HZ212318 · ISSN 1868-5757 · www.datakontext.com Oktober/November 5/2022

IT-SICHERHEIT

Magazin für Informationssicherheit und Datenschutz

Die Zukunft der Authentifizierung

Eine Welt ohne Passwörter ist möglich!

Tobias Becker von LastPass erklärt, wie Mitarbeitende einfach, nahtlos und komfortabel arbeiten – ob im Büro, im Homeoffice oder von unterwegs.

SPECIAL

it-sa 2022

Nürnberg, 25. bis 27. Oktober

- **Orientierung:** Was Sie wo auf der it-sa erwartet
- **Trends:** Welche technologischen Trends Sie auf dem Schirm haben sollten
- **Markt:** Welche Anbieter/ Aussteller Sie dafür ansprechen können

Safe AI:
Wie künstliche Intelligenz nachvollziehbar und sicher werden soll

Cybersicherheit:
Dreigespann gegen Ransomware

Confidential Computing:
IT-Sicherheit und Datenschutz in der Cloud

DATAKONTEXT

interflex
UPGRADES YOUR WORK

Flexibel und sicher in die Cloud.

Jetzt mehr erfahren.

SCHONEN SIE IHRE RESSOURCEN UND SETZEN SIE AUF IT-SICHERHEIT – AUS EINER HAND.

Mit Interflex Managed Services setzen Sie auf eine Systemplattform, die Ihre Zeiterfassung, Zeitwirtschaft und Personaleinsatzplanung mit den Vorteilen der Zutrittskontrolle und des Besuchermanagements in einem cloudbasierten Service vereint.

- **Schnelle Reaktionsfähigkeit für dynamische Märkte**
- **Skalierbare, modulare IT-Lösung nach Ihren Anforderungen**
- **Hohe IT-Sicherheit durch regelmäßige Updates**

Profitieren Sie von einer vielseitigen Gesamtlösung.
Lassen Sie sich jetzt beraten.

www.interflex.com

A BRAND OF
ALLEGION

VERTRAUENSWÜRDIGKEIT IST DAS SCHMIERMITTEL DER MODERNEN IT

Stefan Mutschler

Daten sind heute die Schlüsselkomponente in der Wertschöpfung. Ihre sichere und vertrauenswürdige Verarbeitung ist daher essenziell – auch in Cloud-Infrastrukturen, die per se erst einmal nicht vertrauenswürdig sind. Während die Daten und der Code der sie verarbeitenden Anwendung hier in gespeicherter Form und bei der Übertragung in der Regel verschlüsselt sind, liegt beides während der Verarbeitung von Anwendungen in einer Cloud-Infrastruktur im Klartext vor und ist somit angreifbar. Confidential Computing soll das ändern. Auf der Basis von Sicherheitsfunktionen im Rechenkern sorgt Confidential Computing dafür, dass Anwendungen auf Cloud-Infrastrukturen mit allem drum und dran in isolierten und verschlüsselten Enklaven verarbeitet werden. Die Inhalte der Anwendung in einer Enklave werden so zuverlässig vor unbefugtem Zugriff geschützt.

Auch wenn das alles wenig spektakulär klingt, ist Confidental Computing ein entscheidender Aspekt, der für die Zukunft der IT-Sicherheit unerlässlich ist: Die ständige Interaktion von Softwarebausteinen zwischen verschiedenen IT-Umgebungen gehört zum Wesen der Cloud – und dank Confidental Computing kann das nun in gesicherter Form stattfinden. Damit ist die Basis für sicheres Cloud Computing gelegt – moderne IT kann reibungslos genutzt werden. Was es im Einzelnen mit Confidental Computing auf sich hat, lesen Sie im gleichnamigen Beitrag in unserer Rubrik „Aus Forschung und Technik".

it-sa-SPECIAL

Erfreulicherweise kann die it-sa auch in diesem Jahr wieder in Präsenz stattfinden. Nach einem etwas vorsichtigen postpandemischen Neustart im vergangenen Jahr sind nun offenbar wieder alle Schleusen offen. Im Vergleich zur bisher größten Veranstaltung im Jahr 2019 belegt die it-sa 2022 mit über 600 angemeldeten Unternehmen noch einmal mehr Ausstellungsfläche. Dabei zeichnet sich ab, dass die diesjährige Ausgabe auch sehr international geprägt sein wird. Aus derzeit 27 Ländern sind die bisherigen Beteiligungen eingegangen.

IT-SICHERHEIT hat das zum Anlass für ein umfangreiches it-sa-Special in dieser Ausgabe genommen. Was Sie in unseren Beiträgen nicht finden, sind Produktneuheiten und Firmenlistungen. Vielmehr haben wir aktuelle technische und strategische Megatrends in der IT-Security aufgegriffen und anschaulich erklärt. Vieles davon werden Sie beim it-sa-Rundgang wiederfinden und – so unser Plan – perfekt einzuordnen wissen. Im Marktteil können Sie nachschauen, welche Know-how-Träger und Lösungsanbieter auf jeden Fall einen Besuch auf der Messe lohnen.

Die IT-SICHERHEIT finden Sie wie gewohnt am **DATAKONTEXT-Stand** in **Halle 6, Nummer 6-101.**

Viel Spaß beim Lesen und eine erfolgreiche Messe wünscht Ihnen,

Stefan Mutschler

twitter.com/it_sicherheit24

www.itsicherheit-online.com/newsletter

INHALT

SPECIAL: IT-SA EXPO&CONGRESS 2022 **27**

DIE ZUKUNFT DER AUTHENTIFIZIERUNG **18**

SANS INSTITUTE SCHLIESST RAHMENVERTRAG MIT DEM BUNDESAMT DER BUNDESWEHR

Das SANS Institute, einer der weltweit führenden Anbieter von Cyber-Security-Trainings und -Zertifizierungen, unterstützt ab sofort die Bundeswehr beim Training und der Zertifizierung von Fachleuten auf dem Gebiet der Informationssicherheit. Bis 2026 können sich Angehörige der Bundeswehr durch den Rahmenvertrag über die verschiedenen Kurse des SANS Institutes und den GIAC-Zertifizierungen fort- und weiterbilden. Das SANS Institute unterstützt seit vielen Jahren militärische Organisationen in den USA und in Europa und bietet für die Ausbildung der Soldaten Cyber-Security-Trainings an, die durch die weltweit anerkannte GIAC-Zertifizierung den Wissenstand dokumentieren. Ein Beispiel für dieses Engagement ist der „International Service Cup", eine Cyber Range für militärische Organisationen, an der Teilnehmer aus den 14 Eyes-Ländern teilgenommen haben.

Herbert Abben, Director SANS EMEA (Foto: SANS Institute)

„Dem Bundesamt für Ausrüstung, Informationstechnik und Nutzung der Bundeswehr (BAAINBw) danken wir für die gute Zusammenarbeit und die Unterstützung bislang. Wir freuen uns, damit unseren Beitrag für die optimale Einsatzbereitschaft der Bundeswehr leisten zu können, vor allem vor dem aktuellen Hintergrund des Ukraine-Konflikts. Das Ziel muss sein, die Soldat:Innen so zu befähigen, dass sie Einrichtungen der Bundeswehr vor modernen Cyberattacken, egal aus welcher Richtung und mit welchem politischen oder wirtschaftlichen Ziel, bestmöglich schützen," erklärt Herbert Abben, Director SANS EMEA, verantwortlich für die Region Deutschland und Österreich. ■

CHECK POINT SCHLIESST IOT-KOOPERATION MIT INTEL

Check Point Software Technologies hat eine neue Kooperation mit der Intel Corporation angekündigt. Check Point Quantum IoT Protect wird in der neuen Plattform Intel Pathfinder for RISC-V für IoT-Geräteentwickler verfügbar sein. Zu oft wurde die Cybersicherheit bei der Entwicklung von IoT-Geräten wie IP-Kameras, Routern, Klimatechnik und medizinischen Geräten erst nachträglich berücksichtigt. Der Grund dafür ist, dass diese Geräte in der Regel nur über eine begrenzte Verarbeitungsleistung und einen begrenzten Speicherplatz verfügen, sodass nur wenig Platz für herkömmliche Sicherheitssoftware bleibt. Auf IoT-Geräten laufen außerdem oftmals ältere Betriebssysteme, die nicht gepatcht werden können, schwache oder Standardpasswörter verwenden und nicht auf Sicherheitsverletzungen geprüft werden. Leider haben es Cyberkriminelle auf diese anfälligen IoT-Geräte abgesehen, um sich Zugang zu einem Unternehmensnetzwerk zu verschaffen. Sobald sie in das Netzwerk eingedrungen sind, können sie sich quer durch das Unternehmen bewegen, um Zugriff auf sensibles geistiges Eigentum und Daten zu erhalten, die sie durch Malware und Ransomware ausnutzen können. ■

SENTINELONE KOOPERIERT MIT ARMIS FÜR ASSET INTELLIGENCE

SentinelOne gibt eine neue Integration mit Armis, der führenden Unified Asset Intelligence-Plattform, bekannt. Die Zusammenarbeit ermöglicht es Unternehmen, sich vor modernen Bedrohungen zu schützen und bietet eine einheitliche Sichtbarkeit über Endpunkte, Cloud, Mobile, IoT, OT, IoMT, Assets und mehr. Transparenz ist für Sicherheits- und Betriebsteams unverzichtbar, aber je komplexer die Netzwerke werden, desto schwieriger wird es, den gleichen granularen Überblick zu behalten und die Angriffsfläche zu reduzieren. Da Unternehmen Schwierigkeiten haben, Sicherheitswarnungen zuzuordnen, auf laufende Bedrohungen zu reagieren und ihre Angriffsfläche proaktiv zu verkleinern, werden sie immer anfälliger für Malware und Ransomware.

„Unverwaltete Assets stellen eine äußerst attraktive Angriffsfläche für Bedrohungsakteure dar. Wir bieten einzigartige Asset-Intelligenz und Transparenz sowohl bei verwalteten als auch bei nicht verwalteten Geräten, sodass Kunden die Angriffsfläche schnell reduzieren können, um ihre Unternehmen vor Angriffen von außen zu schützen", so Ed Barry, VP Strategic Alliances bei Armis. „Die Kooperation ermöglicht es uns, ein neues Maß an umfassender Transparenz und Kontext anzubieten, um Angriffe effektiver zu bewerten und zu entschärfen." ■

ZERO TRUST EXCHANGE SICHERHEITSPLATTFORM ERFÜLLT DIE C5-ANFORDERUNGEN DES BSI

Zscaler erhielt seine Compliance mit den Anforderungen des C5-Katalogs des Bundesamts für die Sicherheit in der Informationstechnik (BSI) von einem unabhängigen Auditor bestätigt. Dabei geht es um die Zscaler Cloud-Infrastruktur mit ihren 150 globalen Rechenzentren. Der aktuelle C5-Standard des BSI erfasst 125 Anforderungen in 17 Bereichen und baut unter anderem auf ISO 27001 und 27017 auf, um Behörden und Unternehmen detaillierte Informationen zum Betrieb, der Verfügbarkeit, der Organisation von Informationssicherheit und zur physikalischen Sicherheit eines geprüften Cloud-Anbieters zur Verfügung zu stellen. Für Zscaler belegt der Report das kontinuierliche Commitment für die Einhaltung der erforderlichen Sicherheitskontrollmechanismen zum Betrieb der eigenen Cloud-Infrastruktur Zero Trust Exchange aufbauend auf den Standards der Bundesbehörde.

Der Cloud Computing Compliance Criteria Catalogue (C5) spezifiziert die Mindestanforderungen zur Informationssicherheit eines Cloud-Service-Anbieters. Organisationen erhalten damit die nötige Transparenz zu den implementierten Sicherheitskontrollen eines Cloud-Services, die für die Auswahl des Anbieters sowie für das eigene Risikomanagement und Assessment zum Einsatz kommen kann. Die Cloud-Plattform von Zscaler bietet öffentlichen und privaten Organisationen eine validierte Lösung für den sicheren Zugriff auf Cloud-, Internet- und Software-as-a-Service-(SaaS-)Anwendungen von jedem Gerät oder Standort aus und erfüllt oder übertrifft dabei die behördlichen Anforderungen. ■

RADAR CYBER SECURITY ERHÄLT MILLIONEN-INVESTMENT

Der europäische Anbieter von Cyber-Security-Lösungen Radar Cyber Security gibt den erfolgreichen Abschluss einer Finanzierungsrunde in der Höhe von drei Millionen Euro bekannt. Mit frischem Kapital will der Cyber-Security-Spezialist mit Hauptsitz in Wien auf die massiv gestiegene Nachfrage im Kontext jüngster globaler Entwicklungen reagieren und seine Position bei Cyber Security „Made in Europe" weiter vorantreiben. „Das Thema Cybersicherheit erlebt aktuell eine Zeitenwende. Eine neue politische Situation in Europa hat zu einer enorm gestiegenen Nachfrage unserer Cybersicherheitslösungen geführt. Unternehmen sowie Institutionen sehen sich mit neuen Herausforderungen zu dieser Aufgabe konfrontiert. Diese neue Finanzierung hilft uns als Unternehmen darauf zu reagieren, uns zukunftssicher aufzustellen und uns auf weiteres Wachstum vorzubereiten", so Ali Carl Gülerman, CEO von Radar Cyber Security.

