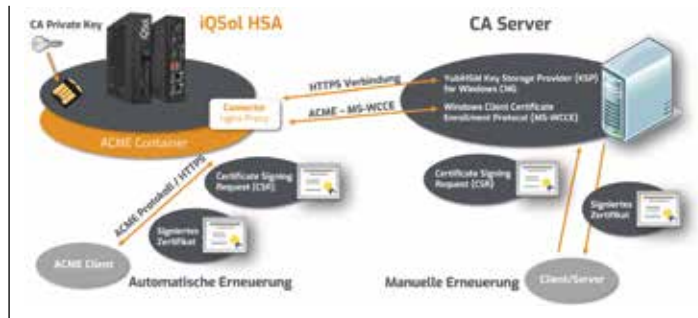
Greifen Cyberkriminelle IT-Infrastrukturen an, haben sie es immer auf den „heiligen Gral“ abgesehen: die PKI, Zertifikate und die wichtigsten „Schlüssel“. Die Hardware Security App (HSA) der niederösterreichischen iQSol GmbH verhindert diese Angriffe durch die hochsichere, zentrale Speicherung sowie die automatisierte Erneuerung von Zertifikaten mit dem neuen ACME-Feature. Kunden sollten ein Update ins Auge fassen, um unvermeidliche Überraschungen durch Ausfälle vorzubeugen.

Von Jürgen Kolb, iQSol GmbH

Mit der iQSol HSA, im Einsatz als physischer Mini-Server mit integriertem YubiHSM, können bis zu 16 PKI-Server angebunden werden. Sie benötigen lediglich eine Netzwerkverbindung und den Treiber. Dann wird das YubiHSM in Domänen unterteilt, wobei jeder Server nur Zugriff auf die eigenen Private-Keys hat. Statt einfacher Passwörter kommen hier also Smartcards zum Einsatz, die eine starke Authentifizierung zum Beispiel in Microsoft-Umgebungen oder im Active Directory ermöglichen. Die iQSol HSA erlaubt zudem das einfache, menügeführte Erstellen von Backups und stellt durch zwei Nodes die Hochverfügbarkeit sicher. Hochsichere Technologie und damit einhergehend die sicheren Abläufe erleichtern die Administration ebenso wie die übersichtliche Benutzeroberfläche.

Höchstes Sicherheitslevel sorgt für Einsparungen

Ein geordnetes Zertifikatsmanagement ist Grundstein dafür, dass keine unnötigen Ausfälle auftreten oder



Die Komponenten der Hardware Security App (HSA) von iQSol. (Bild: iQSol GmbH)

sich häufen. Da allerdings mit der manuellen Abarbeitung der Zertifikate-Deadlines oder der Beseitigung der Stillstände immense Arbeitsaufwände einhergehen, sollte diese rein administrative Aufgabe in einem Tool abgebildet und automatisiert sein. Andernfalls besteht neben der Gefahr der Kostenexplosion auch die hohe Wahrscheinlichkeit, dass besonders global tätige Unternehmen mit einer unübersichtlichen Internet-of-Things-Umgebung (Maschinen, Geräte, Anlagen) rasch den Überblick verlieren.

Leichter ausrollen und automatisch erneuern

Um Unternehmen das Zertifikatsmanagement weiter zu vereinfachen, verfügt die iQSol HSA daher neuerdings zudem über das „Automatic Certificate Management Environment“- (ACME)-Protokoll. Es ermöglicht das Zusammenspiel der Zertifizierungsstellen sowie der Server und damit die Bereitstellung einer kostengünstigen und sicheren Public-Key-Infrastruktur. Die dazu notwendigen Dienste laufen auf der iQSol HSA. Die ACME-Clients kommunizieren mit der HSA, die dann die Anfragen über den sogenannten Certificate-Authority-(CA)-Server abarbeitet. Zertifikate werden so über die Domänenvalidierung ausgerollt und automatisch erneuert. Das reduziert den Aufwand für die manuelle Verwaltung und gewährleistet jederzeitige Sicherheit.

Das Rundum-PKI-Sorglos-Paket

Natürlich kann man das Management auch ausgelagert und als Managed-Security-Service betreiben. Das macht vor allem dann Sinn, wenn die gesamte PKI erst aufgesetzt werden muss. Als eine der technisch anspruchsvollsten und höchstsensiblen Königsdisziplinen in der IT-Security gilt es auch hierbei, auf eine europäische Lösung und vertrauenswürdige Experten zu setzen. ■

Messestand iQSol

Halle 7, Stand 505

(Mitaussteller bei sysob IT-Distribution GmbH & Co. KG)

www.itsa365.de/de-de/companies/s/sysob-it-distribution-gmbh-co-kg/iqsol

NIS-2-Umsetzung

Risikomanagement und Incident-Management effizient meistern

Die NIS-2-Richtlinie macht Cyberrisikomanagement und Incident-Management für Betreiber wesentlicher und wichtiger Einrichtungen zur Pflicht. Aber auch für alle anderen Unternehmen ist beides unverzichtbar, um die Geschäftskontinuität zu sichern. Wie gelingt die Umsetzung am besten – trotz Fachkräftemangel und immer komplexerer IT-Umgebungen?

Von Richard Werner, Trend Micro

Um sich vor der wachsenden Bedrohung durch Cyberkriminelle zu schützen, müssen Unternehmen in der Lage sein, sowohl die Eintrittswahrscheinlichkeit eines Cyberangriffs als auch das mögliche Schadensausmaß zu minimieren. Für Betreiber kritischer Infrastrukturen ist das besonders wichtig, denn wenn sie ausfallen, hat das gravierende Auswirkungen auf die gesamte Gesellschaft. Die NIS-2-Richtlinie der EU schreibt daher Risikomanagement und Incident-Management verpflichtend vor. Während das deutsche Umsetzungsgesetz noch in der Abstimmungsphase ist, sollten Unternehmen jetzt schon aktiv werden.

Betroffene Unternehmen müssen prüfen, wie sie die neuen Security-Pflichten am besten erfüllen können. Eine der größten Herausforderungen ist und bleibt

der Fachkräftemangel. Viele IT- und IT-Security-Teams arbeiten ohnehin schon an ihrer Belastungsgrenze und sind mit immer komplexeren IT-Umgebungen konfrontiert. Doch auch ohne die gesetzliche Pflicht sind Cyberrisikomanagement und Incident-Management heute Security-Themen, an denen kein Unternehmen mehr vorbeikommt. Beide sind unverzichtbar, um alle drei Phasen im Lebenszyklus eines Cyberangriffs abzudecken: vor, während und nach der Attacke. Dabei gibt es einiges zu tun.

Vorbereitung

In der ersten Phase geht es darum, die eigene IT-Umgebung so gut zu schützen, dass Cyberkriminelle gar nicht erst angreifen. Dafür ist es wichtig, die Perspektive der Hacker einzunehmen. Welche Akteure gibt

es gerade, wie gehen diese vor und welche Schwachstellen nutzen sie bevorzugt aus? Dies gilt es, in Relation mit der individuellen Exposition des Unternehmens zu betrachten: Wo sind wir verwundbar? Wo würde bei einem Angriff der größte Schaden entstehen? Zählen wir zur Zielgruppe aktueller Angriffskampagnen? So gelingt es, Risiken zu identifizieren und zu priorisieren. Unternehmen können ihre Security-Ressourcen dann gezielt dort einsetzen, wo sie sie am dringendsten benötigen. Eine individuelle Risikobewertung schafft die Voraussetzung, um die Angriffsfläche zu reduzieren und die Eintrittswahrscheinlichkeit für eine Cyberattacke zu minimieren. Das erfordert eine gründliche Analyse von sowohl internen als auch externen Sicherheitsinformationen. Es reicht nicht, Risikomanagement nur sporadisch zu betreiben. Da sich IT-Umgebungen und Angriffsparameter schnell ändern, müssen Unternehmen ihre Cyberrisiken kontinuierlich im Blick behalten und neu bewerten.

Während des Angriffs: Detection und Response

Da es nie möglich sein wird, alle Risiken zu beseitigen, müssen Unternehmen immer damit rechnen, dass es einmal zu einem Cyberangriff kommt. Deshalb schreibt auch schon

Die Bestandteile der Vision-One-Plattform von Trend Micro (Bild: Trend Micro)



das IT-Sicherheitsgesetz 2.0 sowie demnächst NIS-2 vor, dass sogenannte „Systeme zur Angriffserkennung“ für KRITIS-Betreiber Pflicht sind. Hier kommt es darauf an, einen Vorfall möglichst früh aufzudecken und zu stoppen, bevor größerer Schaden entsteht. Damit das gelingt, brauchen Security-Teams schnell die richtigen Daten. Während eines Cyberangriffs müssen Unternehmen unter hohem Zeitdruck agieren und schwierige Entscheidungen treffen. Sollen wir ein verwundbares System vom Netz nehmen, weil die Hacker sich darauf zubewegen? Was verursacht höhere Kosten: das System abzuschalten oder eine Verschlüsselung? Laut NIS-2 müssen Unternehmen außerdem in der Lage sein, einen erheblichen Cybervorfall voraussichtlich innerhalb von 24 Stunden beim Bundesamt für Sicherheit in der Informationstechnik (BSI) zu melden. Auch dafür ist eine belastbare Datengrundlage unverzichtbar.

Nach dem Angriff: Incident-Response und Root-Cause-Analyse

Ist der Cyberangriff unter Kontrolle, stehen Unternehmen vor der Herausforderung, ihre Systeme schnell wieder – sicher – zum Laufen zu bringen. Immerhin verursacht jede Stunde, die ein Ausfall andauert, enorme Kosten. Dafür ist es wichtig, den Cybervorfall genau zu analysieren. Denn sonst besteht die Gefahr, dass man einen Backup-Stand einspielt, der bereits kompromittiert ist. Mit einer detaillierten Root-Cause-Analyse können Unternehmen nachvollziehen, wo die Eintrittspforte war und was passiert ist. Das schafft die Basis, um aus dem Vorfall zu lernen, die Sicherheitslücken zu schließen und erneute Angriffe zu vermeiden.

Aufwand und Komplexität reduzieren

Am besten lassen sich die Herausforderungen im Risiko- und

Incident-Management mit einem Plattform-Ansatz meistern. Genau dafür wurde Trend Vision One entwickelt: Die Lösung vereint Attack Surface Risk Management (ASRM) für ein effizientes Risikomanagement und Extended Detection and Response (XDR) für eine schnelle Bedrohungserkennung unter einer Plattform. Hier laufen die Daten aller angeschlossenen Security-Sensoren zusammen. Beide Technologien greifen darauf zu, kommunizieren und interagieren miteinander: ASRM errechnet aus internen und externen Security-Informationen kontinuierlich den aktuellen Risiko-Status der IT-Umgebung. XDR analysiert und korreliert Bedrohungsdaten, reduziert False Positives und zeigt auf einen Blick, was passiert ist.

Beide Technologien arbeiten KI-gestützt und bieten einen hohen Automatisierungsgrad, sodass Security-Teams entlastet werden. In einer zentralen Konsole gewinnen Unternehmen umfassende Transparenz sowohl über die Cyber Risiken als auch die Angriffssituation in der gesamten IT-Umgebung – von den Endpunkten über Server, E-Mail, Cloud-Dienste, Netzwerke bis hin zu 5G und Operational Technology (OT). Im Fall eines Cyberangriffs unterstützen die Erkenntnisse aus der Vision-One-Plattform auch bei der Root-Cause-Analyse. Incident-Response-Teams sparen dann viel Zeit, weil sie sofort auf wichtige Daten zugreifen können.

Generative KI optimiert die Gefahrenabwehr

Zusätzliche Entlastung bietet der in Trend Vision One integrierte KI-gestützte Cybersecurity-Assistent Companion. Beispielsweise verbessert das Tool die Effizienz, indem es Suchanfragen in Klartext ermöglicht und schnell relevante Informationen zur proaktiven Bekämpfung von Bedrohungen bereitstellt. Außerdem liefert Companion Erklärungen zu ebenenübergreifenden Ereigniswar-

nungen, Angreifer-Skripten und Befehlen in einfacher Sprache.

Security-Teams erhalten mit Trend Vision One Zugriff auf tiefgreifende Analysen und kontextbezogene, KI-gesteuerte Empfehlungen zur Schadensbegrenzung. Die Automatisierung von E-Mail-Benachrichtigungen, Support-Ticketvergabe und Berichterstattung über Vorfälle optimiert Prozesse und steigert die Effizienz.

Je früher, desto besser

Viele Unternehmen, die unter dem Fachkräftemangel leiden, entscheiden sich dafür, die Security-Plattform zusätzlich mit den Managed Services von Trend Service One Complete zu kombinieren. Spezialisierte Security-Analysten übernehmen dann das 24/7-Monitoring der XDR-Warnungen und unterstützen dabei, schnell die richtigen Gegenmaßnahmen zu ergreifen. Außerdem steht im Ernstfall garantiert ein Incident-Response-Team bereit. In der Kombination aus einem Plattform-Ansatz und Managed-Security-Services gelingt es mit überschaubarem Aufwand, alle drei Phasen im Lebenszyklus eines Cyberangriffs abzudecken und zentrale NIS-2-Anforderungen zu erfüllen. Dabei gilt: Je früher man ansetzt, desto besser. ASRM hilft, die IT-Umgebung so zu härten, dass Angreifer vorbeiziehen oder nur schwer vorwärtskommen. Security-Teams können den Vorfall dann XDR-unterstützt eher stoppen und das Schadensausmaß minimieren. Incident-Response-Teams haben dank der Security-Plattform sofort Zugriff auf wichtige Daten, Unternehmen können ihrer Meldepflicht nachkommen, und Systeme sind schneller wieder betriebsbereit. All das erhöht die Resilienz erheblich und spart am Ende Aufwand sowie Kosten. ■

**Messestand Trend Micro
Halle 7, Stand 235**

Ganzheitliches Risikomanagement: Herausforderungen integriert managen und Kosten senken

Unternehmen, die ihr Risikomanagement über alle Ebenen hinweg durchgängig betreiben und transparente und effiziente Geschäftsprozesse etablieren wollen, sollten sich von ineffizienten Insellösungen mit mangelnder Transparenz, unzuverlässigen Daten, redundanter Datenerhaltung, hoher Fehleranfälligkeit und Schnittstellenproblemen verabschieden.

