HZ203909 · ISSN 1868-5757 · www.datakontext.com August **4/2020**

IT-SICHERHEIT

Mittelstandsmagazin für Informationssicherheit und Datenschutz

Fernkooperation mit Risiko?

Zoom Video Conferencing im Sicherheitscheck

Europa-Cloud:
Was bringt GAIA-X?

Unternehmens-Apps mit Open Source:
Gefahren beherrschbar?

IT-Recht:
Wie Justitia den Einsatz Künstlicher Intelligenz sieht

DATAKONTEXT

Neue Möglichkeiten auf dem Weg zu deinen Zielen.

Der neue SEAT Leon Sportstourer

Mit Business Leasing ab 179 € mtl.[1]

Egal, was deine Ziele sind – mit dem neuen SEAT Leon Sportstourer erreichst du sie. Er hat mit 620 Litern eines der größten Gepäckraumvolumen seiner Klasse. So hast du Platz für alles, was dir wichtig ist.
Mehr erfahren unter seat.de/business

SEAT **FOR BUSINESS**

SEAT

SEAT **CARE** **Ab 10,00 € mtl.[2]** sorgenfrei unterwegs mit Wartung & Verschleiß. Zuverlässige Mobilität zu gleichbleibend günstigen Raten.

Kraftstoffverbrauch SEAT Leon Sportstourer 1.5 TSI (Benzin), 96 kW (130 PS): innerorts 6,3, außerorts 4,0, kombiniert 4,8 l/100 km; CO_2-Emissionen: kombiniert 111 g/km. CO_2-Effizienzklasse: A. [1] 179,00 € (zzgl. MwSt.) mtl. Leasingrate für Siegertypen für den SEAT Leon Sportstourer Style, 96 kW (130 PS), auf Grundlage der UVP von 21.134,45 € bei 24 Monaten Laufzeit und jährlicher Laufleistung von bis zu 10.000 km. 0 € Sonderzahlung. Ein Angebot der SEAT Leasing, Zweigniederlassung der Volkswagen Leasing GmbH, Gifhorner Straße 57, 38112 Braunschweig. Dieses Angebot ist nur für gewerbliche Kunden ohne Großkundenvertrag und nur bis zum 31.12.2020 gültig. Bei allen teilnehmenden SEAT Partnern in Verbindung mit einem neuen Leasingvertrag bei der SEAT Leasing. Die individuelle Höhe der Leasingrate kann abhängig von der Netto-UPE, Laufzeit und Laufleistung sowie vom Nachlass variieren. [2] Bei allen teilnehmenden SEAT Partnern in Verbindung mit einem neuen Leasingvertrag mit der SEAT Leasing, Zweigniederlassung der Volkswagen Leasing GmbH, Gifhorner Straße 57, 38112 Braunschweig. 10,00 € (zzgl. MwSt.) mtl. Servicerate für die Dienstleistung Wartung & Verschleiß bei einer Gesamtlaufleistung von bis zu 30.000 km für den SEAT Leon Sportstourer. Bei einer Gesamtlaufleistung von bis zu 60.000 km beträgt die monatliche Rate 20,00 € (zzgl. MwSt.). Abweichende Staffelpreise bei höheren Gesamtlaufleistungen. Dieses Angebot ist nur bis zum 31.12.2020 gültig und nur für gewerbliche Kunden mit und ohne Großkundenvertrag. Ausgenommen sind Taxi-/Mietwagenunternehmen und Fahrschulen. Abbildung zeigt Sonderausstattung.

EUROPA-CLOUD GAIA-X ALS HEILSBRINGER FÜR DEN DATENSCHUTZ?

Stefan Mutschler

Sehr lange haben die Europäer das Thema Cloud US-amerikanischen Unternehmen überlassen. Viele Jahre herrschte pure Skepsis bezüglich Datenschutz und Datensicherheit – aber mit zunehmender Unentbehrlichkeit der im höchsten Maße skalierbaren und effizienten Cloud-Dienste wuchs auch das Verständnis für die Vorteile bei der Datensicherheit. Entsprechend erfolgreich etablierten sich aus den USA geführte Public-Cloud-Anbieter auch in Deutschland und Europa. Beim Datenschutz wuchs dabei leider eher die Bereitschaft, nicht so genau hinzusehen. Die fundamentalen Unterschiede in der Gesetzgebung in Europa und in den USA – bezüglich Datenschutz – sind nicht erst seit heute bekannt. Das jetzt ohnehin gekippte „Privacy Shield" war bei ehrlicher Betrachtung nie mehr als ein Alibi-Abkommen, das der Wirtschaft eine formal korrekte Nutzung der Cloud erlauben sollte, ohne die Datenschutzproblematik wirklich zu lösen.

In einer zunehmend polarisierenden Industriewelt funktioniert Wegschauen aber nicht mehr. Interessanterweise kam der Anstoß für einen europäisch gesteuerten Cloud-Dienst nicht aus der Wirtschaft, sondern aus der Politik. Sie sah den Handlungsbedarf und rief im Oktober 2019 das Europa-Cloud-Projekt GAIA-X ins Leben. Inzwischen haben sich hier mehr als 300 Unternehmen eingeklinkt, darunter auch einige Nicht-Europäer, wie etwa Google. Was aber die Europa-Cloud genau bringen soll, konnte auch die Anfang Juni abgehaltene Digitalkonferenz mit Bundeswirtschaftsminister Peter Altmaier und seinem französischen Amtskollegen Bruno Le Maire nicht beantworten. Allerdings schürten die beiden GAIA-X-Initiatoren große Hoffnungen auf eine erfolgreiche Cloud, die nach europäischen Datenschutzmaßstäben geführt wird. Und die sei dringend nötig, denn „Cloud-und Dateninfrastrukturen bilden die Grundlage der digitalen Ökonomie – auch in Europa", wie Bitkom-Präsident Achim Berg kürzlich bei der Vorstellung einer Cloud-Umfrage betonte.

Befeuert wird die Situation vom Europäischen Gerichtshof (EuGH): Er hat mit seinem kürzlich gefällten Urteil das sogenannte Privacy Shield, das den Datenaustausch zwischen der EU und den USA regelt, für ungültig erklärt. Außerdem hat er entschieden, dass der Datenaustausch mit Nicht-EU-Ländern auf Basis der sogenannten Standardvertragsklauseln zwar rechtens ist, aber im Einzelfall geprüft werden muss. Während besonders datenschutzaffine Unternehmen und Organisationen das als einen Sieg für den Datenschutz und einen großen Schritt hin zur digitalen Souveränität Europas feiern, sehen Wirtschaft und wirtschaftsnahe Verbände, wie der Bitkom, hohe Risiken. Sollte die Möglichkeit der Datenverarbeitung in den USA für europäische Unternehmen nicht zügig geklärt werden, sehen sie massive Wettbewerbsnachteile auf sich zukommen.

Taugt GAIA-X als nach europäischem Recht datenschutzkonforme Cloud-Plattform? Davon darf man wohl ausgehen. Aber ist sie in der Lage, in der Liga der großen Hyperscaler, wie Amazon, Google und Microsoft, mitzuspielen? Sicher nicht – dafür haben die Europäer die Cloud viel zu lange verschlafen oder verdammt. Selbst heute sind die europäischen Budgets, die zur Entwicklung von Cloud-Plattformen und -Services verwendet werden, im Vergleich zu den Investitionen der großen Cloud-Player eher ein Taschengeld. Wie so oft bleibt die Lage auch hier auf absehbare Zeit ziemlich spannend – oder besser angespannt. Alles Wichtige über die Europa-Cloud lesen Sie in unserem Beitrag ab Seite 14.

Viel Spaß beim Lesen!

Ihr Stefan Mutschler
Chefredakteur

INHALT

ACRONIS ERWIRBT DEVICELOCK

Acronis hat die Übernahme von DeviceLock bekanntgegeben. Im Rahmen dieses Deals soll DeviceLock zu einer hundertprozentigen Tochtergesellschaft von Acronis werden. Als bekannter Player im Bereich Data Leak Prevention (DLP) für Endgeräte/Endpunkte verfügt DeviceLock über eine globale Kundenpräsenz in einer Vielzahl von Branchen, darunter: Banken- und Finanzwesen, Gesundheits- und Pharmabranche, Regierungs- und Verteidigungseinrichtungen sowie Industrie- und Handelskonzerne. Die DLP-Lösung von DeviceLock wurde entwickelt, um Datenlecks direkt an der Quelle zu stoppen. Denn fast zwei Drittel aller Dataleaks mit schwerwiegenden Folgen werden durch Mitarbeiter, Auftragnehmer oder Besucher verursacht – sei es durch unbeabsichtigte Fehler oder böswillige Absichten. Die Lösungen von DeviceLock sollen einen verlässlichen Schutz wertvoller Daten vor den oben genannten Bedrohungen ermöglichen. Mit den neuen Lösungen will Acronis ein zusätzliches Leistungsspektrum abdecken, das dem Unternehmen helfen soll, all seinen Kunden erstklassigen Cyberschutz anbieten zu können.

Acronis will die Technologie von DeviceLock in seine Cyber Platform integrieren und die neuen Services über das Acronis Cyber Cloud Solutions-Portal verfügbar machen. Acronis verspricht, weiterhin an neuen Versionen des DeviceLock-DLP-Komplexes zu arbeiten – unter voller Beibehaltung des technischen Supports. ■

„Indem wir die Lösungen von DeviceLock zu unserem Portfolio aus Cyber-Protection-Produkten und -Services hinzufügen, bieten wir unseren Partnern und Kunden eine einfache Möglichkeit, ein beispielloses Maß an Funktionalität unter den Endpunkt-DLP-Lösungen zu einem erschwinglichen Preis zu erhalten", so Serguei Beloussov, Gründer und CEO von Acronis. (Foto: Acronis)

DELL TECHNOLOGIES UND VMWARE BÜNDELN TOOLS FÜR DEN SCHUTZ VOR BIOS-ANGRIFFEN

Dell Technologies hat angekündigt, sein SafeBIOS-Dienstprogramm mit der Carbon-Black-Konsole von VMware zu verknüpfen und so eine cloudbasierte BIOS-Überprüfung möglich zu machen. Unternehmen können damit den BIOS-Status ihrer PCs von Dell Technologies zentral in einer Konsole anzeigen lassen, egal wo sich die Systeme befinden: Die Überprüfung der BIOS-Integrität der Rechner findet in der Cloud statt und muss nicht direkt auf den Endpoint-Geräten durchgeführt werden, die lokal angegriffen werden können.

Sollte das BIOS korrupt oder manipuliert worden sein, ermöglicht Dell Technologies Unternehmen, das veränderte BIOS-Image zu analysieren, um die Art des Angriffs zu verstehen und entsprechende Gegenmaßnahmen einzuleiten. Dieser gesamte Prozess kann remote stattfinden, sodass IT-Abteilungen Geräte jederzeit absichern können, und zwar völlig unabhängig von ihrem Standort. Dell SafeBIOS ist Teil des umfassenden Lösungsportfolios „Dell Trusted Devices", das sowohl unterhalb als auch oberhalb des Betriebssystems arbeitet, und zuverlässige Endpunkt-Sicherheit bieten soll. ■

SIEMENS UND SALESFORCE KOOPERIEREN FÜR SICHERE ARBEITSUMGEBUNGEN

Salesforce und Siemens haben eine strategische Partnerschaft für die Entwicklung einer neuen Lösungs-Suite für Technologie am Arbeitsplatz bekanntgegeben. Diese soll Unternehmen weltweit bei der sicheren Wiedereröffnung ihrer Büros unterstützen und ein neues Arbeitsplatzerlebnis in physischen Arbeitsumgebungen schaffen. Im Rahmen der Partnerschaft werden Work.com von Salesforce, basierend auf Customer 360, und Lösungen von Siemens Smart Infrastructure, zum Beispiel Angebote von Comfy und Enlighted, kombiniert. Dadurch sollen die Prozesse, Mitarbeiter und Voraussetzungen koordiniert werden, die unerlässlich sind, um sichere, vernetzte Arbeitsstätten der Zukunft zu schaffen.

Zu den wichtigsten Bestandteilen der Lösung gehören ein „touchless office" („berührungsloses Büro") mit digitalen Mitarbeiter-Zugangskarten für den Zutritt zu Gebäuden und Aufzügen sowie ein zuverlässiges System für das Belegungsmanagement. Dies soll es den Mitarbeitern ermöglichen, Konferenzräume und Schreibtische über die Comfy-App zu reservieren, die in Echtzeit Warnmeldungen sendet, wenn Schwellenwerte erreicht werden. Darüber hinaus können Unternehmen auch Belegungs- und Standortdaten, die von Enlighted gesammelt und über Comfy gebündelt werden – etwa Mitarbeiter-Check-ins und Schreibtisch- oder Raumreservierungen – für die Erweiterung der manuellen Kontaktverfolgung über Work.com nutzen. ■

Mit ihrer Zusammenarbeit wollen Siemens und Salesforce eine sichere Rückkehr an die Arbeitsplätze nach der Krise unterstützen und intelligente, vernetzte Arbeitsstätten für die Zukunft gestalten. (Quelle: Siemens)

SICH IM HOMEOFFICE SICHER FÜHLEN – SO AKTUELL WIE NIE ZUVOR.

Dass das Arbeiten im Homeoffice nicht nur in der aktuellen Situation mehr und mehr an Bedeutung gewinnt, sondern bereits Teil einer neuen Arbeitskultur ist, belegen Statistiken schon länger. Laut Statista arbeiteten bereits 2019 knapp 40 Prozent der Mitarbeiter ganz oder teilweise von zu Hause aus. Wie die Statistik in diesen besonderen Tagen aussieht können wir uns wahrscheinlich alle vorstellen und viele Mitarbeiter und die Unternehmen selbst sind dankbar, für die Möglichkeit in einer geschützten Arbeitsumgebung weiterhin arbeiten zu können.

Schützenswert ist aber nicht nur die Gesundheit, sondern auch die personenbezogenen Daten von Kunden und Mitarbeitern etc. Denn auch im Homeoffice müssen die Regelungen der DSGVO eingehalten werden. Dabei trägt der Arbeitgeber auch für die Mitarbeiter im Homeoffice die Verantwortung und muss sicherstellen, dass die Datenschutz regelnden Maßnahmen auch dort eingehalten werden.

Mit einem Partikelschnitt-Aktenvernichter ab der Sicherheitsstufe P-4 sind alle Anforderungen an eine datenschutzgerechte und DSGVO-konforme Vernichtung gewährleistet, und man ist gleichzeitig vor hohen Bußgeldern geschützt. Jetzt ist die beste Gelegenheit, alle Homeoffice-Arbeitsplätze mit einem HSM Aktenvernichter in der korrekten Sicherheitsstufe auszustatten!

Aktenvernichter von HSM trumpfen mit überdurchschnittlich langen Garantien und Serviceleistungen auf. Das Qualitätsversprechen für die HSM SECURIO Aktenvernichter in der Premiumqualität „Made in Germany“: drei Jahre Herstellergarantie sowie eine lebenslange Garantie auf die Schneidwellen (in den Sicherheitsstufen P-2 bis P-5).

HSM BLEIBT LIEFERFÄHIG

Auch in der aktuell angespannten Krisensituation auf der ganzen Welt ist HSM nach wie vor lieferfähig. Die Lagerbestände der „Made in Germany“-Aktenvernichter wurden in den vergangenen Wochen bereits vorsorglich erhöht. Das HSM-Team und die persönlichen Ansprechpartner stehen für Fragen zu individuellen Bestellungen, Lieferzeiten, Schulungen der HSM-Akademie etc. telefonisch und per E-Mail zur Verfügung. ■

Weitere Informationen und passende Aktenvernichter-Modelle finden Sie unter **www.hsm.eu/shred-at-home**

Mehr dazu hier

HSM GmbH + Co. KG
Austraße 1-9
88699 Frickingen / Germany
Tel. +49 7554 2100-0
Fax: +49 7554 2100-160
Internet: **www.hsm.eu**
E-Mail: **info@hsm.eu**

HSM®
Great Products, Great People.

VERONYM UND BRIDGE4IT WOLLEN GEMEINSAM MITTELSTÄNDLER SCHÜTZEN

Umfassender Schutz vor Cyberbedrohungen ist für kleine und mittelständische Unternehmen häufig eine Frage der Ressourcen und Budgets. Cloud Security Services liefern hier nun aber mittlerweile die passenden Antworten. Wichtig dabei ist es, die spezifischen Anforderungen der Unternehmen zu berücksichtigen, die sich je nach Unternehmensgröße, Geschäftsmodell und Branche oft deutlich unterscheiden. Veronym und bridge4IT haben deshalb nun eine Partnerschaft vereinbart. Gemeinsam wollen die beiden Unternehmen in Deutschland kleinen und mittelständischen Firmen aufeinander abgestimmte Lösungen für die Phasen vor, während und nach einem Cyberangriff anbieten. Dadurch soll es gelingen, das Risiko von Schäden durch Cyberangriffe zu minimieren.

Veronym ist seit rund einem Jahr als erster deutscher Cloud Security Service Provider aktiv und bietet speziell für kleine und mittelständische Unternehmen vollständig gemanagte IT-Sicherheitsdienste aus der Cloud. Um Kunden ganzheitlich zu betreuen, arbeitet Veronym mit Partnern zusammen. Als neuer Partner erweitert nun bridge4IT das Angebot von Veronym. Das Unternehmen bildet die Brücke zwischen Cybersicherheit und allgemeiner IT für Unternehmen vor dem Hintergrund der digitalen Transformation und der daraus entstehenden neuen Möglichkeiten. ■

BLACKBERRY UNTERSTÜTZT DIE SUSTAINABLE DEVELOPMENT GOALS DER VEREINTEN NATIONEN

BlackBerry hat angekündigt, das eigene Engagement für die Sustainable Development Goals (SDGs) des United Nations Global Compact (UNGC) zu erweitern. Unter anderem investiert BlackBerry in Initiativen, die der globalen Gemeinschaft den Zugang zu sauberem Wasser ermöglichen. Milliarden von Menschen auf der ganzen Welt haben gegenwärtig keinen Zugang zu sauberem Wasser, adäquaten sanitären Einrichtungen und Handwaschgelegenheiten. Am stärksten davon betroffen sind Communities of Color, Menschen mit niedrigem Einkommen, Stammesgemeinschaften und Entwicklungsländer. Die sanitäre Versorgung mit sauberem Wasser ist ein entscheidender Faktor für den Zugang zu Bildung, insbesondere für Mädchen, und eine Strategie für Wirtschaftswachstum und Armutsbekämpfung. Im Hinblick auf das eigene Engagement hat BlackBerry nun zugesichert, bis 2021 kohlenstoffneutral zu sein, in Abwasserbehandlungstechnologie in Kanada, ebenso wie in die Sanierung und Instandhaltung von Wasserbrunnen in Ruanda zu investieren und bis 2021 weltweit keine Einwegkunststoffe mehr zu verwenden. ■

FORTINET ÜBERNIMMT OPAQ NETWORKS

Fortinet übernimmt OPAQ Networks, einen Secure-Access-Service-Edge-(SASE-)Cloud-Anbieter. Die Zero-Trust-Network-Access-(ZTNA-)Cloud-Lösung von OPAQ schützt die verteilten Netzwerke von Unternehmen – von Rechenzentren über Zweigstellen bis hin zu Remote-Benutzern und Internet of Things (IoT)-Geräten. Die Security Fabric von Fortinet soll in Kombination mit der patentierten ZTNA-Lösung von OPAQ das bestehende SASE-Angebot von Fortinet erweitern. Dadurch entsteht eine SASE-Cloud-Security-Plattform mit integrierter Zero-Trust-Zugriffs- und Sicherheitslösung.

Darüber hinaus ist die OPAQ-Plattform partnerfreundlich konzipiert und solle es Managed Security Service Providern (MSSPs) ermöglichen, Netzbetreibern und Value Add-Partnern, die SASE-Multimandantenplattform unkompliziert in ihr eigenes Angebot zu integrieren. Mit ihrem Fachwissen im Network-Operations- und Security-Operations-Center sowie ihren Dienstleistungen können Partner die Kunden von Unternehmen und Behörden unterstützen. ■

PALO ALTO NETWORKS ERMUTIGT IT-SICHERHEITSBRANCHE ZU MEHR ZUSAMMENARBEIT

Egal ob Wirtschaft, Politik oder Gesellschaft: Im Laufe der Geschichte wurde jede große globale Herausforderung am besten durch Kooperation und Zusammenarbeit gemeistert. Die heutige globale Herausforderung durch Cyberbedrohungen ist nach Meinung von Palo Alto Networks nicht anders: Es ist nicht einfach, Angreifer dauerhaft am Eindringen in ein Unternehmen zu hindern. Selbst das sicherheitsbewussteste Unternehmen bleibt dem Risiko eines Angriffs ausgesetzt. In einer Cybersicherheitslandschaft, die von fragmentierten Sicherheitsanbietern und -tools dominiert wird, haben Unternehmen Mühe, sich zu schützen. Niemand könne hochentwickelte Cyberbedrohungen allein stoppen. Es bedürfe eines kooperativen Ansatzes zwischen Cybersicherheitsanbietern, Managed Security Service Providern (MSSP) und Unternehmen, um sich der globalen Herausforderung der Cyberbedrohungen zu stellen, wie Palo Alto Networks erklärt.

Die heutige komplexe Bedrohungslandschaft, kombiniert mit der Vielfalt und dem Volumen des Netzwerkverkehrs in der modernen Kundenumgebung, mache eine präzise und effektive Bedrohungsprävention zu einer großen Herausforderung. Dieses Problem werde durch die Herausforderung verschärft, neue, noch nie dagewesene oder Zero-Day-Malware und Exploits zu erkennen, sowie bekannte bösartige Inhalte zu identifizieren und zu stoppen. So wie Cybersicherheitsexperten ständig nach Möglichkeiten suchen, bessere und sicherere Softwareprogramme zu entwickeln, bleiben Angreifer immer auf dem neuesten Stand, um die neuesten Abwehrmechanismen zu überwinden. Grenzüberschreitende Organisationen, wie die Cyber Threat Alliance, würden den Informationsaustausch über Cyberbedrohungen auf eine neue Ebene heben. Ziel dieser Anstrengungen ist es, einen besseren Schutz der Öffentlichkeit vor Cyberangriffen zu erreichen. ■

Sec-IT

Mehr Wert.
Mehr Vertrauen.

TÜV SÜD: Vertrauen schaffen in digitale Technologien.

Ihr Partner für Cyber Security Services, Sealed Cloud Lösungen und Trainings für IT-Sicherheit.

TÜV SÜD unterstützt Unternehmen dabei, die Chancen der Digitalisierung zu nutzen. Dabei richten wir unser Augenmerk auf Anforderungen und Risiken. Cyber Security und Datensicherheit sind Teil unserer Kernkompetenz. Wir bieten:

- Industriespezifische Erfahrung, Know-how und Experten, die zu den Besten zählen
- Umfassende Unterstützung von der Risikoanalyse über die Beseitigung von Sicherheitslücken bis zur dauerhaften Absicherung Ihrer Geschäftsprozesse
- Mitarbeiter-Schulungen, damit Kompetenzaufbau und Handlungsfähigkeit gesichert sind

Vertrauen Sie TÜV SÜD rund um die IT-Sicherheit Ihres Unternehmens. 25.000 Mitarbeiter sind weltweit für Sie da.

www.tuvsud.com/de-cybersecurity

TÜV SÜD Sec-IT GmbH Ridlerstraße 57, 80339 München, Deutschland
Tel. +49 89 5008-4208 www.tuvsud.com/de-cybersecurity

TÜV®

MIT EINEM **IT-SICHERHEITSBEAUFTRAGTEN** AUCH IN SCHWIERIGEN ZEITEN FÜR IT-SICHERHEIT SORGEN

Aufgrund der rasch zunehmenden Digitalisierung im Zuge der Corona-Krise ist IT-Sicherheit aktuell wichtiger denn je. So bietet beispielsweise das Homeoffice in vielen Fällen eine leichte Angriffsfläche für Hacker und Computerviren. Eine Störung der digitalen Infrastruktur kann in Unternehmen zu enormen Schäden und hohen Kosten führen. Die IT-Sicherheit sollte daher mit oberster Priorität behandelt werden. Sie steht nicht nur für die Sicherung von sensiblen Informationen oder den Schutz vor ständig neuen Gefährdungslagen, sondern gilt als existenzieller Wettbewerbsfaktor.

Die Benennung eines IT-Sicherheitsbeauftragten im Unternehmen ist ein wichtiger Baustein zur Absicherung vor neuen Risiken und Gefahren. Die AKADEMIE HERKERT bildet IT-Sicherheitsbeauftragte in nur drei Tagen im Rahmen eines Zertifikatslehrgangs aus. Nach erfolgreich bestandener Abschlussprüfung dient ein Zertifikat als qualifizierter Leistungsnachweis.

Die Teilnehmer haben dabei die Wahl, sich online in einem virtuellen Schulungsraum, oder vor Ort weiterbilden zu lassen. Die AKADEMIE HERKERT bietet den nächsten Online-Lehrgang vom 03.11.–05.11.2020 live am PC an. In Hamburg findet der kommende Präsenz-Termin des Lehrgangs vom 24.11.–26.11.2020 statt. Weitere Termine und zusätzliche Informationen zum Lehrgang IT-Sicherheitsbeauftragte/r finden Interessierte unter www.akademie-herkert.de/its20.

Die Leser dieses Beitrags profitieren außerdem mit dem **Vorteilscode its-2020** bis 30.09.2020 exklusiv von zehn Prozent Rabatt. ■

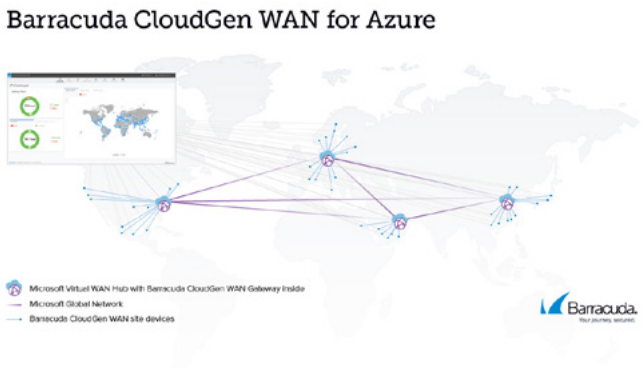
REMOTE KOLLABORATION MIT HÖHERER KAPAZITÄT, SICHERHEIT UND TRANSPARENZ

Cisco erweitert Webex zur Verbesserung ortsunabhängiger Arbeitsprozesse – egal ob für Mitarbeiter im Homeoffice oder für die Rückkehr in das Büro. Zu den Neuerungen gehören Sicherheits- und Compliance-Funktionen, intelligente Einblicke für konsistente User Experience und eine Integration mit Box. Zudem bietet die Integration von Epic für Patienten die Möglichkeit, sich mit Ärzten per Video zu verbinden. Um auch in Zukunft die gewohnte Qualität und Stabilität zu liefern, hat Cisco deutlich in den Ausbau der weltweiten Ressourcen investiert. So besitzt die Webex-Plattform nun die dreifache Kapazität.

Die Sicherheit der Webex-Plattform wurde mit Funktionen für Data Loss Prevention (DLP) und die rechtliche Absicherung von Webex-Meetings verbessert. Dies bietet Schutz für alle Inhalte wie Aufzeichnungen, Transkriptionen, Aktionselemente und Highlights. Auch die Ende-zu-Ende-Verschlüsselung wurde noch einmal gestärkt: Die AES-256-Bit-Verschlüsselung wurde um den GCM-Modus ergänzt. Der Cisco Webex Control Hub bietet intelligente Einblicke, damit die IT-Abteilung alle Collaboration Workloads über eine Ansicht verwalten kann. Das ist unabhängig davon, ob die Mitarbeiter zu Hause oder im Büro sind. ■

AZURE-BASIERTER, SICHERER SD-WAN-DIENST

Eine „Cloud-first"-Strategie erfordert einen anderen Ansatz hinsichtlich der Konnektivität. Traditionelle Konnektivität reicht nicht: Es braucht vielmehr eine Lösung, die den Fokus auf eine verbesserte Performance der Applikationen, etwa Office 365, legt. Barracuda stellt mit seiner neuen WAN-Plattform CloudGen den ersten Secure SD-WAN-Dienst vor, der nativ auf Azure aufbaut. Da das Microsoft Global Network automatisch als Backbone für den orts- und zeitunabhängigen Anwendungszugriff fungiert, können Service Provider eine pragmatische und bedarfsgerechte SASE-Lösung (Secure Access Service Edge) in der Public Cloud erstellen. CloudGen WAN ist ein SaaS-Service, der direkt vom Azure Marketplace für so viele Regionen wie nötig bereitgestellt und zentral im CloudGen WAN-Portal für alle Bürostandorte und Remote-Endpunkte verwaltet wird. ■



Barracuda stellt mit seiner neuen WAN-Plattform CloudGen den ersten Secure SD-WAN-Dienst vor, der nativ auf Azure aufbaut. (Quelle: Barracuda)

3-IN-1-SECURITY-LÖSUNG FÜR MITTELSTÄNDISCHE UND GROSSE UNTERNEHMEN

Die neueste Version der Kaspersky-Flaggschifflösung Endpoint Security for Business für mittelständische und große Unternehmen integriert ab sofort die Cloud-Management-Konsole Kaspersky Endpoint Detection and Response (EDR) Optimum sowie Kaspersky Sandbox. Die neue EDR-Lösung eigne sich jetzt auch für Firmen, die über begrenzte Sicherheitsexpertise und überschaubare Security-Ressourcen verfügen, da IT-Sicherheitsexperten nun sofort einen Überblick und umfassende Informationen über etwaige Sicherheitsvorfälle erhielten – inklusive einer umgehenden Schadensanalyse sowie automatisierten Reaktionsoptionen.

Identifiziert Kaspersky Endpoint Security for Business eine verdächtige Datei, die nicht definitiv als gut- oder bösartig eingestuft werden kann, sendet es diese an die Kaspersky Sandbox. Dieses zusätzliche neue Sicherheitstool führt anschließend die verdächtige Datei automatisch in einer isolierten Umgebung aus und analysiert sie hinsichtlich ihres Gefährdungspotenzials. Die hieraus gewonnenen Auswertungsdaten können durch die von Kaspersky EDR Optimum durchgeführte Analyse weiter angereichert werden. ■

BENUTZERNAMEN UND PASSWÖRTER WERDEN ÜBERFLÜSSIG

Der im Bereich digitales Identitätsmanagement aktive Plattformanbieter ForgeRock präsentiert ForgeRock Go, eine neue Lösung, die Benutzernamen und Passwörter für die Anmeldung bei Websites überflüssig machen soll. Bei durchschnittlich 130 Online-Konten [1] pro Person fällt es zunehmend schwer, sich alle Benutzernamen und Passwörter zu merken, die zur Authentifizierung bei geschäftlichen oder privaten Diensten erforderlich sind. Passwörter können Verbraucher auch daran hindern, Online-Einkäufe zu tätigen. Untersuchungen zeigen, dass mehr als ein Drittel der Menschen einen Online-Einkauf abbricht, wenn sie beim Auschecken auf einer E-Commerce-Website das Passwort vergessen haben oder dieses zurücksetzen müssen. Benutzernamen und Kennwörter sind unsicher und bieten eine schlechte User Experience. Selbst bei Multi-Faktor-Authentifizierungslösungen (MFA) sind viele davon proprietär und erfordern komplexe Integrationen, die möglicherweise nicht den Grad an Agilität bieten, den Unternehmen benötigen.

ForgeRock Go soll es Organisationen ermöglichen, Benutzer mit jedem beliebigen Authentifikator zu authentifizieren, der auf dem Gerät des Benutzers vorhanden ist. Dieses muss WebAuthN, einen Teil des FIDO-Alliance-Standards FIDO2, unterstützen. Beim Zugriff auf einen Dienst oder ein Konto über das Gerät wird der Benutzer „erkannt" und mit Authentifikatoren authentifiziert, die residente Schlüssel, wie Biometrie (TouchID), Windows Hello, oder einen PIN-geschützten Schlüssel, wie Yubico, unterstützen. So erhält er sofort Zugriff auf das Konto. Die Berechtigungsnachweise werden auf dem Gerät gespeichert und niemals online gesendet, wodurch das Risiko eines Zugriffs auf Informationen in einer beschädigten Datenbank verringert werden soll. ■

[1] https://digitalguardian.com/blog/uncovering-password-habits-are-users-password-security-habits-improving-infographic#:~:text=In%20fact%2C%20a%20Dashlane%20analysis,to%20a%20single%20email%20address.

UMFASSENDE ERKENNUNG VON CYBERGEFAHREN DURCH MANAGED SIEM SERVICES

Viele Unternehmen setzen zur Abwehr von Cybergefahren auf Security Information & Event Management (SIEM)-Lösungen. Die Einrichtung und der Betrieb von SIEM-Lösungen setzt tiefes Fachwissen und Erfahrung bei der Erkennung von Cybergefahren voraus – und zwar bei der Formulierung ebenso wie bei der Implementierung der Erkennungsmechanismen. Denn zur Erkennung von Ereignissen, also Security-relevanten Vorfällen, verwenden diese Systeme üblicherweise sogenannte Use Cases. Durch den Use-Case-Ansatz ist es möglich, sehr schnell aus der großen Anzahl täglicher Events potenzielle sicherheitsrelevante Vorfälle herauszufiltern. Der Systemintegrator und Managed Service Provider Controlware hat diesen Ansatz weiterentwickelt und kann so weitaus mehr Cybergefahren erkennen und Attacken erfolgreich stoppen oder verhindern. Denn: In der Praxis beschränken sich die Use Cases der gängigen SIEM-Lösungen meist auf Compliance-getriebene Fälle. Darunter sind Basis Use Cases zu verstehen, die Verstöße gegen Compliance-Richtlinien erkennen oder Auffälligkeiten in System-Protokollierungen beziehungsweise Logdaten feststellen, die eventuell auf Security Incidents hindeuten. Diese Use Cases stellen eine Basisüberwachung sicher, eignen sich jedoch nicht zur vollständigen Erkennung „echter" Cybergefahren und -attacken.

Controlware hat deshalb seinen Use-Case-Katalog um Cyber-Security-Use-Cases auf Basis des MITRE ATT&CK-Modells erweitert. Bei diesen Use Cases liegt der Fokus auf der Erkennung von Cybergefahren beziehungsweise Cyberangriffen. Hier wird versucht, die typischen Angreifer-Techniken in den unterschiedlichen Phasen eines Cyberangriffs über die Auswertung der entsprechenden Logdaten zu erkennen. Diese sind erheblich komplexer als Basis Use Cases und erfordern bei der Formulierung ein sehr profundes Verständnis der Techniken und Vorgehensweisen von Angreifern sowie Erfahrung bei der individuellen Anpassung an die Kundenumgebung. Zudem sind erweiterte Logquellen wie Sysmon- oder Powershell-Logs erforderlich. ■

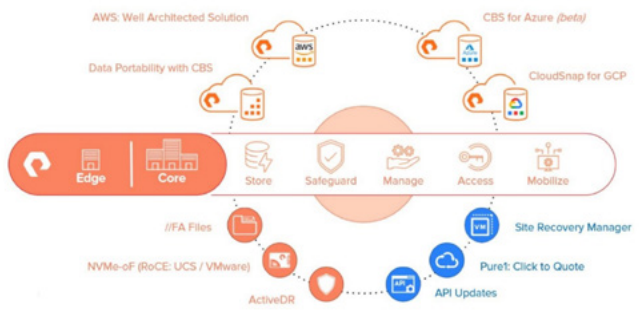
VERTRAUENSWÜRDIGE KÜNSTLICHE INTELLIGENZ (KI/AI)

Datenschutz und vertrauenswürdige KI sind nicht erst in Pandemie-Zeiten zu zentralen Themen geworden. Der Umgang mit personenbezogenen Daten stellt große Herausforderungen insbesondere an die Datenwissenschaft. Denn KI-Algorithmen sind einerseits auf gute Daten angewiesen, andererseits kann mit KI-Methoden selbst oft leicht mehr über Daten verraten werden, als gewünscht. Herkömmliche Ansätze, wie die Anonymisierung, sind oft nicht sicher genug, oder verschlechtern die Qualität zu sehr. Gradient Zero hat dafür DQ0 entwickelt. DQ0 ist eine Plattform für datenschutzkonformes Maschinelles Lernen – ohne aufwendige Anonymisierungsprozesse, mit höherem Schutz und mehr Qualität. DQ0 garantiert mathematisch prüfbaren Datenschutz, basierend auf Differential Privacy. Für vertrauenswürdige KI. https://dq0.io/de/ ■

FLASHARRAY FÜR AGILE DATENDIENSTE

Der Storage-as-a-Service-Pionier Pure Storage hat mit Purity 6.0 für FlashArray die neueste Version seiner zentralen Software Suite vorgestellt. Diese neuen, agilen Datendienste wurden mit Blick auf das moderne Unternehmen entwickelt. Sie sollen Unternehmen eine effiziente Möglichkeit bieten, ihre Daten zu speichern, zu sichern, zu verwalten und auf sie zuzugreifen. Zudem können Unternehmen ihre Daten mittels strategischer Verbrauchsmodelle mobilisieren, die auf ihre Bedürfnisse zugeschnitten sind.

Purity 6.0 vereinfache die moderne Infrastruktur weiter mit einer Unified-Block-and-File-Lösung. Diese hat Pure Storage entwickelt, um Infrastruktur-Herausforderungen zu lösen. Dazu gehören beispielsweise Daten-Silos und -Zerpflückung, die sich auf moderne Unternehmen in jeder Branche negativ auswirken. Mit einer Vielzahl neuer agiler Datendienste können Kunden von Pure Storage sofort zwei neue Schlüsselfunktionen nutzen: die einheitliche Unterstützung der Protokolle NFS und SMB sowie Active Disaster Recovery auf der Grundlage einer neuen Technologie für kontinuierliche Replikation. Als Teil des Evergreen Storage-Subskriptions-Modells sind diese neuen Funktionen ohne zusätzliche Lizenzen, Supportkosten und Komplexität nutzbar. ■



Purity 6.0 für FlashArray soll Unternehmen eine effiziente Möglichkeit bieten, ihre Daten zu speichern, zu sichern, zu verwalten und auf sie zuzugreifen. (Quelle: Pure Storage)

SECURITY CENTER FÜR INCIDENT DETECTION UND RESPONSE LIFECYCLE

Moderne Netzwerke bieten heutzutage eine große Angriffsfläche. Angreifer sind opportunistisch und führen eine Vielzahl an Attacken aus, die früher oder später ihr Opfer finden. Allerdings werden Angriffe oft zu spät oder gar nicht entdeckt. Allgeier CORE und Rapid7 bieten mit der modernen SIEM-Lösung InsightIDR und ihrem gebündelten Know-how einen 24/7-Managed-Service, um frühzeitig Sicherheitsvorfälle zu erkennen und umgehend darauf reagieren zu können.

InsightIDR kombiniert Endpoint-Forensik, Protokollsuche und nutzerorientierte Dashboards in einer Lösung. Das Security-Information-and-Event-Management-(SIEM-)Tool sammelt Daten vorhandener Netzwerksicherheitstools, Authentifizierungsprotokolle und Endgeräte. Dazu aggregiert die Lösung die Daten auf einem lokalen Collector oder einem dedizierten Host-Computer, der die Daten zentralisiert.