Das Unternehmen will seine Aktivitäten als SOC-Ausstatter mit seiner eigenentwickelten SOC-Technologie für den Eigenbetrieb oder als Managed Security Service Provider intensivieren und setzt diese mit seinen SOC-as-a-Service Dienstleistungen im eigenen CDC (Cyber Defense Center) in Wien auch weiter selbst ein. Besonderes Augenmerk legt Radar Cyber Security auf den Schutz der kritischen Infrastruktur (KRITIS) vor Cyberbedrohungen sowie auf die Rüstung dieser betroffenen Unternehmen für gesetzliche Vorgaben (zum Beispiel NIS2-Richtlinie der Europäischen Union oder deutsches IT-Sicherheitsgesetz 2.0). Hier setzt Radar Cyber Security neben der selbstentwickelten Technologie auf anerkannte Standards wie etwa ISO 27001 sowie auf Partnerschaften wie mit der EnBW Cyber Security GmbH, Tochter der Energie Baden-Württemberg. ■

Ali Carl Gülerman, CEO von Radar Cyber Security (Foto: Radar Cyber Security)

AQUA SECURITY STARTET NEUES PARTNERPROGRAMM „AQUA ADVANTAGE"

Aqua Security, Spezialist für Cloud-Native-Security, hat sein neues Channelprogramm „Aqua Advantage Ecosystem" und das begleitende Partnerportal vorgestellt. Das neue Programm wurde entwickelt, um alle Partner und deren Kunden bei Einführung und Nutzung der Cloud Native Application Protection Platform (CNAPP) zu unterstützen. Ziel ist es, Partnern aktiv dabei zu helfen, die digitale Transformation ihrer Kunden zu beschleunigen und sie beim Übergang in die neue Ära von DevSecOps und Cloud Native Applications zu begleiten. Speziell in der EMEA-Region – in der knapp ein Drittel aller Partner beheimatet ist – hat der Anbieter seine Channel-Ressourcen erst kürzlich verdoppelt und regionale technische Bewertungsprogramme eingeführt, um sicherzustellen, dass Partner für die Aqua-Technologie zertifiziert werden können. Das neue Programm geht über kurzfristige Umsatzgenerierung hinaus: Es ist ein komplettes Ökosystem von mehr als 250 branchenführenden Technologiepartnern, Resellern und Dienstleistern. Im Rahmen des neuen Programms arbeitet Aqua mit Partnern aus verschiedenen Geschäftsmodellen zusammen, um eine für alle Seiten vorteilhafte Strategie mit darauf abgestimmten Zielen zu entwickeln und gleichzeitig umfangreiche Ressourcen für den Erfolg bereitzustellen. ■

ARCTIC WOLF ÜBERNIMMT CYBER-THREAT-INTELLIGENCE-ANBIETER VXINTEL

Arctic Wolf gibt die Übernahme von vxIntel, einem führenden Anbieter von Cyber Threat Intelligence, bekannt. Die Malware-Intelligence-Plattform von vxIntel analysiert derzeit über 500.000 Dateien pro Tag und über zehn Terabyte Daten pro Monat aus über 100 globalen Datenquellen. Der enorme Umfang der Plattform hat dazu beigetragen, dass das Unternehmen eine der größten Malware-Datenbanken der Welt aufgebaut und sich zu einer wichtigen Threat-Intelligence-Quelle für Organisationen, Regierungsbehörden und führenden Cybersicherheitsunternehmen auf der ganzen Welt entwickelt hat.

Im Mai dieses Jahres hat Arctic Wolf „Arctic Wolf Labs" angekündigt, eine Initiative, die Sicherheitsforscher, Datenwissenschaftler und Security Development Engineers von Arctic Wolf in einem Team zusammenführt, das sich auf Threat Detection and Response für Kunden, Partner und die gesamte Security Community konzentriert. Das vxIntel-Team soll Teil der Arctic Wolf Labs werden. Sein fundiertes Wissen über die moderne Malware-Landschaft wird eine Schlüsselrolle bei der Verbesserung der Threat-Detection-Funktionalitäten der Arctic Wolf Security Operations Cloud spielen sowie dabei, die operativen Erkenntnisse mit der Cyber-Security-Forschungsgemeinschaft zu teilen. ■

NOTARIELLES ONLINE-VERFAHREN IM GESELLSCHAFTSRECHT

Als „Meilenstein der Digitalisierung des Notariats" bezeichnet die Bundesnotarkammer die erste Online-Gründung einer GmbH, die am 1. August 2022 vorgenommen wurde. Neben der GmbH-Gründung sind nun auch Anmeldungen zum Handels- und Genossenschaftsregister digital möglich. Für die Konzeption und Neuentwicklung der zentralen Fachanwendung zur Umsetzung von Online-Verfahren im Gesellschaftsrecht hat die Bundesnotarkammer den IT-Dienstleister adesso beauftragt.

Die von adesso entwickelte Lösung ist eine ergänzende Option zum persönlichen Termin beim Notar vor Ort: Gesellschaftsrechtliche Vorgänge wie Bestellungen zum Geschäftsführer oder die Änderung der Geschäftsadresse können ab sofort auch einfach und bequem online erledigt werden. adesso hat die Anwendung im Rahmen eines dreijährigen Softwareentwicklungsprojekts im Auftrag der Bundesnotarkammer erstellt. Die Anwendung besteht aus einem webbasierten System für die Notarseite und auf Bürgerseite aus einer Webanwendung und einer kostenfreien Smartphone-App, die unter der Bezeichnung „Notar" in den App-Stores für Android und iOS erhältlich ist. Jens Spitczok von Brisinski leitet bei adesso den Geschäftsbereich Öffentliche Verwaltung und beschreibt die Besonderheit des Projekts: „Wir freuen uns über den erfolgreichen Start der neuen Online-Verfahren bei der Bundesnotarkammer. Für adesso war die Anbindung der geschaffenen Lösung an die Bestands- und Umsysteme im Notarwesen mit Integration moderner Sicherheitsmechanismen wie eID zur elektronischen Fernsignatur und moderner Videokonferenztechnik ein besonderes Highlight." ■

Jens Spitczok von Brisinski (Foto: adesso)

SCHUTZ VON CLOUD-INFRASTRUKTUREN DURCH CONTINUOUS SECURITY VERIFICATION

Mitigant, die cloudnative Sicherheitslösung des Start-ups Resility GmbH, gegründet von Absolventen des Hasso-Plattner-Instituts, stellt sich der deutschen Security-Community vor. Seit ihrem AWS-Public Release am 1. August können deutsche mittelständische Unternehmen von der modernen Cloud-Security-Posture-Management-Lösung profitieren. Zu den Features der aktuellen Version zählen Continuous Cloud Compliance Management, Cloud Assets Inventory, Secure Drift Management und Automated Assessments & Notifications. Weitere Funktionen sollen im Laufe des Jahres hinzukommen.

Von bisherigen Cloud-Sicherheitslösungen unterscheidet sich Mitigant durch seinen Security-Chaos-Engineering-Ansatz. Er ermöglicht es IT-Sicherheitsteams, proaktiv für Sicherheit in Cloud-Infrastrukturen zu sorgen. Die Lösung geht über die reine Erkennung und Behebung falsch konfigurierter Cloud-Ressourcen weit hinaus. Sie ist in der Lage, selbstständig verdächtige Anomalien innerhalb von Cloud-Infrastrukturen aufzuspüren und zu analysieren. Darüber hinaus führt sie ähnlich einem Penetrationstest automatisiert Cloud-Angriffsszenarien durch, um die Widerstandsfähigkeit der Cloud-Infrastruktur gegenüber unterschiedlichen Cloud-Angriffsszenarien zu testen. Der Ansatz erlaubt es IT-Sicherheitsteams zu ermitteln, wie resilient die Cloud-Infrastruktur ihres Unternehmens tatsächlich ist. „Uns war aufgefallen, dass der deutsche Markt keine wirklich zufriedenstellende Lösung zur Abwehr der immer komplexer und erfolgreicher werdenden Cloud-Angriffe bereithielt", so Nils Karn, CEO der Resility GmbH. „Eingehende Recherchen und Nachfragen in der Security-Community bestätigten unsere Einschätzung. 2021 haben wir deshalb Resility gegründet und mit der Entwicklung der kommerziellen Cloud-Sicherheitslösung Mitigant begonnen. Dabei hatten und haben wir vor allem die Cloud-Sicherheitsbedürfnisse des deutschen Mittelstands im Blick." ■

KOSTENLOSE INFORMATIONEN ZUR ABWEHR DER ZUNEHMENDEN „HUMAN LAYER"-ATTACKEN

KnowBe4 bietet ein kostenloses Informationspaket für Cybersicherheit an, um Administratoren dabei zu helfen, ihr Security-Awareness-Training zu intensivieren. Dieses Paket enthält einen Benutzerleitfaden und wöchentliche Schulungsvorschläge, die bei der Planung des Monats helfen. Das „Kit" enthält Benutzerressourcen mit acht interaktiven Schulungsmodulen und Videos, zum Beispiel ein neues interaktives Schulungsmodul, „2022 Social Engineering Red Flags". Darüber hinaus enthält das Kit mehrere Infografiken zur Security Awareness, Hinweise und Tipps, Poster zur Security Awareness, digitale Beschilderungen und vieles mehr – alles zum ersten Mal in mehreren Sprachen verfügbar.

Stu Sjouwerman, CEO von KnowBe4 (Foto: KnowBe4)

„Der Cybersecurity Awareness Month bietet eine hervorragende Gelegenheit, dieses Informationspaket mit IT-Fachleuten und Benutzern zu teilen", sagt Stu Sjouwerman, CEO von KnowBe4. „Diese Ressourcen zielen darauf ab, Organisationen mit Schulungsplänen und Initiativen zur Security Awareness zu helfen, um die Notwendigkeit des Aufbaus einer Sicherheitskultur unter den Benutzern zu vermitteln und zu erkennen." Das Thema des diesjährigen Cybersecurity Awareness Month 2022 der National Cybersecurity Alliance lautet: „See Yourself in Cyber". Das KnowBe4-Informationspaket für den Cybersecurity Awareness Month 2022 ist auf der Seite von KnowBe4 downloadbar. ■

SECRETS HUB FÜR AWS SECRETS MANAGER

CyberArk stellt die neue Software-as-a-Service-(SaaS-)Lösung CyberArk Secrets Hub vor. Secrets Hub erleichtert Entwicklern in hybriden Umgebungen die Nutzung von Secrets auf Amazon Web Services (AWS) mit dem AWS Secrets Manager. Sicherheitsverantwortliche behalten dabei die zentrale Kontrolle und können einheitliche Richtlinien für das Secrets Management umsetzen.

In der Vergangenheit mussten Unternehmen Secrets von CyberArk zum AWS Secrets Manager replizieren, was zeitaufwendig und fehleranfällig sein konnte. Heute arbeitet die Mehrheit der Unternehmen in hybriden Modellen. Ein durchgängiges und automatisiertes Secrets Management über verschiedene Umgebungen hinweg kann die Migration von Unternehmen in die Cloud deutlich beschleunigen, da keine Veränderung der Sicherheitsprozesse erforderlich ist. Secrets Hub ist Teil der CyberArk Identity Security Platform und wurde in Zusammenarbeit mit dem AWS-Secrets-Manager-Team entwickelt, um ein effizientes Secrets Management in hybriden Umgebungen zu ermöglichen. CyberArk Secrets Hub repliziert automatisch die von CyberArk verwalteten Secrets, die für die Verwendung auf AWS bestimmt sind, in den AWS Secrets Manager. Damit können Nutzer:

- Secrets über mehrere AWS-Accounts und hybride Umgebungen hinweg bei gleichzeitiger Sicherstellung der Datentrennung zentral verwalten
- Berechtigungen für Secrets Hub auf dem jeweiligen AWS-Account konfigurieren
- eine synchronisierte Richtlinie erstellen
- auf die synchronisierten Secrets unter Nutzung von AWS zugreifen.

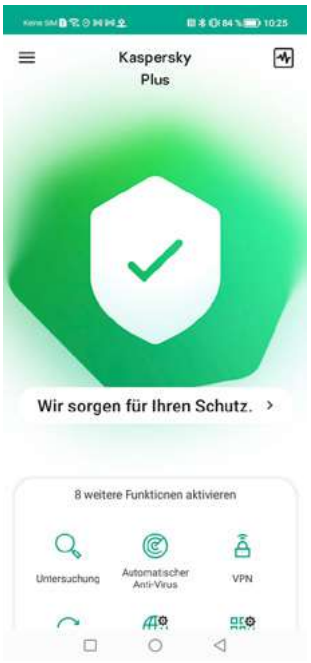
Sicherheitsverantwortliche können eine Richtlinie und einen Standard für das gesamte Unternehmen – auch für verteilte Umgebungen – zentral verwalten und umsetzen, ohne die Compliance- und Audit-Prozesse zu verändern. ■

NEUES HEIMANWENDER-PORTFOLIO VERFÜGBAR

Das überarbeitete Portfolio für Heimanwender von Kaspersky – Kaspersky Standard, Kaspersky Plus und Kaspersky Premium – ist ab sofort in Deutschland, Österreich und der Schweiz im Abo-Modell verfügbar. Neben den neuen Benennungen und einer Reihe neuer Funktionen bietet die neue Produktlinie eine verbesserte Nutzeroberfläche und -erfahrung über mehrere Plattformen hinweg. Darüber hinaus

decken die neuen Heimanwenderlösungen alle Kategorien des modernen Verbraucherschutzes ab: von Cybersicherheit über Datenschutz bis hin zur technologischen Leistungsfähigkeit und Identitätsschutz.

