HZ208310 · ISSN 1868-5757 · www.datakontext.com Dezember 6/2021

IT-SICHERHEIT

Magazin für Informationssicherheit und Datenschutz

Warum im Cyberraum ein technisches Pendant zur menschlichen Empathie nötig ist

Mit Vertrauenswürdigkeit in eine sichere Zukunft

SPECIAL
in Kooperation mit
Innovative Verwaltung:

IT-Sicherheit in der öffentlichen Verwaltung

- Welche besonderen technischen, strukturellen und regulatorischen Anforderungen für Behörden auf die IT warten – und wie sie erfolgreich gemeistert werden können
- Inklusive Marktüberblick von Anbietern und deren Lösungen

Quantencomputer:
Kommt damit das Ende der Blockchain?

Industrie und KRITIS:
IoT- und OT-Standards als Rückgrat für Cybersicherheit

Geschäftliche E-Mail-Kommunikation:
Microsoft 365 sinnvoll ergänzen

DATAKONTEXT

Aktivieren Sie Ihre menschliche Firewall!

Mit SoSafe stärken Sie Datenschutz und IT-Sicherheit im Autopiloten

Die SoSafe Awareness-Plattform integriert Datenschutz und IT-Sicherheit einfach in den Arbeitsalltag. Über ein gamifiziertes E-Learning sowie smarte Angriffssimulationen schulen Sie Ihre Mitarbeitenden nachhaltig für den Umgang mit sensiblen Daten. Prüfen Sie mit unserem strategischen Risk Monitoring außerdem, wie erfolgreich die Schulungsmaßnahmen bereits waren. So haben Sie potenzielle Risiken in Ihrer Organisation jederzeit im Blick – und schützen sich proaktiv vor kostspieligen Vorfällen.

Mehr erfahren:
www.sosafe.de

SoSafe GmbH
Ehrenfeldgürtel 76, 50823 Köln
www.sosafe.de | info@sosafe.de

SoSafe
Cyber Security Awareness

DIGITALISIERUNG – EINE FRAGE DES VERTRAUENS

Stefan Mutschler

Klingt philosophisch – hat aber einen handfesten praktischen Bezug: Vertrauen und Business werden künftig in der digitalen Welt noch stärker zusammenrücken, als das in der analogen Welt üblich war. Digitale Produkte mit fragwürdiger beziehungsweise undurchsichtiger Ausstattung in Sachen Cybersicherheit werden – zumindest im Bereich Unternehmen, KRITIS, Behörden etc. – zunehmend untragbar. Im privaten Sektor sollte wünschenswerterweise eine neue Bewusstseinsentwicklung dafür sorgen, mangelhafte Produkte nicht mehr einzusetzen. Da digitale Produkte aber die unangenehme Eigenschaft haben, immer komplexer und abstrakter zu werden, wird es für Anwender immer schwieriger bis faktisch unmöglich, jeden Sicherheitsaspekt selbst zu überprüfen. Mit welchen Folgen das verbunden ist, zeigt sich etwa an den Ergebnissen des „Online-Vertrauens-Kompass" des Bundesverbands Digitaler Wirtschaft. 46 Prozent der Befragten geben hier an: „Die schnelle Veränderung unserer Lebensbedingungen durch zunehmende Technisierung und Vernetzung macht mir Angst."

Aus diesem Grund ist es notwendig, die Digitalisierung so zu gestalten, dass diese von den Anwendern akzeptiert werden kann. Dies ist ein äußerst wichtiger Aspekt, da aus deren Sicht die Nutzung jeglicher IT-/Sicherheitslösungen theoretisch eine Risikohandlung darstellt – allein aufgrund der Tatsache, dass sie die Technologie nicht mehr komplett verstehen. Von daher sollten Unternehmen beachten, dass sie sehr präzise vorgehen müssen, um ein grundsätzliches Vertrauen in ihre Technologie aufzubauen. Was im zwischenmenschlichen Bereich durch die natürliche Fähigkeit zur Empathie läuft, muss in der Digitalisierung über ein institutionelles Vertrauensverhältnis nachgebildet werden. Wie das aussehen könnte, lesen Sie im Beitrag „Mit Vertrauenswürdigkeit in eine sichere Zukunft" ab Seite 74 in dieser Ausgabe.

Mit dem Jahr 2022 am Horizont trennen uns laut Experten nun lediglich vier Jahre von dem Zeitpunkt, an dem Quantencomputer dazu in der Lage sein könnten, Blockchain-Sicherheit zu umgehen. Ist damit das Ende der Blockchain besiegelt, bevor sie so richtig abhebt? Dieser und weiterer Fragen im Zusammenhang mit Quantencomputing und Blockchain sind wir im Gespräch mit dem Sicherheitsspezialisten William Carter nachgegangen. Die Antworten lesen Sie im Beitrag „Kommt mit dem Aufstieg der Quantencomputer das Ende der Blockchain?" ab Seite 65.

SPECIAL: ÖFFENTLICHE VERWALTUNG

Im Spannungsfeld zwischen dringendem Digitalisierungsbedarf und massiv gestiegenem Angriffsgeschehen in den Behörden müssen Behörden Sicherheit neu denken. Unser Behörden-Special in Kooperation mit der Fachzeitschrift *Innovative Verwaltung* gibt wichtige Antworten zu Gefahren, Gesetzen und aktuellen Trends und Entwicklungen im Bereich der öffentlichen Verwaltung – angereichert mit vielen praxisnahen Lösungen.

Viele Erkenntnisse bei Lesen dieser Ausgabe wünscht Ihnen

Ihr Stefan Mutschler
Chefredakteur

INHALT

KNOWBE4 SCHLIESST ÜBERNAHME VON SECURITYADVISOR AB

KnowBe4 gibt den offiziellen Abschluss der Übernahme von SecurityAdvisor bekannt. Der Kauf der Firma ermöglicht neue Fortschritte bei der Verteidigung gegen Social-Engineering-Angriffe, der Hauptverbreitungsmethode von Ransomware. SecurityAdvisor hat mehr als 50 Integrationen zu führenden Cybersecurity-Produkten, wie Crowdstrike, Zscaler, Okta, Netskope und vielen anderen, entwickelt. Sie helfen bei der Echtzeitanalyse des Benutzerverhaltens, das ein potenzielles Sicherheitsrisiko darstellt. Darüber hinaus blenden sie Mikro-Lernmodule ein, um den Benutzer – in direkter Reaktion auf sein riskantes Verhalten – aufzuklären und zu informieren. Die Kombination von KnowBe4s führender Plattform für Security Awareness Training und simulierte Phishing-Tests mit Echtzeit-Verhaltensanalyse und Micro-Learning resultiert in der Schaffung einer neuen Cybersecurity-Kategorie namens „Human Detection and Response (HDR)".

Stu Sjouwerman, CEO von KnowBe4 (Foto: KnowBe4)

„HDR stellt einen bedeutenden Fortschritt dar, wenn es darum geht, Benutzer in die Lage zu versetzen, sich gegen das ständige Problem der Social-Engineering-Angriffe zu verteidigen", sagt Stu Sjouwerman, CEO von KnowBe4. „Wir werden nun in der Lage sein, das Training und die Tests von Benutzern mit ihrem realen Verhalten zu korrelieren, um dem Security Operations Center (SOC) ein viel umfassenderes Bild der menschlichen Firewall ihres Unternehmens zu liefern. Diese Daten zum Benutzerverhalten können auch an das SOC zurückgespielt werden und Bereiche aufzeigen, in denen Lücken in der aktuellen Technologie geschlossen und die Wirksamkeit der bereits vorhandenen Produkte verbessert werden können. HDR bietet dem SOC eine völlig neue Fähigkeit, die sich in den Human Defense Layer ihrer Cyber-Architektur einfügt." ■

PALO ALTO NETWORKS UND **SIEMENS** KOOPERIEREN BEIM SCHUTZ KRITISCHER INFRASTRUKTUREN

Palo Alto Networks gab eine wichtige Erweiterung seiner Technologiepartnerschaft mit Siemens bekannt. Ziel ist es, die Sicherheit von unternehmenskritischen Netzwerken zu verbessern und die Bedrohung durch Cyberangriffe auf kritische Infrastrukturen zu verhindern. Die Unternehmen wollen virtuelle Next-Generation-Firewalls der VM-Reihe von Palo Alto Networks und Ruggedcom-Multi-Service-Plattformen von Siemens integrieren, um eine durchgängig skalierbare Hardware zu schaffen. Diese erlaubt es den Unternehmen, konsistente Sicherheitsrichtlinien und Sichtbarkeit auf IT-, kritische OT- und ICS-Infrastrukturen auszuweiten.

„Kritische Infrastrukturen, wie intelligente Umspannwerke, intelligente Transportsysteme, Verkehrssignalisierung und private Breitband-Gateways an abgelegenen Standorten, sind unglaublich schwierig gegen Cyberangriffe abzusichern. Die Systeme sind hochgradig verteilt und komplex und befinden sich oft in sehr schwierigen Umgebungen. Die Sicherung dieser Systeme ist jedoch von größter Wichtigkeit, da sie ein beliebtes Ziel für Cyberangriffe darstellen, deren Auswirkungen weit über die wirtschaftlichen Konsequenzen hinausgehen", erklärt Anand Oswal, Senior Vice President of Network Security bei Palo Alto Networks. „Durch die Kombination unserer Next-Generation-Firewall-Technologie mit der Erfahrung von Siemens im Bereich industrieller Steuerungssysteme und anspruchsvoller Umgebungen können Unternehmen ihre industriellen Steuerungssysteme und andere wichtige Infrastrukturen schützen, ohne Kompromisse bei der Sicherheit, Performance oder Skalierbarkeit einzugehen." ■

ROHDE & SCHWARZ CYBERSECURITY UND **PANASONIC** KOOPERIEREN FÜR SICHERES, MOBILES ARBEITEN

Mobiles Arbeiten ist für viele zum Berufsalltag geworden. Dabei sind tragbare Geräte ein beliebtes Angriffsziel von Cyberattacken. Rohde & Schwarz Cybersecurity und Panasonic Mobile Solutions wollen ihren Kunden zukünftig eine gemeinsame VS-NfD-zugelassene Sicherheitslösung für mobiles Arbeiten anbieten. Panasonic Mobile Solutions liefert unter der Marke TOUGHBOOK ausfallsichere IT-Lösungen mit robuster Hardware und Services. Rohde & Schwarz Cybersecurity ergänzt diese mit umfassender, proaktiver IT-Sicherheit – bestehend aus einem hochsicheren Browser, einem softwarebasierten VPN-Client sowie einer Festplattenverschlüsselung.

Die mobilen IT-Lösungen von Panasonic Mobile Solutions basieren auf widerstandsfähigen Notebooks, 2-in-1 Hybridgeräten, Tablets sowie Handhelds und werden explizit für IT-widrige Arbeitsumfelder sowie den strapazierenden 24/7-Dauereinsatz entwickelt. (Foto: Panasonic Connect)

Die mobilen IT-Lösungen von Panasonic Mobile Solutions basieren auf widerstandsfähigen Notebooks, 2-in-1 Hybridgeräten, Tablets sowie Handhelds und werden explizit für IT-widrige Arbeitsumfelder sowie den strapazierenden 24/7-Dauereinsatz entwickelt. Der softwarebasierte R&STrusted VPN Client schützt die Netzwerkkommunikation einer Client-Plattform (Windows-Laptop, -Tablet) mit einem Behörden- oder Unternehmensnetzwerk über ein nicht vertrauenswürdiges Netzwerk, wie zum Beispiel das Internet. Hierbei wurde eine Zero-Trust-Architektur gegenüber dem Betriebssystem umgesetzt, um Risiken aufgrund möglicher

Betriebssystem-Exploits auszuschließen. Für zusätzliche Sicherheit sorgt der „Always On"-Modus: Die Nutzer befinden sich zu keinem Zeitpunkt ungeschützt in einem nicht vertrauenswürdigen Netzwerk. Die Festplattenverschlüsselung R&STrusted Disk schützt sensible Daten mit einer sicheren und transparenten Verschlüsselung in Echtzeit ohne Produktivitätseinschränkung sogar im Fall von Verlust oder Diebstahl vor unbefugtem Zugriff – selbst auf USB-Datenträgern. Und die virtuelle Umgebung zum sicheren Surfen im Web, R&S Browser in the Box, bietet im Zusammenspiel mit R&S Trusted VPN Client und R&S Trusted Disk ein zusätzliches Sicherungssystem für einen hochsicheren, mobilen Arbeitsplatz.

„Die IT-Sicherheit von mobilen Endgeräten ist in vielerlei Hinsicht ein essenzieller Aspekt des Arbeitens von unterwegs", betont Timo Unger, Country Manager CEE bei Panasonic Mobile Solutions. „So sind nicht nur sensible Branchen, wie Polizei- und Sicherheitsdienste, Gesundheitswesen und die Energiewirtschaft, auf die Sicherheit für mobile Endgeräte angewiesen. Mit Rohde & Schwarz Cybersecurity haben wir einen idealen Partner an unserer Seite, um unsere robusten und dadurch ausfallsicheren mobilen Endgeräte kombiniert mit einem proaktiven IT-Sicherheitspaket aus einer Hand anbieten zu können." ■

KONICA MINOLTA UND **TENFOLD SOFTWARE** GEBEN STRATEGISCHE PARTNERSCHAFT BEKANNT

Konica Minolta Business Solutions hilft Unternehmen durch die Auswahl geeigneter IT-Produkte dabei, die Vorteile der Digitalisierung für sich zu nutzen. Um die Zugriffsrechte von Mitarbeitenden auch am vernetzten Arbeitsplatz sicher und effizient zu steuern, ist eine passende Plattform für die Verwaltung von Benutzerkonten und Berechtigungen notwendig. Als Experte für Identity und Access Management (IAM) unterstützt tenfold Software Kunden von Konica Minolta künftig bei der Umsetzung einer sicheren IT-Umgebung.

Die richtige Konfiguration der Zugriffsrechte ist für die Sicherheit des Firmennetzwerks und den Erfolg einer modernen Arbeitsumgebung entscheidend. Für IT-Administratoren sind die dafür notwendigen Prozesse jedoch mit erheblichem Aufwand verbunden: Sämtliche Benutzerkonten müssen händisch angelegt und laufend angepasst werden. Dieses Problem beschäftigt viele Unternehmen. Mithilfe von tenfold Access Management können Kunden von Konica Minolta die Berechtigungsverwaltung in Zukunft weitgehend automatisieren. Mit seiner schnellen Installation und zahlreichen vorgefertigten Schnittstellen hat sich tenfold besonders auf IAM für mittelständische Organisationen spezialisiert.

Den Bedarf für IAM-Software kennt Konica Minolta nur zu gut. „Wir sehen immer wieder, wie viel Zeit Unternehmen in die manuelle Verwaltung von Benutzerkonten und Zugriffsrechten investieren, und welche Sicherheitslücken dabei entstehen," so Bernd Goger, Director Business Unit ITS bei der Konica Minolta Business Solutions Deutschland GmbH. „Mit tenfold können wir unseren Kunden eine effiziente Lösung anbieten, die nicht nur zum Schutz vor Datenlecks und Cyberangriffen beiträgt, sondern auch eine Zeitersparnis für die zuständigen Fachkräfte bedeutet." ■

TENABLE UND **SPLUNK** SICHERN ACTIVE DIRECTORY UND KONVERGIERTE IT/OT-UMGEBUNGEN

Tenable hat eine Erweiterung seiner globalen strategischen Partnerschaft mit Splunk bekannt gegeben. Ziel ist es, Active Directory und konvergierte Operational-Technology-(OT-)Umgebungen zu sichern. Die neu veröffentlichten und aktualisierten Integrationen für Tenable.ad und Tenable.ot sollen es den gemeinsamen Kunden ermöglichen, Sicherheitsschwachstellen in ihren wichtigsten und wertvollsten Systemen zu identifizieren und zu beheben.

Ray Komar, Vice President of Technical Alliances bei Tenable (Foto: Tenable)

„Angesichts der größten Cyberangriffe der vergangenen zwölf Monate wird klar, dass die Angreifer auf kritische Infrastrukturen und Active Directory abzielen. Daher kommt es auf die Fähigkeit an, die Schwachstellen, die Angreifer am ehesten ausnutzen, schnell zu identifizieren und zu verstehen und sie umgehend zu beheben. Genau das ist es, was zwischen der Verteidigung eines Unternehmens und einem erfolgreichen Angriff steht", erklärt Ray Komar, Vice President of Technical Alliances bei Tenable. „Mit unseren neuen Splunk-Integrationen bauen wir auf unsere strategische Partnerschaft auf, indem wir eine einheitliche Ansicht zum Erkennen potenzieller Bedrohungen in OT-Umgebungen und Active Directory bereitstellen. Diese ermöglicht es Sicherheitsteams, stets einen Schritt voraus zu sein." ■

DEAL FÜR NO-CODE-IDENTITÄTS-SICHERHEIT

Ping Identity übernimmt mit Singular Key einen Anbieter von No-Code-Identität und Sicherheitsorchestrierung. Das US-Start-up für End-to-End-Security optimiert die Integration von Identitätsdiensten und bietet ein No-Code-Tool, mit dem sich Workflows über mehrere Identitätstechnologien und -plattformen hinweg erstellen lassen. Identitätsüberprüfung, Fraud-, Risiko- und Zugriffsmanagement, Autorisierung, privilegierte Zugangsmöglichkeiten sowie Identitäts-Governance werden dabei in einer einheitlichen Identitätsstruktur verwaltet.

Unternehmen sollen mithilfe von Identitätsorchestrierung auf einfache Weise dynamische User Journeys erstellen und über sämtliche Entwicklungen des Identitäts- und Zugriffsmanagements hinweg verwalten können. Der intelligente Security-Layer-Ansatz von Singular Key sorgt dabei für mehr Agilität und Flexibilität in Unternehmensprozessen, da Identitäts-Workflows vereinfacht werden und schnell und ohne Codierung bereitgestellt werden können. Singular Key soll über die PingOne Cloud-Plattform zur Verfügung gestellt werden und bestehende Kunden sowie Neuanwender dabei unterstützen, ihre End-to-End User Journeys sowohl über die Systeme von Ping Identity als auch über Dienste von Drittanbietern hinweg zu verbessern. ■

DATENSCHUTZLÖSUNG MIT „OHR“ FÜR PANDEMIEBEZOGENE CYBER-SICHERHEITSPROBLEME

WALLIX bringt WALLIX Bastion 9 auf den Markt, die neue Version des Flaggschiffs der Privileged-Access-Management-(PAM-)Lösung. Die Pandemie hat den weltweiten digitalen Wandel vorangetrieben und durch die Umstellung auf Remote-Arbeit, die Nutzung von Cloud-Diensten, Telemedizin, Fernunterricht und vieles mehr auch zu einer Zunahme mobiler Geräte im Netzwerk geführt. All diese potenziellen Zugangspunkte für Hacker müssen gesichert werden, um die Daten zu schützen. Bastion 9 erweitert den bestehenden Funktionsumfang der Suite durch:

- einen sicheren Fernzugriff auf die IT-Infrastruktur des Unternehmens,
- sichere Verwaltung und Überwachung aller IT-Aktivitäten,
- höhere Sicherheit vor Cyberangriffen auf das Active Directory oder Cloud-Zugänge,
- schnellere Reaktionszeiten im Falle eines Angriffs.

WALLIX Bastion schützt Passwörter für privilegierte Konten, indem es sie in einem Passwort-Tresor speichert, die Aktivitäten von Benutzern mit diesen privilegierten Konten überwacht und ihren Zugang im Fall eines vermuteten Identitätsdiebstahls sperrt. Darüber hinaus ermöglicht Bastion die Einhaltung der Datenschutzbestimmungen (DS-GVO). Bastion 9 ist eine noch robustere Lösung, die das Cybersicherheitsniveau von Kunden drastisch verbessern und aktuelle Herausforderungen wirksam angehen soll. ■

„DIE GRÖSSTE PLATTFORM-EVOLUTION DER UNTERNEHMENSGESCHICHTE“ KONSOLIDIERT CLOUD-, VIRTUAL-APPLIANCE- UND HARDWARE-PORTFOLIO

SonicWall gab die neuesten Ergänzungen für sein Cybersecurity-Portfolio der siebten Generation bekannt, die größten in seiner 30-jährigen Unternehmensgeschichte. So bündelt SonicWall Cloud-, Virtual-Appliance- und Hardware-Produkte in einer einzigen, voll integrierten und cloudbasierten Plattform. Mit seinen drei neuen Firewall-Modellen – NSa 5700, NSsp 10700 und NSsp 11700 – will das Unternehmen nun die größten und komplexesten Unternehmen, Behörden und MSSPs vor hoch entwickelten Cyberbedrohungen, wie Ransomware und brandneuen Malware-Varianten, schützen, ohne dabei Abstriche bei der Netzwerk-Performance zu machen.

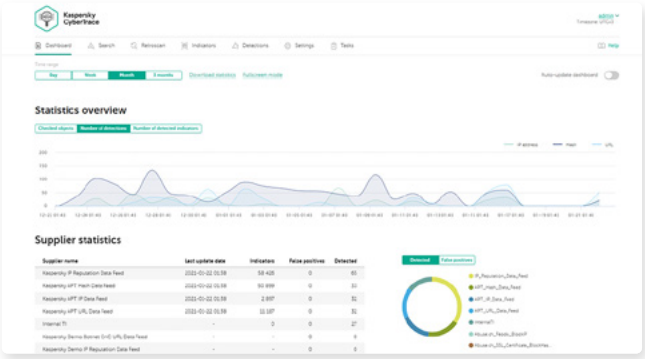
Die modernen, hoch entwickelten Cybersecurity-Produkte des Unternehmens kommen zum richtigen Zeitpunkt auf den Markt. SonicWall Capture Labs verzeichnete im dritten Quartal 2021 einen Anstieg der globalen Ransomware-Attacken um 148 Prozent. Angesichts der 495 Millionen Ransomware-Angriffe, die das Unternehmen dieses Jahr bisher meldete, wird 2021 das bis dato kostspieligste und gefährlichste Jahr sein. ■

ZENTRALISIERTE PLATTFORM FÜR THREAT-INTELLIGENCE-MANAGEMENT

Mehrere Quellen für Bedrohungsdaten verarbeiten ständig riesige Mengen an Informationen und erzeugen Millionen von Warnmeldungen. Diese fragmentierten und unterschiedlich formatierten Daten erschweren die effektive Priorisierung, Einteilung und Validierung von Warnmeldungen und stellen für IT-Sicherheitsteams eine Herausforderung dar. Um die Sicherheits- und Reaktionsteams in Unternehmen bei der Erkennung, Untersuchung und Bekämpfung von Bedrohungen zu unterstützen und die Effizienz der IT-Sicherheitsabläufe zu steigern, hat Kaspersky sein Threat-Intelligence-Fusion- und Analyse-Tool Kaspersky CyberTrace zu einer zentralen Threat-Intelligence-Plattform ausgebaut.

Die Lösung wurde um fortschrittliche Funktionen erweitert, mit denen Sicherheitsteams komplexe Suchvorgänge über alle Indikatorenfelder hinweg durchführen, Observiertes von zuvor geprüften Ereignissen analysieren, die Effektivität integrierter Feeds messen und eine Feed-Schnittstellenmatrix erstellen können. Außerdem bietet sie eine öffentliche API für die Integration automatisierter Arbeitsabläufe. Darüber hinaus stellt die Plattform nun Multi-User- und Multi-Tenancy-Funktionen bereit, um Vorgänge zu steuern, die von verschiedenen Nutzern verwaltet werden, und Ereignisse aus verschiedenen Zweigen getrennt zu behandeln. Die kostenpflichtige Version, die für große Unternehmen und Managed Security Service Provider geeignet ist, unterstützt alle Funktionen und ermöglicht die Verarbeitung und das Herunterladen einer unbegrenzten Anzahl von Indicators of Compromise (IoC). Sie lässt sich mit allen gängigen Security-Information-and-Event-Management-(SIEM-)Lösungen und Sicherheitskontrollen integrieren und bietet eine grafische Visualisierung für eine effiziente Reaktion.

Die Community-Version von Kaspersky CyberTrace ist weiterhin kostenfrei erhältlich. Auch sie bietet die neuen Funktionen, mit Ausnahme der Möglichkeit, Mehrnutzer- und Mehrmandantenkonten hinzuzufügen. Des Weiteren ist die Anzahl der verarbeiteten Ereignisse pro Sekunde (bis zu 250) und die Anzahl der Indikatoren, die heruntergeladen werden können (bis zu einer Million), eingeschränkt. ■



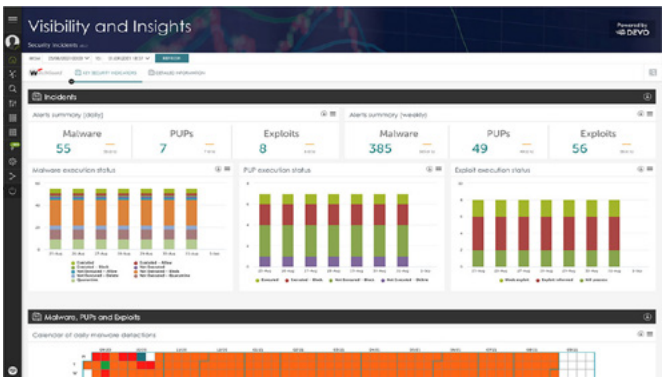
Ein in CyberTrace eingebauter Mechanismus für den Abgleich und die Analyse eingehender Daten ermöglicht die effektive Erkennung selbst verschleierter Bedrohungsindikatoren. (Quelle: Kaspersky)

CLOUD-PLATTFORM MIT ZUSÄTZLICHEN ENDPOINT-SECURITY-FUNKTIONALITÄTEN

Die Vision zur Etablierung einer zentralen IT-Security-Plattform wird von WatchGuard Technologies massiv vorangetrieben. Gerade wurden vier weitere Endpoint-Security-Leistungsbausteine in WatchGuard Cloud eingebunden. Jetzt stehen Anwendern und Partnern auch die Funktionen „WatchGuard Patch Management", „WatchGuard Full Encryption", „WatchGuard Advanced Reporting Tool (ART)" und „WatchGuard Data Control" zur Verfügung. Damit bietet der IT-Security-Spezialist Kunden und Partnern zentralen Zugang für weitreichende Sicherheitslösungen, die vom umfassenden Endpoint-Schutz über Netzwerksicherheit und Multi-Faktor-Authentifizierung bis hin zum sicheren WLAN reichen.

Vor allem MSPs sollen im Tagesgeschäft maßgeblich von der zentralen und einheitlichen Verwaltung unterschiedlichster IT-Security-Lösungen sowie den zusätzlichen Cross- und Upselling-Möglichkeiten profitieren. Partner seien in der Lage, ihre IT-Security-Dienstleistungen effektiv aufzugleisen und würden auf Kundenseite mit erhöhtem, maßgeschneidertem Schutz punkten, der sich zudem flexibel und einfach an neue Anforderungen anpassen ließe. Durch das verbesserte Zusammenspiel aller Leistungsbausteine für Endpoint Security – bereits vorher integriert waren WatchGuard EPP (Endpoint Protection Platform), WatchGuard EDR (Endpoint Detection and Response) und WatchGuard EPDR (Endpoint Protection Detection and Response) – ergibt sich ein noch lückenloserer Schutz bei gleichzeitig hoher betrieblicher Effizienz.

Das Advanced Reporting Tool (ART) etwa liefert detaillierte Informationen über den täglichen Betrieb von Anwendungen und Netzwerken sowie zu den Benutzern. Dies umfasst vordefinierte Abfragen, Dashboards und Warnmeldungen zu Endpunkten. Zudem können Administratoren spezifische Abfragen und Warnungen auf Basis der Telemetriedaten zu Endgeräten erstellen. Data Control beispielsweise dient der Aufdeckung, Prüfung und Überwachung unterschiedlichster, unstrukturierter sensibler oder personenbezogener Daten auf Endgeräten. Dies beinhaltet nicht zuletzt benutzerdefinierte Echtzeit-Suchen, um Dateien innerhalb eines bestimmten Kontexts zu finden. Inklusive aller neuer Tools bietet WatchGuard Cloud jetzt umfassende „Protection, Detection und Response"-Funktionalitäten für Netzwerke mit zehntausenden Endgeräten – inklusive Erweiterungsoptionen für Threat Hunting und Zero Trust Application Services. All diese Möglichkeiten stehen über eine zentrale Oberfläche zur Verfügung. ■

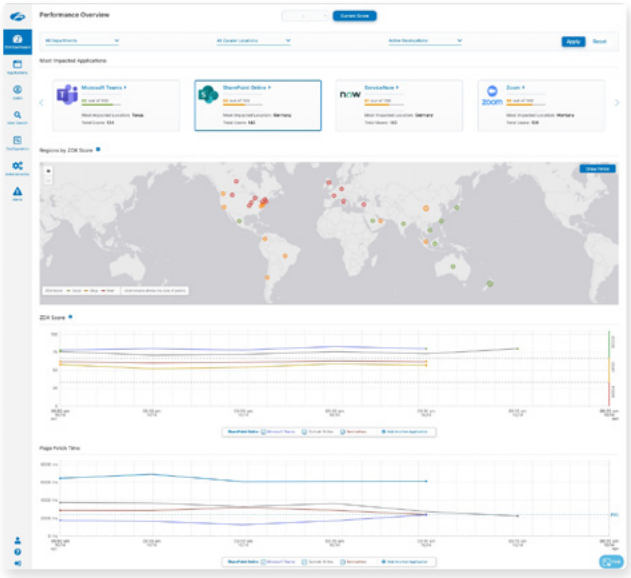


Das WatchGuard Advanced Reporting Tool generiert Sicherheitsinformationen in Echtzeit, indem es tiefe Einblicke in Anwendungen, Netzwerk und die täglichen Vorgänge und Aktionen der Benutzer liefert. (Quelle: WatchGuard)

DIGITAL EXPERIENCE MONITORING FÜR UNIFIED COLLABORATION-PLATTFORMEN

Zscaler erweitert seine Digital Experience (ZDX) um neue Integrationen für Unified Communications as a Service (UCaaS) und digitale Workflow-Plattformen, um Leistungsprobleme automatisch zu erkennen und schnell zu beheben und so die Produktivität von Mitarbeitern zu verbessern. ZDX wird als integrierter Service auf der cloudnativen Zero Trust Exchange-Plattform von Zscaler bereitgestellt. Der Service bietet einen einheitlichen Einblick in Benutzer-, Verbindungs- und Cloud-App-Telemetriedaten, um Verbindungsprobleme zu isolieren und zu beheben. Dank des erweiterten Funktionsumfangs können Sicherheits-, Netzwerk- und Helpdesk-Teams jetzt zusammenarbeiten, um Microsoft Teams- und Zoom-Qualitätsprobleme effizient zu lösen, Reaktionszeiten zu verkürzen und die Mitarbeiterproduktivität zu optimieren. Im Einzelnen bieten die Erweiterungen:

- neue Sichtbarkeit und Verwaltung der UCaaS-Leistung,
- erweiterte Tools zur Fehlerbehebung,
- verbesserte Microsoft 365-Unterstützung,
- umfangreichen Einblick in Zero Trust Secured Private Apps und
- automatisiertes IT Incident Management mit ServiceNow.



Ein zentrales ZDX Dashboard zeigt alle relevanten Telemetriedaten zur Fehlerbehebung und Lösung von Problemen mit privaten Anwendungen. (Quelle: Zscaler)

MIT **API-SCANNING** GEGEN DEN BALD WICHTIGSTEN CYBERANGRIFFSVEKTOR

Veracode hat ein neues Scanning-Tool vorgestellt, mit dem Unternehmen Schwachstellen in ihren APIs (Application Programming Interfaces) finden und beheben können – eine der am schnellsten wachsenden Angriffsflächen für Cyberkriminelle. Die neue Funktion nutzt Veracodes Scanning-Technologie für Dynamic Analysis (DAST), um verlässliche Informationen und Lösungsansätze über API-Schwachstellen schnell und effizient zu präsentieren.

Viele Unternehmen durchleben aufgrund der COVID-19-Pandemie eine Beschleunigung ihrer digitalen Transformation – APIs werden damit kritischer denn je für moderne Anwendungen. Sie erlauben eine einfache Datenübertragung zwischen verschiedenen Produkten oder Diensten und machen Informationen so über viele Systeme verfügbar. Gleichzeit sind sie aber auch ein attraktiver Angriffsvektor für Cyberkriminelle. Laut Gartner wird „API-Missbrauch bis 2022 von einem seltenen zu einem der häufigsten Angriffsvektoren", was mit Sicherheit zu einem Anstieg der Datenvorfälle in Unternehmens-Webanwendungen führt. ■

INTEGRIERTE SICHERHEITSLÖSUNG

Avast bringt mit Avast One eine neue integrierte Lösung auf den Markt, die Sicherheit, Privatsphäreschutz und Leistungsoptimierung in einem bietet – personalisiert und plattformübergreifend. Nutzer müssen mit Avast One nicht mehr auf unterschiedliche Produkte setzen, um für ihre digitale Sicherheit zu sorgen. Avast One schützt die Privatsphäre seiner Nutzer, stellt sichere Verbindungen her, beschleunigt die Leistung der Geräte und bewahrt sie vor Malware. Bereits seit 20 Jahren stellt Avast sein Flaggschiffprodukt Avast Free Antivirus kostenlos zur Verfügung. Mit Avast One Essential definiert das Unternehmen kostenfreie digitale Sicherheit nun neu, um den Bedürfnissen der heutigen Online-Konsumenten gerecht zu werden, die sich neben Sicherheit auch die Wahrung ihrer Privatsphäre wünschen. Kostenpflichtige Versionen für mehrere Benutzer sind ebenfalls erhältlich. Avast One ist ab sofort als Download für Android, iOS, Mac und Windows verfügbar. ■

KAMPF GEGEN **VERSTECKTE DDOS FLOODS**

Mit Quantiles DoS Protection ermöglicht Radware die zuverlässige Erkennung und Blockierung von DDoS-Attacken, die sich gegen spezifische Kunden von Providern und Carriern richten. Solche Phantom Floods werden von vielen Lösungen nicht erkannt, weil sie in Netzwerken mit hoher Bandbreite nicht auffällig sind. Quantiles DoS Protection ist eine Erweiterung von Radwares DDoS-Lösung DefensePro und ermöglicht es Service Providern und Carriern, Phantom-Flood-Angriffe und Verkehrsanomalien, die bisher unentdeckt blieben, automatisch zu entschärfen.

Unter Verwendung innovativer Quantiles DoS-Algorithmen von Radware unterteilt die Lösung den eingehenden Datenverkehr automatisch in Segmente oder Quantiles. Mit dieser neuen granularen Erkennungsstufe können Service Provider und Carrier DDoS-Floods erkennen und stoppen, die im Verhältnis zur gesamten Bandbreite des Providers ein geringes Volumen aufweisen, die Anbindung einzelner Kunden oder Services aber sättigen können. Für Unternehmen entfällt durch diese automatisierte Funktion der kostspielige und komplexe Prozess der umfangreichen manuellen Konfiguration und laufenden Schwellenwertanpassung. ■

Quantiles DoS Protection ist eine Erweiterung von Radwares DDoS-Lösung DefensePro. (Foto: Radware)

Setzen Sie Anforderungen der DSGVO, Orientierungshilfen der DSK, verschiedene ISO-Normen sowie weitere relevante Datenschutz- und Sicheheitsbestimmungen bequem in einer Plattform um

- Verarbeitungsverzeichnis
- Benchmarking
- Bewertungsautomatisierung
- Lieferantenrisikomanagement
- Vorfallreaktion
- Data Discovery
- DataGuidance Datenschutzportal
- Einwilligungen & Präferenzen
- Reifegrad und Planung

Jetzt Demo anfordern:

www.onetrust.de/demo/

OneTrust

PRIVACY, SECURITY & GOVERNANCE

BSI-Lagebericht 2021 und NIS 2

WARUM DIE BEDROHUNGSLAGE IN DEUTSCHLAND IMMER KRITISCHER WIRD

Cyberangriffe führen zu schwerwiegenden IT-Ausfällen in Kommunen, Krankenhäusern und Unternehmen. Sie verursachen zum Teil erheblichen wirtschaftlichen Schaden und bedrohen existenzgefährdend Produktionsprozesse, Dienstleistungsangebote und Kunden. „Informationssicherheit muss einen deutlich höheren Stellenwert einnehmen und zur Grundlage aller Digitalisierungsprojekte werden", heißt es im Bericht. Doch nicht alle Neuerungen an der europäischen NIS-Richtlinie folgen diesem Anspruch.

Der am 21. Oktober 2021 vorgestellte neue Lagebericht zur Lage der IT-Sicherheit in Deutschland des Bundesamts für Sicherheit in der Informationstechnik (BSI) [1] macht deutlich: Die erfolgreiche Digitalisierung ist aufgrund der zunehmenden Vernetzung, einer Vielzahl gravierender Schwachstellen in IT-Produkten sowie der Weiterentwicklung und Professionalisierung von Angriffsmethoden zunehmend gefährdet. Horst Seehofer, zu dieser Zeit noch Bundesminister des Innern, für Bau und Heimat urteilt: „Die Gefährdungslage im Cyberraum ist hoch. Wir müssen davon ausgehen, dass dies dauerhaft so bleibt oder sogar zunehmen wird. Wir haben die letzten Jahre deshalb genutzt, um die Cybersicherheit in unserem Land massiv zu stärken. Wir haben das BSI mit über 700 neuen Stellen in dieser Legislaturperiode fast verdoppelt. Mit seiner Arbeit sorgt das BSI dafür, dass die IT-Sicherheit ein Wettbewerbsvorteil für Deutschland wird." BSI-Präsident Arne Schönbohm legt bei der Drohkulisse noch einen drauf: „Im Bereich der Informationssicherheit haben wir – zumindest in Teilbereichen – Alarmstufe Rot. Der neue Lagebericht des BSI zeigt deutlich wie nie: Informationssicherheit

ist die Voraussetzung für eine erfolgreiche und nachhaltige Digitalisierung."

Am Beispiel von erfolgreichen Ransomware-Angriffen wird deutlich, wie extrem sich mangelnde Informationssicherheit auswirken kann: So musste sich ein Krankenhaus für 13 Tage von der Notfallversorgung abmelden. Immer öfter sind auch ganze Lieferketten von derartigen Angriffen beeinträchtigt, mit Folgen nicht nur für die Opfer, sondern auch für deren Kunden oder für andere unbeteiligte Dritte.

Das BSI beobachtet zudem die Weiterentwicklung von kriminellen Methoden. So wird bei Ransomware-Angriffen neben der Forderung nach einem Lösegeld immer öfter auch damit gedroht, zuvor gestohlene Daten zu veröffentlichen. Mit dieser Schweigegelderpressung erhöhen Cyberkriminelle den Druck auf Betroffene. Auch DDoS-Angriffe haben im Berichtszeitraum deutlich zugenommen. Sie werden dazu eingesetzt, digital Schutzgeld zu erpressen.

Im Februar 2021 hat das BSI den höchsten jemals gemessenen Wert an neuen Schadprogramm-Varianten notiert. Pro Tag kamen durchschnittlich 553.000 neue Varianten hinzu. Insgesamt wurden im Berichtszeitraum 144 Millionen neue Schadprogramm-Varianten gezählt, ein Plus von 22 Prozent gegenüber dem Vorjahreszeitraum.

Auch die Qualität und die Verbreitung vieler gravierender Schwachstellen in IT-Produkten gibt Anlass zur Sorge. So wurde eine gravierende Schwachstelle in Microsoft-Exchange auf 98 Prozent aller geprüften Systeme festgestellt. Das BSI hatte darauf mit einer Warnung der Stufe Rot reagiert und öffentlich und gezielt die Betroffenen zum Handeln aufgerufen.

Als Konsequenz aus der Bedrohungslage fordert das BSI, der Informationssicherheit einen höheren Stellenwert beizumessen. Im Rahmen von Digitalisierungsprojekten sollte die Cybersicherheit fest verankert werden sowie die gesamte Lieferkette umfassen.

„Cyberangriffe sind zu einer enormen Bedrohung für die deutsche Wirtschaft geworden", bestätigt Susanne Dehmel, Mitglied der Bitkom-Geschäftsleitung, die Kernaussagen des BSI-Lageberichts. „Jedes zehnte Unternehmen sieht deshalb laut unseren Erkenntnissen seine Existenz bedroht. Der diesjährige Lagebericht des Bundesamts für Sicherheit in der Informationstechnik untermauert eindrucksvoll, wie ernst die Lage für die deutsche Wirtschaft, aber auch für Privatpersonen, Behörden und andere Institutionen ist."

Susanne Dehmel, Mitglied der Bitkom-Geschäftsleitung (Foto: Bitkom)

Cyberangriffe haben laut Bitkom-Studien bei 86 Prozent der Unternehmen in Deutschland zuletzt einen Schaden verursacht. „Die Wucht, mit der insbesondere Ransomware-Angriffe unsere Wirtschaft erschüttern, ist besorgniserregend und trifft Betriebe aller Branchen und Größen", so Dehmel. „Die Schäden durch Erpressung, verbunden mit dem Ausfall von Systemen oder der Störung von Betriebsabläufen, sind seit 2019 um 358 Prozent gestiegen."

Auch bei der Schutzgelderpressung im Internet sieht Dehmel wachsendes Unheil: „Die Angreifer drohen damit, bestimmte Ressourcen gezielt zu überlasten und zum Beispiel Server mit massenhaften Anfragen in die Knie zu zwingen. Zuletzt waren 27 Prozent der Unternehmen im Land von solchen DDoS-Attacken betroffen.

Als notwendige Reaktion darauf schlägt Dehmel die Möglichkeit vor, „dass sich jeder Mensch und jedes Unternehmen in Echtzeit über die Cyberbedrohungslage informieren kann. Dazu müssen wir Echtzeit-Informationen nutzen und EU-weit in einem zentralen Dashboard sammeln – ähnlich dem Corona-Dashboard des Robert-Koch-Instituts. Nur wenn Hinweise auf Gefahren sekundengenau gesammelt werden, können wir auch umgehend darauf reagieren und uns sowie unsere Wirtschaft besser schützen." Zudem befürwortet Dehmel, Cybersicherheit stärker in die Bildung aller Menschen zu integrieren und Informatik als Pflichtfach ab Sekundarstufe I einzuführen.

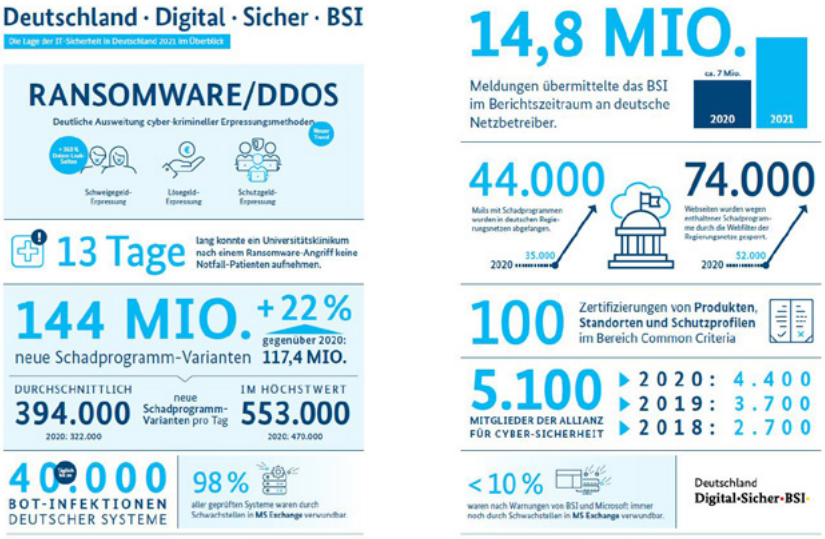
Ähnlich sieht es auch Prof. Norbert Pohlmann, Vorstand IT-Sicherheit im eco – Verband der Internetwirtschaft e. V.: „Aus der Einschätzung des BSI kann nur eines folgen: Wir müssen als Gesellschaft insgesamt die IT-Sicherheit stärken! Sowohl Privatwirtschaft als auch öffentliche Hand müssen noch intensiver als bisher IT-Sicherheit höchste Priorität einräumen und jederzeit in allen IT-Projekten mitdenken. Die neue Bundesregierung muss einen besonderen Schwerpunkt auf IT-Sicherheit setzen, damit die Digitalisierung gelingen kann." Der Lagebericht des BSI gibt einen Überblick über die Entwicklung der Bedrohungslage im Cyberraum vom 1. Juni 2020 bis zum 31. Mai 2021 und über die Aktivitäten und Gegenmaßnahmen des BSI.