Von Ellen und Werner Wüpper, WMC GmbH

In der Praxis stellt ein Risikomanagement, das ein optimales Chancen-Risiko-Verhältnis zur Ertragsgenerierung sicherstellt, nach wie vor eine große Herausforderung für Unternehmen dar. Bei einem solchen Projekt sind verschiedene Aspekte zu berücksichtigen und zu managen. Wichtige Teilbereiche sind hier das strategische, das finanzwirtschaftliche und das operative Risikomanagement.

In vielen Unternehmen ist es jedoch noch üblich, dass Risiken mit unterschiedlichen Vorgehensweisen in verschiedenen Anwendungen ermittelt und über Schnittstellen zusammengeführt werden. Zum einen werden dadurch viele Tätigkeiten doppelt durchgeführt und redundante Daten vorgehalten, zum anderen gehen viele Informationen bei der Übertragung über Schnittstellen verloren oder lassen sich nicht direkt für die Gesamtbewertung nutzen. Ein eher unbefriedigender Zustand. Dazu kommt noch, dass der Betrieb von mehreren Insellösungen im Bereich von Software auch häufig vermeidbare Kosten produziert.

Integriertes Managementsystem

Mit QSEC bietet das Unternehmen WMC bereits seit vielen Jahren ein am Markt erfolgreich eta-

bliertes integriertes Managementsystem an. In QSEC kann komfortabel und effizient nach den unterschiedlichsten Anforderungen und Vorgaben verschiedenster nationaler und internationaler Standards gearbeitet werden. Besonders wichtig ist WMC dabei die Investition in die stetige Weiterentwicklung des Produkts, um Anwendern immer die bestmögliche Usability und Aktualität für ihre jeweiligen Ansprüche zu bieten. Neben der Produktentwicklung, die sich an den aktuellen und zukünftigen Anforderungen orientiert, versteht sich WMC als Lösungspartner, der alle QSEC-Kunden bei Bedarf mit langjähriger Expertise aus der Umsetzung weltweiter Projekte unterstützt.

Mit QSEC V8.0 erweitert das Unternehmen nun die QSEC-Produktfamilie um das Zusatzmodul „Unternehmensrisikomanagement“. Dieses Modul bietet zukünftig die Möglichkeit, die gesamte Prozesskette des Risikomanagements in einer Organisation methodisch, durchgängig und effizient zu betreiben. Damit wird es möglich, alle Teilbereiche des Risikomanagements in einer Lösung bis ins Detail zu betrachten. Die aus dieser Durchgängigkeit resultierenden Synergien und optimierten Prozesse sparen Kosten und ermöglichen eine übergreifende Betrachtung von Chancen und Risi-

ken bei gleichzeitiger Reduzierung des Dokumentationsaufwandes.

Im Modul Unternehmensrisikomanagement werden neben den bisher in QSEC etablierten IT-Risikomanagementfunktionen die Risiken der Geschäftseinheiten, Geschäftsprozesse und Dienstleister ermittelt. Die in dieser QSEC-Ergänzung festgelegte Methodik der Risikobewertung berücksichtigt die unterschiedlichen Anforderungen aus den für das Unternehmensrisikomanagement relevanten Normen der ISO/IEC 31000, der BaFin, der MaRisk und weiterer normativer Vorgaben.

Alle Risiken von den sehr detaillierten IT-Risiken über die Geschäftsprozessrisiken (operationelle Risiken) und die Risiken der Organisationseinheiten bis hin zu denen der Gesellschaft (Legal Entity) können im QSEC-Unternehmensrisikomanagement erfasst, bewertet und aggregiert werden. Innerhalb des Bewertungsprozesses können ergänzend auch Dienstleister- und Projektrisiken identifiziert werden. Damit stehen alle Risiken in einem System zur Verfügung.

Die auf der obersten Ebene der Gesellschaft bewerteten Enterprise-Risiken (Unternehmens-, Markt-, Währungsrisiken etc.) können durch die Anzeige der zur Gesellschaft

zugeordneten Organisationsrisiken ergänzt werden (drill down). Auch die Geschäftsprozessrisiken der Organisationseinheiten lassen sich einsehen. Weiterhin auch die mit den Geschäftseinheiten verbundenen IT-Systemrisiken sowie die eventuell vorhandenen Dienstleister- und/oder Projektrisiken.

Alle Risiken werden nach individuellen Risikokatalogen mit den Bedrohungs- und Schwachstellenkriterien bewertet. Somit können einheitliche Risikostufen (z. B. A – D / rot bis grün) für eine übersichtliche Aggregation beziehungsweise Simulation verwendet werden.

Die Quantifizierung der Risiken erfolgt hinsichtlich ihrer Eintrittswahrscheinlichkeit und ihrer Auswirkungen. Ziel der Bewertung ist es, die identifizierten Risiken qualitativ durch geeignete Verteilungsfunktionen zu beschreiben. Die Risikoquantifizierung erfolgt über Risikokataloge mit den bereits angegebenen Bedrohungs- und Schwachstelleneinstufungen.

Die Risikoermittlung erfolgt nach der Risikoberechnung „Risiko = Eintrittswahrscheinlichkeit x Schadenshöhe“.

Usability und Akzeptanz

Die beschriebenen fachlichen Features und Methoden sind in QSEC die inhaltliche Basis des Enterprise-Risikomanagements. Ein weiterer wesentlicher Erfolgsfaktor für den Erfolg einer ganzheitlichen Riskmanagement-Lösung ist auch die Usability und Akzeptanz aller Anwendergruppen des Systems. In QSEC wird dieser Herausforderung große Bedeutung beigemessen.

WMC bietet den Anwendern – vom IT-Administrator über den Prozessverantwortlichen, der Bereichsleitung bis zur Geschäftsführung – individuelle Ansichten für spezielle Anwendergruppen, Wizards und



In QSEC werden alle Risikogruppen bewertet. (Bild: WMC GmbH)

Workflows. Jede Anwendergruppe erhält genau die Sichtweise, die sie erwartet. So stehen zum Beispiel für die umfangreiche und detaillierte IT-Risikobewertung übersichtliche Bewertungsformulare mit Vorlagen zur Verfügung. Der Akzeptanz der Bereichsleitung und Geschäftsführung wird mit selbsterklärenden Wizards (geführte Workflows, analog beispielsweise einer Flugbuchung) für eine einfache Bewertung Rechnung getragen.

Die verantwortlichen Risikomanager können die Erkenntnisse, die während der Risikoanalyse (besonders während der Risikoidentifikation und -bewertung) über alle Ebenen gewonnen wurden, im QSEC-Risikoinventar beziehungsweise der Risikobehandlungsplan enthält Informationen über die einzelnen Risiken, die Bewertung der Risiken, die Beurteilung der risikoreduzierenden Maßnahmen, Vorschläge zu Verbesserung des Status und eine Priorisierung der Maßnahmen. Zweck eines Risikoinventars ist es, besonders den Entscheidungsträgern einen komprimierten Überblick über die Risikosituation des Unternehmens zu geben. Neben der quantitativen Beurteilung kann auch eine qualitative Bewertung (z. B. potenzielle Schäden als Folge von Industriespionage, gesetzlichen Änderungen, Währungsschwankungen, Pandemie etc.) vorgenommen werden.

Dabei werden nicht nur die Risiken mit internen Auswirkungen betrachtet, sondern auch die Auswirkungen zum Beispiel auf die Kunden. Gerade Prozessrisiken können bei der internen Betrachtung geringere Folgen haben als bei der Kundenrisikobetrachtung.

Fazit

Mit QSEC und dem neuen Modul Unternehmensrisikomanagement bietet WMC als einer der ersten Anbieter eine komplett durchgängige Risikomanagementlösung für Unternehmen aller Branchen und Größenordnungen.

Die fortschreitende Digitalisierung und die damit einhergehende Cyberkriminalität sowie die Notwendigkeit, Risiken, die die Vermögens-, Finanz- und Ertragslage gefährden, frühzeitig zu erkennen, sind wesentliche Gründe, das Thema Risikomanagement systematisch zu bearbeiten. Auch können die Verantwortlichen den Mangel an Fachkräften und Spezialisten in diesem Bereich entschärfen und die Unterstützung und Vorteile einer effizienten Software wie QSEC nutzen. ■

**Messestand WMC Wüpper
Halle 7, Stand 309**

**it-sa Termin mit QSEC-Experten:
[wmc-direkt.de/veranstaltungen/
it-sa-kontaktformular](http://wmc-direkt.de/veranstaltungen/it-sa-kontaktformular)**

Zero Trust – zentrale Antwort auf Bedrohungsszenarien

Durch die aktuellen Rahmenbedingungen wie Fachkräftemangel, politische und wirtschaftliche Krisen oder die Disruptionen in den globalen Lieferketten bieten sich immer mehr Ansatzpunkte für Cybercrime. Nach der Corona-Pandemie haben sich neue Arbeitsmethoden etabliert, und die Netzwerke von Unternehmen, Banken und Verwaltungen sind stärker in den Fokus von Cyberkriminellen gerückt.

Von Heiko Fleschen, macmon secure

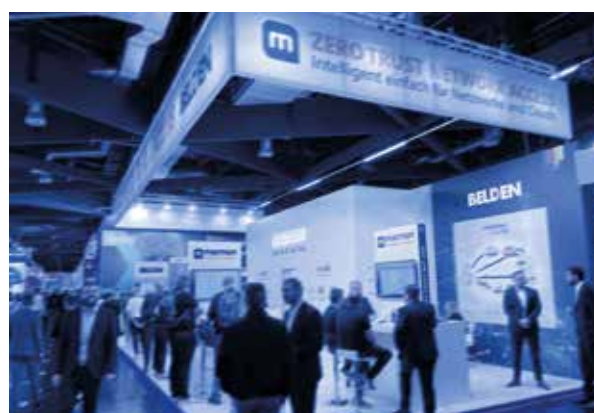
Umfassende Netzwerksicherheit ist unabdingbar, um Risikofaktoren zu reduzieren und den finanziellen Schaden und Reputationsverlust bei einer erfolgten Attacke gering zu halten. Dieser Aufgabe müssen sich CIOs, IT- und Rechenzentrumsleiter, IT-Sicherheitsverantwortliche und das Management bundesweit stellen. Übergeordnetes Thema auf der it-sa ist Zero Trust. Zero Trust Network Access (ZTNA) fußt auf der Philosophie, weder einem Gerät noch einem Benutzer bei der Anmeldung ins Netzwerk einen Vertrauensvorschuss zu geben, bevor es keine völlig sichere Authentifizierung gab. Mit macmon NAC für lokale Netzwerke und macmon SDP für Cloud-Lösungen bietet der deutsche Sicherheitsexperte macmon secure ein zentrales Angebot für die Abwehr von Cyberattacken.

20 Jahre macmon secure

macmon secure hat seine Kompetenz in mehr als 1500 Installationen bewiesen und verfügt über umfassende Erfahrung in unterschiedlichen Branchen. So vertrauen zahlreiche Behörden auf den Netzwerkschutz, denn die öffentlichen Verwaltungen beherbergen eine Fülle an sensiblen Daten – gleichzeitig müssen diese Daten flexibel für die verschiedenen Fachverfahren nutzbar sein – auf diversen Geräten und an unterschiedlichen Standorten. Banken, Kreditinstitute, Finanzdienstleister und Versicherungsunternehmen sind ebenfalls wichtige Kunden, denn sie arbeiten seit jeher mit Daten, die durch Missbrauch erheblichen finanziellen Schaden verursachen können. Gleichzeitig steigen gerade dort die Anforderungen an mobile Systeme. Zugriffsmöglichkeiten von überall und größtmögliche Flexibilität sind gefragt.

Sicherheit für IT- und OT-Netzwerke

Die zunehmende Vernetzung der Produktionssysteme steigert ihre Komplexität und Anfälligkeit. Im Gegensatz zur Office-Welt können sensible Komponenten in Produktionsnetzen, wie Roboter, Maschinen und Steu-



erungen, nicht mit üblichen Mitteln geschützt werden. Mit der Software-Plattform Belden Horizon bietet macmon eine einfache und praxiserprobte Verbindung zu OT-Netzwerken. Die Edge-Orchestrierungsfunktionen ermöglichen es, Anwendungen auf einem oder mehreren Geräten gleichzeitig zu implementieren und zu verwalten – lokal oder remote. Die Secure-Remote-Access-(SRA)-Technologie sorgt für sichere Verbindungen über Mobilfunk oder Kabel.

Zahlreiche Neuigkeiten auf der it-sa

Christian Bücken, Business Director bei macmon secure: „Auf der it-sa können sich interessierte Anwender über innovative Features informieren. Die Version macmon NAC 5.36.1 ist ab sofort verfügbar, und macmon SDP 2.0 stellt das nächste Level der Secure Perimeter Lösung dar. Interessenten zeigen wir gern die vielfältigen Anwendungsmöglichkeiten anhand von Kundenszenarios. Ich freue mich schon auf den regen Austausch mit den Besuchern.“

Messestand macmon secure, Halle 7, Stand 223

Vorträge:

Di: 10:30 Uhr (International Forum) Patrick Deruytter, Security considerations with IT/OT Convergence

Di: 14:45 Uhr (Forum D, Halle 7) Jochen Füllgraf, NAC: Ein kompakter Überblick über Ansätze und Lösungen

Mi: 12:30 Uhr (Forum C, Halle 7) Michael Reinholz, Intelligent Factory 4.0 – macmon NAC supports the Industry

Do: 11:45 Uhr (Forum C, Halle 7) Professor Tobias Heer, Keine Panik auf der Titanic – Wie man der Security-Havarie eines Industrie-Netzwerks mit NAC vorbeugen kann

Wir sichern Ihre digitale Welt

- **Cyber Security Consulting**
Reifegradunabhängige Beratung rund um Informationssicherheitsmanagement (ISMS), Sicherheitskonzepte, Security Trainings und Awareness sowie rund um das Security Operations Center (SOC)
- **Cyber Security Integration**
Von der Konzeption bis zur Umsetzung rund um Cloud Security, Identity Access Management, Network Security und Security Architecture Ihrer IT/OT
- **SOC Services**
Die eigene Sicherheit permanent im Blick mit SOC as a Service, Incident Response/ Forensik und Pentesting und Endpoint Security für Endgeräte-Hosts
- **Cyber Security Products**
Eigenbetrieb eines Security Operations Centers mit bewährter RADAR-Kerntechnologie zur Erkennung und Reaktion auf Sicherheitsvorfälle und damit verbundene Prozesse (RADAR Solutions), ultramobiles, flexibles Arbeiten bei maximaler Sicherheit (Secure PIM) sowie umfassende SAP Security für mehr Resilienz



Ganzheitliche Abwehrstrategien:

G DATA CyberDefense setzt auf Managed EDR

Der Schutz vor Cyberangriffen ist für Unternehmen von essenzieller Bedeutung und stellt sie gleichzeitig vor die große Herausforderung, IT-Sicherheit effektiv zu gestalten. Daher ist es für IT-Verantwortliche wichtig, sowohl auf die passende Lösung zu setzen, als auch einen verlässlichen Anbieter zu wählen. Dieser sollte verstehen, was genau gebraucht wird und Unternehmen dabei individuell unterstützen. Genau das bietet G DATA CyberDefense mit seinem leistungsstarken Portfolio aus Security-Lösungen wie Managed-Endpoint-Detection-and-Response, Security-Awareness-Trainings, Penetrationstests und Incident-Response.