Um auf die aktuelle Bedrohungslandschaft sowie neue Herausforderungen und Bedürfnisse, die unter anderem Smarthome und das Metaverse mit sich bringen, zu reagieren, hat Kaspersky sein Portfolio für Heimanwender vereinfacht und neu konzipiert; es geht jetzt deutlich über einen reinen Antivirenschutz hinaus und weist den Weg für die kommenden Jahre. Die neue, vereinfachte Produktlinie wurde in drei Kategorien unterteilt – Kaspersky Standard, Kaspersky Plus und Kaspersky Premium. Das aktualisierte Angebot ist nun plattformunabhängig und bietet Schutz für verschiedene Gerätetypen unter Windows, Mac, iOS und Android. Sie sind so konzipiert, dass sie genau den Funktionsumfang abdecken, der den Nutzern im gesamten Kaspersky-Ökosystem zur Verfügung steht. ■



So sieht Kaspersky Plus auf Android-Smartphones aus. (Quelle: Kaspersky)

STORNEXT IN AWS

Quantums File System StorNext ist ab sofort als Abonnement im AWS Marketplace verfügbar. Der AWS Marketplace ist ein Katalog mit Tausenden auf Amazon Web Services (AWS) nutzbaren Softwarelösungen unabhängiger Anbieter. Nutzer von AWS können Software im AWS Marketplace einfach finden, testen, kaufen und nutzen. Der AWS Marketplace ist eine der schnellsten Möglichkeiten, um über StorNext gemeinsam nutzbaren Speicher einzurichten. Mit Quantum StorNext in AWS können Kunden ihre Inhalte unter anderem für die Videoproduktion hochflexibel verwalten. Sie können im Team von beliebigen Standorten aus Videos in der Cloud bearbeiten, ohne dass Dateien zwischen den Benutzern kopiert oder übertragen werden müssen. Dies vereinfacht die Zusammenarbeit und beschleunigt Workflows für die Postproduktion enorm. Quantum StorNext in AWS Marketplace ist ab sofort verfügbar. ■

FLASH-SPEICHER FÜR DIE INDUSTRIE

KIOXIA Europe hat mit der Auslieferung von Warenmustern seiner neuen industrietauglichen Flash-Speicher begonnen. In der aktuellen Produktreihe kommt die fünfte und neueste Generation des BiCS FLASH 3D mit TLC-Technologie (Triple-Level Cell) zum Einsatz, die drei Bits pro Zelle speichern kann. Die fünfte Generation der Speichermedien ist zuverlässig, robust und unterstützt industrietypische Temperaturen. KIOXIA wählte für seine Speichergeräte ein 132-BGA-Gehäuse. Die Speicherdichte reicht von 512 Gigabit (64 Gigabyte) bis 4 Terabit (512 Gigabyte), um die Anforderungen industrieller Anwendungen zu erfüllen. Dadurch sind die Flash-Speicher unter anderem für die Verwendung in der Telekommunikation, in Netzwerken sowie beim Embedded Computing geeignet.

Die Anforderungen vieler industrieller Anwendungen stehen im starken Kontrast zu den Bedingungen in klimatisierten Rechenzentren, in denen SSDs normalerweise laufen. Dazu gehört neben dem Einsatz in erweiterten Temperaturbereichen auch die Fähigkeit, hohe Zuverlässigkeit und Leistungsfähigkeit unter rauen Betriebsbedingungen zu gewährleisten. KIOXIA hat seine neuen Flash-Speicher unter Berücksichtigung dieser Anforderungen entwickelt, sodass sie einen breiten Temperaturbereich (–40 °C bis +85 °C) unterstützen. ■

Die fünfte und neueste Generation des BiCS FLASH 3D mit TLC-Technologie. (Foto: KOXIA)

SUITE VON COMPLIANCE- UND SICHERHEITSÜBERWACHUNGS-LÖSUNGEN FÜR GESCHÄFTS-KRITISCHE SYSTEME

Logpoint gibt die Markteinführung von Business-Critical Security (BCS) für SAP bekannt, einer Suite von Sicherheits- und Compliance-Lösungen, die es Unternehmen ermöglicht, ihre geschäftskritischen Systeme zu sichern. BCS für SAP behebt Sicherheitslücken und Compliance-Herausforderungen mit vier verschiedenen Lösungen: Security & Audit Compliance Monitoring, Business Integrity Monitoring, Personal Identifiable Information (PII) Access Monitoring und IT Service Intelligence (IT-SI). SAP ist mit einem Anteil von 87 Prozent am gesamten Welthandel das Rückgrat der Weltwirtschaft. SAP-Anwendungen unterstützen Unternehmen bei der Verwaltung wichtiger Geschäftsprozesse wie Enterprise Resource Planning (ERP), Product Lifecycle Management, Customer Relationship Management (CRM) und Supply Chain Management. Zahlreiche Branchen, darunter die Fertigungsindustrie, die IT-Branche, der Finanzdienstleistungssektor und der Großhandel, verlassen sich auf SAP, um ihr Geschäft am Laufen zu halten. Die neue Suite von Logpoint BCS für SAP-Lösungen ermöglicht es Unternehmen, die Sicherheit zu erhöhen, die Geschäftskontinuität zu gewährleisten und Compliance-Anforderungen zu erfüllen:

- *Security & Audit Compliance Monitoring* bietet vollständige Echtzeit-Sicherheitseinblicke in die gesamte IT- und SAP-Infrastruktur, um die Erkennung von Ereignissen, die die SAP-Sicherheit und Compliance gefährden, sowie die Reaktion auf Vorfälle zu vereinfachen.
- *Business Integrity Monitoring* bietet kontinuierliche Überwachung und automatisierte Kontrollen, um Unternehmen in die Lage zu versetzen, abweichende Muster von Standard-SAP-Geschäftsprozessen zu identifizieren und Fehler und Betrug sofort zu erkennen.
- *PII Access Monitoring* überwacht das Verhalten und die Aktivitäten von SAP-Benutzern, um den unbefugten Zugriff auf kritische Transaktionen oder sensible Daten wie personenbezogene Daten zu erkennen, und unterstützt Unternehmen bei der Einhaltung von GDPR und anderen PII-Anforderungen.
- *IT-SI* bietet eine kontinuierliche Überwachung der Betriebsfunktionen, die es Unternehmen ermöglicht, Ursachen und zukünftige Serviceverschlechterungen zu erkennen, sodass sie schnell auf Probleme reagieren können, die die Stabilität des SAP-Systems gefährden.

Die Suite von Logpoint BCS für SAP-Lösungen basiert auf einer Brückentechnologie, die komplexe Daten aus SAP-Systemen extrahiert und in ein SIEM integriert, um eine proaktive Überwachung zu ermöglichen. ■

Business-Critical Security (BCS) für SAP ermöglicht Unternehmen, ihre geschäftskritischen Systeme zu sichern. (Quelle: Logpoint)

GESCHÄFTSFORTGANG AUCH NACH CYBERATTACKEN AUFRECHTERHALTEN

IGEL, Anbieter des Managed-Endpoint-Betriebssystems IGEL OS für den sicheren Zugriff auf jeden digitalen Arbeitsplatz, führt das IGEL-Desaster-Recovery-Programm ein. Mit diesem neuen Programm können Unternehmen schnell die Kontrolle über von Malware betroffene Geräte wiedererlangen, um die Auswirkungen eines Cyberangriffs, einschließlich Ransomware-Attacken zu mindern und die Produktivität der Endbenutzer schnell wiederherzustellen.

Das IGEL-Desaster-Recovery-Programm soll alles umfassen, was nach einer Cyberattacke für den kurzfristigen Aufbau einer Endgeräte-Landschaft mit IGEL OS benötigt wird: neben der IGEL Hard- und Software ist das vor allem ein Technical Relationship Manager, ein versierter Techniker von IGEL, der die vorhandene Infrastruktur des Kunden kontinuierlich im Blick hat und sicherstellt, dass die IGEL OS-Versionen auf den UD Pockets mit den PC-Konfigurationen des Kunden kompatibel bleiben. ■

florian krumm/unsplash

Die Cybersicherheitsagenda des BMI

Spätestens seit Ausbruch des Ukraine-Kriegs ist sich nicht nur die Politik, sondern auch die Wirtschaft der Notwendigkeit einer Cybersicherheitsstrategie bewusst. So haben seit Beginn des Jahres laut repräsentativer Bitkom-Umfrage 43 Prozent der von Cyberangriffen betroffenen Unternehmen mindestens eine Attacke aus China identifiziert (2021: 30 Prozent). 36 Prozent haben Urheber in Russland ausgemacht (2021: 23 Prozent), was einem rasanten Anstieg seit Ausbruch des Kriegs geschuldet ist.

In der jüngst vorgestellten Cybersicherheitsagenda des Bundesministeriums des Innern und für Heimat (BMI) hat Bundesministerin Nancy Faeser Ziele für die Cybersicherheit des Landes festgelegt. Dabei soll sich das Bundesamt für Sicherheit in der Informationstechnik (BSI) als Zentralstelle für Sicherheitsfragen in der IT im Bund-Länder-Verhältnis etablieren.

Cybersicherheit durch digitale Souveränität

Faeser stellt insbesondere Unternehmen der kritischen Infrastruktur (KRITIS) in die Pflicht, sich bei voranschreitender Digitalisierung auf neue Bedrohungslagen aus dem Cyberraum vorzubereiten. Doch gleiches gelte auch für neue und disruptive Technologiefelder wie automatisiertes Fahren, Telemedizin und Smart-City-Lösungen. Das BMI strebt deshalb einen Informationsaustausch insbesondere unter KMU an, um den Bedrohungen aus dem Cyberraum zu begegnen. Außerdem sollen Forschungsprojekte zur Stärkung der digitalen Souveränität und der Ausbau der Kommunikationstechnologien 5G und 6G vor dem Fremdeingriff in Unternehmen und öffentliche Einrichtungen schützen.

Achim Berg, Präsident des Digitalverbandes Bitkom, weist allerdings darauf hin, dass der Erfolg der Cybersicherheitsagenda unter anderem von der zeitkritischen Umsetzung abhängt: „Es ist wichtig, dass die angekündigte Cybersicherheitsstrategie nun zeitnah folgt und nicht auf die lange Bank geschoben wird. Die Umsetzung der heute vorgestellten Maßnahmen muss schnell spezifiziert und die kritischen Themen müssen geklärt werden."

Weiterbildungsangebot im Bereich IT-Sicherheit

Die Bitkom Akademie bietet zahlreiche Fortbildungen im Bereich IT-Sicherheit an, und ist als anerkannter Schulungsanbieter des BSI in der Lage, die digitalen Kompetenzen zur Umsetzung einer umfassenden Cyberstrategie im Unternehmen zu vermitteln.

Unter anderem bilden die Zertifikatslehrgänge zum BSI IT- Grundschutz-Praktiker und die Aufbauschulung CSN Vorfall-Experte die konkreten Anforderungen des Bundesministeriums im Curriculum ab. Darüber hinaus bietet die Bitkom Akademie Spezialschulungen für Betreiber kritischer Infrastrukturen an, insbesondere im Kontext des neuen IT-Sicherheitsgesetzes 2.0. Doch auch die kostenfreien Angebote der Akademie können bereits den Stein ins Rollen bringen und den entscheidenden Anstoß zur Aufdeckung interner Sicherheitslücken liefern.

Zielgruppe

Das Angebot der Akademie richtet sich an Mitarbeitende aller Branchen mit Arbeitsbezug und Schnittstellen zur Informationssicherheit, ganz gleich ob angehende IT-Administratoren, IT-Fachkräfte, Datenschutzbeauftragte, Projektmanager oder Führungskräfte im Allgemeinen. Das Seminarprogramm der Bitkom Akademie beinhaltet Kurse für Einsteiger als auch erfahrene IT-Fachleute – Vorkenntnisse sind deshalb von Vorteil, aber nicht zwingend erforderlich. Die Seminare haben didaktisch eine allgemeine Ausrichtung, um auch auf individuelle Fragen und Problemstellungen aller Teilnehmenden einzugehen. ■

Für weitere Informationen kontaktieren Sie bitte Vincent Bergner: v.bergner@bitkom-service.de

Mehr dazu hier

https://bitkom-akademie.de/seminare

bitkom akademie

KRITIS-Konferenz in Leipzig verhilft kritischen Infrastrukturen zu mehr Sicherheit

PROTEKT 2022

Vor dem Hintergrund des Kriegs in der Ukraine und den Nachwirkungen der Corona-Pandemie stehen kritische Infrastrukturen vor großen Herausforderungen. Drohende Engpässe in der Energieversorgung zählen ebenso dazu wie gestörte Lieferketten und eine zunehmende Zahl an Cyberangriffen. Diesen und vielen weiteren wichtigen Themen rund um den Schutz kritischer Infrastrukturen widmet sich die protekt (2. bis 3. November 2022 in Leipzig).

Die *protekt* ist eine etablierte Konferenz und versammelt Experten aus ganz Deutschland. Sie vermittelt aktuelles Know-how und treibt den sektorenübergreifenden Austausch voran. Die Schirmherrschaft haben in diesem Jahr Nancy Faeser, die Bundesministerin des Innern und für Heimat, und Thomas Popp, Sächsischer Staatssekretär für Digitale Verwaltung und Verwaltungsmodernisierung, übernommen.

Die *protekt* gilt als die einzige Konferenz in Deutschland, die den Schutz kritischer Infrastrukturen vollumfänglich beleuchtet. Sie thematisiert gleichermaßen IT-Sicherheit und den physischen Schutz. Mit ihrem Konzept aus Vorträgen, Workshops und Diskussionsrunden sowie begleitender Ausstellung und vielfältigen Networking-Möglichkeiten hat sie sich in den vergangenen Jahren als wichtiger Treffpunkt von KRITIS-Betreibern und der Sicherheitsindustrie etabliert. Zum Einzugsgebiet zählt inzwischen auch Österreich.

