IT-SICHERHEIT

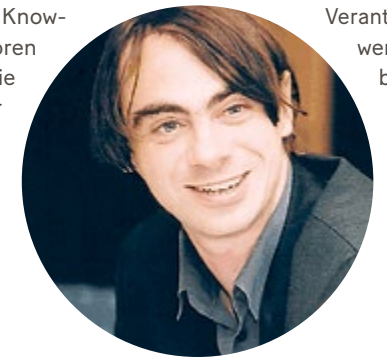
www.it-sicherheit-info.de
EINE PUBLIKATION DES REFLEX VERLAGES Juni 2024

REFLEX VERLAG

GRUSSWORT

Weltweit systemrelevant

Die NIS-2-Richtlinie der EU ist eine Antwort auf die Erkenntnis, dass Cyberattacken immer öfter von staatlichen Akteuren ausgehen. Ressourcen, Kosten, Know-how sind fortan keine begrenzenden Faktoren mehr. So gibt es auch in den Datennetzen die Zeitenwende – heute setzen die Angreifer immer häufiger auf Zerstörung anstelle von Erpressung und Raub. Zweifellos gefährden die Attacken nicht nur die Existenz der angegriffenen Organisationen, sondern den Wirtschaftsstandort Deutschland – die drittgrößte Volkswirtschaft und damit weltweit systemrelevant. Mit dieser Verantwortung heißt es Umdenken, Risiken neu bewerten, Geld in Sicherheit investieren. Weiterbildung, Sicherheitsexpertise und Künstliche Intelligenz sind grundlegende Faktoren für die kommenden Jahre. Für eine resiliente, erfolgreiche Zukunft müssen wir die Informationstechnologie in besonderem Maße schützen.



Christian Raum
Chefredakteur

INHALTSVERZEICHNIS

Für uns steht die bestmögliche Lesbarkeit der Texte an erster Stelle.
Deshalb verwenden wir in der Publikation auch das generische Maskulinum – diese Personenbezeichnungen stehen für alle Geschlechter.

Geschäftsführung im Visier der Cyberkrieger

LEITARTIKEL | VON CHRISTIAN RAUM

Unternehmen müssen sich mit der Tatsache beschäftigen, dass kriminelle Hackerbanden den Organisationen nicht nur erheblich schaden – sondern aufgrund der Fehler und Lücken in den Sicherheitssystemen auf deren Kosten reich werden. Etwa indem sie das Privatleben der Geschäftsführung ausspionieren, deren Mobiltelefone übernehmen, die Buchhaltung manipulieren, Bankkonten plündern oder Daten stehlen.

Kriminelle Hackergruppen ändern ständig ihre Angriffsvektoren und -taktiken und setzen auf langfristige Strategien, bei denen technische und menschliche Schwächen gleichermaßen ausgenutzt werden.

Polizei und Justizbehörden warnen inzwischen, dass Kriminelle nicht nur die Büros in den Chefetagen, sondern auch die privaten Wohnungen, Autos oder Mobiltelefone von Verantwortlichen aus Geschäftsführung oder Topmanagement ausspionieren. Unter anderem schreibt das Bundeskriminalamt, dass Führungskräfte sich mit dem Gedanken befassen müssen, dass sie sowohl in ihrem privaten wie auch im geschäftlichen Umfeld von kriminellen Banden ausgeforscht werden.

Cyberkrieger beobachten die Geschäftsführung, deren Mitarbeitende und Familien.

iStock / chaiyapruek2520

Für die betroffenen Personen grenzt das offensichtlich an ein alptraumartiges Szenario: Unter Anleitung einer kriminellen Zentrale, die sich vielleicht Tausende Kilometer entfernt befindet, sammeln Kriminelle Daten über Geburtsort und Geburtsdatum, Wohnsitz, Familie, Kinder, Kreditkarten, Konten, Autokennzeichen, geschäftliche und private Reisen, Namen und Positionen von Mitarbeiterinnen und Mitarbeitern, E-Mail-Adressen und Telefonnummern.

Alptraum in der Chefetage

Parallel dazu beschaffen sie sich notwendiges Insiderwissen über das Unternehmen und dessen interne Abläufe. Sie manipulieren mithilfe der Künstlichen Intelligenz Stimmen und Videos von Vorständen oder Geschäftsführerinnen und fälschen Mails und Chats.

In einem passenden Moment schlagen die Kriminellen zu. Mit einer gefälschten Mail, einem fingierten Anruf oder in einer manipulierten Videokonferenz fordern sie ihre Kolleginnen oder Kollegen in der Finanzabteilung auf, Geld an ein Konto zu überweisen. Oder sie überzeugen sie, Kontendaten in der Buchhaltung zu ändern und gefälschte Rechnungen umgehend zu begleichen.

Der kriminelle Lohn für diese aufwendigen Angriffe scheint beträchtlich. „Durch CEO-Fraud konnten Kriminelle in den letzten Monaten bereits mehrere Millionen Euro mit zum Teil gravierenden Folgen für das betroffene Unternehmen oder die getäuschten Mitarbeiter erbeuten", heißt es bei der Hamburger Polizei. Nach Angaben des Bayerischen Staatsministeriums der Justiz gelte diese Art des Betrugs nach § 263 Abs. 1 und 3 Satz 2 Nr. 1 StGB als gewerbsmäßiger ▷▷

KI-basierte Cybersecurity erforderlich

Drei Viertel der Unternehmen und Behörden in Deutschland sehen eine drastisch verschärfte Bedrohungslage durch die böswillige Nutzung von Künstlicher Intelligenz. Das ergibt eine aktuelle Studie von Sopra Steria. Wirtschaft und öffentliche Verwaltung sind gefordert, strategisch und operativ umzudenken.

Cyberkriminelle machen sich vermehrt die Stärken Künstlicher Intelligenz zunutze. Mit GenAI und Informationen aus dem Netz erstellen sie beispielsweise individualisierte Phishing-Angriffe. Sprachmodelle helfen beim Coden sogenannter polymorpher Malware. Die passt sich ihrer Zielumgebung an und kann so nicht entdeckt werden.

Cybersecurity im KI-Zeitalter

Die neue Lage erfordert eine angepasste Strategie. Eine für das KI-Zeitalter gerüstete Cybersecurity darf nicht mehr nur nach Regeln arbeiten und nach bekannten Angriffsmustern suchen. Es braucht Flexibilität, Passgenauigkeit und Geschwindigkeit in der Reaktion. Grundlage dafür sind intelligente Muster- und Anomalieerkennung

Barbara Korte, Squad Lead
AI @ Cyber Security bei Sopra Steria

sowie autonome quellenübergreifende Recherche. Personell benötigt die Cybersecurity KI-Expertise und Fach-Know-how.

KI im Dienst der Cybersecurity – vier Beispiele

Eine der großen Herausforderungen für Unternehmen und Behörden ist zu verstehen, wie KI, speziell GenAI in Form von Sprachmodellen, die Cybersecurity verbessert. Vier Anwendungen, um schnell zu profitieren:

1. Risikoanalyse für Informationssicherheitskonzepte nach BSI-IT-Grundschutz: Mithilfe von GenAI-Sprachmodellen lassen sich komplexe Prozesse mit einheitlichem Vorgehen wie der Risikoanalyse deutlich beschleunigen. Die Modelle dienen der Datenvorbereitung, der Produktion von Ergebnissen oder prüfen die Ergebnisse eines anderen Modells.

2. Fehlalarme (False Positives) reduzieren: Mitarbeitende in einem Security-Operation-Center (SOC) prüfen Alerts eines Security-Incident-and-Event-Management (SIEM) auf Echtheit und Relevanz. Mithilfe von KI-Modellen lassen sich die Alarmmeldungen vorqualifizieren. Sprachmodelle vergleichen vergangene Events mit aktuellen und helfen, potenzielle Auswirkungen einzuschätzen.

3. Scoring von CTI-Meldungen: Sprachmodelle analysieren Cyber-Threat-Intelligence-Meldungen (CTI) und vergeben Relevanz-Scores. Mit dieser Information können Incident-, Bedrohungs- und Schwachstellenmanagement vorausschauender betrieben werden.

4. Unterstützung des Regulatory-Compliance-Management: Mithilfe von GenAI lassen sich Anforderungen an die Cyber- und Informationssicherheit aus Gesetzen und Standards damit abgleichen, ob sie für die eigene Organisation relevant sind und welche Lücken im internen Regelwerk zu schließen sind (Gap-Analyse).

Studie „Cybersecurity im Zeitalter von KI"

soprasteria-discover.de/cybersecurity-ki/

MEHR INFORMATIONEN

Sopra Steria berät und begleitet Unternehmen und den öffentlichen Sektor beim notwendigen Umbau ihrer Cybersecurity. Sprechen Sie uns an!

▷▷ Betrug. „Die Täter müssen mit Freiheitsstrafen von sechs Monaten bis zu zehn Jahren rechnen."

Auch automatisierte Systeme werden ausgetrickst

Ob diese Strafen Täterinnen und Täter in einem für sie sicheren Staat wirklich abschrecken, ist fraglich. Aus sicheren Verstecken können sie ihren Angriff auf die Buchhaltung und damit direkt in das finanzielle Zentrum eines Unternehmens lenken. Und wenn die Attacken nicht erkannt werden, können Hacker für lange Zeit aus dem Vollen schöpfen. Unerkannt plündern sie die Organisation und legen dabei ihre Finger direkt auf den Puls eines Unternehmens.

In vielen Betrieben müssen sie sich nicht einmal die Mühe machen, die Chefetage über Wochen auszuspionieren, um dann Mitarbeitende auszutricksen. Denn in diesen Unternehmen haben die Abteilungen wichtige Aufgaben in der Buchhaltung an intelligente, automatisierte Systeme übergeben. Viele Rechnungen werden ohne weitere menschliche Prüfung von Computern überwiesen, wenn sie einen festgelegten Betrag nicht überschreiten oder mit den eigenen, im System hinterlegten Bestellungen übereinstimmen.