Von Kathrin Beckert-Plewka, G DATA CyberDefense AG

Es reicht nicht aus, Bedrohungen im Unternehmensnetzwerk nur zu erkennen (detect). Entscheidend ist eine umgehende Reaktion (respond) auf schädliche Vorgänge im Fall eines erfolgreichen Angriffs. Viele IT-Teams sind damit überfordert, da sie einfach nicht genügend Zeit haben oder es an speziellem Fachwissen fehlt. Effektive IT-Sicherheit ist sehr aufwendig und erfordert Fachpersonal, Know-how und Erfahrung. Der anhaltende Fachkräftemangel macht es Unternehmen schwer, dabei kann man sich auch extern professionelle Hilfe holen, auf die IT-Verantwortliche zurückgreifen können. Eine gute Lösung ist G DATA 365 Managed Endpoint Detection and Response (kurz Managed EDR).

Cyberangriffe entdecken und sofort reagieren

Cyberkriminelle nutzen Feiertage, Wochenenden und Nächte, um Unternehmen anzugreifen. IT-Sicherheit ist daher eine Rund-um-die-Uhr-Aufgabe. IT-Teams müssen die IT-Systeme immer im Auge behalten, und vor allem muss im Fall einer Attacke eine sofortige

Reaktion erfolgen, um große Schäden abzuwenden. Dies können Unternehmen häufig kaum leisten. Bei Managed EDR von G DATA CyberDefense überwachen gut ausgebildete IT-Security-Fachleute alle Aktivitäten auf den IT-Systemen und stoppen Cyberangriffe – egal zu welcher Uhrzeit.

24/7-Expertenschutz

Das Monitoring übernimmt bei G DATA 365 Managed Endpoint Detection and Response ein Team von erfahrenen Fachleuten. Sie sind 24 Stunden täglich, an sieben Tagen in der Woche im Einsatz und werten die Ergebnisse der Sensorik aus. Dabei verifizieren sie zunächst, ob es sich um eine Attacke handelt. Ist dies der Fall, wird der Angriff genauestens analysiert. Danach erfolgen eine umgehende Reaktion und eine Einleitung von Gegenmaßnahmen, wie zum Beispiel das Separieren eines betroffenen Endpoints oder Dienstes vom Netzwerk. Unternehmen werden zudem über den Vorfall informiert. Sollte eine Mitwirkung durch die eigene IT-Abteilung nötig sein, geben die Experten von G DATA klare Handlungsempfehlungen.

Alle Informationen laufen in einer Webkonsole zusammen, in der IT-Teams in Echtzeit eine Übersicht erhalten, ob und welche Security-Vorfälle es gab und welche Maßnahmen die Fachleute von G DATA ergriffen haben. Zudem finden sie hier Handlungsempfehlungen, wenn diese nötig sind.

Unternehmen profitieren beim Einsatz der gemanagten EDR-Lösung von der langjährigen Erfahrung und dem Know-how des deutschen Cyber-Defense-Spezialisten. Mitarbeitende in Unternehmen können sich ihren Aufgaben widmen, während G DATA die IT-Systeme überwacht und Angriffsversuche stoppt. Der deutschsprachige und kostenfreie 24/7-Support unterstützt bei Fragen und Problemen. Ein weiterer Vorzug der Dienstleistung: Die verarbeiteten Daten verbleiben ausschließlich in Deutschland auf den Servern des strategischen Partners IONOS in Frankfurt am Main und Berlin sowie auf den unternehmenseigenen Servern von G DATA am Bochumer Unternehmensstandort. Damit unterliegen die Informationen den strengen deutschen Datenschutzgesetzen und der EU-Datenschutzgrundversorgung.

Human Centered Security

Eine weitere wichtige Komponente im Kampf gegen Cyberkriminelle ist die Belegschaft eines Unternehmens. Eine Studie des Ponemon Instituts aus den USA zeigt, dass 54 Prozent aller Cyberangriffe auf menschlichen Fehlern basieren. Die Angreifergruppen setzen auf Phishingmails, um Angestellte zur Herausgabe von Zugangsdaten für bestimmte Dienste zu bewegen.

Die Security-Awareness-Trainings von G DATA zielen darauf ab, das Bewusstsein für Cyberrisiken und den Umgang damit bei der Belegschaft zu steigern und sie mit dem nötigen Wissen auszustatten. Hierzu lernen sie in Online-Kursen zu verschiedenen Themen der IT-Sicherheit, wie sie sich vor digitalen Gefahren schützen können. Das E-Learning ermöglicht dabei flexibles Lernen an jedem Ort. Die Trainings lassen sich leicht in den Arbeitsalltag integrieren, und durch regelmäßige Wiederholungen festigt sich das Wissen langfristig. Die Security-Awareness-Trainings werden dabei in drei aufeinander aufbauenden Leveln absolviert: In Level eins werden zunächst die Grundlagen vermittelt. Auf der nächsten Stufe bauen Lernende spezielleres Wissen auf, und in Level drei geht es um tiefgreifendes Wissen rund um IT-Sicherheit.

Ein zentraler Baustein der G DATA Security Awareness Trainings ist die Phishing-Trainingsreihe. Durch charakterbasiertes Storytelling und spielerische Interaktion ist maximaler Lerntransfer garantiert, weil ein besonders praxisnaher und nachhaltiger Weg der Wissensvermittlung geschaffen wird.

Virensan in der Cloud

Sinnvoll ist außerdem auch die Absicherung von Diensten, auf denen Daten geteilt werden. Viele Informationen liegen in Unterneh-



Besuchen Sie unsere hybriden Workshops. **Jetzt anmelden** und **Gratis-Ticket sichern!**



men in gemeinsam genutzten Verzeichnissen. Dadurch entsteht ein größeres Risiko, dass darunter auch Schadprogramme sein könnten, die weiterverbreitet und hohen Schaden anrichten können. Mit G DATA Verdict-as-a-Service (kurz VaaS), einem cloudbasierten Virenschutz, können Unternehmen alle Daten auf Schadhaftigkeit prüfen. Der Scan erfolgt dazu nicht auf dem Endpoint, sondern in der Cloud. VaaS ist schnell und leicht skalierbar – von einer einzelnen Datei bis zu einer Vielzahl. Der Dienst lässt sich dabei individuell anpassen und ist einfach in Anwendungen, Webseiten oder Dienste integrierbar.

Für Unternehmen bietet die Lösung dabei mehrere Vorteile: Der Datenbestand ist frei von Malware. Es müssen keine Investitionen in Hardware erfolgen, der Betrieb eines zusätzlichen Servers ist beispielsweise nicht nötig. Zudem sind für die Implementierung keine spezifischen Kenntnisse in IT-Sicherheit erforderlich. G DATA Verdict-as-a-Service wird wahlweise in DSGVO-konformen Rechenzentren von IONOS betrieben oder in der Firma selbst gehostet. ■

Messestand G DATA
Halle 7, Stand 210

G DATA veranstaltet auf der it-sa neben seiner Standpräsenz und Vorträgen auch drei kostenlose Workshops zu aktuellen Cybergefahren und Abwehrmaßnahmen:

Im Workshop „IT-Security über die Cloud: Was bringen 'managed' und 'as-a-Service'-Produkte?“ zeigen Stefan Hausotte (Head of Threat Intelligence & Infrastructure, G DATA CyberDefense), Florian Kuckelkorn (Head of OEM Solutions, G DATA CyberDefense) und Tobias Becker (Senior Partner Cloud Solutions Architect, IONOS) am 10. Oktober 2023 von 14:30 bis 16:00 Uhr im Live-Hacking, wie Angreifer in IT-Systeme einbrechen und wie ein gesamtheitliches Verteidigungskonzept schützen kann.

Wie unkompliziert G DATA VaaS integriert werden kann, wird am 10. Oktober 2023 von 16:00 bis 17:30 Uhr im Workshop „Live Coding: AntiMalware SDK nutzen & eigenes Plugin für MS Teams bauen“ demonstriert.

„Vor & nach dem Cyberangriff: Worauf es ankommt“ heißt es in einem Workshop am 11. Oktober 2023 von 9:30 bis 12:30 Uhr mit dem Fokus Security Awareness Trainings und Incident Response.

Alle Workshops finden auf dem it-sa Kongress in NCC Ost, Raum Singapur statt. Mehr Informationen und die Möglichkeit, sich für die Workshops anzumelden, finden Sie unter www.gdata.de/it-sa.

Notfallübungen als Rückversicherung für den Ernstfall

Unverhofft kommt öfter als erwartet ...



Betriebsunterbrechungen treten zu jeder Tages- und Nachtzeit, meist unerwartet und immer häufiger in nicht vorhersehbarem Ausmaß auf. Lässt sich Ihr Unternehmen von möglichen Störungen, Notfällen und Krisen überraschen – getreu dem Motto „wird schon nicht passieren“? Oder setzen Sie sich schon im Vorfeld mit dem „Udenkbaren“ auseinander, um auf derartige Situationen optimal und vor allem strukturiert mit einer guten Krisenführung zu reagieren? Und drittens die Kernfrage: Bewährt sich das Notfall- und Krisenmanagement im Ernstfall?

Von Silke Menzel, HiScout GmbH

Allein im Jahr 2022 wurden 81 deutsche Unternehmen Opfer einer Cyberattacke, wobei die Dunkelziffer garantiert um einiges höher ist. Dabei sind Cyberangriffe nur eine Form aller Notfälle. Im Allianz Risk Barometer 2023 rangieren Betriebsunterbrechungen mit 46 Prozent noch vor den Cybervorfällen mit 40 Prozent. Vor diesen Ereignissen ist kein Unternehmen gefeit – das gilt für große Konzerne ebenso wie für Kleinbetriebe, Mittelständler, aber auch für die öffentliche Verwaltung. Inzwischen werden viele der Aussage des Technikvorstands des deutschen Energieversorgers EWE vom Mai 2022 zustimmen: „Wir haben kein Erkenntnisproblem, sondern ein Umsetzungsproblem.“ Ein Beispiel hierfür ist eine Notfallübung für einen Stromausfall in einem Krankenhaus. Während der Übung trat tatsächlich ein Stromausfall ein, und es stellte sich heraus, dass die Backup-Stromversorgung des Krankenhauses nicht ordnungsgemäß funktionierte. Dadurch konnten lebenswichtige medizinische Geräte nicht betrieben werden, was die Sicherheit der Patienten gefährdete und zudem das Vertrauen in das Krankenhaus erschütterte.

Dieses Beispiel verdeutlicht: In den meisten Unternehmen sind zwar Notfallkonzepte und -pläne vorhanden, nur die Umsetzung ist oftmals nicht erprobt, geschweige denn optimiert. Um den Prozess der Notfallarbeit hinsichtlich seiner Wirksamkeit und Zweckmäßigkeit zu überprüfen und nach Möglichkeit auch zu verbessern, ist die Durchführung regelmäßiger Notfallübungen erforderlich. Das ist die Königsdisziplin des Business-Continuity-Managements (BCM). Die Notfallplanung kann nur die grundsätzlichen Abläufe festlegen. Daher ist es für eine Organisation überlebenswichtig, dass jedes Ausfallszenario im Idealfall jährlich geübt wird und die Notfallmaßnahmen sowie das Bewusstsein der Mitarbeiter dafür trainiert werden, damit im Ernstfall die Abläufe effizient funktionieren. Hierin zeigt sich die wahre Qualität der Notfallvorsorge.

Die Vorbereitung einer Notfallübung im Unternehmen erfordert eine sorgfältige Planung und Durchführung. Ein Tool kann die Vorbereitung einer Notfallübung erleichtern und mit einem sinnvollen Vorgangsmanagement beim

Durchführen der einzelnen Schritte unterstützen. Folgendes Vorgehen hat sich hierbei bewährt:

1. Identifizieren Sie potenzielle Notfallszenarien: Erstellen Sie eine Liste der möglichen Notfallsituationen, die in Ihrem Unternehmen auftreten könnten.
2. Prüfen Sie, welche Übungsarten Ihr Unternehmen aus regulatorischen Vorgaben oder aufgrund einer Zertifizierung durchführen muss.
3. Wählen Sie basierend auf der Relevanz und Wahrscheinlichkeit der verschiedenen Notfallszenarien diejenigen aus, die in einer Übung simuliert werden sollen, und überlegen Sie, mit welcher Übungsart das jeweilige Szenario geübt werden soll. Berücksichtigen Sie dabei die spezifischen Risiken und Anforderungen Ihres Unternehmens.
4. Erstellen Sie eine Jahresplanung für alle im laufenden Jahr durchzuführenden Übungen. Damit erfüllen Sie gleichzeitig eine

Vorgabe aus Sicht einer Revision oder eines Audits.