InsightIDR identifiziert nicht-autorisierte externe sowie interne Zugriffe und hebt verdächtige Aktivitäten hervor. Auf diese Weise erhalten SOCs oder IT-Abteilungen in Unternehmen einen Echtzeit-Überblick darüber, was in ihrem Netzwerk passiert, ohne selbst Tausende Datenströme überwachen zu müssen. ■

ITSM, SELF-HELP UND REMOTE-SUPPORT INTEGRIERT

Mit ständigem Homeoffice als neue Realität wird die Bereitstellung von sicherem Remote-Support und KI-basierten Self-Help-Lösungen zwingend. Der Service-Management-Spezialist Prevolution hat dazu die jeweils führenden Plattformen Cherwell, EasyVista Self-Help und BeyondTrust nahtlos integriert. Damit können Kunden den neuen Herausforderungen im Service Management effizient und sicher begegnen. Nutzer können durch Self-Help Fragen erheblich schneller lösen, und die Automatisierung steigert die Effizienz deutlich. www.prevolution.de

Bild: ©AndSus/stock.adobe.com

Ermittlung fehlerhafter Berechtigungsvergaben im Active Directory und im NTFS-Filesystem

ENDLICH TRANSPARENZ

KONTINUIERLICHE RICHTLINIENBASIERTE ÜBERWACHUNG MIT DER DACCORD MICROSOFT EDITION

Die Cyberkriminalität ist weiter auf dem Vormarsch. Gerade durch die zunehmende Digitalisierung ergeben sich neue Möglichkeiten für Hacker. Insgesamt steigt nicht nur die Zahl der Cyberattacken, sondern auch die Professionalität der Täter. Umso wichtiger ist es, Sicherheitslücken zu schließen. Darunter fallen unter anderem aktive Benutzerkonten von ehemaligen Mitarbeitern, über die sich Kriminelle in IT-Systeme einschleusen und sensible Informationen abgreifen können. Mit der Access-Governance-Lösung daccord von G+H Systems lassen sich derartige Schwachstellen in der IT-Sicherheit beheben. Seit Kurzem ist die Software auch als Microsoft Edition erhältlich, die Systemadministratoren bei der Überwachung der Richtlinien und Benutzerkonstellationen im Active Directory (AD) und im NTFS-Filesystem unterstützt. Autor **JÜRGEN BÄHR,** Geschäftsführer der G+H Systems GmbH

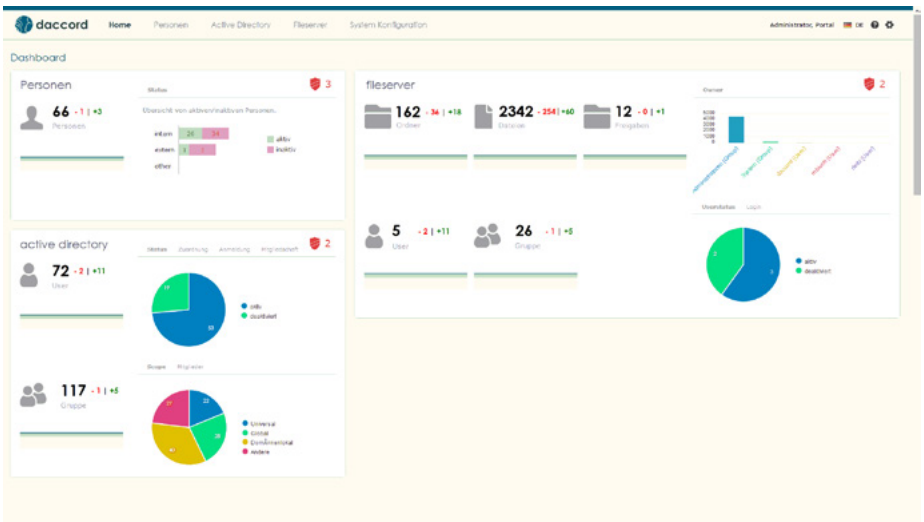
Ohne eine softwarebasierte Auswertung der Berechtigungen von Mitarbeitern geht schnell der Überblick verloren, wer worauf zugreifen darf. Damit es erst gar nicht zu Ungereimtheiten, wie Überberechtigungen, veralteten Mitarbeiterkonten & Co., kommt, ist der Einsatz einer Access-Governance-Lösung, die kontinuierlich Berechtigungen überwacht, anzuraten.

Die daccord Microsoft Edition erspart IT-Administratoren die manuelle Analyse von AD-Objekten und Fileserver-Strukturen, die äußerst zeitaufwendig und noch dazu fehleranfällig ist. Sie lässt sich einfach installieren sowie konfigurieren und erfasst die Zugriffsberechtigungen der einzelnen Benutzer und Gruppen innerhalb der firmeninternen Microsoft-Infrastruktur. Zur Feststellung von Auffälligkeiten ist es möglich, die Berechtigungen automatisiert auf Konformität zu den Microsoft-Best-Practice-Richtlinien zu überprüfen. Dafür wird zusammen mit der Software ein Paket mit mehr als 25 Richtlinien ausgeliefert. So lässt sich beispielsweise analysieren, welche aktiven Personen ohne Verantwortlichen vorliegen, wie viele Benutzerkonten Vollzugriff haben oder wo Gruppen mit sich selbst verschachtelt sind.

Der Systemverantwortliche kann selbst entscheiden, welche Policies er aktiviert, beziehungsweise ein Risikolevel definieren, ab dem ein Wert als kritisch angezeigt wird. Ein in der Lösung integriertes Web Dashboard stellt die Informationen schließlich strukturiert dar, sodass falsche Berechtigungskonstellationen auf den ersten Blick sichtbar sind. Zur Überwachung individueller Berechtigungskonzepte können auch kundenspezifische Richtlinien eingebunden werden.

Abgleich mit Microsoft Guidelines und Personalsystem

Mit daccord lassen sich auf Basis der hinterlegten Policies von Microsoft Abweichungen identifizieren sowie abbilden. Sobald ein Verstoß gegen die aktivierten Richtlinien eintritt, spricht die Software entsprechende Handlungsempfehlungen aus.



Für den Bereich NTFS rät Microsoft zum Beispiel dazu, dass Benutzerkonten besser keine direkt vergebenen Berechtigungen auf Ordner oder Dateien besitzen sollten. Ergibt die Auswertung, dass derartige Konten existieren, wird der Einsatz des AGDLP-Konzeptes empfohlen. Demgemäß haben die Administratoren die Aufgabe, die Benutzerkonten den globalen Gruppen zuzuordnen, die wiederum Mitglieder der domänenlokalen Gruppen werden, um schließlich die Berechtigungen in ebendiesen domänenlokalen Gruppen zu vergeben.

Im Bereich AD sollte etwa die Vergabe von höher privilegierten Konten nach dem Minimalprinzip erfolgen. Folglich kontrolliert die Softwarelösung, wie viele Benutzer der Domänen-Admin-Gruppe zugewiesen sind. Wird das zuvor festgelegte Risikolevel erreicht, zeigt die Software dies unmittelbar an.

Zusätzlich zu den Policies ist ein Abgleich mit einem vorhandenen Personalsystem möglich. Auf diese Weise lassen sich Benutzerkonten ermitteln, die ausgeschiedenen oder zurzeit inaktiven Mitarbeitern zugeordnet sind. Entdeckt die Software einen solchen Missstand, informiert sie den Administrator umgehend.

Fazit

Egal ob Unter- oder Überberechtigungen, aktive Konten früherer Mitarbeiter oder leere Gruppen und Gruppenmitgliedschaften – die daccord Microsoft Edition bringt sämtliche Unstimmigkeiten hinsichtlich Zugriffsberechtigungen ans Licht und trägt in Zeiten zunehmender Cyberrisiken maßgeblich zu einer gesteigerten IT-Sicherheit bei. ■

Mehr dazu hier

Public Cloud mit Datenschutz und Datensicherheit nach europäischen Maßstäben

WAS BRINGT GAIA-X?

Sehr lange haben die Europäer das Thema Cloud US-amerikanischen Unternehmen überlassen. Viele Jahre herrschte pure Skepsis bezüglich Datenschutz und Datensicherheit – aber mit zunehmender Unentbehrlichkeit der im höchsten Maße skalierbaren und effizienten Cloud-Dienste wuchs auch das Verständnis für die Vorteile bei der Datensicherheit – beim Datenschutz aber eher die Bereitschaft, nicht so genau hinzusehen. In einer sich zunehmend polarisierenden Industriewelt funktioniert Letzteres aber nicht mehr, und so war es tatsächlich die Politik, die im Oktober 2019 einen europäisch gesteuerten Cloud-Dienst ins Leben rief – vielleicht schon in Vorahnung des kürzlichen Urteils des Europäischen Gerichtshofs (EuGH). Mit dessen Aufkündigung des höchst umstrittenen EU-US Privacy Shield geraten viele europäische Unternehmen nun in eine Art „Cloud-Vakuum". Entsprechend hoch sind die Erwartungen an GAIA-X.

> „Cloud-und Dateninfrastrukturen bilden die Grundlage der digitalen Ökonomie – auch in Europa“

ACHIM BERG,
Bitkom-Präsident
(Foto: Bitkom)

Anfang Juni hat Bundeswirtschaftsminister Peter Altmaier bei einer Digitalkonferenz zusammen mit seinem französischen Amtskollegen Bruno Le Maire das technische Konzept und die künftige Organisationsstruktur des Infrastruktur- und Datennetzwerks GAIA-X offiziell vorgestellt. Viele Fragen blieben offen – gleichzeitig schürte er Hoffnungen, dass ein europäisch geführtes Cloud-Projekt endlich zum Erfolg geführt werden könnte.

Und das tut not. Laut einer repräsentativen Umfrage von Bitkom Research nutzten im vergangenen Jahr 73 Prozent der Unternehmen in Deutschland Rechenleistungen aus der Cloud. Für die entsprechenden Unternehmen war Datenschutz das Top-Kriterium bei der Auswahl eines Cloud-Dienstleisters. Fast alle (90 Prozent) gaben an, dass für sie die Konformität mit der Datenschutz-Grundverordnung bei Cloud-Lösungen unverzichtbar ist. Für acht von zehn (79 Prozent) war eine transparente Sicherheitsarchitektur essenziell. Auch die Standortfrage beschäftigte die Unternehmen. Für jeweils zwei Drittel mussten der Hauptsitz des Cloud-Anbieters (67 Prozent) sowie das Rechenzentrum im Rechtsgebiet der EU sitzen (66 Prozent). „Cloud- und Dateninfrastrukturen bilden die Grundlage der digitalen Ökonomie – auch in Europa“, so Bitkom-Präsident Achim Berg. „GAIA-X kann das Fundament für die geplanten europäischen Datenräume legen, wie sie die EU-Datenstrategie vorsieht. Damit stärkt Europa langfristig seine Datensouveränität.“

Die Idee zu GAIA-X wurde erstmals auf dem Digital-Gipfel im Oktober 2019 der Öffentlichkeit vorgestellt. Seitdem arbeiten mehrere hundert Experten an dem umfassenden europäischen Datenökosystem mit. So ist entlang konkreter Anwendungsbeispiele aus verschiedenen Wirtschaftsbranchen und dem öffentlichen Sektor eine erste technische Architektur entstanden, auf der sich Daten breit zugänglich machen und vertrauensvoll austauschen lassen sollen. „GAIA-X ist die gemeinsame Chance für Anbieter und Anwender von Cloud-Diensten in Europa“, so Andreas Weiss, Direktor EuroCloud Deutschland, während des Virtual Expert Forum im Anschluss der Digitalkonferenz. „EuroCloud Deutschland arbeitet an der verteilten europäischen Dateninfrastruktur mit und setzt sich für die Interessen von Digitalwirtschaft, Cloud Service Providern, kleinen und mittleren Unternehmen sowie Hyperscalern ein.“

GAIA-X baut föderierte digitale Infrastruktur- und Datendienste für die digitale Wertschöpfung in Europa auf. Auch Edge- und Interconnection-Services sollen sich in die Architektur einbeziehen lassen. Zudem bietet sich GAIA-X als Lösung für Cloud-Native-Projekte an, die ohne Altlasten direkt in die digitale Welt starten. Das soll Cloud-Dienste möglich machen, die nicht nur konkurrenzfähig agil und skalierbar sind, sondern auch mit Datenschutz und Sicherheit nach europäischen Rahmenbedingungen punkten. In diese Richtung engagiert sich beispielsweise das neue EuroCloud Deutschland Mitglied Google Cloud. „Cloud Native – das beschreibt auch unser Unternehmen sehr gut. Daher unterstützt Google Cloud als Mitglied bei EuroCloud Deutschland gern diese und weitere Initiativen zur digitalen Transformation – und auch GAIA-X als europäisches Projekt mit internationalem Anspruch“, so Annette Maier, Managing Director Google Cloud DACH.

Anbieter und Abnehmer planen derzeit, Anfang 2021 ein erstes GAIA-X MVP (Minimal Viable Product) erarbeitet zu haben. „Hier bedarf es einer umfassenden kollektiven Anstrengung, die es allen ermöglicht, gleichwertig mitzugestalten“, so Weiss. „Das gilt in besonderem Maße für weitere Länder neben den aktuellen Initiatoren aus Deutschland und Frankreich.“

Die GAIA-X-Vereinigung besteht aus 22 Gründungsmitgliedern (führende Institutionen aus Industrie, Wissenschaft und Verbände). Derzeit hat das Projekt rund 300 Unternehmen als Mitglieder. Dahinter steht die Auffassung, dass die Schaffung digitaler Ökosysteme den Aufbau von Vertrauen und Interoperabilität zwischen allen Cloud-Benutzern und -Anbietern erfordert. GAIA-X begegnet dieser Herausforderung mit einem gemeinsamen Katalog von Richtlinien, ei-

„GAIA-X ist die gemeinsame Chance für Anbieter und Anwender von Cloud-Diensten in Europa“

ANDREAS WEISS,
Direktor EuroCloud Deutschland.
(Foto: EuroCloud Deutschland_eco e. V.)

ner „Architektur von Standards“ und einer Reihe von „Federation Services“, die bestehende Cloud-Anbieter und ihre Dienste zusammenführen und in denen die souveräne Nutzung von Daten und Anwendungen gewährleistet ist. Fertig ausgearbeitet ist davon aber noch nichts. „Europas digitale Führungsrolle in der Datenwirtschaft erfordert flexible und sichere Cloud-Ressourcen“, so Elie Girard, CEO von Gründungsmitglied Atos. „Durch die Erleichterung der Infrastruktur-, Anwendungs- und Datenübertragbarkeit wird GAIA-X es europäischen Unternehmen und öffentlichen Verwaltungen ermöglichen, ihre dezentralisierten Daten auf zuverlässige und sichere Weise gemeinsam zu nutzen.“ Ursprünglich sollte es schon 2020 mit ersten GAIA-X-Diensten losgehen – Corona sorgte nun für eine Verschiebung nach Anfang 2021. ■

STEFAN MUTS CHLER

FRAGEN ZU GAIA-X AN THOMAS SCHUMACHER, LEITER IT-SECURITY BEI ACCENTURE

ITS: Wie soll GAIA-X im Vergleich zu den großen Hyperscalern positioniert werden? Welche Dienste stehen zunächst im Fokus?

Betrachten wir diesen Aspekt vom Standpunkt Cyber Security aus, ist es sicherlich ein Vorteil, dass man sicherheitsrelevante Überlegungen von Anfang an in die Entwicklung der Cloud-Plattform einfließen lassen kann. Damit wären Security und Privacy by design Differenzierungsfaktoren zu den etablierten Anbietern. Darüber hinaus hat GAIA-X das Potenzial, Sicherheit in Bezug auf Transparenz, Cyber Security und Datenschutz für europäische Unternehmen zu schaffen. Gegebenenfalls besteht die Möglichkeit, spezifische Risikoprofile für lokale Schlüsselindustrien vorzukonfigurieren. Damit ist die Berücksichtigung datenschutzrelevanter Aspekte nach GDPR beziehungsweise DS-GVO von Beginn an sichergestellt. Security ist allerdings nur einer von vielen Aspekten, der über den Erfolg des Projekts entscheidet. Letztendlich ist es die Funktionalität von GAIA-X, die ausschlaggebend dafür sein wird, wie die europäische Cloud-Alternative im globalen Wettbewerb abschneiden wird.

ITS: Viele Köche verderben den Brei. An GAIA-X arbeiten derzeit etwa 300 Unternehmen mit. Wie hoch schätzen Sie die Gefahr ein, dass das Projekt an internen Reibereien erstickt?

Interne Reibung ist immer dann gut, wenn daraus bessere Lösungen resultieren. In der Tat besteht die Gefahr, dass die Anzahl der Akteure, deren unterschiedliche Interessenlage und natürlich auch die Komplexität eines solchen Unterfangens den Innovationsprozess sowie die Markteinführung bremsen. Bei dem Projekt wird es maßgeblich darauf ankommen, sich auf sinnvolle, verbindliche Standards zu einigen, die sich im Markt differenzieren, eine hohe Sicherheit gewährleisten und zeitgleich nicht die realistische Umsetzbarkeit gefährden. Zudem sollte GAIA-X auch noch in puncto Funktionalität und Kosten attraktiv sein.

ITS: Warum ist eine europäische Cloud-Variante für die deutsche (und europäische) Unternehmenslandschaft so wichtig?

Deutschland hat hinsichtlich Digitalisierung noch Nachholbedarf. Das ist im Cloud-Umfeld nicht anders: Im globalen Vergleich agiert die lokale Wirtschaft hier noch langsamer. Des Weiteren ist der deutsche Markt teils stark reguliert, beispielsweise im Hinblick auf Datenschutz. Eine europäische Cloud könnte hier Abhilfe und Rechtssicherheit sowie gleichzeitig eine Alternative zu den etablierten Anbietern schaffen. Damit hätten deutsche Unternehmen eine echte Wahl, welche Daten und Prozesse bei den global agierenden Anbietern verarbeitet und welche, aufgrund ihrer Kritikalität für den Firmenerfolg, eher aus Abwägungsgründen in einer europäischen Cloud betrieben werden. Damit steigt nicht zuletzt die politische Souveränität. Ein Projekt wie GAIA-X sichert nicht nur die zukünftige Handlungsfähigkeit, sondern kann auch Stein des Anstoßes für weitere europäische Initiativen werden.

ITS: Was können europäische und deutsche Unternehmen mit GAIA-X nun besser umsetzen als zuvor?

In der aktuellen Konzeptionsphase lässt sich das nur schwer beurteilen. Im besten Falle stellt GAIA-X eine Alternative zu etablierten Plattformen dar. Es kommt meiner Meinung nach auf die Positionierung und Differenzierung im Markt an – beispielsweise, ob man auf einzelne Industrien zugeschnittene Mehrwehrtsdienstleistungen anbieten kann.

Thomas Schumacher,
Leiter IT-Security bei Accenture (Foto: Accenture)

FRAGEN ZU GAIA-X AN PROFESSOR NORBERT POHLMANN – IF(IS)

ITS: Wie wichtig sind Public Clouds für die deutsche Wirtschaft?

Leistungsfähige digitale Infrastrukturen sind die Basis des Wohlstands unserer Gesellschaft. Künstliche Intelligenz, vernetzte Industrieproduktion (Smart Industrie), autonomes Fahren, Telemedizin oder digitale Verwaltung erzeugen gewaltige Datenmengen. Um diese Daten auszutauschen und zu verarbeiten, braucht es sehr viel Rechenleistung und Speicherplatz. Die nötige Kapazität liefern Cloud-Angebote weltweit verteilter und leistungsfähiger Rechenzentren. Im Nahbereich werden große Datenmengen, wie bei Industrie 4.0, in der Zukunft zunehmend durch Edge-Computing ergänzt, wenn die Daten vor Ort sehr schnell verarbeitet werden müssen.

ITS: Wie ist die Situation in Sachen Cloud heute und wie soll GAIA-X da hineinspielen?

Der Cloud-Computing-Markt wird weltweit von wenigen Plattformanbietern aus den USA und China beherrscht, die damit auch die Regeln, zum Beispiel für die Nutzung und einen Wechsel des Anbieters, in Europa bestimmen. Mit einem Marktanteil von über 75 Prozent und sehr hohen Budgets für Entwicklung und Forschung stellen die Hyperscaler heute das Rückgrat für die digitalisierte Weltwirtschaft.

Da die großen Hyperscaler auch der nationalen Gesetzgebung an ihrem Stammsitz unterliegen, fehlen international vertrauenswürdige Standards zum Schutz von Daten. Aber auch eskalierende Handelskonflikte und der Wettbewerb politischer Systeme machen diese Abhängigkeit zum strategischen Nachteil für die Europäische Union. Laut einer aktuellen Studie von HP glaubt die Hälfte der deutschen Entscheider, dass die Abhängigkeit der Wirtschaft von globalen Cloud-Plattformen größer geworden ist. Für 85 Prozent der deutschen Manager ist digitale Souveränität ein wichtiges Ziel ihrer Digitalisierungsstrategie.

GAIA-X ist ein Projekt zum Aufbau einer leistungs- und wettbewerbsfähigen, sicheren und vertrauenswürdigen Cloud- und Edge-Infrastruktur für Europa. Es soll Cloud- und Edge-Dienste europäischer Anbieter zu einem Ökosystem mit gemeinsamen Regeln, Standards und Technologien vereinen.

ITS: Welches sind die wichtigsten Ziele von GAIA-X?

Die Initiatoren wollen dem undurchsichtigen Dickicht an Einzelprojekten, Anbietern, Technologien und Rechtsvorschriften ein transparentes und rechtssicheres Daten-Ökosystem für Europa entgegenstellen. Vor allem für Unternehmen aus dem Mittelstand soll es künftig einfacher sein, unterschiedliche Services zu kombinieren und Dienstleister nach Bedarf zu wechseln. Drei der wichtigsten konkreten Ziele sind vor diesem Hintergrund:

1. Datensouveränität
Europas Unternehmen und Organisationen müssen immer eine Wahl haben, wo und bei wem sie Daten speichern und verarbeiten und woher sie digitale Dienste beziehen. GAIA-X will Monopole und somit eine einseitige Abhängigkeit Europas von großen außereuropäischen Plattform-Anbietern verhindern oder zumindest reduzieren. Besonders der Mittelstand soll von Markttransparenz und einem einfachen Zugang zu maßgeschneiderten Angeboten profitieren.

2. Datenverfügbarkeit
Wenn Daten zur wichtigsten Ressource werden, brauchen Europas Unternehmen, Behörden, Institutionen sowie Bürgerinnen und Bürger Garantien, um Daten vertrauensvoll, sicher und transparent auszutauschen. Und das auch dann, wenn diese Daten durch viele Hände, Systeme und Wertschöpfungsstufen gehen.

3. Innovation
GAIA-X soll Innovation in Europa fördern und die datenbasierte Wirtschaft stärken. Die unter GAIA-X versammelten Cloud- und Edge-Dienste unterstützen digitale Geschäftsmodelle aus Europa, die auf dieser Infrastruktur weltweit wettbewerbsfähig wachsen.

ITS: Welchen Mehrwert kann GAIA-X Unternehmen bieten – speziell auch im Vergleich zu den etablierten Anbietern, wie Amazon, Google und Microsoft?

Die wesentlichen Punkte sind hier sicher föderierte Dienste und mehr Cybersicherheit. Föderierte Dienste bieten einen Mehrwert, wenn sie gemeinsame Standards für Transparenz und Interoperabilität beinhalten. GAIA-X leistet hierbei einen wertvollen Beitrag und bietet den Rahmen für Anbieter von Rechenzentren, Cloud-Lösungen, High Performance Computing (HPC) und sektorspezifischen Cloud- und Edge-Systemen, um sich aufeinander abzustimmen.

Die Konzeption folgt dabei den Prinzipien von Security by Design und Privacy by Design, um höchste Sicherheitsanforderungen und den Schutz der Privatsphäre zu gewährleisten. Dazu gehört beispielsweise die Implementierung eines sicheren und föderierten Identitätsmanagements sowie die Schaffung von Vertrauensmechanismen für die Cloud-Dienste. Weitere Schwerpunkte sind die Entwicklung von souveränen Daten-Services, welche die Identität von Quelle und Empfänger der Daten gewährleisten und die Zugriffs- und Nutzungsrechte für die Daten sicherstellen, sowie die Bereitstellung eines nutzerfreundlichen Zugangs zu verfügbaren Anbietern, Knoten und Diensten. Die notwendigen Informationen werden durch den föderierten Katalog bereitgestellt. Weitere wichtige Punkte sind die Integration von bestehenden Standards, um die Interoperabilität und Portabilität zwischen Infrastruktur, Anwendungen und Daten sicherzustellen, sowie die Einführung von Compliance-Regeln und Zertifizierungs- sowie Akkreditierungsangeboten.

ITS: Wie bewerten Sie GAIA-X grundsätzlich?

GAIA-X ist eine sehr gute Initiative, die für souveräne digitale Infrastrukturen und Cloud-Dienste sorgt, auf deren Basis sich in Europa Gestaltungsspielraum und Zukunftsfähigkeit entwickelt. Damit werden Cloud-Dienste mit unserem Wertesystem verknüpft, sicher und vertrauenswürdig, um souverän und nach unseren Regeln neue Ökosysteme aufzubauen, die für das Wohl unsere Gesellschaft immer wichtiger werden.

Norbert Pohlmann,
Professor für Informationssicherheit 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.

IT-Sicherheitsgesetz 2.0: Neuregelungen für KRITIS-Betreiber

MIT ISMS UND NOTFALLPLANUNG KRITISCHE INFRASTRUKTUREN SICHERN

Der Großteil der bekannten IT-Sicherheitslücken ist seit mindestens einem Jahr bekannt. Dies belegen Studien wie der aktuelle Data Breach Investigations Report von Verizon, demzufolge sogar 99,9 Prozent aller ausgenutzten Schwachstellen schon seit zwölf Monaten oder länger bestehen. Wer Schaden anrichten möchte, hat ein leichtes Spiel. Bedrohlich wird es da, wo öffentliche Einrichtungen betroffen sind, wie etwa Krankenhäuser, Energieversorger, Staat und Verwaltung oder Transportunternehmen. Die Gefahr durch Cyberangriffe auf die öffentliche Infrastruktur nimmt seit Jahren zu und mögliche Folgeszenarien sind düster. Aus diesem Grund befördert die Bundesregierung nun das bereits seit 2015 geltende IT-Sicherheitsgesetz überarbeitet auf die Zielgerade des Gesetzgebungsprozesses. Die Einführung und Umsetzung eines unternehmensweiten IT-Sicherheitskonzepts ist langwierig und ressourcenintensiv. KRITIS-Betreiber sollten es deswegen bereits jetzt auf den Weg bringen.

Ziel des Zweiten Gesetzes zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-Sicherheitsgesetzes 2.0 oder IT-SiG 2.0) ist kein geringeres, als die IT-Infrastruktur in Deutschland zu den sichersten der Welt zu machen. So sind Betreiber Kritischer Infrastrukturen (KRITIS) bereits heute dazu verpflichtet, ein Mindestmaß an IT-Sicherheit zu gewährleisten und ihre IT-Systeme am Stand der Technik auszurichten. Durch Branchenspezifische Sicherheitsstandards (B3S) werden die Anforderungen dafür definiert. Dass KRITIS-Betreiber diese erfüllen, müssen sie alle zwei Jahre mithilfe entsprechender Formulare gegenüber dem Bundesamt für Sicherheit in der Informationstechnik (BSI) nachweisen. Außerdem umfasst ein Mindestmaß an IT-Sicherheit die Benennung eines Sicherheitsbeauftragten sowie die unverzügliche Meldung von Störungen an das BSI. Die Sektoren der Kritischen Infrastrukturen schließen Energie, Gesundheit, Staat und Verwaltung, Ernährung, Transport und Verkehr, Finanz- und Versicherungswesen, Informationstechnik und Telekommunikation, Medien und Kultur sowie die Wasserversorgung ein. Neu hinzu kommt mit dem IT-SiG 2.0 der Bereich der Abfallwirtschaft. Außerdem wird die neue Kategorie der „Infrastrukturen im besonderen öffentlichen Interesse“ eingeführt, welche die Rüstungsindustrie, die Bereiche Kultur und Medien sowie Anlagen und Systeme umfassen, deren Beeinträchtigung zu Schäden bei Unternehmen aus dem Bereich der Prime Standards der Frankfurter Börse führen würden. Diese Kategorie zählt zwar nicht zu den Kritischen Infrastrukturen, wird aber hinsichtlich der Verpflichtungen so behandelt.

NEUE REGELN IM UMFELD VON KRITIS

Im Wesentlichen müssen sich KRITIS-Betreiber auf vier Neuerungen einstellen: Eine Angriffserkennung muss eingeführt und der Einsatz vertrauenswürdiger KRITIS-Komponenten nachgewiesen werden. Außerdem sind eine drastische Erhöhung der Bußgelder sowie die Ausdehnung der Befugnisse des BSI zu erwarten.

Optimierte Angriffserkennung

KRITIS-Betreiber müssen mit Inkrafttreten des IT-SiG 2.0 eine Angriffserkennung umsetzen und damit sicherstellen, dass sie neben einer Antiviren-Lösung und einer Firewall zusätzlich ein System implementieren, welches sie automatisiert und in Echtzeit über Sicherheitsausfälle informiert. Für KRITIS-Betreiber kommt dazu etwa ein IDS/IPS (Intrusion Detection/Prevention System) oder ein Security Information und Event Management (SIEM) infrage. Dabei wird davon ausgegangen, dass relevante Daten über die Sicherheit einer Firma an verschiedenen Stellen anfallen. Es ist jedoch ratsam, alle Daten zentral zu sammeln, da so vom üblichen Schema abweichende Muster besser zu erkennen sind.

Regeln für Hersteller von IT-Produkten

Neben den Betreibern Kritischer Infrastrukturen müssen zukünftig auch Zulieferer und Hersteller von KRITIS-Kernkomponenten die Standards des BSI erfüllen und dies nachweisen. Auf diese Weise wird sichergestellt, dass die gesamte Zuliefererkette der KRITIS-Komponenten die geforderten Sicherheitskriterien erfüllt.

Erhöhung von Bußgeldern

Entsprechend der EU-DS-GVO wird das bislang maximale Bußgeld von 100.000 Euro auf 20.000.000 Euro oder vier Prozent des weltweiten Unternehmensumsatzes erhöht. Außerdem wird die Liste der Tatbestände erweitert, bei denen ein Bußgeld verhängt werden kann.

ENTSORGUNG ALS NEUER KRITIS-BEREICH

Fällt die Entsorgung über einen längeren Zeitraum aus, zieht dies unter anderem schwerwiegende gesundheitliche Folgen der Bevölkerung nach sich. Deswegen werden Entsorger mit Einführung des IT-SiG 2.0 in die Liste der Sektoren mit Kritischer Infrastruktur aufgenommen. Was müssen also Entsorger mit Inkrafttreten des IT-SiG 2.0 tun?

- ISMS mit Notfallplanung erstellen
- IT-Sicherheitsbeauftragten benennen
- Stand der Technik in der IT regelmäßig nachweisen
- IT-Störungen unverzüglich dem BSI melden

Erweiterte Befugnisse des BSI

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) kann in Zukunft bereits im Verdachtsfall eines unzureichenden Schutzes öffentlicher IT-Systeme von KRITIS-Betreibern eigenständig und ohne vorherige Ankündigung Maßnahmen zur Aufspürung von Sicherheitslücken umsetzen. Wie ein Angreifer kann das BSI dann in die möglicherweise bedrohten Systeme eindringen, um die Betreiber über etwaige Gefahren zu informieren.

EIN ISMS SICHERT KRITISCHE PROZESSE

Unter Berücksichtigung des jeweiligen unternehmerischen Kontextes kann selbst die minimale Umsetzung der im IT-SiG 2.0 gestellten Anforderungen eine enorme wirtschaftliche Mehrbelastung für Betreiber bedeuten. Eine ressourcenschonende Variante ist es, externe Dienstleister mit der notwendigen Erfahrung und dem technischen Know-how zu beauftragen. Welche Schritte sollten KRITIS-Betreiber also im Vorfeld des IT-SiG 2.0 gehen? Zunächst sollte sich jeder Betreiber die folgenden Fragen stellen:

- Wie ist das Unternehmen im Bereich der IT-Sicherheit aufgestellt?
- Sind die kritischen und systemrelevanten Prozesse bezüglich der neuen Anforderungen ausreichend abgesichert?
- Was wird zusätzlich benötigt?
- Mit welchen Maßnahmen ist das geforderte Sicherheitsniveau zu erreichen?

Auch wenn bisher noch nicht alle KRITIS-Betreiber die strengen Auflagen des BSI erfüllen müssen, ist es grundsätzlich sinnvoll, in die IT-Sicherheit zu investieren. Dabei amortisieren sich die anfallenden Kosten schnell, bedenkt man die wirtschaftlichen Schäden, welche ein kritischer Vorfall nach sich ziehen würde. Zur Absicherung ihrer kritischen und systemrelevanten Prozesse sollten KRITIS-Betreiber deswegen frühzeitig ein Information Security Management System (ISMS) sowie eine Notfallplanung einführen und diese fortlaufend optimieren.

PLANEN, UMSETZEN, PRÜFEN, HANDELN

Die Einführung eines ISMS erfolgt nach der Plan-Do-Check-Act-Methode (PDCA). Ein PDCA-Zyklus ist ein wirksames Vorgehen zur Optimierung von Prozessen und wird in vielen Unternehmensbereichen regelmäßig angewendet. Zur Optimierung der IT-Sicherheit wird im Rahmen von Workshops und anhand einer unternehmensspezifischen Gewichtung der Säulen Vertraulichkeit, Integrität und Verfügbarkeit zunächst definiert, welche Sicherheitsniveaus erreicht werden sollen. Anschließend werden Szenarien durchgespielt, die deren Erreichen verhindern könnten. Im Anschluss werden Maßnahmen zusammengestellt, mit denen etwaige Risiken vermieden werden können. Schließlich müssen Maßstäbe zur Validierung der Methodenwirksamkeit festgelegt werden. Ein zentraler Aspekt bei allen Schritten ist der Mensch. Deswegen muss das Thema Social Engineering, also die Berücksichtigung der Mitarbeiter als potenzielle Opfer von Betrugsvorgängen, bei der Einführung eines ISMS eine zentrale Rolle spielen. Dabei müssen im ISMS klare Zuständigkeitsbereiche festgelegt werden, sodass im Ernstfall jeder weiß, was zu tun ist. Erst ganz am Ende dieser Planungsaufgaben steht die Umsetzung der Maßnahmen.

TYPISCHE NOTFALL-SZENARIEN DEFINIEREN

Neben einem ISMS ist es zur Erfüllung der Anforderungen durch das IT-SiG 2.0 für KRITIS-Betreiber wichtig, eine Notfallplanung auf den Weg zu bringen. Sie definiert kritische Ereignisse und Prozesse und legt fest, welche Maßnahmen wann und in welcher Reihenfolge durch wen ergriffen werden müssen. Typische Notfälle sind beispielsweise der Ausfall von IT-Systemen, Hacker-Angriffe, Personalausfall, der Ausfall von Gebäuden und Dienstleistern oder höhere Gewalt und Naturkatastrophen. Als konkretes Ausfallszenario findet sich in vielen Notfallhandbüchern ein Stromausfall, der einen kritischen Serverausfall zur Folge hat. Zur Notfallplanung müssen sich KRITIS-Betreiber bei einem solchen Vorfall eine Reihe von Fragen stellen: Ist ein Notstromaggregat vorhanden? Soll der Server in einem externen Rechenzentrum wieder hochgefahren werden? Gibt es Server an unterschiedlichen Standorten, die bei Ausfall einspringen können? Welche Ausfallzeit können unsere Prozesse verkraften? Was hat den Stromausfall hervorgerufen? Wer ist zuständig für welchen Prozess? Darauf aufbauend können dann konkrete Maßnahmen und Zuständigkeiten festgelegt werden. Analog ist das Vorgehen für weitere Szenarien, die in der Notfallplanung definiert werden.

MIT IT-SICHERHEITSKONZEPT CYBERANGRIFFEN ZUVORKOMMEN

Die Verabschiedung des IT-SiG 2.0 ist zeitlich noch nicht absehbar und auch dann haben KRITIS-Betreiber eine Übergangsfrist, bis alle Anforderungen umgesetzt sein müssen. Die zeitlichen und personellen Ressourcen bei der Einführung eines IT-Sicherheitskonzepts sollten Betreiber Kritischer Infrastrukturen jedoch nicht unterschätzen. Dabei ist ein IT-Sicherheitskonzept mit zeitlichem Vorlauf wirksamer als eines, das in letzter Minute auf den Weg gebracht wird. KRITIS-Betreiber müssen neben allen gesetzlichen Vorgaben vor allem aber in IT-Sicherheit investieren, bevor ein zerstörerischer Cyberangriff sie dazu zwingt und ihre Infrastruktur mit verheerenden Folgen lahmlegt. Und auch wenn der Referentenentwurf bisher noch zentrale Fragen offenlässt, verdeutlicht er einmal mehr die Bedeutung der IT-Sicherheit. ■

MARCO GRÄF,
Teamleiter Vertrieb und Kommunikationsinfrastruktur, Q-SOFT GmbH

LEBEN MIT DER DSGVO

IT-SICHERHEIT ALS KONSTANTER FAKTOR IM UNTERNEHMENSALLTAG

Kingston Technology gibt Tipps zur konstanten DS-GVO-Konformität

„Die unternehmenseigene IT-Infrastruktur ist nur so stark wie ihr schwächstes Element“

CHRISTIAN MARHÖFER,
Regional Director DACH bei Kingston

Seit mehr als zwei Jahren ist die Datenschutz-Grundverordnung (DS-GVO) in Kraft. Inzwischen ist viel passiert. Die Anforderungen an IT-Sicherheitssysteme und an den Datenschutz verändern sich permanent. Die Richtlinien der DS-GVO zu erfüllen, ist daher keine einmalige Aufgabe. Unternehmen müssen die sicherheitsrelevanten Themen vielmehr ständig neu bewerten.

Kingston Technology, unabhängiger Weltmarktführer in Sachen Speicherlösungen, hat vier Tipps ausgearbeitet, um die Konformität auch bei neuen Entwicklungen beizubehalten.

ARBEITSUMGEBUNG AUCH IM REMOTE WORKING ABSICHERN

Eine einzige Person reicht aus, um die Datenschutzbemühungen zum Scheitern zu bringen. In Zeiten von Remote Working müssen Unternehmen daher dafür sorgen, dass ihre Angestellten überall effektiv und produktiv arbeiten können, ohne gegen die Datenschutzbestimmungen zu verstoßen. Mögliche Tools hierfür sind:

- Die Zwei-Faktor-Authentifizierung schützt Netzwerksgrenzen einfach und effizient. In der Regel wird der Benutzer aufgefordert, ein Passwort auf seinem Laptop einzugeben. War die Eingabe erfolgreich, erhält er einen Code auf sein Mobiltelefon, dann wird der Zugang gewährt.
- VPNs eignen sich für den Zugriff auf Geschäftsdaten über öffentliche WLAN-Netzwerke. Kommt beim mobilen Arbeiten allerdings nur eine VPN-Sicherung ohne Hardwareverschlüsselung zum Einsatz, gilt für die lokal gespeicherten Daten kein zusätzlicher Schutz.
- Verschlüsselte SSDs und USBs sind heute nicht mehr viel teurer als die unverschlüsselten Versionen, bieten aber einen entscheidenden Vorteil: Wird das Gerät gestohlen, sind die verschlüsselten Daten vor ungewollten Zugriffen sicher. Je nach Lösung lassen sie sich sogar aus der Ferne zerstören.

- Der eigene Server vor Ort bietet volle Kontrolle über den eigenen Serverbestand. Praktisch sind auch hybride Serverlösungen. Hier speichern Unternehmen, zum Beispiel in Zusammenarbeit mit Managed Service Providern, nur die nicht-sensiblen Daten in der Cloud, persönliche Daten bleiben vor Ort.