Im Gespräch berichten Cybersecurity-Anbieter von Finanzabteilungen, die von der Sicherheit ihrer eigenen Systeme so überzeugt sind, dass sie tatsächlich nur stichprobenartig Überweisungen oder Kontodaten prüfen.

Klare Prozesse und Sicherheitsschulungen fehlen

So macht es das Management den Kriminellen leicht, mit Fake-Rechnung und einem Fake-Betrag Geld auf ein Fake-Konto überweisen zu lassen. Tatsache ist, so bestätigen sowohl Anwaltskanzleien wie auch Cybersicherheitsunternehmen, dass diese Angriffe massiv stattfinden – und dass Unternehmen dadurch erheblich geschädigt werden.

Allerdings – wie diese Angriffe genau ablaufen und wie erfolgreich sie sind, ist kaum nachzuvollziehen. Häufig wird ein solcher Betrug erst nach Wochen oder Monaten entdeckt. Für die Geschädigten bedeutet dies viel Ärger und verursacht hohe Kosten, um überhaupt zu verstehen, wo und wann, wie lange und mit welchen Methoden der Betrug stattgefunden hat. Zu Buche schlagen unter anderem Nachforschungen, forensische Analysen, Anwälte und mögliche Strafzahlungen an andere Geschädigte.

Womöglich stellt sich dann heraus, dass es kein menschlicher Fehler war. Sondern dass ein automatisiertes, vielleicht KI-gesteuertes System in der Finanzabteilung einer Fake-E-Mail aufgesessen ist, in der ein Fake-Konto als valides Konto für zukünftige Fake-Rechnungen bestimmt wurde.

In beiden Fällen wäre dieser Betrug nicht möglich gewesen – oder er könnte sich schneller aufklären lassen –, wenn die Finanzabteilung mit klaren Prozessen, definierten Abläufen und Sicherheitsschulungen arbeiten würde. Die werden in den kommenden Jahren nicht nur für die internen Abläufe vom Gesetzgeber vorgeschrieben und kontrolliert. Auch die einzelnen Branchen werden den Unternehmen vorschreiben, wie sie mit welchen Informationen umgehen müssen.

Bankenbetrug mit SIM-Swapping

Denn bislang machen auch Telefonanbieter und Banken den Kriminellen ihre Arbeit leicht. Europol beschreibt SIM-Swapping als eine Taktik, die auch aufgrund von Sicherheitslücken in den Prozessen der Banken und der Telekommunikationsanbieter gestartet wird.

Auch hier geht es um den Diebstahl persönlicher Daten, um das Ausspionieren des persönlichen Umfelds der Angegriffenen – und es geht um technische Schwachstellen und Geschwindigkeit.

Kriminelle Hacker sammeln über die sozialen Netzwerke oder über gefälschte Internetformulare Daten ein – Name, Geburtsdatum, Arbeitgeber, Telefonnummer, Adresse, Kontonummern. Häufig reichen diese Informationen für die Kriminellen, um in einem Telefonladen eine angeblich verlorene SIM-Karte sperren – und im nächsten Schritt eine neue SIM-Karte mit neuer PIN ausstellen zu lassen.

Ist dies geschafft, muss es schnell gehen. Bevor die geschädigte Person bemerkt, dass ihr Telefon nicht mehr funktioniert, werden die Kriminellen über die gesammelten Informationen in Verbindung mit der Telefonnummer verschiedene Lücken beim Online-Banking ausnutzen. Sie räumen private Konten und Firmenkonten leer. Laut Europol konnte eine inzwischen enttarnte kriminelle Gruppe in mehreren Angriffen Summen zwischen 6.000 und 137.000 Euro von fremden Online-Konten rauben. ❑

Unternehmen sahen sich 2023 vielfältigen Angriffsarten ausgesetzt

31 %	26 %	25 %	18 %	17 %
Spionage (beispielsweise digitales Ausspähen von Kommunikation via E-Mail)	**Ransomware** (Erpressung)	**DDoS** (beispielsweise gezielte Überlastung von Webservern)	**Sabotage** (beispielsweise digitale Störung von industriellen Prozessen)	**Sonstige**

Quelle: DIHK, 2023

So vermeiden Mitarbeitende Cyberangriffe

95 Prozent aller Cyberangriffe werden durch einen Klick auf einen Link oder Anhang in einer E-Mail ausgelöst. Die Folge sind Ausfallzeiten, Datenverlust und finanzieller Schaden. Die beste Abwehr ist ein aufgeklärter Mensch. Daher sind Security-Awareness-Trainings für Mitarbeitende beim IT-Sicherheitsspezialisten Anqa IT-Security fester Bestandteil ihres ganzheitlichen IT-Schutzes.

„Genauso wichtig wie eine sichere IT-Umgebung ist es, das IT-Sicherheitsbewusstsein der Menschen im Unternehmen zu stärken", erklärt Dariush Ansari, Geschäftsführer der Anqa IT-Security GmbH. Mit Phishing-Simulationen und Online-Schulungen sensibilisiert der TÜV-zertifizierte IT-Sicherheitsspezialist in sogenannten Security-Awareness-Trainings Mitarbeitende für den richtigen Umgang mit E-Mails und Daten.

Die Zukunft: Managed Service

Als Managed-Security-Service-Provider und einziger Anbieter übernimmt das Team in Köln von der Planung über die Durchführung bis hin zum Reporting vollumfänglich jeden Schritt der Security-Awareness-Trainings. Die Teilnahme dient den Unternehmen als Nachweis im Rahmen der DSGVO, ISO-Standards oder Cyberversicherung. So können sich IT-Verantwortliche in Unternehmen und Systemhäusern ihrer Kernkompetenz widmen, ohne Zeit in den Bereich IT-Sicherheit investieren zu müssen.

Ganzheitlich gedacht

„Für einen nachhaltigen Lerneffekt funktioniert Security-Awareness nur als 360-Grad-Ansatz", so Ansari. „Die besten Ergebnisse erreichen wir mit einer Kombination aus regelmäßigen Maßnahmen wie Phishing-Simulationen, Online-Schulungsmodulen zu aktuellen Bedrohungen, Awareness-Newslettern, Tools wie der Fake-Webseiten-Detector, Dark-Web-Monitoring und persönlicher Beratung."

Seit über zehn Jahren schützt Anqa IT-Security die IT von 7.000 Unternehmen deutschlandweit.

www.anqa-itsecurity.de

Orchestrierung aller Sicherheitsbelange

INFORMATIONSSICHERHEITSBERATUNG | VON CHRISTIAN RAUM


Clouds sind eine Dienstleistung, mit der die Anbieter lediglich einige genau definierte Problembereiche abdecken.

iStock/pinglabz

Über alle Abteilungen und technischen Grenzen hinweg ist die Sicherheit einer Organisation eine Gesamtaufgabe, die zentral orchestriert werden muss. Dabei ist das Outsourcen der Sicherheitsprobleme in eine Cloud nicht immer eine optimale Lösung.

Die meisten Unternehmen und Organisationen in Deutschland haben inzwischen einen oder mehrere Angriffe von Cyberkriminellen erlitten. Auf deren Leitungsebenen konnten einige Personen die Erfahrung machen, dass sie in die persönliche Haftung genommen werden, falls sie ihre organisationsspezifischen Pflichten schuldhaft verletzt hatten. Allerdings ist umstritten, so bestätigen es auch Anwaltskanzleien, wann genau und in welchem Umfang die Absicherung einer angemessenen Informationssicherheit der Leitungsebene obliegt.

Unternehmen sollten prüfen, ob die Cloud in die Gesamtorchestrierung der IT-Landschaft passt.

Seitens der Kanzleien wird aber sehr deutlich darauf hingewiesen, dass sich mit der Umsetzung der NIS-2-Richtlinie diese Einschätzung und auch die Rechtsprechung ändern werden. Mit der Verabschiedung im Oktober dieses Jahres muss das für Cybersicherheit verantwortliche Topmanagement damit rechnen, dass seine persönliche Haftung deutlich verschärft wird. Parallel dazu wird sein Aufgabenbereich ausgedehnt: Es wird Teil seiner Pflichten, Maßnahmen persönlich zu billigen, die Implementierung zu begleiten und zu überwachen. Die Delegation ist nicht möglich.

Cloud-Angebote: Risiko oder Chance?

Aber mit dem Blick auf die gesamte IT-Landschaft eines Unternehmens können die Sicherheitsexpertinnen und -experten Vorschläge für eine umfassende IT-Sicherheit entwickeln und verwirklichen. Dabei geht es um eine große Zahl von Maßnahmen, Prozessänderungen, Vorgaben zum Archivieren, Speichern und Löschen von Dateien und Dokumenten. Die sind in unterschiedlichsten Gesetzen, Richtlinien und Vorgaben festgeschrieben. Ohne Frage ist es wichtig, dass mit Blick auf diese staatlichen Vorgaben alle Teile als Gesamtheit orchestriert werden.

Jetzt hoffen Geschäftsführer mit einem Wechsel der IT-Landschaften in die Cloud-Systeme ein Rundum-sorglos-Paket für Datenübertragung und Compliance, für Cybersecurity und den sicheren Betrieb der Software zu erhalten.

Cloud-Dienstleistungen sorgfältig prüfen

Doch auch hier ist Sorgfalt gefragt. Denn auch Cloud-Angebote sind lediglich eine Dienstleistung, mit der die Anbieter für ihre Kunden nur bestimmte Teile ihrer Probleme lösen. Und den Cyberverantwortlichen ist geraten, Verträge, Geschäftsbedingungen und Kleingedrucktes aufmerksam zu lesen. In den Unternehmen muss eine Risikoprüfung stattfinden, wie die Leistungen aus der Cloud in die Gesamtorchestrierung passen. Inwieweit darf das Geschäft von einem einzelnen Cloud-Anbieter abhängig sein – und was bedeutet diese Abhängigkeit, wenn etwas nicht funktioniert? Wie lange können Kolleginnen und Kollegen weiter arbeiten, wenn die Verbindungen zum Cloud-Rechenzentrum unterbrochen sind? Und gibt es einen Plan B, wenn die Cloud-Anbieter selbst Opfer einer Hackerattacke werden?