5. Definieren Sie klare Ziele für die Notfallübung: Mögliche Ziele könnten zum Beispiel sein, einen IT-Hot-Stand-by oder die Evakuierung des Gebäudes zu testen, die Kommunikation zwischen den Mitarbeitenden zu verbessern oder deren Reaktionszeit auf einen Notfall zu verkürzen.
6. Ein notwendiger Schritt, der die Durchführung und Auswertung der Übung erleichtert, ist die Erstellung eines Übungskonzeptes, das alle Informationen der Übung detailliert beschreibt und mögliche Abhängigkeiten und Auswirkungen berücksichtigt. Dieses Konzept verschafft Ihnen nicht nur eine Übersicht und erleichtert die Vorbereitung. Damit werden auch die organisatorischen, materiellen und finanziellen Aufwände transparent, und betroffene Fachbereiche und Ressourcen können besser informiert und gesteuert werden.
7. Erstellen Sie einen Aktionsplan oder auch ein Übungsdrehbuch. Diese sollten jeden geplanten Übungsschritt mit Informationen wie Datum, Uhrzeit, beteiligte Mitarbeitende, Rollen und Verantwortlichkeiten, Kommunikationsmittel und übungsbezogene Anweisungen sowie das zu erwartende Ergebnis enthalten.
8. Die leider oft aufwendige Vorbereitung der Übung sichert deren erfolgreiche Durchführung und deren Realitätsnähe. Klären und überprüfen Sie die Sicherheitsvorkehrungen in Ihrem Unternehmen, um sicherzustellen, dass diese den aktuellen Standards entsprechen. Stellen Sie sicher, dass alle Notausgänge gut zugänglich und gekennzeichnet

und dass die Feuerlöscher und andere Notfallausrüstungen in gutem Zustand sind. Informieren Sie je nach geübtem Szenario auch externe Beteiligte. Dies können sowohl Ihre Dienstleister wie auch die örtliche Polizei oder Feuerwehr sein (Es könnte Sie eine Menge Bier für das nächste Feuerwehrfest kosten, sollten diese durch eine Übung unnötig alarmiert werden).

9. Die Ankündigung und Durchführung der Notfallübung gemäß dem Aktionsplan ist der entscheidende Schritt. Bereiten Sie Ihre Mitarbeitenden auf die bevorstehende Notfallübung vor, und geben Sie ihnen klare Anweisungen, wie sie sich während der Übung verhalten sollen. Stellen Sie sicher, dass alle Beteiligten das Vorgehen verstehen, die Handlungsanweisungen, Geschäftsfortführungspläne oder Notfallhandbücher in der aktuellen Version vorliegen haben und wissen, wie sie im Notfall handeln sollten. Stellen Sie sicher, dass alle relevanten Aspekte des Übungsszenarios berücksichtigt werden, und protokollieren Sie die Beobachtungen und Ergebnisse der im Aktionsplan beziehungsweise im Übungsdrehbuch beschriebenen Schritte. Nur eine dokumentierte Übung ist auch eine durchgeführte Übung.
10. Keine Erkenntnis ohne Auswertung und Feedback: Im Anschluss an die Übung sollte eine Bewertung durchgeführt werden, um zu sehen, wie gut die Beteiligten reagiert haben und ob die gesteckten Ziele erreicht wurden. Nicht nur die Auswertung der Beobachtungen, auch das Feedback der Teilnehmenden ist ein wertvoller Beitrag, um mögliche Verbesserungen zu identifizieren. Basierend auf diesen Erkenntnissen ist es sinnvoll, die Notfallpläne ent-

sprechend zu aktualisieren und anzupassen.

Es sind viele Punkte und Aspekte zu berücksichtigen, wenn eine Notfallübung nicht an mangelnder Vorbereitung, Kommunikation, Koordination oder technischen Problemen scheitern soll. Damit man jederzeit den Überblick hat, kann der Einsatz eines BCM-Tools wie das von HiScout hilfreich sein. Zu jedem Planungsschritt gibt es eine entsprechende Dokumentation – und ein integriertes Vorgangsmanagement unterstützt bei der Vorbereitung und Durchführung der Notfallübung. Erkenntnisse, Handlungsempfehlungen und Maßnahmen können ebenso darin festgehalten werden wie deren Umsetzungspflege und -nachweise. Die erreichten und durch die Übung verifizierten Wiederherstellungszeiten von zum Beispiel IT-Services werden in den Soll-Ist-Vergleich zurückgespiegelt, sodass der entsprechende Handlungsbedarf im Sinn einer kontinuierlichen Verbesserung sofort deutlich wird.

Am Ende erhält man ein Ergebnis, dass das Unternehmen resilienter macht und die eigene Position innerhalb des Unternehmens stärkt. Nur so können Verantwortliche sicherstellen, dass im Ernstfall optimal gehandelt wird. ■

Messestand HiScout GmbH Halle 7A, Stand 619

Silke Menzel hält am 10. Oktober um 15:00 Uhr auf der it-sa einen Vortrag zum Thema „Im Ernstfall optimal handeln – Wie Sie toolgestützt Ihre Notfallübungen effektiv vorbereiten, durchführen und auswerten“

HUMAN RISK REVIEW 2023

Neue Brancheneinblicke von führenden Security-Expertinnen und -Experten



Halle 7 | Stand 324

Holen Sie sich Ihr kosten-
loses Exemplar bei uns ab!

- 9 ausführliche Interviews mit Security-Führungskräften
- Umfrage unter Expertinnen und Experten zum Stand von Cyber Security in Europa
- Detaillierte Social-Engineering-Analysen zu den erfolgreichsten Taktiken der Cyberkriminellen



Welche Maßnahmen bei der Abwehr von Cyber-Attacks helfen

Schritt für Schritt zu einem höheren Sicherheitsniveau

Unternehmen und Behörden müssen sich darauf einstellen, dass Cyber-Angriffe weiter zunehmen. Jede Organisation könnte Opfer einer Attacke werden. Unsere Autorin beschreibt, worauf sich IT-Sicherheitsexpert:innen einstellen müssen und wie sie im Wettlauf mit Angreifern die Nase vorn behalten.

Von Heike Abels, Materna



Bild: puhhalstock.adobe.com

Laut Angaben des Bundeskriminalamtes zur Lage der Cyber-Sicherheit wurden im vergangenen Jahr knapp 137000 Unternehmen in Deutschland Opfer von Cyber-Angriffen. Eine Umfrage des Branchenverbands Bitkom zeigt, dass 63 Prozent der Unternehmen mit einem Angriff innerhalb eines Jahres rechnen. Davon wiederum glauben nur 43 Prozent, eine Cyber-Attacke erfolgreich abwehren zu können. Und was ist mit dem Rest?

Wie schätzen Sie Ihre Chancen ein, sich erfolgreich zu verteidigen? Gehören Sie zu den 57 Prozent, die nicht wissen, ob das eigene Unternehmen gut genug vorbereitet ist, oder glauben Sie, dass es nicht im Fokus von Hackern steht? Potenziell alle Unternehmen und auch Behörden können Ziele von Cyber-Attacks werden. Die Angriffe nehmen zu, und die Angreifer entwickeln ihre Methoden kontinuierlich

weiter. Es wird also höchste Zeit, den Kriminellen mit professionellen Schutzmaßnahmen zu begegnen.

Schwachstellen finden und schließen

Irgendwann ist er plötzlich da – der Anruf, den kein IT-Sicherheitsverantwortlicher jemals bekommen möchte: Die Organisation wurde gehackt. An der Stelle ist noch nicht klar, ob Daten verschlüsselt wurden oder abgeflossen sind und wie hoch der Schaden sein wird. Es wird nur deutlich, dass die Schwachstelle sofort geschlossen werden muss. Jetzt sollten die Verantwortlichen einen Notfallplan mit allen erforderlichen Maßnahmen in der Tasche haben. Das setzt voraus, dass sie sich über den Notfall bereits Gedanken gemacht und bestenfalls ein Business-Continuity-Management für den Erhalt der Geschäftsfähigkeit miteinbezogen haben.

Ist die Schwachstelle erst einmal gefunden und geschlossen, beginnt die forensische Arbeit, in der aufgearbeitet wird, an welcher Stelle das Leck entstanden ist. Schwachstellen können verschiedene Faktoren sein, wie zum Beispiel eine unzureichende Security-Software. Der größte Risikofaktor ist jedoch der Mensch – der Mitarbeitende, der einmal in einer harmlos wirkenden E-Mail auf den falschen Button geklickt hat. Jeden Tag erreichen rund 3,4 Milliarden betrügerische E-Mails Postfächer weltweit. Diese E-Mails, die per unbedachtem Knopfdruck Schadsoftware installieren oder vertrauliche Daten abfangen, sind für Laien oft schwer zu identifizieren. Mit regelmäßigen Security-Trainings und Awareness-Schulungen erlangen Mitarbeitende einen sichereren Umgang mit E-Mails und lernen, woran sie verdächtige Mails erkennen. Ebenso können die Infrastruktur und Anwendungen mittels Schwachstel-

lenanalyse und Pentests gezielt auf Schwachstellen geprüft werden.

Überwachung mit Argusaugen

Alle Schwachstellen im Blick zu behalten, ist bei der Vielzahl der Anwendungen innerhalb einer Organisation und der Schnelligkeit der Angreifer nicht einfach. Hier kann ein Security-Operations-Center (SOC) Abhilfe schaffen. Ein SOC ist vor allem ein Überwachungs- und Meldesystem: Auf Basis eines Security-Information- and Event-Managements erfasst und analysiert es sämtliche Aktivitäten im Netz einer Organisation. Anhand vordefinierter Regeln erkennt und meldet es Ereignisse, die auf einen möglichen Sicherheitsvorfall hindeuten, an das Cyber-Security-Incident-Response-Team. Hier laufen dann weitere Analysen und gegebenenfalls Maßnahmen zur Gefahrenabwehr. Der Erfolg des SOC-Konzepts beruht vor allem auf zwei Aspekten. Zum einen bündelt es zentral sämtliche sicherheitsrelevanten Informationen aus den unterschiedlichen Tools zur Überwachung von Clients, Servern, Netzen und Anwendungen. Das ermöglicht es, gefährliche Zusammenhänge zwischen verteilt auftauchenden Events zu erkennen, die ansonsten unentdeckt blieben – wenn zum Beispiel ein Benutzer an mehreren Orten auf verschiedenen Kontinenten gleichzeitig eingeloggt ist. Zum anderen dokumentiert es lückenlos alle sicherheitsrelevanten Daten. Das ermöglicht die Rückverfolgung von Angriffen und deren Urhebern. Außerdem können Unternehmen mit Reportings auf Basis der Informationen aus dem SOC den Status ihrer Sicherheitsvorkehrungen belegen und damit wichtige Compliance-Vorgaben erfüllen.

Sensibilisierung für Risiken

Die Einfallstore für Schadsoftware hat das SOC oder SOC-as-a-Service rund um die Uhr im Blick. Auch die schützenswerten Daten

selbst benötigen einen Schutzwall in Form von Cloud-Security-Maßnahmen wie etwa eine Public-Key-Infrastructure oder eine Multi-Faktor-Authentifizierung, um die digitale Identität eines Users nachzuweisen. Was einfach klingt, erfordert jedoch ebenfalls eine gewisse Vorarbeit. Beispielsweise wissen viele Unternehmen nicht, welche ihrer Informationen und Daten besonders schützenswert sind.

Mit einem Informationssicherheits-Management-System (ISMS) lässt sich das beheben. Informationssicherheit befasst sich nicht nur mit Daten, sondern mit gänzlich allen Informationen eines Unternehmens oder einer Behörde. Bei der Implementierung eines ISMS werden vorhandene Richtlinien beim Aufbau von Prozessen oder der Anpassung bestehender Prozesse berücksichtigt. Auf dieser Basis können regelmäßige Audits erfolgen, um Zertifizierungen wie IT-Grundschutz oder ISO 27001 zu erhalten.

Ebenso können Organisationen sich mit einem ISMS selbst überprüfen oder extern überprüfen lassen. Mittels GAP-Analysen lassen sich Risiken feststellen und bewerten, um daraus ein fundiertes Sicherheitskonzept abzuleiten beziehungsweise weiterzuentwickeln.

Im Ernstfall arbeitsfähig bleiben

Selbst mit allen Sicherheitsmaßnahmen sind Organisationen nicht unverwundbar. Wichtig ist, im Vorfeld einen Plan für den Notfall entwickelt zu haben, in dem Abläufe klar geregelt sind und mithilfe eines Business-Continuity-Managements genauestens vorgegeben ist, wie die Geschäftsprozesse weiter laufen. Denn ein Stillstand verursacht häufig Schäden in Millionenhöhe.

Mit Blick auf die aktuelle Lage zur Cyber-Security lässt sich feststellen, dass noch großer Nach-

holbedarf herrscht. IT-Sicherheit darf kein isoliertes Thema der IT-Abteilung bleiben, sondern muss sich auf die gesamte Organisationsstruktur beziehen. Im Jahr 2023 sollen in Deutschland rund 8,5 Milliarden Euro für IT-Sicherheit ausgegeben werden. Der IT-Branchenverband Bitkom empfiehlt, etwa 20 Prozent der gesamten IT-Ausgaben in das Thema Cyber-Sicherheit zu investieren. Denn eines ist klar: ohne Investitionen gelingt kein umfassendes zukunftsfähiges IT- und Informationssicherheitsystem.