Prof. Norbert Pohlmann, Vorstand IT-Sicherheit im eco – Verband der Internetwirtschaft e. V. (Foto: eco)

DIE EUROPA-EBENE: NIS 2 TEILWEISE KONTRAPRODUKTIV

Cybersicherheit ist seit 2016 eine der Prioritäten der Europäischen Kommission. In diesem Jahr trat die Richtlinie über Netz- und Informationssysteme (NIS), das erste europäische Cybersicherheitsgesetz, in Kraft und sorgt seitdem dafür, dass die regulatorischen Anforderungen an die Cybersicherheit in den Mitgliedstaaten abgestimmt werden. Immerhin setzt Europa mit diesen gemeinsamen Cybersicherheitsregeln der Wettbewerbsverzerrung zwischen den europäischen Ländern für Sicherheitslösungen, die nicht das gleiche Qualitätsniveau haben, ein Ende.

Doch auch wenn die NIS-Richtlinie ein Schritt in die richtige Richtung ist, so ist sie doch kein sehr restriktiver Rahmen und reicht sicher nicht aus, um der globalen Cyberbedrohung zu begegnen. Wie es gelingen kann, die Forderungen des BSI zu erfüllen, warum Frankreich ein Vorbild für Europa sein kann und warum die letzte Justierung



Zahlen und Fakten aus dem aktuellen Bericht zur Lage der IT-Sicherheit in Deutschland 2021 des BSI. (Quelle: BSI)

an der NIS-Richtlinie, NIS 2, ein Rückschritt für die Cybersicherheit der EU ist, erläutert Guillaume Vassault-Houlière, CEO und Mitgründer von YesWeHack:

Guillaume Vassault-Houlière, CEO und Mitgründer von YesWeHack (Foto: YesWeHack)

„Die aktuelle Cyberstrategie der EU ist ein Echo auf die wegweisenden Maßnahmen, die in Frankreich bereits seit zehn Jahren bestehen und sich dort bewährt haben. Mit der Gründung der nationalen Agentur für die Sicherheit von Informationssystemen (Agence nationale de la sécurité des systèmes d'information; ANSSI) im Jahr 2009 und der Aufnahme spezifischer Cybersicherheitsanforderungen in sein Militärisches Programmgesetz (LPM) ab 2013 hat Frankreich seinen Unternehmen und Institutionen einen kompetenteren Umgang mit Cyberrisiken ermöglicht. Beide Initiativen haben eine Reihe von Anforderungen hervorgebracht, die sich hauptsächlich auf die Zertifizierung von Cybersicherheitsprodukten und -dienstleistungen, sowie die kontinuierliche Überwachung von Informationssystemen konzentrieren. Aus diesem Grund ist Frankreich heute eines der Länder, die am besten auf Cyberbedrohungen vorbereitet sind.

Eine kontinuierliche Kontrolle der Informationssysteme durch Sicherheitsaudits, Pentests oder Bug Bounty sind nur einige Möglichkeiten, Anwendungen und Onlineservices zu testen, bevor es zu einem Angriff kommt. Die Einführung einer Politik der koordinierten Offenlegung von Schwachstellen (Coordinated Vulnerability Disclosure – CVD) ist ebenfalls ein Schlüsselelement zur Begrenzung des Cyberrisikos, das sich im französischen Ökosystem bewährt hat. Ein solches Programm besteht darin, Unternehmen zu ermutigen, die Zusammenarbeit mit ethischen Hackern zu fördern, indem sie ihnen einen vertrauenswürdigen Kanal zur Verfügung stellen, über den die Hacker Schwachstellen melden können.

Darüber hinaus sind weitere Maßnahmen zum Schutz vor Cyberangriffen denkbar. Öffentliche Einrichtungen und Unternehmen könnten zum Beispiel verpflichtet werden, eine VDP (Vulnerability Disclosure Policy) für die auf ihrer Plattform verkauften Produkte oder Dienstleistungen anzubieten. Oder man könnte zumindest den Nachweis verlangen, dass die Cybersicherheit bei der Konzeption eines Produkts oder Dienstes vom Hersteller oder Anbieter berücksichtigt wurde. Die Stärkung der Cybersicherheit europäischer Unternehmen und Institutionen könnte auch durch die Konsolidierung der von Softwareherstellern geforderten Auflagen erreicht werden. Es gibt also unzählige Beispiele und Instrumente zum Schutz von Organisationen vor Cyberangriffen.

NIS-2-RICHTLINIE IST EIN RÜCKSCHRITT FÜR DIE CYBERSICHERHEIT

Die jüngsten Vorschläge für die NIS-2-Richtlinie, die im Groothuis-Bericht skizziert werden, senken jedoch die Anforderungen an den Cyberschutz. Von besonderem Interesse ist dabei, dass die Verpflichtung für Anbieter, zertifizierte Produkte und Dienstleistungen zu verwenden, gelockert wurde. Außerdem wird die Häufigkeit der Audits von Informationssystemen auf maximal einmal im Jahr festgelegt. Generell ist der Anreiz für die Mitgliedstaaten, eine dem Stand der Technik entsprechende Cybersicherheitsstrategie zu formulieren, stark herabgesetzt. Gleichzeitig lehnt sich der US-amerikanische Cybererlass vom 12. Mai 2021 [2] sehr deutlich an das französische Regelwerk an. Es besteht also eine gewisse Dissonanz zwischen der US-Strategie, die sich an dem anspruchsvollen französischen Cybermodell orientiert, und einer Nivellierung der Maßnahmen, die derzeit für die europäische NIS-2-Richtlinie diskutiert werden. Bis Mitte 2022 müssen sie von den Mitgliedstaaten umgesetzt werden.

Man kann sich nur fragen, warum die Europäische Union ihre Cyberambitionen zurückschraubt, wenn sie mit Frankreich ein Beispiel für eine anspruchsvolle und erfolgreiche Wette vor Augen hat, die andere große Nationen bereits inspiriert. Neben dem französischen Modell kann Europa viele andere Instrumente einsetzen, um sich zu strukturieren. Wir hoffen daher, dass die gleiche positive Dynamik, die Frankreich an den Tag gelegt hat, auch auf europäischer Ebene eintreten wird. Es braucht eine Cybersicherheitspolitik, die keine Zugeständnisse bei den Anforderungen macht, damit wir wirklich über die nötigen Mittel verfügen, um ein starkes Ökosystem für den Cyberschutz zu schaffen." ■

S.M.

Quellen

[1] *https://www.bsi.bund.de/DE/Service-Navi/Publikationen/Lagebericht/lagebericht_node.html*

[2] *https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/*

Herausforderung: Schließen der strategischen Qualifizierungslücke

Wie sieht der Arbeitsalltag in 20 Jahren aus? Ein Blick zurück zeigt: Hunderttausende von Menschen üben heute Funktionen aus, die es vor 20 Jahren so noch nicht gab: KI-Entwickler, Cloud-Architekten, Data Scientists und viele mehr. Schon heute versuchen viele Unternehmen händeringend, entsprechend qualifiziertes Personal am Markt zu finden. Wir alle sollten uns – wo auch immer wir stehen – über das Ausmaß der zu schließenden strategischen Qualifizierungslücke bewusst sein.

Der Schwerpunkt der heutigen (staatlichen) Bildungsanstrengungen liegt auf der frühkindlichen Erziehung, der Schulbildung, der beruflichen Bildung beim Einstieg in das Berufsleben sowie der Hochschulausbildung. Hier besteht allerdings heute schon ein Bedarf am Aufbau zusätzlicher „digitaler" Kompetenz. Unabhängig von den vermittelten Inhalten bleibt allerdings weitgehend unberücksichtigt, dass der Mensch seine längste Zeit – oft über 40 Jahre – beruflichen Tätigkeiten widmet, deren Anforderungen sich in Zukunft in immer höherem Maße und immer schneller verändern werden.

Unternehmen gehören an die Speerspitze der (digitalen) Bildung

Die Träger der Aus- und Weiterbildung sind gefordert, ihren unverzichtbaren Beitrag zur Qualifizierung zu leisten. Unverzichtbar ist jedoch auch, dass sich jedes Unternehmen über die eigene Verantwortung für die Weiterqualifizierung bewusst wird. Die zu bewältigenden Umbrüche während eines Arbeitslebens sind so groß, dass wir eine zweite oder dritte Berufsausbildung benötigen. Wie gut sind die Träger der Bildung und die Unternehmen heute bereits auf diese Aufgaben vorbereitet?

Gleichzeitig ist und bleibt es auch eine Kernaufgabe jedes einzelnen Angestellten, die eigene Arbeitskraft durch lebenslanges Lernen immer wieder aufzufrischen. Die große Herausforderung für jeden Einzelnen lautet Employability. Schließlich gilt: Ein Vorratslernen gelingt heute nicht mehr! Wir müssen das Lernen in unseren Alltag integrieren und gleichzeitig eine Selbstlern-Kompetenz aufbauen. Das Motto hierzu lautet: Lernen ist Leben und Leben ist Lernen!

Deshalb ist gerade auch die Eigeninitiative von Angestellten und Führungskräften zur Schließung der strategischen Qualifizierungslücke gefragt – auch und gerade dann, wenn der eigene Arbeitgeber die Zeichen der Zeit noch nicht erkannt hat. Jeder Einzelne von uns muss die Verantwortung für seine Entwicklung übernehmen – Unternehmen und Staat können hierbei unterstützen. Doch jeder Einzelne hat die Pflicht, seine eigenen Talente einzubringen und lernfähig und lernwillig zu bleiben, um die eigene Employability zu erhalten und zu entwickeln.

Ist es schon Zeit für die Installierung eines Chief Learning Officers?

Die Zeit der allwissenden Führungskraft ist lange vorbei! Und auch für Angestellte gilt: Das Wissen von gestern reicht häufig schon heute, aber vor allem morgen nicht mehr aus. Warum installieren wir dann nicht gleich auf höchster Unternehmensebene eine Instanz, die den schönen Begriff der „lernenden Organisation" mit viel mehr Leben füllt, als dies bisher meist der Fall war. Ein Chief Learning Officer würde jedem Unternehmen gut zu Gesicht stehen! ■

Dieser Gastbeitrag von Professor Dr. Ralf T. Kreutzer erschien online bei der Bitkom Akademie. Alle Beiträge finden Sie unter: **bitkom-akademie.de**

Mehr dazu hier

bitkom akademie

IT-Dienstleister im Spannungsfeld zwischen besserer Auftragslage und steigendem Risiko

DIGITALISIERUNG IN DEUTSCHLAND

Die aktuelle Hiscox IT-Umfrage 2021 [1] zeigt: Seit Beginn der Corona-Pandemie hat sich zwar die Auftragslage der IT-Dienstleister überwiegend verbessert, mehr als vier von fünf Befragten (81 Prozent) geben jedoch an, dass die Digitalisierung bei ihren Auftraggebern kaum Fortschritte macht. Einer der Gründe ist, dass sich nahezu jedes Unternehmen durch die zunehmende Digitalisierung einer Vielzahl an neuen, dynamischen Risiken ausgesetzt sieht. Hier kommen IT-Dienstleister ins Spiel: Die deutsche Wirtschaft baut auf die Expertise der ITler, damit eine solide digitale Zukunft sichergestellt ist.

Der Weg zum passenden IT-Dienstleister ist oft lang. Von der Konzeption bis zur Umsetzung können Jahre vergehen. Hier ist eine über Jahre bestehende Vertrauensbasis einer der Erfolgs-Schlüssel. Dass Auftraggeber IT-Dienstleistern vertrauen und sie brauchen, zeigt erstens die gute Auftragslage in den Büchern sowie zweitens die Tatsache, dass ein großer Teil der auftraggebenden Unternehmen (40,5 Prozent) sich laut der Umfrage wünscht, Verantwortung im Digitalbereich an externe IT-Spezialisten abzugeben.

Wie schaffen aber IT-Dienstleister den Spagat zwischen Auftragswelle und immer höheren Risiken durch etwa Übernahmen von mehr Verantwortung für den Kunden? Drei wichtige Praxistipps können helfen:

1. Communication is key – steter Austausch und gemeinsame Zielsetzung mit dem Auftraggeber

Hauptgründe von Unternehmen, externe IT-Spezialisten zu beauftragen, sind laut IT-Umfrage zu wenig eigene IT-Kapazitäten (37,1 Prozent) und fehlendes Personal in der eigenen IT-Abteilung (32,2 Prozent). Da IT-Dienstleistern meist der Einblick in Unternehmensziele fehlt und es den beauftragenden Unternehmen oftmals an tiefer IT-Expertise mangelt, ist es essenziell, dass im Vorfeld Vorstellungen, Umsetzung und Zielsetzung zwischen allen Beteiligten klar festgelegt werden. Für eine erfolgreiche gemeinsame Umsetzung ist es enorm wichtig, dass IT-Dienstleister und Auftraggeber an einem Strang ziehen und die gleiche Vision verfolgen. Dies muss sich neben der eigentlichen Arbeit im Projekt auch in der Kommunikation spiegeln.

Denn wirft man einen Blick auf die am häufigsten gemeldeten Schadenfälle, lassen sich vor allem Schäden durch Projektverzug, -ausfall oder -abbruch identifizieren. Nicht zuletzt deshalb, da Auftraggeber und Dienstleister zu Projektbeginn keine klaren Abstimmungen getroffen haben. Durch klare, schriftliche Vereinbarungen

und einem offenen Dialog lassen sich Missverständnisse vorbeugen und daraus resultierende Projektverzüge oder sogar -abbrüche umgehen. Ein konstanter Austausch und realistische Zielsetzungen manifestieren eine erfolgreiche Zusammenarbeit – nicht zuletzt deshalb, da diese Projekte oft agil aufgesetzt werden und laufend anhand neuer Bedürfnisse oder externer Einflüsse wie neuer Gesetzgebungen inhaltlich angepasst werden. Ein gemeinsames Einverständnis zum Verschieben der Deadline geht damit einher.

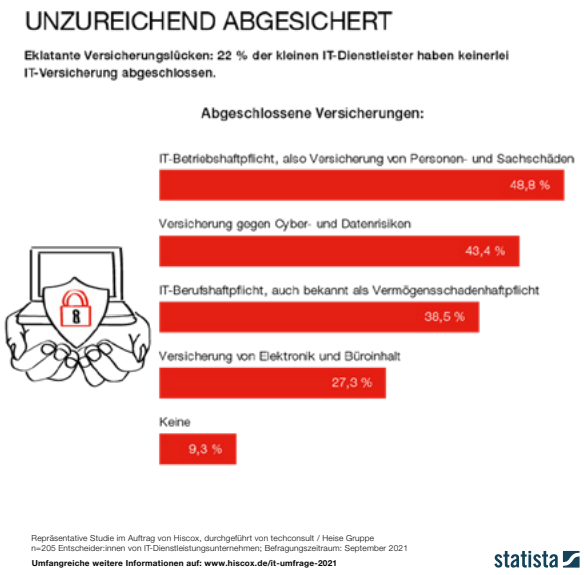
2. Realitätscheck – Wahrnehmung und Praxis zusammenführen

IT-Unternehmen übernehmen durch ihre Aufgaben Verantwortung für einen neuralgischen Unternehmensbereich ihrer Auftraggeber. Mit Verantwortung kommt Risiko, das es einzuschätzen und zu kalkulieren gilt – sowohl für sich selbst als auch für die Kunden. Aktuell herrschen bei IT-Dienstleistern jedoch große Diskrepanzen zwischen Risikowahrnehmung und tatsächlichen Schadenfällen. So gibt laut Hiscox IT-Umfrage jeweils ein gutes Drittel der Befragten (33,7 Prozent) Projektverzug und Datenverlust durch Programmierfehler (33,2 Prozent) als kritisches Risiko an – Werte, die sich nicht von anderen Risikoeinschätzungen abheben. In der Realität sieht das allerdings anders aus: Die meisten gemeldeten Schadenfälle sind auf Projektverzüge zurückzuführen. Zweite wichtige Schadenursache ist Datenverlust bei den Kunden durch Anwendungsfehler des IT-Dienstleisters.

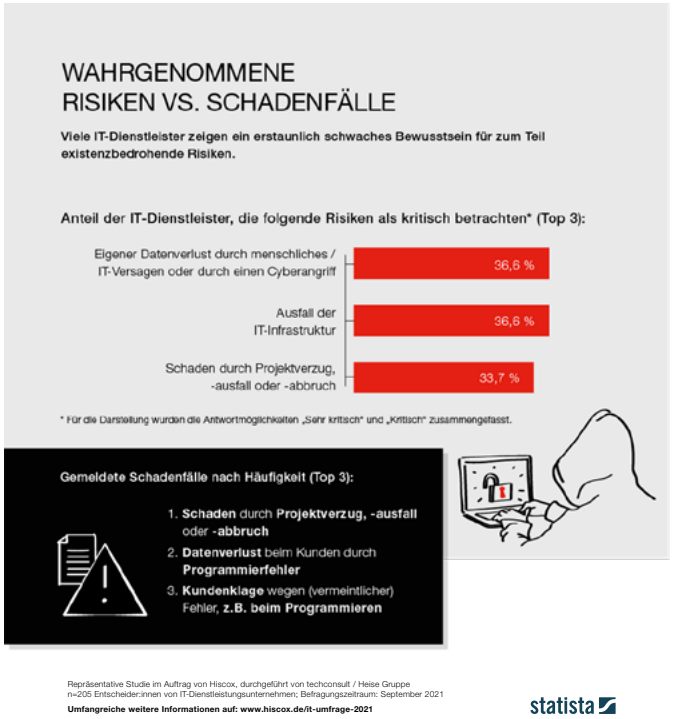
Um Wahrnehmung und Realität zusammenzuführen, sollten IT-Dienstleister tätigkeitsbezogene Risiken aufmerksam analysieren. Darüber hinaus gilt es sich mit vergangenen Fehlern oder bereits eingetretenen Schäden auseinanderzusetzen, um sich ein genaues Bild der Gefahren machen zu können. Zur Annäherung an eine realistische Risikoeinschätzung müssen IT-Dienstleister ihre vertraglichen Haftungs-Vereinbarungen, die potenzielle Schadenhöhe sowie bereits bekannte Schadenfälle in ähnlichen Aufträgen kennen, um das Risiko bei künftigen Aufträgen besser zu kennen. Hierbei kann vor allem für kleinere und mittlere Unternehmen die Unterstützung durch externe Spezialisten, wie Fachanwälte oder Experten für IT-Sicherheit, enorm helfen.

3. Auch für IT-Dienstleister gilt: Vorsicht ist besser als Nachsicht!

Die IT-Branche sieht sich also mit vielfältigen und zum Teil unerkannten oder falsch eingeschätzten Risiken konfrontiert – von Programmierfehlern, Datenverlust über unterstellter Verletzung geistiger Eigentumsrechte bis hin zu Ausfällen der IT-Infrastruktur. Wichtig ist daher die richtige Absicherung, um solche Risiken zu managen. Trotzdem setzen IT-Dienstleister aktuell noch zu wenig auf Risikotransfer in Form des Abschlusses einer IT-Berufshaftpflichtversicherung, Teilweise gibt es sogar IT-Dienstleister,



Eklatante Versicherungslücken: 22 % der kleinen IT-Dienstleister haben keinerlei IT-Versicherung abgeschlossen. (Quelle: Hiscox)



Vorstellung und Realität: Häufig gehen die Risiken, derer sich die IT-Dienstleister bewusst sind, und die tatsächlich anfallenden Schäden weit auseinander. (Quelle: Hiscox)

die gänzlich ohne IT-Versicherung operieren (9,0 Prozent). Betrachtet man nur kleinere Unternehmen, liegt der letztgenannte Wert sogar bei beinahe einem Viertel (22,0 Prozent) der Befragten.

Hiscox beobachtet in der Schadenpraxis Unberechenbarkeit und Vielfältigkeit der Risiken als große Gefahr für externe IT-Dienstleister, gegen die sich IT-Spezialisten unbedingt rüsten sollten. Passiert ein Fehler, werden die ITler von den Auftraggebern finanziell zur Verantwortung gezogen, und nicht selten geht es hier um existenzbedrohende Summen. Der Versicherer nimmt wahr, dass Schadenersatzansprüche immer häufiger gestellt werden. Daher überrascht es nicht, dass immer mehr Auftraggeber den Nachweis von IT-Versicherungen für die Projektvergabe fordern. Aus diesen Gründen ist es überraschend, dass es immer noch Unternehmen in der IT-Branche gibt, die ohne Versicherung agieren – obwohl Versicherungslösungen existieren, die speziell für die Bedürfnisse von IT-Dienstleistern konzipiert wurden. Vor allem für kleine und mittlere Firmen kann im Schadenfall ohne Absicherung die ganze Unternehmung auf der Kippe stehen. Denn: Eine gute IT-Versicherung ersetzt nicht nur den verursachten Schaden, sondern wehrt auch Ansprüche, die man gar nicht zu verantworten hat, in Form der sogenannten Schadenabwehr ab.

DIE MAGISCHEN DREI DER IT-BRANCHE

Zusammenfassend lässt sich also sagen, dass ein konstanter und dokumentierter Austausch die Richtung für das gemeinsame Projekt von Auftraggebern und IT-Dienstleistern vorgibt und eine erfolgreiche Umsetzung sicherstellt. Eine Analyse der eigenen Situation verschafft IT-Unternehmen einen Rundumblick auf potenzielle Risiken und Bedrohungen, und wie man sich dagegen absichern kann. Zu guter Letzt ist es sowohl für kleinere als auch größere IT-Dienstleister jeder Größe sinnvoll, über eine passende Versicherung nachzudenken, die individuellen Schutz für deren Bedürfnisse bietet, im Ernstfall den entstandenen finanziellen Schaden auffängt und beratend zur Seite steht sowie das Fortbestehen des Unternehmens sichert. Erkennen und berücksichtigen IT-Dienstleister die Bedeutung all dieser Punkte, können sie ihrem Auftrag gerecht werden, und einen immensen Beitrag für das digitale Zeitalter leisten. ■

Quellen

[1] *https://www.hiscox.de/it-umfrage-2021/*

MARC THAMM,
Underwriting Manager Technology, Media & Communications bei Hiscox

2B Advice
The Privacy Benchmark

Mit 2B Advice Datenschutzlösungen haben Sie ein Problem weniger.

- DSFA / PIA / Risikoanalyse und -bewertung
- Aufzeichnungen von Verarbeitungstätigkeiten (RoPA)
- Verarbeitungsübersicht und Datenflüsse
- Management von Verarbeitungen & Berichterstellung
- Datenschutz Compliance Check
- Whistleblower
- Assistenten und Kataloge
- Verwaltung von Betroffenenanfragen
- Integrierte webbasierte Trainingsplattform
- Integrierte Onlinekommunikation
- Mehrsprachigkeit
- Planung und Berichterstattung
- Webseiten Analyzer
- Cookie Policy Generator
- Privacy Statement Generator
- Consent Manager
- Web Services & REST-API
- Cookie Banner

Bestellen Sie unsere KOSTENLOSE Einzelplatzversion

2B Advice ist ISO/IEC 27001:2013 zertifiziert

2B Advice GmbH - the privacy benchmark | Joseph-Schumpeter-Allee 25, Bonn
0228 926165-100 | sales.de@2b-advice.com | www.2b-advice.com

Innovativ, digital und manipulationssicher – Alternativen zu E-Mail und Co.

STATE OF THE ART BEIM DOKUMENTENAUSTAUSCH

Es mag etwas weit hergeholt klingen und dennoch: Die Art und Weise des Umgangs mit Dokumenten bestimmt die Zukunftsfähigkeit einer Volkswirtschaft mit. Entscheidend ist, dass die im Einsatz befindlichen Dokumente von Mensch und Maschine gelesen werden können. Mit cleveren Workflows und Prozessmanagementsystemen können die so ausgelesenen Informationen wesentlich effektiver ausgewertet und abgelegt werden als in der herkömmlichen analogen Form. Grundvoraussetzung sollte allerdings eine rechtssichere, zuverlässige und vertrauenswürdige Übertragung zwischen den beteiligten Parteien sein.

Sprachnachricht, Tweet, Chat, E-Mail – Präsenzinformationen kombiniert mit Tools zur übergreifenden Zusammenarbeit sind überaus wichtig und beschleunigen Arbeitsabläufe enorm. Aber alle Instrumente, die dieses Arbeiten ermöglichen, sind nicht für den vertrauenswürdigen Dokumentenaustausch geeignet. In diesen wichtigen Fällen muss der Austausch von Dokumenten nachvollziehbar erfolgen. Zudem sollten Sender und Empfänger direkt miteinander kommunizieren und den Status des Dokuments jederzeit kennen.

Innerhalb von Unternehmen, Behörden, Instituten und verschiedensten Einrichtungen werden Dokumente meist über Dokumentenmanagementsysteme, Fileshares auf Servern oder im schlimmsten Fall über USB-Sticks oder E-Mails ausgetauscht. Verlassen Dokumente das Unternehmen, geht der Weg oft über E-Mail oder Freigaben auf Cloud-Basis. Ein Reizthema nicht nur für Systemadministratoren, denn die Sicherheit dieser sogenannten Schatten-IT liegt in den Händen der Mitarbeiter und ist nur wenig bis gar nicht unter Kontrolle zu halten.

FAX UND E-MAIL – ÜBERHOLTE TECHNOLOGIEN?

Für einen einigermaßen kontrollierten digitalen Austausch bieten sich nach wie vor nur Fax- und E-Mail-Technologie an. Aber warum werden diese etablierten Methoden dann immer wieder angezweifelt? Beim Fax sind die Gründe relativ offensichtlich. Spontan assoziiert damit wahrscheinlich jeder einen hohen Papierverbrauch und laute Piep-Geräusche. Mit Digitalisierung und Fortschritt hat dies nur wenig zu tun und verleitet viele dazu, das Fax aufs Abstellgleis zu schieben. Zu Unrecht, denn das heutige Fax druckt weder aus noch erzeugt es Geräusche. Dokumente werden hier paketvermittelt über moderne IP-Telefonanschlüsse übertragen und digital an das interne Ziel weitergeleitet. Aber es ist nicht abzustreiten, Faxnachrichten in ihren Graustufen und der geringen Auflösung sind alles andere als zeitgemäß.

Mehr Zuspruch findet die E-Mail-Technologie. Ihre Nachteile sind weniger offensichtlich und für Endanwender auch nur schwer nachvollziehbar. So gehört der fehlende Dokumentencharakter einer E-Mail noch zu den kleineren Problemen. Ein nicht zu unterschätzendes Risiko birgt der Übertragungsweg, der nicht End-to-End verläuft. Eine E-Mail springt über diverse unbekannte Server zum vermeintlichen Ziel und erst dort wird geprüft, ob die Nachricht angenommen werden kann oder nicht. Es ist eine Art „Fire and Forget", denn in der Zwischenzeit ist das Dokument beim Versender längst als versendet markiert und am Ende der meisten Workflows angekommen. Würde bereits beim Sendebeginn geprüft, ob die Empfangsseite vorhanden und in der Lage ist, das Dokument zu empfangen, wäre eine große Problematik beseitigt.

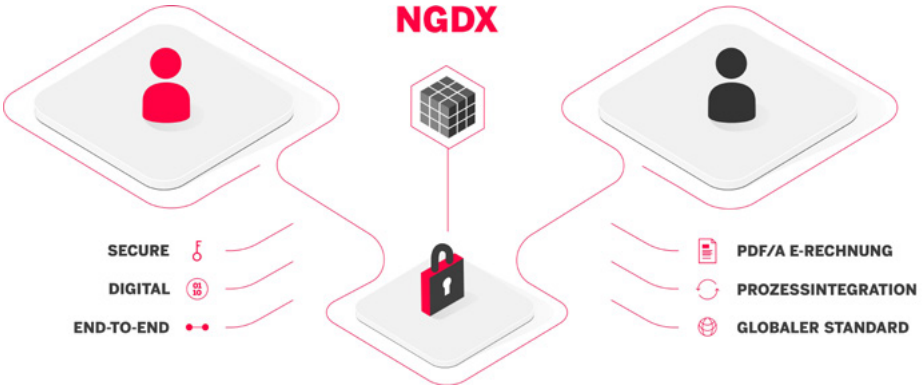
Der offensichtlichste Nachteil der E-Mail ist aber, dass sie neben dem USB-Stick das beliebteste Einfallstor für Malware und Viren darstellt. Im Standardmodus sind kaum Einschränkungen für die angehängten Dateien vorhanden. Ein explizites System zum Dokumentenaustausch kann deutlich restriktiver ausgelegt sein und somit deutlich mehr Gefahrenpotenzial bannen. Auch wäre durch eine Ende-zu-Ende-Übertragung die Herkunft einer Nachricht mit schädlichen Inhalten einfacher zu identifizieren.

Um einen zuverlässigen Dokumentenaustausch zu bewerkstelligen, setzen viele Unternehmen auf Insellösungen. Für sich genommen erfüllen diese ihren Zweck teils sehr gut, sind aber derartig spezialisiert, dass ein branchenübergreifender Einsatz nicht realisierbar ist. Auch ist die Einstiegshürde durch komplexe Hardwarevoraussetzungen häufig relativ hoch.

RECHTS- UND MANIPULATIONSSICHERE ALTERNATIVE FÜR DEN DOKUMENTENAUSTAUSCH

Was vielleicht noch zu wenig bekannt ist: Es gibt bereits Lösungen, die in der Lage sind, diese Herausforderungen zu meistern: Moderne Dokumentenaustauschlösungen auf IP-Basis. Sie sind einfach zu implementieren, nach innen hin hochgradig anpassbar und folgen als Schnittstelle nach extern einem globalen ITU-Standard. Zwischen den Kommunikationsteilnehmern bauen sie eine direkte Verbindung ohne zentrale Serverinstanz über das Telefonnetz auf. Dabei ist es zunächst unerheblich, ob diese Verbindung bereits auf modernen IP-Anschlüssen basiert oder noch über klassische ISDN-Anschlüsse erfolgt. Es ist auch nicht erforderlich, dass die Gegenstelle alle Optionen des Standards unterstützt. Im Verbindungsaufbau einigen sich die beiden Gegenstellen automatisch auf die bestmögliche Übertragungstechnik.

Die Ende-zu-Ende-Übertragung inklusive qualifiziertem Sendebericht und Informationen zu den Dokumenteneigenschaften bietet Rechtssicherheit für Sender und Empfänger. So lässt sich jederzeit nachweisen, wann ein Dokument erfolgreich an welche Gegenstelle übertragen wurde. Potenziell schädliche, aktive Inhalte, wie Hyperlinks oder Applikationen, sind von der Übertragung ausgeschlossen. Um zu verhindern, dass Inhalte mitgelesen oder abgefangen werden, setzen diese neuartigen Lösungen auf ein Zusammenspiel aus Verschlüsselung und Authentisierung auf Basis von vertrauenswürdigen Zertifikaten. Damit sind sowohl das Dokument selbst als auch sein Transportweg kodiert, wobei dies komplett unter Absicherung der Identitäten der Gegenstellen erfolgt. Den Anwendern steht eine rechts- und manipulationssichere Alternative zur E-Mail zur Verfügung.



Mit dem neuen NGDX-Standard (Next Generation Document Exchange) lassen sich Dokumente unabhängig von Device und Dateiformat empfangen und senden – manipulationssicher und DS-GVO-konform. (Quelle: Ferrari electronic)

EINFACHE ANBINDUNG AN VORHANDENE IT-SYSTEME

Auch hochauflösende PDF/A-Dokumente mit oder ohne Metainformationen (beispielsweise bei E-Rechnungen nach ZUGFeRD 2.1 – „Zentraler User Guide des Forums elektronische Rechnung Deutschland") können übertragen werden. Je nach Anforderung erfolgt dabei eine Zertifikatsüberprüfung der beiden Teilnehmer und eine Verschlüsselung des Dokuments. Die übertragenen Dokumente sind durch ihre rein digitale Historie zur automatisierten Verarbeitung bestens geeignet und unterstützen modernste Workflows in den angebundenen Einrichtungen und Unternehmen.

Eine Anbindung an bereits im Einsatz befindliche IT-Systeme ist auf unterschiedliche Weise und mit verschiedenen Integrationstiefen möglich. Je tiefer die Integration, desto komfortabler für den Anwender. Moderne Dokumentenaustauschserver (DAS) bieten mindestens eine der drei folgenden Anbindungsoptionen:

- **Web-Services**
Die wohl tiefste Integration mit einem DAS wird über Web-Services realisiert. Allerdings sind hier teilweise Programmierkenntnisse zu beiden Systemen gefordert, und der Aufwand kann je nach zu integrierendem System relativ hoch sein.

- **Datei-Schnittstellen**
Zur Anbindung etwas älterer Systeme werden oft Dateischnittstellen verwendet. Dabei werden auf Dateiebene Dokumente und Beschreibungsdateien zum Austausch abgelegt.

- **Anbindung über E-Mail**
Eine Anbindung per E-Mail-Versand ist meist der erste einfache Test. Hier entscheidet sich, ob eine komplexere Anbindung notwendig ist.

In einer Welt, die immer vernetzter agiert, ist ein übergreifender, digitaler und vor allem manipulationssicherer Dokumentenaustausch essenziell. Der Aspekt der direkten und nur dadurch wirklich vertrauenswürdigen Kommunikation rundet diese Lösungen ab. Mit innovativen Lösungen, die hybride Dokumente schaffen und übertragen, lassen sich Workflows und Prozesse beschleunigen und eine ganz neue Art des Dokumentenmanagements etablieren. ■

CHRIS HELBING,
Director Product Management,
Ferrari electronic

Managed Detection and Response als Antwort auf aktuelle Security-Probleme

IT-SICHERHEIT FÜR DEN MITTELSTAND NEU DENKEN

Die durch die Pandemie noch einmal deutlich verstärkte Digitalisierungswelle, die beruflich wie privat in jeden Winkel vordrang, blieb auch Cyberkriminellen nicht verborgen. Die plötzliche Verlagerung von immer mehr Prozessen in den virtuellen Raum hat besonders mittelständische Unternehmen vor eine große Herausforderung gestellt. Umfragen zeigen, dass sich diese mit Bezug auf ihre IT-Sicherheit häufig überfordert sahen. Ein Umdenken in der Security-Strategie könnte den ersehnten Ausweg bieten.

Der deutsche Mittelstand steht vor einer riesigen Aufgabe: Auf der einen Seite sind sie gezwungen, ihre Geschäftsabläufe immer mehr zu digitalisieren und dabei deren Verfügbarkeit und wertvolles geistiges Eigentum zu schützen. Auf der anderen Seite ist dies oft schwierig, da es häufig an Ressourcen und dem passenden Know-how fehlt, um auf das vielfältige Repertoire von Cyberkriminellen zu reagieren. Laut Experten werden nur etwa 54 Prozent aller Warnmeldungen, ausgegeben von den unzähligen Sicherheits-Tools, die in Unternehmen eingesetzt werden, überhaupt richtig beachtet und verarbeitet. Mal- und Ransomware, Phishing-Angriffe, Denial of Service Attacken, und gezielter Datenklau durch unentdeckte Angriffsvektoren – das Portfolio potenzieller Angreifer ist breit gefächert. Und nicht nur die Angriffsfläche wird immer größer, sondern auch die Zahl der potenziellen Angreifer. Durch Cybercrime-as-a-Service-Angebote wird es auch für technisch weniger versierte Kriminelle leichter, Angriffe auszuführen oder diese in Auftrag zu geben. Für die Unternehmen steht dabei einiges auf dem Spiel: Es geht nicht nur um den Wert von Daten, die auf keinen Fall in die falschen Hände geraten sollten, auch mögliche Betriebsausfälle, Reputationsschäden oder unbrauchbare IT-Infrastruktur können verheerende Folgen haben.

Diese Ausgangslage führt zu Verunsicherungen, die sich an ganz konkreten Zahlen festmachen lassen: Laut einer im letzten Jahr durchgeführten Studie von Deloitte Consulting sehen 61 Prozent der IT-Verantwortlichen in mittelständischen Unternehmen die größte Herausforderung in der frühzeitigen Erkennung von Cyberangriffen. Zudem gehen 83 Prozent von ihnen davon

Foto: Open Systems

aus, dass IT-Sicherheit zunehmend an Relevanz gewinnt. Zu diesem Ergebnis kommt auch das World Economic Forum in ihrem Global Risks Report. Demnach werden Risiken im Zusammenhang mit IT-Security weltweit als eine der größten Gefahren angesehen. Das Bundeskriminalamt verzeichnet eine gestiegene Anzahl von Cyberangriffen seit Beginn der Pandemie und stuft die Bedrohungslage aufgrund der Verschiebung diverser Lebensbereiche in den virtuellen Raum als „andauernd hoch" ein.

IT-SECURITY MUSS MIT DER ZEIT GEHEN

Der alleinige Einsatz traditioneller Schutzmaßnahmen, wie Firewalls und Malware-Erkennung, bietet keinen zuverlässigen Schutz vor dem Hintergrund zunehmender Professionalisierung von Cyberkriminellen. Diese Erkenntnis ist nicht neu, doch nicht alle Unternehmen waren auf den hohen Digitalisierungsdruck, den Corona mit sich brachte, gut vorbereitet. Das lässt sich auch dem kürzlich veröffentlichten Forschungsbericht des Kriminologischen Forschungsinstituts Niedersachsen entnehmen, der unter anderem das Homeoffice und die Verwendung privater Software auf Arbeitnehmerseite als Schwachstellen identifiziert. Ernstzunehmende Angreifer verfügen über viel Know-how, und es kommt immer wieder vor, dass sie als Teil international operierender Organisationen operieren oder sogar von staatlichen Stellen unterstützt werden. Das führt dazu, dass Cyberkriminelle mit immer neuen Methoden ihren potenziellen Opfern den berühmten Schritt voraus sind. Was läge also näher, als die hauseigene IT-Security auf den neuesten Stand zu bringen? Diese Anschaffungen erfordern allerdings nicht nur Budget, sondern auch fachkundiges Personal, das diese Lösungen verwaltet. Denn um aus der Informationsflut des eigenen Security-Toolbestands und moderner Threat-Intelligence-Lösungen die richtigen Schlüsse zu ziehen, um passende Abwehrmaßnahmen einzuleiten, braucht es viel Erfahrung und genügend Expertenwissen.

Doch genau dieses Fachpersonal ist rar: Laut der (ISC)² Cybersecurity Workforce Study fehlen weltweit etwa vier Millionen Security-Experten und CISOs schätzen, dass etwa 145 Prozent mehr Personal benötigt wird, um auch für die Zukunft noch gerüstet zu sein. Für Profis sind Großkonzerne, im Vergleich zu mittelständischen Unternehmen, häufig die attraktiveren Arbeitgeber. Darüber hinaus hat der Mittelstand es aufgrund seines im Vergleich zu Großunternehmen kleineren IT- und Security-Budges schwer, seine Hard- und Software laufend an die Bedrohungslage anzupassen. Umso wichtiger ist es für diese Unternehmen, ihre Ressourcen sinnvoll einzusetzen.

CYBERANGRIFFE ERKENNEN UND BEHEBEN

Geschwindigkeit ist ein wichtiger Faktor in der IT-Security: Je schneller ein Angriff erkannt wird, desto schneller kann dieser abgewendet werden und desto geringer ist der potenzielle Schaden für das Opfer. Entscheidend bei einer Attacke ist es also, den Zeitraum bis zum Einleiten passender Gegenmaßnahmen so gering wie möglich zu halten und die vorhandene Zeit effektiv zu nutzen. Damit dies gelingt, benötigt es ein Umdenken. Statt auf restriktive, das Tagesgeschäft einschränkende, oft weniger wirksame Maßnahmen zu setzen, sollten Unternehmen einkalkulieren, dass es immer zu Angriffen kommen kann und es im Ernstfall ausschließlich darum geht, diese schnellstmöglich zu erkennen, einzudämmen und den Ursprungszustand wiederherzustellen.

Am besten eignen sich dafür „Managed Detection and Response"-Lösungen (MDR). Dabei ist ein spezialisierter Dienstleister für die Erkennung und Behebung von Cyberangriffen verantwortlich. Dieser Dienstleister stellt dabei sowohl die nötige Technologie als auch die entsprechend qualifizierten Mitarbeiter in der erforderlichen Teamstärke. Dank ihrer Threat Intelligence sind Anbieter von MDR-Lösungen stets am Puls der Zeit und können die Bedrohungslage sehr detailliert einschätzen. Häufig werden sie dabei von künstlicher Intelligenz unterstützt und können so Prognosen treffen, welche Maßnahmen für welchen Kunden sinnvoll sind. Der „Response"-Anteil der Dienstleistung steht bei MDR für die schnelle Abwehr von Angriffen auf das Unternehmensnetzwerk, die zu jeder Tages- und Nachtzeit verfügbar ist. Damit ist MDR für Unternehmen mit begrenzten Ressourcen die perfekte Antwort auf Sicherheitslücken in ihrer IT-Infrastruktur, die bisher kaum zu schließen waren. Diese Vorteile erkennt auch der Markt: So geht beispielsweise das Analystenhaus Gartner davon aus, dass die Hälfte aller Unternehmen bis 2025 MDR-Services nutzen werden.

IMMER AUF DER HÖHE DER ZEIT

Unternehmen, die ihre IT-Sicherheit um das Know-how externer Spezialisten ergänzen, umgehen so mögliche Engpässe, können schnell und flexibel auf Vorfälle reagieren und sind für die Zukunft gerüstet. Dadurch wird ihnen der Auf- beziehungsweise Ausbau eines eigenen Security Operations Center (SOC) erspart, das nicht nur genügend Vorlaufzeit benötigt, sondern auch entsprechende Ressourcen bindet. Zudem minimiert MDR das Risiko, überhaupt Opfer von Angriffen zu werden, da Angriffsvektoren kontinuierlich überwacht werden und das Team in Echtzeit auf Sicherheitsvorfälle reagieren kann. Ein weiterer wichtiger Vorteil von MDR-Lösungen ist, dass sie nur bei tatsächlichen Vorfällen eine Meldung verschickt – IT-Administratoren und Security-Manager werden also nicht mit unbedeutenden Warnmeldungen überhäuft. Das stellt zum einen sicher, dass keine wichtige Warnmeldung im Grundrauschen untergeht und zum anderen können sich die IT-Verantwortlichen weiterhin auf ihr Kerngeschäft konzentrieren. MDR-Dienste sind gut skalierbar: Sie können flexibel an unterschiedliche Risikotoleranzen, Budgets und die Entwicklung eines Unternehmens angepasst werden.

Managed Detection and Response ist für Unternehmen also eine effiziente und sichere Methode, ihre IT-Security auf den neuesten Stand zu bringen und sie auch konstant dort zu halten. Bei der Wahl eines Anbieters sollten Unternehmensentscheider darauf achten, dass sie für diesen kritischen Bereich erfahrene und kompetente Experten ins Boot holen, die sich nahtlos in das bestehende IT-Team einfügen und deren Lösungen ohne große Brüche zu implementieren sind. Die Zukunft der IT-Sicherheit liegt in der Zusammenarbeit – denn MDR-Lösungen sparen Geld, Zeit und Ärger. ■

MORITZ MANN,
Chief Strategy Officer bei
Open Systems

KRITIS-Verordnung 2.0

BERECHTIGUNGEN SICHER VERWALTEN

Die Verschärfung nationaler IT-Sicherheitsstandards setzt sich auch 2021 fort: Durch die Novelle des IT-Sicherheitsgesetzes und der KRITIS-Verordnung erweitern sich die Pflichten für die Betreiber kritischer Infrastrukturen und den weiteren Adressatenkreis des Sicherheitsstandards. Darüber hinaus stehen Aktualisierungen des IT-Grundschutzes und verschiedener branchenspezifischer Sicherheitsstandards (B3S) vor der Tür. Was sich für KRITIS-Betriebe jetzt ändert und welche Rolle Identity Access Management in der vorgeschriebenen Absicherung spielt.

Mit dem IT-Sicherheitsgesetz 2.0 arbeitet die deutsche Bundesregierung weiter an der Absicherung der sogenannten kritischen Infrastrukturen (KRITIS). Durch die Anpassung verschiedener Schwellenwerte und die Ergänzung um den Sektor Siedlungsabfallentsorgung fallen schätzungsweise 270 zusätzliche Betriebe unter die neue KRITIS-Verordnung. Hinzu gekommen ist zudem der vorgeschriebene Einsatz von Angriffserkennungssoftware, welche auch eine laufende Auswertung der Protokolle voraussetzt. Die Kommunikation mit dem BSI (Bundesamt für Sicherheit in der Informationstechnik) wurde verstärkt. So muss eine Kontaktstelle eingerichtet, kritische Komponenten müssen gemeldet werden. Insgesamt ergibt sich ein erhöhter organisatorischer Aufwand für KRITIS-Betriebe.

Umso wichtiger ist es also, durch automatisierte Lösungen die technischen Anforderungen an die Informationssicherheit möglichst effizient abzudecken. Passende Tools gibt es für die unterschiedlichsten Bereiche der Sicherheitsstandards: Back-up- und Verschlüsselungssysteme, Patchmanagement, Überwachungslösungen für fremde Geräte und Netzwerkendpunkte. Ein häufig unterschätzter Aspekt für die Absicherung des eigenen Netzwerks ist die Verwaltung von Zugriffsrechten. Diese bilden jedoch die Grundlage für sichere Arbeitsabläufe.