Kosten für KI sind nicht kalkulierbar

Mit der Nutzung der Cloud werden die Anwender und Chefetagen auch mit KI-Anwendungen konfrontiert. Wichtige Fragen rund um die neuen Technologien – Wie hoch sind die Kosten? Wie groß ist der mögliche Geschäftserfolg? – lassen sich im Moment nicht beantworten. Dafür stehen in den Verträgen häufig Nutzungsbedingungen, die in den Unternehmensführungen wenigstens Bauchschmerzen auslösen können: Wer Daten und Dokumente in der Cloud speichert, erklärt sich laut Geschäftsbedingungen und Kleingedrucktem vieler Anbieter damit einverstanden, dass Datensätze, Rechnungsbelege oder auch Bilder für das Trainieren der Künstlichen Intelligenz genutzt werden. Wer damit nicht einverstanden ist, sollte dies sehr klar sagen oder den Anbieter wechseln. ❑

Kontinuierliche Sicherheitstests

PENTESTING UND MANAGED SECURITY | VON DANIELA HOFFMANN

Um Cyberrisiken effizienter zu begegnen, führt um Automatisierung oder das Nutzen von Security-Services für viele Unternehmen praktisch kein Weg mehr vorbei: Fachkräfte fehlen, und IT-Teams sind oft überfordert. Verantwortliche hoffen, mit generativer Künstlicher Intelligenz diese Engpässe zu überwinden.

Die gesetzlichen Anforderungen an Cybersicherheit werden sich in den nächsten Jahren weiter verschärfen. Insbesondere für mittelständische Unternehmen, die heute ebenso von Cyberangriffen bedroht sind wie Großkonzerne, ist jedoch etwa der Aufbau eines eigenen Security-Operation-Centers (SOC) oft zu herausfordernd. SOCs sind für die Orchestrierung von Sicherheitsstrategie, Hardware, Software, Personal und Security-Prozessen verantwortlich.


Mit Künstlicher Intelligenz testen IT-Abteilungen die Systemsicherheit permanent.

iStock/HYWARDS

Der Markt für Fachkräfte ist hart umkämpft, und Sicherheitsexperten zu finden gleicht der Suche nach der Nadel im Heuhaufen. Rund um das Erkennen von Sicherheitsvorfällen und das schnelle Reagieren geht der Trend deshalb zu Managed Detection and Response. Traditionelle Managed-Security-Services auf Basis von Ticket-Systemen geraten derzeit an ihre Grenzen. Unternehmen sollten deshalb die Entwicklung bei integrierten, Cloud- und KI-basierten Plattformen für die Cybersicherheit genau verfolgen.

Suche nach Schwachstellen

Ein wichtiger Teilbereich der Sicherheitsstrategie sind Penetrationstests (Pentesting). Im Sinne eines „freundlichen Hacks" werden Cyberangriffe auf Anwendungen oder das Netzwerk simuliert. Das Ziel: proaktiv mögliche Schwachstellen aufzudecken, ihr Risikopotenzial zu bewerten und Lösungsvorschläge für das Schließen der Sicherheitslücken zu machen. In der Praxis werden Penetrationstests oft nur in großen Zeitabständen durchgeführt, beispielsweise um jährlich die Compliance mit gesetzlichen Security-Vorgaben nachzuweisen.

Gesetzliche Anforderungen an Cybersicherheit werden sich weiter verschärfen.

Kontinuierliche Pentests sind bisher schlicht an den fehlenden Ressourcen gescheitert – sie erfordern einen hohen manuellen Aufwand. Seit der Veröffentlichung von ChatGPT sind die Potenziale von großen Sprachmodellen (Large Language Models – LLMs) für simulierte Angriffe immer offensichtlicher geworden.

KI erleichtert das Pentesting

Die Entwicklung verläuft äußerst dynamisch, und die Anbieter stellen praktisch wöchentlich neue oder verbesserte Funktionalität zur Verfügung. Besonders hilfreich können die Sprachmodelle bei der Entwicklung von Code sein, aber auch bei der Dokumentation. Damit sind LLMs auch für die Aufgaben rund um das Pentesting in den Fokus geraten, und es gibt bereits erste GPTs, die spezifisch dafür trainiert wurden. In der Forschung ist man sich bereits sicher, dass sie bei den Herausforderungen realer Penetrationstests effektiv unterstützen können.

Eine wichtige Aufgabe ist das Schreiben von Testberichten, hier können LLMs manuelle Aufgaben vereinfachen, insbesondere beim Einhalten von durchgängigen Standards für die Berichte. Auch beim Schreiben von Test-Scripts und für das Vorschlagen von Folgemaßnahmen gibt es Automatisierungspotenzial. Zugleich muss die Nutzung von LLMs natürlich ebenfalls höchsten Sicherheitsvorgaben genügen, denn sie können ebenfalls verschiedene Einfallstore öffnen. Dazu gehört, dass Anfragen an das Sprachmodell böswillig manipuliert werden und so zu falschen Ergebnissen führen oder dass Informationen aus Anfragen unerlaubt preisgegeben werden. In vielen Szenarien rund um generative KI, zu der die großen Sprachmodelle zählen, kommt also mehr Arbeit auf die IT-Security-Verantwortlichen zu. ❑

Sicherheitsparadoxon

SICHERHEIT FÜR BIG-DATA-CLUSTER | VON CHRISTIAN RAUM


Viele Unternehmen vergessen den Schutz für die IT-Systeme, die ihre Organisation schützen sollen.

iStock/NicoElNino

Die IT-Abteilungen nutzen Big-Data-Anwendungen auch für Security-Aufgaben, die durch die immer größere Skalierung von internen IT-Netzwerken notwendig werden. Ein Beispiel ist die Verwaltung von Passwörtern für Mitarbeitende und Kunden etwa in Online-Shops. Doch allzu häufig sind diese Daten-Analyse-Cluster leichte Beute für kriminelle Banden.

Für Banken haben Big-Data-Cluster eine besonders sicherheitsrelevante Funktion; sie dienen zur Analyse von Millionen Finanzdaten täglich. Mithilfe der Analysefunktionen sind die Mitarbeitenden auf der Suche nach möglicher Geldwäsche, nach geplünderten Bankkonten oder sie suchen Anzeichen und Muster, die auf die Umgehung von Sanktionen oder Betrug hindeuten können.

In weltweit agierenden Konzernen unterstützen die Analysesysteme dabei, Zutritte zum Netzwerk und den Verkehr innerhalb der IT-Systeme rund um den Globus zu kontrollieren. Dazu speichern die Cluster jede Bewegung in den Infrastrukturen als sogenannte Logfiles. Regelmäßig suchen die Algorithmen in den Clustern nach Mustern oder Abläufen, nach Anomalien und Unregelmäßigkeiten, die auf Eindringlinge hinweisen, auf Programmierfehler oder auf die Anwesenheit von fremden Künstlichen Intelligenzen.

Unsichere Sicherheitssysteme

Doch Expertinnen und Experten warnen in Diskussionen und Sicherheitsforen im Internet, dass in vielen dieser Analysen die eigene Systemsicherheit der Anwender nicht an erster Stelle steht: „Organisationen nutzen Big-Data-Cluster nicht, weil sie an sich so sicher sind, sondern weil sie die Datenanalyse auf viele Petabytes skalieren können. Bei der Aggregation von gigantischen Datenmengen bieten sie sehr kurze Antwortzeiten."

So lernen IT-Verantwortliche eine andere Seite ihrer Big-Data-Systeme kennen, wenn sie sich über deren Sicherheitsvorkehrungen informieren. „Die Hersteller haben sich seit den ersten Tagen der Produktentwicklung auf die Datenverarbeitung konzentriert und keinen besonderen Wert auf Hacker- oder Cyberangriffe gelegt", erklären die Spezialisten. Und tatsächlich sind im Internet viele Sicherheitslücken und viele erfolgreiche Angriffe dokumentiert.

Wenn Security-Websites von besonders aufsehenerregenden Einbrüchen berichten, geht es in vielen Fällen um aufgebrochene Big-Data-Ökosysteme: Bei einer Hotelkette verschwinden Millionen Kreditkartendaten, bei einem Internethändler Zehntausende Passwörter, ein Krankenhaus verliert Hunderttausende medizinische Daten seiner Patientinnen und Patienten.

Legacysysteme mit Sicherheitslücken

Die Hackergruppen profitieren davon, dass bei vielen IT-Herstellern bis vor einigen Jahren – und das betrifft ganz sicher nicht nur die Produzenten der Big-Data-Cluster – am Beginn der Produktentwicklung Security überhaupt kein Thema war. Erst Jahre später wurden die Produkte nach und nach um Sicherheitsfeatures ergänzt. In vielen Installationen der ersten oder sehr frühen Versionen fehlen die Sicherheitsvorkehrungen noch immer.

Bis heute wurden in den Produkten selbst zwar einige Lücken geschlossen. Aber bei vielen veralteten und nicht mehr gewarteten Clustern – die IT-Verantwortlichen sprechen auch von „Legacy-Systemen" – hat sich in den vergangenen Jahren niemand mehr um Sicherheitsfragen gekümmert.

Und wenn kriminelle Banden dann beim Scannen von Zugängen zu Unternehmensnetzwerken ein offenes Big-Data-Ökosystem finden, gleicht das einem Hauptgewinn. Mit Ransomware verschlüsseln sie Millionen Datensätze und legen auf diese Weise einen entscheidenden Teil der Organisation bis zur Lösegeldübergabe lahm. ❑

SCHON GEWUSST?

Bei Ransomware-Attacken handelt es sich um den Straftatbestand der gewerbsmäßigen Erpressung (§ 253 Abs. 1 und 4 StGB). Die Tat wird mit Freiheitsstrafen von 1 bis 15 Jahren geahndet. Auch wenn es nicht zu Zahlungen kommt; bereits der Versuch ist strafbar.

Essenzielles Sicherheitswissen für das C-Level

CYBERDEFENSE | VON CHRISTIN HOHMEIER

Ab Herbst werden IT-Sicherheitsschulungen für das Topmanagement zur Pflicht. Damit soll die Chefetage Wissen und Führungsstärke erhalten, um gemeinsam mit dem Cyberdefenseteam relevante Entscheidungen zum Schutz der Organisation sicher und umfassend zu treffen.