Das hochkarätige Konferenzprogramm der protekt versammelt namhafte Referenten, die sich aktuellen Themen und Best-Practice-Beispielen widmen, durch interaktive Workshops führen und ihr Fachwissen in Round-Table-Diskussionen teilen. (Foto: protekt)

NAMHAFTE EXPERTEN, AKTUELLE THEMEN UND BEGLEITENDE AUSSTELLUNG

Das hochkarätige Konferenzprogramm der *protekt* versammelt namhafte Referenten, die sich aktuellen Themen und Best-Practice-Beispielen widmen, durch interaktive Workshops führen und ihr Fachwissen in Round-Table-Diskussionen teilen. Themenübergreifende Plenarvorträge gehen Hand in Hand mit vertiefenden Vorträgen in den parallelen Tracks IT-Sicherheit und physischer Schutz.

Mit Spannung erwartet wird die Keynote von Arne Schönbohm, Präsident des Bundesamtes für Sicherheit in der Informationstechnik (BSI). Er wird interessante Einblicke in die Rolle des BSI bei der Cybersicherheit kritischer Infrastrukturen liefern. Über „Resiliente Infrastrukturen in Zeiten von Krisen und Katastrophen" berichtet Christian Reuter, Generalsekretär und Vorstandsvorsitzender des Deutschen Roten Kreuzes (DRK). Der zweite Konferenztag beginnt im Podium mit einem Round-Table namhafter Experten zum brisanten Thema Versorgungssicherheit. Im Anschluss erläutert Prof. Dr. Marcus Wiens von der Technischen Universität Bergakademie Freiberg in seinem Vortrag, wie eine Lebensmittelnotversorgung durch öffentlich-private Partnerschaft gelingen kann.

Der große Themenkomplex Cybersicherheit wird von verschiedenen Seiten beleuchtet. Die Konferenzteilnehmer lernen unter anderem Best Practices zur Erkennung und Abwehr von zielgerichteten Angriffen sowie im Vortrag von Harald Wenisch, Sprecher der Experts Group IT Security der Wirtschaftskammer Österreich, zur Forensik bei Großschadenslagen durch Cybercrime und Cyberwar kennen. Über neueste Methoden bei Spionage, Sabotage und Cyberangriffen informieren zwei Experten vom Wirtschaftsschutz in Niedersachsen und in Nordrhein-Westfalen. Außerdem steht unter anderem das Thema Fachkräftemangel in kritischen Infrastrukturen im Fokus.

In der begleitenden Ausstellung der *protekt* präsentieren acht Premiumpartner ihre Produkte und Dienstleistungen, die sich speziell an den Bedürfnissen kritischer Infrastrukturen orientieren. Vertreten sind unter anderem Myra Security als Spezialanbieter für digitale Sicherheit, der Beratungsdienstleister TTS Trusted Technologies and Solutions und das Deutsche Rote Kreuz (DRK).

HOCHKARÄTIGE UNTERSTÜTZUNG DURCH SCHIRMHERREN, TRÄGER UND PARTNER

Den hohen Stellenwert der *protekt* demonstrieren ihre prominenten Unterstützer. Die Bundesministerin des Innern und für Heimat, Nancy Faeser, und Thomas Popp, Sächsischer Staatssekretär für Digitale Verwaltung und Verwaltungsmodernisierung, Mitglied der Sächsischen Staatsregierung, haben die Schirmherrschaften übernommen. Staatssekretär Popp und ein Vertreter des BMI wollen die *protekt* am ersten Veranstaltungstag mit Keynotes bereichern.

Unterstützt wird die *protekt* von einem kompetenten Partnernetzwerk. Als ideelle Träger fungieren der Bundesverband für den Schutz Kritischer Infrastrukturen (BSKI), der Verband für Sicherheitstechnik (VfS), der Bundesverband Allianz für Sicherheit in der Wirtschaft (ASW) und der Fachinformationsdienstleister DATAKONTEXT GmbH. ■

S.M.

Safe AI – Absicherung von künstlicher Intelligenz

DAS UNKALKULIERBARE BERECHENBAR MACHEN

Ein wichtiges Qualitätsmerkmal von künstlicher Intelligenz (KI) ist deren Sicherheit – zum einen die Sicherheit vor Missbrauch und Schutz der Daten (Security), aber vor allem auch der Schutz der Menschen, die mit dem System interagieren (Safety). Die Forscherinnen und Forscher des Fraunhofer IKS bieten verschiedene Ansatzpunkte zur Absicherung Ihrer KI-Lösung. Für den Einsatz in Fahrzeugen oder in der Industrie ist es besonders relevant, Sicherheit mit Wirtschaftlichkeit zu verbinden.

In einer 2020 veröffentlichten Studie befragte der Verband der TÜV e.V. Personen zu ihren Sorgen im Zusammenhang mit künstlicher Intelligenz. Bedenken, dass KI in sicherheitskritischen Anwendungsfällen Fehler machen könnte, wurden von 67 Prozent der Befragten geäußert. 85 Prozent der Befragten sind der Meinung, KI-basierte Produkte sollten erst auf den Markt gebracht werden dürfen, wenn eine herstellerunabhängige Stelle deren Sicherheit überprüft hat. Die Autoren empfehlen daher, KI-Anwendungen nach Sicherheitsrisiko zu priorisieren und sicherheitskritische Produkte wiederkehrend zu prüfen.

WARUM NEUE METHODEN ZUR ABSICHERUNG VON KI NÖTIG SIND

Im Unterschied zu klassischen Algorithmen besteht bei KI-Anwendungen allerdings das Problem, dass die einzelnen Lernschritte nicht von Menschen interpretiert werden können. Da der Entscheidungsweg der KI undurchsichtig ist, kann die Sicherheit und Zuverlässigkeit der KI bisher nicht ohne Weiteres bewertet werden. Diese Nachvollziehbarkeit ist aber notwendig, um Unsicherheiten der KI messbar zu machen und daraufhin dynamische Sicherheitsmechanismen zu entwerfen. Ziel des Fraunhofer IKS ist es, kognitive Systeme sicherheitsbewusst zu machen. Über eine adaptive, erweiterte Softwarearchitektur werden Fehler der KI abgefangen, damit die KI Menschen nicht gefährden kann.

Ein weiteres Forschungsziel unter dem Schlagwort „Explainable AI" ist es, neuronale Netze selbst nachvollziehbar zu konzipieren. Dies ist eine Grundvoraussetzung für die Absicherung und Zertifizierung von KI-Systemen. Zudem muss das System lernen können, wie es mit gefährlichen Situationen, unklaren Sensordaten oder Fehlverhalten umgeht. Durch die umfassende Absicherung der KI entstehen sichere und gleichzeitig leistungsstarke kognitive Systeme: safe AI

ZUVERLÄSSIGE MASCHINELLE WAHRNEHMUNG BEIM AUTONOMEN FAHREN

Um in Zukunft autonom fahren zu können, müssen Fahrzeuge in der Lage sein, ihre Umgebung zu erkennen, treffsicher zu interpretieren und daraufhin ihre Handlungen zu optimieren. Das ist nur mit KI-Algorithmen möglich. Bisher ist aber das maschinelle Sehen (Perzeption oder Computer Vision) der KI noch nicht so verlässlich, dass es für den Einsatz in autonomen Fahrzeugen auf öffentlichen Straßen geeignet ist.

FRAUNHOFER IKS SAFE AI: UNSICHERHEITEN SICHTBAR MACHEN

Zunächst müssen daher Wege gefunden werden, Unsicherheiten der künstlichen Intelligenz quantifizierbar zu machen, um das Verhalten der KI sinnvoll bewerten zu können. Das Fraunhofer-Institut für Kognitive Systeme IKS arbeitet daran, nachweisbar verlässliche Systeme zu schaffen, indem es Unsicherheiten der KI zunächst einen interpretierbaren Wert zuweist und sichtbar macht. So kann die bisher intransparente Klassifizierung der künstlichen Intelligenz beherrschbar werden. Nur mit dieser Transparenz können passende und flexible Sicherheitskonzepte entworfen werden, um mit den Unsicherheiten der KI umzugehen.

Monitoring

Ein Ansatz des Fraunhofer IKS ist es, künstliche Intelligenz um eine erweiterte Softwarearchitektur zu ergänzen. Diese überwacht die KI und prüft die getroffenen Entscheidungen auf Plausibilität. Dieses Monitoring funktioniert über klassische Software, welche mit bewährten Safety-Methoden beherrscht und überprüft werden kann.

Dynamisches Safety-Management

Gleichzeitig wird der KI durch den Ansatz des dynamischen Safety-Managements mehr Freiraum gegeben als durch klassische Safety-Ansätze, die immer vom Worst-Case-Szenario ausgehen. So können die Vorteile der schnellen Datenverarbeitung durch maschinelles Lernen genutzt und gleichzeitig mögliche Fehlentscheidungen abgefangen werden. Das ist für die Verwendung von kognitiven Systemen in sicherheitskritischen Anwendungen relevant. Ein typisches Beispiel ist, wenn – wie beim autonomen Fahren – durch Fehlentscheidungen der KI Menschenleben gefährdet wären.

Continuous Deployment

Kognitive Systeme müssen auf dem Feld lernen können, denn so kann das System neu kennengelernte Situationen wiedererkennen und passend handeln. Das kann allerdings nicht durch lernende Algorithmen geschehen, da sonst wieder Undurchsichtigkeit entstünde. Das Continuous Deployment ist daher ein wichtiger Bestandteil des Absicherungskonzepts des Fraunhofer IKS. Das System muss regelmäßig aktualisiert werden, um neuentdeckte Sicherheitslücken schnell zu schließen und den Funktionsumfang zu erweitern.

Modulare Architekturen

Als wichtigen zusätzlichen Schritt der Absicherung entwickelt das Fraunhofer IKS modulare Architekturen. Durch eine modulare Safety-Architektur aus individuellen Blöcken ist eine schnelle und unkomplizierte Erweiterung des Systems möglich. So können die Ergebnisse der Safety-Analysen kostensparend implementiert werden, indem nur wenige Module ersetzt werden. ■

FRAUNHOFER IKS/S.M.

Forschende übertragen digitalen Zwilling des Verkehrs ins Auto

(AUTONOMES) FAHREN MIT INSIGHTS AUS DER VOGELPERSPEKTIVE

Nicht „über den Wolken“, aber zumindest über dem Maisfeld und wohl auch über dem Hauseck: Im Forschungsprojekt Providentia++ haben Forschende der Technischen Universität München (TUM) zusammen mit Industriepartnern eine Technologie entwickelt, welche die Fahrzeugperspektive auf Basis von Bordsensoren durch eine Sicht aus der Vogelperspektive ergänzt. Das klare Ziel: mehr Sicherheit im Verkehr – auch und besonders für das autonome Fahren.

Die Sensorik an Masten und auf Schilderbrücken sind die Voraussetzung für den digitalen Zwilling. (Foto: Stefan Woidig/TUM)

Ein Fahrzeug muss nicht nur bei geringem Tempo sicher fahren, sondern auch bei hoher Geschwindigkeit“, so Jörg Schrepfer. Liegt etwa verloren gegangene Ladung auf der Autobahn, reicht die „Ego“-Perspektive des Autos oft nicht aus, um sie frühzeitig zu sehen. „Ein sanftes Manöver wird in diesem Fall schwer“, meint der Head of Driving Advanced Research Germany bei Valeo. Deshalb haben die Forschenden im Projekt Providentia++, welches das Bundesministerium für Digitales und Verkehr (BMDV) im Rahmen einer Förderung für automatisiertes und vernetztes Fahren über fünfeinhalb Jahre unterstützt hat, ein System entwickelt, mit dem eine weitere Perspektive der Verkehrssituation in Fahrzeuge übermittelt werden kann. „Mithilfe von Sensoren an Schilderbrücken und Sensormasten haben wir auf unserer Teststrecke einen zuverlässigen Echtzeitzwilling des Verkehrs geschaffen, der rund um die Uhr im Einsatz ist“, erläutert Prof. Alois Knoll vom Konsortialführer TUM: „Damit haben wir die Voraussetzung dafür geschaffen, die Sicht des Fahrzeugs durch eine externe Sicht – nämlich aus der Vogelperspektive – zu ergänzen und zudem das Verhalten anderer Verkehrsteilnehmer in Entscheidungen einzubeziehen.“

LATENZEN DURCH ALGORITHMEN UND NEUE MOBILFUNKTECHNOLOGIE MINIMIEREN

Das ist nicht trivial: Denn der digitale Zwilling muss wissen, wo genau sich das Fahrzeug befindet, in das die Informationen der Sensorstationen per Funk übertragen werden sollen. Damit das gelingt, setzt Projektpartner Valeo auf ein sogenanntes IMU-GNSS-System (kurz für: Inertial Measurement Unit – Global Navigation Satellite System), bestehend aus einer Messeinheit und einem Satellitennavigationssystem sowie einem Realtime-Kinematik-Kit. „So schaffen wir ein Koordinatensystem in Echtzeit, das zentimetergenau ist", erläutert Valeo-Experte Schrepfer. Damit nun die Informationen aus den Fahrzeugen und den Messstationen des digitalen Zwillings synchronisiert werden können, nutzen die Forschenden den UTC-Standard, welcher eine einheitliche Zeitbasis liefert. Idealerweise würde sich das digitale Abbild wie eine zweite Schicht über die Perspektive des Autos legen.

Allerdings lassen sich Verzögerungen (Latenzen) im Gesamtsystem nicht ganz vermeiden. Von der physikalischen Aufnahme der Sensoren über die Weiterverarbeitung der Daten und Übertragung ins Fahrzeug vergeht Zeit. Daten werden verpackt, codiert, versendet und im Auto wieder decodiert. Hinzu kommen weitere Randbedingungen, die eine Rolle spielen, etwa wie weit das Fahrzeug vom Sendemast auf der Teststrecke entfernt ist und wie belegt das Übertragungsnetz ist. In einer Demonstrationsfahrt arbeitete Valeo kürzlich mit LTE (4G)-Funkgeschwindigkeit, was eine Verzögerung von 100 bis 400 Millisekunden verursachte. „Ganz vermeiden lassen werden sich diese Latenzen nie, allerdings hilft uns hier eine intelligente Algorithmik", erläutert Schrepfer: „Noch besser wird das Ergebnis sein, wenn künftig die Funktechnologien 5G oder 6G flächendeckend im Einsatz sind."