DAS LEAST-PRIVILEGE-PRINZIP

Wie die meisten modernen Sicherheitsstandards schreibt auch KRITIS vor, Zugriffsrechte auf ein notwendiges Minimum zu beschränken. Man spricht auch vom Need-to-know- beziehungsweise Least-Privilege-Prinzip. Doch was genau bedeutet das? Einfach ausgedrückt lässt sich durch die Einschränkung der Berechtigungen auch das Potenzial für Missbrauch reduzieren. Das gilt sowohl für interne Vorfälle, wie Datenpannen, als auch für Attacken von außen. Identitätsbasierte Angriffe zählen nach wie vor zu den meist verwendeten Methoden von Hackergruppen. Insbesondere inaktive Konten stellen ein beliebtes Einfallstor dar, wie vor kurzem im Fall des Colonial-Pipeline-Hacks, der mit einem nicht mehr benötigten VPN-Zugang begann.

Je strenger Zugänge und Berechtigungen limitiert werden, desto geringer die Angriffsfläche einer Organisation. In der Praxis sind überflüssige Rechte jedoch schwer ausfindig zu machen. Wenn Nutzern Rechte fehlen, melden sie sich von selbst. Alte Rechte werden hingegen einfach vergessen und sammeln sich im Laufe der Zeit an. Eine Software-Lösung für Identity und Access Management (IAM) setzt hier an zwei Punkten an: Einerseits erlaubt es ein Standard-Set an Rechten, bei Abteilungswechseln und ähnlichen Prozessen alte Berechtigungen automatisch zu entfernen. Andererseits werden Berechtigungen im Rahmen einer regelmäßigen Rezertifizierung auf Aktualität geprüft, etwa durch automatische Benachrichtigungen an die Verantwortlichen.

EFFIZIENTE VERWALTUNG UND DOKUMENTATION

Unabhängig davon, ob eine Organisation unter die KRITIS-Verordnung fällt, Mindeststandards für Länder- und Bundesbehörden einhalten muss, oder aus eigenem Interesse die Informationssicherheit verbessern möchte, ergeben sich durch die Automatisierung der Benutzerverwaltung Vorteile in der Verwaltung. Die selbstständige Anpassung bei personellen Veränderungen trägt neben der verbesserten Sicherheit etwa auch dazu bei, IT-Admins zu entlasten und für neue Aufgaben freizuspielen. Um die Einhaltung von Compliance-Standards auch rückwirkend nachweisen zu können, dokumentieren Software-Lösungen darüber hinaus sämtliche Änderungen an Zugriffsrechten. ■

HELMUT SEMMELMAYER,
Senior Manager Channel Sales bei tenfold security

Fünf unterschätzte
Microsoft-Tools für die Cyber Defense

ANGRIFFSKETTEN ERFOLGREICH UNTERBRECHEN

Ein Trend, der sich in den letzten Jahren deutlich abzeichnete, ist die Zunahme von Cyberattacken. Fernverwaltung und -Arbeit befeuern den Anstieg der Sicherheitsbedrohungen. Ransomware ist zwar nicht mehr die IT-Bedrohung Nummer Eins, aber sie beschert kriminellen Akteuren jeden Tag beachtliche Summen und kostet Unternehmen jährlich Millionen über Millionen. Glücklicherweise gibt es Tools, auf die Unternehmen in der Regel bereits Zugriff haben und die – richtig eingesetzt – schon am Anfang einer Cyberattacke dabei helfen, klassische Angriffstaktiken zu unterbrechen oder zumindest zu erkennen.

Laut dem Ransomware Incident Response Anbieter Coveware stieg die durchschnittliche Summe für gezahlte Lösegelder im dritten Quartal 2020 auf 196.624 Euro an. Das entspricht einer Steigerung um 31 Prozent gegenüber dem zweiten Quartal. Die durchschnittliche Ausfallzeit, die von Ransomware verursacht wurde, stieg ebenfalls – hier sind es jetzt 19 Tage.

Für Managed Service Provider (MSPs) bedeutet diese verschärfte Bedrohungslage, noch bessere IT-Lösungen zur Verteidigung anbieten zu müssen. Dabei geht es nicht allein um das Blockieren von Schadsoftware, sondern um das Suchen, Abwehren und schnelle Reagieren bei Verdacht auf Cyberattacken, die bereits am Anfang der Angriffskette zu beobachten sind. MSPs sind bemüht, Unternehmen bestmöglich vor Cyberrisiken zu schützen. Problem: Viele ihrer Kunden wollen nicht für Sicherheitssoftware von Drittanbietern bezahlen. Das ist aber auch oft nicht notwendig, denn es gibt fünf kostenlose Tools direkt von Microsoft, auf die Unternehmen in der Regel bereits Zugriff haben. Neben der Vermeidung von Zusatzkosten für Drittanbieter von Sicherheitssoftware bietet sich mit diesen Werkzeugen der zusätzliche Vorteil, dass die meisten der Verteidigungsstrategien zentral über das Remote Monitoring and Management (RMM) oder Intune bereitgestellt und/oder konfiguriert werden können.

TOOL NR. 1: RD-GATEWAY

Dieses Werkzeug entschärft das erste Eindringen, genauer gesagt RDP Brute Force. Es gilt als allgemein bekannt, dass man das Remote Desktop Protocol (RDP) nicht im Internet offenlegen sollte. Trotzdem war ein nicht angemessen abgesichertes RDP für mehr als 50 Prozent der Ransomware-Opfer, mit denen Coveware es im 3. Quartal 2020 zu tun bekam, die Schwachstelle, die den Angriff ursprünglich erst möglich gemacht hatte. MSPs und Sicherheitsbeauftragte können Kompromittierungen durch eine Konfiguration von RD-Gateway und durch das Befolgen zusätzlicher Maßnahmen (darunter: MFA) vermeiden.

Ist sichergestellt, dass es nirgendwo einen Server gibt, dessen RDP ein Cyberrisiko darstellt, empfihlt sich ein zusätzlicher Test mit einem passenden PowerShell-Skript, beispielsweise von Cyberdrain – dazu später mehr.

TOOL NR. 2: ATTACK SURFACE REDUCTION (ASR) – REGELN ZUR VERKLEINERUNG DER ANGRIFFSFLÄCHE

ASR-Regeln entschärfen Taktiken wie:

- das erste Eindringen über problematisch konfigurierte Anwendungen (Microsoft Office, Adobe, E-Mail-Client),
- Diebstahl von Zugangsdaten über lsass.exe,
- Seitwärtsbewegung und Ausnutzen von WMI and PsExec,
- andauerndes Ausnutzen von WMI-Ereignisabonnement und Payload herunterladen oder ausführen durch Schad-Skripte oder Ransomware.

Die Microsoft ASR-Regeln sind extrem hilfreich. Sie bieten Schutz vor einer Vielzahl an Gefährdungen in verschiedenen Angriffsstadien. Der Hersteller bestätigt, dass die von ihm entwickelten ASR-Regeln dazu dienen, einige der Bereiche abzuschirmen, in denen Microsoft am häufigsten Angriffe beobachtet. Ziel ist es, Organisationen, die auf oft gefährdete Funktionen und Programme, wie Office-Macros, Windows Management Instrumentation, kurz WMI, PsExec etc., angewiesen sind, besser zu schützen.

Zur Umsetzung der ASR-Regeln wird vorausgesetzt, dass Windows 10 (Versionen 1709 und spätere) installiert und der Microsoft Defender aktiv ist – für manche Regeln wird ein cloudbasierter Schutz nötig. Außerdem sollten Microsoft Unternehmenslizenzen vorhanden sein.

ASR-Regeln können unter anderem zum Blockieren von Angriffen gegen Microsoft Office eingesetzt werden, hierzu gehören:

- Office-Anwendungen an der Erstellung ausführbarer Inhalte hindern (Blockierungsmodus empfohlen*)
- Win32 API Aufrufe von Windows-Macros blockieren (Überwachungsmodus anfangs empfohlen*)
- Office-Anwendungen am Einfügen von Code in untergeordnete Prozesse hindern (Überwachungsmodus anfangs empfohlen*)
- Alle Office-Anwendungen am Erstellen von untergeordneten Prozessen hindern (Überwachungsmodus anfangs empfohlen*)

Zudem können ASR-Regeln zum Blockieren zusätzlicher Malware und zur Verhinderung des Missbrauchs von Anwendungen sowie zum Blockieren von bösartigen Skripten eingesetzt werden. Hierzu zählen beispielsweise das Blockieren von ausführbaren Inhalten aus dem E-Mail-Client und Web-E-Mail oder auch das

Blockieren nicht vertrauenswürdiger und nicht signierter Prozesse, die aus dem USB-Stick ausgeführt werden. Außerdem lassen sich mit den ASR-Regeln JavaScript und VBScript am Starten heruntergeladener ausführbarer Inhalte hindern und die Ausführung potenziell verborgener Skripts stoppen (Blockierungsmodus empfohlen mit Ausnahme von Entwickler-PCs).

Nicht zuletzt können böswillige Handlungen nach einer Kompromittierung wie etwa Diebstahl von Anmeldeinformationen aus dem Subsystem für die lokale Sicherheitsautorität (lsass.exe) blockiert werden. Aber auch die Erstellung von Prozessen durch PSExec- und WMI-Befehle (inkompatibel bei Verwendung des MS System Center Configuration Manager, kurz SCCM) sowie die Persistenz durch WMI-Ereignisabonnement werden somit verhindert (Blockierungsmodus empfohlen).

TOOL NR. 3: WINDOWS FIREWALL

Die Windows Firewall entschärft folgende Taktiken:

- Seitwärtsbewegung: SMB-basiert
- Payload herunterladen/ausführen: LOLbins Oubound-Verbindungen

Windows Firewall ist eines der zu wenig genutzten Werkzeuge, das einen großen Beitrag zur Sicherheitsstrategie eines Unternehmens leisten kann. Wie Palantirs Chief Information Security Officer Dan Stuckey einst hervorhob, ist sie nicht nur bereits vorkonfiguriert und vorhanden, sondern „stellt auch einen der einfachsten Wege dar, den Fernzugriff auf oft missbräuchlich ausgenutzte Services zu beschränken."

Eine der größten Chancen, die sie für Sicherheitsexperten bietet, ist die Möglichkeit, Kompromittierungen zu isolieren. Dies wird erreicht, indem Angreifer daran gehindert werden, SMB-basierte (Server Message Block) Seitwärtsbewegungen durchzuführen. Dazu gehört die Implementierung eines einfachen abgestuften Administrationsmodells und die Verwendung einer einfachen Windows-Firewall-Regel via GPO, die alle nach innen gerichteten Kommunikationsversuche über die Ports 139 und 445 blockiert. Darüber hinaus wird empfohlen, inbound WinRM und RDP zu Workstations zu unterbinden und ihnen die Verwendung von LLMNR (Link Local Multicast Name Resolution), Netbios, oder mDNS outbound zu untersagen.

TOOL NR. 4: POWERSHELL

PowerShell entschärft folgende Taktiken:

- Erstes Eindringen: Angreifbares RDP und gefährdete, mit dem Internet verbundene Systeme
- Seitwärtsbewegung: Missbrauch von PsExec
- Beharrlichkeit: Neue Benutzerkonten, geplante Aufgaben, WMI Event Abonnement

Die bisher beschriebenen Verwendungsmöglichkeiten für die ersten drei Werkzeuge konzentrierten sich vorwiegend auf Präventionsmaßnahmen. Sie helfen primär, das Eindringen zu verhindern oder zu erschweren und böswillige Aktivitäten zu blockieren. Mit diesem und dem folgenden Werkzeug verlagert sich die Aufmerksamkeit auf das Aufspüren von Kompromittierungen und die Reaktion darauf.

Viele MSPs verwenden PowerShell bereits aktiv, um eine Vielzahl an Fernverwaltungsaufgaben zu automatisieren. Dank der hervorragenden Arbeit von Skripting-Experten wie Cyberdrain-Autor Kelvin Tegelaar, gelingt es mehr und mehr MSPs, die Überwachungsprozesse ebenfalls mit PowerShell zu optimieren. Auf Cyberdrain.com finden sich nützliche PowerShell-Skripte zur Identifikation von Risiken angreifbarer Systeme, aber auch zur Erkennung möglicher Seitwärtsbewegung, andauernden Bedrohungen und Ransomware-Aktivitäten. Beispielsweise kann die Durchführung externer Port-Scans bei Unternehmen Risiken minimieren. Außerdem können MSPs dank einem PowerShell-Skript Alarmierungen bezüglich der Nutzung von PsExec erzeugen. PsExec ist eines der administrativen Werkzeuge, die Angreifer gerne für die Ausführung von Remote-Befehlen missbrauchen. Es ist wichtig, dass man sofort bei Anzeichen für Probleme im Kundennetzwerken reagiert, und zwar logischerweise, bevor Ransomware installiert werden kann.

TOOL NR. 5: AUTORUNS

Autoruns entschärft Einträge in die Registrierungsdatenbank. Eine der andauernden Strategien für gezielte Angriffe besteht darin, bösartige Skripte in der Windows-Registrierungsdatenbank zu platzieren – mit der Absicht, sie bei Systemneustarts auszuführen oder sie von Shortcuts oder Batch Files auslösen zu lassen. Microsoft Autoruns zeigt transparent auf, welche Programme während des Neustarts oder Einloggens automatisch angestoßen werden.

VERFÜGBARE TOOLS ALS ZUSÄTZLICHEN SCHUTZ NUTZEN

Selbstverständlich können diese fünf Werkzeuge das Risiko, von Ransomware betroffen zu sein, nicht vollständig eliminieren. Aber sie helfen, vorhandene Sicherheitslücken zu erkennen und zu beheben. Verantwortliche und MSPs erschweren es potenziellen Angreifern somit enorm, Unternehmen mit wenig Aufwand großen Schaden zuzufügen. Eine Frage stellt sich in Bezug auf Cybersicherheitsvorfällen häufig: Wie schlimm werden die Konsequenzen sein? Mit diesen Werkzeugen und dem Einsatz weiterer Best Practices zum Schutz der Systeme, wie zum Beispiel der Erhöhung von Alarmierungskapazitäten, können MSPs bevorstehende Angriffe früher erkennen und bekämpfen. Das kann den Unterschied zwischen einem unerfreulichen Zwischenfall und der ganz großen Katastrophe bedeuten. ■

ANDRÉ SCHINDLER,
General Manager EMEA
bei NinjaOne

HZ208310 · ISSN 1868-5757 · www.datakontext.com

Dezember 6/2021

IT-SICHERHEIT

Magazin für Informationssicherheit und Datenschutz

innovative VERWALTUNG

SPECIAL

IT-Sicherheit in der öffentlichen Verwaltung

MARKT-ÜBERBLICK:
Relevante Hersteller/ Dienstleister und ihre Angebote

Cyberangriffe:
Was die öffentliche Verwaltung wirklich bedroht

Praxis:
Planvoll zum sicheren Bürgerservice

Notfallkonzepte:
IT-Sicherheit jeder Zeit im Griff

DATAKONTEXT

Behörden brauchen „Security by Design“

Stefan Mutschler

Auch wenn der von vielen Experten befürchtete Super-GAU zur Bundestagswahl 2021 ausgeblieben ist – zumindest technisch –, die Gefahr schwerwiegender Angriffe auf Behörden und Einrichtungen der öffentlichen Hand hat in diesem Jahr schwindelerregende Ausmaße angenommen. Höhepunkt in Deutschland war sicherlich die Cyberattacke auf die Server des Landkreises Anhalt-Bitterfeld. Als Folge konnte die Verwaltung keine Sozialleistungen an die rund 157.000 Bürgerinnen und Bürger des Landkreises auszahlen – auch die KfZ-Zulassungsstelle war betroffen. Die Verwaltung gab im Zuge der Attacke an, ihre Arbeit sogar fast zwei Wochen lang größtenteils einstellen zu müssen. In der Folge wurde der Katastrophenfall ausgerufen. Das Bundesamt für Sicherheit in der Informationstechnik (BSI) wurde eingeschaltet und unterstützte vor Ort. Nach Aussagen der Behörde konnten Elterngeld und Unterhaltsvorschüsse eine Zeit lang noch nicht ausgezahlt werden, auch als die Zahlung der meisten anderen Sozialleistungen wieder funktionierte.

Sicherheitslücken in Microsoft Exchange haben 2021 für Sorgenfalten bei vielen IT-Administratoren gesorgt: Hacker konnten die Internet Information Services (IIS) von Microsoft ausnutzen, unter anderem, um Mailboxen von Behörden auszuspähen.

Das sind nur zwei Beispiele, die aber verdeutlichen, wie ernst die IT-Sicherheitslage aktuell ist. Entsprechende Meldungen schüren Misstrauen in die IT bei Behörden und Bürgern gleichermaßen und erweisen sich als Bremsklotz für die ohnehin schwächelnden Digitalisierungsfortschritte in Deutschland. Speziell in der Verwaltung hat die Corona-Pandemie zahlreiche Digitalisierungsdefizite aufgedeckt. Um sie zu beheben, müssten Dienstleistungen und Prozesse flächendeckend digitalisiert werden. Die Umsetzung des Onlinezugangsgesetzes (OZG) läuft aber nur sehr schleppend. Vom Ziel, Ende 2022 575 Verwaltungsleistungen digitalisiert zu haben, ist die Staatsführung noch sehr weit entfernt.

Im Spannungsfeld zwischen dringendem Digitalisierungsbedarf und massiv gestiegenem Angriffsgeschehen in den Behörden müssen Behörden Sicherheit neu denken. Konzepte wie „Security by Design“ sind Pflicht, untermauert durch angemessene Budgets. Nur mit Sicherheit kann Digitalisierung in den Behörden zum Erfolgsmodell werden. Unser Special „IT-Sicherheit in der öffentlichen Verwaltung“ in Kooperation mit der Fachzeitschrift Innovative Verwaltung gibt wichtige Antworten zu Gefahren, Gesetzen sowie aktuellen Trends und Entwicklungen im Bereich der öffentlichen Verwaltung – angereichert mit vielen praxisnahen Lösungen.

Viel Spaß beim Lesen!

Ihr Stefan Mutschler

IMPRESSUM

IT-SICHERHEIT
Magazin für Informationssicherheit und Datenschutz

www.itsicherheit-online.com

in Kooperation mit

innovative VERWALTUNG

SPECIAL: IT-Sicherheit in der öffentlichen Verwaltung

Verlag:
DATAKONTEXT GmbH
Standort Frechen
Augustinusstr. 9d · 50226 Frechen
www.datakontext.com

Chefredaktion:
Stefan Mutschler (S.M.)
E-Mail: stefan-mutschler@t-online.de
Redaktion:
Dr. Peter Münch (P.M.),
Dr. jur. Martin Zilkens (M.Z.),
Online-Redaktion:
Jessica Herz
Leitung Online
herz@datakontext.com
+49 2234 98949 -80
Silvia Klüglich
Chiara Schönbrunn
Herausgeberbeirat:
Prof. Dr. Michael Backes, Prof. Dr. jur. Dirk-M. Barton, Walter Ernestus, Prof. Dr. Nikolaus Forgó, Prof. Dr. Rainer W. Gerling, Dr. Jan-Peter Ohrtmann, Prof. Dr. Norbert Pohlmann, Dr. jur. Martin Zilkens
Gründer: † Bernd Hentschel

Grafik/Layout/Satz:
Michael Paffenholz
Tel.: +49 173 8382572
E-Mail: michael.paffenholz@gmx.de
Objekt- und Anzeigenleitung:
Wolfgang Scharf
Tel.: +49 2234 98949-60
E-Mail: wolfgang.scharf@datakontext.com
zzt. gilt die Anzeigenpreisliste Nr. 27
Vertrieb/Herstellung:
Dieter Schulz
Tel.: +49 2234 98949-99
dieter.schulz@datakontext.com
Abonnement: Jahresabonnement € 98,- inkl. VK (Inland)

Erscheinungsweise: sechs Ausgaben
Alle Preise verstehen sich inkl. MwSt. Der Abonnementpreis wird im Voraus in Rechnung gestellt. Das Abonnement verlängert sich zu den jeweils gültigen Bedingungen um ein Jahr, wenn es nicht mit einer Frist von 8 Wochen zum Ende des Bezugszeitraumes gekündigt wird.
Erscheinungsweise, Bezugspreise und -bedingungen: Abonnement und Bezugspreis beinhalten die Print-Ausgabe sowie eine Lizenz für das Online-Archiv. Die Bestandteile des Abonnements sind nicht einzeln kündbar. Der Preisanteil des Online-Archivs ist auf der Abonnementrechnung separat ausgewiesen.
Aboservice:
Hüthig Jehle Rehm GmbH, München,
Tel.: +49 89 21 83-7110
Druck: Grafisches Centrum Cuno GmbH & Co. KG, Calbe (Saale)

Titelbild: ©jirsak - stock.adobe.com
Fotos: Firmenbilder; DATAKONTEXT; iStock.com/Kosamtu, iStock.com/metamorworks, iStock.com/StockRocketm; 2020 PaO_STUDIO/Shutterstock, ESB Professional/Shutterstock; (Gorodenkoff, nendrawahyu, nuclear_lily, Rawf8 , sasun Bughdaryan, Sergey Nivens, Suteren Studio, Suteren Studio, wigglestick) - stock.adobe.com

27. Jahrgang 2021 · ISSN: 1868-5757

Inhalt

Anbieter

Warum der öffentliche Sektor zur beliebten Zielscheibe für Cyberkriminelle wurde

Behörden unter Feuer

Stadtwerke Wismar, Europäische Arzneimittelagentur, Flughafen Saarbrücken, die schwere Cyberattacke auf die Server des Landkreises Anhalt-Bitterfeld – immer häufiger geraten Behörden und Organisationen ins Fadenkreuz von Cyberkriminellen. Kein Zweifel: Öffentliche Infrastruktur ist gefährdet. Die Verantwortlichen für IT-Sicherheit müssen hier genau hinsehen, um wirksame Sicherheitsstrategien für die Zukunft zu entwickeln.

Gerade der Angriff in Anhalt-Bitterfeld, der letztlich zum Katastrophenfall ausgerufen wurde, zeigt eindrücklich, wie digitale Angriffe ganz konkrete reale Schäden anrichten. Kritische Infrastrukturen (KRITIS), zu denen auch kommunale Verwaltungen gehören, sichern die Versorgung der Bevölkerung mit essenziellen Gütern und somit unser gesellschaftliches Wohlergehen. „Damit stellen KRITIS-Einrichtungen ein attraktives Ziel für finanziell oder politisch motivierte Angreifer, Cyberterroristen und Hacktivisten dar", so Tobias Lang, Sprecher von Myra Security.

Die Gefahr von Angriffen auf kritische Infrastrukturen steigt und gerade kleinere Kommunen in Deutschland sind oft nicht ausreichend geschützt. Das Myra Security Operations Center (SOC) verzeichnet einen deutlichen Zuwachs der Angriffe auf kritische Infrastrukturen – insbesondere in Form von DDoS-Attacken. Dies deckt sich mit der Statistik des Bundeskriminalamts, nach der seit Anfang des Jahres 2021 allgemein ein signifikanter Anstieg krimineller Cyberaktivitäten in Form von DDoS-Angriffen festzustellen ist. Vorfälle wie in Anhalt-Bitterfeld können jederzeit wieder passieren und sogar sehr viel größere Ausmaße annehmen.

Städte, Gemeinden und Kommunen waren schon oft Ziel von Ransomware-Angriffen. Rund um die Welt sind Hunderte von Städten und Kommunen – große und kleine gleichermaßen – von Ransomware betroffen. „Interessanterweise scheint es, dass größere Städte weniger häufig dazu bereits sind, das Lösegeld zu zahlen, als dies bei kleineren Städten der Fall ist", so Jonathan Couch, SVP Strategy bei ThreatQuotient.

Auf spezialisierte Dienstleister setzen

Kleinere Gemeinden und Landkreise, wie beispielsweise Anhalt-Bitterfeld, verfügen oft gar nicht erst über die notwendigen Ressourcen, um Angriffe auf ihre IT-Systeme so effektiv zu verhindern, wie es größeren staatlichen Einrichtungen oder sogar vielen kommerziellen Unternehmen möglich ist. „Hinzu kommt, dass kleine Städte ihre Netzwerke in der Regel nicht zum Schutz gegen diese Art von Angriffen konzipieren: Sie sind darauf ausgelegt, die für ihre Einwohner notwendige Dienstleistungen so effizient wie möglich für die Bürger der Stadt bereitzustellen. Sie sind unterfinanziert, haben oft veraltete Technologie und verfügen nicht über die nötigen Prozesse, um wichtige Sicherheitslücken effizient zu schließen", so Couch.

„Interessanterweise scheint es, dass größere Städte weniger häufig dazu bereits sind, das Lösegeld zu zahlen, als dies bei kleineren Städten der Fall ist."

JONATHAN COUCH,
SVP Strategy bei ThreatQuotient.
(Foto: ThreatQuotient)

Im Falle von Anhalt-Bitterfeld gilt anzumerken, dass die Schadsoftware über einen sehr populären Print-Spooler-Dienst von Microsoft verteilt wurde, für dessen Sicherung Microsoft erst kurz zuvor einen Notfallpatch veröffentlicht hat. Selbst bei einer wesentlich stärker ausgerüsteten Verteidigung hätte der Angriff mit hoher Wahrscheinlichkeit nicht verhindert werden können. Wirklich geholfen hätte zu diesem Zeitpunkt vermutlich nur die Deaktivierung des Print-Spooler-Dienstes. „Dies ist aber in Anbetracht seiner Funktion problematisch, da der Dienst bei sämtlichen Druckoperationen essentiell ist: Nicht nur ist er für die reibungslose Funktion physischer Drucker, sondern auch für PDF-, XPS- und OneNote-Dokumente notwendig", so Stefan Molls, RVP, Risk & Security bei Tanium. Er empfiehlt, dass Unternehmen den Überblick über ihre Endpunkte und deren Patchstände haben und zeitnah in der Lage sind, notwendige Patches auszurollen

„Eine Lösung für das Endpunkt-Management hilft dabei, Aktualisierungen schnell und ressourcenschonend in Umlauf zu bringen."

STEFAN MOLLS,
RVP, Risk & Security bei Tanium.
(Foto: Tanium

und zu installieren. „Hier hilft eine Lösung für das Endpunkt-Management dabei, solche Aktualisierungen schnell und ressourcenschonend in Umlauf zu bringen. Darüber hinaus kann sie ungepatchte Endpunkte isolieren, sodass im Fall einer Kompromittierung keine Horizontalbewegungen im Unternehmensnetzwerk möglich sind", so Molls.

„Der konsequente Schutz von kritischen Infrastrukturen vor Cyberattacken ist für unsere Gesellschaft elementar", so Lang. „Um ein Maximum an IT-Sicherheit zu erreichen, müssen vorhandene Schutzmaßnahmen fortlaufend überprüft und an die sich stetig verändernde Bedrohungslage angepasst werden. Spezialisierte Dienstleister können mit ihrer Erfahrung und technologischen Expertise dabei unterstützen. Gerade im öffentlichen Sektor kommt es dabei auf ein Höchstmaß an Vertrauen und Zuverlässigkeit an." Bei der Auslagerung von IT-Sicherheit im öffentlichen Sektor und im KRITIS-Bereich allgemein sind bestimmte Kriterien, wie anerkannte Zertifizierungen (zum Beispiel ISO 27001 auf Basis von IT-Grundschutz), zu beachten. Außerdem sollte der Anbieter BSI-KRITIS-qualifiziert sein und 24/7 Full-Service-Betreuung durch ein eigenes SOC bieten. Nur so können Kommunen und andere KRITIS-Einrichtungen langfristig sicherstellen, dass ihre digitalen Prozesse bestmöglich geschützt sind und die Bevölkerung zuverlässig versorgt wird.

„Im Gegensatz zu geschlossenen Systemen liegt bei Open Source meist nicht viel Zeit zwischen Entdeckung und Korrektur einer Schwachstelle."

RICO BARTH,
Geschäftsführer von cape IT

Open Source als effektive Waffe gegen Cybercrime

Dennoch: Mit immer neuen Methoden schaffen es die Cyberkriminellen an den herkömmlichen Sicherheitsmaßnahmen vorbeizukommen. Eine Abwehrmethode, die Experten für Behörden, KRITIS, Unternehmen oder privaten Computern vorschlagen, wird aber noch viel zu selten eingesetzt: Open Source. Bei solchen offenen Programmen haben alle Anwender Zugriff auf den Quellcode. Durch die Zusammenarbeit vieler Menschen und ganzer Communities können Schwachstellen schnell ausgemacht und behoben werden. „Natürlich hilft beim schnellen Patchen auch die Unterstützung großer Unternehmen, die hinter solchen Open-Source-Softwares stehen", so Rico Barth, Geschäftsführer von cape IT. „Im Gegensatz zu geschlossenen Systemen, liegt meist nicht viel Zeit zwischen Entdeckung und Korrektur. Das hätte vielleicht auch den Verantwortlichen der Uniklinik Düsseldorf geholfen." Ein Cyberangriff dort hatte im Herbst 2020 einen Todesfall zur Folge. In einer Pressemitteilung schrieb das Krankenhaus: „Die Sicherheitslücke befand sich in einer marktüblichen und weltweit verbreiteten kommerziellen Zusatzsoftware. Bis zur endgültigen Schließung dieser Lücke durch die Softwarefirma war ein ausreichendes Zeitfenster gegeben, um in die Systeme einzudringen."

Auch Andrea Wörrlein, Geschäftsführerin von VNC in Berlin und Verwaltungsrätin der VNC AG in Zug (Schweiz) setzt auf Open Source: „Eine entsprechende Zeitenwende ist in Städten und Kommunen unverzichtbar". Grund: „Die öffentliche Verwaltung ist verpflichtet, die Daten ihrer Bürger zu schützen. Dies ist nicht mit einer Closed-Source-Lösung machbar", so Wörrlein.

Hacker an Bord holen

Andernorts geht man bei der Aufrüstung der Verteidigung öffentlicher Stellen ganz neue Wege. Das britische Verteidigungsministerium (Ministry of Defence, MoD) etwa suchte dafür im August 2021 die Zusammenarbeit mit Hackern in Form eines Bug-Bounty-Wettbewerbs. Bei dem Programm handelte es sich um einen 30-tägigen, von Hackern durchgeführten Sicherheitstest, der darauf abzielte, Schwachstellen aufzudecken, bevor sie von Gegnern ausgenutzt werden können. Aufgrund der Ergebnisse der sogenannten Integrated Review der britischen Regierung[1] hat diese sich zu „einer stärkeren Position in Sachen Sicherheit und Widerstandsfähigkeit" sowie „einem Fokus auf Offenheit als Quelle des Wohlstands" bekannt. „Regierungen auf der ganzen Welt werden sich zunehmend der Tatsache bewusst, dass sie ihre riesigen, digitalen Umgebungen nicht mehr mit traditionellen Sicherheitstools schützen können", sagt Marten Mickos, CEO von Hackerone, Partner des britischen Verteidigungsministeriums bei der Durchführung des Wettbewerbs. „Ein formelles Verfahren zur Meldung von Schwachstellen durch Dritte wird weltweit als Best Practice angesehen, und die US-Regierung hat es in diesem Jahr für ihre zivilen Bundesbehörden sogar zur Pflicht gemacht. Das britische Verteidigungsministerium ist Vorreiter in der britischen Regierung ... Ich gehe davon aus, dass weitere Regierungsbehörden diesem Beispiel folgen werden." ■

S.M.

Quellen

[1] https://www.gov.uk/government/publications/global-britain-in-a-competitive-age-the-integrated-review-of-security-defence-development-and-foreign-policy

Ausnahmesituation „IT-Sicherheitsvorfall“ jederzeit im Griff

Warum Security durch externe Dienstleister unterstützt werden sollte

Ein Unternehmen, das sich unvorbereitet inmitten eines ausgewachsenen IT-Notfalls wiederfindet, hat meist das erste Mal mit einem solchen Ausnahmezustand zu kämpfen. Das Geschehen kann binnen Minuten vom „Normalbetrieb“ zu „Komplettstillstand“ umschlagen. Damit sind die meisten IT-Abteilungen in kleinen und mittelständischen Unternehmen, ebenso wie in Behörden, rettungslos überfordert. Notfallpläne – sofern diese existieren – sind vielfach entweder veraltet oder wurden nie geprobt. Ein geeigneter Dienstleister kann eine Notsituation schon im Vorfeld entschärfen.

Der Alltag eines Incident Responders ist geprägt von wiederkehrenden Mustern. Ein Kunde, der sich wegen eines Incidents meldet, hat gerade ein echtes Problem. Dabei steht oft der Fortbestand des Betriebs auf dem Spiel. Entsprechend hat der Erstkontakt meist auch eine sehr emotionale Komponente. Angst, Ärger und Verunsicherung spielen hier eine wesentliche Rolle. So verständlich diese Emotionen auch sein mögen, so hinderlich sind sie oftmals in der Praxis.

Vor Ort im Unternehmen erwartet die Incident Responder oft eine Mischung aus veralteten Dokumentationen, gescheiterten eigenen Versuchen, der Krise Herr zu werden, widersprüchlichen Informationen, ungeklärten Zuständigkeiten und technischen Schulden, die teilweise über Jahre angewachsen sind. Ein Zwischenfall, wie ein netzwerkweiter Befall mit Ransomware, setzt alle Beteiligten unter immensen Stress. Mitarbeitende können Aufgaben nicht fertigstellen, das Unternehmen riskiert einen Reputationsverlust und mit jeder Stunde Stillstand häufen sich die Kosten für Produktionsausfälle – um nur einige der Faktoren zu nennen, die Unternehmerinnen und Unternehmer in einer solchen Situation umtreiben. In Behörden steht die Versorgung der Gemeinde auf dem Spiel. Eine spontan auftretende Krise legt in geradezu brutaler Schonungslosigkeit Versäumnisse aus der Vergangenheit offen. Einige davon sind individuell betrachtet vielleicht nicht alleinursächlich für eine aktuelle IT-Krise, doch in Summe kumulieren sie zu einem „perfekten Sturm“.

Sicherungsmaßnahmen oft nur teilweise umgesetzt

Dabei ist es in der Regel nicht so, dass es überhaupt keine Sicherungsmaßnahmen gibt – sie sind jedoch nur teilweise umgesetzt oder nicht konsequent zu Ende gedacht. Ein praktisches Beispiel sind etwa Logging-Server, die Aufzeichnungen über bestimmte Aktivitäten vorhalten sollen. Bereits hier lauern die ersten Stolpersteine, denn in zahlreichen Fällen sind Logdaten entweder nicht vorhanden oder unvollständig. In beiden Fällen ist deren Nutzen zur Aufarbeitung eines sicher-

heitskritischen Vorfalls stark eingeschränkt. Das gilt vor allem dann, wenn es nicht genügend historische Daten gibt. Fälle, in denen die ältesten Logdaten nur wenige Stunden alt waren, sind keine Seltenheit.

Um aussagekräftige Informationen zu haben, ist ein Datenbestand von mindestens sechs Monaten eine gute Ausgangsbasis. Da Angreifer sich schlimmstenfalls monatelang unbehelligt in einem Netzwerk bewegen können, sind Abweichungen in bestimmten Verhaltensmustern besser erkennbar. Fehlen diese Daten oder sind sie unvollständig, ist es schwerer, Abweichungen von der Norm zuverlässig auszumachen. Sind die ältesten Logdaten nur wenige Stunden oder Tage alt, sind Bewertungen zu Abweichungen nahezu unmöglich.

Aktive Helfer, statt stumme Zeugen

Selbst dort, wo Logdaten eigentlich vorhanden wären, bleibt dieser Informationsschatz allzu oft unbeachtet, weil niemand die Logdaten auswertet. Praxisbeispiel: Der Virenscan hat schädliche Dateien zwar erkannt und gelöscht – dennoch hat den Rest des Angriffs niemand bemerkt, weil lediglich ein Teil der maliziösen Dateien des Angriffs erkannt wurde. Zwar lassen sich die vorhandenen Logdaten im Nachhinein zur Analyse nutzen, um den Verlauf eines Vorfalls so gut wie möglich zu rekonstruieren, aber dennoch handelt es sich wieder um eine reine Post-mortem-Untersuchung. Dabei könnten Protokolldateien, die regelmäßig und automatisch ausgewertet werden, einen wesentlichen Beitrag zur Verhinderung eines Zwischenfalls leisten, statt nur im Nachgang als „stumme Zeugen" aufzutreten. Allein das Einrichten und Umsetzen einer Logging-Strategie braucht Fingerspitzengefühl. Ansonsten drohen wirklich wichtige Informationen im „Hintergrundrauschen" unterzugehen. Umso schwerer wird es, wenn ständige Falschmeldungen für Alarmmüdigkeit sorgen. Es ist wie mit einem Feueralarm: Wenn bereits fünf Mal binnen eines Tages der Feueralarm für eine komplette Evakuierung des Büros gesorgt hat, dann wird sehr wahrscheinlich beim sechsten Mal niemand mehr seinen Arbeitsplatz verlassen und Alarme ignorieren – bis es einmal wirklich brennt. Und dann bricht Panik aus.

Entgegen einem weit verbreiteten Irrglauben verhält sich die Höhe der Ausgaben für Sicherheit jedoch nicht proportional zum Sicherheitslevel. Die Erkenntnis, dass IT-Sicherheit inzwischen weit mehr ist als ein Nebenschauplatz, setzt sich immer weiter durch. Vorhandene Mittel klug zu nutzen und zusätzlich eine unabhängige Partei in den Sicherheitsprozess einzubinden, ist in vielen Fällen die weitaus bessere Alternative.

Unternehmen und Behörden finden sich hier in einem Dilemma wieder. Zwar steigen die Anforderungen an die Sicherheit, die zur Verfügung stehenden Mittel stagnieren jedoch vielfach. Eigene qualifizierte Sicherheitsspezialisten einzustellen, ist aus verschiedenen Gründen nicht immer sinnvoll. Zumal solche am Arbeitsmarkt auch eher dünn gesät und entsprechend teuer sind.

IT-Sicherheit in den Händen von Experten

In dieser Situation ist es naheliegend, die IT-Sicherheit in die Hände externer Spezialisten zu legen. Diese verfügen nicht nur über das nötige Fachwissen, sondern können auch bei der Planung und Umsetzung wertvolle Unterstützung leisten, während eine interne IT-Abteilung sich dem operativen Geschäft widmen kann. Auch kleine Unternehmen können von dieser Dienstleistung profitieren. Hier laufen alle Fäden zusammen. Die Unternehmens-IT bekommt nur dann eine Meldung oder einen Report, wenn es wirklich relevant ist.

Für den Notfall können Unternehmen und Behörden ebenfalls vorsorgen, indem bereits so früh wie möglich eine Kooperation mit einem auf IT-Sicherheit spezialisierten Dienstleister auf den Weg gebracht wird. Falls ein Sicherheitsvorfall eintritt, sind im Bedarfsfall binnen Stunden Spezialisten vor Ort, die das Netzwerk kennen und die wissen, was zu tun ist. Diese Vorbereitung spart im Notfall wertvolle Zeit. Schon im Vorfeld lassen sich in Kooperation mit Experten Notfallpläne entwickeln, welche die Schäden im Fall des Falles minimieren und die Handlungsfähigkeit der Organisation sicherstellen. Das kann zum Beispiel in Form eines entsprechenden Incident Response Retainers sein. Die Kosten sind hier kalkulierbar, und in einem Notfall steht ein Expertenteam sofort bereit.

Generell gilt: Wer von außen einen Blick auf bestehende Strukturen wirft, sieht dort Probleme, die von innen heraus oft nicht auffallen. Diese „Betriebsblindheit" ist normal und lässt sich mit diesem unabhängigen Blick eliminieren. Schwierigkeiten lassen sich in vielen Fällen schnell und einfach, vor allem aber mit bestehenden Mitteln, lösen. Praktisches Beispiel: Die Behandlung von Makros in Microsoft-Office-Dateien. Diese stellen mittlerweile einen geradezu klassischen Einfallsvektor für viele Arten von Schadsoftware dar. Kaum jemand scheint jedoch zu wissen, dass sich etwa in einer Active-Directory-Domäne solche unsignierten Makros mittels einer einfachen Gruppenrichtlinie komplett deaktivieren lassen, ohne dass ein Nutzer diese Einstellung für sich ändern könnte. Wer im Arbeitsalltag nicht zwingend auf den Einsatz von Office-Makros angewiesen ist, kann und sollte diese deaktivieren. Und dort, wo Makros unverzichtbar sind, lassen sich diese mittels digitaler Signaturen zuverlässig erkennen und so von externen, potenziell gefährlichen unterscheiden.

Wer mit einem ausschließlich auf IT-Sicherheit spezialisierten Dienstleister kooperiert, investiert langfristig in die Sicherheit des eigenen Unternehmens. Und die Kosten dafür machen sich bereits nach einem verhinderten Incident bezahlt. ■

Jasper Bongertz,
Experte für Netzwerksicherheit mit Fokus auf Netzwerkforensik und Incident Response bei G DATA Advanced Analytics GmbH

Cybercrime gegen Behörden

IT-Sicherheit als permanenter Prozess statt nur Maßnahme

Gegenüber der ständig wachsenden Bedrohung durch Cyberkriminelle müssen öffentliche Einrichtungen, Behörden und Organisationen neue Sicherheitsstrategien entwickeln und IT-Sicherheit als permanenten Prozess begreifen.

Stadtwerke Wismar, Europäische Arzneimittelagentur, Flughafen Saarbrücken – immer häufiger geraten Behörden und Organisationen ins Fadenkreuz von Cyberkriminellen. Kein Zweifel: Öffentliche Infrastruktur ist gefährdet. Die Verantwortlichen für IT-Sicherheit müssen hier genau hinsehen, um wirksame Sicherheitsstrategien für die Zukunft zu entwickeln.

Komplexere IT, anspruchsvollere IT-Sicherheit

Mobility, Cloud, Internet of Things: IT-Landschaften werden immer komplexer und verändern sich durch neue Nutzer, Dienste und Geräte sowie virtuelle und softwaredefinierte Infrastrukturen permanent. Daraus entstehen neue Risiken und das verlangt von den jeweiligen Organisationen, die IT-Security anpassungs- und zukunftsfähig zu gestalten.

Die Zahl der Cyberangriffe – welcher Art auch immer – ist im letzten Jahr rapide gestiegen. In einer Anfang 2021 veröffentlichten Studie der International Data Group (IDG) gaben 66 Prozent der Befragten IT-Manager an, gerade auch im Homeoffice seien die Mitarbeitenden zunehmenden Cyberrisiken ausgesetzt. 31 Prozent behaupteten sogar, die Beschäftigten arbeiteten zu Hause mit ungeschützten Geräten. Die IT-Helpdesks haben dadurch immer mehr Probleme, die Mitarbeitenden zu schützen. Es gilt jedoch, durch das neue „Work-from-Anywhere" den Zugang der User zu ihren Ressourcen zu erleichtern und die Cyberrisiken zu minimieren.

Der wichtigste Schritt dahin ist zunächst, das Sicherheitsbewusstsein zu erhöhen. Egal, ob Mitarbeitende zu Hause oder im Büro ans Werk gehen, ihnen muss klar sein, welche Gefahren von böswilligen Hackern ausgehen und welche Schritte und Tools zur Bekämpfung eingesetzt werden können. Wichtig ist dabei, dass die Mitarbeitenden nicht nur entsprechend geschult werden, sondern dass das Thema Sicherheit fest in der Kultur der Organisation verankert ist. Nur so können IT-Manager sicherstellen, dass sich ihre User während der gesamten Arbeitszeit vorsichtig verhalten und keine Sicherheitspannen durch Leichtsinnsfehler entstehen.

Passwort-Management als Lösungsansatz

Einer der wirklich robusten Schritte in Sachen IT-Sicherheit ist ein starkes Passwort-Management. Passwörter zählen noch immer in vielen Organisationen zu den größten Sicherheitslücken. Viele Nutzer verwenden dasselbe, unsichere Passwort über verschiedene Anwendungen hinweg. Und am beliebtesten ist leider noch immer das berüchtigte „123456". Deshalb müssen Organisationen Kontrolle über die Passwörter-Verwendung durch Mitarbeitende haben, um einen Verstoß rechtzeitig zu verhindern, aber gleichzeitig keine Mehrarbeit für die Nutzer zu verursachen. Dafür gibt es zahlreiche Lösungen.