EFFEKTIVE SCHULUNG VON MITARBEITERN

Wer gut informiert ist, wird weniger wahrscheinlich gegen Datenschutzvorgaben verstoßen. Auch bei einem Datenverlust ist es von Vorteil, Mitarbeiterschulungen nachweisen zu können. Online-Schulungen und Multiple-Choice-Tests mit einfachen Fragen sind zeitsparend, gehen jedoch nicht weit genug. Man muss den Mitarbeitern verdeutlichen, dass immer eine Person hinter den Daten steht, die sie weitergeben, und dass es letztlich um den Schutz der eigenen Privatsphäre geht. Hochwertige Schulungen können echte Verhaltensänderungen herbeiführen.

VERANTWORTLICHKEITEN RICHTIG VERTEILEN

Bei Angestellten, die stark ausgelastet sind oder weitgehend autonom arbeiten, ist ein Regelverstoß schnell passiert. Bei Stress geraten die Vorschriften leicht aus dem Blickfeld. Zwar gibt es mittlerweile Datenschutzbeauftragte in den Unternehmen, oft handelt es sich dabei jedoch um einen technikaffinen Mitarbeiter, der dem Datenschutz neben seiner Arbeit nachkommt. Aber selbst für einen Vollzeitbeauftragten ergeben sich immer wieder Themen, die eine zweite Meinung erfordern. Die Zusammenarbeit mit einer externen Beratungsfirma kann daher sinnvoll sein.

FLAGGEN NICHT BENÖTIGTER DATEN

Laut DS-GVO dürfen einige personenbezogene Daten nicht länger als sieben Jahre aufgehoben werden. Smarte Unternehmen setzen ebenfalls auf das gezielte Reduzieren von Daten – getreu der Devise: „If you don't need it, don't collect it". Damit senken sie die Risiken und erhöhen die Effizienz. So arbeiten Datenbanken besser und kostengünstiger, wenn keine veralteten Daten darin gespeichert sind. Hilfreich sind Tools, mit denen die Datenbank einen Alert an die IT senden kann, der auf das Ablaufdatum bestimmter Informationen hinweist. Und: Die Säuberung von nicht benötigten Daten lohnt sich auch für physische Daten. Weniger Prints und Scans bedeuten weniger Angriffsflächen.

„Die unternehmenseigene IT-Infrastruktur ist nur so stark wie ihr schwächstes Element", sagt Christian Marhöfer, Regional Director DACH bei Kingston. „Es ist erforderlich, Daten überall zu schützen – beim Transport, beim Austausch, bei der Nutzung sowie bei der Ablage. Entscheidend ist ein umfassender Sicherheits-, Wiederherstellungs- und Datenlöschplan. Und letztendlich kostet der Aufbau einer sicheren Infrastruktur weit weniger als mögliche Strafen bei einem Verstoß gegen die DS-GVO-Vorschriften." ■

Mehr dazu hier

Integrierte Software für Unternehmen

INTELLIGENTES FRÜHWARNSYSTEM AUS DER BUCHHALTUNG

Innovative Finanzbuchhaltungssoftware übernimmt inzwischen mehr als nur reine Buchhaltungsaufgaben. Sie kann gezielt zu Controllingzwecken eingesetzt werden, fungiert als sicherer Alarmradar und zeigt relevante Zukunftsszenarien auf.

Noch sind die wirtschaftlichen Folgen der Corona-Krise nicht vollständig absehbar. Ins Auge fällt allerdings schon jetzt, dass eine zunehmende Anzahl von Unternehmen wirtschaftlich unter immer höherem Druck steht. Laut dem Monatsberichts des Bundesministeriums für Wirtschaft und Energie wird die gesamtwirtschaftliche Leistung im Durchschnitt des zweiten Quartals noch einmal sehr viel stärker zurückgehen als dies bereits mit minus 2,2 Prozent im ersten Quartal erfolgte. Der weitere Erholungsprozess im zweiten Halbjahr und auch danach wird schleppend erfolgen und sich länger hinziehen.

Daher rücken Fragen wie beispielsweise „Wie hat sich mein Unternehmen im Vergleich zum Vorjahr entwickelt?“ oder „Welche Produktsegmente sind jetzt besonders lukrativ?“ in den Mittelpunkt. Sie sind ausschlaggebend, um die entscheidenden Weichen für die kommenden Monate erfolgreich stellen zu können. Inzwischen nimmt das Thema Controlling eine immer größere Bedeutung ein.

Eine intelligente Finanzbuchhaltungssoftware (Fibu) ist für Unternehmen ein einfach und effizient einsetzbares, strategisches Steuerungsmittel, insbesondere für kleine und mittlere Betriebe. Sie lässt sich gezielt als Controllinginstrument nutzen — und als Frühwarnsystem einsetzen. So können verlässliche Daten zu Umsatz und Kosten zur Verfügung gestellt werden, um eine exakte betriebswirtschaftliche Planung und Analyse schnell und ohne großen Aufwand durchführen zu können.

FLEXIBLES SCHNITTSTELLENKONZEPT ERMÖGLICHT NAHTLOSE INTEGRATION

Ausschlaggebend für den Einsatz einer Fibu-Software als Controllinginstrument ist ihre Integrationsfähigkeit. Schließlich ist die Fibu-Software keine isolierte Insellösung, sondern bezieht ihre vielfältigen Daten und Zahlen mittels Schnittstellen aus den anderen Softwareprogrammen des Unternehmens wie beispielsweise Lohn und Gehalt. So können ein sicherer Transfer und die effiziente Weiterverarbeitung wichtiger Daten garantiert werden.

CONTROLLING MIT BLICK IN DIE ZUKUNFT

Die Fibu-Software sammelt nicht nur die wichtigsten Kennzahlen, sondern stellt sie einfach und vor allem auch schnell zur Verfügung. Komplexe Abfragen können Nutzer unkompliziert durchführen. Beliebige Auswertungs- und Vergleichszeiträume lassen sich bequem aufrufen. Ferner bietet die Fibu-Lösung besonders detaillierte Analysen sowie eine übersichtliche Darstellung von Gewinn- und Verlust-Rechnungen. Betriebswirtschaftliche Auswertungen für einen

schnellen Überblick lassen sich mit ihr flexibel definieren sowie einfach und schnell generieren. Der Aufbau kann manuell festgelegt werden und so lassen sich die jeweiligen Konten individuell bequem und übersichtlich zuordnen.

Auf Knopfdruck listet die Software alle Standardgrößen, wie Umsatz, sonstige Erlöse, Aufwendungen, Abschreibungen oder Zinsen, benutzerfreundlich auf. Auswertungs- und Vergleichszeiträume für die Umsatzstatistik sind zudem frei bestimmbar. Auch grafisch lassen sich die Ergebnisse umsetzen: So kann mithilfe einer Zeitachse die Veränderung der Zahlen umgehend sichtbar gemacht werden.

Eine besonders nützliche Funktion stellt die ergänzende Verknüpfung mit Microsoft Excel dar. Mit einem Klick holt sich das Microsoft-Office-Programm jederzeit die Zahlen aus der Fibu-Software — und zwar tagesgenau. Die Auswertung wird individuell nach den eigenen Betriebsanforderungen einmal in Excel erstellt. Danach sind die aktuellen Werte per Klick abrufbar. Fehler durch manuelles Erfassen der Daten und langwierige Abstimmungsprozesse entfallen. Alle Auswertungen lassen sich schnell in ein PDF umwandeln und via E-Mail versenden. Ein zeitsparender Vorteil für die Übermittlung an externe Dienstleister wie beispielsweise den Steuerberater.

KURZE CHECKLISTE FÜR DIE AUSWAHL DER FIBU-SOFTWARE:

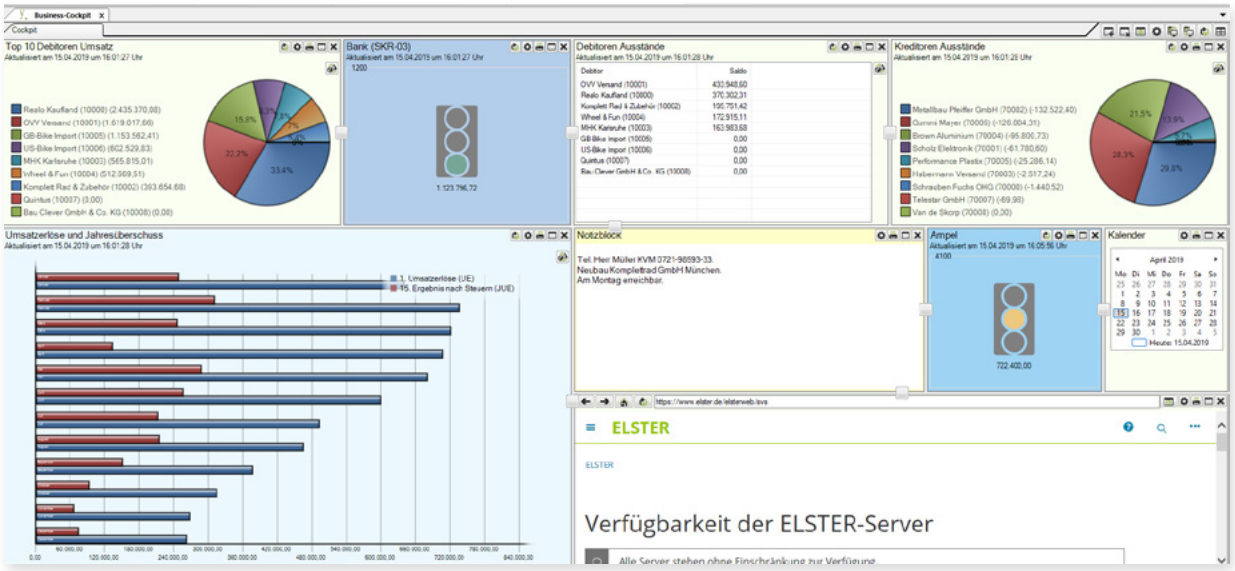
- Ist eine DATEV-Schnittstelle für den Import und Export der Daten für den Steuerberater vorhanden? Sie sollte zum Standard gehören.
- Ist ein flexibles Schnittstellenkonzept vorhanden? Es lässt die Integration in andere Branchensoftware zu.
- Stehen intelligente Importfunktionen aus gängigen Microsoft-Programmen zur Verfügung? So können relevante Zahlen für das Controlling weiterverarbeitet werden.
- Sind Inkasso-Schnittstellen bereits integriert? Das erleichtert das Mahnwesen.
- Lässt sich die Software auch sicher und einfach im Homeoffice nutzen? Können sämtliche Funktionen eingesetzt werden?

Neben den Auswertungen vergangener Perioden bildet die Softwarelösung auch die Zukunft ab. Ausgehend vom aktuellen Bankguthaben und dem Offenen-Posten-Bestand mit Zahlungszielen besteht die Möglichkeit, wochen- oder monatsgenau die verfügbare Liquidität des Betriebs zu berechnen. Schließlich ist es überlebenswichtig, laufend zu überprüfen, ob ausreichend liquide Mittel vorhanden sind. Nur so lässt sich eine drohende Zahlungsunfähigkeit, die schließlich sogar zur Insolvenz führen kann, bereits im Ansatz erkennen und im besten Fall gänzlich vermeiden.

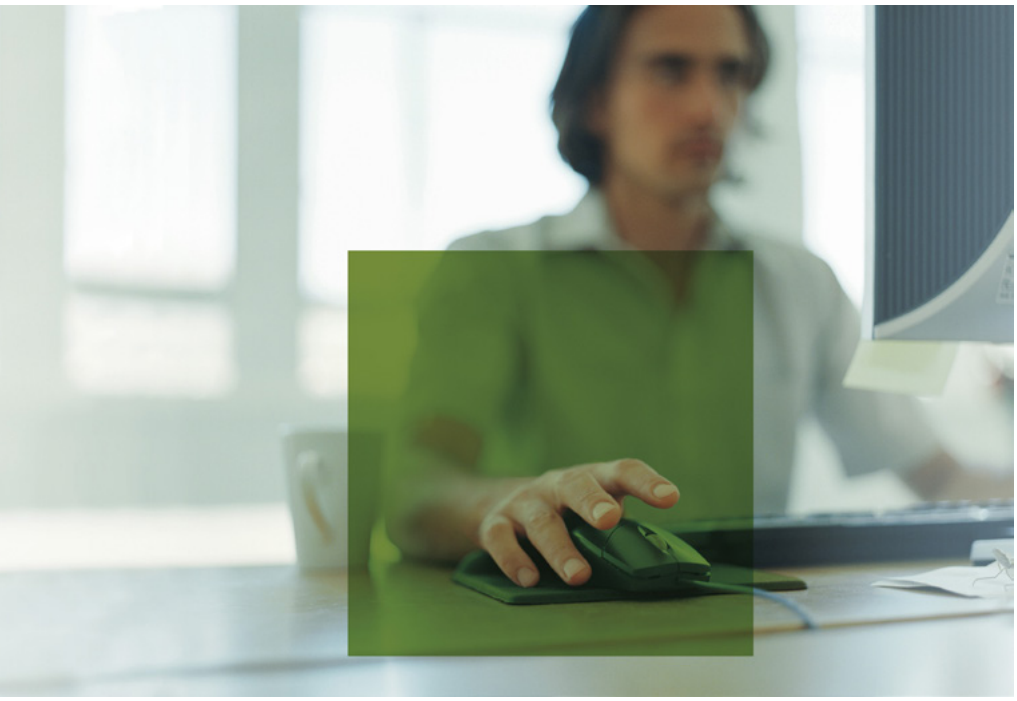
ZEITSPARENDER BUCHUNGSALLTAG

Nicht zu vernachlässigen ist natürlich auch das alltägliche Buchen. Um zeitsparend zu arbeiten, hilft ein übersichtlicher Aufbau der Software: Dank moderner und flexibler Oberflächengestaltung lassen sich Funktionsmenüs und Icon-Leisten individuell konfigurieren, sodass jeder Nutzer die Oberfläche entsprechend seiner benötigten Funktionen einrichten kann.

Automatische Vorlagen für die alltäglichen Geschäftsvorfälle wie individuell angepasste Buchungsschablonen helfen, den Zeitaufwand zu reduzieren. So gestaltet sich die Kontensuche sehr einfach. Mit nur einem Klick ist der passen-



Controlling leicht gemacht: Die grafische Übersicht der syska EURO FIBU macht die Ergebnisse auf einen Blick vergleichbar.



Mit nur einem Klick: Finanzbuchhaltungssoftware einfach und effizient als strategisches Steuerungsmittel einsetzen. (Foto: syska)

de Kontensatz schnell und bequem aufgerufen. Dank einer übersichtlichen Offenen-Posten-Liste – gestaffelt nach einzelnen Mahnstufen – lässt sich auch erkennen, welcher Kostenträger an die Zahlung erinnert werden muss.

Ebenso lassen sich über eine konfipay-Integration beispielsweise im Online-Banking beliebig viele Konten von verschiedenen Geldinstituten einbinden. Darüber hinaus sorgt die Übertragung von Überweisungen an den Webservice mit nur einem Klick oder die Unabhängigkeit von Banking-Software-Updates für deutlich höheren Komfort. Auch im Hinblick auf die Datensicherheit ein klares Plus, denn sensible Zahlungsverkehrsdaten werden nicht in Clearing-Dateien zwischengespeichert.

VEREINFACHTE AUFZEICHNUNGSPFLICHTEN

Intelligente Finanzbuchhaltungssoftware vereinfacht mit innovativen Modulen auch gesetzlich geforderte Aufzeichnungspflichten wie beispielsweise die Verfahrensdokumentation. Sie ist für Unternehmen verpflichtend, und der Betriebsprüfer kann sie jederzeit anfordern. Sie belegt, dass der Betrieb die Anforderungen des Handelsgesetzbuches (HGB) und der Abgabenordnung (AO) bei der täglichen Buchhaltung einhält. So unterstützt die Software Musterdaten und -texte in einer geführten Erfassungslogik. Die Anwendung bezieht alle Mitarbeiter in den Workflow mit ein. Das Ergebnis: Die Dokumentation in der Buchhaltung wird vereinfacht, indem sie über Jahre hinweg mitwächst und die Eingaben nachverfolgt werden können. Aufzeichnungen zu bestimmten Prozessen können regelmäßig auf Aktualität überprüft werden. Zur Aktualisierung bereits erfasster Vorgänge steht eine Wiedervorlage zur Verfügung.

Ein weiterer positiver und zeitsparender Effekt ist, dass auch alle datenschutzrelevanten Informationen strukturiert erfasst werden. Über die geführte Abarbeitung entsteht ein professioneller Datenschutzbericht. Das ist ein nicht zu unterschätzender Vorteil insbesondere für Datenschutzbeauftragte, die die Erstellung des jährlichen Datenschutzberichtes verantworten. Schließlich ist das Zusammentragen und Aufzeichnen von Informationen ein herausfordernder Prozess, in den meist mehrere Personen aus diversen Bereichen involviert sind.

FLEXIBLE LÖSUNG AUCH FÜR DAS HOMEOFFICE

Besonders hilfreich erweist sich in diesen Tagen eine intelligente Fibu-Software, die auch außerhalb des Unternehmens genauso flexibel nutzbar ist und mit der sich unkompliziert im Homeoffice arbeiten lässt – und zwar mit der gewohnten Sicherheit und dem vollen Umfang ihrer Funktionen. Konkret bedeutet dies, dass auch zu Hause der sichere Umgang mit den hochsensiblen Daten garantiert werden muss. Daher sollte der Zugriff auf die Fibu-Software über eine VPN-Remote-Desktop-Verbindung erfolgen.

FIT FÜR DIE ZUKUNFT

Regelmäßige Software-Aktualisierungen sind natürlich Pflicht. Insbesondere die mittlerweile immer stärker verbreiteten elektronischen Rechnungen sollten verarbeitet werden können. Eine intelligente Software unterstützt ihren Import (Bilddateien, PDFs und ZUGFeRD 2.0) und kann aus diesen Belegen vollautomatisch Buchungen erzeugen und diese miteinander verknüpfen. So lässt sich später sehr einfach, zum Beispiel aus dem Buchungsjournal, die Rechnung zu einer Buchung anzeigen. Dies senkt den Arbeitsaufwand sowie die Kosten für die Rechnungserfassung und ermöglicht dem Anwender so, den größtmöglichen Nutzen aus der elektronischen Rechnung zu ziehen. Zudem reduzieren sich Nachkontrollen auf ein Minimum.

Dank ihrer ausgefeilten Controlling- und Reportinginstrumente liefert professionelle Finanzbuchhaltungssoftware die wesentlichen Entscheidungsgrundlagen, um das eigene Unternehmen tagtäglich auch in herausfordernden Zeiten erfolgreich zu leiten und in die Zukunft zu führen. ■

ANGELIKA BENES,
Geschäftsführerin bei syska

KIRCHE HÄLT GEBOTE FÜR IT-SICHERHEIT

Die Evangelische Kirche in Deutschland schlägt mit der ITSVO-EKD bereits seit 2015 einen verbindlichen Weg hin zu mehr Sicherheit ein: Alle zugehörigen Einrichtungen sollten binnen drei Jahren ein IT-Sicherheitskonzept erstellen und sind verpflichtet, es kontinuierlich an die aktuellen Gegebenheiten anzupassen. Das Landeskirchenamt und die Kreiskirchenämter der Evangelischen Kirche in Mitteldeutschland (EKM) setzen bei der Umsetzung der Verordnung über alle Außenstellen hinweg auf eine Kombination aus softwarebasierten Lösungen.

SILVIA FUNKE, freie Fachjournalistin aus Leipzig

Die EKM wird geleitet von der Landessynode und vom Landeskirchenrat, von dem Landesbischof mit Sitz in Magdeburg sowie dem Kollegium des Landeskirchenamtes in Erfurt. Von hier aus steuert das Referat für IT-Sicherheit die Umsetzung und Einhaltung der ITSVO-EKD. Gemäß dieser müssen kirchliche Einrichtungen, die personenbezogene Daten erheben, verarbeiten und nutzen, angemessene technische und organisatorische Maßnahmen zum Datenschutz durchführen. Grundlage des IT-Sicherheitskonzepts sollten die Empfehlungen des BSI zur Informationssicherheit und zum IT-Grundschutz sein. „Ziel war die Einhaltung von Vertraulichkeit, Integrität und Verfügbarkeit der erhobenen und verarbeiteten Daten: Sie sollten wann immer benötigt zur Verfügung stehen, Zugriff und Änderungsberechtigungen eindeutig regeln und vor unberechtigtem Zugriff und Verlust geschützt werden", so der Referent für IT-Sicherheit, Sven Wenzke. „Wir haben nach einem Tool gesucht, das über unsere verteilten Außenstellen hinweg sowohl ein Sicherheitskonzept umsetzen als auch ein Notfallhandbuch abbilden kann."

MODULARES ISMS-DOKUMENTATIONSTOOL FÜHRT DURCH SICHERHEITSPLANUNG

Zur Recherche im Vorfeld der geplanten Maßnahmen besuchte man unter anderem Fachveranstaltungen zur Informationssicherheit beim IT-Dienstleister Q-SOFT aus Erfurt. Schließlich entschied man sich nach einem Anbietervergleich dazu, auch die Einführung von ISMS und Notfallhandbuch durch die Experten begleiten zu lassen. „Die Erfahrungswerte und das Fachwissen der IT-Berater unterstützt durch Software-Tools, die unsere Anforderungen abdecken konnten, haben uns überzeugt", begründet Sven Wenzke die Anbieterwahl. Das Vorgehen erfolgte dann nach der Plan-Do-Check-Act-Methode: Zunächst wurde definiert, welche Sicherheitsniveaus erreicht werden sollten. Anschließend spielte man Szenarien durch, welche das Erreichen des angestrebten Sicherheitsniveaus verhindern könnten. Dann wurden Maßnahmen zusammengestellt, mit denen die Risiken vermieden werden können, um Maßstäbe zur Validierung der Methodenwirksamkeit festzulegen. Im Fokus der Maßnahmen bei der EKM standen unter anderem die E-Mail-Verschlüsselung, interne Netzwerkzugriffskontrollen (NAC) zur Abwehr von Viren, Würmern und unautorisierten Zugriffen sowie die Einführung eines ISMS-Dokumentationstools sowie einer IT-Notfallplanung. Hinzu kommt eine komplette Suite an verschiedenen Modulen zum Einsatz. Sie verfügt über eine zentrale Datenbasis, sodass weitere Lösungen nach Bedarf schrittweise integriert und Daten übernommen werden können. Im Basissicherheitscheck wurden dann die vorhandenen Sicherheitsmaßnahmen anhand eines weiteren Moduls mit den Empfehlungen der IT-Grundschutzkataloge abgeglichen, um das Sicherheitsniveau zu identifizieren und Optimierungspotenziale aufzuzeigen.

SCHNELLER RETURN-ON-INVEST IM NOTFALL

Teil des Sicherheitskonzepts bei der EKM ist eine Notfallplanung. Sie definiert kritische Ereignisse und Prozesse und legt fest, welche Maßnahmen wann und in welcher Reihenfolge durch wen ergriffen werden müssen. „Die Kosten bei der Einführung eines ISMS und einer Notfallplanung amortisieren sich schnell, bedenkt man die Schäden, die durch etwaige Ausfälle entstehen können", so Marco Gräf, Teamleiter Vertrieb Kommunikationsinfrastruktur bei Q-SOFT.

CORONA-PANDEMIE ZEIGT: IT-SICHERHEITSKONZEPT STETIG FORTSCHREIBEN

Ein Notfallszenario, das – wie bei der EKM – in den meisten Notfallhandbüchern bisher fehlte, ist der Ausbruch einer Pandemie. „Die aktuellen Entwicklungen zeigen die Notwendigkeit, das Sicherheitskonzept samt Notfallplanung stetig zu aktualisieren", so Marco Gräf. Viele Firmen und Organisationen erweitern deswegen aktuell ihre Notfallpläne. Die ITSVO-EKD hatte bereits 2015 geregelt, dass beispielsweise private IT-Geräte nur genutzt werden dürfen, wenn alle datenschutzrechtlichen und sicherheitstechnischen Anforderungen erfüllt sind. ■

Mehr dazu hier

Q-SOFT

Mitarbeiter für die digitale Arbeitswelt fit machen

PHISHING-ANGRIFFE ERFOLGREICH ABWEHREN

Seit geraumer Zeit entwickelt sich Phishing zu einer bedeutsamen Bedrohung für Unternehmen. Während der Corona-Krise nahm das Ausmaß der Attacken jedoch neue Dimensionen an – ein Nachlassen ist nicht erkennbar. Aktuelle Daten zeigen: Vor allem Deutschland ist beliebt bei den Angreifern. Regelmäßige Security-Awareness-Trainings sollten diese Tatsache verstärkt berücksichtigen.

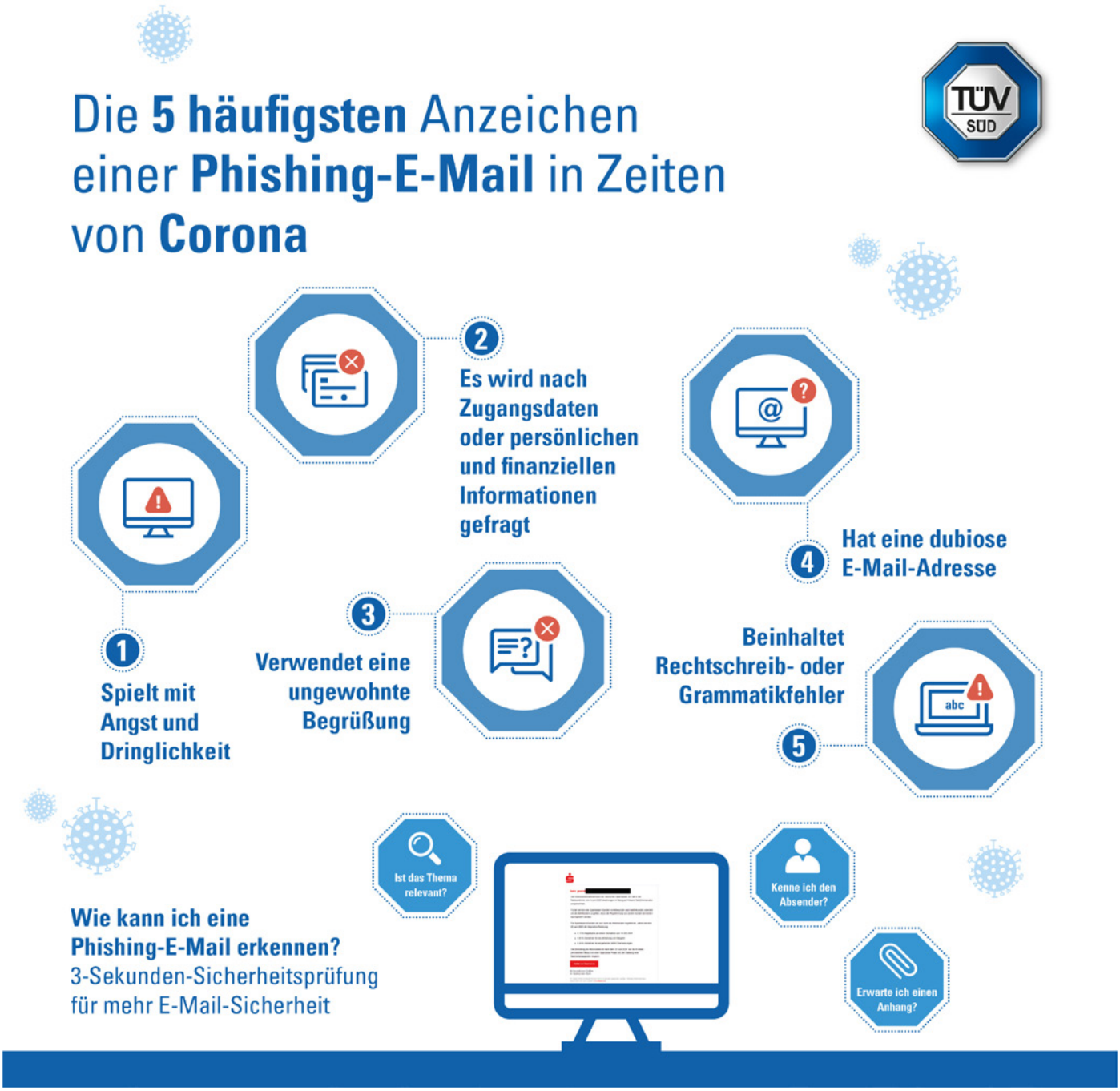
Sie sind eine altbekannte Gefahr: Phishing-Attacken. Meist kommen sie in Form einer E-Mail in das Postfach eines Internet-Nutzers und wollen diesen dazu bringen, auf einen betrügerischen Hyperlink zu klicken oder eine Datei herunterzuladen. Sie locken mit Rabatten, mit Geheimtipps zum Geldverdienen, mit Sonderangeboten, oder drohen mit gefälschten Mahnungen, Rechnungen und Anwaltsbriefen. Fällt der Nutzer darauf herein, lädt er sich entweder einen Computer-Virus herunter oder landet auf einer gefälschten Webseite, wo ihm Zugangsdaten oder Kreditkarten-Informationen gestohlen werden. Zu diesem Zweck imitieren die Seiten oft echte Internet-Auftritte und bekannte Marken, um den Betrug so gut wie möglich zu gestalten.

DEUTSCHE UNTERNEHMEN SIND BELIEBT FÜR PHISHING-KAMPAGNEN

Phishing ist natürlich international eine Bedrohung. Aktuelle Daten eines Berichts aber zeigen, dass besonders Deutschland ein attraktives Ziel für Kriminelle darstellt, die mit einer Phishing-Kampagne Unternehmen angreifen möchten. Die Zahlen belegen, dass 4,78 Prozent aller Command-and-Control-Server (CnC-Server) hinter Phishing-Versuchen in Deutschland stehen. Das sagt zunächst nichts über die tatsächliche Position einer Hacker-Gruppe aus, denn diese kann ihre Verbindungen umleiten, um ihre Identität zu verschleiern, doch aussagelos sind diese Daten nicht. Richtig gelesen offenbaren die hohen Zahlen der CnC-Server nämlich, dass deutsche Unternehmen besonders im Fokus der Attacken stehen, denn: Gehen die Malware-Attacken von einem deutschen Server aus, so sitzt dieser in einem für viele Unternehmen vertrauenswürdigen Land. Daher greifen manche Spam-Regeln nicht, weil sie den Absender für glaubwürdig halten. Zudem sind es vor allem die Postfächer der heimischen Unternehmen gewohnt, von einer deutschen Quelle E-Mails zu erhalten – egal welchen Inhalts.

MITTELSTÄNDLER SIND FÜR KRIMINELLE LUKRATIVER ALS GROSSKONZERNE

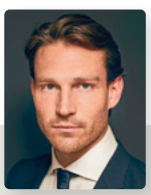
Hinzu kommt, dass in Deutschland viele Weltmarktführer sitzen und es sich dabei nicht ausschließlich um Großkonzerne handelt. Im Gegenteil: Deutschland ist bekannt für seine vielen Mittelständler, die als sogenannte Hidden Champions ihren Bereich beherrschen. Das bedeutet, dass hierzulande viel Industrie und Fachwissen vorhanden ist, und diese Daten sind natürlich besonders lukrativ für Kriminelle. Gleichzeitig bieten die deutschen Unternehmen, vor allem die erwähnten Mittelständler, eine gute Angriffsfläche für virtuelle Angriffe jeder Art, weil sie zwar als Firma sehr wertvoll sind, jedoch nicht über die umfangreiche und



teure IT-Abwehr eines Großkonzerns verfügen. Daher können die erbeuteten Informationen dieser Firmen lukrativer sein als die der großen Unternehmen, weil weniger Aufwand nötig ist, um sie zu stehlen.

MITARBEITER SIND EIN TEIL DER IT-SICHERHEIT

Vor allem die letzte Tatsache verdeutlicht die Wichtigkeit von Anti-Phishing-Services, wie einer Schulung der Mitarbeiter von unabhängiger Seite. Nur wenn die Angestellten eine gewisse Übung darin haben, Phishing-Angriffe zu erkennen und ein Bewusstsein dafür entwickelt haben, wie gefährlich die Bedrohung ist, kann sich ein Unternehmen wirklich effektiv gegen diese Attacken schützen. Die Menschen sind ein Teil der IT-Sicherheit eines Unternehmens und sollten daher einbezogen werden. Das schützt wiederrum sie selbst davor, Opfer einer Hacker-Attacke zu werden – auch zu Hause, im Homeoffice oder außerhalb der Arbeit. Wir sollten außerdem nicht vergessen: Ein Großteil der virtuellen Angriffe beginnt derzeit mit einem Phishing-Versuch. ■



MORITZ WAPPNER,
Team Lead Cyber Security Advisory Services bei TÜV SÜD

Digitales Risikomanagement in Zeiten von Remote Work

IT-GOVERNANCE IN DEN FOKUS RÜCKEN

Die Verbreitung mobiler und vernetzter Geräte hat zu einer explosionsartigen Zunahme von Nutzerkonten, WLAN-Zugangspunkten und zu erteilenden Berechtigungen geführt, die Organisationen managen müssen. Während der Krise kam verschärfend hinzu, dass Mitarbeiter im Homeoffice Zugang zu kritischen Anwendungen und sensiblen Informationen benötigten – und das über verschiedene Geräte hinweg. Um den Geschäftsbetrieb aufrechtzuerhalten, haben Unternehmen dafür in Rekordzeit die entsprechende IT-Infrastruktur aufgesetzt: Mit der Implementierung neuer Authentifizierungsverfahren bis hin zur Einführung neuer Kollaborationsplattformen, wie Microsoft Teams und Zoom, sind Unternehmen schnell in der neuen Geschäftsrealität angekommen.

Im Zuge schnell ergriffener Maßnahmen schleichen sich häufig vorläufige Lösungen für Fragen der Sicherheit und das Management digitaler Risiken ein. „Darum kümmern wir uns später" lautet die Devise. Für Unternehmen, die sich in dem neuen digitalen Geschäftsalltag eingerichtet haben, ist dieses „Später" mittlerweile Gegenwart geworden. Daher ist es jetzt an der Zeit, sich darauf zu konzentrieren und zu verstehen, welche Risiken sich aus den ergriffenen Notfallmaßnahmen ergeben haben. Welcher (Netzwerk-)Zugang wurde wem, zu welchem Zweck und für wie lange gewährt?

In den meisten Fällen haben Unternehmen mittlerweile in einen Remote-Arbeitsmodus gefunden. IT-Verantwortliche stehen im Rahmen des Identitätsmanagements und der Vielzahl an verbundenen Geräten und integrierten Anwendungen vor der Herausforderung, den Überblick zu behalten und die Netzwerktransparenz zu wahren. Die Schwierigkeit liegt darin, berechtigte Geräte von böswilligen Zugriffsversuchen zu differenzieren. Das Zugriffsmanagement und die Identitäts-Governance bieten Cyberkriminellen zusätzliche Angriffsfläche. Ihr Schutz ist angesichts der gestiegenen

TIPPS FÜR DIE IT-GOVERNANCE

IT-Verantwortliche, die kürzlich neue Geräte, Anwendungen und andere Tools eingeführt haben, um ihren Mitarbeitern an verschiedenen Standorten Zugang zu ermöglichen, sollten sich primär auf vier Bereiche der Governance konzentrieren:

1. Eine risikobewusste, kontextgesteuerte Governance ermöglichen, indem das Risiko- und Zugriffsmanagement in die Identity Governance und Lebenszyklusprozesse integriert wird – anstatt sie als separate Fälle zu verwalten.

2. Aussagekräftige Informationen für Entscheidungen bereitstellen, indem Netzwerkaktivitäten nach Risiko, Priorität und Kontext organisiert werden, was dazu beitragen kann, die „Zertifizierungsmüdigkeit" der Geschäftsführung zu verringern.

3. Ausreißer und ungewollte Zugriffe identifizieren, indem ein risikobasierter Ansatz verwendet wird, um ausgefallene Zugriffsanfragen schnell zu identifizieren, sie zu kennzeichnen und für die Behebung zu priorisieren.

4. Prozesse automatisieren, sodass mit einem sicheren Netzwerkzugang auch effektiv und effizient gearbeitet werden kann.

IT-Sicherheitsbedrohungen im Homeoffice daher von sicherheitskritischer Bedeutung.

Der KuppingerCole Identity Governance & Administration (IGA) Leadership Compass 2020 [1] stellt fest, dass sich der Markt für IGA-Lösungen schnell entwickelt. Das liegt vor allem daran, dass die IT-Sicherheitsverantwortlichen bemüht sind, eine höhere Netzwerktransparenz über alle Unternehmensbereiche hinweg zu realisieren. Angestrebt wird zudem, einen Überblick über die einzelnen Zugriffe sowohl in On-Premises-Umgebungen als auch in der Cloud zu haben. Automatisierte Zugriffsanfragen oder Lösungen für das Zurücksetzen von Selbstbedienungs-Passwörtern vereinfachen den Übergang zur Remote-Arbeit, machen den Arbeitsalltag weniger stressig und steigern gleichzeitig die Produktivität der Mitarbeiter. Wenn Remote-Teams über eine benutzerfreundliche Lösung zur Beantragung des Zugriffs auf Anwendungen und Ressourcen verfügen, erleichtert dies auch die Bearbeitung von Anfragen an den Helpdesks, wodurch Prozesse verschlankt und gleichzeitig IT-Kosten gesenkt werden können.

Da Mitarbeiter in Unternehmen kommen und gehen und innerhalb der Organisation das Team oder die Rolle wechseln können, ist es wichtiger denn je, durch einen JML-Prozess vorbereitet zu sein (JML steht für Join, Move, Leave – also Eintritte, Wechsel und Austritte): So können Compliance-Aspekte gewahrt und Zugriffsrichtlinien für Nutzer durchgesetzt werden. Ein temporäres Regel- und Richtlinienmanagement unterstützt dabei, Ausnahmen und Verstöße im Blick zu behalten und gegebenenfalls eingreifen zu können. Zuletzt wird durch eine automatisierte Netzwerkverwaltung auf der Grundlage dieser temporären Regeln, Rollen oder Eigenschaften ein manuelles Eingreifen unnötig und das Risiko für Unternehmen weiter gesenkt.

ANGEKOMMEN IN DER NEUEN GESCHÄFTS-REALITÄT

Durch die Krise arbeiten mehr Beschäftigte als je zuvor von zu Hause. Das macht die (Neu-) Zertifizierung der Zugangsrechte wichtiger denn je. Eine (Re-)Zertifizierung aller Zugangs- und Berechtigungsdaten übersteigt bei Weitem das, was ein Identitätsteam bewältigen kann. Unternehmen benötigen daher eine Lösung, die eine kontinuierliche Wahrung der Compliance-Richtlinien ermöglicht, bei der Verwaltung und Bereitstellung von Nutzerkonten hilft und die Einhaltung gesetzlicher und unternehmensinterner Vorschriften sicherstellt. Mittels fortschrittlicher Analysefunktionen und der Automatisierung gängiger Aufgaben können Identitätsteams unnötigen Zugriff auf Systeme und Anwendungen sowie den Verwaltungsaufwand reduzieren.

GOVERNANCE MACHT DAS LEBEN LEICHTER

Zusammen mit einem guten Richtlinienmanagement, festgelegten Arbeitsabläufen, Audit-Möglichkeiten und einer generellen Change-Management-Bereitschaft sorgt eine abgestimmte IT-Sicherheitslösung dafür, digitale Risiken im Blick zu behalten. Die richtige Sicherheitslösung wird die Identifizierung von Identitäts- und Zugriffsrisiken wesentlich erleichtern, sodass Zeit und der notwendige Überblick zur Behebung derjenigen Sicherheitsprobleme gewonnen wird, die sich aus den rasch getroffenen Notfall- und Business-Continuity-Maßnahmen ergeben haben.