Wirtschaftsunternehmen ebenso wie die öffentliche Verwaltung sind gut beraten, sich mit ersten Maßnahmen dem Thema zu nähern: beispielsweise mit regelmäßigen Awareness-Schulungen für alle Mitarbeitenden und der Erarbeitung des Notfallplans, um im Ernstfall den Schaden gering zu halten. Darüber hinaus bringt eine IST-Analyse Klarheit über den aktuellen Stand der Sicherheit und stellt weitere Maßnahmen in einem absehbaren Zeitraum in Aussicht. So lassen sich Schritt für Schritt Security-Maßnahmen ergänzen, damit Unternehmen und Behörden sich bestmöglich gegen Angreifer schützen können. ■

**Messestand Materna
Radar Cyber Security
Halle 7A, Stand 516**

Vorträge

10. Oktober 2023, 15:45 Uhr, Forum E, Halle 7A

„Cyber-Resilienz ganzheitlich und europäisch gedacht“

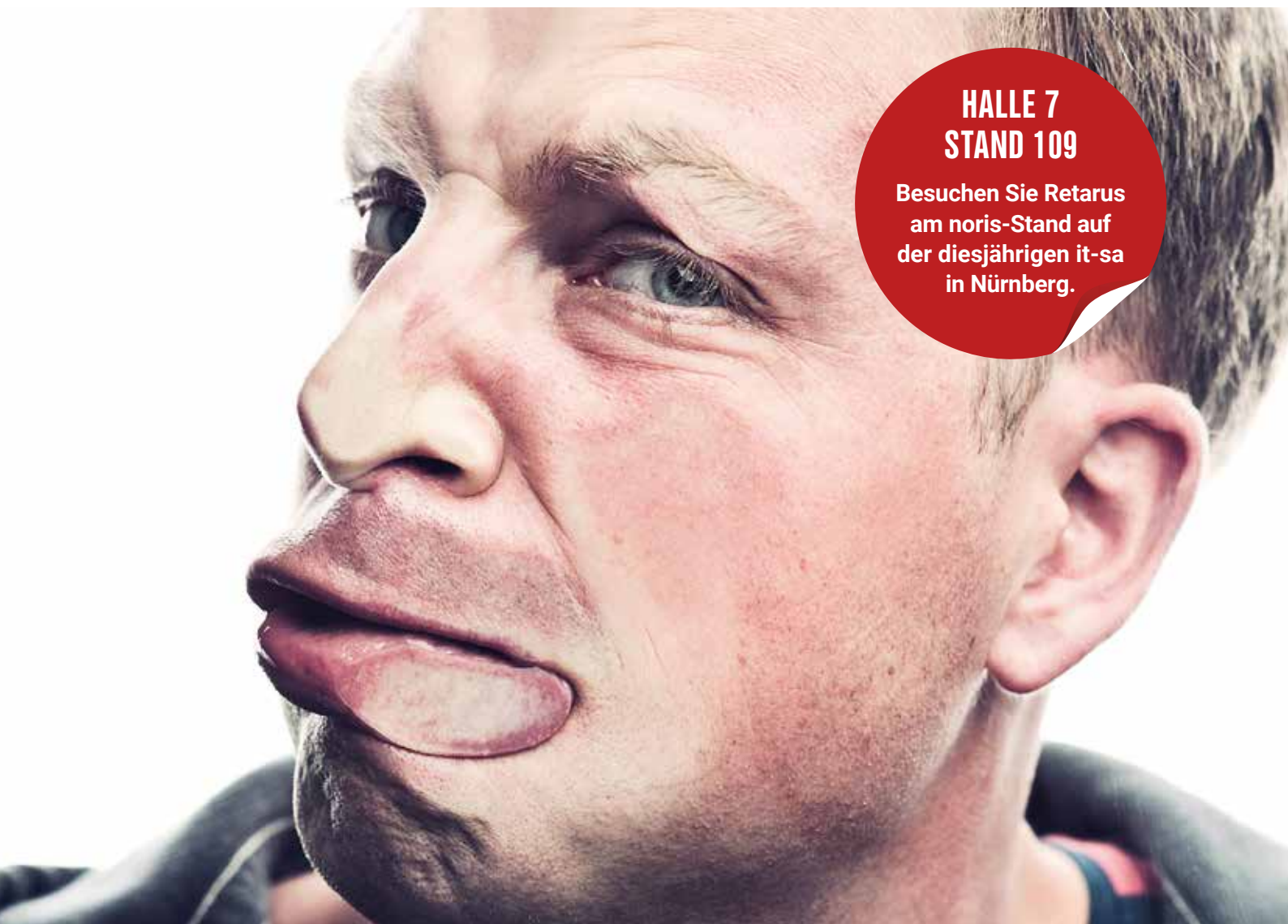
Dr. Christian Polster, Geschäftsführer, RADAR Cyber Security

11. Oktober 2023, 16:00 Uhr, Forum E, Halle 7A

„Der Einsatz von Smartphones und Tablets im sicherheitssensiblen Umfeld“

Christian Severin, Senior Account Manager, Materna Virtual Solution

Unsere Kunden vergessen gerne, dass wir für sie da sind. **Ihre Cyberangreifer nicht.**



**HALLE 7
STAND 109**

Besuchen Sie Retarus
am noris-Stand auf
der diesjährigen it-sa
in Nürnberg.

Lassen Sie Cyberangreifer einfach gegen eine unsichtbare Wand laufen!

Wehren Sie hochentwickelte und persistente Malware- und Phishing-Angriffe effektiv ab und verhindern Sie, dass Cyberkriminelle sensible Daten stehlen, Systeme lahmlegen, Konten plündern oder Lösegeld erpressen.

Mit der patentierten Email Security von Retarus sichern Sie Ihr Unternehmen, Ihre Anwender und Daten zuverlässig gegen alle bekannten Cybergefahren und deren Folgen ab. Als Cloud-Gateway nahtlos integrierbar in jedes E-Mail-System. Egal, ob Cloud, Hybrid oder On-Premises. retarus.de

Die größten Vorteile verhaltenspsychologischer Elemente in Security-Awareness-Trainings

Verhaltenspsychologie trifft Cybersecurity: Unser Autor beschreibt, warum das Verständnis menschlicher Verhaltensmuster für ein erfolgreiches Security-Awareness-Training unerlässlich ist und wie sich Mitarbeiterengagement und Lernerfolg optimieren lassen.

Von Dr. Christian Reinhardt, SoSafe GmbH

Verhaltenspsychologische Elemente haben wichtige Vorteile für die Cybersecurity-Awareness-Schulungen. So können Unternehmen durch das Verständnis menschlicher Verhaltensmuster im Bereich der Cybersicherheit die Motivation ihrer Mitarbeiterinnen und Mitarbeiter zur Teilnahme an Sicherheitsschulungen nachhaltig steigern. Ein wichtiges Element aller verhaltenspsychologischer Ansätze ist Gamification. Der Wechsel von traditionellen Modellen hin zu einer interaktiven Lernerfahrung steigert nicht nur den Lernerfolg, sondern auch die Motivation und den Spaßfaktor. In einer von der Trainingsplattform Talent LMS durchgeführten Umfrage gaben mehr als 80 Prozent der Teilnehmenden an, dass Gamification-Elemente das Lernen erleichtern und sie eine stärkere Verbindung zu den Inhalten herstellen.

Ein weiteres verhaltenspsychologisches Prinzip, das das Engagement der Mitarbeitenden steigert, ist das sogenannte Nudging. So wird laut Human Risk Review 2022 „durch Nudging [...] die Engagement-Rate kontinuierlich um 30 Prozent, in der Einführungsphase sogar um bis zu 90 Prozent, erhöht.“ Nudging in Form von regelmäßigen, automatisierten System-Mails steigert die Interaktion der Nutzenden und sorgt dafür, dass das Thema Informationssicherheit immer präsent ist. Nudges können kleine Anstupsler zur Motivation, zur Erinnerung oder ein Update zum Lernfortschritt sein, die dafür sorgen, dass die Benutzer beim Awareness-Training auf der Spur bleiben.

Kombiniert man Gamification und Nudging, sieht man deutlich, welchen Einfluss Verhaltenspsychologie auf den Erfolg von Security-Awareness-Programmen haben kann. Indem sie das Engagement steigern und eine interaktive Lernumgebung schaffen, verwandeln diese Methoden Security-Trainings von einer lästigen Aufgabe zu einer dynamischen Lernerfahrung, bei der der Mensch im Mittelpunkt steht.

Akzeptanz steigern und Lernerfolg fördern

Psychologisch fundierte Ansätze wie Nudging verbessern aber nicht nur das Engagement, sondern auch den Lernerfolg. In der Vergangenheit wurde Wissen häufig sehr linear und in „hoher Dosis“ vermittelt. Wir wissen jedoch alle nur zu gut, dass langatmige Workshops und eintönige Schulungen längst nicht mehr zeitgemäß sind und nicht die gewünschten Resultate liefern, nämlich Kenntnisse, die wirklich im Gedächtnis bleibt.

Das liegt daran, dass das angeeignete Wissen mit der Zeit von Natur aus exponentiell schwindet – eine der größten Herausforderungen im Bereich Learning und Development. Nach der Vergessenskurve von Dr. Ebbinghaus vergessen Lernende bereits in den ersten sieben Tagen 90 Prozent des Gelernten (<https://blog.neuronation.com/de/die-vergessenskurve-nach-dr-ebbinghaus/>). Das gilt besonders dann, wenn User ihre Lernroutine und -häufigkeit unterbrechen.

Es gibt jedoch Möglichkeiten, die Mitarbeitenden dazu zu motivieren, beim Lernen am Ball zu bleiben und sich Wissen so nachhaltiger einzuprägen. Beim „Spaced Learning“ wird Wissen kontinuierlich in kleinen Portionen über verschiedene Kanäle vermittelt und so immer wieder aktiv wiederholt. Kombiniert mit interaktiven und motivierenden Elementen, wie kurzen Quizzes, lässt sich so die Vergessenskurve abflachen.

Das „beiläufige“ Lernen (auch Incidental Learning) ist ein weiteres Element verhaltensbasierter Security-Trainings, das – ähnlich wie das Nudging – das Lernen in alltäglichen Situationen fördert. In einer Zeit, in der wir von Informationen überflutet werden und Zeit Mangelware ist, macht das Bereitstellen von Inhalten in kleinen

Einheiten und genau im richtigen Moment den entscheidenden Unterschied. Das perfekte Beispiel ist eine Lernseite, die direkt nach dem Klick auf eine Phishing-Simulationsmail angezeigt wird. Ein Security-Awareness-Training, das in leicht verdaulichen 5-Minuten-Einheiten vermittelt wird, lässt sich problemlos in den hektischen Arbeitsalltag integrieren und gewährleistet einen stetigen Lernfortschritt, ohne die Lernenden zu überfordern.

Angriffe erkennen und korrekt reagieren

Ein bedeutender Aspekt einer starken Sicherheitskultur ist, die Mitarbeitenden aktiv in die Verteidigung gegen Cyberbedrohungen einzubinden. Dazu ist es wichtig, ein Umfeld zu schaffen, das sicheres Verhalten fördert und Mitarbeitenden die richtigen Tools an die Hand gibt, die es ihnen erlauben, ihre Organisation selbstbewusst vor möglichen Angriffen zu schützen. Dabei hilft eine psychologisch fundierte Awareness-Plattform mit Features, die das Erkennen und Melden verdächtiger Online-Aktivitäten ermöglicht. Zum Beispiel weisen Mitarbeitende, die Zugriff auf den SoSafe Phishing-Meldebutton haben, eine 30 Prozent niedrigere Interaktionsrate mit Phishingmails auf als andere Mitarbeitende, denen dieses Feature nicht zur Verfügung steht.

Solche Tools erfüllen zwei Aufgaben: Sie befähigen Mitarbeitende, Bedrohungen zu erkennen und korrekt zu handeln, und zeigen ihnen außerdem auf, welchen Einfluss ihr Verhalten auf die gesamte Sicherheitskultur der Organisation hat. Das kontextbasierte Feedback bestärkt sie in ihrem Verantwortungsgefühl und sie sind eher gewillt, zu einem sicheren Umfeld beizutragen. Das Ergebnis: Mitarbeitende stehen nicht länger am Spielfeldrand, sondern werden aktiv in die Verteidigung ihrer Organisation gegen Cyberangriffe eingebunden.

Aussagekräftige verhaltensbasierte Daten

Wenn Organisationen das Verhalten von Angreifenden und Nutzenden verstehen, können sie Angriffe frühzeitig erkennen und abwehren. Dabei helfen aussagekräftige verhaltensbasierte Daten: Sie zeigen den Verantwortlichen auf, wie Mitarbeitende auf verschiedene Bedrohungen reagieren und welche Lernmethoden besonders effektiv sind.

Ein Blick auf die richtigen verhaltensbasierten Kennzahlen ermöglicht ihnen zudem, ihre Awareness-Maßnahmen entsprechend zu optimieren. Weist ein bestimmtes Team zum Beispiel eine geringere Phishing-Meldequote als andere Teams auf, kann den Mitarbeitenden durch zusätzliche gezielte E-Learning-Einhei-



Bei der Sensibilisierung für Cybersicherheit haben verhaltenspsychologische Elemente große Vorteile. (Bild: SoSafe)

ten vermittelt werden, wie sie verdächtige E-Mails erkennen und melden können. Zu guter Letzt veranschaulichen verhaltensbasierte Kennzahlen eindrucksvoll, welchen Einfluss Lernprogramme auf die gesamte Sicherheitskultur der Organisation haben.

Sie sind somit handfeste Argumente, um Entscheidungsträgern von der Führungsebene bis hin zu den Mitarbeitenden die Relevanz der Maßnahmen zu vermitteln.

Langfristige Verhaltensänderungen

Der Schutz des Unternehmens steht und fällt mit den sicheren Gewohnheiten der Mitarbeitenden; sei es, dass sie ihren Bildschirm sperren, wenn sie den Schreibtisch verlassen, ihre E-Mails auf verdächtige Aktivitäten scannen oder die IT-Abteilung zeitnah über Risiken und Zwischenfälle informieren.

Durch Security-Awareness-Trainings mit verhaltenspsychologischen Elementen können Unternehmen und Behörden die täglichen digitalen Gewohnheiten am Arbeitsplatz gezielt optimieren. Es sensibilisiert Mitarbeitende für das Thema der Informationssicherheit und motiviert sie, sichere Verhaltensweisen zu verinnerlichen – im Büro und im Privatleben. Weiter gestärkt wird ihre Motivation durch die richtigen Tools, ein unterstützendes Umfeld und ein Verantwortungsgefühl für die Sicherheit ihrer Organisation.

Sei es der gesteigerte Wissenserhalt durch „Spaced Learning“, der Einfluss von Motivation auf die Engagement-Rate oder die Phishing-Meldequote, die ansteigt, indem wir Mitarbeitende zu sicherem Verhalten befähigen: All diese Kennzahlen veranschaulichen, dass eine starke Sicherheitskultur einen ganzheitlichen Ansatz erfordert. Denn nur durch tief verwurzelte Verhaltensänderungen erzielen Organisationen eine nachhaltige Sicherheitskultur. ■

Messestand SoSafe
Halle 7, Stand 324

Schnell und einfach Berechtigungen managen

Warum Unternehmen No-Code IAM brauchen

Von der NIS-2-Compliance bis zur Abwehr von Cyberangriffen: Für Unternehmen ist Identity- und -Access-Management längst ein Muss. Leider stellt die komplexe Implementierung der Software oft eine große Hürde dar. Mit dem No-Code-Ansatz lassen sich Verwaltungsaufgaben schnell und einfach automatisieren.

Von Helmut Semmelmayr, tenfold Software

Für ihre Arbeit brauchen Benutzer Zugriff: Zugriff auf Fileserver, Business-Software, Fachanwendungen, Kollaborationstools, Clouddienste und vieles mehr. Das stellt Organisationen vor die Herausforderung, den reibungslosen Zugang zu benötigten Ressourcen zu gewährleisten, ohne Sicherheitslücken durch weitreichende, nicht notwendige oder veraltete Berechtigungen entstehen zu lassen.