Über einen Mobilfunkmast an der Autobahn A9 werden die Daten des digitalen Zwillings verteilt. (Foto: Stefan Woidig/TUM)

„Mit dem digitalen Echtzeitzwilling haben die Voraussetzung dafür geschaffen, die Sicht des Fahrzeugs durch eine externe Sicht aus der Vogelperspektive zu ergänzen"

PROF. ALOIS KNOLL,
Technische Universität München.
(Foto: Stefan Woidig/TUM)

PROTOTYP VON DIGITALEM ECHTZEITZWILLING VERFÜGBAR

Die Voraussetzung dafür, dass diese Daten nun im Fahrzeug genutzt werden können, wurde im Forschungsprojekt Providentia++ gelegt. Ziel war es, einen digitalen Zwilling des Verkehrs zu erzeugen, der echtzeitfähig, skalierbar und hochverfügbar ist. Dafür baute das Forscherteam eine 3,5 Kilometer lange Teststrecke in Garching bei München, bestehend aus sieben Sensorstationen. Der Prototyp wurde so entwickelt, dass er künftig bei Bedarf in Serie einsetzbar ist:

- Die Forschenden arbeiten mit dezentralen digitalen Zwillingen, wodurch eine Teststrecke beliebig verlängert beziehungsweise skaliert werden kann.
- Um Datenmengen von mehreren Gigabyte pro Sekunde bewältigen zu können, entstand ein Datenverarbeitungskonzept, das die Leistungen der Rechenkernen (CPUs) und Grafikkarten (GPUs) optimal untereinander aufteilte.
- Als besondere softwaretechnische Herausforderungen stellten sich die Sensorkalibrierung und die Entwicklung der Tracking-Algorithmen heraus. Eine entsprechende Software gab es noch nicht. „Wir haben nun ein automatisches Kalibrierungsverfahren anhand einer hochauflösenden Straßenkarte (HD-Karte) im Einsatz, das es noch nicht gab und von uns entwickelt wurde", erläutert der technische Projektleiter Venkatnarayanan Lakshminarashiman aus dem Lehrstuhl für Robotik, künstliche Intelligenz und Echtzeitsysteme der TUM.

Der Leiter des Konsortiums Prof. Alois Knoll von der TUM zieht ein ausgesprochen positives Resümee: „Der digitale Zwilling ist reif für die sich anschließende konkrete Produktentwicklung, läuft zuverlässig im 24/7-Betrieb und steht nicht nur auf der Autobahn, sondern auch für Landstraßen und im Kreuzungsbereich zur Verfügung." ■

S.M.

Die Zukunft
der Authentifizierung

Eine Welt ohne Passwörter

Einerseits nehmen Cyberangriffe auf Unternehmen weiter zu, andererseits wollen Mitarbeitende möglichst einfach, nahtlos und komfortabel arbeiten – ob im Büro, im Homeoffice oder von unterwegs. Wie IT-Security-Abteilungen diesen Spagat managen, verrät **Tobias Becker,** SaaS Sales Leader für die DACH-Region beim Sicherheitsexperten LastPass, im Interview.

ITS: Die Zahl der Cyberangriffe auf Unternehmen steigt, das ist wohl eine Tatsache. Wie ist Ihre aktuelle Einschätzung diesbezüglich?

Tobias Becker: Da haben Sie recht. Die Zahl der Angriffe auf Unternehmen, Behörden und Institutionen steigt tatsächlich. Das ist zum einen einer steigenden kriminellen Energie geschuldet, andererseits aber auch den neuen Angriffsflächen, die Unternehmen bieten.

Nehmen Sie nur Mobility, Cloud, Internet of Things. Unsere IT-Landschaften werden immer komplexer und verändern sich durch neue Nutzer, Dienste und Geräte. Dazu kommen virtuelle und software-definierte Infrastrukturen. Daraus entstehen eben auch neue Risiken und das verlangt von den jeweiligen Organisationen, die IT-Security anpassungs- und zukunftsfähig zu gestalten.

ITS: Wie zeigt sich das in der Praxis?

Tobias Becker: Nun, in einer International Data Group Studie haben 66 Prozent der befragten IT-Manager angegeben, gerade auch im Homeoffice seien die Mitarbeitenden zunehmenden Cyberrisiken ausgesetzt. 31 Prozent konstatierten sogar, die Beschäftigten arbeiteten zu Hause mit ungeschützten Geräten. Angesichts dessen ist es klar, dass die IT-Helpdesks immer mehr Probleme haben, die Mitarbeitenden zu schützen.

ITS: Also mehr und dickere Bollwerke? Da werden Unternehmen doch zu wahren Festungen?

Tobias Becker: Nein, „intelligentere Lösungen" sollte man sagen. Alles in allem müssen wir zwei Dinge gleichzeitig meistern: Durch das neue „Work-from-Anywhere" den Zugang der User zu ihren Ressourcen erleichtern und andererseits die Cyberrisiken minimieren. Das ist ein Prozess, an dem alle Beteiligten mitarbeiten.

ITS: Intelligentere Lösungen – wie ist das zu verstehen?

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

ITS: Und dann kommt Passwort-Management ins Spiel …?

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

vladgrin - stock.adobe.com

Sobald man den Authenticator mit dem Passwort-Vault gekoppelt hat, kann man sich per einfachem Fingertipp anmelden. Ganz ohne Master-Passwort.

vladgrin - stock.adobe.com

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

ITS: Es ist ja aber auch häufig von einer gänzlich passwortlosen Zukunft die Rede, wird das kommen?

Tobias Becker: Wir können Nutzern jetzt das passwortfreie Anmelden beim Passwort-Vault mit einem Authenticator anbieten. Sobald man den Authenticator mit dem Passwort-Vault gekoppelt hat, kann man sich per einfachem Fingertipp anmelden. Ganz ohne Master-Passwort.

Zusätzlich arbeiten wir auch an der Entwicklung FIDO2-konformer Komponenten und der Unterstützung weiterer Authentifizierungsmethoden wie der biometrischen Gesichts- und Fingerabdruckserkennung. Auch Hardware-Sicherheitsschlüssel wie YubiKey sollen in Zukunft zur Anmeldung möglich sein. Diese passwortfreien Anmeldemethoden werden sehr bald zur Verfügung stehen.

ITS: Das ist ja dann ein ziemlicher Schritt in Richtung besseres Nutzererlebnis für die Mitarbeitenden, oder?

Tobias Becker: Mit Sicherheit. Passwörter stellen für viele Anwender ja noch immer eine echte Hürde bei der Akzeptanz neuer Technologien oder Tools dar. Die meisten Mitarbeitenden haben heute ca. 50 Onlinekonten und möchten diese trotz Sicherheitsbewusstsein ohne großen Aufwand nutzen können. Mit dem passwortfreien Anmelden ist das möglich: auf das Vault zugreifen, ohne jemals ein Passwort einzugeben.

ITS: Und was denken IT-Security-Abteilungen?

Tobias Becker: Viele IT-Administratoren sagen, dass Passwörter in ihrem Unternehmen alle drei Monate zurückgesetzt werden müssen. Wenn Passwörter nun einfach ganz wegfallen, verschwenden IT-Teams keine Zeit mehr mit dem Zurücksetzen und müssen sich nicht mehr mit vergessenen Passwörtern und ähnlich banalen Problemen herumschlagen. Das minimiert ihre Risiken, gibt ihnen Zeit für Wichtigeres und erhöht die Produktivität.

ITS: Bleibt die Frage: Wie steht es dann mit der IT-Sicherheit selbst?

Tobias Becker: Das liegt eigentlich auf der Hand: Zwar wissen über 90 Prozent der Anwender, dass Passwörter aus Sicherheitsgründen nicht wiederverwendet werden sollten, aber fast zwei Drittel tun es trotzdem. Wenn die Leute ein Passwort für mehrere Konten verwenden, freuen sich Hacker natürlich, denn dann können mit nur einem Schlüssel gleich mehrere Türen geöffnet werden. Je weniger Passwörter Sie also insgesamt verwenden, desto weniger wertvolle Daten können potenziell im Darknet preisgegeben werden. Eine simple Rechnung.

ITS: Was bringt die Zukunft der IT-Sicherheit?

Tobias Becker: Man muss das realistisch sehen: Hier ist ein Wettrüsten im Gange, mit dem wir alle leben müssen. Cyberkriminelle und Cyberbedrohungen werden sich weiterentwickeln und häufiger, schneller und perfider zuschlagen. Unternehmen, öffentliche Verwaltungen und Institutionen werden sich deshalb permanent Gedanken machen müssen, welche Sicherheitsmaßnahmen in Zukunft notwendig sind und welche Verantwortungen sie selbst und welche ihre Security-Anbieter übernehmen müssen, um ihre Daten, Infrastrukturen und Nutzer optimal zu schützen.

Klar ist: IT-Sicherheit wird in Zukunft als permanenter Prozess begriffen werden müssen, und nicht lediglich als einzelne Maßnahme.

ITS: Vielen Dank für das Gespräch!

Das Interview führte Stefan Mutschler für IT-SICHERHEIT.

tete_escape - stock.adobe.com

Worauf sich Unternehmen in Sachen Authentifizierung und Passwortmanagement einstellen müssen

Sieben Punkte für die IT-Sicherheit 2022/23

Was sind derzeit die interessanten Themen in der IT-Sicherheit? Mit welchen Herausforderungen in Sachen Authentifizierung und Passwortmanagement müssen Unternehmen rechnen? In sieben Punkten spannen Sicherheitsexperten den Bogen vom Sicherheitsbewusstsein der Mitarbeitenden bis zur nahen Zukunft mit künstlicher Intelligenz (KI) und Machine Learning. Vor allem aber wird deutlich: IT-Sicherheit ist ein permanenter Prozess.

Während Unternehmen im Kontext von Cloud Services, Hybrid-Arbeit oder Internet of Things (IoT) immer komplexere IT-Strukturen aufbauen, wächst zugleich auch das Sicherheitsbedürfnis in diesem Zusammenhang, denn die Zahl der Cyberangriffe steigt weiterhin beträchtlich – und das wird wohl auch so bleiben. Doch worauf genau kommt es jetzt an?

1. NAHTLOSE NUTZERERLEBNISSE

Die Praxis in der IT-Sicherheit zeigt, dass eine wichtige Herausforderung für Sicherheitsexperten darin besteht, eine angenehme Nutzererfahrung für die Mitarbeitenden mit voller Kontrolle für die IT-Abteilung zu verbinden. Mit anderen Worten: Sicherheit muss gegeben sein, darf aber nicht die Produktivität der

Nutzer oder ihre User Experience beeinträchtigen. Dies führt zwangsläufig dazu, dass Enterprise Passwortmanager sich mit Themen wie der passwortfreien Anmeldung beschäftigen, um genau diesen Spagat zu schaffen. Hier gibt es vielversprechende Lösungen.

2. PASSWORTLOS ARBEITEN

Die momentan gängigen Methoden der Authentifizierung mit lediglich einem Usernamen und einem Passwort führen zu Social Hacking. Aber: Fast jeder ist es auch schon gewohnt, bei der Interaktion mit seinem Unternehmen, der Bank oder der Krankenversicherung einen zweiten Faktor zu benutzen wie etwa eine zusätzliche SMS oder ein zweites Einmal-Passwort.

„Passwortlos" ist schlicht und einfach eine Erweiterung davon, bei der man ein Smartphone und biometrische Daten (etwa Fingerabdruck oder Gesicht) nutzt. Das Standard-Protokoll dafür heißt FIDO2 – es wird in der Branche weithin unterstützt, so etwa auch von Microsoft, Apple und LastPass.

Passwortmanager können Nutzern jetzt schon das passwortfreie Anmelden beim Passwort-Vault mit einem Authenticator anbieten. Sobald man den Authenticator mit dem Passwort-Vault gekoppelt hat, kann man sich per einfachem Fingertipp anmelden.

3. DAS ZERO-TRUST-PRINZIP

Unternehmensinterne Zugänge dürfen angesichts neuer IT-Strukturen und Cyberbedrohungen nicht mehr grundsätzlich als vertrauenswürdig angesehen werden. Das Zero-Trust-Modell beantwortet wachsende Anforderungen der IT-Sicherheit mit gesundem Misstrauen. Die Idee: Mitarbeitende, Anwendungen und Geräte dürfen jeweils nur mit geringstmöglichen Privilegien auf das System zugreifen. Dieses „Least Privilege" genannte Prinzip macht dabei keinen Unterschied zwischen internen und externen Zugriffen. Eine so verbesserte Identitätsverwaltung stärkt den Schutz der Infrastruktur von Unternehmen zusätzlich.

4. DARKWEB-ÜBERWACHUNG

Ein guter Enterprise Passwortmanager überwacht kontinuierlich, ob unternehmensrelevante E-Mail-Adressen in Datenbanken mit gehackten E-Mail-Adressen auftauchen. So helfen Darkweb-Scans Unternehmen, sich vor Kontodiebstahl, Netzwerkangriffen, Datenverlusten und Datenschutzverletzungen zu schützen, da sie auf kompromittierte Konten aufmerksam gemacht werden. Dank zeitnaher Warnungen können Mitarbeitende ihre Passwörter sofort ändern und verdächtigen Aktivitäten auf die Spur kommen. So steigert die Darkweb-Überwachung das Cyberbewusstsein und die Cyberresilienz der User.