Die Angriffswucht und der durch eine Cyberattacke angerichtete Schaden wird umso vernichtender, je wichtiger die Systeme sind, die von Hackerbanden stillgelegt werden. Die Spanne reicht vom Aufbrechen einzelner Anwendungen in Fachabteilungen bis zum Zerstören lebenswichtiger Prozesse – beispielsweise der Lohnabrechnung.

In der Vergangenheit mussten Unternehmen lernen, dass es den Angreifern mit Attacken auf die Personalabteilung nicht nur gelingt, persönliche Daten der Mitarbeitenden oder deren Verträge auszuspionieren. Die Kriminellen können die Abrechnung der Gehälter sabotieren, indem sie die Datenverarbeitung stoppen und die Auszahlung – womöglich um mehrere Tage – verzögern.

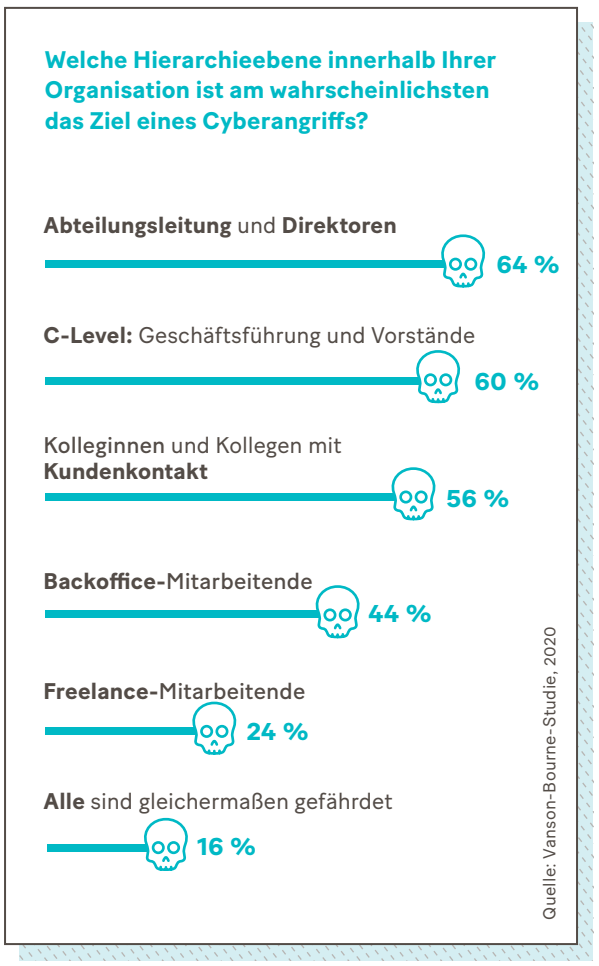
Prinzipien der Cybersicherheit lernen

Im krassen Gegensatz zu solchen Bedrohungsszenarien, so mahnen viele IT-Consultants, fehlen häufig das Interesse und das Hintergrundwissen des Topmanagements für die Sicherheit der digitalisierten Abläufe. Die aus Sicht der Unternehmensführung unangenehmen, teuren und komplizierten Entscheidungen werden nur allzu gern in die IT-Abteilungen oder an Beratungsfirmen delegiert. Dabei ist nach einem solch zerstörerischen Angriff die schnelle Unterstützung der Führungsebene essenziell für das Weiterbestehen der Organisation. Eine Herausforderung ist, praktisch über Nacht ein Budget zur Verfügung zu stellen, das ausreichend ist, um die Lohnabrechnung unmittelbar mit neuen Systemen, etwa bei einem Dienstleister, neu aufzusetzen.

Gefahren beurteilen

Eine zweite Erkenntnis ist – auch die gehört zur Disziplin Cyberdefense –, dass die Infrastruktur niemals „geheilt" werden kann. In Absprache mit den Cyberspezialistinnen und -spezialisten wird das Topmanagement neue Netzwerke, Server und Software installieren. Diese Aufgabe kann sich über Wochen oder Monate hinziehen und endet häufig in einer komplett neu aufgestellten Organisation.

Selbstverständlich ist und bleibt die Leitungsebene auch nach dem Neuaufstellen der Infrastruktur für das Managen der Risiken letztverantwortlich. In enger Abstimmung mit Expertinnen und Experten müssen sie aus der Chefetage heraus alle Vorgänge und Projekte überwachen. ❑



IT-Sicherheit ist Teamplay

Viele IT-Verantwortliche in Unternehmen sind mit der Aufgabe, für ausreichende Cybersicherheit zu sorgen, überfordert. Es mangelt sowohl an Fachpersonal als auch an nötigem Security-Fachwissen. IT-Sicherheit ist komplex und unter diesen Bedingungen nicht leistbar. Eine effektive Lösung für das Problem ist die Nutzung von G DATA 365 | Managed Extended Detection and Response.

Cybercrime ist ein Rund-um-die-Uhr-Geschäft. Angreifergruppen kennen keinen Feierabend und attackieren Unternehmen auch an Wochenenden oder nachts. Daher ist ein 24/7-Schutz der IT-Infrastruktur unbedingt erforderlich. Zudem ist eine sofortige Reaktion im Fall eines erfolgreichen Angriffs entscheidend. Aufgrund des Fachkräftemangels, dem fehlenden Fachwissen sowie der Auslastung der IT-Abteilungen durch den laufenden Betrieb ist MXDR eine lohnende Investition. Dabei überwachen spezialisierte IT-Sicherheitsexperten alle Vorgänge im Netzwerk und auf den Endgeräten und intervenieren bei Cyberangriffen zu jeder Tages- und Nachtzeit.

Überwachung rund um die Uhr

Die Überwachung übernimmt bei G DATA 365 | MXDR ein erfahrenes Analystenteam, das 24/7 im Einsatz ist. Das Team setzt unter anderem auf Threat Hunting, um potenzielle Bedrohungen zu identifizieren und proaktiv vor Cyberangriffen zu schützen. Die Analystinnen und Analysten werten die Ergebnisse der Sensorik aus und reagieren bei einem Angriff sofort. IT-Verantwortliche werden über Vorfälle informiert, in dringenden Fällen auch telefonisch.

Eine Webkonsole bündelt alle relevanten Informationen und ermöglicht es IT-Teams, Einsicht in Sicherheitsvorfälle und ergriffene Maßnahmen zu nehmen. Weiterhin führt das Analystenteam


Die Cyberabwehr in die Hände von Security-Experten geben mit G DATA 365 | MXDR

Root-Cause-Analysen (RCA) durch, um die Ursachen von Sicherheitsvorfällen zu identifizieren und daraus fundierte und verständliche Handlungsempfehlungen in deutscher Sprache abzuleiten.

Verlässlicher Partner

IT-Verantwortliche profitieren durch die Nutzung von G DATA 365 | MXDR von der umfangreichen Expertise des Cyberdefense-Unternehmens. Kunden stehen persönliche Ansprechpartner zur Seite, unterstützt von einem preisgekrönten 24/7-Support in deutscher Sprache. G DATA CyberDefense setzt auf eine direkte, persönliche Betreuung und nutzt eigens entwickelte Software zur Angriffserkennung, die kontinuierlich auf Basis von Kundenfeedback weiterentwickelt wird.

Beim Onboarding berät das Cyberdefense-Unternehmen individuell. Dabei wird unter anderem festgelegt, auf welchen Endpoints welche spezifische Response erfolgen soll. Die Datenverarbeitung geschieht ausschließlich auf Servern in Deutschland. Damit unterliegt sie den strengen deutschen Datenschutzrichtlinien. Der Schutz der Kundendaten sowie der Schutz vor Cyberbedrohungen stehen für G DATA CyberDefense an erster Stelle.

www.gdata.de/mxdr

Zugangsüberwachung im smarten Gebäude

OBJEKTSCHUTZ | VON CHRISTIN HOHMEIER

Künstliche Intelligenz, IoT-Sensoren und intelligente Videosysteme sind digitale Werkzeuge, die beim Werkschutz und bei Sicherheitsdienstleistern zum Einsatz kommen. Sie schützen sowohl Mitarbeitende und Betriebsgelände vor Cyberattacken wie auch vor physischen Angriffen.

Mit den neuen Technologien rund um Sensorik, Künstliche Intelligenz, Smart Building und digitale Vernetzung wird die Abbildung von Vorgängen und Prozessen in Gebäuden und auf Unternehmensflächen in der virtuellen Welt zu einer wichtigen Disziplin im Objektschutz.

Das Herzstück ist in vielen Fällen ein Kommandozentrum, in dem die Daten aus den unterschiedlichen Quellen zusammenlaufen. Im Hintergrund ist es eine Aufgabe der Künstlichen Intelligenz, die unterschiedlichsten Informationen zu analysieren und auf Muster zu prüfen. Auf diese Weise werden beispielsweise die Videoaufzeichnungen ständig analysiert, bei möglichen Bedrohungen Aktionen ausgelöst, Prozesse angestoßen – und, wenn nötig, Personen der Zugang auf das Firmengelände verweigert.

Verdächtige Bewegungen können sofort auf einen Bereich im Gebäude eingegrenzt werden. Auf ihrem Dashboard sehen die Mitarbeitenden, wie eine Person sich einem Hochsicherheitszugang nähert. Hier schützt eine feuerfeste Tür ein Rechenzentrum, dies ist wiederum ein Teil der unternehmenskritischen Infrastruktur.

Das System löst einen Alarm aus. Parallel gleicht es Daten aus Zugangssperren, Aufzügen oder Schließsystemen ab – es findet den Namen und das Bild des Besitzers des Zugangscodes, der benutzt wurde. Diese Informationen erscheinen auf dem Dashboard. Über die Sicherheitssysteme sprechen die Wachschützenden im Kontrollzentrum die Person direkt an und bitten um Authentifizierung.