Sicherheits-, Risiko- und IT-Teams müssen Wege finden, um Netzwerkzugänge zu sichern, die Einhaltung von Vorschriften zu gewährleisten und gleichzeitig den Geschäftsbetrieb aufrechtzuerhalten. Ein gutes Identitäts-Management sorgt für Transparenz in Verbindung mit verlässlichen Risikoanalysen, um Maßnahmen priorisieren zu können und Identitäten im gesamten IT-Ökosystem im Blick zu behalten. Dafür muss die Identitäts-Governance über die IT hinaus mit dem Risiko- und Sicherheitsmanagement langfristig zusammengebracht werden. ■

[1] *https://www.rsa.com/en-us/offers/kuppingercole-compass-iga*

HEIDI BLEAU,
RSA Fraud & Risk Intelligence

Managed Security Services und Firewalls Hand in Hand

DIE ZUKUNFT DER IT-SECURITY IST HYBRID

Die bisherige Sicherheitsinfrastruktur in der IT geht zurück auf eine Zeit, in der die Cloud noch kein Begriff war. Aus diesem Grund nutzen Unternehmen bis heute die klassische Lösung mit einer physischen Firewall, Antiviren-Scannern auf den Clients und für den Fernzugriff einzelner Verbindungen eine VPN-Tunnelung, die allen Datenverkehr durch einen einzigen Bottleneck zwingt: die physische Firewall. Problematisch und wenig performant wird das in Zeiten wie der Homeoffice-Situation bedingt durch Corona. Die Zukunft der IT-Sicherheit liegt in hybriden Konzepten: Moderne Managed Security Services und physische Firewalls gehen Hand in Hand.

Angriffe von außen sind nach wie vor das größte Risiko für eine IT-Infrastruktur. Hackerangriffe, Ransomware, Datendiebstahl oder andere Viren und Würmer können in wenigen Stunden ein komplettes Unternehmen handlungsunfähig machen. Lässt sich der Schaden nicht schnell beheben, droht ebenso schnell eine Insolvenz: Es sind meist nur wenige Tage, die ein Unternehmen im Totalausfall ohne große Geschäftsschädigung überleben kann. Längst haben sich Lösungen mit einer Hardware-Firewall etabliert, die Unternehmenszentralen, Niederlassungen und Data Center sichern. Die heutige IT-Infrastruktur denkt allerdings längst nicht mehr in diesen Dimensionen, sondern umfasst IT-Anwendungen aus der Cloud und auch Datenhaltung an unterschiedlichsten Orten.

ARBEITSWELT IM UMBRUCH

Daten liegen nicht mehr ausschließlich hinter dem Firewall-Schutzschirm des eigenen Unternehmens, sondern in Anwendungen, privaten oder Public Clouds – ein neues Sicherheitsdenken ist also gefordert. IT-Security in Netzwerken endet längst nicht mehr an der Firewall, sondern umfasst komplexe hybride Strukturen, die der Cloud eine aktive Rolle in der Sicherheit geben. Damit lassen sich auch Situationen wie die Corona-Krise besser bewältigen – denn Security aus der Cloud ist da, wo sie gebraucht wird. Zudem ist die Cloud wie kein anderes System dazu geeignet, zu skalieren und problemlos mit wachsenden Ansprüchen mitzuhalten. Die Krise der vergangenen Monate macht deutlich: Die Dezentralisierung der Arbeitswelt über mobile- und Homeoffice-Arbeitsplätze wird nicht mehr abnehmen. Die Arbeitswelt im Umbruch geht mit einer weiteren Verlagerung von Daten und Anwendungen in die Cloud einher.

FIREWALL: SCHUTZ FÜR BESTEHENDE STRUKTUREN

Bei einer klassischen Firewall handelt es sich um ein stationäres System, das in der Lage ist, Datenverkehr zu analysieren und IT-Systeme vor Angriffen oder unbefugten Zugriffen zu schützen. Die Firewall in Unternehmen ist meist als dedizierte Hardware an Netzwerkgrenzen zwischen einem internen und einem externen Netzwerk eingerichtet. An dieser zentralen Stelle kontrolliert die Software auf der Firewall den ein- und ausgehenden Datenverkehr.

Um die Schutzfunktion zu erfüllen, besitzen klassische Firewalls verschiedene Funktionskomponenten. Der Paketfilter ist dabei die Basisfunktionalität der Firewall und kann IP-Pakete anhand von Merkmalen, wie IP-Absenderadressen, IP-Zieladressen und Ports, filtern. Beherrscht der Paketfilter dazu Stateful Packet Inspection, ist er zusätzlich in der Lage, den Zustand von IP-Verbindungen als Kriterium für die Paketfilterung heranzuziehen. Deep Packet Inspection wertet zusätzliche Informationen der in den IP-Paketen transportierten Protokolle aus und blockiert Pakete oder leitet die Daten auf Basis von Regeln weiter. Die Proxyfunktion in der Firewall übernimmt bei Netzwerkverbindungen die Rolle des Absenders und sendet alle Anfragen stellvertretend weiter. Der Proxy führt

die komplette Kommunikation und ist in der Lage, Inhalte zu analysieren und zu beeinflussen. Beispielsweise kann ein Proxy verhindern, dass User aus einem internen Firmennetz nicht erwünschte Inhalte aus dem Internet laden. Der Content-Filter erweitert diese Möglichkeiten und lässt einen noch tieferen Blick in die Daten der Verbindung zu.

In vielen Fällen terminiert die Firewall auch Virtual-Private-Network-(VPN-)Verbindungen. Über diese verschlüsselten Verbindungen wird es möglich, auf das hinter der Firewall gelegene Netzwerk aus dem öffentlichen Internet sicher zuzugreifen. Problematisch: Jeder Standort eines Unternehmens braucht eine separate Firewall. Globale Unternehmen mit zahlreichen Standorten leiden nicht selten unter einer Flut verschiedenster Hardware-Firewalls. Damit einher geht ein Wartungsaufwand, zumal pro Standort auch redundante Systeme als Back-up vorgehalten werden sollten. Große Unternehmen verfügen daher teils über vierstellige Mengen aktiver Firewalls.

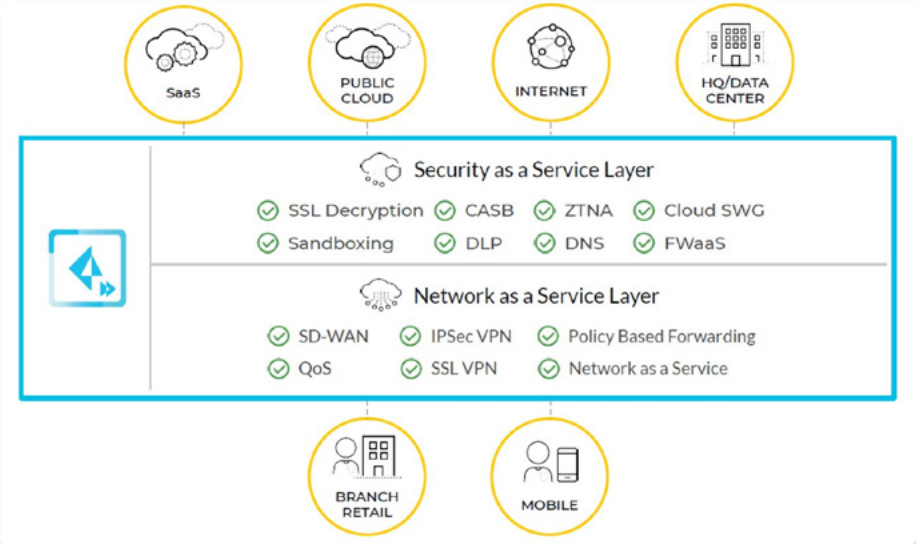
TRIPLE PLAY VON ENDPOINT-, ON PREMISES-FIREWALL UND CLOUD-SECURITY

Mittlerweile werden längst Daten und Anwendungen aus der Cloud bezogen. Systeme wie Office 365 machen das Arbeitsleben leichter, aber auch die Situation rund um die Einhaltung höchster Sicherheitsstandards ungleich komplexer. Das Schutzniveau über lokale Hardware-Firewalls erfüllt nicht mehr alle Bedingungen. Eine moderne Arbeitswelt, in der sowohl Nutzer wie auch Daten an unterschiedlichsten Orten liegen, bedarf auch neuer Sicherheitsstrukturen, die sowohl lokal funktionieren, aber auch die Cloud umfassen und nicht zuletzt den Datenverkehr integrieren, der über mobile Arbeitsplätze erzeugt wird. Eine besondere Herausforderung bot dabei der Beginn der Corona-Krise: Innerhalb kürzester Zeit gingen Tausende Mitarbeiter aus den Unternehmen in das heimische Büro am Küchen- oder Wohnzimmertisch. Statt direktem Anschluss an das Netzwerk galt es, Remote-Zugänge zu legen. Die Performance beim gängigen Modell – einem VPN-Client, der den Verkehr über die Unternehmens-Firewall am jeweiligen Standort routet – geht dann oft schnell in die Knie, vor allem, wenn der Traffic „Haken schlagen" muss, um interne Systemzugriffe, normalen Internetzugriff und Cloud-Anwendungen abzubilden.

Durch die Nutzung von cloudbasierten Security-Lösungen, die direkt in großen und extrem performanten Data Centern gehostet werden, werden die IT-Ressourcen gestärkt und auch Betriebskosten reduziert. Die Bereitstellungszeit lässt sich massiv verkürzen, da die typische physische Infrastruktur nicht erst aufgebaut werden muss. Während klassische Infrastrukturmodelle weiter durch physische Firewalls geschützt werden, wird ein Großteil der Absicherung über Cloud Security abgedeckt und entlastet damit die bestehende Struktur.

Umsichtige Dienstleister setzen daher mittlerweile ein Triple-Play-Modell um, bestehend aus Absicherung des Clients mit einer Antiviren-Lösung, Nutzung von On-Premises-Firewalls für den Schutz klassischer Daten und Anwendungen aus dem eigenen Rechenzentrum und einem Cloud-Security-Paket, das in seiner Nutzung keine Beschränkung kennt. Eine VPN-Tunnelung findet auch weiter statt – sie tritt aber in den Hintergrund und bedeutet keinen Performance-Verlust mehr. Denn statt zu einer physischen Firewall wird der größte Traffic-Anteil per VPN in das Rechenzentrum geleitet, in dem die Cloud Security betrieben wird.

Hierbei entfalten moderne SD-WAN-Strukturen einen besonderen Komfort. Statt einer statischen Verbindung definiert die Software das Netzwerk. Statt eines Routers wird die SD-WAN-Technik installiert, in der per „Plug-and-Connect" alle unterschiedlichen Zugriffsformen hinterlegt sind. Damit können die Mitarbeiter von aufwendigen VPN-Clients und Zugriffssperren auf den einzelnen Clients Abschied nehmen. Unabhängig vom Provider ist die Verbindung stets sicher, ob ins Internet, ins Intranet oder bei der Nutzung von Cloud-Diensten. So behalten die IT-Netze eines Unternehmens die volle Funktionalität und Skalierbarkeit, bei gleichzeitig optimierter Kostenlast. ■



Security als Plattform, bestehend aus Endpoint, On-Premises-Firewall und Security in der Cloud. (Quelle: Palo Alto Systems)

ANDREAS SCHLECHTER,
Geschäftsführer/CEO bei Telonic

IT-Sicherheit für eine digitalisierte Industrie

INDUSTRIE-4.0-GEFAHREN FRÜHZEITIG ERKENNEN

Immer mehr Unternehmen nutzen die Vorteile, die sich aus der umfassenden Digitalisierung ihrer Produktionsumgebungen ergeben. Im Rahmen von Industrie-4.0-Projekten werden konventionelle Fertigungsanlagen zunehmend durch „smarte" Maschinen oder sogenannte Industrial-Internet-of-Things-(IIoT-)Geräte ersetzt. Einerseits erhöhen diese zwar die Produktivität und sorgen für steigende Erträge, andererseits schaffen diese Technologien aber leider auch neue Angriffspunkte für Hacker.

Untersuchungen durch IBM ergaben beispielsweise, dass sich die Anzahl der Cyberangriffe, die Systeme vollständig funktionsunfähig machen, im ersten Halbjahr 2019 zum Vergleichszeitraum des Vorjahres verdoppelten.[1] Brisant: Rund 50 Prozent der betroffenen Unternehmen sind im Industriesektor tätig. Während veraltete Geräte, wie Drucker und Faxgeräte, bekannt dafür sind, mögliche Schwachstellen in der Unternehmenssicherheit darzustellen, finden Hacker jedoch ständig Wege, um selbst die neuesten, mit Intelligenz ausgestatteten Industrietechnologien zu infiltrieren.

IT-Profis sind branchenübergreifend gefordert, die maximale Sicherheit selbst in hochgradig vernetzten und zunehmend komplexeren Unternehmenssystemen zu garantieren. Im Folgenden werden vier potenzielle Gefahrenbereiche vorgestellt, in denen sich für Hacker Einfallstore bieten, und Tipps gegeben, wie sich die Industrie dagegen schützen kann.

INTELLIGENTERE TOOLS, VERGLEICHBARE SCHWACHSTELLEN

IIoT ist für viele Firmen zu einem unverzichtbaren Teil ihrer Produktion geworden. Vernetzte Fertigungsroboter und andere „smarte" Technologien erleichtern die Qualitätssicherung, erhöhen die Genauigkeit sowie Effizienz der Bestandsüberwachung und steigern die allgemeine Betriebsleistung. Trotz all ihrer Vorteile weisen IIoT-Anlagen aber ähnliche Schwachstellen wie nicht-industrielle IoT-Geräte auf, da dem Thema Sicherheit beim Design oft keine allzu große Beachtung geschenkt wird. Cyberkriminellen bieten sich nicht selten zahlreiche Angriffsflächen, um in Unternehmensnetzwerke einzudringen.

Es gibt jedoch verschiedene Maßnahmen, die Industriekunden gegen diese Bedrohungen ergreifen können. Die Netzwerksegmentierung ist eine davon – und sie lässt sich zudem recht einfach umsetzen: Dabei werden die vorhandenen kabelgebundenen und kabellosen Netzwerke in mehrere Bereiche eingeteilt – etwa für IIoT-Devices, separate Gäste-/Mitarbeiter-WLANs etc. Über die Isolierung der IIoT-Infrastruktur von anderen, mit dem Netzwerk verbundenen Geräten, kann einer Ausbreitung potenzieller Cyberangriffe wirksam der Riegel vorgeschoben werden. Mit einer Unified-Threat-Management-(UTM-) Appliance ist dies schnell erledigt. Der klare Vorteil gegenüber der reinen Firewall besteht darin, dass sich mehrschichtige Sicherheitsdienste gleichzeitig und im Idealfall ohne Einbußen in der Performance oder im Durchsatz ausführen lassen. So sorgt ein Intrusion Prevention Service (IPS) beispielsweise dafür, dass verdächtige Aktivitäten von IIoT-Geräten automatisch erkannt und blockiert werden – ohne Unterbrechung des Netzwerkzugriffs. Um auch in kabellosen Netzwerken abgesichert zu sein, lohnt sich darüber hinaus die Installation eines Wireless Intrusion Prevention Systems (WIPS). Damit können WLAN Access Points bequem von jedem Standort aus in der Cloud verwaltet werden.

DER FEIND IM EIGENEN UNTERNEHMEN

Die Situation, dass Mitarbeiter ohne Wissen und Zustimmung der IT-Abteilung eigene Hard- und/oder Software innerhalb der Unternehmensnetzwerke verwenden, wird für viele Unternehmen zunehmend zur Herausforderung. Gerade im industriellen Umfeld sollten die Themen „Schatten-IT" und „Bring your own device (BYOD)" nicht unterschätzt werden, denn dadurch sind die Netzwerke einem deutlich höheren Risiko für Cyberangriffe ausgesetzt.

Eine von Cisco in Auftrag gegebene Studie ergab, dass in Unternehmen zwischen 15 und 22 Mal mehr Cloud-Anwendungen genutzt werden, als die IT-Abteilungen erwartet hatten.[2] Es liegt auf der Hand: Die fehlende Transparenz über sämtliche Vorgänge im Netzwerk erschwert deren angemessene Sicherung massiv. IT-Teams, die keine umfassenden Kenntnisse über die verwendete Software und/oder Endgeräte haben, werden nicht in der Lage sein, die Netzwerksicherheit zufriedenstellend zu überprüfen.

Glücklicherweise gibt es Network-Mapping-(NMAP-)Services, die es IT-Abteilungen ermöglichen, das Netzwerk hinter der Firewall – einschließlich aller bekannten Geräte – mithilfe der Daten aus NMAP-Scans und des DHCP-Fingerprints übersichtlich abzubilden. Darüber hinaus können HTTP-Header oder bestimmte Anwendungen genauer untersucht werden. Auf diese Weise lassen sich sofortige Korrekturmaßnahmen einleiten, sollten neue oder unbekannte Geräte bzw. Applikationen auftauchen.

GESCHÄFTSKRITISCH: DER SCHUTZ VON GEISTIGEM EIGENTUM

Der Diebstahl geistigen Eigentums (Intellectual Property, IP) stellt nach wie vor eine große Bedrohung für die produzierende Industrie dar. Besonders die Informationen über Produktions- und Verarbeitungsprozesse sind für jedes Unternehmen äußerst wertvoll. Durch den Verlust wichtigen geistigen Eigentums an Wettbewerber oder Hacker können große finanzielle Schäden und ein erheblicher Imageverlust entstehen. Um Unternehmenserfolge zu schützen und den Verlust von Kunden zu verhindern, muss dem Schutz geistigen Eigentums also höchste Priorität eingeräumt werden.

Für IT-Teams in Industrieunternehmen ist die Einführung einer Multi-Faktor-Authentifizierung (MFA) ein wesentlicher Schritt, um ihre sensiblen Netzwerkdaten sichern zu können. Es existieren diverse Lösungen, die über die gängige Zwei-Faktor-Authentifizierung (2FA) hinausgehen. Per biometrischer Authentifizierung – oder durch das Einloggen über eine mobile App – kann die sichere Anmeldung bei Computern, Cloud-Services, VPNs und sonstigen Anwendungen garantiert werden.

Data Loss Prevention ist ein weiteres Kernelement, mit dem sich Datenlecks reduzieren lassen. Verstöße gegen die Datensicherheit werden durch die konsequente Analyse versendeter Dokumente entdeckt und eingedämmt. Das Durchsickern vertraulicher Informationen aus dem Netzwerk lässt sich so effektiv verhindern. Denn sobald ein Leak erkannt wurde, wird die Verbindung blockiert oder unter Quarantäne gestellt sowie der zuständige Administrator umgehend benachrichtigt.

MANGEL AN FACHKRÄFTEN FÜR IT-SICHERHEIT

Ein erhebliches Problem ist der Fachkräftemangel im Bereich IT Security, der laut der Analysten von Enterprise Strategy Group von Jahr zu Jahr drastischer wird.[3] Das trifft besonders in der Industrie zu, die von ihren komplexen und spezialisierten Technologien abhängiger ist als die meisten anderen Branchen. Qualifizierte Fachkräfte, die sensible Betriebstechnik (Operational Technology, OT) und industrielle Kontrollsysteme (ICS) ordnungsgemäß verwalten und sichern können, sind selten. In Anbetracht des zunehmenden Mangels an Fachkräften für IT-Sicherheit und der Tatsache, dass es oft mehrere Monate dauern kann, eine freie Stelle in der Fertigung zu besetzen, sollte die Industrie folglich Sicherheitslösungen priorisieren, die einfach zu implementieren und administrieren sind. Zudem lässt sich dadurch auch die Abhängigkeit von hochgradig spezialisierten IT-Profis verringern.

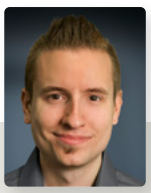
Um die IT-Sicherheit eines Unternehmens zu verbessern, reicht es nicht mehr aus, sich nur auf herkömmliche Netzwerkkomponenten und Computer zu konzentrieren. Es muss das Bewusstsein dafür geschärft werden, dass moderne Cyberkriminelle oft einen mehrstufigen Ansatz verfolgen, wenn sie Industriebetriebe ins Visier nehmen. Bei der Entwicklung von Sicherheitsstrategien sollten Unternehmen deswegen darauf achten, sämtliche Prozesse so weit wie möglich zu vereinfachen. Dabei sind folgende Punkte entscheidend: eine Verbesserung der Transparenz, die Durchführung häufiger Sicherheitsscans und Geräte, die immer auf dem neuesten Stand sind. ■

Quellen

[1] https://securityintelligence.com/posts/from-state-sponsored-attackers-to-common-cybercriminals-destructive-attacks-on-the-rise/

[2] https://www.cio.com/article/2968281/cios-vastly-underestimate-extent-of-shadow-it.html

[3] https://www.esg-global.com/blog/the-cybersecurity-skills-shortage-is-getting-worse



MARC LALIBERTE,
leitender Sicherheitsanalyst bei WatchGuard Technologies

INTERVIEW: Christian Milde, Kaspersky

TOP-TECHNIK GEGEN PERFEKTIONIERTE CYBERBEDROHUNGEN

Besonders im Mittelstand kursieren derzeit massive Ängste, denn Cyberkriminelle werden immer skrupelloser und gleichzeitig geschickter. Die große Frage lautet: Kann ich mein Unternehmen noch angemessen schützen? Christian Milde, General Manager DACH bei Kaspersky, erklärt im Interview, wie groß die Gefahr ist, Opfer eines Cyberangriffs zu werden und wie sich Unternehmen mit neuen Technologien wirksam verteidigen können.

„Cyberkriminelle nutzen zunehmend die Tatsache aus, dass viele Unternehmen der Komplexität ihrer eigenen IT-Landschaft nicht mehr gewachsen sind. Wer den Überblick verliert, kann Attacken nicht umgehend analysieren, abwehren und Folgeschäden beseitigen."

Christian Milde, Kaspersky (Foto: Kaspersky)

◀ *Blick in ein Kaspersky Security Operations Center (SOC) (Foto: Kaspersky)*

ITS: Man liest in den Medien immer wieder von folgenschweren und spektakulären Hackerattacken. Wie groß ist denn derzeit die Gefahr, dass Unternehmen Opfer von Cyberangriffen werden?

Christian Milde: Cyberattacken auf Unternehmen jeder Größe und Branche nehmen immer weiter zu. Insbesondere zielgerichtete Angriffe auf Unternehmen entwickeln sich stetig zu einer immer größeren Gefahr. Die Angreifer gehen hier oftmals sorgfältiger vor als vielleicht noch vor einigen Jahren. So nutzen sie zunehmend die Tatsache aus, dass viele Unternehmen der Komplexität ihrer eigenen IT-Landschaft nicht mehr gewachsen sind. Wer den Überblick verliert, kann Attacken nicht umgehend analysieren, abwehren und Folgeschäden beseitigen. Hinzu kommt, dass wir immer häufiger sehen, dass die Angreifer sorgfältige Spionagetätigkeit im Vorfeld einer Attacke durchführen, um immer zielgerichteter anzugreifen.

ITS: Betrifft der Trend hin zu immer zielgerichteteren Angriffen nur große Unternehmen?

Christian Milde: Das ist ja das Trügerische. Betroffen sind nicht mehr nur große Unternehmen oder Konzerne, sondern auch der Mittelstand. Insbesondere der deutsche Mittelstand hat unter anderem als Zulieferer für Dritte interessante und streng vertrauliche Daten, die es zu schützen gilt. Hinzu kommt, dass kleinere Unternehmen häufig nur Mittel zum Zweck sind: Sie werden durch Kompromittierungen innerhalb der Lieferkette zum Einfallstor für große Konzernnetzwerke. Das Ergebnis solcher Cybersicherheitsvorfälle kann einerseits der Verlust

sensibler Daten sein, ein immenser Schaden für die eigene Reputation – stellen Sie sich vor, ein Automobilzulieferer würde eine Lücke in ein ihm angeschlossenes Konzernnetzwerk öffnen! Andererseits können sehr hohe Kosten entstehen, beispielsweise aus Bußgeldzahlungen durch die EU-Datenschutz-Grundverordnung. Insbesondere für KMU können diese Bußen die Existenz des Unternehmens bedrohen. Die durchschnittlichen Kosten eines Cybersicherheitsvorfalls in einem Unternehmen von bis zu 500 Mitarbeitern beliefen sich in den vergangenen zwölf Monaten durchschnittlich auf etwa 104.000 Euro.[1]

ITS: Unwissenheit oder fehlende Ressourcen – was ist der Grund für die Cyberanfälligkeit im Mittelstand?

Christian Milde: Das ist eine Mischung aus beidem. Oftmals denken mittelständische Unternehmen, dass sie zu klein sind, um für Cyberkriminelle interessant zu sein, oder aber wissen nicht, welchen Bedrohungen sie tatsächlich ausgesetzt sind. Hinzu kommt, dass ihre Ressourcen und Expertise hinsichtlich Cyberabwehr häufig stark limitiert sind, was den Umgang mit komplexen Bedrohungsszenarien erschwert und das Cyberrisiko für das gesamte Netzwerk signifikant erhöht – vor allem wenn es sich um zielgerichtete Attacken handelt. Aber auch die schiere Masse an Schadprogrammen und Angriffen macht Unternehmen zu schaffen. Um mit diesen professionell umzugehen, ist es wichtig, Lösungen und Services zu implementieren, die eine Identifizierung, Analyse und Vorfallreaktion ermöglichen und unterstützen. Das heißt, dass proaktive und präventive Komponenten immer wichtiger werden. Intelligente beziehungsweise integrierte Lösungen können hier helfen.

ITS: Intelligenter? Das heißt, es steht eine Künstliche Intelligenz dahinter?

Christian Milde: Ich würde hier nicht von Künstlicher Intelligenz im Sinne eines Systems, das kognitiv selbstständig agiert, sondern von Machine Learning sprechen wollen. Wichtig ist, dass moderne Unternehmen dank ihrer IT-Sicherheitslösungen auf die immer zielgerichteteren und auch intelligenteren Angriffe reagieren können. Unsere neueste Version für den Mittelstand (siehe Kasten) beispielsweise setzt auf Endpoint Detection and Response (EDR). Damit können insbesondere Unternehmen mit überschaubaren Security-Ressourcen einen professionellen Überblick und umfassende Informationen über etwaige Sicherheitsvorfälle erhalten – inklusive einer umgehenden Schadensanalyse sowie automatisierten Reaktionsoptionen.

ITS: Was genau ist denn EDR?

Christian Milde: Durch den Einsatz von EDR erhalten Unternehmen alle wichtigen Informationen zu schädlichen Aktivitäten in ihrem Netzwerk – einschließlich der Visualisierung von Angriffen, Ausbreitungspfaden und entsprechender Ursachenanalyse. Wird etwa eine verdächtige Datei – die nicht definitiv als bösartig eingestuft werden kann – identifiziert, leitet das EDR-System diese an eine nachgeschaltete Sandbox weiter. Dieses zusätzliche Sicherheitstool führt anschließend die verdächtige Datei automatisch in einer isolierten Umgebung aus und analysiert sie hinsichtlich ihres Gefährdungspotenzials. So kann festgestellt werden, ob es Anzeichen für ein mögliches Eindringen Unbefugter oder unzulässige Aktivitäten von Mitarbeitern oder Partnern gibt. In der Vergangenheit genügten Signaturen, Regeln und Einschränkungen aus, um solchen Angriffen zu begegnen. Im Zeitalter zielgerichteter und mehrstufiger Angriffe genügen solche Maßnahmen häufig nicht mehr. Moderne Lösungen agieren hier wesentlich intelligenter und proaktiver. Mit deren Hilfe erhalten auch Unternehmen mit geringen Ressourcen im Bereich Cybersicherheit einen professionellen Überblick und umfassende Informationen über etwaige Sicherheitsvorfälle. Ebenso eine umgehende Schadensanalyse sowie automatisierte Reaktionsoptionen. Dadurch werden potenziell negative Auswirkungen für Unternehmen minimiert.

Damit die EDR-Lösung aber richtig funktioniert, benötigt sie „darunter" eine gute Endpoint-Lösung; Unternehmen sollten also auf einen mehrstufigen Schutz setzen. Ein einfacher Endpoint-Schutz, wie er häufig noch eingesetzt wird, ist zwar wichtig, angesichts der heutigen Bedrohungslandschaft jedoch definitiv nicht mehr ausreichend. Moderne Schutzlösungen, wie Kaspersky Endpoint Security for Business,[2] ergänzen den Endpoint-Schutz um neue proaktive Ansätze wie Endpoint Detection and Response (EDR)-, Sandbox- und Cloud-Technologie. Mithilfe des integrierten Ansatzes können sich Unternehmen jeder Größe vor immer zielgerichteteren und sich ständig weiterentwickelnden Cyberattacken über alle Endgeräte hinweg schützen.

ITS: Vielen Dank für das Gespräch!

SECURITY-FLAGGSCHIFF

Die Kaspersky-Lösung Endpoint Security for Business für mittelständische und große Unternehmen integriert die Cloud-Management-Konsole, Kaspersky Endpoint Detection and Response (EDR), sowie Kaspersky Sandbox. Die Basiselemente der Lösung:

- Schutz von Endpunkten, Servern und Gateways
- Rationalisierung von Sicherheit, Management und Delegation
- Verstärkung von Systemen und Steigerung der Produktivität
- Verbesserte Angriffs- und Kompromittierungserkennung

Resultate:

- Zeitersparnis durch Automatisierung von Betriebssystem- und Software-Bereitstellungsaufgaben
- Senkung der Gesamtbetriebskosten und Komplexität
- Vereinfachung von Migrationsinitiativen

Quellen:

[1] *https://calculator.kaspersky.com/de/app/all-all-1000?eml=500&budget=0*

[2] *https://www.kaspersky.de/small-to-medium-business-security/endpoint-security-solution*

Wie Machine Learning und Graphdatenbanken gegen Cybercrime wirken

IMMER EINEN SCHRITT VORAUS

Sechs Monate dauert es im Durchschnitt bis ein Cyberangriff entdeckt wird – immer noch. Ein wesentlicher Grund dafür sind die raffinierten Methoden der Angreifer, mit denen sie ihre Ziele infiltrieren. Signaturbasierte Antiviren-Lösungen halten mit dem schnellen Tempo der Cyberkriminellen nicht mit – doch es gibt Abhilfe.

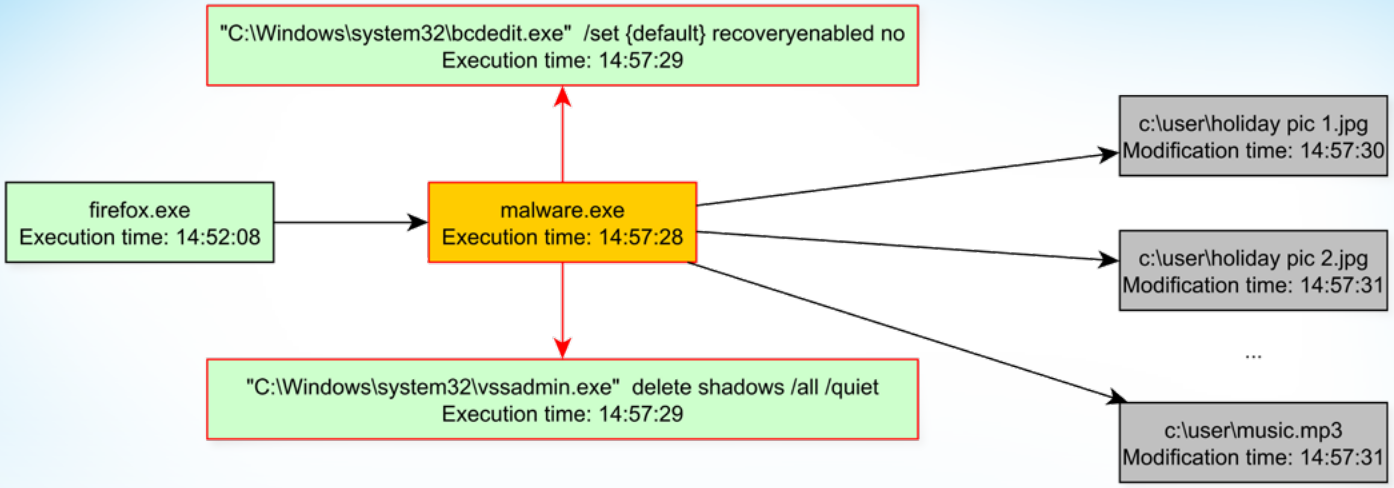
Cybercrime ist ein Milliardengeschäft. Um ihre Einnahmequellen zu erhalten, arbeiten Malware-Entwickler jeden Tag daran, dass Endpoint-Protection-Lösungen den schädlichen Code nicht entdecken. Denn eine Schadsoftwarewelle ist immer in dem Zeitraum effektiv, wenn Virus-Analysten noch keine Signaturen für das neue Sample geschrieben haben.

Um diesen Zeitraum möglichst lange andauern zu lassen, setzen Cyberkriminelle oft Packer ein. Damit verhüllen Sie den Schadcode und verändern etwa die Dateigröße und das Aussehen, um eine Erkennung durch eine Sicherheitslösung zu verhindern.

Um verhüllte Malware erkennen zu können, kommen häufig Machine-Learning-Technologien zum Einsatz – insbesondere, um die Reaktionszeit in der Analyse zu verkürzen. Dabei können etwa statische Indikatoren von Dateien herangezogen werden, um eine dynamische Analyse des Bedrohungspotenzials zu erstellen. Diese Indikatoren können etwa Werte wie die Hashsumme, bestimmte Zeichenketten, Codefragmente, die Dateigröße oder aber Header-Eigenschaften sein. Der Vorteil: Bei der Diagnose muss die Malware nicht erst ausgeführt werden, sondern kann ohne Gefährdung des Kundenrechners analysiert werden. Mit einem solchen Machine-Learning-Verfahren kann bekannte Malware also auch dann entdeckt werden, wenn sie geschickt ummantelt wurde.

DYNAMISCHE VIRENBEKÄMPFUNG

Nur bekannte und immer wieder neu verpackte Schadsoftware aufzuspüren, reicht allein nicht aus. Bei ihren Attacken setzen Kriminelle immer häufiger auf speziell zugeschnittene Malware



Angriff über verteilte Prozesse (Quelle: G DATA)

oder spezialisierte Schadsoftware, von der es nur wenige bekannte Samples gibt – eine Herausforderung für etablierte Analysesysteme. Oder sie fügen Standard-Tools, die auf jedem Windows-Rechner standardmäßig installiert sind, zu einer Angriffskette zusammen – wie etwa Powershell und Bitlocker. Experten sprechen hier von „Living-off-the-Land"-Angriffen.

SCHÄDLICHE PROZESSKETTEN ÜBERWACHEN

Solche aufwendigen Angriffe lassen sich mithilfe klassischer Signaturen kaum erkennen – mit Verhaltensüberwachung hingegen ist das aber sehr gut möglich. Das Erkennungsverfahren analysiert das Verhalten von Prozessen auf dem Computer und überwacht dabei etwa Änderungen im Dateisystem und in der Registry, insbesondere an verdächtigen Stellen wie dem Autostart-Ordner. Allerdings versuchen bestehende verhaltensbasierte Erkennungsansätze, möglicherweise bedrohliches Verhalten in numerische Werte zu übersetzen. Sie definieren also einen Grad von Schädlichkeit. Aber bei der Aggregation des numerischen Werts gehen notwendigerweise immer Informationen verloren, wodurch eine gewisse Unschärfe entsteht. Es lassen sich durchaus auch unbekannte Malware-Familien aufspüren. Die Technologie ist aber für Fehleinschätzungen anfälliger als andere Erkennungsverfahren. Das Problem: Entweder wird der Schwellwert für die Erkennung so hoch angesetzt, dass kaum noch Schadsoftware erkannt wird, oder der Schwellenwert wird so niedrig angesetzt, dass häufig Fehlalarme – sogenannte False Positives – auftreten.

False Positives kommen insbesondere wegen der Verwendung spezialisierter Software besonders häufig im Unternehmensumfeld vor. Dort sind sie gleichzeitig ein besonderes Problem. Ein bekanntes Phänomen: Wer unnütze Warnungen erhält, beginnt diese zu ignorieren. Im Unternehmensumfeld bedeutet das: Wenn die Beseitigung von Fehlalarmen zumindest in der Wahrnehmung mehr Kosten verursacht als das vermutete Kostenrisiko einer Infektion, wird die Verhaltensüberwachung oft einfach abgeschaltet.

MIT GRAPHEN ANGRIFFE NACHVOLLZIEHEN

Hier braucht es einen radikal anderen Ansatz, als bisherige Technologien zur Verhaltensanalyse. Anstatt die verdächtigen Aktionen in einem numerischen Wert zu aggregieren, werden die Prozesse in einem Graphen nachgezeichnet. Tatsächlich liegen die Verhaltensdaten in ihrer natürlichen Form als Graphen vor. Daher bietet sich der Einsatz von Graphdatenbanken an. Ein weiterer Vorteil: So lässt sich auch effizient mit den Daten und dem damit einhergehenden Datenwachstum umgehen. Es funktioniert einfach und schnell.

DEN NÄCHSTEN SCHRITT GEHEN

Der Graph im Bild zeigt exemplarisch einen Angriff über verteilte Prozesse. In diesem Fall wurde ein Nutzer von einem Angreifer

Bild: ©stockphoto-graf/stock.adobe.com

dazu gebracht, einen schädlichen Download aus dem Webbrowser zu öffnen, oder die Angreifer nutzten eine Sicherheitslücke mithilfe eines sogenannten Exploits aus. Beim schädlichen Download „malware.exe" handelt es sich um eine Ransomware, die Daten des Nutzers verschlüsselt und für die Entschlüsselung Lösegeld fordert.

Das zeigt sich darin, dass der Prozess erst eine Instanz des Systemwerkzeugs bcdedit öffnet, um die Wiederherstellungsfunktion von Windows zu deaktivieren. Gleichzeitig unterbindet ein weiteres Systemwerkzeug vssadmin das Anlegen von sogenannten Volume Shadow Copies, die genutzt werden können, um kürzlich versehentlich überschriebene Dateien wiederherzustellen. Im weiteren Schritt beginnt der Schadcode, Dateien im Nutzerverzeichnis zu verschlüsseln. Insgesamt ist dies ein typischer Weg für Ransomware. Aber die einzelnen Prozessschritte dieses Angriffs sehen separat betrachtet nicht verdächtig aus. Teilweise liegen zwischen den einzelnen Schritten auch mehrere Tage oder Wochen.

Prozesse lassen sich etwa als Baum darstellen. Ein übergelagerter Prozess startet mehrere Unterprozesse, die wiederum jeder mehrere untergeordnete Prozesse starten. So sind dann sowohl die Prozessstruktur als auch andere Informationen, wie etwa Dateizugriffe, in einem System gespeichert, sodass die Zusammenhänge nachvollziehbar sind. Die Abläufe bilden dann im Graphen die zentralen Knotenpunkte. Von diesen zweigen weitere Informationsstränge ab, wie etwa Dateizugriffe oder Anpassungen an der Registry. Der Vorteil der Graphdatenbank: Sie zeichnet ein vollständiges Bild auf, das Bedrohungen eindeutig erkennen kann. So lassen sich auch deutlich komplexere und weniger bekannte Kombinationen von Prozessen nachvollziehen. In einer großen Graphdatenbank, die täglich um mehrere Millionen Knoten und Kanten wächst, werden Informationen zu aktuellen Bedrohungen gesammelt und die Beziehungen verschiedener Samples und Indicators of Compromise analysiert. So entsteht ein umfassendes Bild der aktuellen Bedrohungslage. Selbst Schadsoftware, die jede einzelne Aktion auf einen eigenen Prozess verteilt, lässt sich so identifizieren. Damit können Analysten auch den Infektionsweg einer Malware sehr genau nachvollziehen.