Admins können sehen, welche Benutzer Darkweb-Warnmeldungen erhalten haben – das ist gut für die Nachvollziehbarkeit, sollten vertrauliche Unternehmensdaten in die Öffentlichkeit gelangen. So können gegebenenfalls seitens der IT jederzeit und rechtzeitig Gegenmaßnahmen eingeleitet werden.

5. KI UND MACHINE LEARNING

Auch in der Cybersicherheit werden maschinelles Lernen (ML) und Deep Learning (DL) immer wichtiger und technologiebasierte Cybersicherheitspraktiken entwickeln sich kontinuierlich vorwärts, denn Unternehmen und ihre Dienstleister werden in Zukunft noch sehr viel mehr in der Lage sein müssen, Vorfallsdaten, fehlerhafte oder doppelte Datensätze und eine Vielzahl von Malware-Mustern über Tausende von Protokollen zu bewältigen. Deshalb werden künstliche Intelligenz (KI) und ML eine immer bedeutendere Rolle spielen, um schneller und zuverlässiger kriminelle Muster bei großen Datenmengen aufzuspüren und entsprechend frühzeitig Warnungen zu generieren.

Aber: Cyberkriminelle wissen diese Technologien auch zu nutzen und entwickeln ihre Methoden dementsprechend weiter. Unternehmen müssen also endgültig erkennen, dass IT-Sicherheit definitiv keine einzelne punktuelle Aktion ist, sondern als ein dynamischer, permanenter Prozess begriffen werden muss.

6. SICHERHEIT IN DER CLOUD

Mehr und mehr Anwendungen werden in die Cloud ausgelagert. Deshalb müssen Unternehmen sicherstellen, dass die von ihnen genutzten Cloud Services auch was die Sicherheit angeht up to date sind. Sie müssen ihr Cloud-Management im Griff haben – derzeit leider noch keine Selbstverständlichkeit. Betroffen sind hier etwa Fragen zu Verschlüsselung, Authentifizierung oder Audit-Protokollierung. Dienstleister und Unternehmen müssen hier offen miteinander umgehen.

7. LAST BUT NOT LEAST: BEWUSSTSEIN!

Egal, ob Mitarbeitende zu Hause, unterwegs oder im Büro arbeiten, ihnen muss klar sein, welche Gefahren von Cybercrimes ausgehen, welche Rolle sie selbst dabei spielen und welche Schritte und Tools zur Bekämpfung eingesetzt werden. Dabei genügt es nicht, Mitarbeitende einmal zu schulen. Das Thema „IT-Sicherheit" sollte fest in der Kultur des Unternehmens verankert sein. Nur so können IT-Manager sicherstellen, dass sich ihre User während der gesamten Arbeitszeit vorsichtig verhalten und keine Sicherheitspannen durch Leichtsinnsfehler entstehen. ■

PETER VAN ZEIST,
Principal Solutions Consultant, LastPass

Wir qualifizieren die Digitalwirtschaft.

Weiterbildungen für Fach- und Führungskräfte im Bereich IT-Sicherheit, Datenschutz und Big Data & KI.

Jetzt anmelden:
www.bitkom-akademie.de

bitkom akademie

Network Detection and Response, künstliche Intelligenz und IT-Sicherheitsexperten

DREIGESPANN GEGEN RANSOMWARE

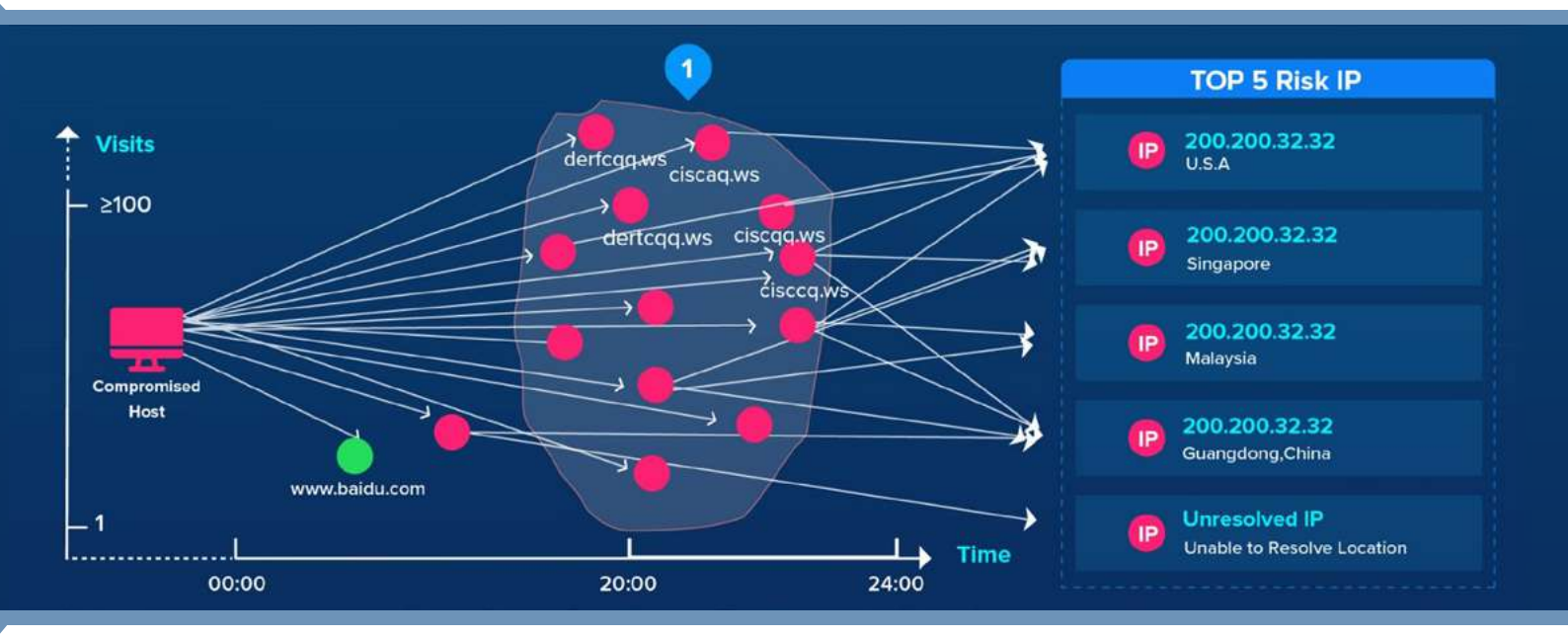
Wenn Cyberkriminelle anfangen, Daten zu verschlüsseln, ist es für die angegriffenen Unternehmen meistens schon zu spät. Komplexe Ransomware nimmt schon mit dem Eindringen der Täter in das Netz ihren Lauf. Kompetente Angreifer haben Daten exfiltriert und auch Backups verschlüsselt, bevor sie das Lösegeld einfordern. Eine frühe Erkennung ist dafür notwendig. Eine Network Detection and Response (NDR) liest bereits die ersten Spuren eines Angriffs. Künstliche Intelligenz (KI) erkennt verdächtige Netzwerkaktivitäten. IT-Sicherheitsexperten analysieren Alarme, leiten die Abwehr und helfen, Angriffe nahezu in Echtzeit zu erkennen. Sie leisten zudem gute Dienste, einmal ausgenutzte Schwachstellen für die Zukunft zu schließen.

Gefährliche, komplexe erpresserische Angriffe haben eine Vorlaufzeit. Hinter solchen Attacken steht ein eigenes Ransomware-as-a-Service-(RaaS-)Ökosystem in einer eigenen Cyber Kill Chain. Arbeitsteilig sind hier viele Akteure mit einbezogen. Drei Beteiligtengruppen hinterlassen ihre Spuren im externen und internen Datenverkehr:

- **Initial Access Broker (IABs)**
  Sie suchen im ersten Schritt mit automatisierten Tools nach Schwachstellen im Unternehmensnetz und verkaufen ihre Erkenntnisse an Hacker. Sie zielen auf offene Ports oder nicht gepatchte, den Cyberkriminellen bekannte Schwachstellen von Anwendungen.

- **Hacker**
  Hacker wissen, wie sie die von den IABs präsentierten Schwachstellen ausnutzen können, um tiefer in das Netz einzudringen und Malware am Endpunkt zu installieren. Diesen sprechen sie dann später von einem Command-and-Control-Server aus an. Als Experten für den unerlaubten Netzwerkzugriff nutzen sie vermeintlich legitime Tools, um die Zielsysteme einer Verschlüsselung zu erkennen. Das bösartige Nutzen dieser Tools lässt sich nur durch eine Verhaltensanalyse erkennen.

- **Böswillige Datenmanager**
  Sie suchen schließlich nach Informationen, um sie zu verschlüsseln und zu exfiltrieren oder um damit zu drohen, diese zu veröffentlichen. Sie begutachten, welche Informationen für das Unternehmen und seine Geschäftsabläufe am wichtigsten sind und wofür die Opfer am schnellsten ein hohes Lösegeld zahlen werden.



Hacker tarnen die Herkunft ihrer illegitimen Anfragen und ihrer C&C-Kommunikation. (Quelle: ForeNova)

KÜNSTLICHE INTELLIGENZ ERKENNT HINWEISE AUF EINEN ANGRIFF IM NETZVERKEHR

Alle diese Aktivitäten hinterlassen Spuren im Datenverkehr. Eine Network Detection and Response (NDR) erkennt die von der Norm abweichenden Muster durch einen anomalen Netzverkehr schon zu einem frühen Zeitpunkt. Einmal eingerichtet, hat sie mithilfe von maschinellem Lernen und künstlicher Intelligenz den gesamten internen und externen Netzwerkverkehr gescannt und den legitimen Normalzustand der Datenübertragung definiert. Danach erkennt sie automatisch, wenn der Datenverkehr von üblichen und damit in der Regel legitimen Mustern abweicht, etwa durch:

- **Unbekannte Teilnehmer**
  Logfiles protokollieren die Interaktion mit den unbekannten Servern der Initial Access Broker.

- **Unklare Herkunft**
  Hacker verbergen die verräterische Herkunft ihres Command-and-Control-Servers. In einem ersten Schritt agieren sie von einer gekaperten legitimen Domain und lenken dann die Antwort des angegriffenen Endpunkts auf eine bösartige IP-Adresse um. Bei komplexen Attacken generieren sie selbst per KI und Algorithmen zahlreiche Zufallsdomänen als Zieladressen, die alle auf die eigentliche Hacker-IP verweisen. Die Malware wechselt in ihrer Kommunikation zwischen diesen Domänen, um unentdeckt zu bleiben.

- **Verschlüsselung**
  C&C-Server und von ihnen in Beschlag genommene Systeme senden ihre Daten verschlüsselt, damit Sicherheitsaudits sie nicht erkennen. Ein lang andauernder, weil verschlüsselter Datenfluss zeichnet sich durch die Metadaten zum Datenverkehr aus.

- **Brute-Force-Attacken**
  Angreifer probieren eine hohe Anzahl von Nutzernamen und Passwort-Kombinationen durch, um Zugriffsrechte zu erlangen. Intelligentere Attacken der IABs tarnen ihr Vorgehen, indem sie die Log-Versuche senken oder Angriffe verteilt durchführen. Diese Muster erkennt die KI ebenso wie die typischerweise kurze Dauer einer erratischen Zugriff-Session, die Protokolle und die Kommunikation des Brute-Force-Tools mit dem C&C-Server.

- **Verdächtige Bewegungen im Netz**
  Legitime Nutzer und Applikationen kennen sich im System aus und bewegen sich gezielt dorthin, wo sie hinwollen. Ein Datenmanager, der nach wertvollen Daten oder zugleich nach zu verschlüsselnden Backups sucht, geht oft mehrere Endpunkte nacheinander ab. Oder er springt erratisch von System zu System.

- **Atypische Zugriffszeiten, -orte, und -häufigkeiten**
  Wer in den Morgenstunden etwa mit einer ungewöhnlichen IP auf ein System zugreift, ist vielleicht ein Hacker.