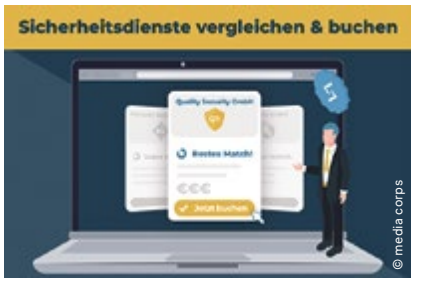
In den allermeisten Fällen ist alles in Ordnung, das Kontrollzentrum öffnet den Zugang für den angemeldeten Wartungstechniker. ❑

Die Revolution von Sicherheit

Sicherheit ist an vielen Stellen von zentraler Bedeutung. Mit SECmarket Booking, einer Plattform für alle Sicherheitsbedürfnisse, wird die Buchung von Sicherheitsdienstleistungen so einfach wie nie. Die Plattform bietet absolute Transparenz rund um die Anbieter und hilft so, den passenden Dienstleister schnell und unkompliziert zu finden und zu buchen.

Als erste übergreifende Online-Plattform erleichtert SECmarket die Buchung qualifizierter Sicherheitsdienste. Dank des detaillierten Anbieterprofils, inklusive Zertifizierungen und Kundenbewertungen, kann man sofort eine fundierte Entscheidung treffen.

Ein Instrument dabei ist der „SECmarket-Score", ein algorithmisch bestimmter Wert, der eine objektive Orientierung liefert.



SECmarket: Easy to use Interface

Ein herausragendes Merkmal von SECmarket ist die Oberfläche. Innerhalb von Minuten können Kunden Sicherheitsdienstleistungen finden und buchen. Zusatzqualifikationen, die für bestimmte Sicherheitsaufgaben erforderlich sind, lassen sich einfach hinzufügen.

Die Digitalisierung birgt weitere Vorteile. Die für die Suche und Buchung notwendige Zeit schrumpft erheblich, was für Unternehmen von großem Wert ist.

SECmarket setzt durch strenge Überprüfungsprozesse und transparente Kundenbewertungen neue Standards im Sicherheitssektor. Die Plattform zeigt, wie moderne Technologien genutzt werden können, um die Branche moderner und effizienter zu gestalten.

booking.secmarket.de

„Mit NIS-2 wird Cybersecurity zur Pflicht"

Entspricht Ihre IT-Sicherheitsstrategie bereits den aktuellen Anforderungen? Ralf Kempf ist Geschäftsführer von Pathlock Deutschland, IT Security Researcher und SAP Security Evangelist seit über 25 Jahren. Er erklärt, warum Cybersecurity mit NIS-2 nun endgültig zur Chefsache wird.

Hallo, Ralf Kempf, was ist dieses neue IT-Sicherheitsgesetz, und klingt das nicht sehr dramatisch? Nein, sondern durchaus angemessen. Da sich die ohnehin hohe Bedrohungslage in den letzten Monaten nochmals zugespitzt hat, wurde es höchste Zeit für die Novelle der europäischen Network and Information Security Directive. Schon im Oktober muss NIS-2 in nationales Recht umgesetzt sein, und dann dürfte so manche Chefetage aus allen Wolken fallen.

Wieso sollte sich das Management überhaupt damit beschäftigen? Weil die bisherigen Anforderungen deutlich verschärft und auf wesentlich mehr Unternehmen ausgeweitet werden. Zusätzlich zu den Betreibern bereits kritischer Infrastrukturen wie Energieversorger und Krankenhäuser gelten sie dann auch für deren Lieferketten und viele weitere Branchen. Auch mittelständische Unternehmen unterliegen jetzt den scharfen KRITIS-Vorgaben, sofern es sich um, wie es heißt, wesentliche Einrichtungen handelt, etwa Logistiker oder manche Maschinenbauunternehmen.

Der Countdown für die verschärften Sicherheitsvorschriften für NIS-2 läuft.

Wenn mein Unternehmen jetzt dazugehört, was wird von mir erwartet? Nun, NIS-2 nimmt alle technisch und organisatorisch sehr stark in die Pflicht, besonders in puncto Risikoanalyse und Schutz der Informationssysteme wie Krisen- und Notfallmanagement. Hinzu kommen verschärfte Meldepflichten in neuer Qualität: Jeder erhebliche Sicherheitsvorfall ist innerhalb von 24 Stunden zu melden. Wenn ein Unternehmen dem nicht nachkommt, folgen Bußgelder von bis zu zehn Millionen Euro oder zwei Prozent des weltweiten Vorjahresumsatzes.

Darum die Chefsache? Genau, ein Management, das es sich jetzt noch leistet, lediglich zu delegieren und ansonsten ahnungslos zu sein, kann sich nicht mehr aus der Verantwortung ziehen. Die Empfehlung ist daher eindeutig: das Thema priorisieren, die Umsetzungsfristen im Auge behalten und vor allem zeitnah die richtigen Partner ins Boot holen. Der Aufbau eines unternehmensweiten Risikomanagements und die Einführung einer Multi-Faktor-Authentifizierung lassen sich nicht in wenigen Wochen realisieren.

Das dürfte für viele Unternehmen eng werden. Wie konnte es so weit kommen? Da gibt es mehrere Gründe: Meist lehnten sich Verantwortliche bei der Frage der Anwendungssicherheit entspannt zurück – man habe doch alles ordentlich beim Outsourcer in der Cloud, inklusive Firewall. Ein Super-GAU der IT-Sicherheit wie letztens der Diebstahl des Generalschlüssels für Microsofts Azure Cloud zeigt drastisch, wie blindes Vertrauen in die Infrastruktur und das Accountmanagement der großen Hyperscaler zu schwerwiegenden Sicherheitslücken führen kann. Gleichzeitig galten Buzzwords wie Zero Trust oder Software Defined Networks als Allheilmittel für die Absicherung von IT-Systemen, und elementare Grundlagen wie ein IT-Security-Management-system oder der Aufbau echter Security-Kompetenz gerieten aus dem Blickfeld.

Und was sollten Managements jetzt tun? Keinesfalls nichts, auch wenn ihr Unternehmen vielleicht noch nicht zu den neuen sogenannten wesentlichen Einrichtungen oder deren Lieferketten gehört, das kann sich bald ändern. Um den neuen Anforderungen gerecht zu werden, brauchen sie eine umfassende Bestandsaufnahme. Zunächst die Gretchenfrage: Cloud oder On-Premise? Zweifellos gibt es sehr gute Szenarien für Cloud-Anwendungen, aber auch hier ist es wichtig, sie mit einer ganzheitlichen Sichtweise auf das IT-System umzusetzen.

Ralf Kempf, Geschäftsführer Pathlock Deutschland

Was meinen Sie mit ganzheitlich? Im konkreten Fall bedeutet das: Ist die IT-Basis nicht sicher, wird es in der Cloud nicht besser. Um sich ganzheitlich aufzustellen, helfen beispielsweise Best Practices für Konfiguration, Betrieb, Überwachung und ein Notfall-Fallback. Alle Komponenten müssen in die unternehmensweite Sicherheitsstrategie integriert werden. Grundsätzlich gilt: Statt blindem Vertrauen in die Cloud ist weiterhin jeder selbst für die Erkennung von Bedrohungen und Angriffen zuständig. Entscheidend ist, dafür ausgewiesene IT-Security-Fachleute oder kompetente externe Partner zu haben.

Abgesehen von externer Unterstützung, wie kann man sich neu aufstellen? Mithilfe von Regelwerken, zum Beispiel dem NIST-Framework oder dem DSAG-Prüfleitfaden für SAP-Systeme kann die IT-Security zügig um ein Vielfaches verbessert werden. Die Methodik ist dabei vorgegeben: Identifiziere deine Assets und Technologien, erstelle eine realistische Risikoeinschätzung, schütze die Systeme, spiele Patches ein, und wirf die Standard-User raus. Etabliere schließlich ein System, das all dies überwacht – und zwar rund um die Uhr.

Das klingt nach erheblichem Aufwand? Ja, aber es ist kein Hexenwerk: Mit konsequenter Methodik, den richtigen Prioritäten und guten Tools lassen sich auch große Unternehmen fit machen für NIS-2 und mit nur ein, zwei Spezialisten überwachen. Allerdings müssen diese exzellent ausgebildet sein, beharrlich skeptisch hinterfragen und immer up to date sein.

Abschließend noch die unvermeidliche Frage, welche Rolle kann KI hier spielen? Tatsächlich eine große, in zweierlei Hinsicht: KI hat die Spielregeln grundlegend verändert, und die neue Bedrohungslage bietet durchaus Grund zur Sorge, da sich die Angriffstechniken rasant verbessern. Während viele Unternehmen gerade beginnen, die Sicherheitsvorgaben von NIS-2 umzusetzen, stehen sie durch neue Angriffsvektoren mittels generativer KI bereits vor der nächsten Hürde. Andererseits kann KI die IT-Security auch meilenweit voranbringen, muss aber bedacht eingesetzt werden und erfordert tiefgreifende Security-Expertise. Es gibt bereits Tools, die die Vorteile sehr gut nutzen, etwa durch automatisierte Prozesse wie unsere Threat-Intelligence-Lösung. Sie bietet Echtzeitabsicherung mit KI-gestützten, integrierten Gegenmaßnahmen.

Vielen Dank, Herr Kempf.

www.pathlock.de

MEHR INFORMATIONEN

Pathlock ist der führende Security-&-GRC-Spezialist für SAP, S/4HANA, Multivendor und hybride ERP-Systeme. Mit 500 Mitarbeitern an 15 Standorten weltweit beraten sie mehr als 1.200 Kunden. Pathlock verbindet umfassende Software, hohe Expertise und etablierte Best-Practice-Methoden für den Schutz geschäftskritischer Applikationen, Daten und Prozesse. So unterstützen sie Unternehmen bei der Erkennung von Anomalien, Hackerangriffen, Manipulationen oder Datendiebstahl.