Das Problem der sicheren Berechtigungsvergabe können nur automatisierte Systeme lösen. Erstens lässt sich der Aufwand bei der Verwaltung hunderter Konten in dutzenden Systemen nur so zeitspa-

rend bewältigen. Zweitens verhindert Automatisierung Fehler bei der Vergabe und dem Entzug von Rechten, zum Beispiel, dass die Konten ehemaliger Mitarbeiter nach deren Austritt bestehen bleiben und zum möglichen Einfallstor für Angreifer werden.

Das Identity- und -Access-Management (IAM) hilft Unternehmen, Zugriffsrechte schnell, sicher und zentral zu steuern. Doch bis die automatische Verwaltung einmal läuft, ist es ein steiniger Weg: Da IAM-Lösungen als Framework ausgeliefert werden, ist viel Programmierarbeit erforderlich, um ihre Bestandteile in die eigene IT

zu integrieren. Es müssen Prozesse definiert, Workflows entwickelt und Anbindungen geschrieben werden. Ein Mehraufwand, der überlastete IT-Abteilungen oft an ihr Limit bringt. Die Folge sind Verzögerungen sowie schlecht oder gar nicht implementierte Funktionen.

Schneller ans Ziel

Welche Möglichkeiten bleiben Unternehmen also? Monate oder Jahre in den Aufbau eines IAM-Systems zu investieren? Für die Entwicklung eigene Fachkräfte von wichtigen Projekten abzuziehen oder sich durch teure Consultants von externer Expertise abhängig zu machen?

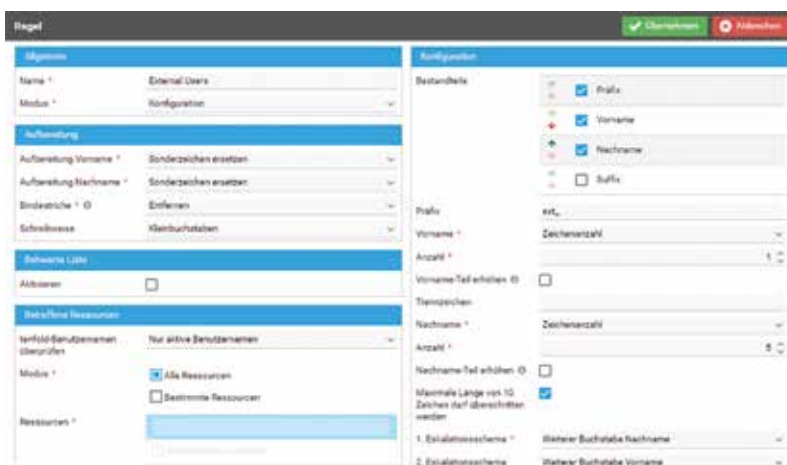
Es gibt einen einfacheren Weg: No-Code IAM von tenfold. Die Lösung zeichnet sich durch sofort nutzbare Workflows und Schnittstellen aus, welche über ein grafisches Interface mit wenigen Handgriffen konfiguriert werden. Kein Coding, keine Programmierung – so sind Unternehmen in kürzester Zeit startklar und profitieren unmittelbar vom vollen Umfang eines IAM-Systems: automatische Benutzerverwaltung, zentrales Reporting und die laufende Rezertifizierung von Rechten.

Fazit

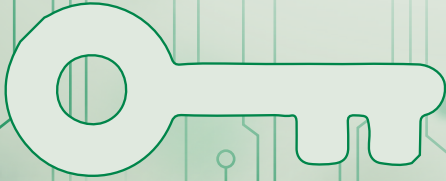
Wer Cyberangriffe verhindern, Sicherheitsstandards einhalten und Admins entlasten möchte, kann es sich nicht leisten, ewig auf eine einsatzbereite IAM-Lösung zu warten. No-Code IAM erlaubt es, die Verwaltung von Konten und Rechten mit minimalem Aufwand zu automatisieren. Das trägt nicht nur zum Schutz sensibler Daten und der Erfüllung gesetzlicher Vorgaben bei, sondern schafft auch Freiräume für IT-Fachkräfte.

Messestand tenfold Software:
Halle 7, Stand 328

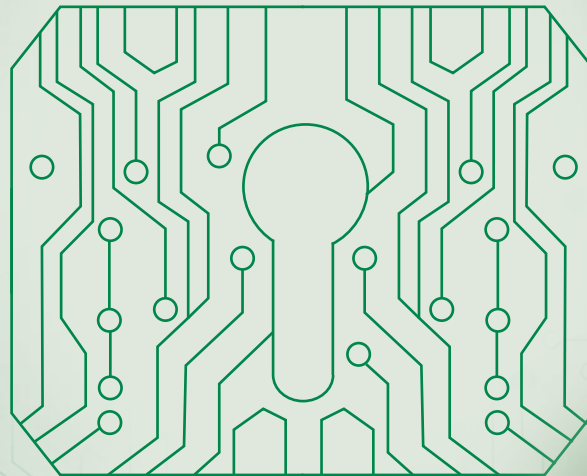
tenfold kann vollständig über seine No-Code-Oberfläche konfiguriert werden. (Bild: tenfold Software GmbH)



QSEC® der Schlüssel zum sicheren und nachhaltigen ISMS und Risikomanagement



Informationssicherheit



Datenschutz

Risikomanagement

*Besuchen Sie uns auf der it-sa
Halle 7 / Stand 309
Jetzt vorab Termin vereinbaren!*

Lesen Sie unseren
Artikel zum
Risikomanagement
in der Beilage

WMC GmbH
+49 40 650336-0
info@wmc-direkt.de
www.wmc-direkt.de



G DATA
CyberDefense

Managed EDR „Made in Germany“

Ihr 24/7-Expertenschutz aus Deutschland:
Wir erkennen und stoppen Cyberangriffe für Sie.



Stand: 7-210

Besuchen Sie unsere
hybriden Workshops.
Jetzt anmelden und
Gratis-Ticket sichern!



TRUST IN
GERMAN
SICHERHEIT



NIS-2: Das nötige Update der KRITIS-Sicherheit

Die weltweit steigende Anzahl von Cyber-Angriffen, besonders auf kritische Infrastrukturen, hat zur Einführung der NIS-2-Richtlinie durch die EU geführt. Sie soll ein einheitliches IT-Sicherheitsniveau für KRITIS-Betreiber in den Mitgliedsstaaten etablieren und erweitert unter anderem den Geltungsbereich. Wir geben einen Überblick, was auf Unternehmen zukommt.

Von Thomas Janz und Alexander Häufßler, TÜV SÜD Management Service GmbH

Die Zahl der Cyber-Attacken nimmt weltweit kontinuierlich zu. Ein besonderer Fokus liegt dabei auf kritischen Infrastrukturen (KRITIS). Um ein gemeinsames IT-Sicherheitsniveau für KRITIS unter den Mitgliedstaaten zu etablieren, hat die Europäische Union (EU) im Jahr 2016 die NIS-Richtlinie verabschiedet, auf deren Basis in Deutschland das IT-Sicherheitsgesetz 2.0 gebaut wurde. Mit der NIS-2-Richtlinie werden KRITIS-Betreiber jetzt auf den aktuellen Stand gebracht. Sie wurde im Dezember 2022 vom Europäischen Parlament und vom Europarat erlassen und muss in den EU-Mitgliedstaaten bis 17. Oktober 2024 umgesetzt werden. Ein Referenten-Entwurf zur Umsetzung der NIS-2-Richtlinie in nationales Recht macht deutlich, welche zusätzlichen Anforderungen auf KRITIS-Betreiber zukommen.

Auch KMU können nun als KRITIS-Betreiber zählen

Im Vergleich zur Vorgänger-richtlinie wurde der Geltungsradius von NIS-2 erweitert. Dabei sind zwei Eigenschaften entscheidend für die Einstufung einer Organisation oder eines Unternehmens: die Sektor-Zugehörigkeit und die Unternehmensgröße. Definiert sind 18 Sektoren, die zweigeteilt sind in elf Sektoren hoher Kritikalität und sieben sonstige kritische Sektoren (siehe Tabelle).

In diesen Sektoren werden von NIS-2 auch kleine und mittlere Unternehmen (KMU) adressiert. Mittlere Unternehmen beschäftigen 50 bis 250 Mitarbeiter und haben entweder einen Jahresumsatz von 10 bis 50 Millionen Euro oder eine Bilanzsumme von höchstens 43 Millionen Euro. Kleine Unternehmen beschäftigen weniger als 50 Personen und haben einen Jahresumsatz beziehungsweise eine Jahresbilanz von höchstens 10 Millionen Euro.

Auf Grundlage der Sektor-Zugehörigkeit und der Unternehmensgröße wird ermittelt, ob eine Organisation oder ein Unternehmen zu den wesentlichen (englisch: „essential“) oder zu den wichtigen (englisch: „important“) Betreibern zählt.

Mit dem Wissen um die Sektor-Kategorie und Kenngröße lässt sich einfach ermitteln, wie eine Organisation einzuordnen ist: Wer zum Sektor hoher Kritikalität gehört und in die Schwellenwerte mittlerer Unternehmen fällt oder diese überschreitet, gilt als wesentlicher KRITIS-Betreiber. Als wichtig gelten alle Betreiber aus Sektoren hoher Kritikalität, die kleiner als mittlere Unternehmen sind – und zusätzlich alle Einrichtungen, die zu den sonstigen kritischen Sektoren gehören. Es gibt jedoch Ausnahmen: Die NIS2-Richtlinie gilt auch für Einrichtungen, die zum Beispiel wegen ihrer Monopol-Stellung oder einer speziellen Tätigkeit den wesentlichen Sektoren zugeordnet werden können. In diesem Fall spielt die Unternehmensgröße keine Rolle.

Sektoren mit hoher Kritikalität	
Digitale Infrastruktur	Verwaltung von IKT-Diensten (Business-to-Business)
Energie	Finanzmarkt-Infrastrukturen
Trinkwasser	Abwasser
Verkehr	Bankwesen
Öffentliche Verwaltung	Gesundheitswesen
Weltraum	
Sonstige kritische Sektoren	
Anbieter digitaler Dienste	Post- und Kurierdienste
Produktion, Herstellung und Handel mit chemischen Stoffen	Produktion, Verarbeitung und Vertrieb von Lebensmitteln
Verarbeitendes Gewerbe/Herstellung von Waren	Forschung
Abfallbewirtschaftung	

Neue Technologie und EU-weite Zusammenarbeit

Um die EU-Mitgliedstaaten widerstandsfähiger zu machen, listet NIS-2 zehn Maßnahmen, die aktuelle Standards in der Informationstechnologie abbilden. Dazu gehört Technologie für Disaster-Recovery und Business-Continuity. Damit haben Unternehmen die Möglichkeit, Daten aus Backups wiederherzustellen und so den Arbeitsbetrieb nach einem Zwischenfall zügig wieder aufzunehmen. Weitere Maßnahmen betreffen die Implementierung von Systemen zur Prävention und Erkennung von Zwischenfällen, regelmäßige Schulungen von Mitarbeitern zur Schärfung des Sicherheitsbewusstseins, oder die Einführung einer Multi-Faktor-Authentifizierung bei System-Anmeldungen. Die NIS-2-Richtlinie schreibt zudem Konzepte und Verfahren zur Bewertung der Wirksamkeit des Risiko-Managements in der IT-Sicherheit vor. Das bedeutet: KRITIS-Betreiber sollen regelmäßig evaluieren, ob die von ihnen gewählten Maßnahmen noch zeitgemäß sind und angemessen funktionieren.

Meldepflichtige Sicherheitsvorfälle

KRITIS haben einen direkten Einfluss auf das öffentliche Leben. Wenn das Stromnetz ausfällt oder das Leitungswasser verunreinigt wurde, müssen die Behörden und die Bevölkerung so schnell wie möglich informiert werden. Sicherheitsvorfälle sind meldepflichtig, wenn Betriebsstörungen, finanzielle Verluste oder schwerwiegende Schäden für juristische oder natürliche Personen drohen. Wenn Einrichtungen von solchen Vorfällen betroffen sind, müssen sie das Bundesamt für Sicherheit in der Informationstechnik (BSI) innerhalb von 24 Stunden informieren und innerhalb von 72 Stunden eine erste Bewertung mit einer Einschätzung des Schwe-

regrads abgeben. Zudem muss dem BSI spätestens einen Monat nach dem Vorfall ein Abschlussbericht vorgelegt werden.

Die Sicherheit von Unternehmen hängt auch von der Sicherheit ihrer Zulieferer und ihrer Lieferketten ab. Daher verpflichtet NIS-2 die wesentlichen und wichtigen Einrichtungen dazu, ihre Lieferketten zu prüfen. Allerdings sind die Ausführungen zu diesem Punkt grob. Das bedeutet, dass die Einrichtungen die Angemessenheit der getroffenen Maßnahmen selbst bewerten können und müssen. Als Anhaltspunkte nennt die Richtlinie, dass auch die Beziehungen zwischen den Einrichtungen betrachtet werden sollen und die Gesamtqualität in Bezug auf die IT-Sicherheit ebenso zu bemessen ist wie ein möglicher Entwicklungsprozess.

Umsetzung in nationale Gesetzgebung

Inzwischen liegt ein Referenten-Entwurf zur Umsetzung der NIS-2-Richtlinie in nationales Recht vor. Im Rahmen des NIS-2-Umsetzungs- und Cyber-Sicherheitsstärkungsgesetz (NIS2UmsuCG) sollen die Vorgaben der Richtlinie in die deutsche Gesetzes- und Verordnungslandschaft eingebunden werden. Obwohl es sich noch um einen Entwurf handelt, ist abzu-sehen, dass sich durch das Gesetz die Anforderungen an Betreiber und Einrichtungen ändern werden. Dazu wird das BSI-Gesetz durch das NIS2UmsuCG neu strukturiert und um NIS-2-Aspekte ergänzt. Die bisherigen Anforderungen werden in diesem Zusammenhang teilweise präziser formuliert und geschärft.

Einen spezifischen Ausblick gibt der Entwurf auf das Risiko-management für besonders wichtige Einrichtungen: Sie müssen „geeignete, verhältnismäßige und wirksame technische und organisatorische Maßnahmen“ ergreifen,

um „Störungen ... zu vermeiden und Auswirkungen ... zu verhindern oder möglichst gering zu halten.“ (§ 30 (1)). Diese Maßnahmen sollen dem Stand der Technik entsprechen und die „einschlägigen europäischen und internationalen Normen“ berücksichtigen (§ 30 (2)).