DIE ZEIT ZURÜCKDREHEN

Gleichzeitig wird auch die Historie der Prozesskette gespeichert. Das ist ein großer Vorteil gegenüber dem alten System ohne Historie mit einem Scoringwert, der die Datei ausschließlich als gut oder böse einstuft. Graphdatenbanken ermöglichen daher auch „Retrospective Removal". Retrospective meint dabei die zeitliche Komponente. Das System prüft, was in der Vergangenheit passiert ist und kann damit jetzt auch Prozesse in Betracht ziehen, die schon lange nicht mehr existieren. Indicators of Compromise gibt es im Verlauf von Infektionen immer – sei es ein besuchter Server oder eine geöffnete Datei. Bis diese Indikatoren aber als schadhaft identifiziert werden, sind sie häufig auf dem betroffenen System nicht mehr verfügbar, weil etwa die Malware zum Beginn der Infektionskette zugehörende Dateien gelöscht hat. Im Graph bleiben diese Informationen erhalten und die verbliebenen Artefakte im System lassen sich trotzdem aufspüren. Denn mit dem Retrospective Removal lässt sich, ausgehend von einem Knoten, der bereits als schädlich erkannt wurde, der ursprüngliche Ausgangsprozess identifizieren und im Nachgang genauer untersuchen. Hat er etwa verdächtige Dateien heruntergeladen und weitere Programme gestartet? Dann liegen genügend Informationen vor, um die Infektion vollständig zu bereinigen. Solche komplexen Zusammenhänge bleiben gewöhnlichen verhaltensbasierten Technologien verborgen. Das bietet besonders dann Vorteile, wenn sich Malware zum Beginn der Infektion schlafen legt oder auf ein Kommando des Botnet-Operators wartet, aber noch keine schädlichen Aktionen durchgeführt hat.

FAZIT

Verhaltensanalyse ist seit vielen Jahren ein fester Bestandteil in den führenden Sicherheitslösungen. Anders als herkömmliche Verhaltensanalysen liefern Graphdatenbanken eine ganzheitliche Betrachtung. Sie spielen ihre Stärken aus, wenn schadhaftes Verhalten über mehrere Prozesse verteilt ist. So können auch Angriffe erkannt werden, die ganz ohne den Einsatz von Malware auskommen. ■

HAUKE GIEROW,
G DATA CyberDefense

Neue Standards und Biometrie sind der Schlüssel zu mehr digitaler Sicherheit im neuen Jahrzehnt

DIE TAGE DER PASSWÖRTER SIND GEZÄHLT

Für die Mehrheit der Verbraucher und Unternehmen sind Passwörter nach wie vor ein notwendiges Übel für den Zugang zu Konten und Daten. Passwörter haben aber ein großes Problem: Während sich die Technologie ständig verändert, weiterentwickelt und angepasst hat, ist die einfache Kombination aus Benutzername und Passwort gleichgeblieben und hat sich sowohl in Bezug auf Sicherheit als auch Benutzerfreundlichkeit als völlig unzureichend erwiesen.

Glücklicherweise ist es sehr wahrscheinlich, dass die Tage der Passwortnutzung gezählt sind. Schließlich sind diese von Natur aus schwach, leicht mit anderen Nutzern teilbar und einfach zu erraten (zum Beispiel ist „123456" laut einer Untersuchung des Hasso-Plattner-Instituts der Universität Potsdam[1] das häufigste Passwort). Passwörter können außerdem unkompliziert aus Datenbanken mit gestohlenen Informationen nach Datenlecks abgegriffen werden.

Unternehmen können diese Schwächen teilweise ausgleichen, indem sie komplexere Anmeldedaten durchsetzen, die aus einer Mindestlänge mit Zahlen und Sonderzeichen bestehen, aber die Sicherheit von Passwörtern hängt weitgehend vom Benutzer ab, und menschliches Versagen kann die Sicherheit schnell untergraben. Ein Mitarbeiter kann ein technisch sicheres Passwort haben, aber dann fährt er in den Urlaub und gibt sein Passwort an einen Kollegen weiter, um den Zugang zu seiner Arbeit während seiner Abwesenheit zu ermöglichen. Dies passiert überraschend häufig – in der jüngsten Untersuchung des Ponemon Institute „2020 State of Password and Authentication Security Behaviours Report"[2] geben 51 Prozent der Einzelnutzer und sogar 44 Prozent der IT-Fachleute zu, Log-in-Daten mit ihren Kollegen am Arbeitsplatz zu teilen.

Selbst wenn ein Arbeitgeber zum Schutz vor diesen Problemen Barrieren errichtet, ist dieser immer noch angreifbar, wenn er eine Datenpanne erleidet und die Passwörter seiner Mitarbeiter online weitergegeben werden. Nach einer groß angelegten Datenschutzverletzung ist zu erwarten, dass ein Unternehmen Passwörter zurücksetzen und seine Sicherheit überholen wird. Bei kleineren Angriffen passiert das aber häufig nicht: Nur 56 Prozent der vom Ponemon Institute für den erwähnten Report befragten Personen, die einen Phishing-Angriff, den Diebstahl von Anmeldedaten oder einen Man-in-the-Middle-Angriff (MitM) erlebt haben, gaben an, dass ihre Organisation die Art und Weise, wie Passwörter oder geschützte Firmenkonten verwaltet werden, seither geändert hat.

ZWEI-FAKTOR-AUTHENTIFIZIERUNG

Ein verbreiteter erster Schritt zur Verbesserung der digitalen Sicherheit ist die Implementierung von Zwei-Faktor-Authentifizierungsmethoden (2FA). Während grundlegende 2FA-Methoden – wie einprägsame Wörter oder SMS-Einmal-Passwörter („One Time Passwords", OTPs) – die Sicherheit über einen einfachen Benutzernamen

und ein Passwort hinaus verbessern, sind auch sie anfällig für moderne Phishing- und MitM-Angriffe. Tatsächlich werden telefonbasierte Angriffe immer häufiger, wobei „SIM-Swap"-Betrug heute ein wichtiger Faktor bei der Erleichterung organisierter Angriffe auf die Geräte der Ziele ist. Wenn OTPs per SMS verwendet werden sollen, ist es ratsam, dass diese ebenfalls durch einen separaten, externen Authentifikator abgesichert werden.

Phishing-Angriffe können auch verheerend wirksam sein – denn alles, worauf sich Cyberkriminelle verlassen müssen, um erfolgreich zu sein, ist einfaches menschliches Versagen. Spoofing-E-Mails sind auf dem Vormarsch, und hier können sich selbst die versiertesten Mitarbeiter dazu verleiten lassen, auf bösartige Links zu klicken oder mit Malware beladene Anhänge zu öffnen. Schließlich können Phishing-E-Mails, die vorgeben, von einer legitimen Quelle zu stammen, sehr überzeugend sein. Diese Angriffe werden von IT-Sicherheitsexperten als eine große Bedrohung angesehen, da ihnen nur ein einziger Mitarbeiter zum Opfer fallen muss, damit ein Täter legitime Zugangsdaten erhalten und sich lateral im Netzwerk bewegen kann.

Darüber hinaus nutzen vielbeschäftigte mobile Mitarbeiter gern öffentliches WLAN. Dies kann sie anfällig für MitM-Angriffe machen, da Hacker mit fingierten Access Points Verbindungen zu öffentlichen WLAN-Netzwerken fälschen. In diesen Szenarien loggen sich ahnungslose Benutzer ein und bieten so einem Hacker unwissentlich Zugang zu ihren Einwahldaten – es sei denn, ihre Verbindungen sind verschlüsselt. Angreifer sind dann auch in der Lage, die einfacheren 2FA-Methoden problemlos zu umgehen.

SMS-OTPs sind zudem als eine Ergänzung und nicht als Ersatz von Passwörtern zu sehen, und die Neueingabe von Codes von einem Gerät zum anderen ist umständlich und fehleranfällig. Dies hat sich als Hindernis für die Akzeptanz dieser Methoden erwiesen. Als zusätzliche Sicherheitsebene ist 2FA eine Grundvoraussetzung für alle Organisationen – aber es ist wichtig, daran zu denken, dass nicht alle 2FA-Methoden gleich effektiv sind. Die oben diskutierten Methoden sind anfällig für den Missbrauch durch Cybergegner, die immer geschickter mit Spoofing-Verbindungen umgehen können.

Mit Beginn des neuen Jahrzehnts ist es höchste Zeit, dass Unternehmen sich von der unbequemen und unsicheren Kombination von Benutzernamen und Passwörtern lösen, bekannte Schwachstellen mit einfachen 2FA-Methoden angehen und stattdessen auf anspruchsvollere Formen der Authentifizierung, einschließlich biometrischer Technologien konzentrieren.

NEUE GENERATION VON SICHERHEITSSTANDARDS

Organisationen können die Sicherheit und die Benutzerfreundlichkeit erhöhen, indem sie die Abhängigkeit von Passwörtern verringern und neue Standards einführen, die biometrische Technologien unterstützen. Die FIDO2-Spezifikationen befassen sich in der Tat mit allen Fragen, die mit der traditionellen Authentifizierung verbunden sind, und ermöglichen es den Benutzern, gängige Mittel zur einfachen Authentifizierung bei Online-Diensten sowohl mobil als auch in Desktop-Umgebungen zu nutzen.

So wurde beispielsweise WebAuthn, der erste weltweit akzeptierte Standard für die Web-Authentifizierung, 2019 eingeführt. WebAuthn ist eine Kernkomponente von FIDO2 und ermöglicht es Online-Diensten, die FIDO-Authentifizierung über eine Standard-Web-API zu nutzen, die in Browser und die zugehörige Web-Plattform-Infrastruktur eingebaut werden kann. WebAuthn wurde von führenden Unternehmen der Branche mitentwickelt sowie vom W3C genehmigt. Es bietet Websites, Diensten und Anwendungen eine verstärkte, benutzerfreundliche Multi-Faktor-Authentifizierung. Der Standard basiert auf Kryptografie mit öffentlichen Schlüsseln, wodurch die Notwendigkeit entfällt, Passwörter an einem zentralen Ort zu erstellen und zu speichern, wo sie anfällig für Datenverletzungen wären. Darüber hinaus bietet er den Anwendern eine breite Palette von Möglichkeiten zur Authentifizierung, wie externe Hardware-Sicherheitsschlüssel oder im jeweiligen Gerät eingebaute biometrische Sensoren und viele mehr.

Zusammenfassend lässt sich sagen, dass WebAuthn Unternehmen mehrere Optionen zur Auswahl anbietet, wodurch ein gewisser Grad an Personalisierung eingeführt und eine Abkehr von Benutzername/Passwörtern hin zu sichereren, benutzerfreundlicheren Sicherheitsmethoden gefördert wird. In Kombination mit biometrischer Technologie – die eine weitaus robustere Authentifizierungsmethode als die 2FA-Basistechnologie allein bietet und gleichzeitig ein nahtloses Benutzererlebnis ermöglicht – bietet FIDO2/WebAuthn einen deutlich besseren Schutz vor Bedrohungen wie MitM und Phishing-Angriffen. Tatsächlich hat Google erklärt, dass es seit der Einführung von FIDO-zertifizierten physischen Sicherheitstoken Anfang 2017 keine gemeldeten oder bestätigten Kontoübernahmen mehr gegeben hat.

Die Stärke der biometrischen Technologie liegt darin, dass sie sich auf die einzigartige menschliche Biologie, einen Fingerabdruck oder ein Gesicht stützt, die nicht leicht kopiert oder gehackt werden kann. Die Fingerabdrucktechnologie ist mittlerweile allgegenwärtig: Es ist die Art, wie viele Menschen ihr Telefon entsperren, sich in Anwendungen einloggen und mobile Zahlungen autorisieren. Die Erweiterung dieser Funktionalität zur Sicherung einer breiteren Palette von Geräten ist eine logische Fortsetzung dieser Technologie.

Biometrie und die Möglichkeiten, die FIDO2 und WebAuthn bieten, sind der Anfang vom Ende der Passwörter. Durch den Einsatz neuer Technologien, einschließlich der biometrischen Authentifizierung, werden Organisationen von einer weitaus höheren Sicherheit profitieren, während die Benutzer vom unseligen Passwortproblem befreit sind. ■

Quellen

[1] *https://hpi.de/pressemitteilungen/2019/die-beliebtesten-deutschen-passwoerter-2019.html*

[2] *https://www.yubico.com/authentication-report-2020/*

ALEXANDER KOCH,
VP Sales DACH und CEE
bei Yubico

Mapping eines mehrstufigen Botnetzes am Fallbeispiel Emotet

NETZWERKFORENSIK ALS ANGRIFFSSCHUTZ

2014 tauchte Emotet erstmals als reiner Banking-Trojaner auf. Heute nutzen Cyberkriminelle die dynamische Schadsoftware für Identitätsdiebstahl, Network Spreading, E-Mail-Harvesting sowie das Auslesen von Kontakten und Adressbüchern. Globale Netzwerkforensik ermöglicht es, die Struktur des Emotet-Botnetzes zu mappen und so Cyberattacken proaktiv entgegenzuwirken.

Emotet verbreitet sich heute typischerweise über bösartige Links sowie Anhänge in Phishing-E-Mails. Phishing-Kampagnen wurden bisher nur bei der Auslieferung von Emotet selbst beobachtet. Ein Rechner kann jedoch, sobald er durch Emotet kompromittiert wurde, mit weiteren Malware-Varianten infiziert werden. Die Emotet Command-&-Control-Infrastruktur (C2) ist komplex. Die Akteure betreiben permanent über hundert verschiedene C2-Server und aktualisieren im Laufe des Tages, welche C2-Server gerade aktiv sind. Die C2-Infrastruktur ist mehrstufig aufgebaut, was sie gegen Ausfälle einzelner C2-Server absichert.

TRAFFIC-ANALYSEN

Viele, die sich mit dem Tracking von Emotet beschäftigen, überwachen eingehende Spam-Mails und extrahieren das C2-Skript durch das Ausführen der Binärdatei in einer Sandbox-Umgebung. Das Black Lotus Lab (BLL) – das Threat Research und Operations Center des US-amerikanischen Kommunikationsdienstleisters CenturyLink – erweitert diesen Ansatz, indem es Verbreitungsmuster des Botnetzes beobachtet. Hierzu kommen – aufsetzend auf dem Seed bereits identifizierter C2-Server – Netflow-basierte Heuristiken zum Einsatz, um Bots, die mit der C2-Infrastruktur kommunizieren, zu erkennen. Kommuniziert eine IP-Adresse häufig mit einem C2-Server über dessen C2-Port, ist es sehr wahrscheinlich, dass es sich bei dieser IP-Adresse um einen Bot handelt.

Das BLL nutzt mehrere markierte C2-Server und einen Pool bekannter Bots, um neue C2-Server proaktiv zu identifizieren und lernt hierzu einen Machine Learning Classifier an. Da Bots sowohl mit vielen beliebten Hosts als auch C2-Servern kommunizieren, vertraut das Lab nicht nur auf das Ergebnis des Klassifizierungsverfahrens. Es emuliert das Protokoll, um einen Emotet C2-Server zu validieren, und stellt so sicher, dass die IP-Adresse korrekt reagiert. So konnten unbekannte C2-Server im Durchschnitt eine Woche früher als herkömmliche Tracker identifiziert werden.

Da die Emotet C2-Liste in der Binärdatei fest kodiert ist und sich die Infrastruktur des Botnetzes rasch ändert, müssen Code und C2-Liste, die auf einem infizierten Gerät ausgeführt werden, häufig aktualisiert werden. Wechseln Bots zu neuen C2-Servern, so registrieren dies Algorithmen und erkennen die neuen C2-Server. Mitunter gelingt dies bereits, bevor Bots über Spam-Kampagnen in einer neuen Binärdatei verteilt werden.

BOTS ALS C2-SERVER

Emotet setzt bei bestimmten Kompromittierungen ein Universal-Plug-&-Play-Modul (UPnP) ein, das es einem infizierten Gerät ermöglicht, als C2-Server zu agieren. Die meisten infizierten Geräte befinden sich hinter einem Router, der keine eingehenden Verbindungen zum infizierten Host zulässt. Das UPnP-Modul öffnet einen Port auf dem Router des Benutzers, der dann eingehende Verbindungen an einen Port auf dem infizierten Gerät weiterleitet. Über diese Bot C2-Server läuft nicht die eigentliche C2-Kommunikation, sondern sie dienen als Proxy

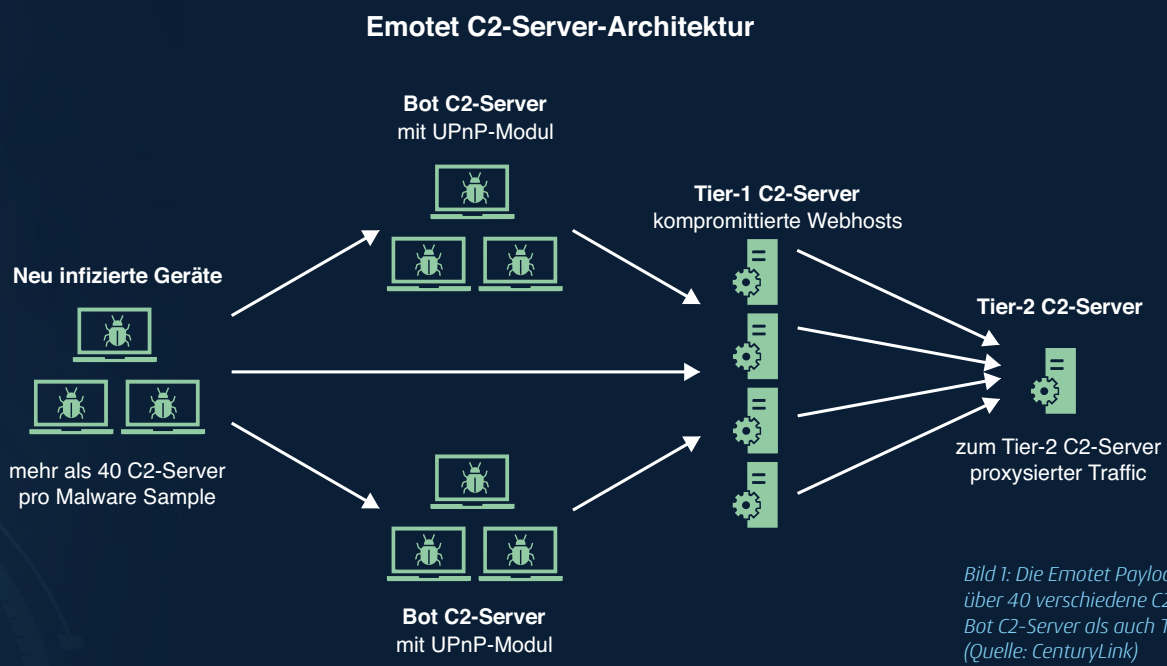


Bild 1: Die Emotet Payloads sind typischerweise über 40 verschiedene C2-Server verteilt, die sowohl Bot C2-Server als auch Tier-1 C2-Server beinhalten. (Quelle: CenturyLink)

und leiten die Kommunikation an einen Tier-1 C2-Server weiter. Im Gegensatz zu den Bot C2-Servern handelt es sich bei den Tier-1 C2-Servern typischerweise um kompromittierte Webhosts, die ihre C2-Kommunikation an einen Tier-2-Server weiterleiten. Die Emotet Payloads sind typischerweise über 40 verschiedene C2-Server verteilt, die sowohl Bot C2-Server als auch Tier-1 C2-Server beinhalten (Bild 1). Nachfolgend werden Tier-1 C2-Server als kompromittierte Webhosts und die Bot C2-Server als infizierte Geräte mit dem eingesetzten UPnP-Modul bezeichnet.

Seit Mitte 2018 beobachtete das Lab diese Verbreitungsstrategie allein auf Grundlage des Netzwerkverkehrs. Der Einsatz eines UPnP-Moduls wurde erstmals identifiziert, als validierte C2-Server begannen, mit anderen validierten C2-Servern über ihre C2-Ports zu kommunizieren.

Stellt man die C2-zu-C2-Kommunikation als Grafik dar, lassen sich zwei voneinander getrennte C2-Cluster erkennen (Bild 2). Die beiden Infrastrukturen werden typischerweise in Epoche 1 und Epoche 2 unterschieden.

Im Mai 2019 identifizierte und validierte das BLL Botnetz-Trackingsystem 310 C2-IP-Adressen. Im gleichen Monat wurden 208 dieser C2-Server auch über Bot-Finding-Heuristiken als Bots identifiziert. Die Analyse dieser identifizierten Bot C2-Server zeigt, dass die Mehrzahl der Bots in dynamischen Breitband IP-Bereichen gehostet wird. DNS-Einträge sowie das Scannen der Historie über Dienste wie Shodan belegten, dass es sich bei diesen IP-Adressen um solche von regulären Internetnutzern und nicht um kompromittierte Webhosts handelt. Die anderen 102 C2-Server sind Hosting-Provider. Scans zeigen, dass die meisten dieser IPs verwundbare Webhosts sind.

Über 80 Prozent der C2 IPs scheinen Bot C2-Server zu sein. Dies liegt wahrscheinlich daran, dass die Bot C2-Server häufiger als die kompromittierten Webhosts ihre IP-Adressen wechseln. Das Lab berechnete für beide C2-Server-Sets die durchschnittliche Dauer zwischen der ersten und letzten C2-Validierung. Für Tier-1 C2-Server betrug diese 38 Tage, für Bot C2-Server 17 Tage. Dies bedeutet, dass der C2-Server während dieses Zeitraums mindestens zweimal erreichbar war. Tier-1 C2-Server scheinen häufiger aktiv zu sein als Bot C2-Server. Kompromittierte Webhosts sind also viel häufiger online als Bot C2-Server. Die Bilder 3a und 3b (nächste Seite) zeigen die geografische Verteilung der Tier-1 C2-Server im Vergleich zu den Bot C2-Servern.

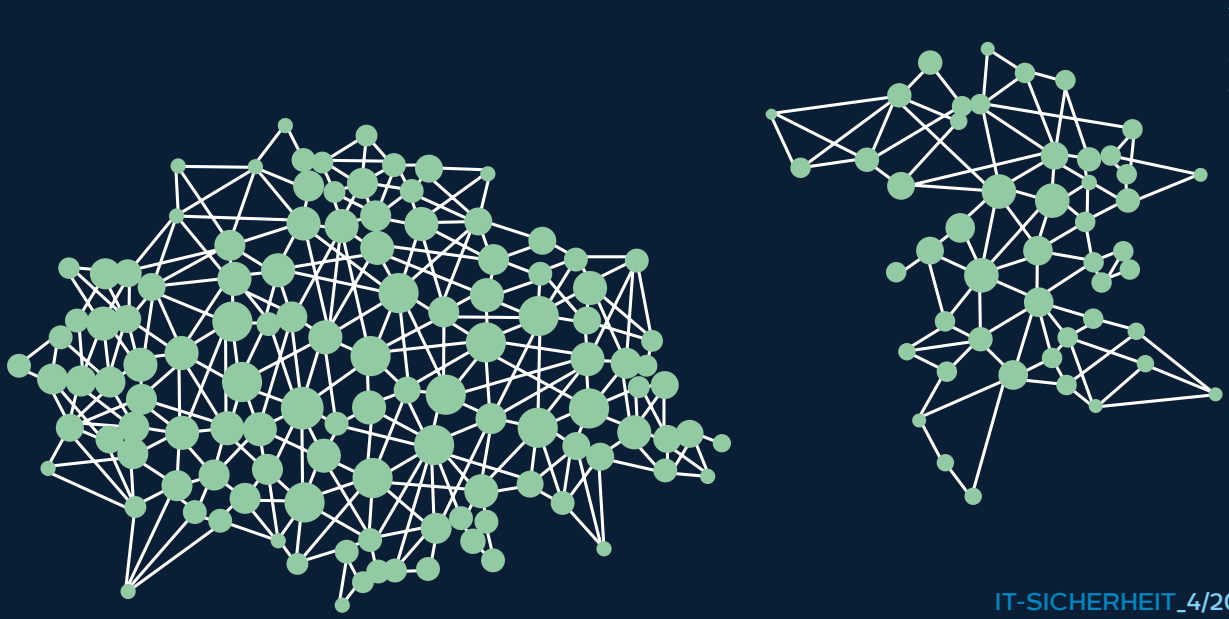


Bild 2: Stellt man die C2-zu-C2-Kommunikation als Grafik dar, lassen sich zwei voneinander getrennte C2-Cluster erkennen. (Quelle: CenturyLink)

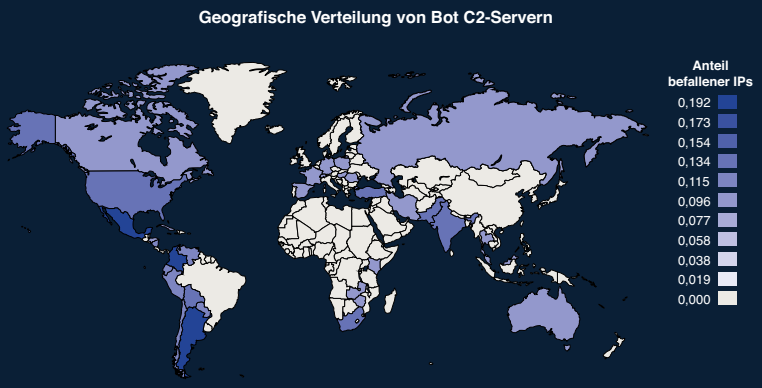


Bild 3a: Geografische Verteilung der Tier-1 C2-Server im Vergleich zu den Bot C2-Servern. (Quelle: CenturyLink)

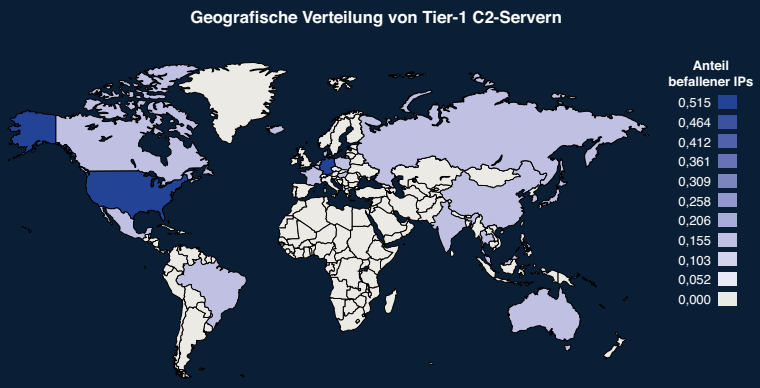


Bild 3b: Geografische Verteilung der Tier-1 C2-Server im Vergleich zu den Bot C2-Servern. (Quelle: CenturyLink)

IDENTIFIZIEREN VON TIER-2 C2-SERVERN

Das BLL ist in der Lage, Tier-2 C2-Server allein über Korrelationen im Netzwerkverkehr zu identifizieren. Frühere Ansätze zur Identifizierung von Tier-2 C2-Servern erforderten einen direkten Zugang zu einem Tier-1 C2-Server mithilfe eines Hosting-Providers. Da die Tier-1 C2-Server ihren Traffic auf einen Tier-2 C2-Server lenken und es für jede Epoche typischerweise einen Tier-2 C2-Server gibt, lassen sich die Tier-2 C2-Server durch die Analyse der Gemeinsamkeiten zwischen den Tier-1 C2-Servern und mit wem diese kommunizieren, identifizieren. Jeder Tier-2 C2-Server kommuniziert nur mit Tier-1 C2-Servern aus derselben Epoche. Dies bestätigt die anhaltende Trennung der beiden Epochen. Das Lab beobachtet hierbei nicht den gesamten Traffic der Tier-2 C2-Server, jedoch die Struktur des Traffics von Tier-1 C2-Servern, der das Netzwerk passiert.

MALWARE-DISTRIBUTION-AS-A-SERVICE

Emotet ist dafür bekannt, weitere Malware-Varianten, wie Trickbot, IcedID, QakBot, Gookit, Dridex und andere, zu verbreiten. Mithilfe der zuvor beschriebenen Bot-Heuristiken lassen sich Emotet-Infektionen mit den weiteren Malware-Varianten – basierend auf der Kommunikation mit dem infizierten Bot C2-Server – korrelieren. So kommunizierten im Untersuchungszeitraum in den letzten 30 Tagen mehr als 17.000 unterschiedliche Bot-IP-Adressen, die mit Emotet C2-Servern in Verbindung stehen, auch mit Trickbot C2-Servern. Trickbot zählt zu den häufigsten Malware-Varianten, die von Emotet verbreitet werden. Die am zweithäufigsten mit Emotet korrelierende Malware-Familie im Untersuchungszeitraum war Azorult. Es wurden zudem etwa hundert Bots identifiziert, die mit Danabot in Verbindung stehen.

Es zeigte sich, dass validierte C2-Server mit anderen Malware-Familien kommunizieren (Bild 4). Nachdem wie beschrieben die validierte C2-Liste in Tier-1 C2-Server und Bot C2-Server unterschieden wird, stellte sich heraus, dass dies lediglich bei Bot C2-Servern der Fall ist. Dies könnte bedeuten, dass die Emotet Akteure Payloads anderer Malware-Varianten auf den gleichen Geräten verbreiten, die sie über das UPnP-Modul als C2-Server nutzen. In der Regel möchten Botnetz-Betreiber ihre C2-Infrastruktur von anderen Malware-Familien frei halten. Nicht so im Fall von Emotet. Von den 208 bereits erwähnten Bot C2-Servern waren acht Prozent auch mit Trickbot infiziert. Die Vermutung liegt nahe, dass Bot C2-Server erst später für andere Zwecke genutzt werden sollen. Das Lab hat jedoch auch C2-Server validiert, die am selben Tag sowohl von Emotet als auch Trickbot genutzt wurden.

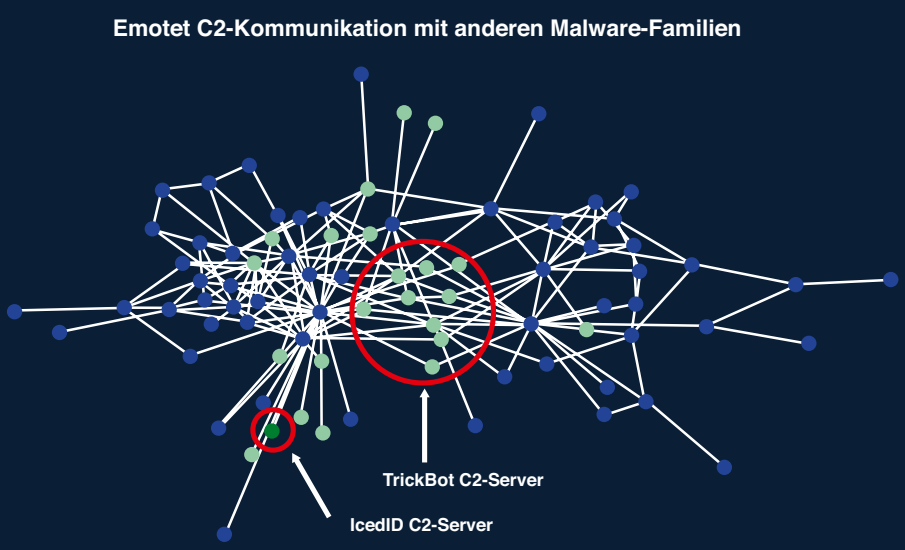
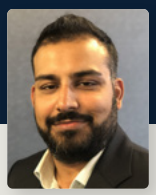


Bild 4: Validierte C2-Server kommunizieren mit anderen Malware-Familien. (Quelle: CenturyLink)

FAZIT

Die C2-Infrastruktur von Emotet lässt sich, unabhängig von Malware-Samples, mittels automatisiertem Botnet-Tracking allein über das Netzwerkmonitoring verfolgen. Bot-Heuristiken können zudem vorhersagen, mit welchen Malware-Varianten Emotet korreliert, und helfen, den Malware-Distribution-as-a-Service-Ansatz von Emotet zu verfolgen. ■



AATISH PATTNI,
Director Security Solutions EMEA bei CenturyLink

NEU

Live-Webinare und Videos

In unserer Webinarthek finden Sie aktuelle Webinar-Termine und Aufzeichnungen zum Thema IT-Sicherheit.

Jetzt anschauen: **www.webinarthek.de**

DATAKONTEXT

IT-RECHT KOMMENTAR

**SCHUSTER, FABIAN/
GRÜTZMACHER, MALTE**

IT-Recht - Kommentar

1. Auflage, 2020,
2.175 Seiten,
Verlag Otto Schmidt, Köln,
ISBN 978-3-504-56106-2,
249,– €
(Quelle: Otto Schmidt)

Die Informationstechnologie ist in den letzten Jahrzehnten, zunächst getrieben durch Großrechner, Server, PCs, lokale Netze und Internet, zuletzt durch Embedded Systems, Smartphones und das Cloud-Computing, zum Rückgrat der modernen Informationsgesellschaft geworden. Kommerzielle Standard- und Open Source-Software schöpfen das Potenzial der leistungsstarken IT-Infrastruktur, zunehmend unterstützt durch Technologien wie Big Data und KI. Eine datengetriebene Wirtschaft ist so heute bereits Realität. Zugleich entwickeln sich immer wieder und immer rasanter neue Anwendungsmöglichkeiten und neue Technologien, und zunehmend hält Digitalisierung auch in klassische Branchen und Industrien Einzug.

Thematisch ist der vor diesem Hintergrund nun in der „blauen Reihe" bei Otto Schmidt erschienene – und überdies auch online (über Beratermodul IT-Recht) erhältliche – Kommentar eine Neuheit. Er bündelt die Querschnittsmaterie IT-Recht in nur einem Band. Dabei liegt der inhaltliche Schwerpunkt auf dem IT-Recht im klassischen Sinne, abgedeckt werden rechtliche Aspekte in Sachen Hard- und Software, ebenso wie die Bereiche IT-Outsourcing und neue Technologien. Mit Konzentration auf diese Felder werden sowohl nationale als auch europäische IT-rechtsrelevante Vorschriften und Themen aus 25 Gesetzen, Verordnungen, Verwaltungsvorschriften und Open-Source-Lizenzen erläutert: BGB, DS-GVO, Dual-Use-Verordnung, GeschGehG (Gesetz zum Schutz von Geschäftsgeheimnissen), GWB, GVO (Gruppenfreistellungsverordnungen), HGB, StGB, UrhG und zahlreiche weitere Rechtsquellen.

Dabei erweist sich IT-Recht als interdisziplinäres Recht. Anders als in vielen anderen Rechtsgebieten, wie etwa der Telekommunikation (TKG) oder bei den Mediendiensten (TMG beziehungsweise MDStV), sind die relevanten Aspekte des IT-Rechts nicht in einem Gesetzeswerk gebündelt, sondern erstrecken sich über Teilbereiche ganz unterschiedlicher Gesetze. Der Aufbau des vorliegenden Werks orientiert sich dementsprechend als klassischer Kommentar an der Gesetzessystematik und erschließt das gesamte IT-Recht von der Norm her. Der alphabetische Aufbau nach Regelwerken erleichtert das Arbeiten hiermit.

Über die Kommentierungen der IT-rechtsrelevanten Regelungen nationaler und europäischer Rechtsakte sowie internationaler Lizenzen, auch die Berücksichtigung der Rechtsprechung auf neuestem Stand, gewinnt der Nutzer des Werks ein Mehr an Rechtssicherheit in diesem interdisziplinären Rechtsgebiet. Das Werk untergliedert sich dabei in drei Teile:

1. Teil – EU-Recht: AEUV | DS-GVO | Dual-Use VO | F&E-GVO | Rom I-VO | Rom II-VO | TT-GVO | Vertikal-GVO;

2. Teil – Nationales Recht: AWG | BGB | GeschGehG | GWB | HGB | InsO | KWG | PatG | ProdHaftG | ProdSG | StGB | UrhG | WpHG;

3. Teil – Besondere Vertragsbedingungen: ASL (Apache License) | BSD (Berkeley Software Distribution) | GPLv2 (GNU General Public License)| GPLv3 | LGPLv2.1 (GNU Lesser General Public License) | LGPLv3.

Die beiden Kommentarherausgeber sind bereits langjährig im IT-Recht tätig und durch zahlreiche einschlägige Veröffentlichungen als Experten ausgewiesen. Auch finden sich als weitere Autoren im Werk namhafte Praktiker, überwiegend aus der Anwalt- und Fachanwaltschaft, versammelt.

Mit seinem umfassenden Überblick über das klassische IT-Recht ist die Neuerscheinung sowohl für Studierende, vornehmlich der Informatik, der Rechts- und Wirtschaftswissenschaften, als auch für Praktiker in den gesamten Feldern der Informationstechnologie äußerst geeignet und zu empfehlen. ■

DR. THOMAS P. STÄHLER,
Justiziar und Datenschutzbeauftragter,
Frankfurt am Main

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**

Sicherheitsfragen in Zeiten des Remote Work:

IT-EXPERTEN ANTWORTEN

Mit der Corona-Krise, die Mitarbeiter weltweit an den heimischen Schreibtisch schickte, kamen auf Security-Verantwortliche in Unternehmen über Nacht neue Herausforderungen zu. Wie sie die Situation wahrgenommen und in den Griff bekommen haben, darüber gibt eine aktuelle, im Mai 2020 durchgeführte Umfrage von Bitglass zu den Auswirkungen der Covid-19-Pandemie auf die IT Security, Aufschluss. Umgesetzt wurde die Studie, für die 413 IT-Security-Experten aus einem Querschnitt von Unternehmen verschiedener Größen und Branchen befragt wurden, in Zusammenarbeit mit der Information Security Community.

www.itsicherheit-online.com/Bitglass-2020-04

Anurag Kahol,
CTO, Bitglass
(Foto: Bitglass)

Sicherung von Remote-Arbeitskräften auf Grundlage einer Zero-Trust-Sicherheits-Strategie

VERTRAUEN SIE NIEMANDEM!

Die Belegschaft vieler Unternehmen arbeitet derzeit noch immer fast vollständig von Zuhause aus. Das hat natürlich Einfluss auf die Sicherheitsstrategie eines Unternehmens, da die Mitarbeiter nun nicht mehr geschützt durch die Unternehmenssicherheit Zugang zu verschiedenen internen Unternehmensressourcen haben. Für Unternehmen ist es jetzt natürlich besonders wichtig, ihre Endbenutzer zu schützen, da ein kompromittiertes Konto potenziell zu größeren Sicherheitsverletzungen führen kann, wenn es nicht frühzeitig in der Angriffskette erkannt und gestoppt wird. Da Sicherheit für Unternehmen auch in diesen besonderen Zeiten oberstes Gebot ist, sollte ein Zero-Trust-Modell die Basis einer sinnvollen Sicherheitsstrategie sein.

www.itsicherheit-online.com/Exabeam-2020-04

Egon Kando,
Area Vice President Of Sales Central, Southern and Eastern Europe bei Exabeam
(Foto: Exabeam)

Was Unternehmen beim Datenschutz beachten müssen

ZUSAMMENARBEIT MIT FREELANCERN

Freelancer haben viele Vorteile: Unternehmen müssen keine Sozialabgaben für sie entrichten, sie sind flexibel einsetzbar, oft auf ein bestimmtes Fachgebiet spezialisiert und können auch kurzfristig anfallende Projekte umsetzen. Firmen, die mit freien Mitarbeitern kooperieren, können es jedoch nur selten vermeiden, personenbezogene Daten mit ihnen zu teilen. An dieser Stelle kommt der Datenschutz ins Spiel: Was müssen die Beteiligten hier alles beachten – und wer trägt im Einzelfall die Verantwortung für die Datenverarbeitung?

www.itsicherheit-online.com/DataGuard-2020-04

Maren Wienands,
Projektmanagerin bei DataGuard
(Foto: DataGuard)

Worauf mittelständische Unternehmen bei der Einbindung von quelloffener Software achten müssen

OPEN SOURCE

EIN RISIKO, ABER BEHERRSCHBAR

Open-Source-Komponenten machen heute den Löwenanteil vieler Anwendungen aus – und sind für den Mittelstand oft die einzige Möglichkeit, mit dem Entwicklungstempo der Software-Branche Schritt zu halten. Bei allen Vorteilen, die Open Source bietet, müssen sich Entwickler aber der Risiken bewusst sein, die Open-Source-Code birgt. Dabei erweisen sich moderne Software-Composition-Analysen als wertvolle Helfer.