Sicherer Wechsel in die Cloud

SAP-SICHERHEIT | VON CHRISTIAN RAUM

Unternehmen machen den nächsten Schritt bei der Digitalisierung und stellen auf Cloud-Systeme um. Parallel mit diesem Neuanfang gehen ein geordnetes Herunterfahren und Abschalten der bisher genutzten Rechenzentren einher. Auf den alten Servern und Speichern lagern Daten, Unterlagen, Dokumente, Verträge, die einen erheblichen Wert haben. Sie stellen das Gedächtnis der Organisation dar.

Wenn ein Unternehmen mit der digitalen Transformation ernsthaft beginnt und ERP, Personalwirtschaft und Produktion in die Cloud überführt, diskutiert das Projektteam, was mit den alten Systemen und Daten im bisher genutzten Rechenzentrum geschehen soll.

Für viele ist es die einfachste Lösung, alle alten Geräte mit der gesamten Software so lange stehen zu lassen und weiterzubetreiben, bis sie nicht mehr gebraucht werden. Für das Projekt bedeutet dies eine Vereinfachung und damit eine deutlich schnellere Umsetzung.

Doppelte Kosten statt Einsparungen

Allerdings scheint es auf den zweiten Blick ein eher schlechter Kompromiss zu sein. Denn anstelle der versprochenen und im Projekt angestrebten Kostenreduzierung aufgrund der Transformation werden jetzt die doppelten Kosten fällig. Schließlich bleibt die alte Systemlandschaft stehen. Die IT-Abteilung wird sich über Jahre um die Wartung kümmern, das Wissen rund um Betrieb und Sicherheit muss weiter vorhanden sein.

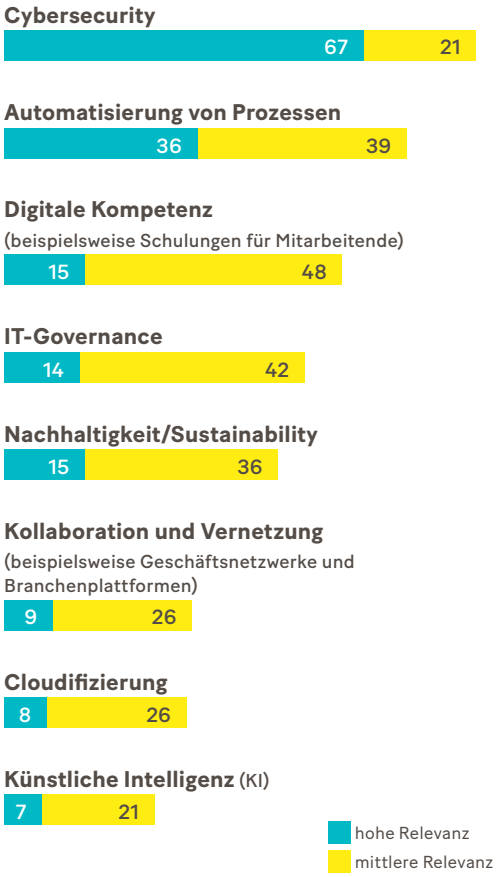
Und das gesamte Vorgehen widerspricht dem Vorhaben, eine cybersichere und langfristige Lösung zu finden. Jedem Mitglied im Projektteam sollte klar sein, dass die Wartungszusagen des Herstellers langfristig auslaufen, es in absehbarer Zeit keine Systemsicherheit mehr gibt.

Compliance beachten

In diesem Fall hat nach der Projektlaufzeit, nach vielen Diskussionen und verbrauchten Budgets und Ressourcen der Wechsel der Plattform nur sehr halbherzig oder eben – für große Teile des Unternehmens – gar nicht stattgefunden.

Die bessere Lösung ist es, wenn die Verantwortlichen sich für die compliancekonforme Dekommissionierung von Altsystemen Expertinnen und Experten an Bord holen, die bei der Qualifizierung von Daten helfen. Sie unterstützen das Projektteam, die Daten zu analysieren, deren Wert und Bedeutung zu ermitteln. Sie beraten bei der Entscheidung, welche Daten einen so hohen Wert haben, dass sie mit auf die neue Plattform in die Cloud genommen werden sollten. ❑

Inwieweit sind folgende Themen für die Investitionsplanung 2024 von SAP-Kunden relevant?
in Prozent



Quelle: DSAG e. V., 2024

Fokusinterview

„Sichere Software für sichere Produkte"

Autos, Maschinen oder Medizintechnik – digitalisierte und mit dem Internet verbundene Produkte werden nicht ausschließlich von spezialisierten Systemhäusern entwickelt und produziert. Laut Bundesverband IT-Sicherheit e. V. (TeleTrusT) unterschätzen Hersteller den Entwicklungsaufwand für cybersichere Geräte. TeleTrusT-Geschäftsführer Dr. Holger Mühlbauer erklärt Grundsätze der Produktentwicklung.

Herr Dr. Mühlbauer, was ist aus Ihrer Sicht die Voraussetzung für sichere Software in einem sicheren Produkt? Security by Design ist ein Prinzip, das gewährleistet, dass Sicherheitsanforderungen bereits zu Beginn des Entwicklungsprozesses systematisch ermittelt und berücksichtigt werden. Das Prinzip ist

Dr. Holger Mühlbauer, Geschäftsführer TeleTrusT

nicht neu und im Grunde genommen eine Anleitung zum Bau und Betrieb sicherer Systeme.

Welche Rolle spielt Security by Design? Die Hersteller von digitalisierten Produkten, von Prozessen und Dienstleistungen werden in die Lage versetzt, gesetzliche und regulatorische Vorgaben zur IT-Sicherheit sowie diesbezügliche marktübliche und kundenspezifische Anforderungen einzuhalten und entsprechende Zertifizierungen zu bekommen.

Security by Design ist eine unabdingbare Voraussetzung, um Gefährdungen der Betriebssicherheit von Produkten und Diensten durch Sicherheitslücken abzuwehren. Ebenso ist dies die Grundvoraussetzung für die Gewährleistung von Privacy-by-Design-Prinzipien, die zum Schutz der Privatsphäre bei Verarbeitung personenbezogener Daten von der EU-DSGVO gefordert werden.

Wie wird eine langfristige Produktsicherheit erreicht? Entscheidend ist ein sicheres Produkt-Lebenszyklus-Management. Voraussetzung hierfür ist die Einbindung aller Phasen in ein Qualitäts- und Informationssicherheits-Management-System. Auf dieser Basis haben alle beteiligten Unternehmensbereiche wie beispielsweise die Geschäftsführung, das Produktmanagement, Produktentwicklung, Datenschutzbeauftragte oder auch IT-Sicherheitsexperten ihren jeweiligen Teil der Verantwortung für die Cybersecurity des Produkts zu übernehmen.

Welche Rolle spielt die Unternehmensführung bei der Umsetzung dieser Konzepte – und welche Pflichten sind damit verbunden? Eine eindeutige Zuordnung der Umsetzungsverantwortung innerhalb der Organisation durch das Topmanagement gilt als entscheidend für den Erfolg. Hierbei ist die Regelung wichtig, ob die jeweilige Instanz lediglich für die Einführung der Compliance-Normen zuständig ist. Oder ob nach erfolgreichem Abschluss der Einführung diese mit der nachfolgenden dauerhaften Betreuung der Normumsetzung beauftragt wird.

Auch eine nachhaltige Überprüfung der Umsetzungsstände in den eigenen Organisationen ist dringend zu empfehlen. Etwa indem ein Vertreter des Projektsteuerungs-Teams in regelmäßigen Abständen an die Unternehmensführung berichtet.

Produkte von Grund auf sicher

SECURITY BY DESIGN | VON DANIELA HOFFMANN

Mit der EU-Richtlinie NIS-2 und dem Cyber Resilience Act stehen neue strenge Regelungen bei Produktsicherheit an. Diese betreffen auch Hersteller von Sicherheitsprodukten und digitalen, IoT-basierten Services.

Security by Design bedeutet, die Cybersicherheit von Produkten vom ersten Entwicklungsschritt an mitzudenken. Dieser Ansatz ist einer der in der Richtlinie NIS-2 festgelegten Cybersecurity-Mindeststandards für Kritische Infrastrukturen. Gerade dort, wo es um digitale Services für Produkte geht, die über Sensoren im Internet of Things Echtzeitdaten etwa an den Hersteller senden, ist besondere Aufmerksamkeit geboten.

Ob das eine Webmaschine in der Textilindustrie ist, die ihre Muster IoT-gesteuert fertigt, eine Photovoltaik-Anlage, die ihre Daten in das Unternehmensnetz einspielt oder ein IT-Sicherheitsservice, der für NIS-2-Installationen Software anbietet: Für jedes Gerät und Produkt muss sichergestellt werden, dass es über seinen Lebenszyklus hinweg nicht gehackt und als Teil eines Bot-Netzes missbraucht werden kann.

Cybersecurity gehört zum Fundament von Software und IT-gesteuerten Produkten.

iStock / sarayut

Neue Konzepte für IT-Services

Die Sicherheitsvorgaben betreffen dann auch sämtliche vernetzten Geräte wie Sensoren, IoT-Gateways oder Edge-Computer. Für eingebettete Systeme gilt ebenfalls, dass ihre Herstellung nach Secure-by-Design-Vorgaben erfolgt sein muss. Das beginnt schon mit einem sicheren Betriebssystem und erstreckt sich über nach sicheren Produktionsprozessen gefertigte Hardware und Software.

Weil digitale Services ein recht neues Thema für viele Hersteller sind, wird rund um IoT-Anwendungen nach wie vor viel experimentiert. Zugleich zeigt die Praxiserfahrung, dass es in puncto Sicherheit keine einfachen, vorgefertigten Lösungen gibt: Dafür sind die Anwendungsfälle und Einsatzszenarien schlicht zu unterschiedlich. So kann es etwa um das remote Einspielen von Software-Updates oder um Fernwartung gehen, damit Servicetechniker keine teuren, zeitintensiven Vor-Ort-Einsätze machen müssen.

Höhere Standards für Maschinen

Rund um vorausschauende Wartung werden Echtzeitdaten zur „Maschinen-Gesundheit" übermittelt. Jeder Zugriff von außen muss so abgesichert sein, dass keine Angriffsfläche für Cyberkriminelle entsteht. Um neue Produkte und Services auf den Markt zu bringen, müssen Hersteller sich also dringend auf erheblich höhere Cybersecurity-Standards einstellen. ❑

IT-Infrastrukturen unter Beschuss – Zeit, das Spiel zu ändern!