Die Umsetzung der Maßnahmen nachzuweisen, dazu sollen nach dem Entwurf zumindest besonders wichtige Einrichtungen verpflichtet werden. Dies soll gegenüber dem BSI alle zwei Jahre in Form von Sicherheitsaudits, Prüfungen oder Zertifizierungen geschehen.

Mit Zertifizierungen sind KRITIS-Betreiber auf der sicheren Seite

Der Referenten-Entwurf zur Umsetzung der NIS-2-Richtlinie macht deutlich, dass sich KRITIS-Betreiber frühzeitig mit NIS-2 auseinandersetzen müssen. Ihnen drohen bei Nachlässigkeiten in der Umsetzung empfindliche Strafen. Zudem scheint es wahrscheinlich, dass die Bundesregierung mit der Überführung der Richtlinie in nationales Recht eine dritte Fassung des IT-Sicherheitsgesetzes verabschieden wird und dieses mögliche IT-Sicherheitsgesetz 3.0 auch eine Verpflichtung zu Sicherheit-Audits, Prüfungen oder Zertifizierungen enthalten wird. Daher sollten KRITIS-Betreiber diese derzeit noch freiwilligen Audits als Chance begreifen, um ihre eigenen IT-Defensivmaßnahmen von unabhängigen Experten prüfen und zertifizieren zu lassen. Dann können sie diese einfacher an aktuelle Sicherheitsstandards und kommende gesetzliche Anforderungen anpassen, sogar bequem vor dem Ablauf der Frist am 17. Oktober 2024, wodurch ein nützlicher Puffer entstünde. ■

Plötzlich offline kann sich heute keiner leisten



Zusammen bringen
wir Ihre IT-Sicherheit
auf den Stand der Technik.

Datensouveränität bei voller Konnektivität:

Wire integriert Federation

Wer sicher kommunizieren will, muss oft Kompromisse zwischen Nutzbarkeit und Sicherheit eingehen. Mit der Integration von Federation in das eigene Produkt schafft Wire diese Kompromisse ab.

Von Hauke Gierow, Wire

Im vergangenen Jahrzehnt hat sich der Einsatz von Cloud-Computing auch im Enterprise- und Regierungsumfeld in vielen Bereichen durchgesetzt – aus gutem Grund. Einfache Bereitstellung, weniger Wartungsaufwand im eigenen IT-Team und vereinfachte Haftungsregelungen. Wer aber volle Datensouveränität will, setzt in kritischen Bereichen weiterhin auf On-Premises-Installationen, zum Beispiel im Kommunikationsbereich.

Aus diesem Grund bietet Wire seit vielen Jahren neben dem Cloud-Dienst auch skalierbare On-Premises-Lösungen an. Diese können Unternehmen auf Wunsch selbst betreiben oder von Wire warten lassen (Private-Cloud). So kann jeder Kunde das für seine Organisation richtige Sicherheitsniveau bestimmen und umsetzen.

Dabei kann das benötigte Sicherheitsniveau innerhalb einer Organisation durchaus verschieden sein – je nach Abteilung oder Funktion. Möglicherweise unterliegen bestimmte Bereiche speziellen Compliance-Anforderungen oder wollen sich besonders gegen Angriffe absichern, ohne die entsprechenden Sicherheitsstandards überall anwenden zu wollen oder können.

Eine weitere Herausforderung: Wer seinen eigenen Kommunikationsserver für Instant-Messaging, Audio- und Videokommunikation

betreibt, kann erst einmal nur mit Menschen innerhalb der eigenen Organisation kommunizieren – oder muss externe Nutzer in der eigenen Infrastruktur anlegen. Beides ist für viele keine gangbare Lösung.

Federation verbindet Backends

Aus diesem Grund bietet Wire mit seinem sicheren Messenger seinen On-Premises-Kunden die Möglichkeit an, verschiedene Wire-Backends mittels Federation miteinander zu verschalten, um gestufte Sicherheitsanforderungen innerhalb eines Unternehmens oder zwischen Behörden umsetzen zu können und um Kommunikation auch außerhalb des eigenen Rechenzentrums zu ermöglichen. Die Verschaltung kann dabei sowohl zwischen zwei On-Premises-Backends als auch zum Cloud-Dienst von Wire erfolgen.

„Mit Federation ermöglichen wir unseren Kunden sichere Kommunikation mit maximaler Datensouveränität bei gleichzeitiger Anbindung an unsere Cloud oder zu anderen wichtigen Partnern mit eigenem On-Premises-Backend“, sagt Sascha Haase, Vice President Product Management bei Wire. „Besonders interessant ist dabei unsere Umsetzung, denn wir ermöglichen es, verschiedene Abteilungen oder Nutzergruppen mit hoher Granularität und nach klaren Regeln zu verschalten. So können wir unser

Sicherheitsversprechen einhalten, auch wenn die Kommunikationspartner unterschiedliche Sicherheitsniveaus haben.“

Non-Fully Connected Graphs

Die granulare Verschaltung wird im Englischen mit dem Fachbegriff „Non-Fully Connected Graphs“ bezeichnet. Gemeint ist, dass nicht alle Nutzerinnen und Nutzer der beiden Backends einfach miteinander kommunizieren können, sondern bei Bedarf Regeln für die Verschaltung umgesetzt werden.

Ein Beispiel: Stellen Sie sich vor, Sie werden von einem Bekannten in einen Chat eingeladen, kennen aber die anderen Teilnehmer nicht und sind sich nicht sicher, über welche Themen sie sprechen können. Auf der Ebene von hochsicherer Kommunikation ist das nicht akzeptabel. Wir ermöglichen die partielle Verschaltung, das heißt, Sie können nur dann in eine solche Gruppe eingeladen werden, wenn diese bestimmten Standards entspricht. Ist das nicht der Fall, kann ihr Bekannter sie auch nicht hinzufügen.

Die möglichen Anwendungsfälle sind vielfältig. In einem großen Unternehmen könnten zum Beispiel die Vorstandsetage und der Aufsichtsrat in einer eigenen Wire-Instanz kommunizieren, der Rest des Unternehmens nutzt den

Cloud-Dienst. Mittels der granularen Verschaltung könnte beispielsweise festgelegt werden, dass der Aufsichtsrat keinen direkten Kontakt zu den Mitarbeiterinnen und Mitarbeitern auf der Arbeitsebene aufnehmen kann, aber zur Überprüfung wichtiger Kennzahlen mit der Finanzabteilung sprechen kann.

Warum es sinnvoll ist, klare Regeln für die Kommunikation einzuziehen, zeigt das Beispiel E-Mail. Grundsätzlich können alle E-Mail-Server, die die Standards einhalten, ohne Beschränkung miteinander kommunizieren. Für Nutzerinnen und Nutzer ist aber in der Regel nicht erkennbar, ob eine E-Mail von einem vertrauten oder nicht vertrauten Server kommt. Mit der partiellen Verschaltung im Messaging-Bereich kann dieses Risiko ausgeblendet werden.

Auch im Behördenumfeld ist Federation von hoher Bedeutung, denn so wird Kommunikation zwischen verschiedenen Backends ohne technische Hürden möglich – es können aber, klare Regeln für die Kommunikation umgesetzt werden.

So könnten Behörden und Ministerien aus dem Sicherheitsumfeld mit einem höheren Sicherheitslevel konfiguriert werden als andere Ministerien. Und eine dritte Sicherheitsebene würde dann geschaffen, um die Kommunikation von Ministerien mit externen Unternehmen wie IT-Dienstleistern oder PR-Agenturen zu ermöglichen. So können alle relevanten Akteure untereinander im Austausch bleiben, ohne Sicherheitsrisiken einzugehen.

Visuelle Indikatoren zeigen das Sicherheitsniveau an

Damit Nutzerinnen und Nutzer auch in verschalteten Kommunikationsumgebungen stets den Überblick behalten, auf welchem Sicherheitsniveau sie sich befinden,

werden oberhalb des Textfeldes im Messenger entsprechende Statusbalken angezeigt. Dort kann etwa abgelesen werden, ob der aktuelle Chat Vorgaben wie etwa die für Verschlusssachen (VS NfD) erfüllt, oder nicht. Das trägt dazu bei, das versehentliche Versenden vertraulicher Dokumente an unberechtigte Personen zu verhindern.

„Mit der Umsetzung von Federation stellen wir dem Markt ein oft nachgefragtes Feature zur Verfügung“, sagt Juan Perea Rodriguez, General Manager und Chief Commercial Officer von Wire. „Nachdem in der Corona-Zeit viele Prozesse in kurzer Zeit und ohne klares Sicherheitskonzept digitalisiert wurden, sehen wir jetzt, dass die Themen Digitale Souveränität und Cybersecurity auch in der Führungsebene einen hohen Stellenwert einnimmt. Gründe dafür sind die unruhige geopolitische Lage, aber auch steigende regulatorische Anforderungen.“

Tatsächlich sollten sich Unternehmen in regulierten Bereichen verstärkt mit dem eigenen Sicherheitskonzept auseinandersetzen. Denn die zweite Auflage der EU-Richtlinie über Netzwerk- und Informationssicherheit (NIS-2) schreibt Unternehmen in Bereichen wie Strom- und Wasserversorgung, im Gesundheitssektor oder der Abfallwirtschaft vor, dass gesicherte Kommunikationsdienste genutzt werden müssen. Zudem sollten Unternehmen in diesen und weiteren Bereichen geeignete Systeme zur Notfallkommunikation bereithalten, um auch in Katastrophenfällen kommunikationsfähig zu bleiben.

Über Wire

Wire ist ein deutscher Hersteller von Messaging-Lösungen mit Hauptsitz in Berlin. Die Forschung und Entwicklung des Unternehmens findet fast ausschließlich in Deutschland statt und unterliegt deutschen Datenschutzgesetzen.

Alle Kommunikationslösungen von Wire arbeiten mit ständig aktivierter Ende-zu-Ende-Verschlüsselung nach dem Zero-Knowledge Prinzip. Das Unternehmen kann daher unter keinen Umständen auf Kommunikationsinhalte von Kunden zugreifen und minimiert zugleich die Sammlung von Metadaten auf das absolut notwendige Minimum. Bei selbst-gemanagten On-Premises-Instanzen hat Wire nicht einmal auf diese Metadaten Zugriff.

Wire ist aktiver Teil der Open-Source-Community und stellt den Quellcode aller Apps und der Wire-Backends auf Github unter der GPL v3 zur Verfügung. So können die Sicherheitsversprechen des Unternehmens unabhängig überprüft werden. ■

<kes>

+

<kes> SPECIAL

Die perfekte Kombination für CISO & Co



- ✓ Verlagsbeilage mit wechselnden Mitherausgebern
- ✓ auf ein Thema fokussierte Beiträge der Mitherausgeber
- ✓ Printausgabe liegt <kes> bei
- ✓ digitales eMagazine kostenfrei verfügbar

weitere Specials hier kostenfrei downloaden:
kes.info/archiv/specials/



- ✓ führende Fachzeitschrift in der IT-Sicherheit
- ✓ hohes technisches Niveau und redaktionell unabhängig
- ✓ offizielles Organ des Bundesamtes für Sicherheit in der Informationstechnik (BSI)
- ✓ nur im Abonnement erhältlich unter: datakontext.com/kes

<kes> genauer kennenlernen?

Einfach kostenfreies Probeheft anfordern unter:
kes.info/service/probeheft/

Leseproben <kes> unter: kes.info/archiv/leseproben/

In AI we Trust – secure it anyway we must

Generative künstliche Intelligenz ist eine wichtige Technologie für die Cybersicherheit, da sie beispielsweise die Automatisierung von Aufgaben und die Erkennung von Bedrohungen verbessert. Sie kann jedoch auch von Cyberkriminellen genutzt werden, um neue und schnellere Angriffsmethoden zu entwickeln. Ist KI die Antwort auf alle unsere Fragen?

Von Bastian Hallbauer, Kafka Kommunikation GmbH

Generative künstliche Intelligenz (KI) und die KI-getriebenen Projekte ermöglichen, was der Security-Community von der Sicherheitsindustrie schon seit Langem angepriesen wurde: Security-Automatisierung. Nach den Marktanalysen von Vantage Market & Research wird die Sicherheitsindustrie bis 2030 mit KI mehr als 22 Milliarden US-Dollar umsetzen. Fachkräftemangel, Skills Gap, Alarmfatigue, Technology Sprawl – alle diese Herausforderungen werden dann ein für alle Mal gelöst. Doch die gleichen Chancen stehen auch den Cyberkriminellen zur Verfügung. Die Möglichkeiten, Prozesse zu optimieren, die Geschwindigkeit und die Performance zu erhöhen, muten für beide, Angreifer wie Verteidiger schier unbegrenzt an. Kurz ausgedrückt, KI erscheint wie die „42“, die Antwort auf alle Fragen. Doch genau hier liegt das Problem, die über KI generierten „Antworten“ müssen interpretiert, oftmals noch geschliffen und auf jeden Fall bis auf Weiteres regelmäßig nach bestimmten Qualitätsmerkmalen überprüft werden. Ist KI daher wirklich schon die „42“ für die Security-Community oder ist sie eine weitere Technologie, die genauso abgesichert werden muss wie alle bisherigen? Diese Fragen und viele andere werden am Mittwoch, dem 11. Oktober auf der it-sa im International Forum B von 15:30 bis 16:15 Uhr, diskutiert.