Eine davon kann sicherlich ein solider Passwort-Manager sein. Er verwaltet alle Passwörter, die individuell für ein Konto erstellt werden, in einem sicheren Tresor, der nur über ein starkes Master-Passwort des Users zugänglich ist. Die Mitarbeitenden müssen sich also nur ein Passwort merken. So wird vermieden, dass diese ihre Passwörter unsicher gestalten oder mehrfach für verschiedene Anwendungen verwenden.

Doch professionelle Tools für die IT-Sicherheit sind heutzutage mehr als reine Passwort-Management-Lösungen. So spielt auch das Thema IT Reporting für mehr Transparenz und einen besseren Service eine zunehmend wichtiger werdende Rolle. Mitarbeitende werden zum Beispiel benachrichtigt, sobald Daten bedroht sind. Auf diese Weise kann kontinuierlich überwacht werden, ob E-Mail-Adressen in einer Datenbank gehackter E-Mail-Adressen auftreten.

Zudem bieten solche Lösungen auch weitere Funktionen, um die IT-Sicherheit zu stärken, beispielsweise Single Sign-on (SSO) oder Multi-Faktor-Authentifizierung (MFA). Mit SSO kann die Anzahl der Passwörter, die Mitarbeitende erstellen, sich merken und verwalten müssen, erheblich reduziert werden. SSO verbindet einen Mitarbeitenden sicher mit den Anwendungen, die ihm zugewiesen wurden, ohne dass er ein Passwort eingeben muss. Ist SSO mit einem Passwort-Manager verbunden, kann eine Organisation, Behörde oder Verwaltung die vollständige Kontrolle über sowohl die Passwörter als auch den Benutzerzugriff erreichen. So bekommen die Logins eine zusätzliche Sicherheitsstufe. Und: MFA geht hier noch einen Schritt weiter. Hier ist es zum Einloggen erforderlich, neben dem Passwort auch einen Code einzugeben, der an ein anderes Gerät des Nutzers oder über Biometrie – zum Beispiel den Fingerabdruck – geschickt wird. Nur mit Eingabe dieses zweiten Faktors wird der Anmeldevorgang abgeschlossen.

Das gut gesicherte Virtual Private Network (VPN)

In der erwähnten IDG-Umfrage gaben 45 Prozent der IT-Verantwortlichen auch an, dass Mitarbeitende auf ungesicherte WLAN-Netze zugreifen. Daher ist es wichtig, auch den Zugang zum Netzwerk des Unternehmens beziehungsweise der Behörde abzusichern. Ein Virtual Private Network (VPN) ist hier ein unverzichtbares Werkzeug für Organisationen auf der ganzen Welt geworden.

Durch die einfache Nutzung, einen einzigen Zugangspunkt und eine sichere Datenübertragung schafft die VPN-Technologie hohe Akzeptanz. Allerdings bergen genau diese Eigenschaften auch ein hohes Potenzial für Cyberangriffe. Mit nur einem einzigen Satz gestohlener Log-in-Daten oder einem durch Malware kompromittierten Computer kann sich ein Hacker Zugang zu sensiblen Daten im Netzwerk einer Organisation verschaffen – und es im schlimmsten Fall komplett kapern. Daher braucht auch ein VPN eine zusätzliche Absicherung. Mit MFA lässt sich die Sicherheitsebene verdoppeln. Damit wird vermieden, dass sich unberechtigte Personen Zugang zum Netzwerk verschaffen, ohne zusätzliche Komplexität für die Mitarbeitenden zu kreieren.

Ausblick: Was bringt die Zukunft der IT-Sicherheit?

Kein Zweifel: Es ist ein Wettrüsten im Gange, mit dem wir alle leben müssen. Cyberkriminelle und Cyberbedrohungen werden sich weiterentwickeln und Angreifer häufiger, schneller und perfider zuschlagen. Auch öffentliche Verwaltungen und Behörden werden sich deshalb permanent Gedanken machen müssen, welche Sicherheitsmaßnahmen in Zukunft notwendig sind und welche Verantwortungen sie selbst und welche ihre Security-Anbieter übernehmen müssen, um Daten, Infrastrukturen und Nutzer optimal zu schützen.

Fakt ist: Technologiebasierte Cybersicherheitspraktiken werden sich kontinuierlich weiterentwickeln. Behörden und ihre Dienstleister müssen in der Lage sein, riesige Mengen an Vorfallsdaten, fehlerhaften oder doppelten Datensätzen, eine Vielzahl von Malware-Mustern über Tausende von Protokollen zu bewältigen. Schon in naher Zukunft werden hier mit Sicherheit künstliche Intelligenz (KI) und Machine Learning eine wichtigere Rolle spielen, um schneller und zuverlässiger kriminelle Muster bei großen Datenmengen zu erkennen und entsprechend frühzeitig Warnungen zu generieren.

Diese Dynamik macht klar: IT-Sicherheit wird in Zukunft als permanenter Prozess begriffen werden müssen, und nicht lediglich als einzelne Maßnahme. ■

Tobias Becker,
Manager, Enterprise Sales DACH,
LogMeIn

Die wichtigen IT-Sicherheitsaspekte in der öffentlichen Verwaltung

Planvoll zum sicheren Bürgerservice

Nicht nur der zeitlich beschleunigte Übergang zum Homeoffice im Jahr 2020 und 2021 hat Kommunen und die öffentliche Verwaltung auf Bundes- und Landesebene vor große Herausforderungen gestellt. Auch die Zunahme von Cyberangriffen und grundsätzlich die komplexe Bedrohungslage im Umfeld von Behörden und Ministerien wurden zu einem echten Prüfstein. Was genau die öffentliche Verwaltung jetzt tun muss.

Erst im Oktober hat das Bundesamt für Sicherheit in der Informationstechnik (BSI) in seinem Bericht „Die Lage der IT-Sicherheit in Deutschland 2021" über die aktuellen Bedrohungen im Cyberraum informiert und die Situation in Deutschland als „angespannt bis kritisch" eingestuft. Hierbei spielen auch die Folgen für veränderte Arbeitssituationen, wie Homeoffice oder „Work from Anywhere", eine herausfordernde Rolle.

Verantwortung für unterbrechungsfreie Bürgerservices

Die öffentliche Verwaltung besitzt eine essenzielle Verantwortung und muss zu jeder Zeit die bedeutenden Services für Land und Bevölkerung aufrechterhalten und unterbrechungsfrei gewährleisten. Dabei steigt der Druck auf IT-(Security-) Teams, die für die Sicherstellung der Geschäftskontinuität bei gleichzeitiger Sicherheit zuständig sind.

Cyberangriffe auf kommunale Verwaltungen können weitreichende Konsequenzen haben, wenn etwa Bürgerservices über längere Zeit nicht zur Verfügung stehen und dadurch teils monatelange Auswirkungen im Betrieb spürbar werden. Dies reicht von Services wie der Beantragung einer Geburtsurkunde, über den Kauf einer Immobilie bis hin zur Anmeldung eines Kraftfahrzeugs.

Welche Überlegungen jetzt anzustellen sind

Um gar nicht erst zum Opfer eines Cyberangriffs zu werden, müssen sich die verantwortlichen Teams und Entscheider Gedanken machen, wie sie vorbeugen können. Als größtes bekanntes Risiko stehen vor allem die eigenen Mitarbeiter und deren Information und Sensibilisierung in IT-Sicherheitsbelangen im Mittelpunkt.

Auch aktuelle Trendthemen, wie Zero Trust, spielen eine Rolle, wenn sich Verwaltungen nicht nur für die Gegenwart, sondern auch zukunftssicher aufstellen möchten. Eine ganzheitliche Betrachtung ist hierbei entscheidend. Die richtigen Überlegungen drehen sich also um die Fragestellungen, wie man sein Netzwerk, die Mitarbeiter (User), Daten, Zugriffe und Geräte so absichert, dass die Kommune als Ganzes geschützt ist:

Benutzerverwaltung

Ein sehr guter und sicherer Weg ist die Kopplung einer IT-Sicherheitslösung mit dem favorisierten, im Einsatz befindlichen Verzeichnisdienst wie beispielsweise dem Active Directory (AD) oder anderen. So wird auf einfache Weise ein automatisiertes und synchrones User-/Gruppen- und Rechte-Konzept etabliert.

Dies bedeutet, dass für jeden einzelnen User, für Gruppen oder gesamte Organisationseinheiten, wie Referate oder Fachabteilungen, dedizierte Zugriffsrechte und Attribute zentral und automatisiert vergeben und auch gelöscht werden können.

Wenn beispielsweise Mitarbeiter die Verwaltung verlassen sollten, wird dies besonders wichtig. Sobald der User im AD gelöscht wird, erlöschen auch sämtliche Zugriffsrechte im Netzwerk automatisch und werden gesperrt. Dadurch wird eine Kompromittierung durch einen alten Account verhindert und Angriffsszenarien eines sogenannten „kalten“ Accounts von vornherein ausgeschlossen.

Authentifizierung/Authentisierung

Bei allen Themen rund um Authentifizierung sollten User und Geräte gleichermaßen betrachtet werden. Für Mitarbeiter im Homeoffice sollte beispielsweise mindestens eine Zwei-Faktor- (2FA) oder besser eine Multi-Faktor-Authentifizierung eingesetzt werden.

Nach der Regel „wissen und besitzen“ ist so ein höheres Security-Level erreichbar – typisches Beispiel ist ein Remote-Access-User. Dieser meldet sich mit Benutzernamen und Passwort an und muss als zweiten Faktor einen sicheren, zeitbasierten Token, wie ein Time-based One-time Password (TOTP), eingeben. Somit kann sich ein Angreifer mit einem erbeuteten Passwort ohne den zusätzlichen Token nicht verbinden und erlangt keinen Zugriff.

Darüber hinaus können zum Beispiel über dedizierte Maschinenzertifikate auch die verwendeten Geräte, wie Laptops, entsprechend identifiziert werden. Damit ist für die IT zu jeder Zeit sichergestellt, dass es sich bei dem verwendeten Gerät um ein bekanntes und sicheres handelt.

Endpoint Security / Policy Enforcement

Gerade bei Remote-Zugriffen ist es besonders wichtig, höchstmögliche Sicherheit zu gewährleisten. Neben dem User muss auch das Endgerät unter die Lupe genommen werden, mit dem auf Unternehmensdaten zugegriffen wird.

Genau hierfür gibt es adäquate Technologien und Features, die bereits beim Aufbau eines verschlüsselten Tunnels eine Vielzahl von sicherheitsrelevanten Paramatern überprüfen. Hierbei können das aktuelle Patch-Level des Betriebssystems, Zertifikatsgültigkeiten, aktuelle Virendefinitionen oder gar Dienstinformationen auf dem Endgerät gecheckt werden. Sogar technisch vollautomatisierte Compliance ist so einfach realisierbar.

Ganz besonderes Augenmerk sollte bei diesem sogenannten Endpoint Policy Enforcement auf eigene Anpassbarkeit (Customizability) gelegt werden, um in der Lage zu sein, individuelle Policies (Regeln) zu definieren, die automatisch bei allen Usern und Gruppen Anwendung finden. Bedeutsam ist dies vor allem dann, wenn flexibel und schnell auf sich ändernde Situationen reagiert werden muss.

Network-Filtering

Um die Hoheit über die eigene Infrastruktur und das Netzwerk inklusive aller Assets zu sichern und zu behalten, sind detailliert definierte Filter für die User ausschlaggebend. Hierbei sollte granular konfiguriert werden, welche Netzwerk-Assets, -Ressourcen, -Daten, -Anwendungen und -Bereiche für User zugänglich sein sollen und welche nicht. Durch ein solch professionelles Vorgehen hat die IT alle Fäden zentral in der Hand und kann sich zu jeder Zeit sicher sein, dass es keine unbefugten Zugriffe oder fehlerhaftes Nutzerverhalten gibt.

Netzwerksegmentierung/Mikrosegmentierung

Damit ein User nur auf relevante Assets im Netzwerk zugreifen kann, sind die Zugriffe bei der Segmentierung des eigenen Netzwerks und insbesondere bei der Mikrosegmentierung wie folgt zu steuern: im Incident-Fall, also im Fall eines erfolgreichen Angriffs, wie zum Beispiel einer Ransomware-Attacke, muss dieser Angriff absolut isoliert bleiben, damit er sich nicht im Netzwerk ausbreitet.

Durch dieses Vorgehen lassen sich Schäden erheblich verringern und Auswirkungen schnell beheben, denn es ist immer nur ein kleiner Teilbereich des Netzwerks betroffen.

Diese und andere Aspekte sind immens wichtig, um den Bedrohungen und Herausforderungen im Cyberraum Rechnung zu tragen. Wie bei persönlichen Versicherungen gilt auch hier der Grundsatz: „Haben ist besser als brauchen“! ■

Benjamin Isak,
Director Sales Public & Defence bei NCP

Warum die öffentliche Verwaltung die Sicherheit ihrer Daten in den Mittelpunkt stellen muss

Cyberangriffe werden gezielter und gefährlicher

Auch wenn Ransomware derzeit die Schlagzeilen beherrscht, ist sie nur die Spitze des Eisbergs von Sicherheitsrisiken, denen sich öffentliche Verwaltungen ausgesetzt sehen: Cyberkriminelle und staatlich unterstützte Angreifer nehmen in jüngster Zeit vermehrt Universitäten, Forschungs- und Regierungseinrichtungen ins Visier. Und als ob dies alles noch nicht reichen würde, darf auch, gerade wenn es um sensible Informationen geht, die Gefahr durch Insider nicht außer Acht gelassen werden.

Größer könnte die Bandbreite der getroffenen Ziele kaum sein: Die Landtage von Sachsen-Anhalt und Mecklenburg-Vorpommern, Landesministerien, Gerichte, Polizeidienststellen, Schulen, Universitäten und Krankenhäuser wurden in der jüngsten Zeit Opfer von Ransomware-Attacken. Immer häufiger steht die öffentliche Verwaltung im Fokus von Cyberkriminellen, die Daten verschlüsseln, um auf diese Weise ein Lösegeld zu erpressen. Dabei ist keine Organisation zu klein oder zu groß – so reichen die betroffenen Stadt- beziehungsweise Gemeindeverwaltungen von Frankfurt am Main über Neustadt am Rübenberge bis ins unterfränkische Dettelbach. Die Folge: Geschlossene Bürgerämter [1], verschobene Operationen und ein enormer Arbeits- und Kostenaufwand.

Ransomware ist derzeit weltweit wohl das größte Übel der Digitalisierung. Wie Recherchen des Bayerischen Rundfunks und „Zeit Online" ergaben, wurden in den letzten sechs Jahren mehr als 100 deutsche Behörden und öffentlichen Einrichtungen Opfer von Ransomware[2]. Weltweit beträgt die Schadenssumme durch Kryptotrojaner Schätzungen zufolge mehr als 20 Milliarden US-Dollar. Wesentlich für diesen „Siegeszug" ist sicherlich die ständige Anpassung der Techniken und Taktiken seitens der Angreifer. Dies gilt sowohl für die Auswahl der Opfer als auch für die Vorgehensweise: Früher folgten Ransomware-Angriffe meist dem Gießkannen-Prinzip. Heute dringen Angreifer gezielt und sehr subtil in Organisationen ein, um an wertvolle, sensible Informationen zu gelangen. Sie gehen unauffällig vor, indem sie – oftmals durch Phishing gewonnene – Anmeldedaten autorisierter Benutzer verwenden, um nach wichtigen Informationen zu suchen. Oder sie nutzen sie, um innerhalb des Netzwerks mehr Rechte zu erhalten, bevor sie Daten stehlen, verschlüsseln und ein Lösegeld fordern. Einen regelrechten Boom erlebte die Angriffsart durch das Geschäftsmodell der Ransomware-as-a-Service. Hier benötigen Cyberkriminelle kein eigenes spezifisches Know-how und können Technik und Dienstleistungen mieten.

Nach wie vor unterschätzt: Insider-Bedrohungen

Wenngleich Ransomware derzeit wohl die prominenteste Cyberbedrohung darstellt, sehen sich öffentliche Verwaltungen auch weiteren Risiken ausgesetzt. Oftmals wird dabei die Gefahr aus dem Inneren unterschätzt. So sollen beispielsweise interne Informationen der Staatsanwaltschaft im Fall Attila Hildmann[3] von einer Mitarbeiterin der IT-Abteilung und System-Administratorin bei der Staatsanwaltschaft an den Beschuldigten weitergegeben worden sein. Und trotz dieser enormen Gefahr, insbesondere was die Reputation und das Vertrauen in staatliche Organisationen anbelangt, bleiben Insider-Vorfälle ein heikles, mitunter unangenehmes Thema. Niemand möchte seine Mitarbeiter unter einen Generalverdacht stellen. Trotzdem gibt es gute Gründe, sich diesem Risiko zu stellen und es entsprechend zu adressieren: Der 2021 Data Breach Investigations Report von Verizon[4] hat gezeigt, dass bei gut einem Viertel aller Sicherheitsverletzungen Insider involviert waren.

Dabei handelt es sich bei Insider-Vorfällen nicht immer um gezielte, böswillige Aktionen. Die meisten Mitarbeiter wollen in erster Linie möglichst einfach und bequem ihre Arbeit erledigen. Hierbei halten sie sich jedoch nicht zwingend an die entsprechenden Richtlinien, die den Umgang mit Daten regeln. So teilen sie Dateien oder speichern sie auf gemeinsam genutzten oder vernetzten Laufwerken, ohne sich bewusst zu sein, welche weitreichenden Folgen das haben könnte.

Spionage im 21. Jahrhundert: Staatlich unterstützte Cyberangriffe

Schließlich sehen sich öffentliche Einrichtungen auch gezielten Spionage-Versuchen ausländischer, staatlich geförderter Angreifer ausgesetzt. Die Ziele reichen hier von Bundestagsabgeordneten bis hin zu Universitäten und Forschungseinrichtungen. Die Angriffe sind meist sehr ausgefeilt und bleiben oftmals lange Zeit unbemerkt. So wurde eine Attacke auf 23 Hochschulen[5] in Deutschland erst nach Jahren entdeckt, deren Ziel Forschungsergebnisse, Dissertationen und Konferenzberichte waren. Im Fall des Angriffs auf den Bundestag im Jahr 2015 verfügten die Angreifer gemäß einer Einschätzung des Bundesnachrichtendienstes[6] über „eine hohe bis punktuell sehr hohe Fachexpertise" sowie „große Finanzmittel und personelle Ressourcen". Diese stehen meist unterfinanzierten und unterbesetzten IT-Abteilungen gegenüber.

Das Ziel aller Angriffe: Daten

Was haben diese drei grundverschiedenen Angriffsarten gemeinsam? In ihrem Zentrum stehen stets die Daten: Sie sind das eigentliche Ziel der Angreifer. Entsprechend müssen sie in den Mittelpunkt der Sicherheitsstrategie gestellt werden und zu jedem Zeitpunkt dort geschützt werden, wo sie sind – sei es lokal oder in der Cloud.

Im Grunde lässt sich die Datensicherheit auf drei scheinbar einfache Fragen reduzieren: Wissen wir, wo unsere wichtigen Daten gespeichert sind? Haben nur die richtigen Personen Zugang zu den Daten? Und ist gewährleistet, dass die Daten korrekt verwendet werden? Drei einfache Fragen, die jedoch von den meisten Sicherheitsverantwortlichen erschreckenderweise nicht mit „Ja" beantwortet werden können. Wenn die Antwort nur einmal „Nein" lautet, sind die Daten nicht sicher. Transparenz in die Zugriffsrechte und Datennutzung wird so zum Schlüssel. Nur wenn man weiß, wer wann auf welche Dateien zugreift, lässt sich erkennen, ob es sich um eine legitime Nutzung oder um Anzeichen eines Angriffs oder Missbrauchs handelt. Um zu erkennen, welche Daten überhaupt wichtig beziehungsweise sensibel sind, und um Datenmissbrauch zu identifizieren, führt kein Weg an der Klassifizierung aller Dateien auf den Fileservern vorbei. Ohne Klassifizierung können die drei oben genannten einfachen Fragen nicht beantwortet werden.

Die traurige Wahrheit ist, dass es Angreifer immer hinter den Perimeter, also hinter die traditionell stark gesicherten Grenzen der Unternehmensinfrastruktur, und in die Systeme schaffen werden. Die entscheidende Frage ist dann, wie man mit diesem unvermeidlichen Feind im Inneren umgeht. In erster Linie kommt es darauf an, den Schaden zu reduzieren, den ein Eindringling verursachen kann. Hierbei spielen Zugriffsrechte die entscheidende Rolle. Untersuchungen zeigen, dass ein Mitarbeiter im Durchschnitt Zugriff auf mehrere Millionen Dateien hat. Wird ein solches Konto etwa durch Phishing korrumpiert, hat auch der Angreifer Zugriff auf Millionen Dateien. Diesen enormen Explosionsradius gilt es gemäß dem Least-Privilege-Ansatz auf ein Minimum zu reduzieren. Demnach können Mitarbeiter nur auf die Dateien zugreifen, die sie auch tatsächlich für ihre Arbeit benötigen. Auf diese Weise ist die Gefahr zwar nicht vollständig gebannt, das Risiko und das Ausmaß jedoch bereits deutlich reduziert. Kommt dann noch die intelligente Analyse des Nutzerverhaltens hinzu, die auffälliges Verhalten wie das reihenweise Öffnen, Kopieren oder Verschlüsseln von Daten erkennt, oder Zugriffe zu unüblichen Zeiten oder von verdächtigen Orten identifiziert, lassen sich Angriffe nahezu aller Art frühzeitig erkennen und automatisiert stoppen. ■

Quellen

[1] https://www.behoerden-spiegel.de/2021/10/18/ransomware-angriff-auf-landesverwaltung/

[2] https://www.tagesschau.de/investigativ/br-recherche/ransomware-103.html

[3] https://www.handelsblatt.com/politik/deutschland/rechtsextremismus-hildmann-rechnete-mit-verhaftung-hatte-er-noch-mehr-spitzel-in-der-berliner-justiz/27759016.html?ticket=ST-8233713-KMjzaKunGxlQnuNgqfht-cas01.example.org

[4] https://www.verizon.com/business/en-au/resources/reports/dbir/

[5] https://www.spiegel.de/lebenundlernen/uni/iranische-hacker-attackieren-23-hochschulen-in-deutschland-a-1203973.html

[6] https://www.tagesschau.de/investigativ/ndr-wdr/hacker-bundestag-113.html

Michael Scheffler,
Country Manager DACH
von Varonis Systems

Sichere Verwaltung von Apple-Geräten im öffentlichen Dienst

WORAUF KOMMT ES BEI DER AUSWAHL EINER MOBILE-DEVICE-MANAGEMENT-LÖSUNG AN?

Autor: Oliver Hillegaart,
Senior Regional Sales Manager bei Jamf

Digitales Frontend und Offline Backend?" – Diesen provokanten Titel gab Christoph Verenkotte, der Präsident des Bundesverwaltungsamts, seinem Vortrag auf dem Fachkongress des IT-Planungsrats zum Onlinezugangsgesetz (OZG), der Mitte März 2021 stattfand. Er forderte mehr Automatisierung, Transparenz und Vernetzung von Daten und Prozessen. Außerdem attestierte er staatlichen und kommunalen Behörden einigen Nachholbedarf, wenn das Ziel des OZG, rund 6.000 Leistungen im öffentlichen Dienst bis Ende 2022 in digitaler Form anzubieten, erreicht werden soll. In der Tat gibt es noch viel zu tun, wenn bis dahin nicht nur die Bürgerinnen und Bürger, sondern auch die Mitarbeitenden in Behörden, Kommunen und Gemeinden von der Digitalisierung profitieren sollen. Ein wichtiger Schritt ist die sichere und effiziente Verwaltung der digitalen Arbeitsgeräte.

MOBILE DEVICE MANAGEMENT (MDM): GELUNGENES ZUSAMMENSPIEL VON FRONT- UND BACKEND

Bei den Themen Hosting, Compliance und Datensicherheit gelten im öffentlichen Dienst strengere Kriterien bei der Auswahl von Software als in der freien Wirtschaft. Bevor eine Entscheidung für eine Software fällt, sollte daher sorgfältig geprüft werden, ob sie die besonderen Anforderungen nachweislich erfüllt. Eine MDM-Lösung, wie etwa Jamf Pro, sorgt für

reibungslose Verwaltung und zuverlässigen Schutz von Mobilgeräten. Bei der Auswahl sollte auf folgende vier Punkte besonders geachtet werden:

▪ Hosting und Datensouveränität

Der MDM-Server ist der wichtigste Teil der Verwaltung von Apple-Geräten, da er kontinuierlich mit dem Push-Benachrichtigungen-Server von Apple (APNS) in Verbindung steht und Daten übermittelt. Das ist wichtig, denn durch den Austausch zwischen Gerät und MDM-Server erhalten die Endbenutzer die von der IT-Abteilung festgelegten Befehle, Konfigurationen und Apps. IT-Verantwortliche sollten zunächst prüfen, ob der MDM-Anbieter ein Hosting in der Cloud bzw. der Private Cloud und zusätzlich lokal ermöglicht. Denn auch in Behörden müssen nur bestimmte Daten vor Ort (On-Premises) gehostet werden. Die Möglichkeit, unterschiedliche Methoden zu kombinieren, kann Kosten sparen. Weiterhin sollte geklärt werden, ob die Daten in der EU gehostet werden und die Datenschutz-Grundverordnung der Europäischen Union (DS-GVO) eingehalten wird. Dies ist bei Jamf Pro der Fall. Jamf unterstützt den Kunden außerdem bei der Einhaltung der Anforderungen zu Anfragen in Bezug auf das Auskunftsrecht und das Recht auf Löschung gemäß der DS-GVO.

▪ Gerätesicherheit

Apple verfügt über integrierte native Sicherheitsfunktionen, wie Geräteverschlüsselung, Touch-ID und den „Lost Mode", sowie einen einheitlichen Zeitplan für die Betriebssystem-Upgrades. Dennoch ist Mobile Device Management für Apple-Geräte entscheidend, damit Aktivierung und Durchsetzung dieser Sicherheitsfunktionen auch tatsächlich auf sämtlichen Geräten greift. Mit Mobile Device Management können IT-Verantwortliche Geräte aktiv überwachen und Sicherheitsbefehle an Geräte senden, um sicherzustellen, dass sie geschützt und konform sind. Wird ein Gerät als gestohlen oder verloren gemeldet, ermöglicht es MDM, das Gerät aus der Ferne zu orten. Indem sie das Gerät sperren und den Standort feststellen, erhöhen IT-Verantwortliche die Chancen, das Gerät wiederzufinden beziehungsweise vor Fremdzugriff zu schützen.

▪ Compliance

Im Gegensatz zur Privatwirtschaft gibt es im öffentlichen Sektor nur selten einen Compliance-Beauftragten. Beim Kauf neuer Hardware oder Software ist daher die IT-Abteilung in der Pflicht, sich zu informieren, ob neue Lösungen mit den internen Anforderungen konform sind. Führende Anbieter machen ihre Compliance-Zertifizierungen und Initiativen öffentlich einsehbar und informieren ihre Bestandskunden fortlaufend über Neuerungen in diesem Bereich. Einige MDM-Lösungen, darunter auch Jamf Pro, bieten zudem eine integrierte Auditing- und Compliance-Lösung.

TIPP: MIT MDM GELINGT EINE SICHERE DIGITALE VERWALTUNG AUCH VOM HOMEOFFICE AUS

Durch die Digitalisierung der Dienstleistungen, wie sie laut OZG bis Ende 2022 geplant sind, bietet sich nun auch für Mitarbeiter im öffentlichen Dienst die Chance, ihre Tätigkeiten vom Homeoffice aus zu erledigen. Hier bietet ein MDM wertvolle Dienste:

1. Effizientes Mitarbeiter-Onboarding mit Zero-Touch-Deployment

Mit einer unternehmensweiten Strategie für die Bereitstellung von Zero-Touch-Geräten können Mitarbeiter ihr Gerät direkt aus der Originalverpackung in Betrieb nehmen. Möglich wird dies mit dem Apple Business Manager, der den Mac, das iPad oder das iPhone bei der Erstanmeldung anweist, sich automatisch für die MDM-Lösung des Unternehmens zu registrieren. Packt ein Nutzer ein neues Gerät aus und schaltet es ein, wird er bereits direkt namentlich begrüßt, und das Gerät ist fertig vorkonfiguriert. Durch diesen Workflow entfällt der Prozess des Auspackens jedes Geräts und dem manuellen Prozess der einzelnen Bereitstellung, um es für jeden Mitarbeiter zu personalisieren und zu konfigurieren. Die Zeiten, in denen die IT unter einem Berg neuer Hardware begraben wurde, sind damit vorbei.

2. Laufender Support für alle Mitarbeiter, egal wo sie arbeiten

Die meisten Apple-MDM-Lösungen kommunizieren über den Apple Push Notification Service (APNs) mit den Geräten und geben ihnen entsprechende Anweisungen. Wenn die IT-Abteilung Änderungen an einem (extern oder intern genutzten) Gerät vornehmen möchte, sendet sie einfach per APNs ein Konfigurationsprofil oder einen MDM-Befehl. VPN, E-Mail, WLAN und zahllose andere Einstellungen werden dann automatisch auf den Geräten der Mitarbeiter als Auswahloption angezeigt. Der Apple Business Manager trägt ferner zur Verwaltung von Apple-IDs bei, wenn er mit einer MDM-Lösung kombiniert wird. Mit Managed Apple IDs erhalten IT-Abteilungen die volle Kontrolle über die Bereitstellung und Verwaltung von Apple-IDs. Mitarbeiter profitieren von einer Apple-ID-Strategie, die eindeutig für die Arbeit bestimmt ist, damit es keine Verwirrung darüber gibt, ob sie ihre persönliche Apple-ID am Arbeitsplatz verwenden sollen oder nicht.

3. Innovative App-Verwaltung und -Bereitstellung

Jamf Pro bietet die Möglichkeit, Mitarbeitern Elemente per Self Service on demand zur Verfügung zu stellen. Die IT-Mitarbeiter richten den Self-Service-App-Katalog mit freigegebenen Konfigurationen, Ressourcen, Skripts zur Behebung gängiger Probleme, Lesezeichen und vertrauenswürdigen Apps ein. Die Mitarbeiter können die Apps dann eigenständig herunterladen und nutzen. Die Benutzer sind so in der Lage, jederzeit und von jedem Standort aus auf alle Ressourcen zuzugreifen, ohne dass in der IT-Abteilung auch nur eine Helpdesk-Supportanfrage zu diesen Themen eintrifft. Neben der Entlastung der IT sorgt dies auch für zufriedenere Nutzer, da diese eigenständiger arbeiten können, egal ob im Homeoffice oder vor Ort im Büro. ■

Mehr dazu hier

Mehr Wissenswertes zum Thema MDM finden Sie unter **www.jamf.com/de**

VORSORGE IST ALLES: PASSENDE MAßNAHMEN FÜR DEN IT-NOTFALL

Ein IT-Sicherheitsvorfall ist eines der größten Risiken für Unternehmen und für öffentliche Einrichtungen. Zusätzlich zu Endpoint-Protection-Lösungen können Organisationen weitere Maßnahmen umsetzen, um sich zu schützen oder im Worst Case wieder handlungsfähig zu werden. Die IT-Fachleute von G DATA Advanced Analytics unterstützen Sie dabei, die Resilienz zu verbessern.

Erste Hilfe und Brandschutz sind für Unternehmen und öffentliche Einrichtungen eine Selbstverständlichkeit. Angestellte kennen die Fluchtwege beim Feueralarm und wissen, wo der Erste-Hilfe-Kasten hängt. Anders ist es bei Cyberattacken. Sie sind eine alltägliche Bedrohung – die Schäden und Folgekosten aus erfolgreichen Angriffen sind enorm. Unabhängig von den Investitionen in IT-Sicherheitstechnologien bleibt immer ein Restrisiko, dass Angreifer dennoch Infrastrukturen kompromittieren. Jedoch sind die Investitionen für Fachleute für viele Organisationen in der Regel nicht tragbar. Sie sind auf externe Unterstützung angewiesen.

Als hundertprozentige Tochter von G DATA CyberDefense AG hat sich G DATA Advanced Analytics auf die Bedürfnisse von Unternehmen und öffentlichen Einrichtungen in den Feldern Malware-Analyse, Incident Response sowie IT-Infrastruktursicherheit spezialisiert und liefert kundenspezifische Sicherheitslösungen. Hochqualifizierte Fachleute erbringen hochspezialisierte Dienstleistungen und setzen kundenspezifische Sicherheitslösungen effektiv und zeitnah um.

PENETRATION TEST – SCHWACHSTELLEN FINDEN UND BEHEBEN

Cyberkriminelle nutzen aktive Schwachstellen im Netzwerk aus. Sie suchen gezielt nach Zugängen und verwundbaren Anwendungen, und sammeln Informationen, um einen Angriff vorzubereiten. Solche Schwachstellen lassen sich mit einem professionellen Penetration Test (Pentest) aufspüren und beheben. Pentests sind damit ein unabdingbares Werkzeug des Risikomanagements und zur Verteidigung der eigenen Infrastruktur. Sie ermöglichen es, Einfallstore zu erkennen, zu priorisieren und zu schließen,

bevor diese aktiv bei einem Cyberangriff ausgenutzt werden. Die erfahrenen Pentester der G DATA Advanced Analytics verfügen über weltweit anerkannte Zertifikate und weitreichende Erfahrungen in einer Vielzahl von IT-Umgebungen. Sie kombinieren automatisierte und manuelle Angriffsschritte und identifizieren mithilfe von realistischen und kontrollierten Angriffen Sicherheitsmängel in IT-Systemen. Die genutzten Angriffsmethoden entsprechen denen realer Angreifer und decken deren gesamte Bandbreite an Methoden ab. Jede Sicherheitslücke, die sie finden, können auch Angreifer missbrauchen.

Nach dem Pentest erhalten die G DATA Advanced Analytics Kunden einen umfangreichen Bericht, der die einzelnen Schritte des Tests sowie deren Ergebnisse ausführlich, transparent und verständlich dokumentiert. So können Verantwortliche nachvollziehen, welche Angriffsvektoren potenziellen Angreifern zugänglich sind. Sie erhalten eine individuelle Risikoeinschätzung der identifizierten Schwachstellen. Der abschließende Bericht versetzt interne IT-Organisationen, wie auch Managed Service Provider in die Lage, Sicherheitslücken auch selbstständig zu beheben. Dazu erhalten sie konkrete und nachvollziehbare Handlungsempfehlungen.

SECURITY MONITORING MIT SECMON

Die Erfahrungen zeigen, dass viele erfolgreiche Cyberattacken lange unentdeckt bleiben – nicht selten liegen zwischen der Erstinfektion und der Lösegeldforderung bei einer Ransomware-Attacke viele Monate. Dabei lassen sich schon frühzeitig Hinweise auf solche Angriffe erkennen, etwa aus den Logdaten der Infrastruktur. Als Ergänzung zu bestehenden IT-Sicherheitsmaßnahmen kombiniert G DATA Advanced Analytics mit SecMon, dem innovativen, hybriden Ansatz im Security Monitoring, die wirkungsvollsten Maßnahmen aus den Bereichen SOC-as-a-Service, Managed-SIEM und anderen Managed-Security-Angeboten. Wir überwachen zentrale Logdaten auf den kritischen IT-Systemen und analysieren diese auf mögliche Bedrohungen. Im Fall des Falles erhalten Unternehmen und öffentliche Einrichtungen unverzügliche Ad-hoc-Meldungen sowie klar nachvollziehbare Handlungsanweisungen zum weiteren Vorgehen. Zusätzlich kommuniziert die G DATA Advanced Analytics nichtzeitkritische Auffälligkeiten im Rahmen von Übersichtsreports. SecMon ist schlank, mit kleinem Footprint und hat keine Auswirkungen auf die Performance der IT. Darüber hinaus ist keine Hardware zusätzlich erforderlich, das Onboarding ist schnell, einfach und preiswert.

Unsere Analysten arbeiten mit Ihren Daten aus unserer Hochsicherheitsumgebung heraus, dabei bleiben Ihre Daten stets im deutschen Rechtsraum – ein echter Sicherheitsgewinn. Ein weiterer Vorteil: SecMon ist vollständig produkt- und herstellerunabhängig und integriert sich nahtlos in existierende Lösungslandschaften.

INCIDENT RESPONSE RETAINER: VORBEREITEN FÜR DEN WORST CASE

Angesichts der stetig steigenden Cybergefahr entscheiden sich viele Organisationen für eine langfristige Zusammenarbeit mit Fachleuten und vereinbaren schon vor dem Eintritt des Worst Case eine Kooperation – einen sogenannten Incident Response Retainer. Ihr Ziel: Die bestmögliche Resilienz gegen IT-Sicherheitsvorfälle. Unternehmen und öffentliche Einrichtungen, die sich für eine Zusammenarbeit mit Incident Response spezialisierten Fachleuten entscheiden, profitieren auf vielen Ebenen. Im Fall eines Angriffs vermeiden die Firmen teure Ausfallzeiten, weil im Vorfeld eine Recovery-Strategie definiert wurde. So lassen sich IT-Systeme deutlich schneller wiederherstellen. Gleichzeitig können sich Organisationen darauf verlassen, dass sich im Notfall ein spezialisiertes Incident-Handling-Team um die betroffenen Systeme kümmert. Ein weiterer Vorteil: Auch ohne Hilfe im Notfall leisten die Fachleute wertvolle Arbeit. Sie beraten zu präventiven Maßnahmen und helfen mit, die IT-Sicherheit zu verbessern. Dabei decken die Fachleute technische und organisatorische Schwachstellen auf, sodass Organisationen diese schließen können – von Netzwerksegmentierung, Härtung der Systeme und Back-up-Prozessen bis hin zu Remote-Zugängen und BYOD-Policies. Nicht zuletzt sichern sich die Organisationen durch den Rahmenvertrag reduzierte Stundensätze und die Verfügbarkeit von Experten, wenn es darauf ankommt.

FAZIT

Die Frage ist nicht, ob ein Unternehmen und öffentliche Einrichtungen einer Cyberattacke zum Opfer fallen, sondern wie sie damit umgehen. Die richtige Vorbereitung sichert auch im Schadensfall Handlungsfähigkeit und das Überleben der eigenen Organisation. ■

Mehr dazu hier

G DATA Advanced Analytics GmbH
G DATA Campus
Königsallee 178
44799 Bochum
www.gdata-advancedanalytics.de

Ansprechpartner
Tim Rediske
IT-Security Sales Consultant
Tel.: +49 2349762694
E-Mail: Tim.Rediske@gdata-adan.de

G DATA | ADVANCED ANALYTICS

- ADVERTORIAL -

IT-Sicherheit bei Behörden

WAS KÖNNEN GUTE PASSWORT-MANAGER LEISTEN?

Öffentliche Einrichtungen und Behörden müssen angesichts häufigerer Cyberattacken neue Sicherheitsstrategien entwickeln. Was ein guter Passwort-Manager in diesem Kontext leisten kann? Das erfahren Sie hier.

Verfolgt man die aktuelle Presse, so wird schnell deutlich: Behörden werden in letzter Zeit immer häufiger zur Zielscheibe von Cyberattacken. Das heißt auch, dass öffentliche und für das Gemeinwesen wichtige Infrastruktur kompromittiert wird. Ein Grund dafür: Durch sich ändernde IT-Landschaften (Mobility, Cloud, neue Dienste) entstehen neue Gefahren und Schwachstellen.

Die Verantwortlichen für IT-Sicherheit müssen hier also sehr genau hinsehen, um diese Infrastruktur für die Zukunft zufriedenstellend zu sichern und die IT-Sicherheit anpassungs- und zukunftsfähig zu gestalten.

ANZAHL DER CYBERATTACKEN STEIGT RASANT

Aber blicken wir zurück: Die Zahl der Cyberattacken generell ist in den vergangenen Monaten bedenklich gestiegen. In einer Anfang des Jahres veröffentlichten International Data Group Studie gaben zwei Drittel der Befragten IT-Manager zu, dass User im Homeoffice zunehmenden Cyberrisiken ausgesetzt sind. Mehr als 30 Prozent gaben sogar an, dass die Beschäftigten zu Hause mit ungeschützten Geräten arbeiten. Die logische Folge: IT-Security-Verantwortliche haben dadurch immer mehr Probleme, die Mitarbeitenden zu schützen.

Es gibt hier schlicht und einfach neue Voraussetzungen. Die neue Prämisse muss sein: durch das neue Prinzip „Work from anywhere" den Zugang der User zu ihren Ressourcen einerseits zu erleichtern und andererseits die Cyberrisiken zu minimieren.

SICHERHEITSBEWUSSTSEIN ALLER BETEILIGTEN ERHÖHEN

Der wichtigste Schritt dahin ist zunächst, unter den Beteiligten das interne Sicherheitsbewusstsein zu steigern. Ganz gleich, ob Mitarbeitende zu Hause oder im Büro arbeiten, ihnen muss klar sein, welche Gefahren von böswilligen Hackern ausgehen und welche Schritte und Tools zur Bekämpfung eingesetzt werden können. Wichtig ist dabei, dass die Mitarbeitenden nicht nur einmal geschult werden, sondern dass das Thema

„Sicherheit" fest in der Kultur der Organisation verwurzelt ist. Nur so können IT-Manager sicherstellen, dass sich ihre User während der gesamten Arbeitszeit vorsichtig verhalten und keine Sicherheitspannen durch Leichtsinnsfehler entstehen.

SMARTE PASSWORT-MANAGER HELFEN WEITER

Einer der wirklich robusten Schritte in Sachen IT-Sicherheit ist ein starkes Passwort-Management. Passwörter zählen noch immer in vielen Organisationen zu den größten Sicherheitslücken. Viele Nutzer verwenden dasselbe, unsichere Passwort über verschiedene Anwendungen hinweg. Und am beliebtesten ist leider noch immer das berühmte „123456". Deshalb müssen Organisationen die Kontrolle über die Passwort-Verwendung durch Mitarbeitende haben, um einen Verstoß rechtzeitig zu verhindern aber gleichzeitig keine Mehrarbeit für die Nutzer zu verursachen. Dafür gibt es zahlreiche Lösungen.

Eine davon kann sicherlich ein solider Passwort-Manager sein, wie er etwa von den Sicherheitsexperten von LastPass als cloudbasierte Lösung angeboten wird:

- Er verwaltet alle Passwörter, die individuell für ein Konto erstellt werden, in einem sicheren Tresor, der nur über ein starkes Master-Passwort des Users zugänglich ist.
- Mitarbeitende müssen sich nur ein Passwort merken. So wird vermieden, dass diese ihre Passwörter unsicher gestalten oder mehrfach, für verschiedene Anwendungen verwenden.
- Mit Single Sign-on (SSO) kann die Anzahl der Passwörter, die Mitarbeitende erstellen, sich merken und verwalten müssen, erheblich reduziert werden. SSO verbindet einen Mitarbeitenden sicher mit den Anwendungen, die ihm zugewiesen wurden, ohne dass er ein Passwort eingeben muss.
- Ist SSO mit einem Passwort-Manager verbunden, kann eine Organisation, eine Behörde oder eine Verwaltung die vollständige Kontrolle über sowohl die Passwörter als auch den Benutzerzugriff erreichen. So bekommen die Log-ins eine zusätzliche Sicherheitsstufe.
- Die Multi-Faktor-Authentifizierung (MFA) geht hier noch einen Schritt weiter. Hier ist es zum Einloggen erforderlich, neben dem Passwort auch einen Code einzugeben, der an ein anderes Gerät des Nutzers oder über Biometrie – zum Beispiel den Fingerabdruck – geschickt wird. Nur mit Eingabe dieses zweiten Faktors wird der Anmeldevorgang abgeschlossen.

MULTI-FAKTOR-AUTHENTIFIZIERUNG UND VIRTUAL PRIVATE NETWORK (VPN)

In der oben zitierten International-Data-Group-Umfrage gaben 45 Prozent der IT-Verantwortlichen zu Protokoll, dass Mitarbeitende auf ungesicherte WLAN-Netze zugreifen. Deshalb ist es unumgänglich, auch den Zugang zum Netzwerk des Unternehmens beziehungsweise der Behörde abzusichern. Ein Virtual Private Network (VPN) ist hier zu einem unverzichtbaren Werkzeug für Organisationen auf der ganzen Welt geworden.

Durch die einfache Nutzung, einen einzigen Zugangspunkt und eine sichere Datenübertragung genießt die VPN-Technologie hohe Akzeptanz. Allerdings bergen genau diese Eigenschaften auch ein hohes Potenzial für

Cyberangriffe. Mit nur einem einzigen Satz gestohlener Log-in-Daten oder einem durch Malware kompromittierten Computer kann sich ein Hacker Zugang zu sensiblen Daten im Netzwerk einer Organisation verschaffen – und es im schlimmsten Fall komplett kapern. Daher braucht auch ein VPN eine zusätzliche Absicherung. Mit der oben beschriebenen Multi-Faktor-Authentifizierung lässt sich die Sicherheitsebene verdoppeln. So wird vermieden, dass sich unberechtigte Personen Zugang zum Netzwerk verschaffen, ohne zusätzliche Komplexität für die Mitarbeitenden zu kreieren.