Die Bedrohungslage im Cyberraum ist enorm. Da die Existenz von Unternehmen und die Sicherheit der Unternehmenswerte auf dem Spiel stehen, ist es Zeit, altmodische Einzellösungen zu vergessen. Sie sind: teuer, kompliziert, ineffizient. Die Lösung: Enginsight.

Was Unternehmen wirklich brauchen: integrierte Security-Lösungen, die Kontrolle und Transparenz über IT-Infrastrukturen und -Netzwerke garantieren. So gelingt auch der Balanceakt zwischen begrenzten Security-Ressourcen und steigenden -Anforderungen. Mit der einzigartigen Unified Security Management-Plattform von Enginsight bekommen Sie das Thema Cybersicherheit nachhaltig in den Griff und bauen eine effektive Sicherheitsarchitektur auf.

MEHR INFORMATIONEN

Hallo zur einen Lösung, die (fast) alles kann:

- Visualisierung, Überwachung: Das gesamte Netzwerk in Echtzeit im Blick.
- Angriffserkennung und automatische Reaktion: Bedrohungen erkennen, bevor sie Schaden anrichten, und automatische Abwehrmechanismen starten.
- Angriffssimulationen: Verteidigung testen und optimieren.
- Eventlogs: Ereignisdokumentation und -Analyse zur Verbesserung der Sicherheitsstrategien.
- Reports: Umfassende Berichte, um Maßnahmen zu bewerten und zu verbessern.
- Ersparnis: Lizenz- und Betreuungskosten überflüssiger Software sparen.
- Compliance: Erfüllen der technischen Anforderungen von Regularien wie NIS-2.

Transformieren Sie jetzt Ihre Cybersicherheitsstrategie.

www.enginsight.com

„NIS-2 – der Turbo für Cyberresilienz?"

Angesichts steigender Cyberbedrohungen ist Cyberresilienz wichtiger denn je. Welche Rolle dabei NIS-2 spielt und welches Vorgehen die Unternehmensberatung Horváth empfiehlt, erklärt Dennis Müllerschön.

Besteht Handlungsdruck? Unsere CxO-Studie, für die wir über 750 Vorstände befragt haben, zeigt: Ein Viertel der Unternehmen wurde in den letzten zwölf Monaten Opfer signifikanter Cyberangriffe. Cyberrisiken zählen zu den größten Geschäftsrisiken unserer Zeit. Mit der EU-Richtlinie NIS-2 hat der Gesetzgeber verschärfte Sicherheitsanforderungen für kritische Wirtschaftsbereiche eingeführt. Dies spiegelt sich in der steigenden Nachfrage nach Beratungsleistungen wider.

Welche Auswirkungen hat NIS-2? Durch erweiterte Schwellenwerte und Geltungsbereiche sind allein in Deutschland rund 30.000 Unternehmen betroffen. Sie müssen Maßnahmen zur Stärkung der Cyberresilienz ergreifen. Im Fokus stehen Risikomanagement, Sicherheitskonzepte und Vorfallsbewältigung. NIS-2 bietet dabei eine große Chance: Wer sie korrekt umsetzt, erhöht sein Resilienzlevel auf ein adäquates Niveau.

Dennis Müllerschön, Principal und Solution Manager für Cyber Security bei Horváth

Wie sollten Unternehmen agieren?
Es heißt: handeln! Unsere Erfahrung zeigt klar, ein systematisches Vorgehen zahlt sich aus. Eine Reifegrad-Analyse bietet die nötige Orientierung. Identifizieren Sie die wichtigsten Handlungsfelder, definieren Sie das Zielniveau entlang Ihres Risikoappetits, und setzen Sie risikobasiert um.

www.horvath-partners.com/de

Paradigmenwechsel bei Kritischen Infrastrukturen

NIS-2 UND KRITIS | VON CHRISTIN HOHMEIER

Der Schutz der Kritischen Infrastrukturen ist eine zentrale Herausforderung innerhalb der EU. Deshalb argumentierten die Verantwortlichen bei Diskussionen und Abstimmungen der NIS-2-Richtlinie immer mit der verschärften Gefahrenlage aufgrund des Kriegs in der Ukraine. Wichtig ist es, dass die Organisationen und Unternehmen umfassend Ressourcen, Know-how und Technologien einsetzen, die den größten Cyberrisiken ausgesetzt sind.

Die aktuellen und sehr hitzig geführten Sicherheitsdiskussionen in Politik und Wirtschaft drehen sich um die Network and Information Systems 2.0 Directive – oder kurz NIS-2-Richtlinie. In Deutschland werden diese Richtlinien innerhalb des NIS-2-Umsetzungs- und Cybersicherheitsstärkungsgesetzes –NIS-2UmsuCG – in nationales Recht überführt. Der für die Umsetzung relevante Stichtag ist der 17. Oktober 2024. Bis dahin wird es im Bundestag noch Anhörungen geben, der endgültige Gesetzestext soll dann verabschiedet werden.

Das von der Politik vorgegebene Ziel ist es, die Cyberresilienz innerhalb der EU zu stärken, indem in den Mitgliedsstaaten ein einheitliches und sehr hohes Sicherheitsniveau verwirklicht wird. Die betroffenen Unternehmen sollen sicher sein, dass die Anforderungen EU-weit einheitlich gelten, dass es zu keiner Verzerrung des Wettbewerbs kommt – und dass die von einem Unternehmen in einem Wirtschaftsraum umgesetzten Maßnahmen auch in jeder anderen Region Europas gleichermaßen gelten.


Heute geht es um den Schutz weltweiter Netzwerke.

iStock/NicoElNino

Sofort mit der Planung beginnen

Die Vorschriften für die Unternehmen sind umfassend und betreffen die unterschiedlichsten Bereiche – häufig geht in der Debatte unter, dass es am Ende nicht nur um Computer und Netzwerke, digitale Prozesse und das neu zu installierende Informationssicherheits-Management-System geht. Auch viele Maßnahmen zum physischen Schutz von Betriebsgelände, Anlagen und Büros stehen auf der Umsetzungsliste.

Diese Liste scheint für die Unternehmensführungen unendlich lang – immerhin gehen Expertinnen und Experten gleichermaßen davon aus, dass viele Einrichtungen und Unternehmen bis zu zwei Jahre für die vollständige Umsetzung benötigen könnten. Deshalb ist sofortiges Handeln wichtig: Die Unternehmen unterliegen einer Melde- und Registrierungspflicht gegenüber den EU-Behörden, sie sollten also sofort mit den Planungen und Umsetzungen beginnen.

Viele Betroffene sehen ihre Pflichten nicht

Dies wird auch deshalb eine Herausforderung, da nach Einschätzungen aus der Politik der größte Teil der von der NIS-2-Gesetzgebung zum Handeln gezwungenen Unternehmen bislang keine Ahnung haben, dass sie überhaupt von den Richtlinien betroffen sind. Selbst bei den Recherchen zum Thema ist ein erheblicher Unterschied bei den Schätzungen zu der Zahl der betroffenen Unternehmen erkennbar.

Manche Beobachtenden sprechen von insgesamt 90.000 Unternehmen in Deutschland. Zur Umsetzung der Richtlinien seien alle die verpflichtet, die mehr als 50 Mitarbeitende beschäftigen und in 18 relevanten Branchen tätig sind. Sie rechnen, dass 40 bis 50 Prozent aller Unternehmen in Deutschland von NIS-2 betroffen sind – kommen im Ergebnis also auf 40.000 bis 45.000.

Andere Quellen gehen von rund 30.000 Organisationen aus, die zu der Umsetzung von NIS-2 verpflichtet sind. Und verschiedene Kritiker weisen darauf hin, dass die EU die Richtlinien mittelfristig für weitere Branchen als verbindliche Sicherheitsstandards festlegen könnte. ❑

SCHON GEWUSST?

Im Umsetzungsgesetz (Art. 1 § 59 (5) NIS-2UmsuCG) sind mit Verweis auf das Gesetz über Ordnungswidrigkeiten (§ 30 (2) Satz 3 OWiG) Bußgelder von bis zu 20 Millionen Euro vorgesehen. Hier bezieht sich der Gesetzgeber allerdings auf Ausnahmefälle, bei denen einer Anordnung des BSI (Bundesamt für Sicherheit in der Informationstechnik) zuwidergehandelt wird.

Strategien gegen Spionage und Sabotage

CYBERSICHERE PRODUKTIONSNETZWERKE | VON CHRISTIAN RAUM

Internet-of-Things-Netzwerke verbinden Maschinen und Lager, Prozesse und Systeme über Unternehmensgrenzen hinweg. Ihre Aufgabe ist es, Produktionsstandorte zu vernetzen, die Zusammenarbeit der Geschäftspartner zu verbessern oder auch Störungen in der Lieferkette rechtzeitig zu erkennen und entsprechend darauf zu reagieren. Damit die automatisierten Komponenten und Schnittstellen reibungslos arbeiten, müssen alle Bereiche des IoT-Netzwerks gegen Cyberangriffe geschützt sein.

In den vergangenen Jahren erlebten Unternehmen einen Umbruch. Bis dahin waren Probleme mit Produktionsstandorten und den Lieferketten, die sie verbinden, nie ein großes Thema. Die wichtigen betriebswirtschaftlichen Kriterien waren Effizienz, niedrige Kosten, geringe Lagerbestände, Single Source und flexible Verträge.

Heute sind Unternehmen von Faktoren umgeben, die sie nur zum Teil beeinflussen können. Bislang kaum relevante makroökonomische Ereignisse stellen die Unternehmen vor neue Herausforderungen. Dazu zählen Unterbrechungen der Lieferkette durch Kriege, Sanktionen, Cyberkriminalität. Industriespionage und Sabotage beeinflussen das Handeln und die Entscheidung ebenso wie Rohstoffkrisen und die Folgen klimabedingter Katastrophen.