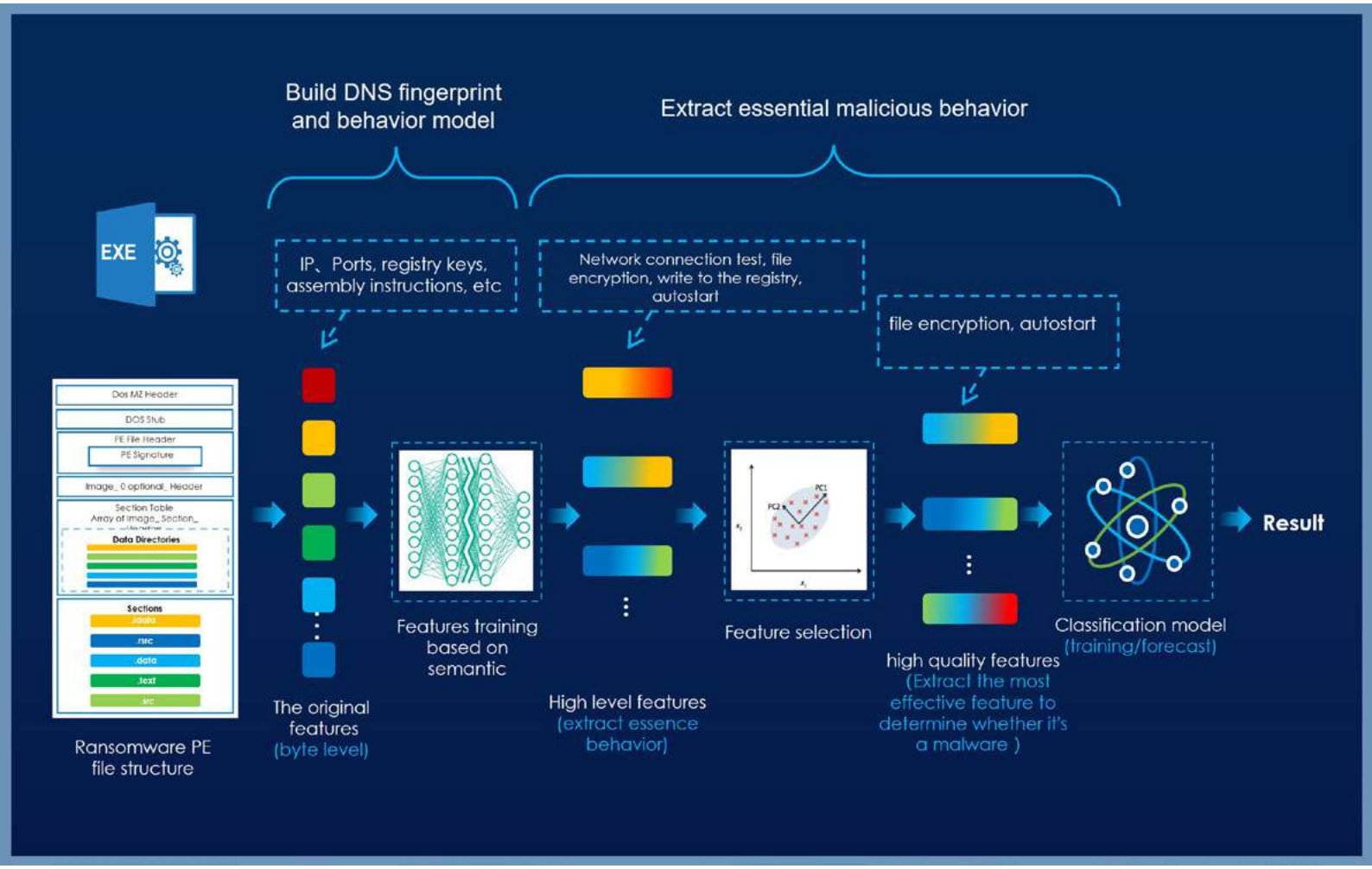
- **Datenabfluss**
  KI erkennt die Lesevorgänge, Exporte oder Kopien der böswilligen Datenmanager durch den erhöhten Datendurchsatz, den solche Prozesse verursachen.

KI UND MENSCHLICHE INTELLIGENZ IN KOMBINATION

Die KI erkennt Anomalien auf der Basis einmal erhobener und durch Machine Learning ständig kontrollierter und optimierter statistischer Werte. Doch selbst ein feinkörniges Modell des Netzverkehrs kann zu Fehlalarmen führen und analysiert nicht die weitergehenden Absichten der Kill-Chain-Mitglieder.

Schon das einfache Beispiel der unbekannten IP-Adresse zeigt, dass eine KI die Expertise von Sicherheitsexperten und das Unternehmenswissen von IT-Administratoren benötigt. Ein Partner, eine neue Niederlassung oder ein Mitarbeiter im Homeoffice beziehungsweise auf Reisen erklärt und legitimiert nämlich eine auf den ersten Blick ungewöhnliche IP-Adresse aus einem anderen geografischen Raum. Ein IT-Administrator, der über das notwendige Unternehmenswissen verfügt, und der von ihm informierte Sicherheitsexperte können daher einen atypischen oder neuen, aber legitimierten Nutzerzugriff vom Hackerangriff unterscheiden.

Sie berücksichtigen bei der Analyse der Zugriffe auch Informationen, die im Netzverkehr nicht sichtbar sind – wie etwa zum neuen Standort



Künstliche Intelligenz erkennt die einzelnen Elemente einer Ransomware – vom Byte-Level bis zum großen Merkmalbündel. (Quelle: ForeNova)

oder zu Geräten im Homeoffice des Mitarbeiters, die nicht zentral verwaltet sind.

Konkretes Unternehmenswissen hilft zudem, die tatsächliche Gefahr der einzelnen Ransomware-Attacke für Datensicherheit und die Verfügbarkeit der Geschäftsabläufe zutreffend zu beurteilen. Nur aufgrund dieser Basis kann ein Sicherheitsexperte wissen, welche Systeme, Applikationen und Informationen zusammenspielen, voneinander abhängig sind und weiterreichenden Zugang verschaffen. Dadurch kann er die zukünftigen Schritte eines Hackers vorwegnehmen, der mit seiner Ransomware-Attacke den größtmöglichen Schaden androhen will. IT-Sicherheitsexperten, IT-Teams und Management wissen zudem, welche Daten besonders wertvoll, welche Informationen im Notfall über Backup oder andere Wege wieder zu beschaffen sind oder für Dritte ohnehin nicht von Nutzen sind. Unter Umständen können sie so entscheiden, dass die Lösegeldforderung mangels wirklicher Drohkulisse ins Leere läuft.

Das menschliche Unternehmenswissen spielt eine entscheidende Rolle, um die Verhältnismäßigkeit von Abwehrmaßnahmen zu beurteilen. Der Angriff auf unternehmenskritische Daten, auf Informationen, die dem Datenschutz unterliegen, oder deren Verfügbarkeit für einzelne Prozesse unverzichtbar sind, erfordert eine schnellere Abwehr und rechtfertigt einschneidende Maßnahmen. Allein der Mensch kann entscheiden, ob etwa die Ultima Ratio der Ransomware-Abwehr – das Trennen von Geräten vom Netz – verhältnismäßig ist. Führt es etwa zum Abschalten lebenserhaltender Systeme im Krankenhaus, lässt es sich nicht rechtfertigen. Menschen müssen entscheiden, ob ein Angriff eine höhere Prioritätsstufe einfordert.

Der Beitrag des Menschen ist ebenso zentral, wenn es um die Abwehr von Folgeangriffen geht. Die Angreifer kehren gern an den Ort erfolgreicher Aktionen zurück, zumal wenn Hacker die Einfallstore und die bösartigen Datenmanager das Unternehmen schon kennen. Eine zukunftssichere und zugleich nachhaltige Abwehr erfordert daher ein lückenloses Schließen von Schwachstellen durch eine Root-Cause-Analyse des einmal erfolgreichen Hacks anhand des gespiegelt aufgezeichneten Netzwerkverkehrs. Gerade die Prävention durch das Nachbessern der IT-Abwehr wird aber zur Aufgabe für die menschlichen Experten. ■

PAUL SMIT,
Director Professional Services
bei ForeNova

HZ212318 · ISSN 1868-5757 · www.datakontext.com Oktober/November 5/2022

IT-SICHERHEIT SPECIAL

Wieder auf Wachstumskurs:

it-sa 2022 erwartet mehr als 600 Aussteller

Das **„Home of Security"** bringt Unternehmen, Verbände und Organisationen aus dem Bereich der Cybersicherheit im Messezentrum Nürnberg zusammen.

Orientierung:
Was Sie wo auf der it-sa erwartet

Trends:
Welche technologischen Trends Sie auf dem Schirm haben sollten

Markt:
Welche Anbieter/Aussteller Sie ansprechen können

DATAKONTEXT

it-sa-Special

Erfreulicherweise kann die it-sa auch in diesem Jahr wieder in Präsenz stattfinden. Nach einem etwas vorsichtigen post-pandemischen Neustart im vergangenen Jahr sind nun offenbar wieder alle Schleusen offen. Im Vergleich zur bisher größten Veranstaltung im Jahr 2019 belegt die it-sa 2022 mit über 600 angemeldeten Unternehmen noch einmal mehr Ausstellungsfläche. Dabei zeichnet sich ab, dass die diesjährige Ausgabe auch sehr international geprägt sein wird. Aus derzeit 27 Ländern sind die bisherigen Beteiligungen eingegangen.

Während der it-sa Expo&Congress 2022 erwartet die Teilnehmer ein vielfältiges Informationsangebot. Das frei zugängliche Vortragsprogramm mit Expertenbeiträgen zu aktuellen Sicherheitsthemen aus den Bereichen Technik und Management sowie die produktneutralen Beiträge und Diskussionsrunden aus der Reihe it-sa insights bringen das neueste Fachwissen der Branche nach Nürnberg. Zusätzlich bietet das Kongressprogramm Congress@it-sa ab dem 24. Oktober in Kooperation mit namhaften Verbänden und Organisationen einen intensiven Austausch zu aktuellen Themen der IT-Security.

IT-SICHERHEIT hat das zum Anlass für ein umfangreiches it-sa-Special in dieser Ausgabe genommen. Was Sie in unseren Beiträgen nicht finden, sind Produktneuheiten und Firmenlistungen. Vielmehr haben wir aktuelle technische und strategische Megatrends in der IT-Security aufgegriffen und anschaulich erklärt. Vieles davon werden Sie beim it-sa-Rundgang wiederfinden und – so unser Plan – perfekt einzuordnen wissen. Im Marktteil können Sie nachschauen, welche Know-how-Träger und Lösungsanbieter auf jeden Fall einen Besuch auf der Messe lohnen.

Die IT-SICHERHEIT finden Sie wie gewohnt am DATAKONTEXT-Stand in Halle 6, Stand 6-101.

Viel Spaß beim Lesen und eine erfolgreiche Messe wünscht Ihnen,

Stefan Mutschler

Stefan Mutschler

IMPRESSUM

IT-SICHERHEIT
Magazin für Informationssicherheit und Datenschutz

www.itsicherheit-online.com

SPECIAL: it-sa 2022

Verlag:
DATAKONTEXT GmbH
Standort Frechen
Augustinusstr. 11 A · 50226 Frechen
www.datakontext.com

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

Grafik/Layout/Satz:
Michael Paffenholz
Tel.: +49 173 8382572
E-Mail: michael.paffenholz@gmx.de
Objekt- und Anzeigenleitung:
Wolfgang Scharf
Tel.: +49 2234 98949-60
E-Mail: wolfgang.scharf@datakontext.com
zzt. gilt die Anzeigenpreisliste Nr. 27
Vertrieb/Herstellung:
Dieter Schulz
Tel.: +49 2234 98949-99
dieter.schulz@datakontext.com
Abonnement: Jahresabonnement € 104,- inkl. VK (Inland)

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

Titelbild: tampatra | wacomka - stock.adobe.com
Fotos: Firmenbilder; DATAKONTEXT; (Adobe stock, ArtemisDiana, arthead, Blue Planet Studio, Blue Planet Studio, buravleva_stock, DIgilife, languste15, MH, NicoElNino, Oleksandr, orbcat, pavel siamionov, Photocreo Bednarek, sdecoret , viperagp, Who is Danny, Zaleman) - stock.adobe.com; greenbutterfly/Shutterstock

28. Jahrgang 2022 · ISSN: 1868-5757

_Inhalt

Anbieter

it-sa 2022, Nürnberg ausgebucht

Das „Home of Security“ erwartet mehr als 600 Aussteller

Die it-sa 2022 bringt – leider wieder in den mit öffentlichen Verkehrsmitteln anreisenden Besuchern umständlich zu erreichenden Hallen 6, 7 und 7A – ausstellende Unternehmen, Verbände und Organisationen aus dem Bereich der Cybersicherheit im Messezentrum Nürnberg zusammen. Sie belegen bereits einen Monat vor Showbeginn die gesamte für dieses Jahr verfügbare Ausstellungsfläche der it-sa Expo&Congress. Zusätzliche Beteiligungsoptionen bietet die digitale Informations- und Dialogplattform it-sa 365.

Die it-sa bringt vom 25. bis 27. Oktober erneut internationale IT-Sicherheitsspezialisten und Entscheider im Messezentrum Nürnberg zusammen. „Die Rückmeldung der Aussteller zur it-sa 2022 ist überwältigend. Branchengrößen, Verbände, Institutionen und junge innovative Unternehmen – gleichermaßen fiebern sie dem persönlichen Austausch in Nürnberg entgegen“, so Veranstaltungsleiter Frank Venjakob.

Das untermauern auch die Zahlen: Im Vergleich zur bisher größten Veranstaltung im Jahr 2019 belegt die it-sa 2022 mit über 600 angemeldeten Unternehmen noch einmal mehr Ausstellungsfläche. Dabei zeichnet sich ab, dass die diesjährige Ausgabe auch sehr international geprägt sein wird. Aus derzeit 27 Ländern sind die bisherigen Beteiligungen eingegangen. „Für uns ist die positive Resonanz Grund zur Vorfreude und Ansporn zugleich. Zusammen mit dem Team der it-sa arbeiten wir weiter intensiv an der Finalisierung des Rahmenprogramms und dem Angebot unserer Online-Dialogplattform it-sa 365, die zusätzliche Beteiligungsmöglichkeiten bietet“, so Venjakob weiter.

Attraktive Beteiligungsmöglichkeiten im Rahmen der it-sa 365

Die it-sa Expo&Congress wird für die it-sa Community durch die Digitalplattform it-sa 365 parallel zur Vor-Ort-Veranstaltung erlebbar – online und damit weltweit. Beispielsweise werden Vorträge aus der Reihe „it-sa insights“ live übertragen. Ausstellende Unternehmen bringen Q&A-Sessions mit potenziellen Kunden zusammen, und User können an Live-Interviews mit Ausstellern teilnehmen. „it-sa@home“ bündelt das entsprechende Angebot als eigenen Programmpunkt auf der Plattform und sichert teilnehmenden Unternehmen damit maximale Aufmerksamkeit während der Messelaufzeit und darüber hinaus.