DIE ZUKUNFT DER IT-SICHERHEIT IST SCHON DA

Kein Zweifel: Es ist ein Wettrüsten im Gange, mit dem wir alle leben müssen. Cyberkriminelle und Cyberbedrohungen werden sich weiterentwickeln und häufiger, schneller und perfider zuschlagen. Auch öffentliche Verwaltungen und Behörden machen sich deshalb permanent Gedanken, welche Sicherheitsmaßnahmen notwendig sind und welche Verantwortungen sie selbst und welche ihre Security-Anbieter übernehmen müssen, um Daten, Infrastrukturen und Nutzer optimal zu schützen.

Technologiebasierte Cybersicherheitspraktiken werden sich kontinuierlich weiterentwickeln. Behörden und ihre Dienstleister müssen in der Lage sein, Unmengen an Vorfallsdaten, fehlerhaften oder doppelten Datensätzen, eine Vielzahl von Malware-Mustern über Tausende von Protokollen zu bewältigen. Schon in naher Zukunft werden hier mit Sicherheit künstliche Intelligenz (KI) und Machine Learning eine wichtigere Rolle spielen, um schneller und zuverlässiger kriminelle Muster bei großen Datenmengen zu erkennen und entsprechend frühzeitig Warnungen zu generieren.

Diese Dynamik macht klar: IT-Sicherheit muss als permanenter Prozess begriffen werden, und nicht lediglich als einzelne Maßnahme. Ein smarter Passwort-Manager, wie LastPass, kann hier einen wesentlichen Beitrag leisten. ■

Mehr dazu hier

LastPass

Zero Trust – strategischer IT-Security-Ansatz in der öffentlichen Verwaltung

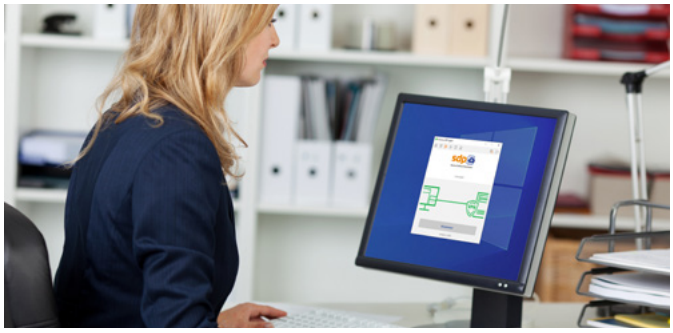
Die Interaktion zwischen Bürgerinnen, Bürgern und Unternehmen mit der Administration soll in Zukunft deutlich schneller, effizienter und nutzerfreundlicher werden. Eine digitale Gesellschaft braucht nicht nur eine moderne, sondern auch eine sichere IT-Infrastruktur.

Andreas Wendt, macmon secure GmbH, Experte für IT-Sicherheit im Behördenumfeld, beschreibt die besonderen Anforderungen an die IT-Sicherheit im Austausch von Daten mit der Öffentlichkeit: „Klassische Sicherheitskonzepte gehen davon aus, dass alle Endgeräte innerhalb des Behördennetzwerks vertrauenswürdig sind. Doch diese Vermutung trifft aufgrund von Mobilität, Cyberattacken, Cloud-Diensten und behördenübergreifender Zusammenarbeit nicht mehr zu. Mit **Zero Trust Network Access (ZTNA)** lässt sich ein durchgehendes Sicherheitskonzept zwischen Cloud und Rechenzentrum-Architektur realisieren. Eine mit ZTNA gesicherte, hybride IT-Architektur entspricht den Sicherheitsanforderungen des Bundesamts für Sicherheit in der Informationstechnik (BSI) und schützt den Zugriff in allen Anwendungen im Netzwerk. Somit wissen die Bediensteten einer Behörde jederzeit, welche Geräte sich in ihrem Netzwerk befinden. Die IT-Administration kann eingesetzte PC, Drucker, Laptops und andere technische Geräte jederzeit effizient überwachen."

Die sich in der BSI-Zertifizierung befindliche Sicherheitslösung der Berliner IT-Experten erkennt, meldet und unterbindet den Betrieb von Fremdsystemen im behördeneigenen Netzwerk und verhindert den Einsatz von nicht autorisierten Geräten. Gast- und Mitarbeitergeräte (Bring your own device – BYOD) können außerdem über das Gästeportal, mithilfe eines dynamischen Managements der Netzwerksegmente, einfach und sicher zugelassen werden.

NETZWERKSICHERHEIT FÜR LOKALE INFRASTRUKTUREN UND CLOUD-ANWENDUNGEN IM FOKUS DER GEFAHRENABWEHR

Die **IT-Grundschutz-Kataloge des BSI** stellen in der öffentlichen Verwaltung den Standard für die Informationssicherheit und den Aufbau eines funktionierenden IT-Sicherheitsmanagements dar. Das Einbringen von nicht autorisierten und unsicheren Geräten ins Netz ist konsequent zu unterbinden. Entscheidend ist, dass diese Maßnahme heute nicht mehr nur lokale Infrastrukturen betrifft, sondern auch externe Ressourcen, wie Private oder Public Clouds.



SECURE DEFINED PERIMETER (SDP) SCHÜTZEN VOR ANGRIFFEN AUF SENSIBLE, PERSONENBEZOGENE DATEN IN DER CLOUD

Mit macmon SDP wird der Schutz auf sämtliche Cloud-Dienste ausgedehnt. Der **SDP-Agent** übernimmt transparent eine hochsichere Authentifizierung gegenüber dem SDP-Controller, um die Identität des Benutzers sowie des Geräts und dessen Sicherheitszustand zu prüfen. Die DSGVO-konforme Lösung ist gehostet in einem ISO-27001 zertifizierten Rechenzentrum in Deutschland. Und auch der Support wird von einem internen Expertenteam in Berlin-Mitte sichergestellt.

Wendt ergänzt: „Um heutige Netzwerke vollständig kontrollieren zu können, muss eine NAC-Lösung (Network Access Control) auch jede Authentifizierungstechnologie unterstützen. Nicht alle Anbieter stellen diese Möglichkeit bereit oder ermöglichen die Arbeit auch im gemischten Betrieb mit Technologien wie 802.1X und SNMP. Unsere Lösung bildet dies nicht nur ab, sondern skaliert mit dem Netzwerk. Die bestehende Infrastruktur kann einfach weiterverwendet werden, wie sie ist."

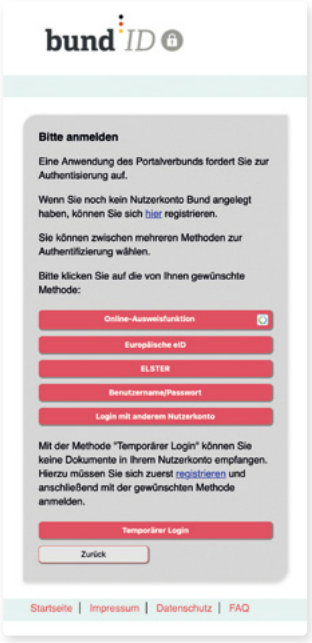
Fazit: **IT-Sicherheit** ist in der öffentlichen Verwaltung ein sensibles Thema, da für viele Dienstleistungen äußerst persönliche Daten hinzugezogen werden. Auch bei internen Prozessen ist die Wahrung von datenschutzrechtlichen Leitlinien und Gesetzen außerordentlich wichtig. Durch eine Sicherung der notwendigen IT-Infrastruktur können positive Effekte der Digitalisierung in der öffentlichen Verwaltung realisiert werden. ■

Mehr dazu hier

DIE HERAUSFORDERUNGEN DIGITALER BEHÖRDENGÄNGE

Einfach, nachvollziehbar, sicher – so soll sie sein. Die digitale Verwaltung startet durch. Genauer gesagt hat der Gesetzgeber in Deutschland mit dem neuen Onlinezugangsgesetz (OZG) eine Basis geschaffen, die es Bürgern sowie Unternehmen erlaubt über eine zentrale Plattform behördliche Dienste in Anspruch zu nehmen oder danach zu suchen. Diese Plattform, **Bundesportal** genannt, ist seit 2019 online.

Der erste Schritt zu einem digitalen Behördengang ist die Verifizierung persönlicher Daten im Rahmen einer Registrierung. Je nach Vertrauensniveau, die die behördliche Leistung beansprucht, gibt es verschiedene Optionen zur Identifikation des Nutzers:



Screenshot: Anmeldung im Bundesportal

Im Bild zu sehen sind die Anmeldeoptionen. Diese können ungleicher nicht sein, da für verschiedene Services unterschiedliche Vertrauenslevel vom Nutzer eingefordert werden. Ein Beispiel, wie schwierig es ist, dem „Otto-Normalbürger" Online-Behördengänge einfach zu machen. Dabei kennen viele Bürger das Anmelde-Prozedere schon von anderen, nicht-behördlichen Identitätsanbietern, wie die Deutsche Post, Google, Facebook oder Microsoft.

Das Ergebnis der Registrierung ist die Anlage eines Nutzerkontos sowie die Erstellung einer ID, hier die „bund ID". Manche Bundesländer bieten eine eigene ID an, z.B. die BayernID des Freistaats Bayern. Bei den ganzen Möglichkeiten geht der Überblick schnell verloren.

Für manche Nutzer sind Online-Anmeldeprozesse ein Buch mit sieben Siegeln. Das Bundesportal verspricht auf seiner Hauptseite, dass „online zur Behörde gehen" so schnell sei, wie „Onlineshopping". Das mag wohl wahr sein, für diejenigen, die sich auskennen. Die meisten Onlineshopping-Portale sind heutzutage so gestaltet, dass die Hürden eine Online-Bestellung zu tätigen sehr niedrig sind. Das ist mittlerweile für viele Menschen einfach umsetzbar. Bei der Online-Verwaltung fehlt jedoch die positive Nutzererfahrung, die eigentlich von Anfang an da sein sollte.

Es ist eine Mammutaufgabe: die digitale Transformation der Registrierung, der Anmeldung, der Informationssuche und der Prozesse. So gilt es, auch das wichtige Thema Schutz und Qualität der Daten zu berücksichtigen.

Welche Identitätsmanagementfunktionen braucht ein Betreiber, um seine Webservices für die Nutzer attraktiv und sicher zu gestalten?

Als Anwendungen noch nicht im Web unterwegs waren, hat man diese in die Anwendungen selbst integriert. Durch die Verbreitung von Internet, Cloudtechnologien und höheren Anforderungen an die Compliance ist es viel effizienter geworden, solche Aspekte einem spezialisierten Identitäts- und Zugriffsmanagementsystem (kurz: IAM-System) zu überlassen. Auch, weil die notwendigen Prozesse immer die gleichen sind.

Was verbirgt sich hinter einem IAM-System für Webapplikationen?

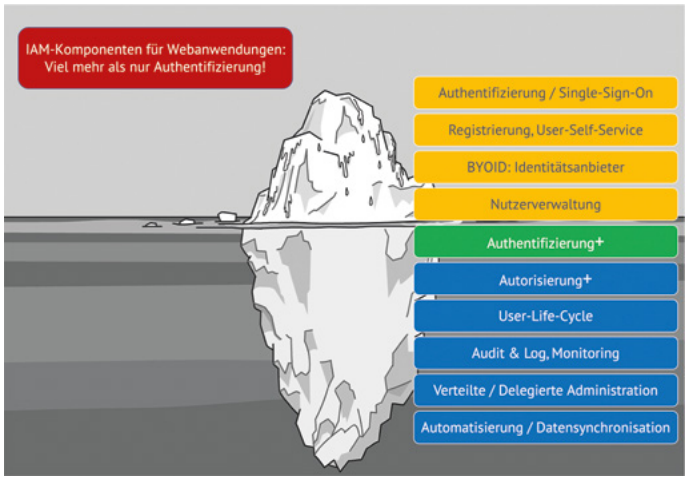


Abbildung: IAM-Komponenten für Webapplikationen

Die Komponenten zielen darauf ab, Identitäten und ihre Berechtigungen sicher, einfach und gesetzeskonform zu verwalten. Und damit ist nicht der Funktionsumfang gemeint, den der eigentliche Webservice leisten soll. Sondern viel mehr Softwareteile, die die relevanten Identitätsdaten verwalten. Ein wichtiger Baustein ist der User-Life-Cycle: Registrierung, Informationsprüfung und Datenabgleich zwischen Systemen. Oder das Zugriffsmanagement mit der Festlegung des aktuellen Status (zum Beispiel Standesamt) und die damit zusammenhängenden Befugnisse.

Vielleicht wird damit ein wenig verständlicher, dass ein solches Projekt sich über Jahre hinziehen kann, viele einschlägige Experten braucht und erst möglich wird, wenn der Gesetzgeber die Voraussetzungen dafür geschaffen hat. ■

Mehr dazu hier

login>master | login-master.com

intension

syntlogo

Bild: iStock.com/metamorworks

BSI-zugelassene VPN-Software für VS-NfD:

DER MOBILE ARBEITSPLATZ HEUTE UND IN ZUKUNFT!

Die IT-Welt dreht sich bekanntermaßen besonders schnell. In den letzten zehn Jahren gab es viele verschiedene Entwicklungen im Bereich von Hard- und Software zur sicheren Datenkommunikation der Geheimhaltungsstufe VS-NfD (Verschlusssachen – nur für den Dienstgebrauch).

Erhielten anfangs noch Produkte nach gewissen Kriterien eine Einsatzempfehlung des Bundesamts für Sicherheit in der Informationstechnik (BSI), wurde ab 2012 eine BSI-Zulassung durch die höhere Bedrohungslage zur Vorgabe. Es entstanden Hardware-Lösungen oder Produkte basierend auf Virtualisierung, da Windows als Betriebssystem als unsicher galt. An letzterem Sachverhalt hat sich bis heute nichts geändert.

VPN FÜR VS-NFD: HARDWARE GEHÖRT DER VERGANGENHEIT AN

Seit 2019 kam es aufgrund der schlechten Usability und Skalierbarkeit von Hardware zu einem Umdenken. Die prekäre Situation in der Corona-Pandemie durch Hardware-Lieferschwierigkeiten und den plötzlich erhöhten Homeoffice-Bedarf auch bei Bedarfsträgern, Behörden und der geheimschutzbetreuten Wirtschaft goss noch mehr Öl ins Feuer.

Als Vorreiter konnte NCP bereits im Juli 2020 mit dem NCP VS GovNet Connector die erste Softwarelösung mit Freigabeempfehlung des BSI für Endgeräte mit Standard-Windows 10 auf den Markt bringen. Zudem ist der Anbieter seit April 2021 „Qualifizierter Hersteller für das Qualifizierte VS-NfD-Zulassungsverfahren im Sinne des Bundesamtes für Sicherheit in der Informationstechnik" und kann daher innovativ und trotzdem schnell auf Marktanforderungen reagieren. Auf Hardware oder Hardware-Abhängigkeit setzt man beim Nürnberger Software-Spezialisten aus guten Gründen nicht mehr.

AKTUELLE EINSATZMÖGLICHKEITEN

Die Version 2.0 des NCP VS GovNet Connectors besitzt seit dem 14.05.2021 eine BSI-Zulassung für die Geheimhaltungsstufen „VS-NfD", „RESTREINT UE/EU RESTRICTED" und „NATO RESTRICTED". Durch ihre Leistungsfähigkeit, die Skalierbarkeit und den ausgereiften Funktionsumfang unterscheidet sich die Lösung im Einsatzverbund mit den zentralen NCP-Software-Komponenten deutlich von Produkten anderer Hersteller auf dem Markt.

Rollout, Inbetriebnahme, Software-Update und Administration der gesamten „NCP VS GovNet Lösung" erfolgen komfortabel über eine zentrale Management-Komponente, das NCP Secure Enterprise Management (SEM). Der für VS-NfD zugelassene NCP Secure VPN GovNet Server schließt den Kreis der Gesamtlösung. Im Zusammenspiel mit den hochleistungsfähigen, zentralen Softwarekomponenten können Nutzerzahlen jenseits der 100.000 problemlos abgebildet werden.

Die Verwendung von Standard-Hardware in Verbindung mit einem Standard Windows 10 Betriebssystem eröffnet Anwendern ganz neue Möglichkeiten und erlaubt maximale Flexibilität. Ein Integritätsdienst sorgt in gleichem Maße für erhöhte Sicherheit wie starke Authentisierungsmöglichkeiten und weitere Sicherheitsfunktionen, z.B. im Rahmen von Network Access Control und Endpoint Policy Checks.

Über sichere und zugleich komfortable Möglichkeiten der Administration, wie z. B. das zentrale Rechte- und Konfigurationsmanagement oder

Wir freuen uns, dass die NCP VS GovNet Lösung so gut im Markt ankommt. Mit dieser reinen Softwarelösung haben wir den VS-NfD-Markt revolutioniert und erfüllen mit ihr genau die Bedürfnisse von Ministerien, Behörden und geheimschutzbetreuten Unternehmen. Wir arbeiten mit Hochdruck daran, unsere GovNet-Lösung noch weiter auszubauen. Dabei wird natürlich auch die Anwenderfreundlichkeit nicht vernachlässigt. Die Roadmap ist vollgepackt mit neuen Funktionen, die unsere Kunden langfristig in die Lage versetzen werden, den Anforderungen des Marktes und der Bedrohungslage Rechnung zu tragen.

PATRICK OLIVER GRAF,
CEO & Managing Director,
NCP engineering GmbH

„Quality of Service"-Unterstützung, freuen sich IT-Verantwortliche. Verschiedene anwender- bzw. bedarfsgerechte Lizenzmodelle, wie z. B. das Pay-per-Use-Lizenzmodell, runden die VS-NfD-Software-Lösung ab.

SICHERE HOTSPOT-ANMELDUNG UND FRIENDLY NET DETECTION

Diese und weitere Vorteile orientieren sich durch jahrelange Erfahrung und Zusammenarbeit ganz eng am tatsächlichen Praxisbedarf. Die Lösung weiterer für die Bedarfsträger relevanter Probleme folgen bei der Zulassung der nächsten Produktversion 2.10 des NCP VS GovNet Connector bereits im Dezember.

Im Fokus stehen hier insbesondere die sichere Nutzung öffentlicher Hotspots und eine Friendly Net Detection (FND). Die übliche Anmeldung über eine Website des Hotspot-Betreibers mit einer Kommunikation am VPN-Tunnel vorbei ist im Behörden- und Business-Umfeld meist nicht gestattet, weswegen die Nutzung öffentlicher Hotspots quasi unmöglich wird.

Wählt ein Anwender der NCP-Lösung einen Hotspot aus, baut der VS GovNet Connector automatisch die Verbindung zum Unternehmensnetz auf. In den meisten Fällen ist ein Internetzugang nicht ohne Anmeldung möglich, sodass der Client zu diesem Zweck aus Sicherheitsgründen einen funktionsreduzierten Webbrowser startet. So können Anwender auf sichere Weise einen öffentlichen Hotspot nutzen, ohne an den Sicherheitseinstellungen etwas ändern zu müssen.

Das Feature „Friendly Net Detection (FND)" erkennt zertifikatsbasiert, ob sich der Anwender in einem sicheren oder unsicheren Netz befindet und aktiviert die entsprechenden Firewall-Regeln. Im sicheren Netzwerk kann der VPN-Verbindungsaufbau somit unterbunden werden, damit beispielsweise administrative Zugriffe auf das Endgerät gestattet sind, während dies im unsicheren Netz nicht erlaubt ist. Im Gegensatz zu herkömmlichen Firewalls ist die des NCP VS GovNet Connectors bereits beim Systemstart aktiv. Voraussetzung für die Verwendung des FND-Features ist der Einsatz des NCP Friendly Net Detection Servers ab Version 4.0.

QUO VADIS? WAS KANN VPN-SOFTWARE FÜR VS-NFD IN ZUKUNFT?

Die Vision einer leistungsstarken, zentral administrierbaren NCP-Softwarelösung für VS-NfD wird in den kommenden Monaten auch Punkte wie REST-API, eine Single-Sign-on-Lösung, Clientsoftware für weitere Betriebssystem-Plattformen und zusätzliche Komfortfunktionen bei der Installation und Konfiguration großer Nutzerzahlen beinhalten.

Ziel ist es, Kunden hochskalierbar, hochsicher und gleichzeitig maximal flexibel auch für die Datenkommunikation nach „VS-NfD" auszustatten. Auch VS-Arbeitsplätze müssen remote für Homeoffice und mobiles Arbeiten bei großen Nutzerzahlen gut administrierbar sein. Managed-Service-Betreiber und Landesrechenzentren können einzelne Mandanten über eine zentrale Plattform sicher und voneinander getrennt betreuen, auch wenn Kunden einen Mischbetrieb aus VS-NfD und normalen Nutzern fahren. ■

Informieren Sie sich über die Einsatzmöglichkeiten und Funktionen unter
www.ncp-e.com

Mehr dazu hier

NCP
SECURE COMMUNICATIONS

HOCHSICHERE VERSCHLÜSSELUNG ALLER BEHÖRDEN

Das Saarland nimmt die Digitalisierung ernst. Mit einer einheitlichen und starken Verschlüsselung der IT-Kommunikation der Landesbehörden ist nun eine sichere Basis geschaffen, auf der die weitere Digitalisierung vorangetrieben werden kann.

Autor: Falk Herrmann, CEO Rohde & Schwarz Cybersecurity

Tobias Hans, Ministerpräsident des Saarlandes, hat einen Digitalisierungsrat mit Experten einberufen, der über die Digitalisierungsroadmap des Saarlands wacht. Im Wirtschafts- und Arbeitsministerium wurden eigens neue Strukturen geschaffen, um die digitale Agenda voranzutreiben. „Meine Vision ist, dass das Saarland mit seiner Marke ‚Digitales Saarland' der Inbegriff für Digitalisierung, Cybersicherheit und künstliche Intelligenz wird", erläutert der Ministerpräsident des Flächenlandes mit etwa einer Million Bürgern.

Einen der ersten Meilensteine auf der Digitalisierungsroadmap hat das Saarland nun gemeistert. Gemeinsam mit dem IT-Sicherheitsexperten Rohde & Schwarz Cybersecurity und seinem Partner T-Systems hat das Saarland als erstes Bundesland eine moderne, flexible und flächendeckende Verschlüsselung der Landesbehörden umgesetzt. Diese Verschlüsselung erlaubt nun auch den Austausch von Verschlusssachen mit der Einstufung VS-NfD (VS – NUR FÜR DEN DIENSTGEBRAUCH).

HOCHPERFORMANTE VERSCHLÜSSELUNG VON SENSIBLEN DATEN

Täglich werden im Landesrechenzentrum des IT-Dienstleistungszentrums (IT-DLZ) in Saarbrücken, mit einer redundanten Anbindung von 10-GBit-Leitungen, riesige Datenmengen von öffentlichen Einrichtungen verarbeitet. Darunter befinden sich zahlreiche vertrauliche Daten mit sensiblen Inhalten und personenbezogenen Daten, wie beispielsweise Finanzdaten der Bürgerinnen und Bürger. Die geltenden Regularien geben vor, dass diese Daten nur verschlüsselt innerhalb eines Landesnetzes transportiert werden dürfen. Das Saarland geht aber noch einen Schritt weiter und kommt damit der Forderung des Bundesamts für Sicherheit in der Informationstechnik (BSI) nach: Empfohlen wird eine tiefe Verschlüsselung nach gehobenen Standards. „Wir haben uns dazu entschlossen, unsere existierende Verschlüsselung nach IP-Sec auf ein neues Niveau zu heben. Daher haben wir uns für den Einsatz der hochperformanten Verschlüsselungslösung R&S®SITLine ETH von Rohde & Schwarz Cybersecurity entschlossen", so der Bevollmächtigte für Innovation und Strategie und CIO des Saarlandes, Ammar Alkassar.

Mit über 30 Jahren Kryptokompetenz bietet Rohde & Schwarz Cybersecurity mit R&S®SITLine ETH eine „Security Made in Germany"-Lösung zur Ethernet-Verschlüsselung für Bandbreiten bis zu 40 Gbit/s. Als Layer-2-Verschlüsseler schützt er Unternehmen und Organisationen vor Spionage und Manipulation von Daten während der Übertragung, die mithilfe von Ethernet über Festnetz, Richtfunk oder Satellitenverbindungen transportiert werden. Die Geräte sind vom BSI zugelassen.

ERSTES BUNDESLAND MIT MODERNER LAYER-2-VERSCHLÜSSELUNG

Mit der neuen Multipunkt-zu-Multipunkt-Verschlüsselung verfügt das Saarland als erstes Bundesland über eine moderne Layer-2-Verschlüsselungslösung, die die strikten Vorgaben des BSI für den Transfer von VS- NfD-Materialien erfüllt. R&S®SITLine ETH verhindert wirksam, dass ausgetauschte Dokumente, Datenströme oder E-Mails von Außenstehenden mitgelesen werden können. ■

Mehr dazu hier

ROHDE&SCHWARZ

SCHUTZ VOR RANSOMWARE BEDEUTET SCHUTZ VOR DEM TOP-ANSTIFTER DER CYBERKRIMINALITÄT

Die Schlagzeilen zu Ransomware-Angriffen sind allgegenwärtig. Zahlreiche Unternehmen, Organisationen und Behörden waren schon betroffen, und die Lösegeldforderungen haben sich kontinuierlich in die Höhe geschraubt. Die Verschlüsselung von Daten ist dabei längst nicht mehr das einzige Erpressungsszenario – gestohlene Daten nicht öffentlich zu machen, lassen sich die Erpresser ebenso teuer bezahlen wie die Wiederherausgabe „eingesperrter" Daten. Ein Ende der Entwicklung ist nicht in Sicht. Ransomware ist vom Dauerbrenner zum Brandbeschleuniger innerhalb der Cyberkriminalität geworden und nimmt im florierenden Markt der Cyberbedrohungen eine Schlüsselrolle ein.

RANSOMWARE – GEKOMMEN, UM ZU BLEIBEN

Im neuen Threat Report für das Jahr 2022 geht Sophos davon aus, dass Ransomware noch mehr an Einfluss auf die Bedrohungslandschaft gewinnen wird. Wurden zum Beispiel in der Vergangenheit die Angriffe überwiegend durch einzelne Gruppen Ransomware-Krimineller durchgeführt, sind inzwischen vermehrt Ransomware-as-a-Service-(RaaS-)Angebote zu beobachten. Der Cyberangriff ist zur lukrativen Dienstleistung geworden, bei der spezialisierte Ransomware-Gruppen Schadcode und Infrastruktur an andere Cyberkriminelle vermieten. Die Erpressungs-Malware erweist sich als so gewinnbringend, dass auch andere, etablierte Cyberbedrohungen immer mehr für ihre Verbreitung genutzt und mit einbezogen werden. Dazu gehören Loader, Dropper und andere Standard-Malware sowie zunehmend fortschrittliche, von Menschen betriebene Initial Access Broker, Spam und Adware.

BEHÖRDEN SIND EIN BELIEBTES ZIEL

Die Ziele für Angriffe werden sorgsam ausgewählt und nicht selten verbleiben Angreifende monatelang unbemerkt im betroffenen Netzwerk, kundschaften aus, suchen Sicherheitslücken auch für andere Cyberkriminelle oder Malware und schlagen dann zu. Der Sophos-Report **„The State of Ransomware 2021"** zeigt auf, dass Behörden und staatliche Einrichtungen zu beliebten Zielen für Ransomware-Angriffe gehören. So besteht der Studie zufolge hier offenbar eine 69-prozentige Wahrscheinlichkeit, dass Cyberkriminelle mit Verschlüsselungsversuchen Erfolg haben könnten (insbesondere bei Behörden auf Landes- und Kommunalebene) sowie auf eine vergleichsweise hohe Bereitschaft treffen, Lösegeld zu bezahlen. Während dieser Wert im Branchendurchschnitt bei 32 Prozent liegt, sind Behörden mit 42 Prozent am zweithöchsten zahlungsbereit. Nur Energie, Öl und Gas sowie Versorgungsbetriebe greifen mit 43 Prozent noch eher zur Zahlung.

MEHRSCHICHTIGER SCHUTZ MIT MENSCHLICHER EXPERTISE

Ein guter Ansatz, sich gegen Ransomware-Angriffe zu wappnen, ist ein Wiederherstellungs-plan. Diesen besitzen laut der Sophos-Studie 73 Prozent der Behörden auf Landes- und Kommunalebene und 81 Prozent der Bundesbehörden und öffentlichen Einrichtungen. Das wird allein jedoch nicht reichen. Neben regelmäßigen Back-ups, die nach wie vor notwendig sind, ist es wichtiger denn je, Cyberkriminelle von vornherein fernzuhalten oder sie zu entdecken, bevor sie Schaden anrichten können. Derart anspruchsvolle Bedrohungen erfordern intelligente Security-Lösungen, die vorausschauend, vielschichtig und systemübergreifend interagieren. Mit **Sophos Intercept X** in Kombination mit der **XG Firewall** zum Beispiel verfügen Unternehmen über Next-Generation-Security-Technologien und profitieren zudem von den Vorteilen der **Synchronized Security**. Diese Sicherheitstechnologien sind Teil des **Adaptive Cybersecurity Ecosystems,** das zudem die Komponenten der menschlich durchgeführten Prävention und Notfallhilfe durch erfahrene Expert:innen einschließt. Es bildet eine Sicherheitsumgebung, die sich kontinuierlich und automatisch verbessert und in der Lage ist, die verräterischen Taktiken, Techniken und Verfahren frühzeitig zu erkennen und umgehend zu bekämpfen. ■

WEITERE INFORMATIONEN ZUM THEMA

- **Materialien zum Stoppen von Ransomware**
- **Sophos Intercept X Endpoint**
- **Sophos Intercept X Advanced for Server**
- **Sophos XG Firewall**
- **Synchronized Security**
- **Sophos Threat Report 2021**
- **Managed Threat Response (MTR)**

Mehr dazu hier

SOPHOS

Datenschutzorganisationen prüfen und bewerten nach der Systematik der Aufsichtsbehörden

Datenschutzorganisationen prüfen und beurteilen mit begrenztem Zeitaufwand

Ihr ständiger Begleiter im Datenschutz-Management

Ihre DS-GVO Umsetzung smart auditiert und visualisiert ab 259 €.

Kirchliche Stellen mit begrenztem Zeitaufwand zum Datenschutz auditieren

Wie DS-GVO-konform arbeitet Ihr Unternehmen?

Machen Sie den Test mit unseren Excel-Tools!

Bestellen Sie direkt unter: **datakontext.com**

DATAKONTEXT

Schutz vor Ransomware

VORBEREITUNG FÜR DEN IT-ERNSTFALL

Im Juli ruft der Landkreis Anhalt-Bitterfeld nach einer Malware-Attacke den bundesweit ersten Cyber-Katastrophenfall aus. Behörden geraten immer häufiger ins Visier von Hackern und riskieren massive Betriebsunterbrechungen sowie Datenverluste. Können sich öffentliche Verwaltungen gegen Attacken schützen? Zumindest müssen sie sich besser vorbereiten, um Schäden zu minimieren, erklärt André Walsleben, Director Public bei Veeam Software.

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) spricht von Alarmstufe rot, Europol warnt vor zunehmender Cyberkriminalität. Warum Behörden – sind Wirtschaftsunternehmen für Hacker nicht lukrativer?

Lösegeld ist bei Unternehmen vielleicht mehr zu holen, aber auch erbeutete Daten, besonders vertrauliche Bürgerdaten, lassen sich im Darknet gut verkaufen. Manche Hacker wollen auch den Betrieb der kritischen Infrastruktur (KRITIS) in Deutschland stören, zum Beispiel Krankenhäuser oder Versorgungsnetze lahmlegen.

Behörden sind leider auch ein leichteres Angriffsziel: Sie stehen unter Druck, die Digitalisierung voranzutreiben und dabei bleibt die IT-Sicherheit schnell auf der Strecke. Eine Umfrage von BR und ZEIT Online bei den deutschen Bundesländern im Juni ergab, dass in mehr als 100 Fällen IT-Systeme von öffentlichen Institutionen verschlüsselt wurden, um digitales Lösegeld zu erpressen.

Wie kann Verwaltungsdigitalisierung möglichst effizient umgesetzt werden?

Durch einheitliche Plattformen und Lösungen. Das ist ja auch das Prinzip von EfA – Einer für Alle –, auf das sich Bund und Kommunen geeinigt haben, um die Standardisierung von Abläufen und Lösungen zu fördern.

Das Onlinezugangsgesetz (OZG) und die Digitalisierung bedeuten ja aber auch mehr Einfallstore für Hacker?

Die Absicherung personenbezogener Daten ist daher das zentrale Thema, Datensicherung eine Kernaufgabe in der Verwaltungsdigitalisierung. Dabei müssen alle Maßnahmen für Datensicherung und Datenmanagement vereinheitlicht werden. Umfassende und kontinuierliche Datensicherung ist die Basis – für den Tagesbetrieb ebenso wie den Ernstfall. Mithilfe einer Software-Lösung, wie der Veeam Availability Suite, können alle Daten zuverlässig abgesichert und wiederhergestellt sowie die entsprechenden Prozesse zentral gesteuert und überwacht werden. Es geht ja nicht nur um Datenschutz, sondern auch darum, Daten zuverlässig und schnell wiederherzustellen, damit sie für alle Verwaltungsprozesse verfügbar sind. Werden Kommunen von Hackern lahmgelegt, sind ja auch wichtige Bürgerdienste oft über Tage oder Wochen gestört, von Sozialleistungen bis hin zur Kfz-Zulassung.

Es herrscht ja allgemein ein Mangel an IT-Fachkräften. Wie sollen gerade kleinere Kommunen das lösen?

Mit Unterstützung externer IT-Dienstleister, die sich auf öffentliche Verwaltungen spezialisiert haben. Die haben viele, bereits standardisierte Dienst- und Systemleistungen im Angebot, für Verwaltungsprozesse und Bürgerdienste ebenso wie zum Beispiel Datenmanagement – Backup-as-a-Service oder Disaster Recovery-as-a Service – und andere Cloud-Dienste. Bewährte SaaS-Angebote wie Microsoft 365 sind bedienerfreundlich, schnell einsatzfähig und unterstützen die digitale Zusammenarbeit. In Kooperation mit externen IT-Experten lassen sich viele Standardabläufe und Sicherheitsprozesse zuverlässig umsetzen und automatisieren, ob in der Rechteverwaltung, in der Systemüberwachung oder in der Datensicherung.

Würde das nicht bedeuten, dass im Ernstfall vielleicht kein IT-Personal vor Ort ist?

Technische Störungen kommen vor, auch ohne Hacker. Automatische Überwachung und Alarme helfen, Störungen und Ausfälle bereits im Vorfeld zu erkennen und zu minimieren, auch das kann zentralisiert werden. Software vereinfacht zudem die Definition und Automatisierung von Disaster Recovery, inklusive Notfallplänen sowie regelmäßigen Tests und Updates. Und Software kann auch sicherstellen, dass nach einem Systemausfall vordefiniert alle Systeme korrekt und in der richtigen Reihenfolge wieder in Betrieb gehen. ■

Mehr dazu hier

Weitere Informationen:
Veeam Software GmbH,
Tel. 0 89/20 70 42-800,
www.veeam.com/de

VEEAM

RANSOMWARE: TRANSPARENZ IST DIE BESTE VERTEIDIGUNG

Michael Scheffler, Country Manager DACH des Datensicherheitsspezialisten **Varonis,** erläutert die entscheidende Bedeutung der Datentransparenz für den Schutz von Unternehmen vor einer immer komplexeren Bedrohungslandschaft.

Wie haben sich die Techniken und Arbeitsweisen von Cyberkriminellen in den letzten Jahren weiterentwickelt?

Scheffler: Mit dem Aufkommen von Ransomware-as-a-Service muss man nicht einmal mehr selbst ein erfahrener Hacker sein, sondern kann einfach von Anderen entwickelte Tools verwenden, um Ransomware-Angriffe durchzuführen. Zudem bieten Kryptowährungen den Kriminellen die Möglichkeit, hohe Geldsummen zu fordern und dabei relativ anonym zu bleiben. Aber auch die Taktik hat sich verändert. Früher folgten Ransomware-Angriffe meist dem Gießkannen-Prinzip. Heute dringen Angreifer gezielt und sehr subtil in Unternehmen ein, um an wertvolle, sensible Informationen zu gelangen. Sie gehen unauffällig vor, indem sie – oftmals durch Phishing gewonnene – Anmeldedaten autorisierter Benutzer verwenden, um nach wichtigen Informationen zu suchen oder um innerhalb des Netzwerks mehr Rechte zu erhalten, bevor sie diese stehlen, verschlüsseln und ein Lösegeld fordern. Die Forderungen werden dabei immer größer und gehen mittlerweile bis in den Millionen-Euro-Bereich. Cybercrime-Gruppen sind wie die Köpfe der mythischen Hydra: Wenn eine von den Behörden ausgeschaltet wird, was selten genug passiert, formieren sie sich durch die Zusammenarbeit mit anderen Kriminellen sehr schnell um, organisieren sich neu und beginnen erneut mit Angriffen.

Welchen Risiken sind Unternehmen ausgesetzt, wenn sie keine Transparenz über ihre Daten haben?

Scheffler: Das größte Risiko sind übermäßig exponierte Daten. Sie stellen für fast jedes Unternehmen eine große Herausforderung dar. Im

Durchschnitt hat ein Mitarbeiter Zugriff auf etwa 17 Millionen Dateien. Das klingt enorm, und das ist es auch. Wenn nun ein x-beliebiges Konto kompromittiert wird, haben die Cyberkriminellen Zugriff auf alle diese Dateien. Nicht umsonst sprechen wir in diesem Zusammenhang von einem Explosionsradius, denn die Auswirkungen sind ähnlich verheerend.

Die schiere Menge an Daten bedeutet, dass die Angriffsfläche von Unternehmen viel größer ist, als sie sein sollte, und darauf sind Unternehmen nicht vorbereitet. Fehlende Transparenz und damit fehlendes Wissen darüber, wo sich die wichtigsten und sensibelsten Daten befinden, wer Zugriff darauf hat und wer sie verändert, kopiert, gelöscht oder gestohlen hat, macht die Bewältigung eines Angriffs noch schwieriger.

Wie groß ist die Herausforderung speziell für Unternehmensdaten, On-Premises und in der Cloud?

Scheffler: Es ist eine enorme Herausforderung. Die Daten werden an vielen verschiedenen Orten gespeichert und wachsen täglich weiter an. Dies führt zu einer steigenden Komplexität, wodurch wiederum Daten oftmals zu vielen Zugriffsrechten ausgesetzt werden und damit das Risiko weiter steigt. Die meisten Unternehmen sind blind, wenn es um ihre sensibelsten Daten geht. Wenn man nicht weiß, ob ein Nutzer sensible, DS-GVO-relevante Daten auf seinen eigenen Computer kopiert oder vertrauliche Dateien mit persönlichen Informationen geöffnet hat, auf die er keinen Zugriff haben sollte, wird die Identifizierung eines Angriffs sehr schwierig, wenn nicht unmöglich. Wenn man nicht überwacht, wer auf Daten zugreifen kann und was diese Personen mit den Daten machen, wird man unweigerlich klare Anzeichen für einen Cyberangriff übersehen. Ohne detailliertes Wissen über den eigenen Datenbestand ist es unmöglich, verdächtige oder ungewöhnliche Aktivitäten frühzeitig bzw. überhaupt zu erkennen. Und genau dies ist der Schlüssel. Wenn man seinen Explosionsradius kennt, kann man ihn verringern und gezielte Schritte einleiten – und so die Auswirkungen eines Angriffs minimieren.

Wie hilft Varonis Unternehmen dabei, die Datentransparenz zu erhöhen und ihre Cyberabwehr zu verbessern?

Scheffler: Wir haben mit vielen Unternehmen zusammengearbeitet, die bereits von Ransomware betroffen waren, und kennen den Aufwand und die Kosten für die Wiederherstellung nur zu gut. Resiliente Unternehmen verringern proaktiv ihren Explosionsradius, indem sie die Zugriffsrechte auf diejenigen begrenzen, die sie tatsächlich benötigen. Sie archivieren und löschen Informationen, die sie nicht mehr nutzen oder brauchen. Häufig identifizieren wir mehr als 80 Prozent alte Daten, also solche, auf die seit langer Zeit keine Zugriffe erfolgt sind. Bei einer Verschlüsselungsattacke müssen diese ggfs. wieder entschlüsselt werden ohne dass jemand diese Daten benötigt. Im Idealfall werden Altdaten ausgelagert und so vor Angriffen komplett geschützt. Vorbeugung ist der Schlüssel zur Verringerung der Angriffsfläche, und damit beginnen wir bei allen unseren Kunden. Man muss sein Ökosystem kennen und dann so viele Präventionsmaßnahmen wie möglich ergreifen, um die Angriffsfläche zu verringern.

Wir adressieren zudem auch Insider-Bedrohungen, ganz gleich, ob es sich dabei um kompromittierte Konten oder um gezielte Aktionen von Mitarbeitern handelt. Es ist wirklich schwierig festzustellen, wann ein loyaler Mitarbeiter, der Zugang zu sensiblen Daten hat, plötzlich anfängt, sich verdächtig zu verhalten. Einer unserer Kunden entdeckte einen Mitarbeiter, der geheime Preisinformationen stahl, die er an einen Konkurrenten weitergeben wollte. Das Unternehmen konnte ihn daran hindern, weil es Einblick in die Vorgänge um seine sensibelsten Daten hatte.

Michael Scheffler, Country Manager DACH von Varonis Systems

Wie wird sich die Cyberrisikolandschaft Ihrer Meinung nach weiter verändern?

Scheffler: Einerseits werden sich die Techniken und Taktiken der Cyberkriminellen immer weiterentwickeln. Andererseits sehen wir, nicht zuletzt durch die Pandemie beschleunigt, deutlich veränderte Unternehmensinfrastrukturen. Remote- und Hybridarbeit ersetzen die traditionellen On-Premises-Netzwerke durch Netzwerke ohne Perimeter, in denen jeder Laptop oder jedes Mobiltelefon zu einem Einfallstor zu kritischen und sensiblen Daten wird. All dies macht es nur noch wichtiger, einen Überblick über die Unternehmensdaten zu erhalten. Zudem macht es Sinn sich mit Lösungen zu befassen die nicht den klassischen Useransatz nutzen. Es wird immer wichtiger, die Zugriffe auf Daten zu erfassen und sich nicht darauf zu verlassen, dass eine Userberechtigung passen wird. Ein Benutzer, der trotz Berechtigung nie auf sensible Daten zugegriffen hat und plötzlich anfängt dies zu machen, ist ein echtes Risiko, da alle klassischen auf der Userberechtigung basierenden Ansätze hier zu versagen drohen. ■

Mehr dazu hier

VARONIS

powered by GDD

Foto: peshkova - AdobeStock

Der einfache Weg zum organisierten Datenschutz!

DA DATA AGENDA Datenschutz Manager

Der Experte an Ihrer Seite!

- ✓ webbasiert, On Premise oder PC-/Laptop Installation
- ✓ professionelle Schritt-für-Schritt Anleitung mit vielen Vorlagen
- ✓ einfaches Erfassen und Dokumentieren aller Datenschutzmaßnahmen
- ✓ effektive Zusammenarbeit aller verantwortlichen Stellen
- ✓ besonders für externe DSBs geeignet: Alle Mandanten in einem System

Jetzt informieren: **www.DataAgenda.de/datenschutzmanager**

DATAKONTEXT

Cybersicherheit für Industrie und KRITIS

IOT- UND OT-STANDARDS BILDEN DAS RÜCKGRAT

Für die Industrie gibt es ein allgemeines und ein spezielles Risiko bezüglich der IT-Sicherheit aufgrund fortschreitender Technologie – je nach Branche. Neuerungen rund um die Bereiche IoT (Internet of Things), OT (Operational Technology) und ICS (Industrial Control System) können neue Schwachstellen auftreten lassen oder alte in den Vordergrund rücken, die bisher nachlässig betrachtet wurden. Klare Richtlinien über Branchen hinweg würden für mehr Sicherheit und Verlässlichkeit sorgen.

Das Ziel ist klar: Die sichere Vernetzung von Geräten und Anlagen. Das gilt besonders für Produktionsstätten in der Industrie: Die Geräte und Maschinen in den Fabriken wurden in den letzten Jahren vernetzt und an das Internet angeschlossen. Konzepte für Cybersicherheit gab es in diesem Bereich nicht, denn bei der Entwicklung dieser Maschinen war der Gedanke an Vernetzung – zumal global über das Internet – noch völlig fremd. Zum Beispiel können die veralteten SCADA-Protokolle als Betriebssysteme zur Bedrohung werden. Wirksamer Schutz erfordert daher nicht nur Fachwissen über IT-Sicherheit, sondern die Kenntnis der Branche. Das Thema ist sehr komplex. Aus diesem Grund ziehen sich solche Initiativen jedoch oft lange hin und führen zu ungeplant hohen Kosten. Oft verfolgen die Verantwortlichen dabei unterschiedliche Interessen, was die Konsensbildung erschwert. Dennoch hat sich in letzter Zeit einiges getan.