Der Mittelstand ist das Rückgrat der deutschen Wirtschaft und sollte eigentlich nachhaltig von der Digitalisierung profitieren. Die Praxis zeigt aber, dass sich mittelständische Unternehmen, vom Kleinbetrieb bis zum Hidden Champion, schwertun, diese Potenziale auszuschöpfen – einfach, weil es ihnen oft an Fachpersonal fehlt, um ihre kritischen Prozesse stabil und sicher in die digitale Welt zu überführen. Immerhin umfassen moderne Business-Anwendungen häufig Millionen von Code-Zeilen – für kleine Teams oft ein kaum zu bewältigender Aufwand.

Open-Source-Software verspricht, Abhilfe zu schaffen: Open-Source-Komponenten machen es kleinen Entwicklerteams leicht, einfache, gängige oder repetitive Funktionalitäten in Topqualität und mit minimalem Aufwand aus bestehenden Libraries zu übernehmen. Selbst programmiert werden dann nur die Spezialfeatures und USPs der jeweiligen Software – und natürlich die Schnittstellen, die den Open-Source- und den selbstentwickelten Code verzahnen.

In der Praxis haben qualifizierte Entwickler so die Möglichkeit, sich ganz auf kreative Lösungen und Features für ihre Kunden zu konzentrieren. Auf diese Weise können kleine, aber kreative und engagierte Teams mitunter weitaus größeren Wettbewerbern den Schneid abkaufen. Wobei auch Großunternehmen die Open-Source-Komponenten zu schätzen wissen – immerhin lassen sich damit die Entwicklungskosten nachhaltig senken.

WAS BEI VERWENDUNG VON OPEN SOURCE BESONDERS ZU BEACHTEN IST

Kein Wunder also, dass Open-Source-Code heute überall ist: Über 30 Millionen Entwickler sind inzwischen an Community-Plattformen wie GitHub angebunden und tragen von dort Open-Source-Code in ihre Unternehmen. Nach Expertenstudien verwenden 95 Prozent aller Unternehmen selbst in geschäftskritischen Anwendungen inzwischen Open Source. Doch angesichts dieser Vorzüge unterschätzen viele von ihnen die Risiken und Gefahren, die mit dem Einsatz von Drittanbietercode einhergehen.

1. Herausforderungen im Bereich Sicherheit

Wie jede Software sind auch Open-Source-Komponenten angreifbar. Jedes Jahr werden über 3.000 neue Schwachstellen in Open-Source-Code entdeckt, und für viele davon sind schon wenige Tage nach Bekanntwerden erste Exploits verfügbar. Gerade bei weit verbreiteten Komponenten steht Angreifern so ein einfacher Angriffsvektor offen.

Hinzu kommt, dass Unternehmen schon mit Blick auf die Code-Menge keine Möglichkeit haben, die Qualität der von ihnen verwendeten Open-Source-Komponenten manuell zu überwachen. Sie wissen auch nicht, ob sich der Autor an etablierte Secure Coding Practices gehalten hat, und die Untersuchung des Codes mit vorhandenen Code-Analyse-Lösungen ist unpraktikabel. Auch gängige Faustregeln („Immer den aktuellsten Patch verwenden.“) bieten im Bereich Open Source keinen Schutz: Natürlich schließen viele Patches kritische Sicherheitslücken, aber es gibt umgekehrt auch unzählige Beispiele, in denen neue Versionen neue Angriffspunkte öffneten.

Welche Gefahr von Sicherheitslücken in Open-Source-Komponenten ausgeht, illustriert anschaulich das Beispiel von Heartbleed (CVE-2014-016), einer Schwachstelle in einer Open-Source-Bibliothek (openSSL), welche die Basis aller sicheren Kommunikation darstellt.

2. Herausforderungen im Bereich Lizenzierung

Die Verwendung von Open-Source-Code ist aber nicht nur mit Blick auf die Sicherheit riskant – auch die heterogenen Lizenzierungsmodelle von Open-Source-Software bergen Gefahren: Grundsätzlich können Autoren von Open-Source-Projekten frei entscheiden, welchen Regeln die Verwendung ihrer Software unterliegt – und nutzen diese Freiräume auch kreativ aus, wie die populäre Beerware License („Wer den Code nutzt, muss dem Autor ein Bier ausgeben.“) zeigt.

In der Praxis übernehmen die meisten Open-Source-Devs aber eines der vielen Hundert etablierten Modelle. Diese lassen sich in zwei Kategorien einteilen: regulierte Copyleft-Lizenzen, wie die GNU General Public License (GPL) sowie deutlich liberalere Permissive Licences. Während Letztere in der Praxis meist unproblematisch sind, unterliegt die Verwendung von Copyleft-lizenziertem Quellcode oft rigorosen Auflagen – von der Nennung des Urhebers bis hin zur Verpflichtung, jegliche Weiterentwicklungen der Software ebenfalls lizenzfrei bereitzustellen. Bettet ein Entwickler Copyleft-lizenzierte Komponenten in seine proprietäre, kommerzielle Software ein, kann das Unternehmen also im Worst Case die Rechte an seinen Eigenentwicklungen einbüßen.

3. Herausforderungen im Bereich Community

Und noch einer dritten Gefahr sollten sich Unternehmen bei der Verwendung von Open-Source-Code bewusst sein: Sie haben keinerlei Garantie, dass die Distribution, die sie in ihre Business-App eingebettet haben, von der Community dauerhaft gepflegt wird. Lässt der Urheber sein Projekt einschlafen – und hört beispielsweise auf, Updates und Security-Patches bereitzustellen – stehen die Entwickler vor einem unangenehmen Dilemma: Entweder übernehmen sie selbst die Pflege der Software, was für kleine Teams kaum zu stemmen ist, oder sie ersetzen die verwendeten Open-Source-Bestandteile durch eigene Entwicklungen – auch das ist in vielen Fällen keine realistische Option.

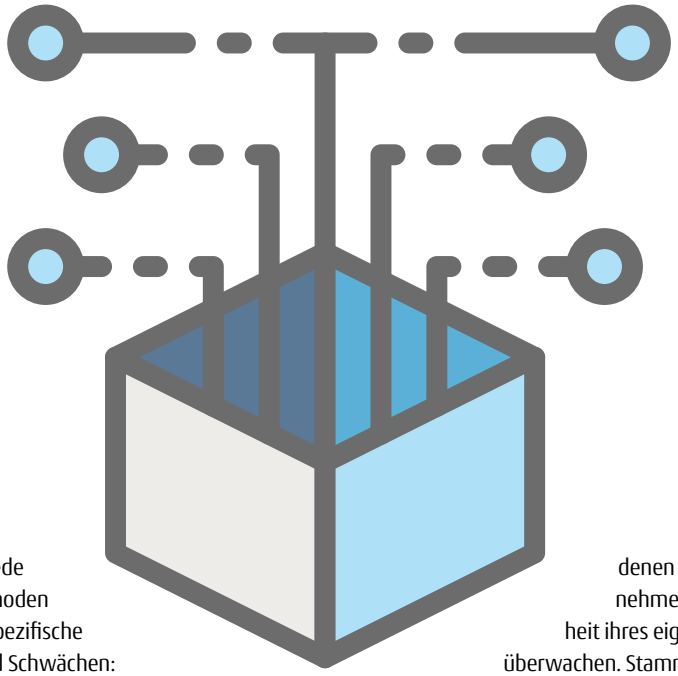
Es gibt aber auch gute Nachrichten: Alle drei Herausforderungen sind heute mit sogenannten Software-Composition-Analysen, oder kurz SCA, technisch lösbar. Der Begriff SCA bezeichnet dabei dedizierte Analyse-Lösungen, die Open-Source-Komponenten und Drittanbieter-Libraries in Software identifizieren und mit Blick auf ihr Risikopotenzial bewerten. Dabei deckt die aktuelle Generation der SCA-Systeme sowohl Security- als auch Lizenzierungsrisiken ab – und berücksichtigt auch das Schadenspotenzial, das von disruptiven Community-Aktivitäten ausgeht.

SCA ALS TEIL DES ENTWICKLUNGSPROZESSES

Ähnlich wie die statische Code-Analyse (SAST) setzt auch die SCA im Idealfall bereits ganz am Anfang des Software Development Lifecycles (SDLC) an. So lassen sich potenziell gefährliche Open-Source-Komponenten schnellstmög-

WAS EINE SOFTWARE-COMPOSITION-ANALYSIS-LÖSUNG KÖNNEN SOLLTE

- Erkennung, Identifizierung und Bewertung von Security-, Lizenz- und Community-Risiken
- Zuverlässige Analyse, automatische Priorisierung der Ergebnisse und Minimierung der False Positives
- Einbindung etablierter Datenbanken bekannter Open-Source-Schwachstellen
- Enge Integration in die DevOps-Prozesse und den SDLC
- Anleitung der Entwickler bei der Behebung der Schwachstellen
- Schnittstellen zu vorhandenen Package Managern, Build-Tools, Code-Repositories und Issue-Management-Lösungen
- Unterstützung interner und externer Anforderungen – etwa mit Blick auf die Einbindung in die Security Policy oder die Erfüllung von Branchenstandards
- Integration und Korrelation mit vorhandenen SAST-, DAST- und IAST-Plattformen
- Individuelle Policy für den Umgang mit Schwachstellen



lich identifizieren – und je schneller sie erkannt werden, desto geringer ist der Aufwand für die Behebung. Die Analyse erfolgt dabei in der Regel in drei Schritten:

1. Erkennung von Open-Source-Komponenten:
Im ersten Schritt gilt es, den Open-Source-Code in den Anwendungen zuverlässig zu lokalisieren. Je nach SCA-Lösung kommen hierbei unterschiedliche Verfahren zum Einsatz – etwa Signatur-Scanner, Snippet-Scanner oder Package Manager. Jede dieser Methoden hat dabei spezifische Stärken und Schwächen: Manche liefern schnelle, aber unter Umständen lückenhafte Ergebnisse. Andere sind deutlich akkurater, lassen sich wegen der längeren Analysedauer aber schlecht in schnell getaktete DevOps-Prozesse integrieren. Daher geht der Trend in der Praxis hin zu SCA-Lösungen, die mehrere Verfahren kombinieren.

2. Identifizierung der Komponenten:
Als nächstes muss die SCA-Lösung die erkannten Open-Source-Komponenten akkurat identifizieren. Dabei greifen die meisten SCA-Lösungen auf vorhandene Open-Source-Datenbanken zu. Diese liefern neben grundlegenden Informationen oft auch granulare Angaben zur Distribution, Herkunft, Version oder anderen Metadaten.

3. Risikobewertung:
Im dritten und letzten Schritt gilt es, das Risikopotenzial der Komponenten zu bewerten – und zwar sowohl mit Blick auf die Security als auch auf die Lizenzierung. Auch bei dieser Einstufung greifen die meisten SCA-Lösungen auf etablierte Datenbanken, wie die US-amerikanische NVD (National Vulnerability Database), zu und bewerten das Risikopotenzial dann nach fest definierten Standards, wie CVSS2.0 oder CVSS3.0. Auf dieser Basis können die Unternehmen anschließend individuell regeln, wie mit welchem Risikolevel umzugehen ist.

SCA-Lösungen schaffen also die Voraussetzungen für einen rundum sicheren Einsatz von Open-Source-Komponenten – und sind damit eine sehr gute Ergänzung zu den statischen und interaktiven Code-Analyse-Lösungen (AST), mit denen viele Unternehmen die Sicherheit ihres eigenen Codes überwachen. Stammen SCA und AST aus einer Hand, lassen sich die Ergebnisse beider Technologien darüber hinaus korrelieren, um eine noch höhere Analyse-Genauigkeit zu erreichen.

FAZIT

Moderne Software-Entwicklung ist ohne Open-Source-Komponenten undenkbar, und daran wird sich auch in Zukunft nichts ändern. Entwickelnde Unternehmen sind damit mehr denn je auf leistungsfähige SCA-Technologien angewiesen, die eine granulare Risikoanalyse und Bewertung der Open-Source-Komponenten sicherstellen. Für eine erfolgreiche Implementierung ist dabei entscheidend, dass die Lösung nahtlos in vorhandene Entwicklertools integrierbar ist, interne und externe Standards unterstützt und zeitnah handlungsrelevante Ergebnisse liefert. Auf diese Weise können sich Software-Unternehmen zuverlässig vor potenziell riskanten Open-Source-Libraries schützen, Schäden durch intransparente Lizenzierungsmodelle verhindern – und dauerhaft von den Vorzügen der Open-Source-Bewegung profitieren. ■

JÜRGEN KERSTAN,
Channel Manager DACH
bei Checkmarx

ENTERPRISE SECURITY FÜR KMU

Westcon präsentiert maßgeschneiderte Check Point-Bundles für SMB zum attraktiven Preis

Mit den SMB-Appliances von Check Point profitieren kleine und mittelständische Betriebe jetzt von vielen innovativen Security-Technologien, die bislang Konzernen und Fortune-100-Unternehmen vorbehalten waren. Bei Value-Added Distributor Westcon gibt es die Lösungen jetzt in maßgeschneiderten Bundles zum besonders attraktiven Preis.

Die von Check Point und Westcon gemeinsam entwickelten SMB-Bundles bieten zuverlässigen Rundumschutz „Out-of-the-Box" – inklusive automatisch generierter Security-Policies und integrierter Best Practices von Check Point. Die kompakten Appliances ermöglichen es KMUs, individuelle Risikokategorien zu definieren, ausgehend davon unerwünschte Anwendungen und Inhalte zu blockieren sowie bandbreitenintensive Dienste einzuschränken. Wichtig für kleine Unternehmen ohne dediziertes Security-Team: Die Systeme unterstützen die gleiche leistungsfähige Threat Intelligence wie die Enterprise-Appliances von Check Point – und lassen sich einfach und schnell installieren, konfigurieren und managen.

„Kleine und mittelständische Unternehmen geraten immer öfter in das Visier von Cyberkriminellen. Sie haben deren professionellen Attacken aber nur wenig entgegenzusetzen, da es an Ressourcen, Tools und Awareness fehlt", erklärt Robert Jung, Managing Director bei Westcon DACH. „Unsere mit Check Point entwickelten SMB-Pakete sind exakt auf die Anforderungen kleiner Unternehmen zugeschnitten. Sie bieten den gleichen zuverlässigen Schutz und die gleichen innovativen Technologien, die wir aus dem Enterprise-Segment kennen – erfordern aber kein tiefes Know-how und binden kein eigenes Kapital. So bleiben KMU jederzeit geschützt und stellen die Einhaltung aller gesetzlichen Cybersecurity-Vorgaben sicher."

Bei Fragen zur Vermarktung, Konfiguration oder Administration der Systeme steht den Unternehmen Westcon als erfahrener Value Added Distributor jederzeit zur Seite – und hilft ihnen, das Potenzial der Lösungen voll auszuschöpfen.

Wenn Sie mehr darüber wissen möchten, wie Sie Ihre Daten, Anwender und Systeme zuverlässig schützen und von innovativen Security-Technologien profitieren können, wenden Sie sich einfach an die Check Point Business Unit von Westcon. Das Expertenteam steht Ihnen jederzeit unter **checkpoint.de@westcon.com** zur Verfügung.

CHECK POINT SECURITY CHECK-UP

Möchten Sie wissen, wie sicher die von Ihnen betreuten Netzwerke wirklich sind? Dann auf zum Security Check-Up! Dabei stellt Westcon Ihnen ein Security Gateway zur Verfügung, das den Datenverkehr im gesamten Netzwerk analysiert und untersucht. Damit keine Netzwerkkonfigurationen und -änderungen notwendig sind sowie Ausfallzeiten vermieden werden, wird der Netzwerk-Datenverkehr an ausgesuchten Punkten gespiegelt. Hierfür wird der Monitor-Port genutzt, der mit einem Test Access Point (TAP) oder einem Mirror-Port (bzw. Span-Port) auf dem Netzwerk-Switch verbunden ist. Bei der Auswertung zusammen mit einem unserem Security Consultants bekommen Sie einen kompletten Report – inklusive der genutzten Anwendungen, der dazugehörigen Bandbreiten und aller erkannten Security-Events. ■

Mehr dazu hier

ÜBER WESTCON-COMSTOR

Westcon-Comstor ist ein weltweit führender Technologiedistributor mit einem Jahresumsatz von über drei Milliarden US-Dollar. Das Unternehmen, das in über 70 Ländern vertreten ist, bringt führende IT-Hersteller mit einem Netzwerk etablierter Technologiepartner, Systemintegratoren und Service Provider zusammen – und schafft auf diese Weise echten Mehrwert und neue Business-Chancen. Aufsetzend auf tiefe Marktkenntnis, umfassendes technisches Know-how und mehr als 30 Jahre Erfahrung in der Distribution ist Westcon-Comstor hervorragend positioniert, um die Weichen für das erfolgreiche Wachstum der Hersteller und der Partner zu stellen. Westcon-Comstor ist mit zwei Marken auf dem Markt vertreten: Westcon und Comstor.

Westcon Comstor

Fallstricke der DS-GVO

UNTERSCHÄTZTE HERAUSFORDERUNG

Seit zwei Jahren treibt die DS-GVO schon ihr Unwesen in der deutschen beziehungsweise europäischen Unternehmenslandschaft. Die ersten saftigen Bußgelder und Kontrollen der Datenschutzbehörden lassen erahnen, in welche Richtung sich der Datenschutz in den kommenden Jahren entwickeln wird. Zwar muss nicht jedes Unternehmen einen Datenschutzbeauftragten bestellen, die vorgeschrieben Dokumentationspflichten und alles was damit zusammenhängt, müssen trotzdem umgesetzt werden. Als Knackpunkt bei der Umsetzung der DS-GVO stellen sich für viele Unternehmen die Nachweispflichten nach Artikel 5 und 24 heraus.

Die Musik spielt bei der Accountability, also den vielfältigen Verpflichtungen, die korrekte Umsetzung der DS-GVO nachzuweisen", sagt Christian Volkmer, geschäftsführender Gesellschafter bei Projekt 29. „Verfahrensverzeichnis oder Dokumentation von AV-Verträgen stehen nicht so im Fokus der Aufsichtsbehörden, wie von vielen angenommen. Die praktische Umsetzung und Einführung der Accountability-Themen stehen bei den Behörden verstärkt auf dem Prüfstand."

Nach Art. 5 Abs. 1 DS-GVO muss der Verantwortliche nicht nur dafür sorgen, dass die Prinzipien der DS-GVO eingehalten werden, sondern er muss nach Abs. 2 die Einhaltung auch nachweisen. In der englischen Fassung der Verordnung taucht hier der Begriff „Accountability" auf. Das lässt sich mit Rechenschaftspflicht ins Deutsche übersetzen. Die Nachweispflicht findet sich dann in Art. 24 Abs. 1, der besagt, dass der Verantwortliche den Nachweis dafür erbringen können muss, „dass die Verarbeitung gemäß dieser Verordnung erfolgt".

„Viele Vorschriften der DS-GVO zum konkreten Schutz personenbezogener Daten hatten sich ja in ähnlicher Form auch schon im Bundesdatenschutzgesetz gefunden. Die Rechenschafts- und Nachweispflichten aber sind komplett neu", so Volkmer. Und der Experte erläutert die Tragweite an einem einfachen Beispiel, dem Recht auf Löschung nach Art. 17.

Bisher, sagt Volkmer, sei dem Gesetz genüge getan gewesen, wenn auf Verlangen des Betroffenen die Daten tatsächlich gelöscht wurden. Nach DS-GVO folgen aus Art. 17 aber vier Dokumentationspflichten:

Erstens muss der Prozess als solcher definiert und beschrieben werden: Was müssen die Mitarbeiter tun, wenn eine Kunde die Löschung seiner Daten verlangt?

Zweitens muss der Datenverarbeiter nachweisen können, dass die Mitarbeiter tatsächlich wissen, was sie tun müssen. Nötig ist der Nachweis einer Schulung, eine schriftliche Handlungsanweisung oder ein ähnliches Dokument.

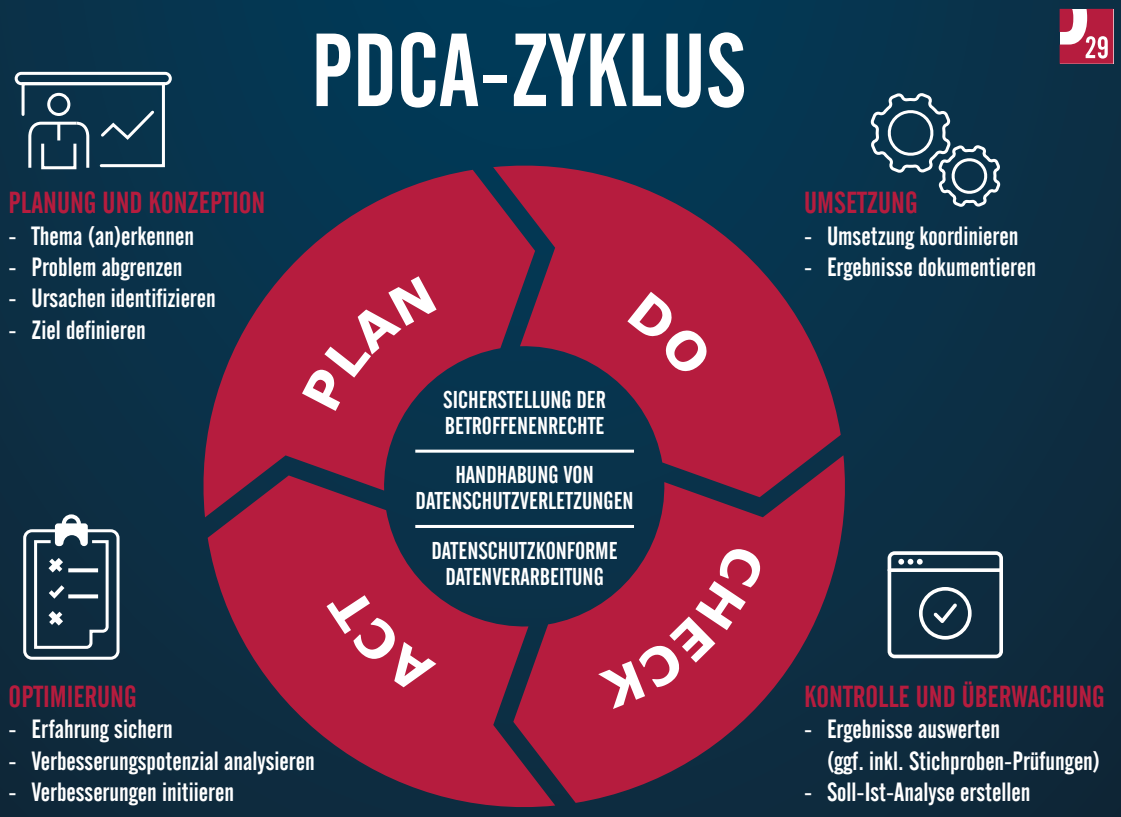
Drittens muss die konkrete Umsetzung dokumentiert werden: Wann und wie ging die Bitte um Löschung ein, wann und wie wurde sie umgesetzt?

Viertens muss dokumentiert sein, dass der Prozess Löschersuchen in regelmäßigen Abständen überprüft wird und welche Ergebnisse die Überprüfung gezeigt hat.

„Stellt sich bei der Prüfung heraus, dass beim Löschen alles klappt und wird das dokumentiert, dann ist alles gut", sagt Volkmer. „Wenn nicht, dann gilt es nachzujustieren und zu dokumentieren: Welche Fehler sind aufgefallen, wie wurde der Prozess geändert, wie wurden die Mitarbeiter geschult und so weiter?"

DATENSCHUTZ ALS DYNAMISCHER PROZESS

Das Datenschutzhandbuch, in dem einmal für alle Zeiten steht, wie mit personenbezogenen Daten umgegangen wird, reicht also nicht aus. „Das erfüllt höchstens ein Drittel des insgesamt geforderten Umfangs", so Volkmer. Die Dokumentation



Das Datenschutzmanagement muss zyklisch nach der PDCA-Methode aktualisiert werden. (Quelle: Projekt 29)

muss ständig fortgeschrieben und ergänzt werden, denn Datenschutzmanagement nach DS-GVO bedeutet einen dynamischen Prozess.

Wie im Qualitätsmanagement nach ISO 9001 oder im Informationssicherheits-Management nach ISO 27001 gefordert, muss auch das Datenschutzmanagement zyklisch nach der PDCA-Methode aktualisiert werden:

„P" steht für das englische „plan", also planen. Dieser Schritt entspricht noch am ehesten dem gewohnten Verfahrensverzeichnis. Als Verfahren wird aufgeschrieben, was unter bestimmten Umständen passieren muss.

„D" steht für „do", also die konkrete Umsetzung des Verfahrens.

„C" meint „check", die Überprüfung, ob das Verfahren tatsächlich in allen Fällen korrekt umgesetzt worden ist. Fällt dabei auf, dass doch nicht alles korrekt läuft, gilt

„A" oder „act": Der im ersten Schritt gefasste Plan, das Verfahren, muss korrigiert werden.

RECHENSCHAFTSPFLICHT BEDEUTET UMKEHR DER NACHWEISLAST

Die Brisanz des Themas Rechenschaftspflicht lässt sich aus den Aktivitäten der Landesdatenschutzbehörden ableiten. Im Herbst 2018 hat das Bayerische Landesamt für Datenschutzaufsicht (BayLDA) zwei Prüfverfahren zum Stand der Umsetzung der DS-GVO aufgesetzt (siehe: www.lda.bayern.de/de/kontrollen). Eins untersucht kleine und mittelständische Unternehmen ab 100 Mitarbeitern. „Der dreiseitige Fragebogen hat es in sich", sagt Volkmer. 20 Themengebiete fragt die Aufsichtsbehörde ab und verlangt zu fast jedem Einzelnen davon, die Dokumentation vorzulegen.

Im erläuternden Text auf seiner Website weist das BayLDA ausdrücklich darauf hin: „Die DS-GVO verlangt vom Verantwortlichen, dass die Einhaltung der DS-GVO nachgewiesen wird (Art. 5 Abs. 2 DS-GVO). Diese ‚Rechenschaftspflicht' stellt vom Grundsatz her eine ‚Nachweislast-Umkehr' dar, was bedeutet, dass die Einhaltung der gesetzlichen Anforderungen der Aufsichtsbehörde bei einer Kontrolle dargestellt werden muss."

BEISPIELE FÜR BEREICHE, FÜR DIE ACCOUNTABILITY BESONDERS RELEVANT SIND

Aus Sicht von Projekt 29 ergibt sich die Accountability nach DS-GVO für 20 verschiedene Themenbereiche, einige mit höherer, andere mit geringerer Priorität. Hier eine Auswahl.

Erteilung der Einwilligung, Art. 7 DS-GVO

Einwilligungen zur Datenverarbeitung müssen nicht nur eingeholt werden, es muss auch dokumentiert werden, dass sie für jeden einzelnen Fall vorliegen. Transparente Information, Kommunikation und Modalitäten für die Ausübung der Rechte des Betroffenen, Art. 12 DS-GVO.

In einem Register muss hinterlegt sein, wo überall Erklärungen zum Umgang mit personenbezogenen Daten veröffentlicht sind. Das können Websites, Infoflyer, Verträge, der Onlineshop

> **„Die Musik spielt bei der Accountability, also den vielfältigen Verpflichtungen, die korrekte Umsetzung der DS-GVO nachzuweisen“**

CHRISTIAN VOLKMER,
geschäftsführender Gesellschafter
bei Projekt 29.

und andere Stellen mehr sein. Ändert sich etwas in der Datenschutzerklärung, muss die Organisation wissen, wo überall sie das anzupassen hat.

Datenschutz durch Technik, Art. 25 DS-GVO

Hierbei geht es um die technischen und organisatorischen Maßnahmen (TOM), die im Verarbeitungsverzeichnis aufgeführt sein müssen. Neu ist, dass in einer Risikobewertung abgeschätzt werden muss, ob die ergriffenen TOM dem Risiko eines Datenabflusses angemessen sind – was wiederum dokumentiert sein muss.

Umsetzung der Speicherbegrenzung, Art. 5 DS-GVO

Ist dokumentiert, welche Daten im Unternehmen vorliegen, wo sie abgespeichert sind, wann sie im Einzelnen gelöscht werden müssen? Zum Löschkonzept hat das BayLDA mit dem Thema Archive und Back-ups eine weitere kniffelige Frage in seinen Erhebungsbogen aufgenommen. Denn ein Unternehmen muss sicherstellen und dokumentieren, dass gelöschte Daten nicht über den Umweg eines zurückgespielten Back-ups wieder zum Leben auferstehen.

Umsetzung der Sicherheit der Verarbeitung, Art. 32 DS-GVO

„Platz 1 der IT-Sicherheitsbedrohungen stellen heute Computersysteme dar, die nicht regelmäßig upgedatet werden“, weiß Christian Volkmer. Das Management von Sicherheits-Updates, die Schulung der Mitarbeiter und regelmäßige Überprüfungen und Anpassungen der Maßnahmen müssen dokumentiert werden.

Umgang mit Datenschutzverletzungen, Art. 33 DS-GVO

Nach dem alten deutschen Recht lag eine Datenschutzverletzung vor, wenn tatsächlich Daten abgeflossen waren. Die DS-GVO betrachtet es schon als Verstoß, wenn nicht auszuschließen ist, dass Daten abgeflossen sein könnten.

Jeder Verdachtsfall muss dokumentiert werden. „Mitarbeiter müssen sich also eventuell selbst kleinerer Schlampereien zum Beispiel auf der Dienstreise bezichtigen. Das Thema ist sensibel. Damit sie das tun, brauchen sie ein hohes Bewusstsein, wie wichtig Datenschutz und das Datenschutzmanagement inzwischen sind“, sagt Volkmer.

Darstellung der Meldepflicht an Aufsichtsbehörden, Art. 33 DS-GVO

Das BayLDA fragt: „Gibt es einen (dokumentierten) Prozess, um Datenschutzverletzungen innerhalb 72 Stunden (auch an Wochenenden/Feiertagen) bei der zuständigen Aufsichtsbehörde zu melden?“ Dazu bedarf es eines definierten Prozesses, der geschult und regelmäßig überprüft werden muss – samt seiner Dokumentation.

Dokumentation von Audits

Dabei reichte früher die Bestätigung, dass ein Audit stattgefunden hat. Heute will die Behörde es laut ihrem Fragebogen genauer dokumentiert haben: „Sind … die letzten (zwei) Audits des Datenschutzbeauftragten vorhanden und besitzen diese eine einheitliche Prüfmethodik?“ „Wer sich intensiv mit dem Thema beschäftigt, sieht schnell ein: Mit Word-Dokumenten oder Excel-Files kann weder das Management nach dem PDCA-Zyklus noch die Dokumentation so gelingen, dass die Behörde bei einer Prüfung zufrieden wäre“, gibt sich Volkmer überzeugt.

Sein Unternehmen hat deswegen Privacysoft entwickelt, eine Online-Software, die Verantwortliche an die Hand nimmt und Schritt für Schritt durchs Datenschutzmanagement leitet. Nach den ersten Erfahrungen mit den neuen Rechenschafts- und Nachweispflichten legt Projekt 29 einen besonderen Schwerpunkt auf das entsprechende Modul in Privacysoft. „Wir haben es so weiterentwickelt, dass Verantwortliche genau wissen, was zu tun ist und den Fragebogen des BayLDA nicht mehr fürchten müssen.“, sagt Volkmer. ■

MANFRED GERBER,
Leiter Privacysoft

E-LEARNING
IT-SICHERHEIT

DATENSICHERHEIT

Geschulte Mitarbeiter machen den Unterschied!

Schulen Sie alle Mitarbeiter via E-Learning in den Grundlagen der IT-Sicherheit und erhöhen Sie so den Schutz für Ihre Daten.

- ✓ Moderation in TV-Studioqualität
- ✓ moderne Didaktik
- ✓ Dauer: 45 Minuten
- ✓ praxisnah und interaktiv
- ✓ auch in englischer Sprache verfügbar

Jetzt informieren: datakontext.com/eLearning

UNIVADO

DATAKONTEXT

DS-GVO – EU-Kommission zieht Bilanz

KMU IM NACHTEIL?

Trotz dieser Probleme wurden auch die Erfolge der Datenschutz-Grundverordnung insgesamt betont, denn es seien neue globale Grundsätze geschaffen worden, die neue Möglichkeiten für einen sicheren Datenverkehr ermöglichen. Dies komme sowohl Einzelpersonen als auch Unternehmen zugute. So trage die DS-GVO dazu bei, dass sich globale Datenschutzstandards ihr anpassen – sie werde oftmals als Bezugspunkt genutzt, etwa in Ländern wie Chile, Südkorea, Brasilien oder Japan. Bezogen auf Betriebe und im speziellen kleinere und mittelständische Betriebe – noch Probleme bei der Compliance haben, nicht überraschend. Schließlich erfordert die Verordnung eine umfassende Überprüfung, wer Zugriff auf welche Daten hat, wo sich die regulierten Daten befinden sowie die Fähigkeit, erforderliche Sicherheitsaudits und kontinuierliche Kontrollen durchzuführen. Eine lückenlose Compliance ist hier essenziell, denn die DS-GVO sieht für gravierende Verstöße ein Mindestbußgeld von 20 Millionen Euro oder vier Prozent des weltweiten Jahresumsatzes vor.

Die Komplexität, die mit Unternehmens-Identity, der DS-GVO-Compliance und dem Datenschutz verbunden ist, bedeutet: Der effektivste und sicherste Weg besteht darin, so viele Identity- und Access-Management-Tools sowie Sicherheitsauditprozesse wie möglich zu automatisieren. Schließlich ist Automatisierung unerlässlich, wenn Prozesse regelmäßig wiederholt werden müssen und Reaktionen in Echtzeit erfolgen sollen. Durch die Automatisierung der Zugriffsbereitstellung und -entfernung können Unternehmen die Sicherheitskontrollen verschärfen und

Gut zwei Jahre nach Inkrafttreten der DS-GVO zieht die EU-Kommission Bilanz. Eine Erkenntnis: Die Compliance für kleine und mittlere Unternehmen (KMU) stellt sich häufig noch als schwierig dar. So haben KMU vor allem steigende Kosten im Rahmen von Mitarbeiterschulungen und externen Beratungsleistungen zu beklagen. Laut der Kommission ist dies für viele von ihnen eine Belastung. Die Möglichkeit, diese kleineren und mittleren Firmen von der DS-GVO auszunehmen, bestehe nicht, denn auch diese verarbeiten teilweise personenbezogene Daten in großem Umfang.

KMU hält die Kommission fest, dass die Verordnung für gleiche Bedingungen im Wettbewerb mit anderen Firmen sorge – auch solche, die ihren Sitz außerhalb der EU haben, aber hier tätig sind. Weiterhin trage das vermehrte Bestreben um mehr Datenschutz dem Wunsch der Kunden Rechnung, die diesen Punkt heute immer häufiger in ihre Kaufentscheidung mit einbeziehen. Wenn die DS-GVO-Compliance auf transparente Weise erreicht werde, stärke dies das Vertrauen zwischen Betrieben und Endkunden.

Dass auch Großkonzerne Probleme bei der Einhaltung der Richtlinie haben, zeigte kürzlich eine Nachricht aus Frankreich. So muss Google in Frankreich wegen undurchsichtiger Privatsphäre-Einstellungen und der fehlenden rechtlichen Grundlage für personalisierte Werbung die höchste Strafe zahlen, die europäische Aufsichtsbehörden im Rahmen der Verordnung bisher verhängten. Konkret geht es um eine Summe von 50 Millionen Dollar.

Zunächst einmal ist die Tatsache, dass Unternehmen jeglicher Größe – vor allem aber Gerade weil die Nicht-Einhaltung für viele Betriebe geschäftskritisch sein kann, sollten diese neben organisatorischen Maßnahmen auch die Nutzung technischer Lösungen in Erwägung ziehen. Denn: Die DS-GVO erfordert nicht nur, dass Organisationen Least-Privilege-Rechte für PII-Daten (Persönlich identifizierende Informationen) von EU-Bürgern integrieren – sondern auch, dass sie in der Lage sind, Verstöße gegen die Richtlinie sofort zu erkennen und zu beheben. Firmen haben maximal 72 Stunden Zeit, um eine Datenpanne im Zusammenhang mit Kundendaten zu melden – nachdem sie selbst von der Verletzung Kenntnis erlangt haben – und müssen Einzelpersonen benachrichtigen, wenn nachteilige Auswirkungen festgestellt werden.

Darüber hinaus muss die Person im Unternehmen, die für die Datenverarbeitung verantwortlich ist, den betrieblichen Kontrolleur sofort benachrichtigen, wenn er von einem Datenabfluss der personenbezogenen Informationen erfahren hat. Deshalb ist es unerlässlich, firmeninterne Sicherheitslücken umgehend zu erkennen und zu schließen.

gleichzeitig ihre Geschäftseffizienz steigern. So geschützt können Betriebe jeglicher Größe ein neues Zeitalter des Datenschutzes beginnen und empfindliche Geldbußen im Rahmen der Verordnung verhindern, die gerade für kleinere Betriebe nicht selten geschäftskritisch sein können. ■

VOLKER SOMMER,
Area Vice President DACH and Eastern Europe

Perspektiven für das Identity and Access Management (IAM)

VERWALTUNG VON IDENTITÄTEN UND BERECHTIGUNGEN

Unternehmen nutzen eine Vielzahl von Identitäten, um Geschäftsprozesse ausführen zu können. Diese Identitäten können unterschiedlicher Natur sein. Unternehmen benötigen interne Mitarbeiter wie auch externe Dienstleister – sie alle müssen eindeutig zuordenbar sein. Identitäten müssen zudem über ihren gesamten Lebenszyklus verwaltet werden. Das gilt sowohl für den logischen Zugriff auf Informationen, als auch für physische Zutrittsberechtigungen. In der Praxis wird beides aber in der Regel separat verwaltet. Mehr Effizienz versprechen Systeme, die beide Bereiche unter einem gemeinsamen Dach vereinen.

Identitäten werden beispielsweise benötigt, um Berechtigungen für Zutritt, Zugang und Zugriff zu definieren. Hier kann zunächst eine Verifikation einer Person mit einem Ausweisdokument erfolgen. Aber auch Informations-, Kommunikations-, Sicherheits- und Gebäudetechnik sowie Informationen selbst bestehen aus Objekten, die eindeutig zuordenbar sein müssen. Neudeutsch wird bei diesem Themenkomplex gern vom Asset Management, frei übersetzt der Verwaltung der Aktiva (im betriebswirtschaftlichen Sinne) eines Unternehmens gesprochen.

Wer also die Vermögenswerte nutzen möchte, muss ein berechtigtes Interesse nachweisen. In vielen alltäglichen Prozessen ist dies einfach umsetzbar. Personen müssen die ihnen zugewiesene Tätigkeit ausführen und Ressourcen entsprechend nutzen können. Gleiches gilt für die dazu erforderliche Informationstechnik (IT) und operative Technologie (OT) sowie die notwendigen Applikationen.