Der aktuelle Stand der KI in der Cybersicherheit

Geschäftsführender Gesellschafter von Pinnow & Partner, Carsten Pinnow, stellt zunächst fest, dass KI in der Cybersicherheit, sowohl für Angreifer als auch für Verteidiger, immer wichtiger wird. „Durch sie lassen sich zum Beispiel bei Massendatenanalysen, Erstellung von Prognosen und bei Vorbereitungen und Durchführung von Angriffen Geschwindigkeits- und Effizienzgewinne realisieren. Darauf müssen die Verteidiger sich zwingend einstellen.“

Dr. Martin J. Krämer, Security Awareness Advocate bei KnowBe4 meint, dass KI aktuell vor allem erfolgreich

zur Erkennung und Analyse von Netzwerkdatenverkehr, Spam und Phishing-E-Mails sowie Schadsoftware wie zum Beispiel Malware eingesetzt wird. „Neuartige und verbesserte Verfahren können vor allem auch für Penetration-Testing eingesetzt werden – Schwachstellen in Hardware und Software sowie beim Co-Design von Hardware und Software können schneller erkannt werden, wie zum Beispiel für den KRITIS-Bereich.“

Nathan Howe, VP Emerging Technologies bei Zscaler, sieht hingegen, dass viele Sicherheitsansätze die künstliche Intelligenz bereits sehr gut integriert haben. Er sagt: „Bisher diente der Einsatz allerdings vor allem als Mechanismus, um sich gegen den Mitbewerber abzugrenzen nach dem Motto: Mein Produkt basiert bereits auf KI und ist dadurch besser aufgestellt als Lösungen, die noch keine künstliche Intelligenz nutzen. Generative KI spielt dabei eine untergeordnete Rolle. Der nächste evolutionäre Schritt wird durch die vorhandenen Data-Lakes gesteuert werden. Unternehmen werden darauf schauen, wie sie diese Datensätze einsetzen können, um Sicherheitsansätze generell zu verbessern.“

Rik Ferguson, Vice President Security Intelligence bei Forescout Technologies, sieht den Hype um KI in den jüngsten Fortschritten bei LLMs. Er hält dagegen, indem er sagt: „Diese Entwicklungen hätten vielleicht den Eindruck erweckt, dass KI etwas Neues im Cyberbereich ist, aber das ist nicht der Fall. KI ist seit fast zwanzig Jahren ein Aspekt der Cybersicherheit, und es gibt keine Anzeichen dafür, dass sich das ändert. Die Fortschritte in diesem Bereich bedeuten lediglich, dass sie zu verschiedenen Zeiten auf unterschiedliche Weise zum Einsatz kommt.“

Einfluss der KI auf die Cybersicherheit von Unternehmen

„Allgemein führt die Effizienzsteigerung durch Automatisierung und Massendatenverarbeitung zur Verbesserung von Threat Intelligence, insbesondere der

Open Source Intelligence“, meint Dr. Krämer. Ein Beispiel dafür seien Datenlecks, die schneller erkannt, identifiziert und eingedämmt werden können, wenn Überwachungssysteme mittels KI effizienter gestaltet werden.

Carsten Pinnow empfiehlt den Blick auf beide Seiten der Medaille: „Software-Werkzeuge oder auch Tools, wie sie im Fachjargon genannt werden, haben immer Dual-Use-Eigenschaften. Sie können somit sowohl von Angreifern wie auch von Verteidigern eingesetzt werden. Unternehmen müssen auf KI-gestützte Bedrohungen selbstverständlich reagieren. Notwendige Voraussetzungen sind ausreichende Zeit- und Finanzbudgets und ausreichendes Know-how.“

Nathan Howe erinnert daran, dass eine KI nur so gut ist wie seine Daten. Entscheidend ist für ihn, dass die vorhandenen Daten bereits heute genutzt werden, um aus den Analyseergebnissen Handlungen abzuleiten. Er stellt die Frage, wie IT-Sicherheit effizienter gestaltet oder der Datenverkehr besser fließen kann. „Die eigentliche Revolution liegt darin, wie Mechanismen und Prozesse effektiver und effizienter gestaltet werden können.“ Rik Ferguson schließt hier an, wenn er sagt, dass „die Fortschritte bei den LLMs sich dadurch auszeichnen, dass sie das Komplexe einfach machen.“ Er sieht erhebliche Verbesserungen bei der Entschlüsselung komplexer bösartiger Aktivitäten, bei der Auswertung großer Datenmengen und bei der Unterstützung von Security-Analysten bei deren Suche nach Bedrohungen.

Cybersicherheit mit KI verbessern

Dr. Krämer schätzt, dass die Komplexität der KI wohlbekannte Herausforderungen an Entwickler, Anwender und Aufsichtsbehörden stellen wird. Für ihn müsste bereits

während der Entwicklung mehr auf die Möglichkeiten der KI geachtet werden. Er mahnt den verantwortungsbewussten Umgang mit Trainingsdaten (Vermeidung von Bias und Data Poisoning) sowie die Gefahren des Reverse-Model-Engineering an.

Carsten Pinnow sieht hier die gleichen Regeln wie bei der Cybersicherheit ohnehin: „Es ist im Wesentlichen eine Frage der Softwaresicherheit, ebenso wie bei herkömmlicher IT- und OT-Software. Ausbildung von Mitarbeitern und die stringente Definition und Implementierung von Prozessen ist essenziell, um die Cybersicherheit von Software-Werkzeugen, wie KI eines ist, zu verbessern und damit das Niveau der Cybersicherheit allgemein zu heben.“

Drei Ebenen zur Verbesserung sind für Nathan Howe entscheidend „Daten, Prozesse und der Mensch“. Der schwierigste Punkt liegt seiner Meinung nach darin, Grenzen zu ziehen für den ethischen Einsatz von KI. Eine zweite Ebene würde sich auf den Umgang mit Datenquellen zum Training von KI-Modellen beziehen. Rik Ferguson warnt vor KI-„Halluzinationen“, die es zu reduzieren gelte, um Verzerrungen in den Trainingsdaten und den daraus resultierenden Algorithmen zu beseitigen. Seine Forderung besteht darin, dass die Algorithmen transparenter werden müssen, damit der Mensch nicht nur verstehen kann, welche Entscheidungen eine KI trifft, sondern auch warum.

Fazit

Dr. Krämer gibt zu bedenken, dass KI kein Hype ist, der in wenigen Jahren abebbt. Er erkennt schon jetzt eine größere Wahrnehmung nicht zuletzt dadurch, dass es bereits auf Managementebene diskutiert wird, also auf Leitungsebene angekommen ist. Seine Schlussfolgerung daraus ist, dass „Cybersicherheit weiterhin un-

bedingt notwendig sein wird, gerade in einer zunehmend destabilisierenden geopolitischen Landschaft, in der auch die Gesellschaft vor immer neuen Herausforderungen steht.“ Nathan Howe sieht es ebenso, auch er schätzt, dass sich KI als Teil der Sicherheitsdiskussionen etablieren wird.

Carsten Pinnow denkt dagegen an ein Abflachen der Aufmerksamkeitskurve: „Möglicherweise wird sich der Hype um das Thema bis dahin ein wenig gelegt haben, aber die Bedrohungslage durch KI-gestützte Angriffe wird sicherlich nicht einfach verschwinden.“ Rik Ferguson sieht darin sogar eine Gefahr, wenn er sagt, dass: „Wenn wir aufhören, über KI zu sprechen, sei es im Bereich der Sicherheit oder in anderen Bereichen, dann riskieren wir, dass die aktuellen Probleme einfach Teil des Status quo werden und wir uns in eine Welt begeben, in der wir ‘der Maschine vertrauen‘ und dabei ignorieren, dass wir sie anfangs mit all unseren eigenen Vorurteilen und Annahmen gefüttert haben.“ ■

Messestand KnowBe4
Halle 6, Stand 114

Messestand Zscaler
Halle 7A, Stand 304

Messestand Forescout
Halle 7, Stand 343a

11. Oktober, 15:30 Uhr,
International Forum B
Diskussionsrunde it-sa insights
In AI we Trust – secure it anyway
we must
Moderation: Norbert Luckhardt,
Chefredakteur <kes>

News und Produkte

it-sa 2023: Highlights im Rahmenprogramm

Vom 10. bis 12. Oktober bietet Europas größte Fachmesse für IT-Sicherheit den Verantwortlichen neben dem umfangreichen Angebot der bereits über 700 angemeldeten Aussteller ein vielfältiges Rahmenprogramm: In fünf offenen Foren informieren IT-Sicherheitsanbieter über aktuelle Angriffsvektoren und Abwehrmaßnahmen sowie Produkte und Lösungen.

Zu den Highlights des Forenprogramms zählen die it-sa insights. Dabei handelt es sich um produktneutrale Beiträge und Diskussionsrunden mit aktuellen Informationen beispielsweise zur IT-Sicherheitslage, der europäischen KI-Verordnung und dem Data Act, dem IT-Sicherheitsgesetz oder den Spuren von Hackern im Unternehmensnetzwerk. Mehrere it-sa insights widmen sich zudem dem drängenden Thema Fachkräftemangel: Panels unter dem Motto „Women in Cybersecurity“ mit Vertreterinnen aus IT-Sicherheitsunternehmen, Behörden und Forschung diskutieren, welche Ausbildungsformate und Strategien es für mehr Frauen in der IT-Sicherheit braucht, wie moderne Unternehmen Diversity als Teil der Unternehmensstrategie verankern und wie Frauen der Einstieg in eine IT-Sicherheitskarriere gelingt.

Ein besonderes Highlight der diesjährigen Messe ist die Special Keynote von Mark T. Hofmann. Der Kriminal- und Geheimdienstanalyst gibt Einblicke in das Cyber-Profiling und spricht über die Zukunft des Social-Engineering und darüber, wie

Unternehmen eine menschliche Firewall aufbauen können. Die Special-Keynote findet am dritten Messetag im Internationalen Forum statt.

Alle Informationen zum Rahmenprogramm gibt es unter www.itsa365.de/de-de/it-sa-expo-congress/rahmenprogramm.
www.itsa365.de

Fünf Startups im Finale des ATHENE Startup Awards UP23@it-sa

Im Rennen um den ATHENE Startup Award UP23@it-sa sind fünf Unternehmen: Enclave, Quantum Optics Jena, KeeQuant, Mondoo und ZenAdmin wurden von der Fachjury für das finale Pitch-Event nominiert. Der Pitch um den Preis als bestes Cybersecurity-Startup findet am 11. Oktober auf der it-sa in Nürnberg statt. Diese Startups sind im Finale:

_____ Enclave: Confidential-Computing schützt Daten auch während der Verarbeitung in jeder Cloud-Umgebung. Durch hardwaregestützte Kryptografie werden containerisierte Anwendungen von der Ausführung auf derselben physischen Plattform isoliert. Die Enclavation-Technologie von Enclave sorgt so für ein Höchstmaß an Anwendungssicherheit und Datenschutz.

_____ Quantum Optics Jena: Quantencomputer werden einige aktuelle, mathematisch basierte Verschlüsselungstechniken infrage stellen. Quantum Optics Jena stellt dieser Herausforderung Quantentechnologie entgegen: Das Unternehmen entwickelt Systeme zum

Quantenschlüsselaustausch (Quantum Key Distribution, QKD), die auf verschränkten Photonen basieren.

_____ KeeQuant: Produkte von KeeQuant ermöglichen es Anwendern, kryptografische Schlüsselpaare innerhalb eines Glasfasernetzes zu erzeugen und die Kontrolle über die Schlüssel in die Hände des Netzbetreibers zu legen. Dafür nutzt KeeQuant das Potenzial photonischer ICs. QKD soll so den breiten Markt erreichen.

_____ Mondoo: Das Unternehmen automatisiert die Suche nach Schwachstellen und Richtlinienverstößen – in Cloud-Umgebungen, VMs, Kubernetes-Workloads und Containern. Alle Schichten der Anwendungsinfrastruktur werden so geschützt und Exploits effektiv verhindert.

_____ ZenAdmin: Compliance-Vorgaben einzuhalten erfordert Wissen, Strukturen und Prozesse. ZenAdmin unterstützt bei der Implementierung wichtiger Compliance-Standards für die gängigen Regelwerke und hilft so, das Risiko von Sicherheitsvorfällen zu reduzieren und Organisationen für die entsprechende Zertifizierung fit zu machen.

Der ATHENE Startup Award UP@it-sa ist eine Initiative des Nationalen Forschungszentrums für angewandte Cybersicherheit ATHENE beziehungsweise von seinem Projekt Digital Hub Cybersecurity, des IT-Sicherheitscluster e.V. und der it-sa. Mit dem Preis wolle man erfolgreiche Neugründungen und aussichtsreiche junge Unternehmen

im Bereich IT-Sicherheit und Datenschutz würdigen.
www.itsa365.de/up-award

Hacking-Challenge: „Deutschlands bester Hacker“

Deutschlands bester Hacker 2023 wird im Rahmenprogramm der it-sa vorgestellt. Die Initiative um Marco di Filippo hat es sich zum Ziel gesetzt, „die nächste Generation dafür zu begeistern, sich mit IT und IT-Security auseinanderzusetzen“ und die positive Wahrnehmung ethischer Hacker zu fördern. In mehreren Online-Challenges und einem abschließenden Finale in Dortmund wird klar, wer den Sieg nach Hause trägt und in Nürnberg auf der Bühne steht.

Bei der Hacking-Challenge kann jeder mitmachen: Erfahrene IT-Sicherheitsfachkräfte, Schüler:innen, Student:innen oder Quereinsteiger:innen, die ihre Skills unter Beweis stellen möchten. Durch die Teilnahme an der Challenge soll dauerhaft eine Community von legalen und ethischen Sicherheits-hackern, auch „White Hat Hacker“ genannt, entstehen, die sich den Machenschaften der Cyberkriminellen entgegenstellt. Die zukünftigen IT-Sicherheitsspezialisten sollen verstehen lernen, wie kriminelle Hacker vorgehen. Darüber hinaus sollen sie das Rüstzeug erhalten, IT-Schwachstellen zu erkennen, bevor sie von Kriminellen ausgenutzt werden. Aus- und Weiterbildungsangebote sowie der Erfahrungsaustausch innerhalb der Community sollen dazu beitragen, dass die digitale In-

frastruktur von Unternehmen und Institutionen in Deutschland und Europa so sicher wie möglich bleibt. Dazu sollen Interessierte aller Altersgruppen über „Deutschlands Bester Hacker“ durch Schulungen und Fortbildungen an die Schutzziele der Informationssicherheit wie Vertraulichkeit, Verfügbarkeit und Integrität herangeführt beziehungsweise weitergebildet werden.

www.itsa365.de/

<https://deutschlands-bester-hacker.de>

IT-SICHERHEIT
Management und Technik

<kes>
Die Zeitschrift für
Informations-Sicherheit



Wir sind IT-Sicherheit!

Besuchen Sie uns auf der it-sa 2023.

Halle 7

Stand 503



Die einheitliche Cybersecurity-Plattform für Ihr Unternehmen



Global Leader in
Cybersecurity

Entdecken Sie, was möglich ist: trendmicro.com/one