BESTEHENDE STANDARDS UND BEDARF AN KONTINUIERLICHER ZUSAMMENARBEIT

In Deutschland gibt es seit einiger Zeit Bestrebungen, kritische Infrastrukturen (KRITIS) besser abzusichern. Das Projekt „UP KRITIS“ ist eine öffentlich-private Kooperation zwischen KRITIS-Betreibern, deren Verbänden und den zuständigen staatlichen Stellen. Besonders im Bereich der Energieversorgung oder des Gesundheitswesens sind einheitliche Standards für industrielle Netzwerke und die eingesetzten Produkte von weitreichender Bedeutung. Von Seiten des Bundes war zuletzt mit der Einführung des IT-Sicherheitsgesetz 2.0 im Frühjahr 2021 erneut Bewegung in die Thematik gekommen. Außerdem gibt es auf internationaler Ebene Bestrebungen zur Vereinheitlichung der Richtlinien. Im Juni 2020 legte das ETSI (European Telecommunications Standards Institute) mit dem Sicherheitsstandard ETSI EN 303 645 eine neue Zertifizierung für IoT-Produkte vor, welche danach um technische Spezifikationen ergänzt wurde. Diese gemeinnützige Organisation zählt in Deutschland derzeit 143 Mitglieder und ist von der EU als Europäische Organisation für Normung anerkannt. Ziel ist es, weltweit anwendbare Standards für die Informations- und Kommunikationstechnologie zu ersinnen. Von behördlicher Seite wurde bereits vor einigen Jahren ein Dokument der ENISA (European Network and Information Security Agency) mit dem Titel geschaffen: Baseline Security Recommendations for IoT in the context of Critical Information Infrastructures. Derzeit dient es aber lediglich als Anhaltspunkt für Initiativen und Entwicklungen.

NACHHOLBEDARF BEI IOT-GERÄTEN UND INDUSTRIE-SYSTEMEN

Festhalten lässt sich: Es gibt Bemühungen von Seiten der Industrie und der Staaten, branchenübergreifende Grundnormen einzurichten. Diese müssen nach ihrer Festlegung langsam von der Industrie übernommen werden, bis über alle Hersteller hinweg dafür gesorgt wurde, dass IoT-Geräte bereits ab Werk, das heißt von der Konzeption an, bis zur Konstruktion gesichert und Sicherheitslücken einheitlich geschlossen werden. Dies erfordert sowohl IT-Sicherheit- als auch Branchen-Wissen, weswegen es eines Wissenstransfers und -austauschs zwischen Technik- und Sicherheitsexperten bedarf, um gemeinsam zu verstehen und umzusetzen, was für eine effektive Bewertung des Cyberrisikos notwendig ist.

EXKURS

Während Fahrzeuge bereits gewisse Standards in Sachen der Sicherheit – auch bezüglich der IT-Sicherheit – erfüllen müssen, bevor sie eine Straßenzulassung bekommen, gibt es im IoT-Sektor vergleichbare Vorgaben nicht, obwohl diese Geräte den Alltag beherrschen. Diese Geräte können aber selbst ein Risiko darstellen, weil sie oft als Gateway zu größeren Netzwerken fungieren, was eine Gefahr für die gesamte Netzwerkstruktur darstellt. Aus diesem Grund sind Normen und gemeinsame Grundlagen dringend erforderlich. Die Herstellung und Verwendung solcher Geräte muss bereits beim Bau überwacht werden, um deren Sicherheit für den Nutzer zu gewährleisten. Das bedeutet: diese Geräte müssen von Anfang an mit einem Sicherheitdesign erdacht werden.

NETZWERKSEGMENTIERUNG HILFT DER INDUSTRIE

Ähnliche Forderungen gelten für den Bereich der digitalen Industrieanlagen – besonders den der KRITIS-Betreiber: einheitliche Standards schaffen. Bei modernen ICS, wie der Fabrikautomation oder Prozesssteuerung, zeichnet sich der Trend zum Einsatz von Apps auf Smartphones und Tablets ab. Diese werden meist, ähnlich wie konventionelle HMI (Human Machine Interfaces), zur Visualisierung und Parametrierung verwendet. Darüber hinaus gibt es weitere Anwendungsfälle, wie die Integration in Konzepte für Fernwartung und Ferndiagnose. Solche Netzwerke werden schnell gefährdet, wenn einzelne dieser mobilen Geräte ein Einfallstor für Bedrohungen sein können. Hier hilft als Maßnahme die Netzwerk-Segmentierung, einschließlich der logischen Trennung klassischer Office-IT-Netze und industrieller Shopfloor-OT-Netzwerke. Dies kann zum Beispiel durch die Aufteilung von Web-Servern, Datenbank-Servern und Standard-Benutzermaschinen in eigene Segmente geschehen, die getrennt sind und an deren Grenzen der Netzwerkverkehr scharf kontrolliert wird. Malware, wie Ransomware, oder Hacker werden dann nach erfolgtem Einbruch in einem Segment „eingesperrt" und können nicht von System zu System springen. Außerdem trägt die Netzwerk-Segmentierung zu einer effizienten Überwachung und Prüfung auf Sicherheitslücken bei, weil jeder Teil für sich betrachtet werden kann.

HARMONISIERUNG DER GLOBALEN VORSCHRIFTEN

Entscheidend für den Erfolg der verschiedenen Standards und Normen, auch der künftigen, ist die Harmonisierung der Anforderungen. Sie wären dann einfach zu übernehmen, zu verstehen und umzusetzen. Die Charter of Trust, eine Cybersecurity-Allianz von Unternehmen und Organisationen dieser Welt, arbeitet über Branchen und Länder hinweg zusammen, um sogenannte Baseline Requirements, also Grundanforderungen, für die Sicherheit im Bereich der Lieferkette zu entwickeln. Diese Anforderungen werden bereits auf gültige Standards und bewährte Verfahren abgestimmt.

Zudem werden für internationale Normen, wie die IEC 62443, grundlegende Anforderungen von den Standardgebern so entwickelt, dass sie sich einheitlich implementieren lassen. Sie orientieren sich an den jeweils geltenden Vorschriften und Normen, wodurch eine leichtere Übernahme und Kompatibilität mit verschiedenen globalen Normen und Vorschriften gewährleistet wird. Diese Kompatibilität zu den verschiedenen Richtlinien macht die Anforderungen transparent und prüfbar durch unabhängige Tests. Dies schafft Vertrauen in die Unternehmen.

STELLENWERT VON VERIFIZIERUNG UND TESTS FÜR DIE SICHERHEIT VON GERÄTEN

Jedes Gerät, welches mit dem Internet verbunden ist, kann zu einem Ziel von Angreifern werden, die versuchen, es zu übernehmen. Daher ist eine neutrale Bewertung der IT-Gefahren für die Gewährleistung der Sicherheit dieses Geräts von entscheidender Bedeutung. Eine solche Bewertung durch entsprechende Tests und simulierte Angriffe erlaubt es einem Hersteller, etwaige Schwachstellen zu ermitteln. Die Prüfung kann dabei gemäß den geltenden allgemeinen Normen oder nach spezifischen Vorgaben der Branche erfolgen. Einfache Dinge, wie die Prüfung der Passwörter, Software-Updates oder die Meldung von Schwachstellen, werden immer verlangt. Tiefergehende Penetrationstests können jedoch jederzeit zusätzlich durchgeführt werden. Auf diese Weise lassen sich IT-Bedrohungen für das Netzwerk früh erkennen und es kann die Sicherheit des Geräts erhöht werden.

AUF DEM WEG ZU EINHEITLICHEN STANDARDS

Verschiedene Akteure bemühen sich also bereits, einheitliche Regulierungen zu schaffen, um im Sinne aller, die Industriesysteme sicherer zu gestalten. Die Harmonisierung der Richtlinien sorgt für geringeren Aufwand bei Planung und Koordination, erhöht die Transparenz der Abläufe und Anforderungen, und macht die Bewertung des Risiko einfacher. Die große Vereinheitlichung dieser Regularien über Länder und Kontinente hinweg ist zwar ein weit entferntes Ziel, doch die Industrie-Vertreter, Regulierer und Beamten sind bereits auf einem guten Weg. ■

SUDHIR ETHIRAJ,
Global Head of Cybersecurity Office (CSO), TÜV SÜD

Wir qualifizieren die Digitalwirtschaft.

Die Bitkom Akademie ist seit 2005 der erste Ansprechpartner für die Weiterbildung von Fach- und Führungskräften zu IT-Themen und digitalen Trends.

Alle Seminare unter:
www.bitkom-akademie.de

bitkom akademie

Maßnahmen für Unternehmen im Ernstfall

HACKERANGRIFF! WAS NUN?

Vielleicht wurde eine kompromittierte E-Mail geöffnet oder Angreifer nutzten in der Breite eine Sicherheitslücke wie beim Microsoft Exchange Server im Frühjahr 2021: Hackerangriffe sind eine reale Bedrohung für Unternehmen und können schnell teuer werden. Wenn der Worst Case eintritt, gilt es Ruhe zu bewahren und möglichst keine Beweise, das heißt, Angriffsspuren zu vernichten. Dann kann ein Incident-Response-Team an die Arbeit gehen, das Einfallstor und den Angriff nachvollziehen und die Integrität der Systeme wiederherstellen.

Ein Unternehmen ist ins Visier von Hackern geraten, Fehlermeldungen tauchen auf, vielleicht wurden erste Systemteile bereits gesperrt und Erpressungsbotschaften übermittelt. Der Angreifer wird versuchen, zu Accounts mit mehr Rechten vorzustoßen, um Daten zu stehlen oder mit einem Trojaner Systeme zu verschlüsseln. Erreicht er die Domain-Controller-Privilegien, ist das der Worst Case für Unternehmen, da dem Angreifer damit im wahrsten Sinne des Wortes alle Türen offenstehen.

Wenn Unternehmen einen Angriff bemerken, breitet sich schnell Panik aus, Mitarbeiter werden nach Hause geschickt und man versucht, den Schaden zu begrenzen. Hier gilt: Ruhe bewahren und so schnell es geht einen Experten einschalten, der mit einem Incident-Response-Team den Angriffsverlauf nachvollziehen und Empfehlungen geben kann, welche Systeme mit welchem Back-up wiederhergestellt werden können. Um den Cyberdetektiven die Arbeit zu erleichtern, sollten Unternehmen einiges beachten. Optimal ist es, wenn ein IT-Experte bereits den Umfang des Schadens abschätzen kann.

MALWARE NICHT LÖSCHEN, SYSTEME WENN MÖGLICH ISOLIEREN

Malware darf, wenn sie identifiziert wurde, nicht gelöscht werden. Das erschwert dem Response-Team die Arbeit, da auf diese Weise Spuren vernichtet oder manipuliert werden können. Zudem kommt der Löschvorgang meistens zu spät, und die Wahrscheinlichkeit, alle betroffenen Systeme zu identifizieren, ist gering. Besser ist es, das System im Ist-Zustand zu belassen, sodass die Experten Beweise wiederfinden und analysieren können und Rückschlüsse auf die Vorgehensweise des Angreifers und seine Tools möglich werden. Auch eine Weiternutzung des Systems sollte wenn möglich unterbleiben. Es ist ebenfalls nicht ratsam, Back-ups selbst einzuspielen, da auch diese infiziert sein können.

Sinnvoll kann es dagegen sein, die infizierten Systeme wenn möglich zu isolieren. Zwar weiß der Angreifer dann, dass er entdeckt wurde, eine frühe Isolation kann ihn aber daran hintern, sich im Netzwerk weiter fortzubewegen. Allerdings besteht die Gefahr, dass die Isolation nicht vollständig gelingt, wenn der Angriffsumfang noch nicht bekannt ist. Es ist deswegen wichtig, eine valide Einschätzung geben zu können, wie weit der Hacker vorgedrungen ist – für die meisten Systemadministratoren keine einfache Aufgabe.

Es ist zudem sinnvoll, das Netzwerk zu trennen, bei einem Laptop das WLAN auszuschalten und an den Strom anzuschließen. Das Vorgehen bei Servern hängt von ihrer Funktionsweise und Verwendung ab: Ist ein Server geschäftskritisch, weil er zum Beispiel den Online-Shop bereitstellt, wäre es ratsam, das Gerät zu isolieren, da ein Angreifer sich sonst im Netzwerk ausbreiten kann. Das betroffene Unternehmen muss die Entscheidung fällen – grundsätzlich ist meist aber empfehlenswert, lieber mehr statt weniger zu isolieren.

Im Fall von Ransomware-Attacken sind Back-ups der einzige Weg, die Systeme wiederherzustellen. Deswegen müssen sie gesondert außerhalb des Netzwerks gesichert werden und offline verfügbar sein. Nur so laufen Unternehmen nicht Gefahr, dass ihre Back-ups bei einem Angriff mitverschlüsselt und damit wertlos werden.

SYSTEMVERHALTEN ÜBERWACHEN UND AUFFÄLLIGKEITEN SCHNELL ERKENNEN

IT-Verantwortliche haben die Möglichkeit, das Verhalten der Systeme und Prozesse zu überwachen, Daten aller Geräte im Netzwerk zu sammeln und zu visualisieren, was im Angriffsfall schnelle Rückschlüsse erlaubt und eine solide Entscheidungsbasis darstellt. So können zum Beispiel Meldungen von Antiviren-Scanner an den Admin kommuniziert werden, über die sonst nur der User im Bilde ist. Mit einer solchen zentralen Lösung können durch die Auswertung bestenfalls Angriffsmuster sofort entdeckt werden, etwa, wenn sich auf einem Gerät hunderte Log-in-Versuche in wenigen Minuten häufen.

Alle Beobachtungen und ergriffenen Maßnahmen sollten für das Einsatzteam schriftlich und formlos dokumentiert werden. Sie sollten möglichst genau und dürfen gern ausführlich sein. Dazu gehören alle Änderungen, die am System vorgenommen wurden, wie ein Neustart, aber auch das Verhalten des Systems oder Hinweise

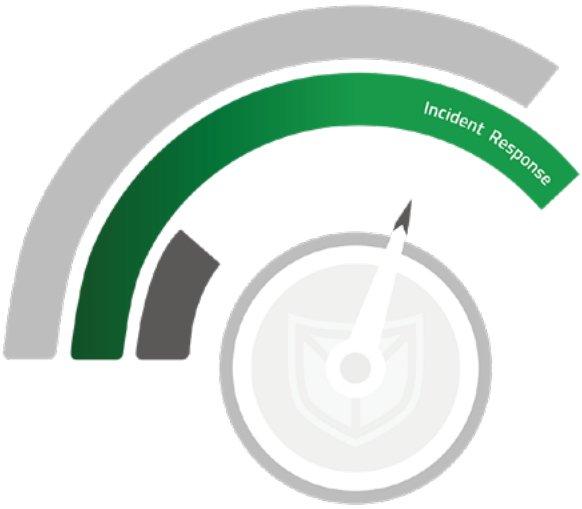
von Mitarbeitern, etwa, wenn Phishing-mails eingegangen sind, die nach wie vor das zentrale Einfallstor für Hacker-angriffe sind. Diese Verdachtsmomente sind relevant, ebenso Antworten auf die Fragen: Wer hat das System als Letzter benutzt, und was wurde im System gemacht, nachdem der Angriff bemerkt wurde? Zentral ist hier die Frage, was wann passiert ist. Denn herrscht Klarheit über den Beginn des Angriffs, kann zum Beispiel die Sicherheit von Back-ups eingeschätzt werden, wenn sie vor dem Angriff erfolgt sind.

DIE CYBER-DETEKTIVE VOLLUMFÄNGLICH MIT INFORMATIONEN VERSORGEN

Ist das Einsatzteam im Bilde, werden im nächsten Schritt der Scope (Umfang) und der Auftrag, das Einsatzziel, festgelegt: Welche Unterstützung benötigt das Unternehmen – wurden Daten entwendet, soll der Angriffsverlauf festgestellt werden, welche Systeme sind sauber, muss eine Wiederherstellung beziehungsweise ein Wiederaufbau erfolgen? Von den Antworten hängen die Werkzeuge ab, die das Einsatzteam mitbringt. Meist geht es darum, den Patient Zero in einer Root-Cause-Analyse zu finden und festzustellen, welche Systemteile infiziert sind.

Die Cyber-Detektive nutzen dann die zur Verfügung stehende Information und verschiedene Datenquellen, um dem Angreifer auf die Spur zu kommen: Das Team benötigt optimalerweise eine Übersicht der IT-Systeme mit Servern und Clients, der Art der Systeme – Windows, Linux oder Mac – und muss wissen, ob Mitarbeiter mit eigenen Geräten arbeiten dürfen, was nicht nur ein zusätzliches Risiko für Angriffe darstellt, sondern auch den Datenschutz erschwert. Aus der Logging-Policy gehen Prozesse und Verhalten von Sicherheitssystemen hervor, etwa, welche Quellen angebunden sind und in welchen Zyklen geloggt wird. Auch Sicherheitstools verfügen meist über eine Aufzeichnungsfunktion und liefern weitere Informationen.

Im besten Fall sind die Netzwerke segmentiert und die User mit Rollen und Zugriffsrechten ausgestattet, was einen Angriff erschwert. Wichtig für das Einsatzteam ist darüber hinaus die Kenntnis des Patch-Standes der Systeme, besonders der Webserver, die von außen erreichbar sind. Wurden diese seit einer längeren Zeit nicht mehr gepatcht, können sie ein wahrscheinliches Einfallstor für Hacker sein. Threat Intelligence in Form einer technischen Beschreibung von Spuren vergangener Angriffe lassen potenziell Rückschlüsse auf den aktuellen Fall zu: Im Frühjahr 2021 sorgte zum Beispiel eine Sicherheitslücke im Microsoft Exchange Server für eine Welle erfolgreicher Angriffe.



Ein Incident-Response-Team sollte nach einem Angriff frühzeitig eingesetzt werden, um das Einfallstor und den Angriff nachzuvollziehen und die Integrität der Systeme wiederherzustellen. (Quelle: SECUINFRA)

IM AUSTAUSCH BLEIBEN UND AUS FEHLERN LERNEN

IT-Verantwortliche und Response-Experten stehen während des Einsatzes im engen Austausch. So wird zum einen sichergestellt, dass das Response-Team alle notwendigen Informationen erhält und andererseits die IT-Verantwortlichen auf dem aktuellen Stand bleiben. Formlose Telefonate eignen sich für den täglichen Austausch. Hilfreich für das Einsatzteam ist dabei die Teilnahme eines IT-Spezialisten, der Fragen zu Systemen beantworten kann, sodass das Team diese Informationen nicht erst mit einer aufwendigen Analyse erschließen muss. Der zeitliche Umfang, bis ein Angriff abgewehrt werden kann, hängt von diversen Faktoren ab.

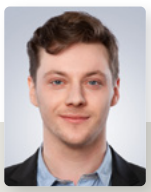
Ein Incident ist immer ein Schock und meist teuer – er kostet Zeit, Geld, Ressourcen und bringt negative PR. Deswegen ist es umso wichtiger, daraus zu lernen und Handlungsempfehlungen mitzunehmen, wie man Angriffen künftig vorbeugen und seine Systeme sichern kann. Die Bedeutung von Cyber Security wird Unternehmen meist erst dann klar, wenn ein Angriff erfolgt ist. Auch hier kann das Response Team eine erste Empfehlung geben, welche Tools notwendig sind, um das Sicherheitsniveau zu erhöhen.

Unternehmen sollten außerdem die Kommunikation mit Behörden und ihre Meldepflichten berücksichtigen. Abhängig vom Schaden wie etwa Datenabfluss müssen verschiedene Stellen benachrichtigt werden, bei Unternehmen mit KRITIS-Status zum Beispiel das BSI (Bundesamt für Sicherheit in der Informationstechnik).

Ob ein Krisenmanager eingesetzt wird, entscheidet das Unternehmen. In manchen Fällen ist diese Rolle auch durch externe Dienstleister besetzt. Ihre Funktion besteht darin, die Organisation zu leisten und interdisziplinär zu arbeiten. Denn von einem Angriff ist die Rechtsabteilung eines Unternehmens meist ebenso betroffen wie die Kommunikation.

FAZIT

Ein Hackerangriff paralysiert viele Unternehmen. Besser ist es, Ruhe zu bewahren und Experten hinzuzuziehen. Je weniger an den Systemen gemacht wird, umso besser – auf diese Weise werden keine Spuren verwischt und das Incident-Response-Team kann den Angriffsverlauf leichter nachvollziehen, die Systeme bereinigen und wiederherstellen. ■



EVGEN BLOHM,
Cyber Defense Consultant beim SECUINFRA Falcon Team

Bild: ©Andrew Derr - stock.adobe.com

Interview mit William Carter

KOMMT MIT DEM AUFSTIEG DER QUANTENCOMPUTER DAS ENDE DER BLOCKCHAIN?

Mit dem Jahr 2022 am Horizont trennen uns laut Experten nun lediglich vier Jahre von dem Zeitpunkt, an dem Quantencomputer dazu in der Lage sein könnten, Blockchain-Sicherheit zu umgehen. Und das, während der Markt an Blockchain-Anwendungen kontinuierlich wächst und sich über DeFi (Dezentralisierte Finanzmärkte), NFTs (Non-Fungible Token), das Web 3.0, Gaming, bis hin zu Logistik und Smart Manufacturing erstreckt. Gleichzeitig helfen Quantencomputer bereits dabei, noch bessere Versionen ihrer Selbst zu entwickeln und werden zeitnah in der Cloud verfügbar. Ist damit bereits vor dem Durchbruch das Ende von Blockchain-Systemen und dem Versprechen auf Sicherheit absehbar? Die Antwort darauf verrät William Carter, CTO bei xx network, im Gespräch mit IT-SICHERHEIT.

ITS: Wie sehen Sie die Entwicklung des Quantencomputing und wie können sich Quantencomputer selbst verbessern?

William Carter: Die Entwicklungen im Bereich der Quanteninformatik haben im letzten Jahr rasante Fortschritte gemacht. Seit IBM seinen ersten kommerziellen Quantencomputer vorgestellt hat, häufen sich die Nachrichten fast täglich. Es ist schon beeindruckend, wie schnell hier in letzter Zeit Fortschritte erzielt wurden. Das kürzliche Investment von Trumpf in ein Unternehmen, welches spezielle Chips entwickelt, die Quantenberechnungen auf herkömmliche binäre und elektronische Computer bringen sollen, spricht ganz klar für eine starke Fokussierung auf Quantentechnologien in der Zukunft. Schließlich bieten Quantencomputer ganz neue Rechenkapazitäten und dementsprechend auch schnellere Chancen zur Verbesserung. Wir nutzen bereits bestehende Computer, um herauszufinden, wie man die Rechenleistung verbessern kann und genauso arbeitet es sich von nun an mit Quantencomputern. Sie verbessern sich also gewissermaßen auf Dauer selbst. Natürlich stehen wir erst am Beginn – Quantencomputer werden kaum kommerziell genutzt, sondern vormalig für die riesigen Datenmengen in der Forschung verwendet. In fünf bis zehn Jahren rechnen Experten mit der ersten kommerziellen Nutzung. Das bedeutet aber auch, dass Quantenhacking, also Angriffe von Quantencomputern aus, dann ein Thema werden.

ITS: Wo liegen die Schwächen heutiger Blockchains hinsichtlich Quantenfestigkeit?

William Carter: Eigentlich sind nicht nur Blockchains das Problem, sondern vielmehr ist unsere ganze digitale Welt angreifbar, weil sie mit veralteter asymmetrischer Verschlüsselung abgesichert wird. Onlinebanking, der Log-in auf einer Seite oder im Bitcoin-Wallet – alles basiert auf dem Grundprinzip der Public-Key-Authentifizierung, bei welcher der rechtmäßige Besitzer den öffentlichen Schlüssel in Form einer langen Zahlenreihe nur durch den passenden privaten Schlüssel entziffern kann. Ein normaler Computer kann den privaten Schlüssel für die Authentifizierung oder den RSA-Algorithmus nicht knacken, weil es viele Jahre dauern würde, um die möglichen Zahlenkombinationen zu errechnen. Ein Quantencomputer kann hingegen aufgrund seiner hohen Geschwindigkeit und Rechenkraft, sowie mithilfe eigener für Quantencomputer entwickelten Algorithmen (z.B. dem Shor-Algorithmus) die Faktorisierung in kürzester Zeit durchführen und so die Verschlüsselung brechen.

ITS: Was passiert mit digitalen Währungen wie Bitcoin in ein paar Jahren, wenn ihre Blockchain nicht modernisiert wird?

William Carter: Bis zum Jahr 2030 werden Quantencomputer wahrscheinlich für verschiedene Regierungen, Unternehmen und finanzstarke Einzelpersonen verfügbar sein. Wenn Kryptowährungen bis dahin nicht quantensicher sind, wird dies zu großen Sicherheitsproblemen führen: Derzeit gehen Experten davon aus, dass ein Quantencomputer die aktuellen Verschlüsselungsalgorithmen ab einer Leistung von 70 Qubits knacken kann, was auch Bitcoin-Wallets angreifbar machen würde. Zum Vergleich: Der neue Quantencomputer von IBM und Fraunhofer ist der schnellste in Europa und hat bereits 27 Qubits – wir müssen also schnell handeln. In Zukunft werden Quantenhacker in der Lage sein, ihre eigenen Quantencomputer zu nutzen, um Wallets zu umgehen oder Transaktionen zu manipulieren, noch bevor sie getätigt wurden, indem sie einfach den privaten Schlüssel der Wallet-Inhaber berechnen. Um es klar zu sagen: Eine Person mit einem Quantencomputer wird in der Lage sein, den Besitz und die Kontrolle über ein beliebiges Wallet zu erlangen, indem sie den privaten Schlüssel knackt. Solche Angriffe werden das Vertrauen in Währungen und die Blockchain-Technologie völlig untergraben. Auch wenn die Quantensicherheit in den meisten Bereichen derzeit noch ein „nice-to-have" ist, wird sie zu einem entscheidenden Wettbewerbsvorteil werden, wenn Quantencomputer kommerziell genutzt und damit günstiger werden.

ITS: Sind aktuelle Blockchain-Technologien aufrüstbar, um quantensicher zu sein? Wenn ja, wie?

William Carter: Bestehende Blockchain-Konsensprotokolle können nicht ohne Weiteres auf quantenresistente Kryptografie umgestellt werden, indem die derzeit verwendete ECDSA-Kryptografie ersetzt wird. Das Problem ist ein zweifaches: Die Mechanismen zur Änderung des Codes sind nicht einfach anzuwenden, und die

bestehende Kryptografie ist im Code weitverbreitet, so dass eine Umstellung in der Praxis sehr schwierig wäre. Schlimmer noch: Aufgrund der Art und Weise, wie die meisten Protokolle, einschließlich Bitcoin und Ethereum, konzipiert sind, würde die einfache Einführung von Quantensignaturen die Leistung dieser Blockchains aufgrund des enormen Rechenaufwands für die Nodes und die Inhaber von Wallets erheblich beeinträchtigen.

Um quantensichere Algorithmen zu verwenden, sollte eine Blockchain von Grund auf dafür ausgelegt sein. Für unsere Blockchain, die zum Beispiel für xx-consensus genutzt wird, haben wir einen solchen Algorithmus entwickelt: Die Blockchain besteht aus einer Blockchain-Datenstruktur – in der Transaktionsergebnisse unveränderlich veröffentlicht werden – und einem Konsensmechanismus, um eine kollektive Vereinbarung über den Zustand der Daten durch ein Quorum einer kleinen Gruppe zufällig ausgewählter Nodes zu erzwingen. Und diese xxnodes nutzen ein neuartiges, effizientes Gruppensignaturverfahren, das hashbasiert ist. Wir haben es entwickelt, um die Kommunikation und die Zustimmung der Nodes zu beschleunigen. Auf diese Weise erreicht die Blockchain lineare Skalierbarkeit, hat geringe Latenzzeiten und ist sicher. Dies funktioniert auch bei großflächigen Ausfällen, etwa wenn bis zu einem Drittel des Netzwerks kompromittiert wird.

ITS: Was bedeutet Proof of Quantum und wo liegen die wesentlichen Unterschiede zu bisherigen Technologien?

William Carter: Die Kernkomponente einer dezentralen Blockchain ist der Konsensalgorithmus, der eine Einigung zwischen den Nodes im Netzwerk ermöglicht. Dieser legt auch fest, welcher Node den nächsten Block erzeugen darf. Diese Konsensmechanismen basierten größtenteils auf dem Proof-of-Work (PoW)-Verfahren, während neuere Blockchains meist eine Version von Proof-of-Stake (PoS) mit ECDSA, einem alten Kryptoverfahren, verwenden.

Für xx consensus verwenden wir den xx BFT Konsensmechanismus, der extra für Quantensicherheit entwickelt wurde und einige Verbesserungen gegenüber herkömmlichen BFT-Mechanismen beinhaltet. Jeder Block beinhaltet dabei einen nicht manipulierbaren Zufallswert, auf dessen Basis die Nodes aus dem Netzwerk ausgewählt werden, die dann den nächsten Block produzieren. Gleichzeitig haben wir zwei neue Ausweichmechanismen eingeführt, sollten diese ausgewählten Nodes zu keiner Einigung kommen oder sich betrügerisch verhalten. Das allein reicht aber noch nicht, um die Quantensicherheit zu gewährleisten. Hierzu verwenden wir ein spezielles, quantensicheres Signaturverfahren. Diese Signaturen, die wie Winternitz-OTS+-Signaturen hashbasiert sind, werden verwendet, um die Validität von Blöcken und Transaktionen festzustellen. Normalerweise benötigen solche Signaturen im Verhältnis relativ viel Speicherplatz, was die Verwendung der Technologie auf mobilen Endgeräten verhindern würde. Mit xx BFT haben wir diese Signaturen noch einmal kompakter gestaltet, damit Nutzer xx-consensus auch auf ihren Handys verwenden können. Insgesamt erreichen wir durch xx BFT nicht nur Quantensicherheit, sondern auch lineare Skalierbarkeit mit der Anzahl der Nodes und einen geringeren Energieverbrauch als herkömmliche Blockchain-Infrastrukturen.

ITS: Was bedeutet die neue Technologie für den Stromhunger von Blockchains?

William Carter: Das Proof-of-Work-(PoW-)Verfahren ist rechenintensiver, was auch einer der Gründe ist, warum die Ethereum-Blockchain derzeit auf ein Proof-of-Stake (PoS)-Verfahren umgestellt wird. xx BFT basiert nicht auf dem PoW-Verfahren, sondern wir verwenden unser eigenes effizientes Signaturschema in Kombination mit einer Version von „Nominated" PoS, um sicherzustellen, dass unsere Blockchain extrem effizient auf normaler Konsumenten-Hardware läuft.

ITS: Wann sehen Sie den Einsatz in kommerziellen Lösungen?

William Carter: Bislang sind PoW-Blockchains langsam und teuer in der Nutzung, weshalb viele der Anwendungen finanzieller Natur sind und mit dem Aufbau einer kryptobasierten Finanzanlagekategorie zu tun haben. Außerdem werden bei Blockchain dezentralisierte Ledger verwendet, in denen Transaktionsaufzeichnungen und Daten öffentlich veröffentlicht werden, was für die meisten Unternehmen ein Problem darstellt, da sie wichtige Wettbewerbsinformationen nicht preisgeben wollen. Unternehmen sind außerdem über die Sicherheit von Plattformen besorgt, die von Servern betrieben werden, über die sie keine Kontrolle haben. Diese Sicherheitsbedenken nehmen angesichts des Aufkommens von Quantencomputing noch zu.

Deswegen arbeiten wir derzeit am xx messenger, einem Messenger-Dienst, der wirklich privat ist. Dasselbe xxdk-Softwarepaket, das der Messenger für den Zugriff auf das xx Netzwerk verwendet, kann von Unternehmen genutzt werden, um die vertrauliche Übertragung von Daten und Nachrichten zu gewährleisten. Es gibt eine Reihe von Problemen mit bestehenden Nachrichten- und Kommunikationssystemen:

- Erstens wird die Ende-zu-Ende-Verschlüsselung von zentralisierten Unternehmen kontrolliert, die selbst Zugriff auf alle Nachrichten haben.
- Zweitens verwendet die Ende-zu-Ende-Verschlüsselung das veraltete ECDSA-Verschlüsselungsverfahren, das durch Quantencomputer geknackt werden kann.
- Und drittens geben alle Nachrichtensysteme Informationen über die Metadaten preis, zum Beispiel mit wem man spricht, wie viel und wann.

Durch die Kombination von Ende-zu-Ende-Verschlüsselung und cMix-Metadaten-Shredding-Technologie bieten wir Anonymität zwischen den Parteien, die das Netzwerk nutzen. Unsere Technologie unterbricht die Verbindung zwischen Absender und Empfänger und eliminiert den digitalen Fußabdruck vollständig. Die Daten verbleiben beim Absender. Und durch die Verwendung des quantensicheren, effizienten, skalierbaren xx Konsensprotokolls und der Blockchain können wir alle Informationen und Daten vor Manipulationen schützen und gleichzeitig eine leistungsstarke Plattform anbieten. Die Behebung von Schwachstellen in den Bereichen Datenschutz, Sicherheit und Leistung wird für die kommerzielle Nutzung der Blockchain-Technologie entscheidend sein.

ITS: Vielen Dank für das Gespräch!

Das Interview mit William Carter führte Stefan Mutschler, Chefredakteur IT-SICHERHEIT

Geschäftliche E-Mail-Kommunikation

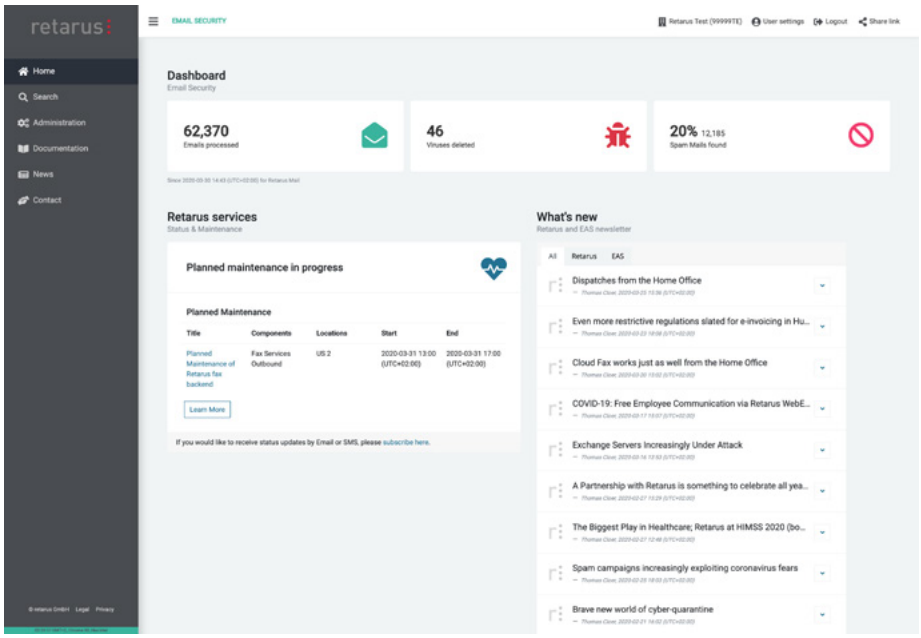
MICROSOFT 365 SINNVOLL ERGÄNZEN

Immer mehr Unternehmen entscheiden sich für einen Umstieg auf Microsoft 365. Dabei sollten sie sich nicht ausschließlich auf die integrierten Sicherheitsmechanismen der Cloud-Office-Lösung verlassen, sondern zusätzliche spezialisierte Business E-Mail-Security-Services einsetzen.

Wenn per Management-Entscheidung eine „Cloud-first"-Strategie ausgerufen wird, bedeutet dies in den meisten Fällen eine Entscheidung für Microsoft 365. Dabei wandert auch die Filterung von unerwünschten oder bösartigen eingehenden E-Mails und ausgehenden Lecks sensibler Daten immer öfter in die Cloud. Kleine Betriebe decken ihre Sicherheitsanforderungen für die geschäftliche E-Mail-Kommunikation mit dem Microsoft-Angebot oft ausreichend ab. Für komplexe oder hybride Infrastrukturen treten hingegen schnell Herausforderungen zutage. So hat beispielsweise im Frühling 2021 die weltweite Cyberattacke auf hunderttausende Organisationen, die Microsoft Exchange Server im Einsatz haben, gezeigt, dass Sicherheitsmechanismen bei On-Premises- oder One-Vendor-Ansätzen nicht ausreichen, um die E-Mail-Kommunikation im Krisenfall aufrechtzuerhalten.

ALLE ANGRIFFSFLÄCHEN VOLLUMFÄNGLICH SCHÜTZEN

Unternehmen sollten sich nicht ausschließlich auf eine Cloud-Office-Lösung und die dort integrierten Sicherheitsmechanismen verlassen, sondern vielmehr auf zusätzliche „Best-of-Breed"-Lösungen spezialisierter Drittanbieter setzen, um ihre Business-Kommunikation möglichst vollumfänglich abzusichern. Einige Unternehmen berücksichtigen diesen Aspekt bereits in ihrer IT-Strategie. So plant laut dem Analystenhaus Gartner bereits etwa die Hälfte der Microsoft-Office-365-Käufer, Anti-Virus- beziehungsweise Anti-Spam-Lösungen von spezialisierten Drittanbietern einzusetzen oder nutzen diese bereits. Jedes vierte Unternehmen setzt zusätzliche Content- oder E-Mail-Migration-Tools ein oder hat dies vor, und etwa jedes fünfte setzt auf ergänzende Content- oder E-Mail-Archiving-Produkte.



Der Einsatz innovativer E-Mail-Security-Services, die zusätzlich zu Microsoft 365 aus der Cloud bezogen werden, erhöht das Sicherheitsniveau deutlich. (Quelle: Retarus)

Für einen sicheren, globalen Informationsaustausch im Enterprise-Umfeld ist das E-Mail-Angebot von Microsoft 365 nicht ausreichend. Moderne E-Mail-Services berücksichtigen neben Sicherheitsaspekten auch Faktoren wie Continuity, Compliance und Applikations-Traffic und ergänzen Microsoft 365 sinnvoll.

SICHERHEIT AUF HOHEM NIVEAU

Durch den zusätzlichen Einsatz innovativer E-Mail-Security-Services, die wie Microsoft 365 aus der Cloud bezogen werden können, lässt sich das Sicherheitsniveau deutlich erhöhen und vereinheitlichen, ohne die interne Infrastruktur zu belasten. Dies senkt die Kosten und steigert die betriebliche Effizienz. Mithilfe eines zusätzlichen Security Layers wird die primäre E-Mail-Lösung nach außen hin „verschleiert". Auf Microsoft-Infrastrukturen spezialisierte Angreifer haben es somit schwerer. Im Gegensatz zu API-basierten Microsoft-Zusatzlösungen können Administratoren bei einem Gateway-Ansatz zudem rechtzeitig in den Kommunikationskanal E-Mail eingreifen und diesen vollständig steuern und absichern.

EINHEITLICHES SCHUTZNIVEAU

Auch in puncto Lizenzierung, die bei Microsoft nicht nur komplex, sondern auch kostspielig sein kann, leisten auf Business-E-Mail spezialisierte Lösungen wertvolle Unterstützung. Dies gilt insbesondere bei der Absicherung hybrider Infrastrukturen und weitverzweigter Firmenkonstellationen, bei denen unterschiedliche Microsoft-Lizenzen (E1/E3/E5) oder gar vereinzelte On-Premises-Mailserver zum Einsatz kommen.

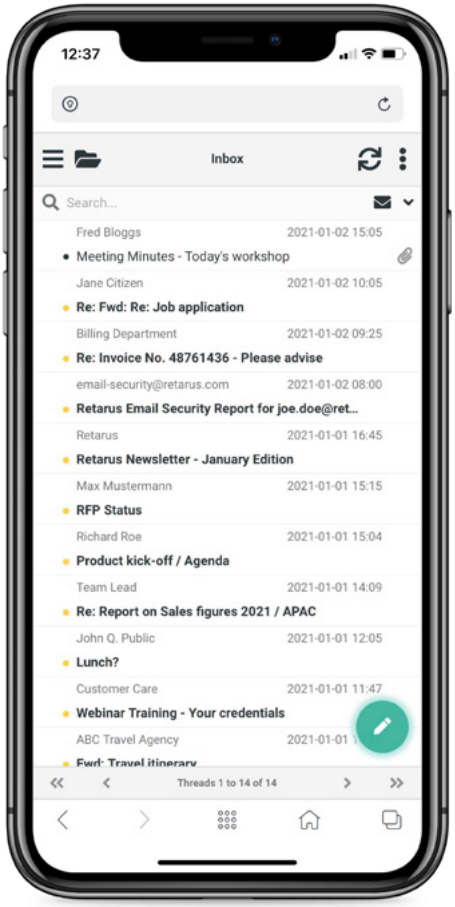
KEINE ABHÄNGIGKEITEN

Insbesondere bei sensibler Geschäftskommunikation per E-Mail sollten Unternehmen für bestmöglichen Schutz und Flexibilität auf eine Multi-Vendor-Strategie setzen. Moderne Cloud Services basieren deshalb idealerweise nicht nur auf vom Anbieter selbst entwickelten Technologien, sondern bieten zusätzlich einen offenen Best-of-Breed-Ansatz, der bewusst auf State-of-the-Art-Lösungen marktführender Anbieter setzt. Dadurch können Unternehmen sichergehen, stets auf die neuesten Quellen für Bedrohungsdaten in der Cybersicherheit zurückzugreifen und von besonders hohen Erkennungsraten zu profitieren.

VERSCHIEDENE SICHERHEITSLEVEL

Idealerweise bietet eine Lösung für E-Mail-Security verschiedene Sicherheitslevel, um die E-Mail-Infrastruktur gemäß individueller Anforderungen abzusichern:

- *Basis-Schutz durch multiple und intelligente Filter und Anti-Virus-Software,*
- *Advanced Threat Protection zur Abwehr von neuartigen, intelligenten Angriffen, etwa durch Sandboxing, automatische Pattern-Erkennung unterstützt durch Machine Learning sowie smartes Traffic-Handling,*
- *Post-Delivery Protection, um gefährliche E-Mails auch nach der Zustellung unschädlich zu machen,*
- *Information Protection mit modernen Verschlüsselungstechnologien, Archivierung und Frameworks zum Schutz sensibler Informationen wie persönlichen Daten, Unternehmensgeheimnissen oder Patenten*
- *sowie Compliance und die strikte Einhaltung gesetzlicher Regelungen mithilfe nachprüfbarer Kontrollmechanismen.*



E-Mail-Continuity-Services stellen vorab provisionierte Postfächer bereit, die alle Mitarbeiter per Webbrowser und mobil nutzen können, falls Exchange Online ausfällt. (Quelle: Retarus)

SO ERGÄNZEN E-MAIL-SERVICES AUS DER CLOUD MICROSOFT 365

- *Einheitlicher Schutz für alle Mailboxen*
- *Erhöhtes Schutzniveau durch zusätzlichen Security-Layer*
- *Höhere Erkennungsraten durch State-of-the-Art-Technologien und Best-of-Breed-Ansatz*
- *Provider-unabhängige E-Mail Continuity als Kommunikations-Back-up für den Krisenfall*
- *Flexible Verschlüsselung und revisionssichere Archivierung*
- *Optionaler Versand transaktionaler E-Mails mit hoher Reputation*

PROVIDER-UNABHÄNGIGE E-MAIL CONTINUITY FÜR DEN ERNSTFALL

Es erweist sich auch in Sachen E-Mail-Continuity als sinnvoll, im Sinne eines solchen Multi-Vendor-Ansatzes auf eine von Microsoft 365 und anderen gängigen E-Mail-Providern unabhängige Lösung zu setzen – gerade für den Fall großflächiger, anbieterweiter Ausfälle oder Sicherheitsvorkommnisse. E-Mail-Continuity-Services sind stets im Hintergrund aktiv und funktionieren auch dann noch, wenn etwa Exchange Online großflächig ausfällt oder gezielt angegriffen wird. In diesem Fall springt sofort das stets im Hintergrund aktive Notfallsystem ein und leitet die E-Mails des betroffenen Unternehmens über ein unabhängiges und leicht zu bedienendes E-Mail-System mit Zugriff über den Web Browser. Für einen möglichst nahtlosen Übergang stehen damit vorab provisionierte Postfächer bereit, die ohne technische Hürden von überall und für alle Mitarbeiter – auch mobil – zugänglich sind. So wird sichergestellt, dass die E-Mail-Kommunikation unterbrechungsfrei weiterläuft.