Einheitliche Prozesse für die Gesamtheit aller Dienste und Services sind in Unternehmen oft nicht durchgängig etabliert. Beispielsweise organisiert sich die Sicherheitsabteilung losgelöst von der Unternehmens-IT oder das Facility Management orientiert sich im Bereich Gebäudeautomation völlig eigenständig.

Anforderungen aus Compliance-Vorgaben, die für das gesamte Unternehmen gelten, werden dabei auf unterschiedliche Art und in unterschiedlicher Tiefe umgesetzt. Beispielsweise sind Vorgaben von Gesetzgebern, Aufsichtsbehörden oder Versicherungen regelkonform und revisionssicher umzusetzen. Revisionssicherheit bedeutet hierbei, Wirtschaftsprüfern, Auditoren und gegebenenfalls auch Richtern nachweisen zu können, regeltreu gehandelt zu haben. Hierzu dienen als probates Hilfsmittel unter anderem Maßnahmen zur Informationssicherheit.

GETRENNTE WELTEN

Personaldaten werden typischerweise in eigens dafür entwickelten IT-gestützten Systemen verwaltet. Sollen Zugang und Zugriff von Personen organisiert werden, kommen oft weitere Technologien ins Spiel. Bislang lief es im informationstechnischen Bereich meist so, dass Personen Rollen mit gewissen Rechten zugewiesen wurden, um Dinge auf IT-Systemen, Anwendungen und Verzeichnissen auszuführen. Hierbei erfolgt gewissermaßen die Verwaltung des „Logical Access". In der Sicherheitstechnik hingegen kennt man ein solches Vorgehen kaum, da die Systeme und die Nutzerkreise häufig zu klein sind.

Zugangs- und Zugriffsrechte werden hier oft autark und lokal verwaltet. Wird ein Verzeichnisdienst genutzt, dann allenfalls für vereinzelte Systeme der Sicherheitstechnik. So stellt es sich als eine große bis unüberwindbare Herausforderung dar, auf vielen verschiedenen Systemen, die von unterschiedlichen Anwendern betreut werden einheitlich, regelkonform sowie revisionsfest zu agieren.

Ein sogenanntes Identity and Access Management System (IAMS) setzt sich wie ein Regenschirm über alle genannten Verzeichnisdienste. Mit einer Schnittstelle zur Personalverwaltung werden aus den dort vorhandenen Daten Identitäten, denen wiederum dienst- und serviceübergreifend Rollen und somit Berechtigungen zugewiesen werden können. Über Schnittstellen zu den darunter liegenden Verzeichnisdiensten erfolgt der Datenaustausch. Moderne IAM-Systeme bieten die Möglichkeit, Audit-Reports zu generieren und Workflow-Prozesse einfach und transparent zu generieren. Getreu dem WYSIWYG-Prinzip (What you see is what you get!).

Im Bereich des „Physical Access" sind ebenfalls Softwareprodukte am Markt erhältlich, die genau dies machen. Hier werden ebenfalls per Schnittstelle zur Personalverwaltung aus den dort vorhandenen Daten Identitäten erzeugt: Diese Identitäten können nun einem Rollenkonzept folgen, innerhalb dessen Berechtigungen für den Zutritt zu Gebäuden, Bereichen und Räumen zugeordnet werden. Die Berechtigungen werden an die darunter liegenden verschiedenen elektronischen Zutrittskontrollsysteme weitergegeben.

Die Realisierung der erforderlichen Schnittstellen sollte nun idealerweise nicht über „Reverse Engineering" von proprietären Datenstrukturen und -protokollen erfolgen, sondern über offene und standardisierte Programmierschnittstellen, wie REST API, SOAP oder WSDL, mit textbasierter Übertragung auf XML oder CSV-Basis.

WARUM EINE VERSCHMELZUNG VON LOGISCHEM ZUGANG UND PHYSISCHEM ZUTRITT SINNVOLL WÄRE

Identitäten und Berechtigungen könnten künftig auf einer einzigen dedizierten Plattform verwaltet werden. Es könnten dann einerseits Berechtigungen für den physischen Zutritt entweder mittels elektronischer Zutrittskontrolle (online/offline) oder auch mit mechanischen Schlüsseln organisiert werden. Andererseits kann der logische Zugang zu IT-Systemen genauso wie der logische Zugriff auf Informationen geregelt werden. Dieser Ansatz stellt eine ganzheitliche Strategie im Sinne von Regeltreue und einer entsprechenden Dokumentation dar.

Zum Nachweis der Identität von Systemen ist eine Public Key Infrastruktur (PKI) erforderlich, um Zertifikate integer für Verschlüsselung und Authentisierungsmechanismen erzeugen zu können. Die Einführung eines IAMS stellt somit eine große Aufgabe dar. Die erforderlichen Ressourcen betreffen hierbei nicht nur Hard- und Software. Ein großer Teil der Aufgabe besteht darin, die geltenden Compliance-Regelungen und die etablierten Arbeitsabläufe abzubilden, bei Bedarf zu optimieren und in der Software zu implementieren. Im Anschluss daran sollte es möglich sein, die Prozesse an einer Stelle durch die jeweils fachverantwortlichen Mitarbeiter transparent und nachvollziehbar zu bearbeiten, die Datenhaltung insbesondere von personenbezogenen Informationen zu minimieren, eine schnelle Nachweiserbringung von Vorgaben zu erbringen und dennoch eine Produktivitätssteigerung zu erreichen.

Ist ein solches IAMS inklusive PKI etabliert, können nach wie vor physische Ausweise mit kontaktbehafteten und kontaktlosen Leseverfahren für Zutritt, Zugang und Zugriff sowie weitere Dienste genutzt werden. Genauso ist es jedoch möglich, andere Authentifizierungslösungen, wie Token, webbasierende Lösungen oder auch das Smartphone, einzusetzen. ■

Mehr dazu hier

DIPL.-ING. (FH, NACHRICHTENTECHNIK) LUTZ ROSSA,
Sicherheitsberater bei VZM mit den Spezialgebieten Leitstellen, Videotechnik, Zutrittskontrolle und Information Security Management (ISO 27001 Lead-Auditor)

Videokonferenzsystem Zoom im Sicherheitscheck

FERNKOOPERATION MIT RISIKO?

Mit den Reisebeschränkungen in der Corona-Krise ist der Bedarf an einfach zu handhabenden Videokonferenzsystemen sprunghaft gestiegen. Krisengewinner war dabei ohne Zweifel der amerikanische Hersteller Zoom Video Communications. Mit seinem „Zoom Meeting"-Dienst preschte das junge Unternehmen an bisherigen Branchenlieblingen vorbei. Derzeit gilt Zoom als populärstes Konferenzsystem auf dem Markt. Mitten im Aufstieg ist Zoom jedoch auch heftig in Kritik geraten: Schlechte Umsetzung des Datenschutzes, hohe Angreifbarkeit durch klaffende Schwachstellen und unzureichende Verschlüsselung lauteten die Vorwürfe. Der Hersteller zeigte sich bei der Behebung der Schwachstellen kooperativ. Doch ist jetzt alles sicher und vertrauenswürdig?

Mit dem Erfolg stieg auch die Aufmerksamkeit bei einschlägigen Security-Unternehmen. Und das, was diese im April über den Shooting-Star unter den Videoconferencing-Tools herausfanden, war wenig vertrauenserweckend: So konnten Angreifer recht einfach öffentliche Zoom-Meetings mithören, zweckentfremden und sogar zum Absturz bringen – das sogenannte „Zoom Bombing". Über eine Schwachstelle im UNC-Handling (Uniform Naming Convention) konnten die Kriminellen via Chat die Windows-Anmeldedaten der Nutzer ergattern. Generell wurden Schwächen bei der Verschlüsselung moniert.

Zoom hat sehr schnell auf die Vorwürfe regiert und zur Verbesserung der Sicherheit 90 Tage (das war der Zeitraum vom 23.04.2020 bis zum 21.07.2020) für die Kontestation zur Behebung von Sicherheitsproblemen festgesetzt. Im Rahmen dieses 90-Tage-Plans wurde regelmäßig ein Fortschrittsbericht veröffentlicht, welcher die Entwicklungen in Sachen Security dokumentierte. Zusätzlich stellt Zoom jetzt regelmäßig White Paper zur Sicherheit und Verschlüsselung bereit. Zoom geht im Verbesserungsprozess der Sicherheit seiner Software sehr transparent vor, und die dazu publizierten Informationen sind auch für Nicht-Informatiker verständlich. Inzwischen hat das Unternehmen Zoom in Version 5.0 veröffentlicht – die bis zum Beginn des 90-Tages-Plans bekannten Sicherheitsmängel sind ab dieser Version behoben.

ZOOM IM VERGLEICH ZU ANDEREN VIDEO-KONFERENZ-LÖSUNGEN

Das Erstaunliche an Zoom ist, dass es auch die ganz großkalibrigen Platzhirschen am Markt, wie Microsoft Teams und Google Meet, innerhalb kurzer Zeit auf die Plätze verwies. Bild 1 zeigt die täglichen Nutzer von Zoom, Google Meet, Microsoft Teams.

ZOOM UND SEIN ERFOLG

Zoom startete seinen Betrieb im Frühjahr 2011, zwei Jahre später kam das erste Produkt auf den Markt. Im Jahr 2019 verzeichnete Zoom bereits einen Umsatz von 622,7 Millionen US-Dollar.[1] Der Erfolg von Zoom lässt sich auf drei wesentliche Faktoren zurückführen:

- die einfache Nutzung und Zugänglichkeit,
- die Qualität der Konferenzen und
- die vergleichsweise niedrigen Kosten.

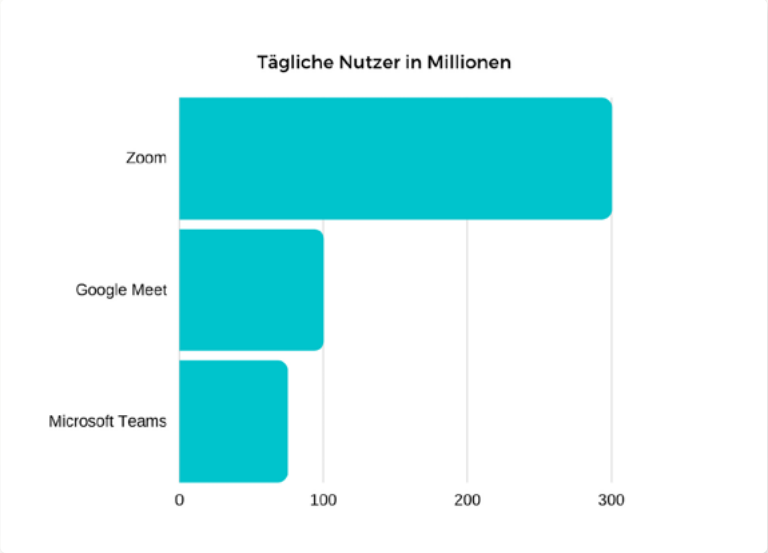


Bild 1: Zoom verzeichnet ca. 300 Millionen Nutzer täglich. Google Meet ca. 100 Millionen und Microsoft Teams ca. 75 Millionen tägliche Nutzer.[2]

Im Vergleich zu anderen Videoplattformen ist Zoom für jeden zugänglich. Zu Beginn des Jahres 2020 war es nicht erforderlich, einen Zoom Account zu besitzen, um an Meetings teilzunehmen. Aus Sicherheitsgründen ist dies heute nicht mehr der Fall und jeder Nutzer von Zoom muss einen Account anlegen. Dennoch ist Zoom für jeden zugänglich, da ein Account nicht speziell an ein Unternehmen oder eine Institution, wie Schulen oder Universitäten, gebunden ist. Gerade gegenüber Microsoft Teams ist die Verwendung von Zoom auch für nicht IT-affine Nutzer einfacher. Nur ein Klick ist ausreichend, um an einem Meeting teilzunehmen. Dazu ist dank der Browser-Funktion keine weitere Software nötig.

Die Qualität der Konferenz hängt hauptsächlich von Quality-of-Service-Parametern ab, die bei leistungsstarken Endgeräten und Netzwerken sehr hoch sind. Dabei werden die Übertragungskapazität, die Laufzeitverzögerung, die Laufzeitschwankung und der Paketverlust betrachtet. Zoom empfiehlt eine verfügbare Bandbreite von 600 KBit/s für qualitativ hochwertige Videos und 1,2 MBit/s für HD-Videos. Eine einfache Sprachverbindung (Voice-over-IP-Verbindung) kann bereits mit 60–80 KBit/s realisiert werden. Im Zoom Client können die Parameter unter „Einstellung und Statistiken" eingesehen werden. Die Laufzeitverzögerung wird als Latenz, die Laufzeitschwankung als Jitter angegeben. Diese Werte sollten so klein wie möglich sein, um eine gute Gesprächs- und Bildqualität zu gewährleisten.

Der Zoom Account kann in einer Basisversion kostenlos genutzt werden. Einschränkungen, wie die Dauer von Meetings, die für einen kostenlosen Account bei 40 Minuten liegt, sind anlässlich der Corona-Pandemie deaktiviert worden. Kostenpflichtige Accounts beginnen bei Zoom mit 13,99 Euro pro Monat pro Moderator oder 18,99 Euro pro Monat pro Moderator.[3] Microsoft Teams ist im Businessbereich in Office-365-Paketen enthalten, diese liegen preislich zwischen 4,20 und 16,90 Euro pro Monat pro Nutzer.[4] Google Meet bietet neben dem kostenlosen Paket mit Einschränkungen ebenfalls Enterprise-Lösungen an. Die Kosten liegen bei 10 bis 20 Dollar pro Monat pro aktiven Nutzer.[5] Im Gegensatz zu Zoom benötigen bei Microsoft Teams und Google Meet alle Teilnehmer ein Konto. Auch für die private Nutzung ist ein Konto erforderlich.

Zusätzlich bietet Zoom eine Handvoll Plug-ins an, um die Nutzung so einfach wie möglich zu gestalten. Die Plug-ins sind für die Webbrowser Chrome und Firefox sowie für das E-Mail-Programm Outlook verfügbar und ermöglichen die Planung eines Meetings in gleicher Form.

Ebenfalls ist die Planung mittels des Google-Kalenders möglich.

SICHERHEITSASPEKTE DER SOFTWARE

In den vergangenen Monaten sind mehrere Schwachstellen rund um die Zoom-Software bekannt geworden. Bei einer maßgeblichen Schwachstelle handelt es sich um die Verschlüsselung von Daten und Gesprächen. Ein wesentlicher Sicherheitsaspekt ist die Ende-zu-Ende-Verschlüsselung, die nicht gewährleistet war. Zoom stellte nur eine Verbindungsverschlüsselung (Link Encyption) bereit, dabei waren die Daten unverschlüsselt auf den Zoom-Servern vorhanden. Außerdem behauptete Zoom, dass die Verschlüsselung mit AES-256 umgesetzt wurde. Tatsächlich wurde AES-128 im Electronic-Codebook-(ECB-)Modus verwendet und Schlüssel wurden von nicht näher bestimmten „chinesischen Servern" generiert. Natürlich lässt sich nicht mit Bestimmtheit sagen, ob die chinesische Regierung Zugriff auf die Schlüssel hat – die Wahrscheinlichkeit ist jedoch hoch. Daraus ergibt sich ein unkalkulierbares Risiko für die Nutzer. Die Übermittlung von sensiblen Daten über ausländische Server stellt sogar einen veritablen Sicherheitsverstoß dar, wenn die Regeln auf Nutzerseite generell kein Routing über bestimmte Länder zulassen. Der bekannte IT-Sicherheitsexperte Bruce Schneier sagte dazu: „I'm okay with AES-128, but using ECB (electronic codebook) mode indicates, that there is no one at the company, who knows anything about cryptography."[6] (frei übersetzt: „Mit AES-128 könnte ich noch leben, aber die Verwendung des ECB-Mode zeigt, dass in diesem Unternehmen offenbar niemand auch nur einen Schimmer von Verschlüsselung hat") Zwischenzeitlich hat Zoom zunächst für zahlende Kunden eine Ende-zu-Ende-Verschlüsselung zur Verfügung gestellt.

Eine weitere Schwachstelle, die medial viel Aufmerksamkeit bekam, war der Diebstahl von Zugangsdaten mittels UNC-Hyperlinks. Diese beschreiben Adressen zu Webseiten (Server) im Internet (Netz). Beispielsweise führt der Link \\evil.server.com\images\cat.jpg auf eine vom Angreifer kontrollierte Infrastruktur und öffnet dort eine Bild-Datei. Dabei konnten Angreifer UNC-Hyperlinks in den Chat des Zoom-Meetings schreiben, welche von Zoom als Hyperlinks angezeigt wurden. Ein Klick auf diese Links führte dann über eine durch den Angreifer kontrollierte IT-Infrastruktur dazu, dass das Windows-Betriebssystem den Nutzernamen und Passwort als NTLM-Hash verschickte.

Im April dieses Jahres wurden Schwachstellen des Zoom-Client für eine halbe Million Dollar zum Verkauf angeboten. Dabei handelte es sich um sogenannte Zero-Day-Exploits für Windows und MacOS. Diese Schwachstellen ermöglichten es Angreifern, Zoom-Meetings auszuspionieren. Bei Windows wird dies durch eine Remote Code Execution ermöglicht, also das Ausführen von Schadcode auf fremden Endgeräten.[7] Der hohe Preis verdeutlicht, wie schwer es ist, eine fatale Schwachstelle zu entdecken. Ob Zoom sie gekauft hat, ist nicht bekannt.

MÄNGEL BEIM DATENSCHUTZ

Wegen der gravierenden Mängel beim Datenschutz wurde die Verwendung von Zoom in zahlreichen Unternehmen und Organisationen beschränkt – zum Teil, etwa in politischen Institutionen, sogar verboten. Beispielsweise haben Google und SpaceX, aber auch deutsche Konzerne und mittelständische Unternehmen, die Nutzung von Zoom eng limitiert. Regierungen und Behörden in Ländern wie England, USA und Taiwan untersagen die Verwendung von Zoom. In Deutschland riet das Auswärtige Amt ebenfalls davon ab.

Die größten Probleme hinsichtlich des Datenschutzes war die Übermittlung von Daten an Drittanbieter, die nicht angegeben worden waren. Auch das sogenannte Zoom-Bombing, welches das unerwünschte Eindringen und Stören von Unbefugten in einer Videokonferenz beschreibt, stellte einen Verstoß gegen den Datenschutz, die Privatheit und die Vertrauenswürdigkeit dar. Unter anderem konnten sich Unbefugte in Konferenzen einwählen und dort unberechtigt mithören sowie Straftaten begehen. Beispielsweise durch pornografische, gewaltverherrlichende oder rechtsextreme Inhalte.[8] Ebenfalls wurden Namen von Teilnehmern der Anonymen Alkoholiker erkannt und veröffentlicht. Zusätzlich machte Zoom negative Schlagzeilen, da Daten von der iOS-App an Facebook übermittelt worden sind.

Funktionen wie „Attention Tracking", also das Beobachten von Aktivitäten der Teilnehmer während eines Meetings, stellt in Deutschland nicht nur einen Datenschutzverstoß, sondern auch einen Verstoß gegen das Arbeitsrecht dar: Die Administratoren und Hosts von Meetings konnten die Aktivitäten der Teilnehmer (Mitarbeiter) verfolgen und überwachen – beispielsweise, ob das Meeting über Zoom als primäres Fenster geöffnet ist, oder ob der Teilnehmer zusätzlich anderen Tätigkeiten an seinem IT-System nachgeht. Die Rolle des Administrators beschreibt den Verantwortlichen für die gesamte Zoom-Instanz innerhalb eines Unternehmens oder Organisation. Er ist in der Lage, globale Einstellungen für Meetings vorzunehmen. Der Host ist für die einzelnen Meetings verantwortlich. Er kann bestimmte Sicherheitseinstellungen vornehmen, kann Teilnehmer zulassen oder entfernen etc. Ein Teilnehmer kann keine generellen sicherheitsrelevanten Einstellungen im Meeting vornehmen, dafür aber einige persönliche Einstellungen vornehmen.

Die Datenschutzerklärung von Zoom wurde zum 29. März 2020 aktualisiert.[9] Außerdem wurde das „Attention Tracking" entfernt. Dadurch ist es nicht mehr möglich, die Aktivitäten der Teilnehmer während eines Meetings nachzuverfolgen. Zoom speichert nur noch Basisinformationen, wie E-Mail-Adresse, Passwort, sowie Vor- und Nachname. Alle weiteren Angaben sind optional vom Nutzer anzugeben.

Zoom versichert, dass sie niemals Informationen über Nutzer verkaufen wollten und werden. Ebenfalls sichert Zoom zu, dass Meetings nicht überwacht werden. Damit ist die Datenschutzerklärung konform mit der Europäischen Datenschutz-Grundverordnung – in Deutschland also der DS-GVO.

ZOOM-PLATTFORMEN UND IHRE RISIKEN

Ist der Einsatz von Zoom damit nun bedenkenlos möglich? Nicht ganz – einige Risiken bestehen nach wie vor. An manchen Stellen ist es für den sicheren Einsatz sehr ratsam, die Einstellungen entsprechend zu justieren. Doch zunächst ein Blick auf die Zoom-Plattformen.

1. Client

Der Zoom-Client bietet eine komfortable Lösung, um Zoom auf dem Notebook oder PC zu nutzen. Die Teilnehmer können unter anderem

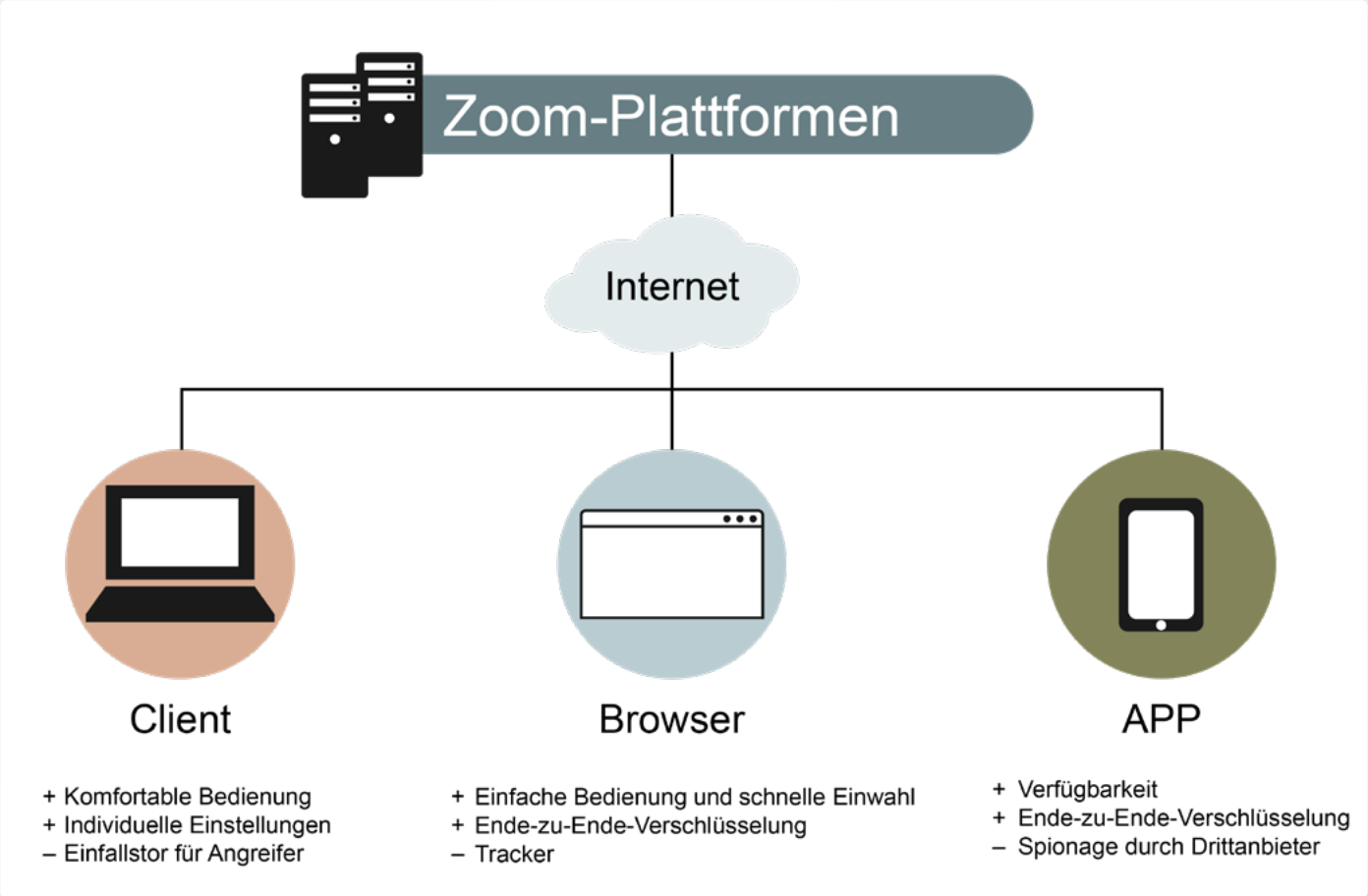


Bild 2: Technologien und Zusammenhänge der Zoom-Videokonferenz-Lösung.

einen virtuellen Hintergrund verwenden und individuelle Einstellungen vornehmen. Auch das Teilen von Ansichten während eines Meetings ist komfortabel, da alle Teilnehmer eine Präsentation zeigen und auch angezeigt bekommen können. Mitschnitte von Meetings können außerdem direkt lokal gespeichert werden. Ein Risiko bei der Verwendung des Zoom-Clients besteht darin, dass er direkt auf dem IT-System installiert wird und so Angreifer potenziell Zugriff auf das IT-System der Nutzer erlangen konnten.

2. App

Die App bietet dem Nutzer die Möglichkeit, von überall an Meetings teilzunehmen. Die App ist für Android- und iOS-Betriebssysteme verfügbar. Die App für iOS geriet stark in die Kritik, da Informationen an Facebook weitergegeben worden sind, ohne dass der Nutzer darüber in Kenntnis gesetzt worden ist. Da die App auch über Ende-zu-Ende-Verschlüsselungen kommuniziert, sind Informationen von Dritten geschützt.

3. Browser

Der Browser bietet dem Nutzer die Möglichkeit, ohne die Installation weiterer Software an Zoom-Meetings teilzunehmen. Dabei sind die Konfigurationsmöglichkeiten des Nutzers gegenüber den Client- und App-Versionen etwas eingeschränkt. Sofern die Nutzer nicht auf Links klicken oder sich in nicht vertrauenswürdigen IT-Infrastrukturen bewegen, bietet die Anwendung im Browser eine hohe Sicherheit, da diese keinen direkten Zugriff auf das System des Nutzers ermöglicht. Auch die Kommunikation über den Browser ist Ende-zu-Ende-Verschlüsselt.

SICHERHEITSUPDATES

Am 27. April 2020 veröffentlichte Zoom die Version 5.0. In dieser Version sind alle soweit bekannten Schwachstellen behoben worden, und es wurden enorme Verbesserungen an der Verschlüsselung vorgenommen.[10] Die Sicherheitsrichtlinien von Zoom sind an die Cloud-Sicherheitsrichtlinien des National Cyber Security Centre (NCSC) angelehnt und können in einem externen Dokument eingesehen werden. Das Ziel der NCSC-Cloud-Sicherheitsrichtlinien ist unter anderen der Schutz der Daten von Nutzern sowie der Zugriff auf das Zoom-System. Ebenfalls wird der Umgang mit Schwachstellen und sicherheitsrelevanten Vorfällen klar definiert.[11]

Seit der Version 5.0 werden Daten auch tatsächlich mittels AES 256-Bit verschlüsselt und zwar im Galois/Counter Mode (GCM) . Der GCM ist der neuste und fortschrittlichste Betriebsmodus und bietet einen authentifizierten Verschlüsselungsmodus mit assoziierten Daten.[12] Das Verfahren ist seit 2007 im NIST-Standard 800-38D spezifiziert. Seit dem 30. Mai 2020 verwenden alle Nutzer des Zoom-Clients die Version 5.0 oder höher. Clients mit niedrigeren Versionen sind nicht mehr der Lage, an Meetings teilzunehmen. Dadurch ist die Verschlüsselung für alle Clients garantiert. Ursprünglich war geplant,

eine Ende-zu-Ende-Verschlüsselung (E2EE) nur zahlenden Nutzern zur Verfügung zu stellen. Nach massiven Anwenderprotesten arbeitet das Unternehmen an einer Lösung, sie zeitnah auch Nutzern der freien Version anzubieten. Allerdings will Zoom dafür eine Verifikation des Accounts per Handy.[13] Außerdem können Hosts nun beim Planen eines Meetings auswählen, über welches Rechenzentrum der Zoom-Dienst umgesetzt und der Datenverkehr laufen soll, zum Beispiel ein US- oder EU-Rechenzentrum. Diese Information kann im Client-Fenster eingesehen werden.

EMPFEHLUNGEN FÜR DEN SICHEREN UMGANG MIT ZOOM

Um Zoom weiterhin verwenden zu können und die maximale IT-Sicherheit zu gewährleisten, sind einige Konfigurationen notwendig. Dabei handelt es sich größtenteils um Einstellungen, die bereits vor dem Erstellen eines Meetings durch die verantwortlichen Administratoren umgesetzt werden. Allerdings sind auch während eines Meetings diverse Einstellung zu beachten. Diese werden im folgenden Abschnitt genauer erläutert. Darüber hinaus bietet Zoom eine Zwei-Faktor-Authentifizierung an, die einen zusätzlichen Sicherheitsfaktor für den Schutz des Zoom-Accounts darstellt. Für die Verwendung des Browsers können zusätzliche kostenlose Add-ons installiert werden, die den Nutzer vor unerwünschtem Verhalten schützen. Zusätzlich sollten allgemeine Sicherheitshinweise für den Umgang mit Videoplattformen beachtet werden.

Pre-Meeting-Einstellungen

Pre-Meeting-Einstellungen sind Sicherheitseinstellungen, die bereits beim Erstellen des Meetings durch den Host oder den Administrator vorgenommen werden müssen. Eine von Zoom empfohlene Einstellung ist die Nutzung von Warteräumen. Startet ein Teilnehmer den Zugang zum Meeting, gelangt er erst einmal in einen Warteraum. Der Host des Meetings holt dann jedem Teilnehmer aus dem Warteraum zum Meeting. Somit ist es für Unbefugte nicht mehr möglich, einem Meeting beizutreten, außer der Host lässt ihn rein. Darüber hinaus sollte ein Meeting immer mit einem Passwort versehen werden. Dabei kann entweder das von Zoom generierte Passwort oder ein Individuelles verwendet werden. Das Passwort sollte durch eine aktive Eingabe der Teilnehmer abgefragt werden und nicht bereits im Einladungslink enthalten sein. Durch die manuelle Eingabe des Passworts wird weiterhin festgestellt, dass der Teilnehmer berechtigt ist, an dem Meeting teilzunehmen. Da Meetings nur authentifizierten Nutzern zugänglich gemacht werden sollten, kann so ein Missbrauch des Einladungslinks mit Passwort vorgebeugt werden. Diese Einstellungen können auch global vom Administrator der Zoom-Instanz vorgegeben werden.[14]

In-Meeting-Einstellungen

Während eines Meetings können vom Host weitere Einstellungen vorgenommen werden, diese werden In-Meeting-Einstellung genannt. Seit der Version 4.6.10 verfügt Zoom über ein Security-Icon in der Toolbar des Hosts. Dem Host ist es möglich, ein Meeting zu schließen, sodass keine neuen Teilnehmer dem Meeting beitreten können. Dadurch kann der unbefugte Beitritt in ein Meeting auch nachträglich unterbunden werden. Ebenfalls ist es möglich, die Video- und Audioverbindung einzelner Teilnehmer zu unterbinden. Der Host kann Teilnehmer aus dem Meeting entfernen und bei Verstößen einen Nutzer dem Zoom Trust & Safety Team melden. Zusätzlich kann der Host den Dateitransfer über den Chat sowie die Whiteboard-Funktion für geteilte Bildschirme sperren. Dies stellt einen enormen Sicherheitsgewinn dar, da somit die Verteilung von möglicherweise schadhafter Software unterbunden wird. Außerdem lässt sich das Teilen eines Bildschirms sowie das Aufnehmen von Meetings durch Teilnehmer vom Host deaktivieren. Somit sichert sich der Verantwortliche des Meetings in Hinblick auf den Datenschutz rechtlich ab. Das Ändern der ID von Teilnehmern kann ebenfalls vom Host unterbunden werden. Auch während eines bereits laufenden Meetings kann der Warteraum aktiviert werden. Ist bei einem Meeting auch die Teilnahme per Telefon zugelassen, ist zuvor die entsprechende Telefonnummer zu checken.[14]

WEITERE SICHERHEITSHINWEISE

Zwei-Faktor-Authentifizierung

Zoom stellt seit kurzem die Möglichkeit zur Zwei-Faktor-Authentifizierung bereit. Dadurch können Konten von Nutzern und Administratoren geschützt werden. Die Authentifizierung kann mittels einer App von Google, Microsoft oder FreeOTP durchgeführt werden.

Verwendung im Browser

Für die Nutzung von Zoom im Browser wird ein Werkzeug zum Blockieren von Trackern, kostenlos erhältlich von Antivirus-Herstellern, sowie ein Add-on für den Schutz von persönlichen Daten (beispielsweise Privacy Badger) empfohlen. Weiterhin sollten Teilnehmer nicht auf Links klicken, die nicht vertrauenswürdig sind.

BEWERTUNG VON VIDEOKONFERENZ-SYSTEMEN

Wichtig für die Bewertung der Sicherheit und Vertrauenswürdigkeit von Videokonferenz-Systemen sind unter anderen die angebotenen Sicherheitsfunktionen der Videoplattformen. Gerade die Verschlüsselung, die für den Datenverkehr verwendet wird, ist ein entscheidendes Kriterium. Zur Verschlüsselung sollte eine Ende-zu-Ende-Verschlüsselung verwendet werden. Dazu sollte mindestens ein Verschlüsselungsverfahren AES-128, besser noch AES-256, eingesetzt werden. Außerdem sollte der Videoplattformanbieter in Europa niedergelassen sein oder den Datenverkehr über europäische Rechenzentren leiten. Am besten ist eine Videokonferenzlösung, die in der eigenen IT-Infrastruktur betrieben werden kann, um eine hohe Souveränität zu erreichen. Der Vorteil von Open-Source-Lösungen ist eine hohe Unabhängigkeit. Weiteres Kriterium für die Vertrauenswürdigkeit eines Video-Systems ist die Einhaltung der DS-GVO.

Auch Google verzeichnet mit seinem Videokonferenz-System seit Ausbruch der Corona-Pandemie einen deutlichen Zuwachs. Google nutzte die öffentliche Diskussion um Zoom, um eine sichere Grundkonfiguration für sein Meet (ehemals Hangout) aufbauen. Beispielsweise können Hosts jetzt standardmäßig kontrollieren, welche Teilnehmer in einem Meeting erlaubt sind.

Microsoft Teams ist als Teil von Office 365 oder als Einzellösung erhältlich. Für die private Nutzung ist es kostenlos, allerdings muss ein Account bei Microsoft verknüpft werden. Im April dieses Jahres machte Teams durch eine Schwachstelle auf sich aufmerksam, bei der es den Angreifern möglich war, den Account ihres Opfers zu übernehmen.[15] Die Schwachstelle wurde bereits behoben. Im Office-365-

Enterprise-Paket bietet Teams eine Handvoll Sicherheitseinstellungen – unter anderem eine teamübergreifende und organisationsweite zweistufige Authentifizierung. Ebenfalls integrierte Microsoft einen erweiterten Bedrohungsschutz (Advanced Threat Protection, ATP), um Anwendungen zu überprüfen und Zugriffe blockieren zu können. Die Datenschutzrichtlinien in Teams sind identisch mit denen aus Office 365.

Der Vorteil von Open-Source-Videokonferenz-Systemen liegt ganz klar in der souveränen Nutzung und Verfügbarkeit. Ein Beispiel ist das Videokonferenz-Systemen Jitsi Meet. Jitsi Meet bietet Videokonferenzen über einen Webbrowser oder über eine App für Android und iOS an. Die Funktionen und die Übertragungsqualität können sich sehen lassen. Die maximale Anzahl an Meeting-Teilnehmern ist allerdings deutlicher geringer als bei Zoom. An einem Jitsi Meeting können maximal 75 Personen teilnehmen, für eine besser Qualität werden maximal 35 empfohlen. Bei Zoom sind 100 Teilnehmer Standard, erweiterbar auf 1.000 – ohne qualitative Einbußen. Jitsi Meet verfügt über eine Hop-by-hop-Verschlüsselung, in der jede Phase der Videokonferenz verschlüsselt wird.[16]

FAZIT & AUSBLICK

Zoom ist ein einfach zu bedienendes Videokonferenz-Tool. Die Zoom-Lösungen machen es dem Nutzer sehr leicht, sich zurechtzufinden und bieten eine intuitive Bedienbarkeit. Aber gerade am Anfang wurde die IT-Sicherheit stark vernachlässigt und kein „Security by Design" umgesetzt. Durch den enormen wirtschaftlichen und gesellschaftlichen Druck wurde Zoom dazu gezwungen, Schwachstellen ernst zu nehmen und schnellstmöglich zu beheben. Damit Zoom auch nach der Corona-Pandemie erfolgreich bleibt, sind nach IT-Sicherheitsmaßnahmen, wie dem 90-Tage-Plan, aber weitere IT-Sicherheits- und Datenschutzverbesserungen zwingend notwendig. Mit Version 5.0 sind bereits viele Schwachstellen innerhalb der Software behoben worden, auch dem Datenschutz wird bei der Verwendung von Zoom nun Rechnung getragen. Es ist zu erwarten, dass Zoom sich nun weiterhin allen Schwachstellen stellen und diese beheben wird. Eine wünschenswerte Erweiterung von Zoom wäre die Möglichkeit, die Zoom-Technologie in der eigenen IT-Infrastruktur zu betreiben, um eine höhere Souveränität/unabhängigere Verfügbarkeit zu erreichen.

Besonders erwähnenswert ist, dass während der Corona-Pandemie vielseitige und erfolgreiche Veränderungen der Sicherheitsaspekte in Zoom umgesetzt wurden. Aber auch andere Anbieter von Videokonferenz-Systemen partizipieren stark von den in Zoom gefunden Schwachstellen und der damit verbundenen medialen Aufmerksamkeit.