Die Unternehmensführung reagiert, verändert die Strategie, baut Produktionen um, organisiert die Beschaffung neu, indem sie sich online mit Lieferanten und Kunden eng vernetzt. Die Verantwortlichen verstärken ihre Cybersicherheitssysteme, sie wechseln zu Just-in-Case, setzen auf höheres Inventory, auf lokale Lieferanten und Alarmsysteme. Ziel ist immer, dass das Unternehmen unabhängig von weltweiten Störungen arbeiten kann. Und dass trotz aller Probleme die Produktion auf keinen Fall zum Stehen kommt – beispielsweise weil die Lieferung wichtiger Teile in einem Hafen blockiert ist oder sie in überfluteten Regionen versinken.

Sichere Abschottung von Maschinennetzen

Der Schutz der Produktionen und hier wiederum die Sicherheit jeder einzelnen Maschine ist innerhalb dieser neuen und besorgniserregenden Szenarien ein entscheidender Faktor. Grundsätzlich sollen die Standorte von der Außenwelt maximal abgeschottet sein – gleichzeitig aber auch einen sicheren Zugang für den nötigen Datenaustausch über das IoT-Netzwerk zur Verfügung stellen. Mit diesem Datenaustausch und der Datenanalyse garantiert die IoT-Installation die nötige Transparenz, um unvorhersehbare Ereignisse abzufedern, ohne dass die Fertigungsstraßen stocken.


Die Sicherheit jeder einzelnen Maschine ist die Grundlage für die Sicherheit aller.
iStock / marchmeena29

Sichere Maschinen – sichere Prozesse

Je besser die IoT-Netze geschützt sind, desto mehr können sie skalieren und neue Funktionen und Services einbinden. Neben der Beschaffung, Logistik und Lagerhaltung ist es denkbar, auch Design und Produktentwicklung direkt mit den Maschinen zu verlinken. Auf diese Weise erfahren Produktentwickler Details über die Produktionsplanung oder die bereits produzierten Komponenten und deren Verfügbarkeit.

Zusätzlich können sie Kosten oder CO_2-Abdruck schon im Entwicklungsprozess berücksichtigen. Auch die Anbindung von Banken oder Versicherungen an IoT-Netzwerke wird von den Betreibern angeboten. Mit den Versicherungs- und Finanzierungskomponenten können Unternehmen ihre Lagerbestände finanzieren und ihre Supply Chain absichern.

Compliance und Prozesssicherheit

Auch die Anforderungen an die Compliance kann über die IoT-Funktionen sichergestellt werden. Mitarbeiterinnen und Mitarbeiter in den Finanzabteilungen und im Controlling sehen per Klick, welche Aufträge und Leistungen wann über das Netzwerk abgewickelt wurden. Die Finanzabteilungen erhalten Visibilität über die Einkaufs- und Lieferprozesse, in die Produktionsabläufe und Lagerbestände. Anstelle von E-Mails, die aus verschiedenen Abteilungen hin- und hergeschickt werden, sind alle Bestellungen und Rechnungen übersichtlich auf einer rundherum abgesicherten Plattform gespeichert. ❑

SCHON GEWUSST?

Durch den Aufbau einer resilienten Beschaffungsbasis mithilfe von IoT-Netzwerken profitieren Unternehmen von einer transparenten Zusammenarbeit zwischen Herstellern, Händlern und Dienstleistern wie Logistikpartnern. Unternehmen können sich vor Lieferengpässen oder sogar Ausfällen schützen und ihre Produktion am Laufen halten, ihre Lieferkette zuverlässig planen und Risiken und Chancen frühzeitig identifizieren.

KOMMENTAR

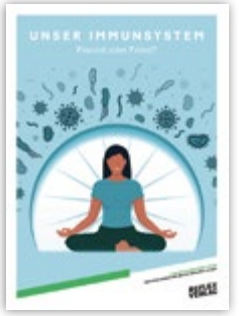
Erbschaft aus Amerika!

Ja, eine 99 Jahre alte Tante erinnert sich. Damals, sie war gerade fünf Jahre alt, hatte sie während der Wirtschaftskrise der Cousine beim Packen geholfen. Am Bahnhof der Abschied, Tränen, Umarmung, aus Bremerhaven eine letzte Lebewohl-Postkarte, wir vergessen euch nie! Dann 45 Jahre Schweigen. Es klingelt. Männer mit Cowboyhüten bringen Grüße aus Montana. Sie schauen sich im Haus um, bestaunen den Obstgarten. Noch einmal spaziert die Familie zum Bahnhofsgelände, dort wo heute der Baumarkt steht. Dann sind die Jungs auf dem Weg zurück in die Rocky Mountains. Die nächsten drei oder vier Jahre schicken sie Familiengrüße.

Ein Neffe hat in die weit verzweigte, viele Jahrhunderte alte Familie eines der Gründerväter der „Mayflower" eingeheiratet. Hochhäuser, Golfplätze, der Besitz der Familie wächst. Wie traurig, dass sie über die lange Zeit ihre Wurzeln vergessen. Weitere 45 Jahre Schweigen, Mitte Juni 2024 pingt es, die Mail eines Anwalts aus Toronto. Ein Gentleman sei verstorben, der Nachname stimme, zehn Millionen Dollar warten auf einen Erben. Also klickt man auf „Formular Download" – logisch –, und bei den Kolleginnen und Kollegen gehen Lichter aus, Bildschirme werden schwarz oder blau. Aber, denkt man sich, na ja, rund zehn Millionen Dollar Waren das Risiko wert.

Christian Raum
Chefredakteur

UNSERE NÄCHSTE AUSGABE



Unser Immunsystem
Autoimmunerkrankungen verlaufen chronisch und sind unheilbar. Was aber wäre, wenn wir gezielt auf die betroffenen Zellen und das Gewebe einwirken könnten, ohne das Immunsystem insgesamt zu schwächen? Könnten wir Autoimmunerkrankungen womöglich besser behandeln oder sogar heilen?

Erfahren Sie mehr am 22. Juli in der Frankfurter Allgemeinen Zeitung.

IMPRESSUM

Projektmanagement Moritz Duelli, moritz.duelli@reflex-media.net **Redaktion** Daniela Hoffmann, Christin Hohmeier, Christian Raum **Layout** Lydia Krüger, grafik@reflex-media.net **Fotos** iStock / Getty Images, Coverbild iStock / KanawatTH **Druck** Badische Neueste Nachrichten Badendruck GmbH **V.i.S.d.P.** Redaktionelle Inhalte Christian Raum, redaktion@reflex-media.net **Weitere Informationen** Pit Grundmann, pit.grundmann@reflex-media.net, Reflex Verlag GmbH, Hackescher Markt 2–3, D-10178 Berlin, T +49 (0)30 / 200 8949 0, www.reflex-media.net

Diese Publikation des Reflex Verlages erscheint am 26. Juni 2024 im Handelsblatt. Der Reflex Verlag und die Handelsblatt Media Group & Co. KG sind rechtlich getrennte und redaktionell unabhängige Unternehmen. Inhalte von Werbebeiträgen wie Unternehmens- und Produktporträts, Interviews, Advertorials, Anzeigen sowie Gastbeiträgen und Fokusinterviews geben die Meinung der beteiligten Unternehmen beziehungsweise Personen wieder. Die Redaktion ist für die Richtigkeit der Beiträge nicht verantwortlich. Die rechtliche Haftung liegt bei den jeweiligen Unternehmen.

JETZT SCANNEN
Unsere Ausgaben finden Sie auch auf unserem Reflex-Portal:
www.reflex-portal.de

Wir sind dabei

NETCOMM GmbH 2
Wiesentfelser Straße 1
81249 München
www.netcomm-gmbh.de
www.sicherheitsexpo.de

Sopra Steria SE 3
Hans-Henny-Jahnn-Weg 29
22085 Hamburg
barbara.korte@soprasteria.com
www.soprasteria.de

Anqa IT-Security GmbH 4
Edmund-Rumpler-Straße 5
51149 Köln
www.anqa-itsecurity.de

Opexa Advisory GmbH 5
Franz-Joseph-Straße 11
80801 München
www.opexaadvisory.de

DGC AG 6
Ballastkai 9
24937 Flensburg
www.dgc.org

Search Guard – floragunn GmbH 7
Tempelhofer Ufer 16
10963 Berlin
search-guard.com

G DATA CyberDefense AG 8
Königsalle 178 a
44799 Bochum
www.gdata.de

SECmarket GmbH 9
Elsterstraße 53
04109 Leipzig
booking.secmarket.de

MESSE ESSEN GmbH 9
Messeplatz 1
45131 Essen
www.security-essen.de/impulsgeber

Pathlock Deutschland GmbH 10
Werner-Otto-Straße 6
22179 Hamburg
www.pathlock.de

Bundesverband IT-Sicherheit e. V. 11
Chausseestraße 17
10115 Berlin
www.teletrust.de

Enginsight GmbH 12
Hans-Knöll-Straße 6
07745 Jena
www.enginsight.com

Horváth & Partner GmbH 12
Rotebühlstraße 100
70178 Stuttgart
www.horvath-partners.com/de

PASSION4IT GmbH 13
Am Regen 5
94234 Viechtach
www.passion4it.de

ads-tec Industrial IT GmbH 14
Heinrich-Hertz-Straße 1
72622 Nürtingen
www.ads-tec-iit.com

SECUINFRA GmbH 16
Stefan-Heym-Platz 1
10367 Berlin
www.secuinfra.com

Managed Detection & Response (MDR)

Made in Germany.
Für eine sichere Welt!

- Cyberangriffe erkennen und abwehren, bevor hoher Schaden entsteht
- Rund-um-die-Uhr Schutz vor Cyberbedrohungen
- Cyber Defense für alle Unternehmensgrößen

SECUINFRA
Cyber Defense. Made in Germany.

Cyber Defense • Made in Germany • 24/7 • SECUINFRA

Cyber Defense • Made in Germany • ISO 27001 certified • SECUINFRA

Vereinbaren Sie eine kostenlose Beratung durch einen unserer Cyber Defense Experten

www.secuinfra.com