VERSCHLÜSSELUNG UND ARCHIVIERUNG

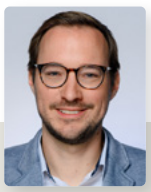
Auch für eine benutzerfreundliche, sichere Verschlüsselung geschäftskritischer Nachrichten kommt E-Mail-Services eine zentrale Funktion zu, die Microsoft 365 sinnvoll ergänzen. Im Idealfall unterstützt die Cloud-Lösung mehrere Verschlüsselungsalternativen und -standards. Als Managed Service sollte sie eine weite Verbreitung, ein Schlüssel-Management sowie einen leichten Zugang für alle Kommunikationspartner sicherstellen. Darüber hinaus sollte sie die Möglichkeit bieten, die Geschäftskommunikation mit einer modernen Lösung für E-Mail-Archivierung jederzeit gemäß aktuellen Compliance-Vorgaben revisionssicher und in lokalen Rechenzentren aufzubewahren.

TRANSAKTIONALE E-MAILS AUS APPLIKATIONEN

Ist der Umzug Richtung Microsoft 365 beschlossene Sache, stehen viele Unternehmen vor der Frage, wie mit dem E-Mail-Versand aus Applikationen umzugehen ist, wenn die eigenen Mailserver endgültig der Vergangenheit angehören. Microsoft selbst rät aufgrund eigener Volumenbeschränkungen in diesem Zusammenhang zur Nutzung von spezialisierten Drittanbietern. Eine gute Cloud-Komplettlösung für die E-Mail-Kommunikation bietet daher die Möglichkeit, E-Mails von Mensch zu Mensch (P2P) sowie den Massenversand aus Anwendungen (A2P, transaktional) voneinander zu trennen und auf diese Weise die geschäftskritische Kommunikation hoch verfügbar zu halten. Eine Cloud-Lösung für Transaktions-E-Mails sollte dabei so performant sein, dass sie auch bei Lastspitzen den sicheren und zuverlässigen Versand von mehreren Millionen E-Mails pro Stunde gewährleistet. Dabei ist darauf zu achten, dass der Anbieter entsprechende Zertifizierungen nachweisen sowie eine hohe Reputation und „Inbox Placement"-Raten sicherstellen kann und bestenfalls per Service-Level-Agreement zusichert.

FAZIT

Für einen sicheren, globalen Informationsaustausch reicht das E-Mail-Angebot von Microsoft 365 im Enterprise-Umfeld vielen Unternehmen schlicht nicht aus. Moderne E-Mail-Services berücksichtigen neben Sicherheitsaspekten auch Faktoren wie Continuity, Compliance und Applikations-Traffic, decken somit flexibel alle Anforderungen an die geschäftliche E-Mail-Kommunikation durch modulare und umfassende Zusatzdienste ab und ergänzen Microsoft 365 sinnvoll. ■



SÖREN SCHULTE,
Senior Product Marketing Manager
bei Retarus

Einsatz von Cloud-Services planen und Risiken erkennen

INTERNE PROZESSE CLOUD-GERECHT ANPASSEN

Viele Unternehmen setzen bereits Cloud-Services ein oder planen dies aus Gründen der Kostenreduktion, der einfachen Nutzung, Skalierbarkeit und Flexibilität im Geschäftsprozedere. Die Tendenz zur Cloud hat im Corona-Jahr einen Schub erhalten, wie der „Cloud Monitor 2021" der Bitcom Research und KPMG belegt. Der Einsatz von Cloud-Services sollte jedoch immer gut geplant sein: Denn auch die internen IT- beziehungsweise Geschäftsprozesse müssen zum Erreichen von Compliance und Sicherheit an die Cloud-Nutzung angepasst werden.

Der Weg in die Cloud sollte nicht überstürzt erfolgen. Besser ist es, sich informiert für das zum Unternehmen passende Cloud-Modell zu entscheiden, die Cloud-Nutzung vorab zu planen sowie auch die eigenen Ziele und Vorgaben zu ermitteln, die erreicht werden sollen. Eine Risikoanalyse ist der richtige Weg, um die grundsätzlichen Gefährdungen zu erkennen, die mit dem Cloud-Einsatz verbunden sind. Erst dann können die Kriterien formuliert werden, die der Beschaffung des Cloud-Services und der Auswahl des Anbieters (Provider) zugrunde liegen.

WELCHES MODELL UND WELCHER PROVIDER?

Cloud-Services werden in der Regel durch Provider gestellt. Das können Standardlösungen sein, aber auch hoch kundenspezifische Leistungen. Damit der Kunde die Leistungen abrufen kann, benötigt er eine Internetanbindung und speziell konfigurierte Endgeräte, die sogenannten Endpoints. Die wichtigsten Cloud-Modelle sind Private-, Public-, Hybrid- und Multi-Cloud.

Je nach Service-Modell verlagert der Nutzer Schutzobjekte (Daten, Anwendungen) in die Cloud, wofür er Nutzungskosten zu zahlen hat. Das preislich meist attraktivste Modell ist die

Public Cloud, denn hier teilen sich viele Kunden die Ressourcen des Anbieters. Die Leistung ist schnell aktivierbar und dynamisch skalierbar und erlaubt dadurch das Umverteilen von Investitions- zu Nutzungskosten. Der Nachteil liegt auf der Hand: Die Schutzobjekte liegen außerhalb des eigenen Sicherheitsperimeters und die Nutzer sind von den Sicherheits- und Administrationsmaßnamen des Providers abhängig. Sie haben wenig Kontrolle über die Vertragsvorgaben zu Compliance und Security, wie zum Beispiel über den physischen Aufenthaltsort der Daten. Aus Sicht des Datenschutzes – spätestens bei einer steuerrechtlichen Prüfung – kann das schnell zum Problem werden. Was passiert, wenn der Provider Konkurs anmeldet? Oder wenn man selbst zu einem anderen Provider wechseln möchte – gelingt die Datenmigration? Alles Fragen, die in der Risikoanalyse betrachtet werden müssen. Generell gilt: Sensible Daten gehören nicht in eine anonyme Public Cloud.

Private-Clouds bieten die Wahl zwischen einer Off- und On-Premises-Variante. Während im On-Premises-Modell die Cloud innerhalb der Infrastruktur des Nutzers (selbst oder durch einen beauftragten Dienstleister) betrieben wird, erfolgt dies im Off-Premises in einer fremden Infrastruktur, quasi als Outsourcing. Beiden gemein ist, dass die Leistungen exklusiv für den Kunden erfolgen und er die Vorgaben für Administration und Betrieb bestimmt. Deshalb ist das Einhalten der gesetzten Vorgaben praktisch und schnell überprüfbar und auch der Wechsel zu einem anderen Dienstleister ist unproblematisch. Im Vergleich zur Public-Cloud ist dieses Modell teurer und erfordert mehr Aufwand für das Management der Services.

Bei einem **Hybrid-Cloud-Modell** verwendet der Kunde zwei Grundtypen: Zum Beispiel hält er die sensiblen Daten in der privaten Cloud vor und andere in der öffentlichen (Public) Cloud. Die Private-Cloud kann nahtlos erweitert werden und Workloads können bei einer hohen Auslastung schnell in die Public-Cloud verschoben werden. Umgekehrt können Services aus der Public-Cloud auf Daten in der Private-Cloud zugreifen.

Ähnlich sieht das **Multi-Cloud-Modell** aus. Hier werden vom Kunden neben der eigenen Private-Cloud zusätzlich mehrere Public-Cloud-Services unterschiedlicher Provider genutzt.

Vorteile hier: Redundanz, Erhöhen der Ausfallsicherheit, Reduzierung von Abhängigkeiten.

Mit dem Einsatz von Cloud-Services geht ein veränderter Sicherheitsperimeter einher. Die Sicherheit der eigenen IT und die Compliance gemäß DS-GVO ist nicht mehr der alles bestimmende Faktor. Nun zählt auch die Vertrauenswürdigkeit des Providers hinsichtlich einer sicheren Infrastruktur, einer abgesicherten IT, qualifizierter Prozesse und geschultem Personal.

WOFÜR SOLL DIE CLOUD GENUTZT WERDEN?

Im nächsten Schritt gilt es, die Cloud-Nutzung zu planen. Was soll verlagert beziehungsweise gemietet werden? Oft gewünscht und nachgefragt werden Software, Betriebssysteme, Server, Speicher. Die Angebote hierfür nennen sich:

SaaS: Software as a Service	Provider stellt (Standard-) Applikationen zur Verfügung
PaaS: Plattform as a Service	Infrastruktur/Betriebssysteme/Schnittstellen/Werkzeuge zum Beispiel für die eigene Software/oder das Management mobiler Systeme
IaaS: Infrastructure as a Service:	Provider bietet IT-Ressourcen (Server/Speicher/Netzwerk)
Storage-as-a-Service	(nur) Speicherplatz wird zur Verfügung gestellt
NaaS Network as a Service:	Zurverfügungstellen virtueller Netzwerke / VPN. Alle Geräte werden vom Provider registriert. Management übernimmt andere Stelle.
DaaS Data as a Service:	Provider stellt besondere Daten(banken) zur Verfügung
IPMaaS Identity & Policy Management as a Service:	Provider verwaltet Identitäten und/oder Regelwerke zur Zugriffskontrolle für Kunden

UNTERNEHMENSSTANDARDS MIT DEM CLOUD-EINSATZ ABGLEICHEN

Sind im Unternehmen Standards definiert, beispielsweise zu Informationssicherheit, Compliance oder Business Continuity Management (BCM), ist zu prüfen, ob diese durch den beabsichtigten Cloud-Einsatz tangiert werden. Gegebenenfalls ist zu untersuchen, welche Maßnahmen erforderlich sind, um die Cloud-Services einzubeziehen und welcher Aufwand dadurch entstehen wird. Wie kann die Umsetzung erfolgen und die Einhaltung kontrolliert werden?

SICHERHEITSVORGABEN COMPLIANCE

Zur Klärung dieser Fragen und zur Bestimmung des weiteren Vorgehens ist es wichtig, die Be-

auftragten für Datenschutz, Informations-/IT-Sicherheit und Business Continuity einzubeziehen. Im Rahmen der Compliance sind alle relevanten Gesetze, Richtlinien, Konzern- und Kundenvorgaben einzuhalten. Das betrifft auch die Datenschutzziele (nach Art. 5 DS-GVO): Integrität und Vertraulichkeit der Daten, rechtmäßige und transparente Verarbeitung, Datenminimierung, Zweckbindung und Richtigkeit der Daten, Speicherbegrenzung, Rechenschaftspflicht des Verarbeiters etc.

SICHERHEITSVORGABEN INFORMATIONSSICHERHEIT

Teils sind diese Ziele auch im IT-Sicherheitsgesetz (IT-SIG) formuliert und gelten daher für die Informationssicherheit mit. Dementsprechend hat die Verarbeitung der Informationen nach Stand der Technik zu erfolgen und das Ergreifen angemessener organisatorischer sowie technischer Maßnahmen ist Pflicht. Unternehmen, die den kritischen Infrastrukturen (KRITIS) zugerechnet werden, sind verpflichtet, sicherheitserhebliche Vorkommnisse dem BSI (Bundesamt für Sicherheit in der Informationstechnik) zu melden und durch regelmäßige Audits nachzuweisen, dass sie die Forderungen des IT-SIG erfüllen. Bei der Vertragsgestaltung mit Cloud-Dienstleistern gibt es Sonderpunkte, die auch für solche Unternehmen gelten, die gemäß ISO 27000 zertifiziert sind.

SICHERHEITSZIELE IM BUSINESS CONTINUITY MANAGEMENT

Für Geschäftsprozesse mit IT-Unterstützung ist die Verfügbarkeit von Daten, Anwendungen und Prozessen inklusive maximal möglicher Ausfallzeiten oder auch Transaktionsleistungen festzuschreiben, was gewöhnlich in Form von Service Level Agreements geschieht. Weitere Sicherheitsziele des BCM sind daneben das Gewährleisten von Vertraulichkeit, Integrität und Authentizität sowie das Vorsehen von Kontrollmöglichkeiten.

SCHUTZOBJEKTE BESTIMMEN

Bevor man anhand der Risikoanalyse mögliche Gefährdungen ermittelt, sind die Werte der eigenen Objekte festzulegen und zu klassifizieren. Im Kern werden das Daten, IT-Anwendungen/Apps (eigene, fremdgeleistete) und IT-Systeme (Endgeräte, Homeoffice-Geräte, Server, Firewalls etc.) sein. Zu jedem Punkt ist zu überlegen: Was soll in der Cloud gespeichert werden? Vielleicht Mitarbeiter- und Patientendaten? Betriebsgeheimnisse? Verschlusssachen? Authentisierungsdaten? Logs/Protokolle? Die beiden erstgenannten sind personenbezogen und sensibel. Es macht Mühe, aber das IT-Geschehen ist zu durchforsten und im Detail zu betrachten. Die Schutzobjekte sollten inklusive Speicherort und Zuständigkeit im Rahmen des Assetmanagements inventarisiert werden.

VERANTWORTLICHKEITEN FESTLEGEN

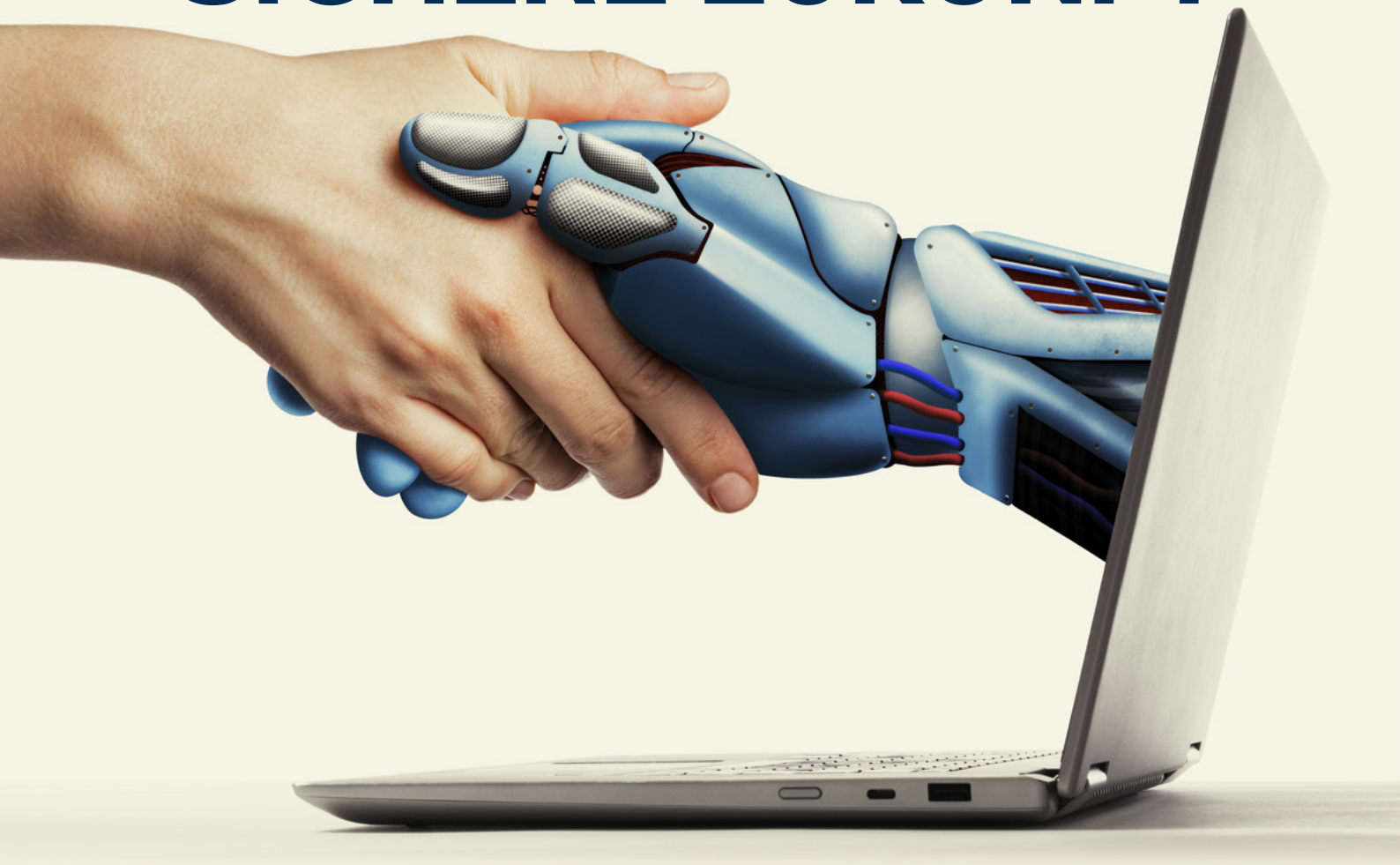
Ein weiterer Aspekt: „Data in Transit" (Daten während der Übertragung), „Data at Rest" (Daten im Ruhezustand) und „Data in Use" (in Gebrauch) – das heißt, auch der gegenwärtige Verarbeitungszustand und die Lokalität der Daten sind zu beachten. Daten im unternehmenseigenen Sicherheitsperimeter obliegen der eigenen Zuständigkeit; liegen die Daten in einer Cloud, lässt sich ihr Schutz meist nur über rechtliche Vorgaben umsetzen. Dazwischen liegt der Transportweg. Hier ist abzuwägen, wer für den Schutz sorgen soll, der Provider mit seinen Sicherheitsoptionen oder das eigene IT-Team.

Festzuhalten ist, dass sich die Vorgaben für die Sicherheit der eigenen Daten und Anwendungen durch das beabsichtigte Nutzen von Cloud-Services nicht ändern. Jedoch sind sie bezüglich der Cloud-Architektur neu zu interpretieren und zu bewerten, denn aus der Inanspruchnahme von Cloud-Services können sich teils gravierende Risiken für Datenschutz, IT-Sicherheit und Business Continuity ergeben. ■

CORNELIA LAST,
Diplom-Geografin, Datenschutzbeauftragte (GDDcert. EU), Sicherheitsberaterin der VZM GmbH mit dem Spezialgebiet Datenschutz

Warum im Cyberraum ein technisches Pendant zur menschlichen Empathie nötig ist

MIT VERTRAUENS-WÜRDIGKEIT IN EINE SICHERE ZUKUNFT



Digitale Werte benötigen hohes und vor allem spezifisches Schutzniveau. Da es für Anwender mittlerweile nicht mehr einfach ist, dieses effektiv nachzuprüfen, müssen sie darauf vertrauen, dass die Hersteller alles tun, um den Anforderungen gerecht zu werden. Andererseits sind die Hersteller darauf angewiesen, dass Anwender ihnen Vertrauen gewähren und ihre IT-/Sicherheitslösungen tatsächlich nutzen. Um eine hohe Vertrauenswürdigkeit zu erreichen, müssen Unternehmen Vorgehensweisen wählen, die einigen bestimmten Kriterien folgen.

In Zukunft werden zunehmend mehr und vor allem auch neue Werte geschaffen, die (nur) digital vorhanden sind, und in der Konsequenz sowohl einen weitaus höheren als auch individuelleren Schutzbedarf benötigen als bei Werten, die in beiden Welten greifbar sind. Dieses Schutzniveau zu erreichen ist aufwendiger als es je in der analogen Welt der Fall war – denn auf abgeschlossenen Unternehmensarealen ist es eher möglich, hier geschaffene Werte gut zu überwachen beziehungsweise sicher in Tresoren aufzubewahren. Dieser Schutz ist auch für die Unternehmensleitung gut darstell- und nachvollziehbar.

Im Gegensatz dazu unterliegt in der digitalen Welt der Schutz nicht mehr unmittelbar der Kontrolle der Anwenderunternehmen. Nicht nur, dass sie die Absicherung ihrer digitalen Werte keinesfalls mehr physisch nachprüfen können – sie müssen gleichzeitig auch darauf vertrauen, dass die IT-Hersteller bei Entwicklung, Auswahl und Umsetzung von Cybersicherheitsmaßnahmen wie etwa Verschlüsselung, Multi-Faktor-Authentifikation oder Isolierung von Anwendungen alles tun, um die richtige Vorgehensweise zu gewährleisten. Im Hinblick auf die Zukunftsfähigkeit von Anbieterunternehmen ist es wichtig zu sehen, dass dieser Aspekt – allein aufgrund der zunehmenden Vulnerabilität in der Digitalität durch immer versiertere Angriffe – mehrere Ebenen tangiert. Die Forderung nach einem gewissenhaften Umgang mit der Cybersicherheit bezieht sich zum einen auf die Verantwortung der Hersteller dahingehend alle Maßnahmen zu ergreifen, um ihr eigenes Unternehmen vor Angriffen zu schützen. Zum anderen jedoch gleichzeitig, ihre IT-/Sicherheitslösungen gemäß dem Stand der Technik zu entwickeln, um so die bestmögliche Technologie zur Verfügung stellen zu können.

Hieran zeigt zum einen die Relevanz von Vertrauen beim Einsatz von IT-/Sicherheitslösungen seitens der Anwender und unterstreicht gleichzeitig die Notwendigkeit, dass Unternehmen vertrauenswürdig agieren müssen, damit dieses Vertrauen auch gerechtfertigt ist.

CYBERSICHERHEIT ALS GRUNDLAGE FÜR VERTRAUENSWÜRDIGKEIT?

Das Vertrauen von Anwendern wird in einem hohen Maß über die Vertrauenswürdigkeit von IT-/Sicherheitslösungen und Hersteller-/Anbieterunternehmen aufgebaut. Dabei sind sowohl

EXKURS: WARUM IST DAS VERTRAUEN DER ANWENDER NOTWENDIG?

Durch die immer schnellere und komplexere Digitalisierung werden innovative IT-/Sicherheitslösungen aus Sicht des Anwenders zunehmend weniger berechenbar – sie sind nicht mehr in der Lage, die Technologie zu durchdringen. Dass dies mit Folgen verbunden ist, zeigt sich auch an den Ergebnissen des Online-Vertrauens-Kompass des „Bundesverband Digitaler Wirtschaft" in der 46 Prozent der Befragten angeben: „Die schnelle Veränderung unserer Lebensbedingungen durch zunehmende Technisierung und Vernetzung macht mir Angst" [1].

Aus diesem Grund ist es notwendig, die Digitalisierung so zu gestalten, dass diese von den Anwendern akzeptiert werden kann. Dies ist ein äußerst wichtiger Aspekt, da aus deren Sicht die Nutzung jeglicher IT-/Sicherheitslösungen theoretisch eine Risikohandlung darstellt, allein aufgrund der Tatsache, dass sie die Technologie nicht mehr komplett verstehen. Denn im Prinzip stellt jede Entscheidung, die ohne ein vollständiges Wissen über das Ergebnis des Handelns getroffen wird, ein Risiko dar. Dies trifft zwar auf nahezu alle Handlungen zu, wird aber im Regelfall nicht bewusst wahrgenommen. Doch obwohl sehr oft keine Sicherheit darüber besteht, dass Alltagshandlungen im Sinne des Handlungsziels gelingen, bezeichnet kaum einer diese durchgehend als riskant. Erst in dem Moment, wenn im Fall des Misslingens einer Aktion zugleich die Gefahr eines Verlusts besteht, also der Einzelne tatsächlich spürbar „etwas aufs Spiel setzt", wird das Risiko als solches auch empfunden.

Dieses Empfinden ist subjektiv und bei jedem Menschen unterschiedlich ausgeprägt. Von daher müssen Unternehmen sehr präzise vorgehen, um ein grundsätzliches Vertrauen in ihre Technologie aufbauen zu können. Grundsätzlich basiert die Hypothese eines künftigen Vertrauens zwischen zwei Personen – also interpersonal – darauf, dass eine unmittelbare Einschätzung des Gegenübers vorgenommen werden kann, zum Beispiel anhand der Mimik. Die Möglichkeit, einem Fremden vertrauen zu können, lässt sich allgemein auf die menschliche Fähigkeit zur Empathie zurückführen. Verkürzt gesagt: Die soziale Ader ist anatomisch im Gehirn verankert, von daher können Menschen zwischenmenschliche Informationen ganz mühelos aufnehmen und so die Motive anderer nachvollziehen.

In der Digitalisierung müssen Menschen dabei unterstützt werden, ihre Fähigkeit zu Vertrauen auf Institutionen mit ihren IT-/Sicherheitslösungen zu übertragen. Daraus lässt sich für Institutionen ableiten, dass sie sehr sorgfältig eruieren müssen, was zu tun ist, um dieses institutionelles Vertrauensverhältnis zu etablieren.

Umsetzung als auch die Darstellung von Cybersicherheit ein wichtiger Bestandteil der Vertrauenswürdigkeit (Bild 1).

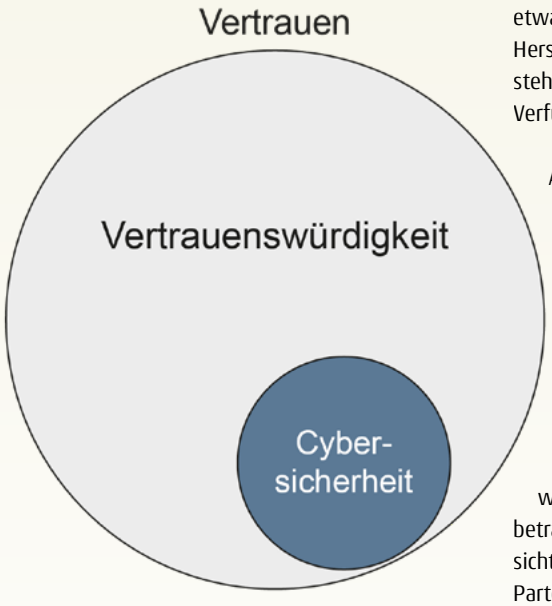


Bild 1: Zusammenhang zwischen Vertrauen, Vertrauenswürdigkeit und Cybersicherheit

Doch um hier ihre Vertrauenswürdigkeit glaubhaft zu demonstrieren und damit das Vertrauen sowie die Akzeptanz in ihr Unternehmen aber auch ihre Cybersicherheitslösungen oder IT-/Sicherheitslösungen mit Cybersicherheitsmechanismen zu manifestieren, sind zusätzlich weitere Aspekte zwingend notwendig. Es gilt eine reale Überprüfbarkeit zu bieten, dass ein Unternehmen und/oder eine IT-/Sicherheitslösung tatsächlich verlässlich sind. IT-/Sicherheitslösungen beispielsweise gelten als vertrauenswürdig, wenn sie sich immer in der erwarteten Weise für den beabsichtigten Zweck verhalten.

NOTWENDIGKEIT EINES VERTRAUENSWÜRDIGKEITSMODELLS

Mit der Digitalisierung zeigt sich, dass eine starke Abhängigkeit zwischen Herstellern, Dienstanbietern und Anwendern entstanden ist. In dieser Wechselbeziehung kann auch die Akzeptanz der IT-Technologie und einzelner IT-/Sicherheitslösungen sowohl positiv als auch negativ beeinflusst werden [2].

Dabei greifen folgende Mechanismen: Einerseits, dass die Anwender heute deutlich mehr Möglichkeiten zur Kontrolle der Handlungsweise und Leistung von Herstellern haben als früher, denn über die sozialen Medien können Anwender unmittelbar kundtun, wenn ihnen etwas missfällt oder bestimmte Aktivitäten der Hersteller beurteilen. Das heißt, den Anwendern stehen Mittel der direkten Einflussnahme zur Verfügung.

Andererseits haben die Anwender weniger Möglichkeiten, die IT-/Sicherheitslösungen zu durchdringen, was teilweise ihre Urteilsfähigkeit einschränkt und ihre Entscheidungsmacht verringert. Dadurch wird ihnen bei ihrem Einsatz eine höhere Vertrauensbereitschaft abverlangt. Dieser grundlegende, und für den Erfolg von IT-/Sicherheitslösungen und Unternehmen relevante Faktor muss aufgrund eines weiteren Parameters noch differenzierter betrachtet werden: Denn es gilt auch zu berücksichtigen, dass die Interessen der beteiligten Parteien teilweise diametral sind: etwa dann, wenn der Hersteller möglichst viele Kundendaten mit seiner IT-/Sicherheitslösung generieren sowie für jegliche Zwecke verwenden möchte – dies aber weder im Sinne des Anwenders ist noch seinen Wünschen entspricht. Ob und in welchem Maße sich dieser Zielkonflikt auf die Vertrauensfähigkeit beziehungsweise -bereitschaft auswirkt, lässt sich nicht pauschal beantworten, da diese Eigenschaft bei Menschen individuell unterschiedlich ausgeprägt ist. Zudem spielen dabei verschiedene weitere Faktoren eine Rolle – etwa, ob der Anwender mit der Nutzung des Dienstes aus seiner Sicht ein hohes Risiko eingeht – aber ebenso, welche Intention er dabei verfolgt und ob für ihn die eigentliche Zweckerfüllung an erster Stelle steht.

In jedem Fall ist davon auszugehen, dass der Anwender jeweils alle für ihn relevanten Informationen generiert, die ihm als Kriterien für seine Entscheidungsfindung – und damit letztendlich zum Aufbau von Vertrauen – dienen können.

Hier ein kleines Zwischenfazit: Die hohe Vertrauenswürdigkeit einer IT-/Sicherheitslösung sowie des Unternehmens ist notwendig, um die Akzeptanz für die IT-/Sicherheitslösung positiv zu beeinflussen. Generell kann davon ausgegangen werden, dass sich durch Vertrauenswürdigkeit die Kundenloyalität steigern lässt, was sich gleichzeitig auf die Akzeptanz aller Produkte/Dienstleistungen eines Unternehmens affirmativ auswirkt.

GRUNDLAGE: AUFBAU DES VERTRAUENSWÜRDIGKEITSMODELLS

Die Zusammenhänge zum Aufbau von Vertrauen sind in dem Vertrauenswürdigkeitsmodell (Bild 2) dargestellt und werden nachfolgend anhand der einzelnen Aspekte erläutert [3].

Vertrauen, Vertrauensgeber und Vertrauensnehmer:
Vertrauen bezeichnet unter anderem die subjektive Überzeugung der Richtigkeit von Handlungen. Grundsätzlich ist Vertrauen zur Reduzierung von Komplexität notwendig und immer dann erforderlich, wenn der Anwender mit einer ungewissen oder unsicheren Situation konfrontiert wird, oder der Ausgang seiner Handlung risikobehaftet sein kann. Das „Zulassenkönnen" des Vertrauensgebers (Anwender) einem Vertrauensnehmer (Unternehmen) zu vertrauen, bedeutet von daher die Bereitschaft, den jeweiligen Vertrauensnehmer nicht infrage stellen zu wollen sowie gleichzeitig, sich damit einem bestimmten Risiko auszusetzen. Insbesondere bei IT-/Sicherheitslösungen ist ein wichtiger Aspekt, dass Vertrauen beim Anwender in erster Linie aufgrund der Vertrauenswürdigkeit eines Unternehmens und/oder deren IT-/Sicherheitslösungen entstehen kann – also dadurch, dass Unternehmen als Vertrauensnehmer mit verschiedenen Maßnahmen eine Vertrauensgrundlage schaffen.

Institutionelles Vertrauen:
Eine Grundvoraussetzung dafür, dass Menschen IT-/Sicherheitslösungen nutzen ist das Versprechen eines Mehrwerts. Das bedeutet im Umkehrschluss, wenn für die Anwender kein Wertzuwachs durch deren Einsatz entsteht, sind sie kritischer in ihrer Beurteilung und dadurch weniger bereit, sich auf das jeweilige Produkt per se zu verlassen. Darüber hinaus müssen Unternehmen weitere Maßnahmen ergreifen, um Anwender in die Lage zu versetzen, ihre genuine Vertrauensfähigkeit auf IT-/Sicherheitslösungen zu extendieren. Das kann ermöglicht werden, indem es gelingt, interpersonales Vertrauen – also das Vertrauensverhältnis, das aufgrund bestimmter individueller Kriterien zwischen Menschen entsteht – auf IT-/Sicherheitslösungen zu übertra-

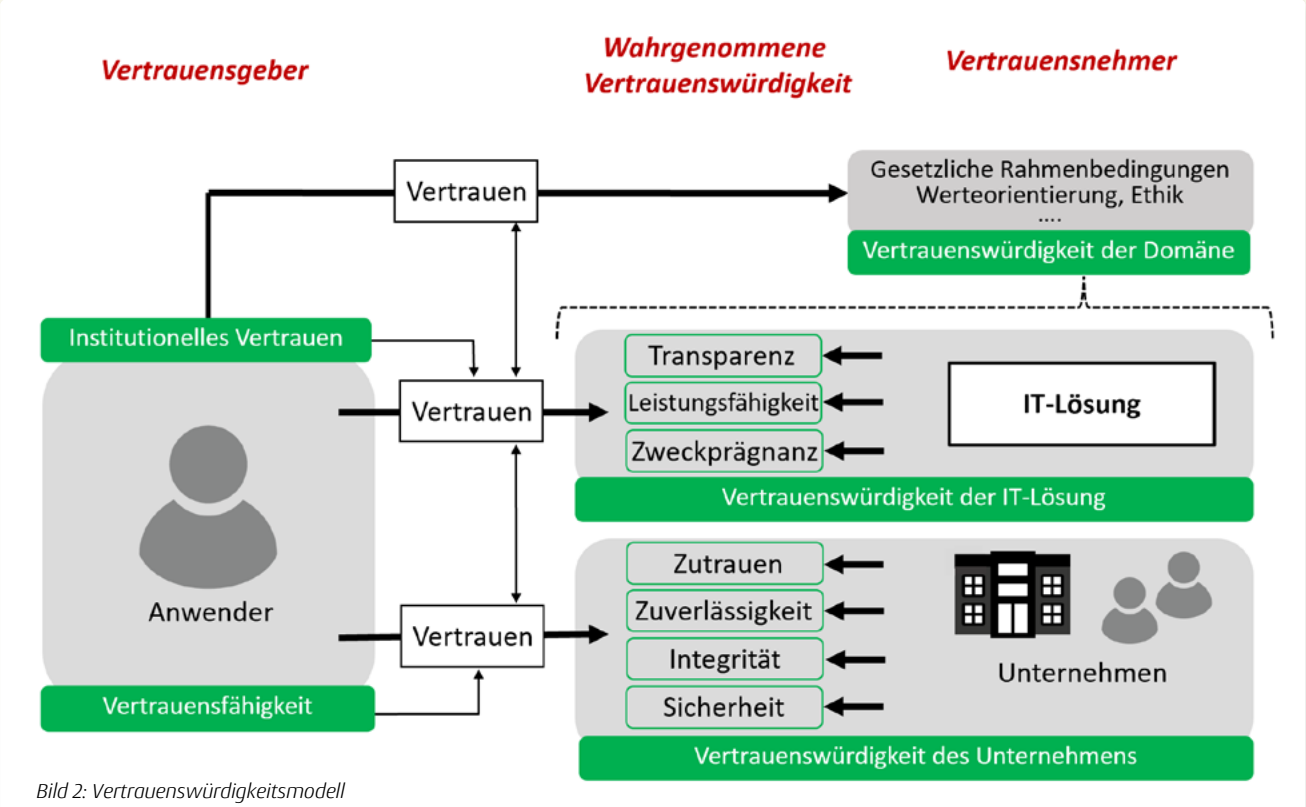


Bild 2: Vertrauenswürdigkeitsmodell

gen. Dabei ist es wichtig zu beachten, dass im Verhältnis zwischen zwei Personen Vertrauen aufgrund der Fähigkeit zur Empathie aufgebaut wird und die individuell relevanten Kriterien direkt nachprüfbar sind. Diese Option ist in Bezug auf IT-/Sicherheitslösungen nicht gegeben, allein unter dem Aspekt, dass sich deren Verhalten beziehungsweise Funktionsweise nicht unbedingt nachprüfen lässt. Das institutionelle Vertrauen ist das Ergebnis der Transferleistung – also inwieweit Anwender fähig und auch dazu bereit sind, ihr Vertrauen auf Institutionen, wie etwa Unternehmen, zu übertragen. Dieses Vertrauen kann in erster Linie durch das Unternehmen selber, über die IT-/Sicherheitslösung (positiv) als auch über die Vertrauenswürdigkeit der Domäne beeinflusst werden.

Wahrgenommene Vertrauenswürdigkeit:
Vertrauenswürdigkeit basiert auf der Annahme, dass es möglich ist, sich auf etwas Bestimmtes verlassen zu können. Im Regelfall beruht die wahrgenommene Vertrauenswürdigkeit auf offensichtlichen Funktionalitäten der IT-/Sicherheitslösung und Maßnahmen des Unternehmens, die dem Anwender als Vertrauensgeber entweder aufgrund des ersten Eindrucks oder aus eigener Erfahrung oder über Dritte bekannt sind. Daran wird deutlich, dass es für Unternehmen zunehmend wichtig wird, eine Vertrauensgrundlage zu schaffen, indem sie relevante Aspekte der Vertrauenswürdigkeit sowohl für die IT-/Sicherheitslösung als auch das Unternehmen explizit darstellen, damit die Anwender Vertrauen aufbauen können.

Vertrauensfähigkeit:
Grundsätzlich ermöglicht Vertrauensfähigkeit, Personen oder auch Unternehmen, zu vertrauen beziehungsweise ihnen etwas zuzutrauen. Basierend auf der individuellen Prägung eines Menschen oder dessen Vorerfahrung ist die Fähigkeit jeweils unterschiedlich dominant ausgebildet. In diesem Sinne hat die wahrgenommene Vertrauenswürdigkeit einen Einfluss auf die Vertrauensfähigkeit des Anwenders und kann sich positiv auf diese auswirken.

Unternehmen:
Als Unternehmen gelten Hersteller oder Anbieter von IT-/Sicherheitstechnologien, -produkten oder -diensten. Die genannten Kategorien werden als IT-/Sicherheitslösungen zusammengefasst.

Anwender:
Unter Anwender werden alle subsummiert, die IT-/Sicherheitstechnologien, -produkten oder -diensten nutzen, also auch Anwenderunternehmen.

IT-/Sicherheits-Lösung:
Im Kontext der Cybersicherheit ist eine IT-/Sicherheitslösung eine allgemeine Anwendung mit entsprechenden Cybersicherheitsmechanismen oder ein Cybersicherheitssystem.

ALLGEMEINE VORBEDINGUNG: VERTRAUENSWÜRDIGKEIT DER DOMÄNEN

Für Unternehmen ist grundsätzlich von Vorteil unabhängig zu agieren, um auf Basis einer hohen Anwender-Orientierung Wettbewerbsvorteile generieren zu können. Doch oftmals ist es nicht einfach oder sogar unmöglich, eine Vorreiterrolle einzunehmen und dadurch den Markt zu gestalten. Denn vielfach kann über die Vertrauenswürdigkeit eines einzelnen Unternehmens nicht ein generelles Vertrauen etwa in einen innovativen Ansatz grundsätzlicher IT-/Sicherheitslösungen geschaffen werden.

Von daher ist es für Unternehmen notwendig an der Vertrauenswürdigkeit von Domänen mitzuwirken. Mit anderen Worten: Teilweise kann es von Vorteil sein, kollaborativ mit anderen Herstellern Werte zu kreieren oder Wertevorstellungen umzusetzen, um die gesamte Branche respektive Domäne zu entwickeln und so im Weiteren die erfolgreiche Einführung von neuen Geschäftsmodellen oder Technologien zu gewährleisten. Im Prinzip gibt es mehrere Optionen, um eine Vertrauenswürdigkeit für (neue) Technologien und IT-/Sicherheitslösungen zu schaffen. Nachfolgend einige Beispiele in Bezug auf Domänen:

Schaffung von Rahmenbedienungen
Der Staat schafft die Randbedingungen, indem domänenspezifisch vorgegeben wird, wie Unternehmen den Einsatz der Technologie und IT-/Sicherheitslösungen zu gestalten haben. Ein Beispiel dafür ist das IT-Sicherheitsgesetz, in dem die Rahmenbedingungen für die Sicherheit von kritischen Infrastrukturen definiert sind.

Motivierung von Ökosystemen
Ein Beispiel in diesem Bereich stellt Self-Sovereign Identities (SSI) dar. Mit SSI soll die Basis eines europäisches Ökosystems zur Ausgabe und Verifizierung digitaler Identitäten sowie Nachweise aufgebaut werden. Darüber lassen sich relevante Ziele verwirklichen: unter anderem der Schutz der Privatsphäre. Denn auf diese Weise könnten Anwender zukünftig selbstbestimmt entscheiden, welcher Anwendung sie wann ihre digitalen Identitätsdaten und weitere Nachweise zur Verfügung stellen. Letztendlich führt der souveräne Umgang mit den eigenen Daten auch dazu, dass die Abhängigkeit von einzelnen monopolierten Anbietern minimiert wird, womit das Ziel einer unabhängigen schnelleren Digitalisierung gefördert wird. Ein zusätzlicher Vorteil: Überholte Geschäftsmodelle ließen sich so durchgängig ablösen, zum Beispiel „Unfreiwillig Bezahlen mit den eigenen Daten".

Ein weiteres Beispiel stellt das Industriekonsortium GAIA-X dar. Denn nicht nur für neue IT-Technologien kann es relevant sein, eine Vertrauenswürdigkeit zu etablieren – auch bei bereits eingeführten ist es teilweise notwendig, Werteorientiert Standards neu zu definieren und damit zu erhöhen. Aufgrund der Intention von GAIA-X soll den Anwendern garantiert werden, dass die eingesetzten IT-/Sicherheitslösungen europäisches Recht einhalten und Datenportabilität, höchste Kriterien der IT-Sicherheit sowie eine klare Transparenz rund um die Datenverwendung gewährleisten. Darüber ist es dann möglich, eine verstärkte Speicherung von Daten in Europa zu forcieren.

Allerdings ist es nicht immer im Sinne des Staates oder von Konsortien die Vertrauenswürdigkeit als wichtigstes Kriterium anzuerkennen. So werden teilweise Maßnahmen ergriffen, die hier eher kontraproduktiv sind und zu einer Schwächung der Domäne führen.

Schutzmechanismen des Staates
Ein Negativbeispiel ist die Anwendung des Bundestrojaners. Dessen Einsatz schwächt die Cybersicherheit von Bürgern und Unternehmen, weil das Wissen über bestimmte Sicherheitslücken nicht an die Hersteller weitergegeben, sondern für den Bundestrojaner genutzt wird [4].

IM SPEZIELLEN: VERTRAUENSWÜRDIGKEIT DER IT-/SICHERHEITSLÖSUNG

Die Vertrauenswürdigkeit der Domäne unterstützt die Vertrauenswürdigkeit von einzelnen IT-/Sicherheitslösungen. Wenn allgemein anerkannt ist, dass der Einsatz von Multi-Factor Authentification dazu geeignet ist, einen höchst zuverlässigen Nachweis über die Echtheit des Anwenders zu erbringen, wird sich dies im ersten Schritt positiv auf alle im Markt befindlichen Lösungen auswirken. Damit ein Hersteller dieses Vertrauen dediziert auf seine Lösung übertragen kann, spielen – im Sinne der wahrgenommenen Vertrauenswürdigkeit – neben der Cybersicherheit noch weitere Aspekte eine relevante Rolle: Transparenz, Leistungsfähigkeit und Zweckprägnanz. Erst durch die Darstellung aller Aspekte wird der Anwender in die Lage versetzt, Vertrauen zur angebotenen IT-/Sicherheitslösung aufzubauen.

ASPEKT: TRANSPARENZ EINER IT-/SICHERHEITSLÖSUNG

Der Entschluss zur Transparenz zeigt sich in erster Linie darin, dass ein Unternehmen die Bedürfnisse der Anwender ernst nimmt und bereit ist, offen zu kommunizieren. Dies bedeutet jedoch keinesfalls, jedes Details der IT-/Sicherheitslösung oder aller damit einhergehenden geschäftlichen Aktivitäten preisgeben zu müssen. Vielmehr geht es daraum, alle relevanten Informationen zur Verfügung zu stellen, die für den Anwender erforderlich sind, um im gegebenen Kontext eine valide Entscheidung über die Vertrauenswürdigkeit der IT-/Sicherheitslösung treffen zu können. Insgesamt fällt der Informationsqualität somit eine entscheidende Rolle zu – sie sollte partizipativ und besonders ausgewogen sein, also die Interessen aller Parteien gleichermaßen berücksichtigen.

In der Vergangenheit war diese Form der Kommunikation nicht erforderlich. Aufgrund des mittlerweile hohen Komplexitätsgrads ist es jedoch unumgänglich, so zu agieren, um die Bereitschaft zur Nutzung zu erhöhen. Hier zeigt sich die Wechselwirkung zwischen Vertrauen und Vertrauenswürdigkeit: Ein Unternehmen ist auf die Akzeptanz der Anwender angewiesen. Andererseits ist es für den Anwender – aufgrund der zunehmend intelligenten Angriffe und komplexeren Cybersicherheitsmechanismen – immer wichtiger, dass seine Cybersicherheitsbedürfnisse auch angemessen durch die IT-/Sicherheitslösung befriedigt werden.