Insgesamt lässt sich feststellen, dass sich bei den Videokonferenz-Systemen sehr viel getan hat und der Datenschutz und die IT-Sicherheit deutlich besser geworden sind. Mit der immer größeren Beliebtheit der Videokonferenz-Systeme sollten die Hersteller allerdings „Privacy and Security by Design" berücksichtigen und einen kontinuierlichen IT-Sicherheitsprozess aufrechterhalten, der bei neuen Schwachstellen unmittelbar Updates zur Verfügung stellen kann. ■

Literatur

[1] *Zoom: https://www.sec.gov/ix?doc=/Archives/edgar/data/1585521/000158552120000095/zm-20200131.htm , 2020*

[2] *Alex Kannenberg: „Zoom korrigiert runter: Nicht 300 Millionen Nutzer, sondern Teilnehmer" , https://heise.de/-4712509, 2020*

[3] *Zoom: https://zoom.us/pricing, 2020*

[4] *Microsoft Pricing: https://www.microsoft.com/de-de/microsoft-365/business?market=de#compareProductsRegion*

[5] *Google: https://apps.google.com/meet/pricing/,2020*

[6] *Bruce Schneier: „Security and Privacy Implications of Zoom", https://www.schneier.com/blog/archives/2020/04/security_and_pr_1.html, 2020*

[7] *Lorenz Franceschi-Bicchierai: „Hackers Are Selling a Critical Zoom Zero-Day Exploit for $500,000", https://www.vice.com/en_us/article/qjdqgv/hackers-selling-critical-zoom-zero-day-exploit-for-500000, 2020*

[8] *Max Hoppenstedt: „Polizei ermittelt wegen Kinderpornografie in Videokonferenzen", https://www.spiegel.de/netzwelt/web/zoombombing-polizei-ermittelt-wegen-kinderpornografie-in-zoom-videokonferenzen-a-a51c49f3-40b3-4614-a347-d071f8b4089f, 2020*

[9] *Zoom Privacy Policy https://zoom.us/privacy, 2020*

[10] *Zoom 5.0 https://zoom.us/docs/de-de/zoom-v5-0.html, 2020*

[11] *Zoom: „Zoom Video Communications Cloud Security Principles", https://zoom.us/docs/doc/NCSC-Cloud-Security-Principles-Zoom-%282005%29.pdf, 2020*

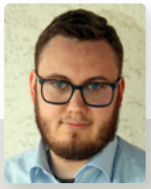
[12] *N. Pohlmann: „Cybersicherheit – Das Lehrbuch für Konzepte, Mechanismen, Architekturen und Eigenschaften von Cybersicherheitssystemen in der Digitalisierung", Springer-Vieweg Verlag, Wiesbaden 2019*

[13] *Dirk Srocke, Peter Schmitz: "E2E-Verschlüsselung für alle Zoom-Nutzer", https://www.security-insider.de/e2e-verschluesselung-fuer-alle-zoom-nutzer-a-942802/?cmp=nl-36&uuid=A74996FA-CB6C-4565-8D3EB1C2810899A5, 2020*

[14] *Zoom Privacy & Security for Zoom Video Communications, https://zoom.us/docs/en-us/privacy-and-security.html?zcid=3797&creative=437995777397&keyword=zoom%20security&matchtype=e&network=g&device=m&gclid=Cj0KCQjwz4z3BRCgARIsAES_OVfhWlXwBrGFhr4lGOjSDGuS8wuiF2-MCH5t6zDO_JGspitYS3knNBoaAjbKEALw_wcB, 2020*

[15] *Omer Tsarfati: „Beware oft he GIF: Account Takeover Vulnerability in Microsoft Teams", https://www.cyberark.com/resources/threat-research-blog/beware-of-the-gif-account-takeover-vulnerability-in-microsoft-teams , 2020*

[16] *Gavin Phillips: „What Is Jitsi and Is it More Secure Than Zoom?", https://www.makeuseof.com/tag/jitsi-secure-zoom/#:~:text=It%20means%20that%20the%20server,eavesdropping%20on%20private%20video%20conversations, 2020*



CHRISTIAN BÖTTGER
studiert im Master Internet-Sicherheit an der Westfälischen Hochschule Gelsenkirchen und beschäftigt sich im Rahmen des Studiums mit der Bewertung von Video-Systemen.

NORBERT POHLMANN
ist Professor für Informationssicherheit 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.

Was Tracking des Surfverhaltens über den Nutzer verrät

DEINE SPUREN IM WEB

Das Tracking des Surfverhaltens gehört zum Alltag der Internetnutzung. Unternehmen verwenden es beispielsweise, um Werbeanzeigen auf die persönlichen Belange der potenziellen Kunden zuzuschneiden oder ihre Reichweite zu messen. Viele Anbieter von Tracking-Diensten werben mit sicherem Datenschutz, indem sie die Datensätze generalisieren und so anonymisieren. Wie sicher dieses Verfahren ist, haben Informatikerinnen und Informatiker des Karlsruher Instituts für Technologie (KIT) und der Technischen Universität Dresden (TUD) nun untersucht und anlässlich der IEEE Security and Privacy-Konferenz in einem wissenschaftlichen Paper veröffentlicht.

◀ *Beim Surfen im Internet sammeln Unternehmen nicht nur Daten über besuchte Webseiten, sondern auch über den Zeitpunkt des Abrufs oder Ortsinformationen. (Foto: Amadeus Bramsiepe, Markus Breig, KIT)*

> **„Selbst wenn lediglich die Domain, die Themenzuordnung, wie ‚Politik' oder ‚Sport', und die Zeit nur tagesgenau gespeichert werden, können 35 bis 40 Prozent der Daten individuellen Personen zugeordnet werden."**

PROFESSOR THORSTEN STRUFE,
Leiter der Forschungsgruppe „Praktische IT-Sicherheit" am KIT (Foto: Amadeus Bramsiepe)

Tracking-Dienste sammeln große Datenmengen der Internetnutzerinnen und -nutzer. Darunter fallen neben den besuchten Webseiten beispielsweise auch Informationen zu den verwendeten Endgeräten, der Zeitpunkt des Abrufs (Zeitstempel) oder Ortsinformationen. „Da diese Daten sehr sensibel sind und einen hohen Personenbezug haben, nutzen viele Unternehmen die Generalisierung, um sie scheinbar zu anonymisieren und damit Datenschutzregelungen zu umgehen", sagt Professor Thorsten Strufe, Leiter der Forschungsgruppe „Praktische IT-Sicherheit" am KIT. Bei einer Generalisierung wird der Detailgrad der Informationen reduziert, sodass eine Identifizierung von Einzelpersonen nicht mehr möglich sein soll. So werden beispielsweise die Ortsinformationen auf die Region beschränkt, die Abrufzeit auf den Tag oder die IP-Adressen um einige Zahlen gekürzt. Ob so wirklich keine Rückschlüsse mehr auf das Individuum gezogen werden können, hat Strufe gemeinsam mit seiner Forschungsgruppe und Kolleginnen und Kollegen der TU Dresden untersucht.

Mithilfe einer Vielzahl an Metadaten deutscher Webseiten mit etwa 66 Millionen Nutzern und über zwei Milliarden Seitenaufrufen konnten die Informatikerinnen und Informatiker nicht nur Rückschlüsse auf die aufgerufenen Seiten, sondern auch auf die Verkettung der einzelnen Seitenaufrufe, sogenannte „Click Traces", ziehen. Die Daten stellte ihnen INFOnline, eine Institution für Reichweitenmessung in Deutschland, zur Verfügung.

DER VERLAUF VON SEITENAUFRUFEN HAT GROSSE AUSSAGEKRAFT

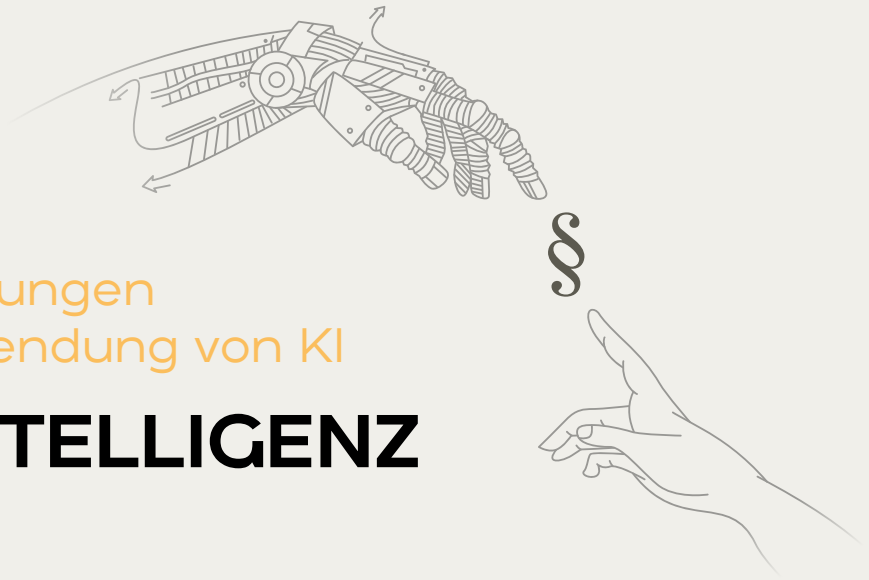
„Um die Wirksamkeit der Generalisierung zu testen, haben wir zwei unterschiedliche Anwendungsszenarien betrachtet", sagt Strufe. „Zum einen haben wir die gesamten Click Traces auf ihre Eindeutigkeit untersucht. Denn ist ein Click Trace, also der Verlauf vieler aufeinanderfolgender Seitenaufrufe, klar von anderen abgrenzbar, so ist er nicht mehr anonym." Dabei zeigte sich, dass Informationen zur besuchten Webseite und benutztem Browser komplett aus den Daten entfernt werden müssen, um Rückschlüsse auf Personen zu vermeiden. „Die Daten werden erst dann anonym, wenn die Sequenzen entweder zu einzelnen Klicks verkürzt, also völlig ohne Zusammenhang gespeichert werden, oder alle Informationen mit Ausnahme des Zeitstempels entfernt werden", so Strufe. „Selbst wenn lediglich die Domain, die Themenzuordnung, wie ‚Politik' oder ‚Sport', und die Zeit nur tagesgenau gespeichert werden, können 35 bis 40 Prozent der Daten individuellen Personen zugeordnet werden." In diesem Szenario konnten die Forscherinnen und Forscher zeigen, dass der Ansatz der Generalisierung nicht der Definition der Anonymität entspricht.

WENIGE BEOBACHTUNGEN REICHEN, UM NUTZERPROFILE ZU IDENTIFIZIEREN

Die Wissenschaftlerinnen und Wissenschaftler haben außerdem untersucht, wie man auch nur mit Teilmengen von Click Traces Rückschlüsse auf ein Individuum ziehen kann. „Wir haben die generalisierten Informationen aus der Datenbank mit weiteren Beobachtungen, wie in den Sozialen Medien oder in Chats geteilten Links, verbunden. Wird beispielsweise die Zeit auf eine Minute genau generalisiert, reicht mit dieser Methode eine Beobachtung, um über 20 Prozent der Click Traces eindeutig einer Person zuzuordnen", sagt Clemens Deusser, der als Doktorand in Strufes Arbeitsgruppe maßgeblich an der Studie beteiligt war. „Zwei weitere Beobachtungen steigern diesen Erfolg auf über 50 Prozent. In der Datenbank kann dann einfach abgelesen werden, welche anderen Webseiten die Person noch besucht und welche Inhalte sie betrachtet hat." Selbst wenn der Zeitstempel nur tagesgenau gespeichert werde, benötige man für die Personenerkennung nur fünf weitere Beobachtungen.

„Unsere Ergebnisse zeigen, dass einfache Generalisierung nicht geeignet ist, um Webtrackingdaten wirksam zu anonymisieren. Die Daten bleiben personenscharf und die Anonymisierung ineffektiv. Um einen effektiven Datenschutz zu erreichen, müssten Verfahren angewandt werden, die darüber hinausgehen, wie beispielsweise eine Verrauschung durch zufälliges Einfügen kleiner Fehlbeobachtungen in die Daten", so Strufes Empfehlung. ■

KIT-PRESSE/STEFAN MUTSCHLER



Rechtliche Herausforderungen bei Gestaltung und Anwendung von KI

KÜNSTLICHE INTELLIGENZ UND RECHT

Von der Idee künstlicher Intelligenzen geht seit jeher eine große Faszination aus. Vielfach wurde dieses Thema künstlerisch bearbeitet – und zumeist mit negativen Assoziationen verbunden. Man denke nur an einige der berühmtesten Beispiele wie den bereits vor 200 Jahren veröffentlichten Roman „Frankenstein" oder das verhängnisvolle Verhalten der Künstlichen Intelligenz Skynet aus dem Film „Terminator". In der Realität haben vor allem Erfolge wie der Sieg des Schachcomputers Deep Blue gegen Schachweltmeister Garri Kasparow 1996 in der breiten Öffentlichkeit für Aufmerksamkeit gesorgt. Inzwischen ist unter und neben solchen Besonderheiten ein weites Feld praktisch eingesetzter KI entstanden.

Auch wenn keine einheitliche Definition für den Begriff der Künstlichen Intelligenz (KI) existiert, kann sich ihm mit einigen Merkmalen genähert werden. Als Teilgebiet der Informatik eingestuft, muss KI zu Prognosen und eigenständigen Lernprozessen in der Lage sein. Der US-amerikanische Informatiker John McCarthy prägte den Begriff 1955 und erklärte: „KI ist die Wissenschaft und Technik der Herstellung intelligenter Maschinen, insbesondere intelligenter Computerprogramme." Mittlerweile ist die Unterscheidung zwischen schwacher und starker KI allgemein bekannt. Während erstere Muster erkennen und auf unbekannte Probleme reagieren, allerdings nicht abstrahieren und daher nur in ihrem spezifischen Anwendungsfeld agieren kann, zeichnet sich zweitere durch logisch-intellektuelles Denken und eine Abstraktionsfähigkeit aus, die an menschliche Eigenschaften heranreicht oder sie gar übertrifft. Vielfach werden allerdings alle KI-Anwendungen, die bis heute entwickelt worden sind, noch als schwache KI, beziehungsweise Machine Learning (ML) qualifiziert. Dennoch schreitet die Entwicklung von Technologien rund um KI weiterhin stark voran. Während noch 2015 weltweit über 60.000 Patente im KI-Bereich angemeldet worden waren, sind es 2018 schon knapp 150.000 gewesen, mit stark steigender Tendenz. Die Systeme werden stetig „intelligenter" und autonomer.

HÄUFIGE EINSATZFELDER VON KI

KI ist zu vielfältigen Anwendungen fähig. Mit künstlichen neuronalen Netzen und Deep Learning kann KI ihre Fähigkeiten selbst verbessern, indem sie Schlussfolgerungen abspeichert und einen eigenen Lernprozess durchläuft. So können besonders große Datenmengen analysiert und für Anwendungen wie Gesichtserkennung genutzt werden. In Bereichen wie den Anwendungsfeldern Gesundheit, Datensicherheit, Industrie 4.0 und Mobilität, auf welche sich weltweit die meisten KI-Patente verteilen, wird KI in Form der Subtechnologien Spracherkennung, Zeichenerkennung, Bild- und Datenanalyse eingesetzt.

Innerhalb dieser Anwendungsfelder sind ganz unterschiedliche Einsatzmöglichkeiten denkbar. Im Gesundheitswesen beispielsweise können mithilfe von Deep

Learning Röntgenbilder analysiert oder Tumorstrukturen und -entwicklungen beim einzelnen Patienten analysiert werden. Genauso ermöglichen Big-Data-Analysen eine bessere Erforschung von Krankheiten. Zugleich hilft KI durch Übersetzungshilfen für Blinde und Gehörlose oder assistiert in der Chirurgie. Darüber hinaus gibt es in der Telemedizin KI-Anwendungen, die etwa Daten von Herzkranken vorverarbeiten, sodass Patienten in größerer Anzahl und effektiver betreut werden können.

Im Bereich der Datensicherheit kann KI verdächtige Vorgänge und Bedrohungen erkennen und passende Gegenmaßnahmen selbstständig einleiten. Selbstlernende KI kann hier sogar auf bisher unbekannte Malware oder Cyberangriffe angemessen reagieren. Zudem können KI-gestützte Authentifizierungsverfahren die Datensicherheit erhöhen, indem zum Beispiel bei einer Zwei-Faktor-Authentifizierung eine KI biometrische Daten verifiziert.

KI UND RECHT – EIN KURZER ÜBERBLICK

Auch wenn die heutige Realität mit den eingangs erwähnten Schreckensvisionen nicht viel gemein hat, birgt KI dennoch einige Risiken und Gefahren, insbesondere für die Sicherheit der Daten, die die Grundlage für KI-Technologien sind. Die Rechtsentwicklung steht in Deutschland und anderswo noch am Anfang. Einige Ansätze und Vorgaben, die für KI-Anwender und Entwickler relevant sind, gilt es aber bereits jetzt zu beachten. Ein einheitliches „KI-Recht“ gibt es dabei nicht, sondern viele allgemeine gesetzliche Bestimmungen aus unterschiedlichen Rechtsgebieten lassen sich gut auf Künstliche Intelligenz anwenden. Dazu gehören der Grundrechtsschutz und das sich daraus ergebende Datenschutzrecht, das Haftungsrecht oder auch das Leistungsschutzrecht.

Da sich die rechtliche Regulierung in einem Spannungsverhältnis zur technischen Innovationsfähigkeit befinden kann, gibt es teils sehr unterschiedliche Positionen, welcher Rechtsrahmen für KI angemessen erscheint. Die EU-Kommission etwa hat sich hier klar positioniert und ethische Leitlinien, wie Transparenz, Schutz der Privatsphäre und Schutz vor Diskriminierung, in den Vordergrund gestellt, da technische Innovationen nicht zuletzt auch auf Zustimmung und Vertrauen in der Bevölkerung angewiesen seien. Andere Stimmen, wie der Digitalverband Bitkom, warnen vor einer Überregulierung, die dem technischen Fortschritt entgegenstehen würde und verweisen auf Qualitätsstandards sowie die bereits jetzt sehr effektive Rechtslage.

> „KI ist die Wissenschaft und Technik der Herstellung intelligenter Maschinen, insbesondere intelligenter Computerprogramme.“
>
> *John McCarthy,*
> *US-amerikanischer Informatiker*

DATENSCHUTZ IM FOKUS

Der Erfolg Künstlicher Intelligenz fußt auf den Daten, mit denen KI trainiert und verbessert wird und die das Fundament der Lernprozesse bilden. Entsprechend spielt das Datenschutzrecht eine große Rolle bei der Reglementierung von KI. Zur Stärkung dieser Rolle hat die Datenschutzkonferenz (DSK) – ein Zusammenschluss aller deutschen Datenschutz-Aufsichtsbehörden – in der sog. Hambacher Erklärung Leitlinien verabschiedet, die rechtlich zwar nicht bindend sind, aber die Richtung für die Zukunft vorgeben dürften. Zentraler Ausgangspunkt soll danach der sich aus der Menschenwürde ergebende Grundsatz sein, dass KI den Menschen nicht zum Objekt degradieren darf. KI soll nur für verfassungsrechtlich legitime Zwecke eingesetzt werden und diese Zwecke sollen vorab klar und deutlich festgelegt sein. Weiterhin soll KI transparent und nachvollziehbar arbeiten, den Grundsatz der Datenminimierung berücksichtigen sowie Diskriminierungen vermeiden. Für jede KI soll es eine verantwortliche Stelle geben, und technische sowie organisatorische Mindeststandards sollen gewahrt werden.

WANN IST DATENSCHUTZRECHT ANWENDBAR?

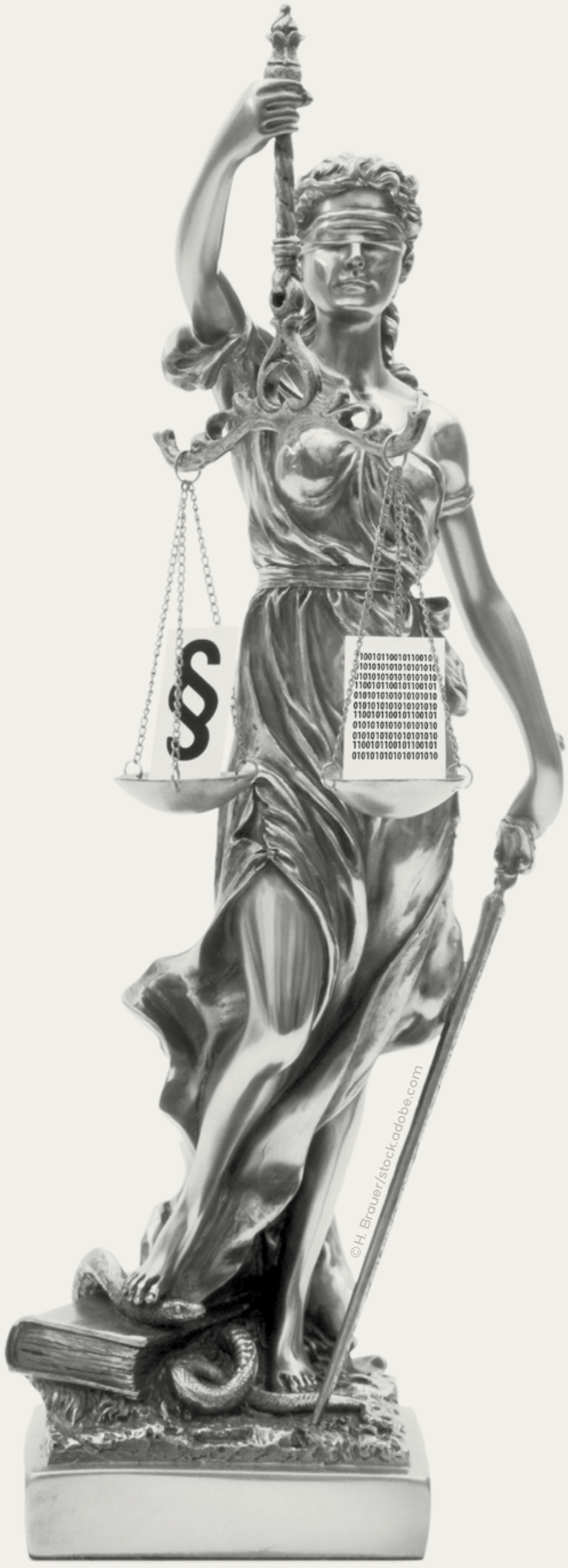
Das Datenschutzrecht und insbesondere die Datenschutz-Grundverordnung (DS-GVO) ist bei der Verarbeitung personenbezogener Daten zu berücksichtigen. Personenbezogene Daten sind alle Informationen, die sich auf eine identifizierte oder identifizierbare Person beziehen (Art. 4 Nr. 1 DS-GVO). Verarbeitung ist jeder Vorgang mit personenbezogenen Daten, wie das Erheben, Speichern, Verändern oder Verwenden (Art. 4 Nr. 2 DS-GVO).

Ein Ausweg kann das Verfahren der sogenannten Anonymisierung der Daten sein, da bei der Verarbeitung anonymisierter Daten die DS-GVO nicht anzuwenden ist. Denn personenbezogene Daten sind dann anonymisiert, wenn die Person, auf welche die Informationen sich beziehen, nicht mehr identifizierbar ist. Da diese Person in diesem Fall keinen Risiken mehr ausgesetzt ist und daher nicht mehr geschützt werden muss, ist ein Schutz der Daten nicht mehr erforderlich. Allerdings muss eine Re-Identifikation auch wirklich ausgeschlossen sein. Vielfach sind Daten nämlich nur pseudonymisiert, das heißt die Person kann etwa durch die Zuhilfenahme weiterer Informationen mit vertretbarem Aufwand wieder ermittelt werden. Vor allem, wenn für die jeweilige Anwendung eine Vielzahl verschiedener Daten erforderlich ist, kann aus Informationen wie Alter, Gewicht, Vorerkrankungen etc. schnell wieder ein Personenbezug hergestellt werden. Um Rechtsverstöße zu vermeiden, sollten Verwender hier sorgfältig prüfen, ob eine Anonymisierung möglich und zweckmäßig ist.

Sobald es sich bei KI-Trainingsdaten um personenbezogene Daten handelt, ist also die DS-GVO anzuwenden. Das dürfte in vielen Fällen zutreffen, da sich die Erhebung personenbezogener Daten meist nicht verhindern lässt. So kann der Personenbezug etwa wichtig sein, um die Daten über einen längeren Zeitraum einem konkreten Kunden oder Patienten zuordnen zu können, oder die Trainingsdaten wären nach einer Anonymisierung nicht mehr ausreichend verwertbar. Bei den personenbezogenen Daten kann es sich um Nutzer- oder Kundendaten, wie Name, Anschrift oder E-Mail-Adresse, oder um Meta-, biometrische oder Prognosedaten handeln.

KI: VIELE POTENZIALE BEDEUTEN VIELE RISIKEN

KI-Systeme bergen eine Menge datenschutzrechtlicher Risiken. Nimmt eine KI Personalisierungen vor, können die Gefahren beispielsweise in Preismanipulationen, der Beeinflussung von Inhalten und Wissen oder auch von Wahlen liegen. Identifikationssoftware kann mittels Tracking, Gesichtserkennung und intelligenter Videoüberwachung zum Verlust anonymer und privater Bereiche (online wie offline) führen. Zudem kann KI Verhaltensanalysen betreiben, wie es sich etwa in der Bewertung von Bewegungen, Tastatureingaben, Klickverhalten und Emotionen niederschlägt. Damit verbundene Risiken sind beispielsweise die psychologische Einschätzung von Personen, die Manipulation des Kaufverhaltens oder ein allgemeiner Kontrollverlust über das eigene Handeln. Um diesen und anderen Risiken vorzubeugen, bestimmt die DS-GVO eine Reihe an rechtlichen Vorgaben und datenschutzrechtlichen Grundsätzen.



WELCHE VORGABEN ERGEBEN SICH AUS DER DS-GVO?

Ohne eine entsprechende Rechtsgrundlage ist keine Verarbeitung personenbezogener Daten zulässig. Die für den Gebrauch von KI relevantesten Rechtsgrundlagen werden in der Praxis die Vertragserfüllung, die Wahrung berechtigter Interessen sowie die Einwilligung sein.

Der Abschluss eines entsprechenden Vertrags ist eine sichere und eindeutige Variante. Bei der Wahrung berechtigter Interessen muss dagegen sorgfältig geprüft werden, ob der Einsatz der KI einen legitimen Zweck verfolgt, die entsprechende Datenverarbeitung erforderlich ist und etwaige entgegenstehende Interessen der betroffenen Personen das berechtigte Interesse an der Verarbeitung nicht überwiegen. Möchte man die Datenverarbeitung durch KI auf eine Einwilligung der betroffenen Person stützen, ist darauf zu achten, dass sie freiwillig, bestimmt und informiert abgegeben wird, verständlich formuliert ist und jederzeit nachgewiesen werden kann. Zudem kann sie mit Unsicherheiten behaftet sein, da sie jederzeit widerrufbar ist. Das kann vor allem dann ein Problem sein, wenn die Daten bereits in den Lernprozess einer KI eingeflossen sind, was nachträglich nur schwer rückgängig zu machen ist. Welche Rechtsgrundlage am Ende in Betracht kommt, hängt stark von den jeweiligen Gegebenheiten ab.

Beim Einsatz von KI besonders wichtig sind die datenschutzrechtlichen Grundsätze Privacy by Design sowie Privacy by Default nach Art. 25 DS-GVO. Unter Privacy by Design ist „Datenschutz durch Technikgestaltung“ zu verstehen. Dazu sollten Datenschutzmaßnahmen bereits bei der Entwicklung der KI und in ihren Verarbeitungsvorgängen technisch integriert und die Verarbeitungstätigkeiten durch technisch-organisatorische Maßnahmen abgesichert werden. Privacy by Default meint daneben „Datenschutz durch datenschutzfreundliche Voreinstellungen“, sodass der Datenschutz bereits in den Werkseinstellungen einer Anwendung berücksichtigt wird. Darüber hinaus umfasst dieser Grundsatz das Prinzip der Datenminimierung: Es dürfen nur die Daten verwendet werden, die für den Zweck auch wirklich notwendig sind. Hier sollte auch geprüft werden, ob synthetische, also künstlich erzeugte und nicht aus realen Ergebnissen stammende Daten ohne praktische Einbußen genauso eingesetzt werden können.

In diesem Zusammenhang ist auch der bereits erwähnte Grundsatz der Zweckbindung entscheidend. Daten dürfen demnach nur für zuvor genau festgelegte Zwecke verarbeitet werden – dementsprechend sind Verarbeitungen für noch unbekannte Zwecke und Datensammeln „auf Vorrat“ grundsätzlich unzulässig. Ändern sich im Laufe der Zeit die Zwecke, muss die Rechtsgrundlage erneut überprüft werden. Besonders relevant wird der Grundsatz der Zweckbindung bei KI im Zusammenhang mit Big-Data-Analysen und Mustererkennung. Denn zum einen ist bei der Analyse großer Datenmengen häufig nicht im Vorfeld klar, zu welchen Zwecken die Daten am Ende eingesetzt werden sollen, zum anderen bedeutet Mustererkennung in aller Regel die Erfassung von Mustern, die vorher nicht bekannt waren. Hier gilt es, die genauen Umstände des KI-Einsatzes so genau, eindeutig und konkret wie möglich zu beschreiben.

DISKRIMINIERUNG DURCH KÜNSTLICHE INTELLIGENZ

Das Allgemeine Gleichbehandlungsgesetz (AGG) bestimmt in Deutschland den Schutz vor Diskriminierungen, vor allem im Bereich Bewerbungen und Zugang zu Dienstleistungen. Amazon beispielsweise setzte im Bewerbungsprozess für Arbeitsplätze im Tech-Bereich eine KI zur Unterstützung ein. Aus der höheren Anzahl an Bewerbungen von Männern als von Frauen in der Vergangenheit ergab sich eine entsprechend höhere Rate männlicher Mitarbeiter. Aus diesem Umstand schlussfolgerte die Software, dass Männer grundsätzlich zu bevorzugen seien und filterte Frauen daher vielfach direkt heraus. Diskriminierungsverhalten kann sich also auch ungewollt in das Verhalten von KI einschleichen oder bestehende Diskriminierungsverhältnisse verfestigen. Um dem entgegenzuwirken, sollten so weit wie möglich Regeln für die Zusammensetzung der Trainingsdaten festgelegt sowie diskriminierende Kriterien erfasst und ausgesondert werden. Idealerweise sind technische Korrekturmöglichkeiten zu implementieren.

HAFTUNGSFRAGEN

Neben Diskriminierung kann beim KI-Einsatz noch einiges anderes schiefgehen, Roboter oder selbstfahrende Autos können Menschen verletzen oder Sachen beschädigen. Bei all diesen Problemen stellt sich die Frage, wer für Schäden haftet, die eine KI verursacht hat. Denn das deutsche Recht kennt eine Haftung bislang nur für menschliches Verhalten.

Hier ist zu unterscheiden: Vielfach wird KI von einem Menschen „nur“ als Werkzeug eingesetzt. In diesem Fall ist der Verwender unproblematisch der Schädiger, der rechtlich haften muss. Bei selbstlernender und autonomer KI ist allerdings zunehmend davon auszugehen, dass sie über die bloße Werkzeugeigenschaft hinausgeht. Nach aktueller Rechtslage muss aber auch hier auf das Fehlverhalten eines Menschen abgestellt werden.

Aufgrund der allgemeinen und bewusst technologie-neutral formulierten gesetzlichen Regelungen ist der Einsatz Künstlicher Intelligenz allerdings kein rechtsfreier Raum.

Zum einen kommt der Hersteller bzw. Programmierer als Haftender in Betracht. Er steht, indem er die KI entwickelt hat, ihr wohl am nächsten. Für diesen kann vor allem die sog. Produzentenhaftung aus § 823 Abs. 1 des Bürgerlichen Gesetzbuchs (BGB) greifen. Danach muss er allerdings vorsätzlich oder fahrlässig eine fehlerhafte KI in den Verkehr gebracht haben. Fahrlässigkeit setzt voraus, dass die im Verkehr erforderliche Sorgfalt nicht beachtet wurde. Vorsätzlich handelt, wer wissentlich und willentlich ein fehlerhaftes Produkt in den Verkehr gebracht hat. Hersteller sollten hier beachten: Sie sind im Rahmen der Produzentenhaftung beweispflichtig und müssen zeigen, dass sie gerade kein fehlerhaftes Produkt in den Umlauf gebracht haben. Das dürfte einfacher gelingen, je autonomer die KI ist. Am mangelnden Verschulden dürften auch die meisten Haftungsansprüche gegen den Verwender der KI scheitern. Jeder Verwender, der die KI so wie vorgesehen einsetzt, haftet für kein fehlerhaftes „Verhalten" der KI. Daher dürfte für viele das Haftungssystem bei autonomen Systemen lückenhaft erscheinen: Sobald weder Hersteller noch Verwender ein Verschulden trifft, haftet niemand für einen Schaden, den eine KI verursacht hat. Andererseits kann man darin auch die vom Gesetz beabsichtigte Lösung sehen: Wenn jemandem kein Fehlverhalten zur Last gelegt werden kann, sollte er auch nicht haften. Ob das so bleibt oder andere Haftungsregeln eingeführt werden, bleibt abzuwarten. Ein Lösungsansatz kann auch eine Pflichtversicherung für besonders risikoreiche KI-Anwendungen sein.

Einen Sonderfall stellt die Haftung beim autonomen Fahren dar, da hier das Straßenverkehrsgesetz (StVG) gilt. Wenn den Fahrer kein Verschulden trifft, haftet noch immer der Halter des Fahrzeugs unabhängig vom Verschulden. Durch eine Gesetzesänderung von 2017 ist klargestellt, dass diese Systematik auch bei autonomen Fahrzeugen bestehen bleibt. Halter ist der, der das Auto auf eigene Rechnung in Gebrauch hat.

FAZIT

Ob man die Entwicklung von Künstlicher Intelligenz auch heute noch als Bedrohung auffassen möchte, mag jeder selbst entscheiden. Die allermeisten Anwendungen im täglichen Gebrauch dürften jedoch vor allem Vorteile in den unterschiedlichsten Bereichen und Branchen hervorbringen. Dass KI dennoch mit Risiken verbunden ist, bleibt unbenommen. Aufgrund der allgemeinen und bewusst technologieneutral formulierten gesetzlichen Regelungen ist der Einsatz Künstlicher Intelligenz allerdings kein rechtsfreier Raum. Viele Sachverhalte sind bereits jetzt rechtlich ausführlich reguliert, sodass Entwickler wie Anwender zahlreiche Vorgaben beachten müssen. Deshalb, aber auch weil das Recht längst nicht alle technischen Entwicklungen mitbedacht hat und daher nicht völlig lückenlos ist, sind Entwicklung und Einsatz von KI mit zahlreichen rechtlichen Herausforderungen verbunden. Vor allem bei autonomer KI besteht kein voll umfänglicher Schutz, wenn es um Schäden oder Diskriminierungen geht. Daher befindet sich die Rechtslage genau wie die technische Entwicklung auch weiterhin in einem Prozess und in einem Spannungsfeld zwischen dem Fortschreiten der Technik und rechtlicher Regulierung.

Eine starke Rolle nimmt im Rahmen Künstlicher Intelligenz das Datenschutzrecht ein. Es engt KI-Anwendungen rechtlich ein, indem es viele Vorgaben macht und Pflichten auferlegt, die dem Schutz der Personen dienen, deren Daten in irgendeiner Weise von KI betroffen sind. Die DS-GVO sollte hier aber nicht als Hemmnis, sondern im Gegenteil als Chance wahrgenommen werden, um die technischen Innnovationen mit Vertrauen und Sicherheit zu begleiten. Schließlich ist der deutsche wie der europäische Gesetzgeber offen für neue Technologien, sodass die meisten KI-Anwendungen in die Rechtslage gut integrierbar sind. Dies dürfte auch in Zukunft so bleiben. ■

Foto: SRD Rechtanwälte

KATHRIN SCHÜRMANN
ist Rechtsanwältin und Partnerin bei Schürmann Rosenthal Dreyer. Neben dem Urheber- und Medienrecht, Datenschutz und Wettbewerbsrecht ist Frau Schürmann auf den gesamten Marketing-Bereich spezialisiert, insbesondere auf der Schwelle zwischen Wettbewerbs- und Datenschutzrecht. Ein besonderer Fokus ihrer Tätigkeit liegt dabei auf der Beratung von Unternehmen aus den Bereichen Digital Business, Technologie und Medien.

www.srd-rechtsanwaelte.de

Mitarbeiter schulen via E-Learning

kosteneffizient - flexibel - einfach

TV-Studioqualität

E-LEARNING-KURSE:

- Antidiskriminierung
- Einführung in die IT-Sicherheit
- Einführung in den Datenschutz
- Haftungsrisiken in der Entgeltabrechnung

Jetzt informieren: **datakontext.com/eLearning**

UNIVADO

DATAKONTEXT

VORSCHAU Ausgabe 5|20 OKTOBER/ NOVEMBER

SELF-SOVEREIGN IDENTITY (SSI)

Eine vollkommen selbstbestimmte Identität galt in der IT lange als Wunschtraum. Noch besser, wenn sich mit der Identität gleichzeitig kontrollieren lässt, wie die persönlichen Daten geteilt und verwendet werden. Eine der Schlüsseltechnologien bei diesem Ansatz, der nun in Europa als Projekt im Rahmen der eIDAS-Verordnung (electronic IDentification, Authentication and trust Services) Gestalt annimmt, ist die Block Chain.

Doch was genau verbirgt sich hinter SSI? Was steht technisch dahinter? Was bringt die SSI in der Praxis? Welche Gremien sind an der Entwicklung beteiligt? Wann wird sie kommen? Diese und viele weitere Fragen werden in der nächsten Ausgabe der IT-SICHERHEIT beantwortet.

Weitere geplante Themen sind unter anderem:

- *Zukunft von Firewalls*
- *Sichere E-Mail-Kommunikation – auch mit übergroßen Dateien möglich?*
- *Was sollte ein modernes Mail-Gateway heute leisten?*

... und vieles mehr.

IN UNSEREM VERLAG ERSCHEINEN AUSSERDEM NOCH FOLGENDE ZEITSCHRIFTEN

IMPRESSUM

IT-SICHERHEIT
Mittelstandsmagazin 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:
Viktoria Meyer
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. 26
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)

Beilagen: DATAKONTEXT GmbH, Frechen;
Titelbild: ©Oleksandr Hrinchenko/stock.adobe.com; ©Tryfonov/stock.adobe.com; ©Martin Capek/stock.adobe.com
Fotos: Firmenbilder; DATAKONTEXT; stockunlimited.com; Amadeus Bramsiepe, Markus Breig; ©iStock.com/Chiradech, ©iStock.com/ipopba; ©Gorodenkoff Productions OU; ©AndSus/stock.adobe.com, ©dani3315/stock.adobe.com, ©dennizn/stock.adobe.com, ©electriceye/stock.adobe.com , ©grandeduc/stock.adobe.com, ©H. Brauer/stock.adobe.com, ©j-mel/stock.adobe.com, ©jamesteohart/stock.adobe.com, ©jirsak/stock.adobe.com, ©K.-U. Häßler/stock.adobe.com, ©nikolae/stock.adobe.com, ©photoschmidt 2018/stock.adobe.com, ©Redshinestudio/stock.adobe.com, ©Robert Kneschke/stock.adobe.com, ©rost9/stock.adobe.com, ©Siarhei/stock.adobe.com, ©stockphoto-graf/stock.adobe.com, ©Studicon/stock.adobe.com, ©tomasknopp/stock.adobe.com, ©tostphoto/stock.adobe.com

26. Jahrgang 2020 · ISSN: 1868-5757

Foto: fotogestoeber, Adobe Stock

GDD-Datenschutz-Akademie:

Jetzt wieder mit Präsenzschulungen

...und weiterhin auch digital.

Alle Schulungstermine finden Sie unter:
www.datakontext.com

Was wir wollen: Deine digitale Seite

Foto ©Markus Feger; Composing ©Jens Ripperger

Bundesamt
für Sicherheit in der
Informationstechnik

Als Cyber-Sicherheitsbehörde des Bundes kümmern wir uns darum, dass die Menschen in Deutschland der digitalen Welt vertrauen können. Mit derzeit rund 1000 Beschäftigten gestalten wir IT-Sicherheit in Deutschland – aber auch in Europa und der Welt.

Eine große Aufgabe für engagierte Fachleute, deren Herz auf der digitalen Seite schlägt.

Erfahren Sie mehr: **www.bsi.bund.de/karriere**

Weitere Informationen: **bewerbung@bsi.bund.de** oder unter Tel.: 0228 99 9582 6388.

Deutschland
Digital·Sicher·BSI·