Beipackzettel Cybersicherheit: Eine Möglichkeit der Transparenz ist zum Beispiel die Bereitstellung eines Beipackzettels, in dem beschrieben wird, wie mithilfe von Cybersicherheitsmechanismen in der IT-/Sicherheitslösung dafür gesorgt wird, die Wahrscheinlichkeit der verschiedenen Angriffe zu reduzieren. Wichtig ist zudem, aufzuzeigen, welche Restrisiken bestehen, wie der Anwender damit umgehen und wie das Unternehmen dabei unterstützen kann.

ASPEKT: LEISTUNGSFÄHIGKEIT EINER IT-/SICHERHEITSLÖSUNG

Die Leistungsfähigkeit einer IT-/Sicherheitslösung ist das, was der Anwender unmittelbar erfassen und auch kontrollieren kann. Von daher ergeben sich daraus die messbaren Kriterien für dessen Beurteilung, inwieweit er sich bei der Erreichung des beabsichtigten Einsatzzweckes unterstützt fühlt und wie gut die IT-/Sicherheitslösung tatsächlich dafür geeignet ist. Als Bewertungsmaßstab sind hier unter anderem Zuverlässigkeit und Berechenbarkeit zu nennen. Von hoher Relevanz ist dabei auch, dass sich im Wirkungsgrad der IT-/Sicherheitslösung die Kom-

petenz des Unternehmens dokumentiert. Denn letztendlich entsteht mangelnde Leistungsfähigkeit durch Fehler im Kompetenz- oder Strategiebereich. Daran zeigt sich somit sowohl die Verbindung als auch Wechselwirkung zwischen der Vertrauenswürdigkeit der IT-/Sicherheitslösung und dem Unternehmen. Als Bewertungsmaßstab kann einem Anwender unter anderem die Bedienbarkeit oder die Leistungsfähigkeit der Cybersicherheitsmechanismen dienen.

Bedienbarkeit
Sind Cybersicherheitsmechanismen und -management für den Anwender einfach oder sogar intuitiv zu bedienen?

Leistungsfähigkeit der Cybersicherheitsmechanismen
Wie stark verringert sich die Leistungsfähigkeit der IT-/Sicherheitslösung, zum Beispiel durch Verschlüsselung der Daten? Oder wie lange benötigt ein Angriffserkennungssystem von dem Erkennen eines Angriffs bis zur Reaktion, zum Beispiel dem Versenden eines Alarms oder einer automatischen Reaktion darauf?

ASPEKT: ZWECKPRÄGNANZ EINER IT-/SICHERHEITSLÖSUNG

Die Zweckprägnanz manifestiert sich im Verwendungszweck der IT-/Sicherheitslösung. Für Unternehmen bedeutet dies, dass bei der Entwicklung Funktion und Intention der IT-/Sicherheitslösung zielgenau definiert sind. Daraus resultierend sollte in der Konsequenz der Einsatzzweck der IT-/Sicherheitslösung für den Anwender klar offensichtlich sein. Aus diesem Grund gilt es darauf zu achten, dass der Zweck der IT-/Sicherheitslösung – auch durch den Einsatz charakteristischer Eigenschaften – leicht und unmittelbar erfasst werden kann. Im Umkehrschluss bedeutet dies jedoch keinesfalls, dass mit der Zweckprägnanz eine geringe Funktionalität einhergehen muss. Des Weiteren ist es notwendig, jede relevante Änderung oder Erweiterung der IT-/Sicherheitslösung offen darzulegen – vor allem dann, wenn dadurch der originäre Verwendungszweck nicht mehr eindeutig erkennbar ist.

Bietet eine IT-/Sicherheitslösung neben der eigentlichen Anwendung weitere Funktionen an, die nur im Sinn des Unternehmens oder dritter Parteien sind, müssen auch diese klar dargestellt und beschrieben werden. Beispiele dafür sind:

Offenlegung des Geschäftsmodells
Dass mithilfe des Geschäftsmodells „Bezahlen mit persönlichen Daten" sensitive Daten der Anwender gesammelt und für individualisierte Werbung genutzt oder/und lukrativ an Dritte verkauft werden, muss eindeutig kommuniziert werden.

Einblick geben in neue Features
Das neue Erkennungssystem von Apple, mit dem anlasslos alle Daten auf dem iPhone nach Kinderpornografie durchsucht werden sollen, hat zwar einen hohen gesellschaftlichen Wert, stellt aber für den Anwender ein Risiko im Sinne seiner Privatsphäre dar – allein aus dem Grund, da der Abgleich auf dem Endgerät stattfindet. Da es darüber zudem auch prinzipiell möglich ist, beliebig nach anderen Inhalten zu suchen, kann damit sogar für bestimmte Gruppen (in einigen Ländern) eine echte Gefährdung einhergehen. Gravierende Abweichungen von der Zweckprägnanz müssen für den Anwender unmittelbar transparent gemacht werden.

IM SPEZIELLEN: VERTRAUENSWÜRDIGKEIT DER UNTERNEHMEN

Bei der Entscheidung zur Nutzung neuer IT-Technologien sind nicht ausschließlich die Aspekte der jeweiligen IT-/Sicherheitslösung ausschlaggebend. Im Gegenteil – die Reputation des Unternehmens spielt hierbei ebenfalls eine wichtige Rolle. Da sich aktuell zeigt, dass ein Vertrauen in IT-Technologien, -Anwendungen und -Dienste prinzipiell (noch) nicht uneingeschränkt gerechtfertigt ist, sind die Unternehmen gefordert, weitere Bedingungen zu erfüllen, um den Grad ihrer Vertrauenswürdigkeit zu steigern. Hierzu müssen sowohl Hersteller als auch Diensteanbieter ihre Strategie nach außen sichtbar machen.

In der Umsetzung bedeutet dies, ihr Handeln an den definierten Kriterien Zutrauen, Zuverlässigkeit, Integrität und Sicherheit auszurichten. Maßgeblich für die Definition ist dabei, dass die unternehmensspezifische Vertrauenswürdigkeit rational bewertbar gestaltet wird, um dem Anwender die Möglichkeit zu geben, die entsprechenden Parameter schnell und einfach beurteilen zu können.

ASPEKT: ZUTRAUEN IN EIN UNTERNEHMEN

Zutrauen ist ein relevantes Kriterium für die Vertrauenswürdigkeit. Generell kann dieses im Hinblick auf die Funktionalität dadurch erzeugt werden, dass Unternehmen sowohl über die Fähigkeit, als auch über die entsprechenden Mittel verfügen, um verlässliche sowie sichere Technologie, respektive Dienste und Anwendungen bereitzustellen.

Wichtig hierbei ist, eine Strategie zu entwerfen, um dieses Kriterium sowohl zu erfüllen als auch in einer Zutrauens-Leitlinie dokumentieren zu können. Hierzu muss unter anderem ein Konzept erstellt werden bezüglich der Parameter, die zwingend erfüllt sein müssen. In diesem Kontext sind beispielhaft folgende Faktoren von hoher Relevanz:

Mitarbeiter
Parameter zur Ausbildung, Qualifizierung und Fortbildungsmaßnahmen der Mitarbeiter: Haben die Mitarbeiter einen Studiengang mit Ausrichtung IT-Sicherheit absolviert oder eine entsprechende fachliche Weiterbildung? Welche Erfahrungen haben sie in diesem Bereich, über welche Zusatzqualifikation wie T.I.S.P. oder CISSP verfügen sie [5].

Qualitätsstandards
Parameter zur Entwicklung und Produktion: Beschreibung des Entwicklungsprozesses, Definition der begleitenden Qualitätssicherung inklusive Durchführung, Spezifizierung des Lebenszyklus-Management.

Betriebsmittel
Parameter zu Qualität und Quantität von Software und Hardware: Beschreibung der Standards, die erfüllt sind, damit die – für das geschäftliche Handeln und insbesondere die Entwicklung – eingesetzten IT-Systeme allen Anforderungen gerecht werden, Benennung von Qualitätskriterien.

ASPEKT: ZUVERLÄSSIGKEIT DES UNTERNEHMENS

Mit Zuverlässigkeit ist gemeint, dass IT-Technologien sowie IT-/Sicherheitslösungen nur die Prozesse ausführen, die seitens der Anwender gewünscht sind, beziehungsweise die er er-

wartet – und dies möglichst hundertprozentig verlässlich. Zuverlässigkeit impliziert somit, dass Unternehmen grundsätzlich wohlwollend sind. Das bedeutet, dass sie im besten Sinne ihrer Anwender handeln, sich also an deren Bedürfnissen orientieren, statt ihre eigenen Interessen besonders in den Mittelpunkt zu stellen. Ein Beispiel hierfür ist, dass sie offensichtliche Schwachpunkte ihrer Anwender nicht instrumentalisieren, um dadurch einen (finanziellen) Vorteil zu erzielen und es somit unterlassen, ihnen Schaden zuzufügen. Dies wäre im Rückschluss möglich, indem die Schwäche eines Kunden für Sonderangebote ausgenutzt wird: Dem Anwender würden regelmäßig veraltete Lagerbestände von Anti-Malware-Produkten zum stark vergünstigten Preis angeboten, die nicht mehr dem Stand der Technik genügen und daher keinen angemessenen Schutz gegen aktuelle Angriffe bieten.

Doch kein Unternehmen ist perfekt, somit bedingt Zuverlässigkeit auch die Bereitschaft zur Weiterentwicklung. Um momentan noch bestehende Defizite zu kompensieren, müssen Hersteller daher Mechanismen integrieren, mittels derer sie proaktiv den Grad ihrer Zuverlässigkeit beständig optimieren können und im Weiteren dann diese Entwicklungsschritte adäquat darstellen. Ein Idealzustand ist dann erreicht, wenn das Anwendervertrauen kongruent der faktischen Zuverlässigkeit des Unternehmens respektive der IT-/Sicherheitslösung entspricht. Dies bedeutet im Umkehrschluss, dass Unternehmen ihre Vertrauenswürdigkeit riskieren oder verlieren, wenn ihre Handlungsweise nicht mit ihrer Außendarstellung übereinstimmt. Wie müssen Unternehmen hier zukünftig agieren und was sollte in deren Zuverlässigkeitsmanagement einfließen? Nachfolgend einige Faktoren, die dabei von Relevanz sind:

Kooperativ handeln, um die wahren Bedürfnisse der Anwender besser identifizieren zu können und bei Problemstellungen den Anwender individuell unterstützen. Die Übernahme einer Gesamtverantwortung im Schadensfall oder Rückrufaktionen bei identifizierten Problemen sind Beispiele für ein kooperatives Handeln. Das bedeutet, Hersteller müssen – wenn möglich auf direktem Weg – ihre Anwender bei Erkennen von gravierenden Schwachstellen umgehend informieren. Wird diese Information zuerst von anderen Quellen zum Beispiel über soziale Medien oder die Fachpresse veröffentlicht, mindert dies die Vertrauenswürdigkeit der Hersteller.

Verantwortlich handeln, um durch den richtigen Einsatz von Funktionen – die zum Vorteil der Anwender sind – für diese einen Mehrwert zu schaffen. Aber auch die Überprüfung und kontinuierliche Kontrolle der Lieferketten unter den verschiedensten Aspekten sowie das Ergreifen aller Maßnahmen, um Betrugsprävention durchzuführen gehören zum verantwortlichen Handeln. Das bedeutet zum Beispiel, Hersteller müssen alles tun, um Supply-Chain-Angriffe zu verhindern, etwa durch Überprüfung der Lieferanten und/oder auch der Kontrolle der Inhalte sowie der Software des jeweiligen Lieferanten. Speziell hier aber ebenso in vergleichbaren Konstellationen kann Vertrauenswürdigkeit nur durch Übernahme einer Gesamtverantwortung aufgebaut werden.

ASPEKT: INTEGRITÄT DES UNTERNEHMENS

Integrität zeigt sich darin, dass seitens der Hersteller und Diensteanbieter alle Faktoren berücksichtigt werden, die jeweils die relevanten Aspekte der Vertrauenswürdigkeit beinhalten. Dazu zählen insbesondere die ethischen Dimensionen des Handelns. Das bedeutet, dass ein Hersteller als Vertrauensnehmer prinzipiell in der Lage ist, alle Versprechen, die er abgegeben hat, einhalten zu können und auch tatsächlich einhält, sowie generell dazu bereit ist, sowohl Normen als auch Werte der Gesellschaft zu berücksichtigen.

Insbesondere die ethische Ausrichtung von Unternehmen wird zukünftig noch stärker auf dem Prüfstand stehen. Dies lässt sich anhand verschiedener Studien belegen: zum Beispiel dadurch, dass 93 Prozent der Anwender in Deutschland einen ethisch vertretbaren Einsatz von IT-Technologie fordern. Von daher sollte Wahrhaftigkeit in allen geschäftlichen Aktivitäten konsequenterweise zu einem Muss deklariert werden. Eine eindimensionale rein technisch-orientierte Denkweise, ohne Berücksichtigung ethischer Aspekte und Werte wird zunehmend weniger – oder sogar nur kurzfristig – rentabel sein, da das Verhalten der Anwender volatil ist und sie sich schnell durch negative Ereignisse oder Posts beeinflussen lassen. Aber auch dem Aspekt, dass das Potenzial zur Vertrauensfähigkeit bei den Anwendern unterschiedlich stark ausgeprägt und somit die Grundhaltung relativ schwer kalkulierbar ist, fällt in diesem Zusammenhang eine wichtige Bedeutung zu.

Von daher gilt es für Unternehmen als einer der wichtigsten Schritte hier eine Integritäts-Maxime zu entwerfen – mit klaren Bekenntnissen zu ihrem Geschäftsmodell und im Weiteren den unternehmensspezifischen Aspekten. Dazu gehört definitiv, die ethischen Anforderungen klar zu adressieren. Einige ethische Anforderungen werden nachfolgend exemplarisch vorgestellt:

Schutz der Privatsphäre
Diese Forderung beinhaltet zum einen den guten Umgang mit Kundendaten, etwa sofortige Löschung, wenn diese nicht mehr benötigt werden und auch, diese Daten durch Verschlüsselung zu schützen sowie zum anderen das Versprechen, die Daten der Anwender nicht für weitere wirtschaftliche Zwecke zu verwerten.

Rechenschaftspflicht
Mit der Rechenschaftspflicht wird unter anderem auf die Nachprüfbarkeit der Qualität von IT-/Sicherheitslösungen abgehoben. Zudem sollte für Unternehmen die Überprüfung eingesetzter Technologien, inklusive entsprechender Offenlegung von eventuell negativen Auswirkungen auf die Gesellschaft, obligatorisch sein.

Keine eingeschränkte Cybersicherheit
Die Hersteller und Anbieter müssen sich dazu verpflichten, dass die genutzten Cybersicherheitsmechanismen keine geschwächten Verschlüsselungen, Zufallszahlengeneratoren oder weitere Kryptografie-Verfahren verwenden und sichere Schlüssel nutzen. Ebenso ist sicherzustellen, dass keine Backdoors in den Cybersicherheitslösungen eingebaut sind. In der Darstellung zum Anwender hin können Hersteller dies zum Beispiel mithilfe des Vertrauenszeichens „IT Security made in Germany“ deklarieren [6].

ASPEKT: SICHERHEIT DES UNTERNEHMENS

Das Anerkennen der Bedeutung von Cybersicherheit sowie deren Umsetzung gewährleistet, dass Technologien, respektive Dienste und Anwendungen, im Internet risikoarm zu nutzen sind. Dieser Anspruch ist jedoch (noch) eine Fiktion, da unter

anderem Ransomware, DDoS- oder Phishing-Angriffe heute an der Tagesordnung sind. Alltäglich genutzte Dienste, wie etwa E-Mail-Programme, Onlinebanking oder Online-Shops, bieten bei weitem nicht den Level an Vertrauenswürdigkeit der notwendig ist, um damit kritische Geschäftsprozesse sicher abwickeln zu können.

Von daher benötigen Unternehmen eine adäquate und ausformulierte IT-Sicherheitsrichtlinie, um im Sinne der Kunden den bestmöglichen Schutz gewährleisten zu können. Die kontinuierliche Umsetzung gemäß aktueller Sicherheitsanforderungen ist notwendig, da Anwender im Allgemeinen nicht dazu in der Lage sind, sich angemessen zu schützen. Unter anderem haben die folgenden Faktoren im Kontext der Sicherheit eine hoher Relevanz:

Darstellung der verwendeten Cybersicherheitsmaßnahmen
Hier sollten die Hersteller aufzeigen, was sie tun, um sowohl die jeweilige IT-/Sicherheitslösung als auch ihr eigenes Unternehmen vor Cybersicherheitsrisiken zu schützen. Anders als beim „Beipackzettel Cybersicherheit" können Beschreibungen und Hintergrundinformationen hier detaillierter ausfallen.

Zertifizierung der IT-/Sicherheitslösung
Die Zertifizierung von Qualität und Vertrauenswürdigkeit der IT-/Sicherheitslösungen muss durch qualifizierte unabhängige Organisationen erfolgen, die nach definierten Kriterien überprüfen und testieren. Kriterien ergeben sich zum Beispiel aus den Bereichen IT-Sicherheit, Datenschutz sowie den Entwicklungs- und Qualitätssicherungsprozessen. Die Zertifizierung der IT-/Sicherheitslösung aber auch des Unternehmens ist eine wichtige Maßnahme zur Vertrauensbildung.

Regelmäßige Überprüfung der Produkte und des Unternehmens
Das Ziel hierbei ist, Schwachstellen aktiv und kontinuierlich mithilfe von Penetrationstests und Red-Teams zu identifizieren, damit Sicherheitslücken so schnell wie möglich durch Updates eliminiert – und somit nicht für Angriffe verwendet – werden können. Dies gilt sowohl für die angebotenen IT-/Sicherheitslösungen als auch für die Unternehmen und deren Zulieferer. Dadurch lässt sich ein – für den Anwender jederzeit nachweisbares – hohes Sicherheitsniveau im laufenden Entwicklungsprozess erreichen.

Bug-Bounty-Programm
Die zentrale Idee von Bug-Bounty-Programmen ist, die Hacker-Community, Wissenschaftler oder weitere Akteure mit finanziellen Anreizen zu animieren, Schwachstellen in den IT-/Sicherheitslösungen der jeweiligen Unternehmen aufzufinden. Dadurch wird es möglich, Schwachstellen möglichst zeitnah zu beheben, möglichst bevor kriminelle Organisationen sie nutzen können.

Cybersicherheitsstrategie
Eine Cybersicherheitsstrategie ist ein längerfristig ausgerichtetes, planvolles Vorgehen mit dem Ziel, die vorhandenen Risiken eines Angriffes auf digitale Werte des Unternehmens so gering wie möglich zu halten. Da deren Darstellung die Vertrauenswürdigkeit eines Unternehmens erhöht, sollte die prinzipielle Strategie auch nach außen kommuniziert werden.

FAZIT

Anhand bestimmter Kriterien lässt sich die Vertrauenswürdigkeit von Unternehmen und deren Technologie näher definieren und auch, was Vertrauen faktisch bedeutet. Es ist insbesondere im Hinblick auf IT-/Sicherheitslösungen von hoher Relevanz, Vertrauen bei den Anwendern aufzubauen, da sich so die Akzeptanz für die Nutzung steigern lässt.

Natürlich klingt das in der Theorie nicht nur logisch, sondern auch als problemlos durchzusetzbar. Tatsächlich ist es jedoch notwendig, dass Unternehmen sich eingehend damit auseinanderzusetzen, wie sie ihre Vertrauenswürdigkeit durch Umsetzung der relevanten Kriterien erhöhen und ebenso wie sie diese explizit nachweisen können. ■

Quellen/Literaturverzeichnis

[1] *Online-Vertrauens-Kompass 2020, https://www.bvdw.org/themen/publikationen/detail/artikel/online-vertrauens-kompass/*

[2] *U. Coester, N. Pohlmann: „Artikelserie über Facetten der Künstlichen Intelligenz", Warum Vertrauenswürdigkeit und KI unbedingt zusammengehören (Teil 1), https://www.onpulson.de/63805/warum-vertrauenswuerdigkeit-und-ki-unbedingt-zusammengehoeren/ IT-Systeme: Warum Vertrauen für Unternehmen so wichtig ist (Teil 2), https://www.onpulson.de/64428/it-systeme-warum-vertrauen-fuer-unternehmen-so-wichtig-ist/*

[3] *Nils Backhaus: „Nutzervertrauen und -erleben im Kontext technischer Systeme: Empirische Untersuchungen am Beispiel von Webseiten und Cloudspeicherdiensten", Dissertation, Technischen Universität Berlin, 2016*

[4] *Tagesspiegel-Background: „Über Zielkonflikte in der Cybersicherheitspolitik wieder mehr diskutieren", https://background.tagesspiegel.de/digitalisierung/cybersicherheitspolitik-lauter-zielkonflikte*

[5] *N. Pohlmann: „Ex schola pro vita – Studien- und Fortbildungsangebote zur Cybersicherheit", KES – Die Zeitschrift für Informations-Sicherheit, DATAKONTEXT-Fachverlag, 3/2021*

[6] *TeleTrusT: „IT Security made in Germany", https://www.teletrust.de/it-security-made-in-germany/*

ULLA COESTER,
als Gründerin/CEO des Unternehmens xethix Empowerment, berät sie in Prozessen zur Corporate Digital Responsibility, Fokus Vertrauenswürdigkeit/Digitale Ethik. Zudem ist sie Lehrbeauftragte für digitale Ethik (Hochschule Fresenius, Köln) und Mitglied der Standardization Evaluation Group 10/IEC: Ethics in Autonomous and Artificial Intelligence Application.

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

Die neuen Standardvertragsklauseln nach dem „Schrems II“-Urteil

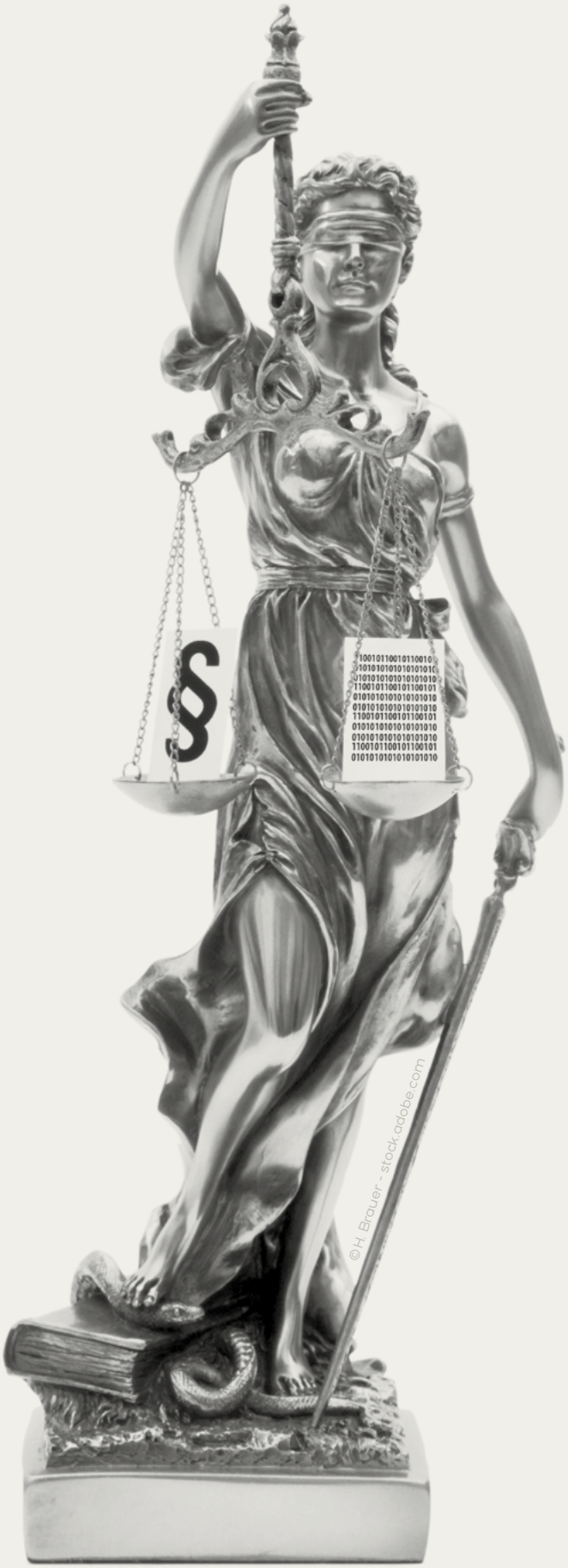
COMPLIANCE-GERECHTE DATEN-ÜBERMITTLUNGEN IN DRITTLÄNDER

Seit Ende September sind für Datenübermittlungen in Drittländer die neuen Standardvertragsklauseln (SCC) abzuschließen, welche die Europäische Kommission im Beschluss 2021/914/EU angenommen hat. Diese stellen nunmehr eine neue Rechtsgrundlage für den Datentransfer in Länder dar, in denen nicht dasselbe Datenschutzniveau herrscht, wie in der Europäischen Union (EU). In diesen Standardvertragsklauseln hat die Kommission die umfassenden Voraussetzungen adressiert, die der Europäische Gerichtshof (EuGH) in seinem „Schrems II“-Urteil im Juli 2020 formuliert hat. In diesem vieldiskutierten Urteil hatte der EuGH das EU-US Privacy Shield für unwirksam erklärt und die Anforderungen für alle Datenübermittlungen nach Artikel 46 Datenschutz-Grundverordnung (DS-GVO) konkretisiert.

Um Daten in ein Land außerhalb der EU (Drittland) übermitteln zu können, muss eine rechtliche Grundlage im Sinne der Art. 44 ff. DS-GVO vorliegen. Beispielsweise kann die Europäische Kommission nach Artikel 45 DS-GVO einen Angemessenheitsbeschluss als Grundlage für eine Datenübermittlung fassen. Mit einem solchen Beschluss stellt sie fest, dass die Rechtslage im Drittland ein Datenschutzniveau aufweist, das mit dem der EU vergleichbar ist. Liegt ein Angemessenheitsbeschluss vor, können personenbezogene Daten von EU-Mitgliedstaaten und den Mitgliedstaaten des Europäischen Wirtschaftsraums ohne weitere Anforderungen an dieses Drittland übermittelt werden. Dazu zählen derzeit:

- Andorra,
- Argentinien,
- Kanada,
- die Färöer-Inseln,
- Guernsey,
- Israel,
- die Isle of Man,
- Japan,
- Jersey,
- Neuseeland,
- die Schweiz,
- Uruguay und
- Großbritannien.

Zudem läuft derzeit ein Verfahren zur Anerkennung von Südkorea als sicheres Drittland. Allerdings ist fraglich, wie lange Großbritanniens Status als sicheres Drittland gelten wird: Die britische Regierung verkündete Ende August 2021 wesentliche Änderungen im Datenschutz und damit eine eigenständige Datenschutzpolitik. Sobald der konkrete Entwurf vorliegt, wird dieser von der



EU-Kommission geprüft werden. Ist eine Vereinbarkeit nicht gegeben, ist wohl die Aussetzung oder die Beendigung des Angemessenheitsbeschlusses zu erwarten.

Liegt kein Angemessenheitsbeschluss vor, besteht die Möglichkeit des Abschlusses von Standardvertragsklauseln beziehungsweise Standard Contractual Clauses (SCC) oder verbindlichen Datenschutzvorschriften beziehungsweise Binding Corporate Rules (BCR), Art. 46 Abs. 2 lit. c, b DS-GVO. Zuletzt ist auch die Rechtgrundlage der Einwilligung und der Vertragserfüllung, Art. 49 DS-GVO, möglich – stellt aber eher die Ausnahme dar.

DIE NEUEN STANDARDVERTRAGS-KLAUSELN

Im Juni hat die Europäische Kommission die finale Fassung der neuen Standardvertragsklauseln im Beschluss 2021/914/EU veröffentlicht. Diese schaffen seit dem 27. Juni 2021 eine neue Rechtsgrundlage, welche bei EU-weiten, sowie internationalen Datentransfers angewendet werden können. Dabei hat die Europäische Kommission Vorgaben aus dem Schrems-II-Urteil sowie die Anforderungen der DS-GVO berücksichtigt. Die Klauseln berücksichtigten auch die gemeinsame Stellungnahme des Europäischen Datenschutzausschusses und des Europäischen Datenschutzbeauftragten, die Rückmeldungen der Interessenträger im Rahmen einer breit angelegten öffentlichen Konsultation sowie die Stellungnahme der Vertreter der Mitgliedstaaten. Die wichtigsten Neuerungen sind:

- Ein neuer modularer Aufbau ermöglicht eine flexible Vertragsgestaltung in verschiedenen Konstellationen;
- Begrifflichkeiten von Datenexporteur und Datenimporteur sind jetzt offener gestaltet;
- Prüfung des Datenschutzniveaus für den Datenexporteur ist eine explizite Verpflichtung;
- Ausweitung der Anwendungsfälle: vier unterschiedliche Module, von denen eines ausgewählt werden muss;
- optionale Kopplungsmöglichkeit (Klausel 7): Beitritt zu den Standardvertragsklauseln durch weitere Parteien;
- Haftung für Verletzung von Betroffenenrechten (Klausel 12 lit. b);
- Umsetzung des EuGH-Urteils Schrems II insbesondere in Klauseln 14 und 15.

Nunmehr sehen die Klauseln einen modularen Ansatz vor. Dadurch wird die bisherige lineare Konstellation zwischen Verantwortlichen und Verantwortlichen beim

Empfänger beziehungsweise Verantwortlichen und Auftragsverarbeitern aufgebrochen. Für verschiedene Anwendungsfälle gibt es verschiedene Module, aus denen bei dem Abschluss einer Standardvertragsklausel ausgewählt werden kann. Damit wird eine flexible Vertragsgestaltung ermöglicht:

- Modul 1: Datenübermittlung zwischen zwei Verantwortlichen;
- Modul 2: Datenübermittlung Verantwortlicher an Auftragsverarbeiter;
- Modul 3: Datenübermittlung von einem Auftragsverarbeiter an einen (Unter-) Auftragsverarbeiter;
- Modul 4: Datenübermittlung (Rückübermittlung) Auftragsverarbeiter innerhalb der EU an einen Verantwortlichen im Drittland.

Die Standardvertragsklauseln ermöglichen die Abbildung unterschiedlicher Verarbeitungsketten und unter bestimmten Umständen den nachträglichen Beitritt weiterer Verantwortlicher/Auftragsverarbeiter. Durch die Kopplungsklausel (Klausel 7) können Standardvertragsklauseln nun auch zwischen mehr als zwei Parteien geschlossen werden. Auch die Begrifflichkeiten von Datenexporteuren und Datenimporteuren sind jetzt offener gestaltet.

Damit eine Übermittlung von Daten in ein Drittland zulässig ist, müssen die Daten vor dem weitreichenden Zugriff der Behörden geschützt sein: Im Hinblick auf einen Zugriff von Behörden auf Daten bei Datenimporteuren obliegen diesem umfassende Benachrichtigungs- (Klausel 15.1) und Handlungspflichten (Klausel 15.2) – insbesondere zur Abwehr der behördlichen Maßnahmen.

Je nach Rolle werden Datenimporteure von den Standardvertragsklauseln vertraglich den wesentlichen Grundsätzen und Verpflichtungen der DS-GVO unterworfen. Dazu zählen vor allem die Bindung an die Datenminimierung und Speicherbegrenzung, die Gewährleistung der Sicherheit der Datenverarbeitung und die Einhaltung von Informations-, Meldepflichten sowie Betroffenenrechten.

Nun ist die Prüfung des Datenschutzniveaus im Drittland als explizite Pflicht in den Standardvertragsklauseln enthalten: Bei einer Übermittlung von personenbezogenen Daten mittels Standardvertragsklauseln müssen Datenexporteure zukünftig bewerten, ob für die vom Transfer betroffenen Daten ein angemessenes Datenschutzniveau im Empfängerland gewährleistet ist. Dabei muss nicht das allgemeine Datenschutzniveau im Empfängerland bewertet werden, sondern das konkrete Schutzniveau für die zu übertragenen Daten. Damit hat die Europäische Kommission auf die Risiken für den Schutz personenbezogener Daten reagiert, die aus Vorschriften und Behördenpraktiken im Empfängerland resultieren können.

Seit dem 27.09.2021 sind für neue Datenübermittlungen ausschließlich die neuen Standardvertragsklauseln abzuschließen; der Abschluss der alten Standardvertragsklauseln ist nicht mehr zulässig. Alte Standardvertragsklauseln, die Verantwortliche vor dem 27.09.2021 abgeschlossen haben, können bis zum 27.12.2022 verwendet werden, sofern die vereinbarten Verarbeitungsvorgänge unverändert bleiben und die Anwendung der alten Klauseln gewährleistet, dass die Datenübermittlung geeigneten Garantien unterliegt.

FAZIT

Die neuen Standardvertragsklauseln bringen mehr Klarheit und Flexibilität in die Gestaltung von Datentransfers; gleichzeitig sind diese aber auch deutlich umfangreicher geworden. Auch die Umstellung auf die neuen Standardvertragsklauseln bringt Unternehmen viel neuen Handlungsbedarf. Denn die Nutzung aller Dienstleister mit Drittlandbezug muss überprüft und die Umsetzung der neuen Klauseln begleitet werden. Trotzdem wird sich der Aufwand langfristig lohnen, um die sichere Übermittlung von Daten zu gewährleisten. ■

Foto: SRD Rechtsanwälte

SIMONE ROSENTHAL
ist Partnerin bei der Technologiekanzlei Schürmann Rosenthal Dreyer und spezialisiert auf das digitale Business. Die Rechtsanwältin hat sich erfolgreich als Expertin für Datenschutz-, IT-Recht und Wettbewerbsrecht etabliert. Sie ist ebenfalls Geschäftsführerin der ISiCO Datenschutz GmbH – einem Unternehmen, welches Analyse, Auditierung, Beratung und Zertifizierung in den Bereichen Datenschutz, Datenschutz-Compliance und Informationssicherheit anbietet – sowie Mitgründerin von lawpilots, einem E-Learninganbieter für Datenschutz, IT-Sicherheit und Compliance und seit 2020 Mitgründerin von caralegal, einer KI-basierten Datenschutzmanagement-Software.

www.srd-rechtsanwaelte.de

Das Webportal von IT-SICHERHEIT

IM WEB GEHT'S WEITER!

Sie haben die IT-SICHERHEIT schon durchgelesen? Unter www.itsicherheit-online.com finden Sie parallel zu den Printausgaben der IT-SICHERHEIT tagesaktuelle Informationen rund um das Thema IT-Sicherheit. Neben Fachartikeln, Studienergebnissen, Whitepapers und Meldungen zu Unternehmen und Produkten können Abonnenten hier ab sofort auch in unserem neuen Zeitschriften-Archiv stöbern.

Schauen Sie am besten gleich jetzt und regelmäßig bei uns rein!

Weitere **FACHINFORMATIONEN** zum **THEMA IT-SICHERHEIT**

Mit Network Detection and Response verdächtigen Netzwerkaktivitäten auf der Spur

DEN ANGRIFF KOMMEN SEHEN

Wer Ransomware erst bemerkt, wenn sie auf dem Endpunkt installiert wird, kommt unter Umständen schon zu spät. Erpresserische Attacken bahnen sich nämlich viel früher an, wobei Cyberkriminelle verräterische Spuren im Netzwerk hinterlassen. Mit Network Detection and Response (NDR) können Unternehmen bereits die Vorbereitungsphase dieser Angriffe entlarven. War traditionelle NDR-Technologie bisher nur sehr großen Unternehmen vorbehalten, ermöglichen neue NDR-Tools mittels Machine Learning und künstlicher Intelligenz nun auch mittelständischen Unternehmen mit begrenzten Ressourcen, verdächtige Netzwerkaktivitäten nahezu in Echtzeit zu erkennen und zu unterbinden.

www.itsicherheit-online.com/ForeNova-2021-06

Paul Smit, Director Professional Services bei ForeNova (Foto: ForeNova)

Wenn Hacker ihre Phishingnetze auswerfen

BEST PRACTICES ZUM SCHUTZ VOR KÖDERANGRIFFEN

Eine Infiltration des eigenen Netzwerks lässt sich für die Aufklärung über die Gegenseite nutzen. Dafür existieren mittlerweile Technologien, die mittels Köder in Webapplikationen oder Endpoints hinterlegt, ausschließlich von Akteuren mit böswilligen Absichten gefunden werden können. Soweit die gute Nachricht. Doch umgekehrt nutzen auch Cyberkriminelle verstärkt Köder, mit denen sie Informationen sammeln, die sie zur Planung künftiger gezielter Phishing-Angriffe verwenden können.

www.itsicherheit-online.com/Barracuda-2021-06

Dr. Klaus Gheri, General Manager Network Security bei Barracuda Networks (Foto: Barracuda)

Angriffe verhindern und Auswirkungen reduzieren

ERFOLGREICHE STRATEGIEN GEGEN RANSOMWARE

Die jüngsten Opfer (Media Markt und Saturn, der Medizin-Dienstleister Medatixx sowie der US-Broker Robinhood) zeigen die Bandbreite der Ziele von Ransomware-Angreifern: Letztlich ist jede Branche und jedes Unternehmen gefährdet. Aber auch wenn Ransomware wie ein unvermeidliches Übel wirkt, können Unternehmen zahlreiche Maßnahmen ergreifen, um einen Angriff und Datenverlust in ihrem Unternehmen zu verhindern.

www.itsicherheit-online.com/Varonis-2021-06

Michael Scheffler, Country Manager DACH bei Varonis Systems (Foto: Varonis)

VORSCHAU Ausgabe 1|22 FEBRUAR/ MÄRZ

SPECIAL: IT-SICHERHEIT IM KRANKENHAUS

Eine ebenso unschöne wie hinterhältige Begleiterscheinung der aktuellen Pandemie sind Angriffe auf Kliniken und Krankenhäuser. Ohne Hemmungen und Rücksicht auf Leib und Leben von Menschen versuchen Angreifer massiv Einrichtungen des Gesundheitswesens lahmzulegen – meist mithilfe von Ransomware, um von den betroffenen Institutionen Geld zu erpressen. In der nächsten Ausgabe der IT-SICHERHEIT werfen wir einen Blick auf die aktuelle Situation in diesem Bereich und zeigen, wie Krankenhäuser eine erfolgreiche Verteidigung aufbauen können. Ein weiteres wichtiges Thema ist das Gesetz zum Schutz elektronischer Patientendaten in der Telematikinfrastruktur (Patientendaten-Schutz-Gesetz – PDSG).

(Beitragsangebote für das Special bitte an Wolfgang.Scharf@datakontext.com)

INDUSTRIELLE IT-SICHERHEIT

Industrielle IT-Sicherheit oder OT-Sicherheit (Operational Technology) ist nach wie vor eine große Herausforderung für Unternehmen. Der Beitrag beleuchtet die besonderen Risiken in den industriellen Netzwerken von Energieversorgungsunternehmen. Wie lassen sich die modernen und stark dezentralisierten Infrastrukturen erfolgreich absichern? Dabei kommen Themen wie IEC 61850, Advanced Metering Infrastructure und alleinstehende Erneuerbare-Energie-Anlagen zur Sprache.

Weitere geplante Themen:

- **Identity Access Management (IAM):** Schlüsselanforderungen und Produktvergleich
- **Mobile Device Management:** Apple-Geräte professionell steuern
- **Recht:** Was beim Einsatz von Microsoft 365 aktuell zu beachten ist

... und vieles mehr.

IN UNSEREM VERLAG ERSCHEINEN AUSSERDEM NOCH FOLGENDE ZEITSCHRIFTEN

IMPRESSUM

IT-SICHERHEIT
Magazin für Informationssicherheit und Datenschutz

Verlag:
DATAKONTEXT GmbH
Standort Frechen
Augustinusstr. 9d · 50226 Frechen
www.datakontext.com

Chefredaktion:
Stefan Mutschler (S.M.)
E-Mail: stefan-mutschler@t-online.de
Redaktion:
Dr. Peter Münch (P.M.),
Dr. jur. Martin Zilkens (M.Z.),
Online-Redaktion:
Jessica Herz
Leitung Online
herz@datakontext.com
+49 2234 98949-80
Lisa Bieder
Chiara Schönbrunn
Silvia Klüglich
Herausgeberbeirat:
Prof. Dr. Michael Backes, Prof. Dr. jur. Dirk-M. Barton, Walter Ernestus, Prof. Dr. Nikolaus Forgó, Prof. Dr. Rainer W. Gerling, Dr. Jan-Peter Ohrtmann, Prof. Dr. Norbert Pohlmann, Dr. jur. Martin Zilkens
Gründer: † Bernd Hentschel

Grafik/Layout/Satz:
Michael Paffenholz
Tel.: +49 173 8382572
E-Mail: michael.paffenholz@gmx.de
Objekt- und Anzeigenleitung:
Wolfgang Scharf
Tel.: +49 2234 98949-60
E-Mail: wolfgang.scharf@datakontext.com
zzt. gilt die Anzeigenpreisliste Nr. 27
Vertrieb/Herstellung:
Dieter Schulz
Tel.: +49 2234 98949-99
dieter.schulz@datakontext.com

Abonnement:
Jahresabonnement € 104,- inkl. VK (Inland)

Erscheinungsweise: sechs Ausgaben
Alle Preise verstehen sich inkl. MwSt. Der Abonnementpreis wird im Voraus in Rechnung gestellt. Das Abonnement verlängert sich zu den jeweils gültigen Bedingungen um ein Jahr, wenn es nicht mit einer Frist von 8 Wochen zum Ende des Bezugszeitraumes gekündigt wird.
Erscheinungsweise, Bezugspreise und -bedingungen:
Abonnement und Bezugspreis beinhalten die Print-Ausgabe sowie eine Lizenz für das Online-Archiv. Die Bestandteile des Abonnements sind nicht einzeln kündbar. Der Preisanteil des Online-Archivs ist auf der Abonnementrechnung separat ausgewiesen.
Aboservice:
Hüthig Jehle Rehm GmbH, München,
Tel.: +49 89 21 83-7110
Druck: Grafisches Centrum Cuno GmbH & Co. KG, Calbe (Saale)

Beilagen: DATAKONTEXT GmbH, Frechen

Titelbild: ©svetazi - stock.adobe.com

Fotos: Firmenbilder; DATAKONTEXT; ©(Alex, Andrew Derr, Artranq, Elena, flashmovie, H. Brauer, Inna, Julien Eichinger, leremy, m.mphoto, MH, Rawf8, Sergey Nivens, sutlafk, xiaoliangge) - stock.adobe.com

27. Jahrgang 2021 · ISSN: 1868-5757

Der neue Themenguide IT-Sicherheit

www.itsicherheit-online.com/themen

Wir bedanken uns bei unseren Partnern:

arvato BERTELSMANN · BÜCKER IT-Security GmbH · corewill SOFT · ConSecur [security and consulting] · controlware · CROWDSTRIKE

CuriX Makro Asset Management Group · DATA AGENDA Datenschutz Manager · DARKTRACE · GRADIENTO · g+h systems · IT-SEAL Social Engineering Analysis Labs

LastPass by LogMeIn · noSpam proxy · seculution application whitelisting · SEPPMAIL · SPECOPS

TELONIC nonstop networking · totemo securing data in motion · TÜV NORD Akademie · VZM · WatchGuard · zscaler

Jetzt mitmachen und Firmenpartner werden:

wolfgang.scharf@datakontext.com

DATAKONTEXT

Cyber-Security-Zertifizierungen von TÜV SÜD.

Eine sichere IT-Infrastruktur ist in fast jedem Unternehmen die Basis für gute Geschäfte. Mit ihr steht und fällt das Vertrauen von Kunden und die Motivation der Mitarbeiter. Mit unseren systematischen Cyber-Security-Zertifizierungen legen Sie ein belastbares Fundament – für eine sichere IT und langfristiges Vertrauen Ihrer Stakeholder.

- ISO/IEC 27001 Zertifizierung
- ISO/IEC 20000-1 – Zertifiziertes Service-Management (in der IT)
- Zertifizierung nach IT-Sicherheitskatalog
- KRITIS – Nachweis über angemessene IT-Sicherheit nach §8a BSIG
- TISAX® – Der Nachweis für IT-Sicherheit in der Automobilbranche

www.tuvsud.com/cyber-security-zertifizierungen

TÜV SÜD
Management Service

Mehr Wert.
Mehr Vertrauen.

TÜV SÜD Management Service GmbH Ridlerstr. 57, 80339 München, Deutschland
Tel. +49 89 5791-2500 ms-anfragen@tuvsud.com www.tuvsud.com/tms

TÜV®