Erfolgreicher it-sa-Restart 2021

Der Restart ist gelungen: 274 Aussteller* aus 18 Ländern und rund 5.200 Fachbesucher aus 28 Ländern machten die it-sa 2021 vom 12. bis 14. Oktober zum Treffpunkt für IT-Sicherheitsexperten und -entscheider. „Die it-sa 2021 war ein voller Erfolg: Wie in der aktuellen Situation erwartet kleiner als die letzte Veranstaltung, für die teilnehmenden Unternehmen aber ein äußerst wirkungsvolles Marketing-Instrument“ resümiert Frank Venjakob, Director it-sa, die erste Veranstaltung nach dem coronabedingten Aussetzen im vergangenen Jahr.

IT-Sicherheit ist wichtiger denn je, darüber waren sich die Teilnehmer der Messe mit Blick auf die Zunahme von Cyberangriffen einig. Zwar steige das Bewusstsein für IT-Sicherheit, ebenso die Ausgaben in Deutschland, wie der Digitalverband Bitkom zur it-sa berichtete. Es gelte aber, Strukturen

zu schaffen, die das weitere Wachstum des IT-Sicherheitsmarktes fördern. So forderte Luigi Rebuffi, Generalsekretär der European Cyber Security Organisation, die Stärkung des Cybersicherheitssektors im europäischen Wirtschaftsraum. Der Markt für IT-Sicherheit in Europa leide im internationalen Vergleich unter einer Finanzierungslücke von mehr als vier Milliarden Euro jährlich.

Rahmenprogramm it-sa Expo&Congress 2022

Während der it-sa Expo&Congress 2022 erwartet die Teilnehmer ein vielfältiges Informationsangebot. Das frei zugängliche Vortragsprogramm mit Expertenbeiträgen zu aktuellen Sicherheitsthemen aus den Bereichen Technik und Management und die produktneutralen Beiträge und Diskussionsrunden aus der Reihe it-sa insights bringen das neueste Fachwissen der Branche nach Nürnberg. Zusätzlich bietet das Kongressprogramm Congress@it-sa ab dem 24. Oktober in Kooperation mit namhaften Verbänden und Organisationen einen intensiven Austausch zu aktuellen Themen der IT-Security.

Der begleitende Congress@it-sa bietet intensive Wissensvermittlung und vertiefte fachliche Diskussionen mit Verbänden, Branchenvereinigungen und Anbietern von IT-Security-Lösungen. Abseits des Messetrubels ein perfekter Rahmen für Know-how aus erster Hand und intensive Dialoge mit Experten. Das Kongressprogramm mit hochrangiger Beteiligung findet im im NCC Ost statt und startet bereits am 24. Oktober 2022.

Auch die offenen Vortragsbühnen sind ein regelmäßiger Besuchermagnet. An drei Messetagen findet ein attraktives Nonstop-Programm in den Fachforen der it-sa statt. Aussteller und Partnerverbände der it-sa zeigen in den Fachvorträgen, Studienanalysen und Diskussionen, wohin die Reise in der IT-Sicherheit geht. In den it-sa insights geben Experten produktneutrale aktuelle Einblicke in Branchen, Trends, Rechtsfragen und Spezialthemen. Mit Startups@it-sa bietet die it-sa jungen internationalen IT-Security-Unternehmen auch in den Foren eine Plattform, sich den Fachbesuchern zu präsentieren. ■

S.M.

Bilder: itsa 2021-Eindrücke (Fotos: Stefan Mutschler)

it-sa Expo&Congress – ÜBERBLICK

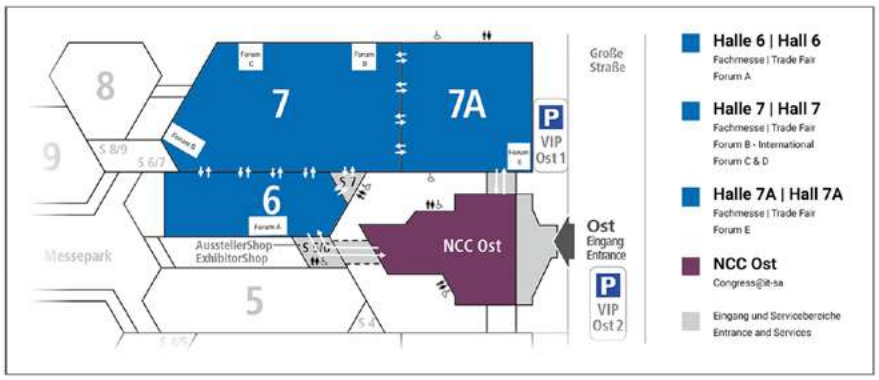
Veranstaltungsort:
Messezentrum Nürnberg

Veranstaltungstermin:
Dienstag, 25., bis Donnerstag, 27. Oktober 2022

Öffnungszeiten it-sa Expo
Dienstag, 25. Oktober 2022: 09:00–18:00 Uhr
Mittwoch, 26. Oktober 2022: 09:00–18:00 Uhr
Donnerstag, 27. Oktober 2022: 09:00–17:00 Uhr

Congress@it-sa
Montag, 24., bis Donnerstag, 27. Oktober 2022

Hallenplan und Forenplatzierung it-sa Expo&Congress 2022
Floor plan and forum placement it-sa Expo&Congress 2022



Warum moderne App-Infrastrukturen neue Sicherheitsansätze fordern

Microservice-, Container- und (Multi-)Cloud-gerechte Security

Digitalisierung steht für Innovation, Agilität, Flexibilität, Offenheit, Geschwindigkeit und Verfügbarkeit. In diesem Zuge erlebt die Entwicklung von Apps als Kern der Digitalisierung einen grundlegenden Wandel: Klassische Webapplikation werden immer häufiger durch APIs abgelöst, um offenere Strukturen zu schaffen und mehr Flexibilität zu erreichen. Auch der Aufbau von digitalen Ökosystemen spielt dabei eine maßgebliche Rolle. Um Security in komplett neu gestalteten Strukturen und Architekturen von vornherein angemessen mitzubauen, kommen neben neuen Entwicklungsmodellen wie DevOps und DevSecOps auch neue Security-Ansätze zum Einsatz - allen voran risikobasierte Authentifizierung und Continuous Adaptive Trust.

Um höhere Agilität, Verfügbarkeit und Dynamik in den Digitalisierungsbestrebungen der Unternehmen zu gewinnen, vollzieht sich ein starker Wandel der IT-Infrastruktur – weg von On-Premises hin zu hybriden Cloud-Umgebungen mit modernen Container-Technologien und Microservices. DevOps ist hier eines der großen Schlagworte. In Verbindung mit dem Continuous-Integration- und Deployment-Modell (CI/CD) lassen sich zusätzliche Vorteile realisieren, um schnell mit neuen Entwicklungen und Services auf den Markt zu kommen. Schließlich ist die Digitalisierung ein Wettlauf, bei dem es häufig darum geht, als Erstes mit neuen Diensten zu glänzen.

Schnelligkeit ist aber nur die halbe Miete. Apps müssen auch sicher sein. Und hier haben Cloud-Umgebungen mit ihren neuen Technologien einiges grundlegend verändert: Um Applikationen, APIs und Microservices bereitzustellen, werden Container-Umgebungen eingeführt und zumeist von Kubernetes oder anderen Systemen zur Verwaltung von Containeranwendungen gemanagt. All diese neuen Ansätze erfordern aber auch eine Erneuerung der Applikationssicherheit und des Zugriffsmanagements.

Was diese Veränderungen für die Security bedeuten

Webapplikationen und APIs sind die beliebtesten Angriffsziele für Hacker. Ihre Popularität unter den Angreifern verdanken sie vor allem der Tatsache, dass sie besonders exponiert sind und weltweit in sehr hoher Zahl verwendet werden – nicht zuletzt auch im DACH-Raum (Deutschland, Österreich, Schweiz). So haben laut einer im deutschsprachigen Raum durchgeführten IDG-Studie[1] 83 Prozent der Unternehmen mehr als zehn Webapplikationen im Einsatz. Zwei Drittel der befragten Unternehmen hatten dabei mehr als 20 schutzbedürftige Apps im Einsatz.

Allein in den neuen Entwicklungsprozessen (DevOps, DevSecOps) lässt sich der geforderte Schutz der Apps nicht realisieren, denn weniger als die Hälfte (44 Prozent) der Unternehmen hat überhaupt einen Einfluss auf deren Entwicklung: Der größere Teil der Web-Apps sind „ältere Erbstücke", welche die Unternehmen nicht mehr anfassen wollen, Open-Source-Web-Apps unter Copyleft-Lizenz, bei welchen die Entwicklung nicht oder kaum beeinflusst werden kann, oder proprietäre Web-Apps, bei welchen die Entwicklung grundsätzlich nicht beeinflusst werden kann.

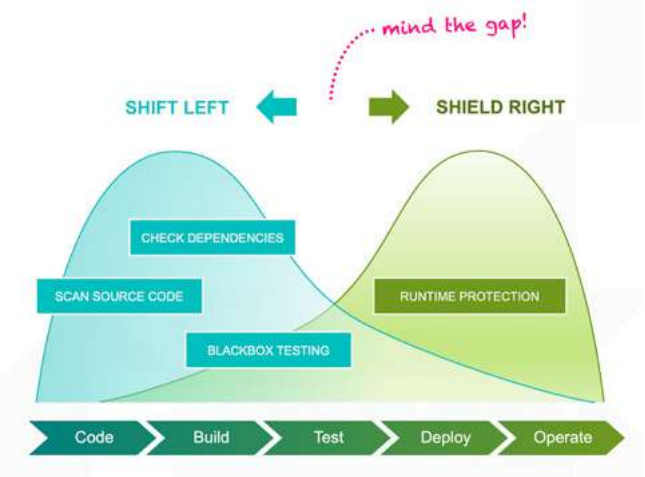
Für den Schutz der Web-Apps sind also eigenständige Security-Lösungen nötig, um gerade bei Zero-Day-Angriffen schnell mit Virtual Patching und Web Application and API Protection (WAAP) kontern zu können. Virtuelles Patching wird zunehmend als robuste Alternative zum Hersteller-Patching genutzt. Unternehmen können damit Schwachstellen in Anwendungen schnell beheben, Sicherheitsrichtlinien kurzfristig umsetzen und so ihre Anfälligkeit für Angriffe heruntersetzen. Virtuelles Patching hilft Unternehmen, Angriffe abzuwehren, indem es jederzeit vor bekannten und unbekannten Schwachstellen, einschließlich Zero-Day-Exploits, schützt. Im Gegensatz zu einer herkömmlichen Firewall ist ein WAAP ein hoch spezialisiertes Sicherheitstool, das speziell für den Schutz von Webanwendungen und APIs entwickelt wurde. Eine WAAP befindet sich am äußeren Rand eines Netzwerks, vor der öffentlichen Seite einer Webanwendung, und

analysiert den eingehenden Datenverkehr. Ein WAAP konzentriert sich nur auf die Anwendungsschicht.

Der große Vorteil von Virtual Patching und WAAP: Sicherheitslücken werden zentral und vor allem schnell beseitigt – ohne dass sofort die gesamte Web-App geprüft und umgeschrieben werden muss, getreu dem Motto „Secure now, fix later". Eine klassische Web Application Firewall (WAF) reicht dafür heute nicht mehr: Auch APIs und Microservices müssen geschützt werden und das nicht nur On-premises, sondern auch in verteilten Cloud-Umgebungen.

Security in die Entwicklungsprozesse einbinden

Nutzer, ob Mitarbeiter, Lieferanten, Kunden etc., greifen auf Hunderte Micro Services zu, die über unterschiedliche Standorte verteilt sind. Sie alle kommen mit verschiedenen Rollen ins Netzwerk, während Software gerade entwickelt, ausgerollt oder schon produktiv geschaltet ist. Die IT-Landschaft ändert sich also ständig. In einem solch dynamischen Szenario ist es nicht zielführend, am Ende noch kurz die Security anzuschauen. Es ist wichtig, dass auch Security agil wird. Agile Sicherheit bedeutet, dass es klare Prozesse gibt. Das wiederum bedeutet beispielsweise, dass standardmäßig automatisierte Tests durchgeführt werden. Ein weiterer wichtiger Aspekt von Agile Security ist Security by Design: Entscheidend ist, Security bereits beim Design zu berücksichtigen, kontinuierlich weiterzuentwickeln und damit ein Shift-Left der Security zu vollziehen. Die gesamte Infrastruktur muss regelmäßig nach Schwachstellen durchsucht werden. Das vielleicht Wichtigste ist jedoch, schnell auf Fehler, neue Bedrohungen und neue Erkenntnisse reagieren zu können. In einem agilen Unternehmen arbeiten Entwicklung und Betrieb als ein Team zusammen (DevOps). Wo – wie dringend zu empfehlen – auch agile Security integriert ist, handelt es sich um ein DevSecOps-Team. Hier wird die Sicherheit bereits in der Entwicklung integriert. Microgateways können als eine Art kleine WAAP direkt den jeweiligen Container absichern und schon während der Entwicklung und des Testens eingesetzt werden. Die anwendungsspezifischen Sicherheitsregeln werden dabei vom Entwickler definiert.



DevSecOps: Ein wichtiger Aspekt von Agile Security ist Security by Design: Entscheidend ist, Security bereits beim Design zu berücksichtigen, kontinuierlich weiterzuentwickeln und damit ein Shift-Left der Security zu vollziehen.

Warum die Identität zunehmend in den Mittelpunkt rückt

Durch die Herausforderungen von diesen stark verteilten Systemen mit Multicloud-Ansätzen in heterogenen Architekturen wurde auch Zero Trust zur neuen Pflicht: Damit rückt die Identität stärker in den Mittelpunkt der Application- und API-Security. Denn wenn es um Sicherheitsentscheidungen geht, steht fast immer die Identität im Zentrum. Der Satz „Identität ist der neue Perimeter" wurde zum neuen Security-Paradigma.

Identität schafft Vertrauen, auch in der digitalen Welt. Viele Security-Entscheidungen setzen voraus, dass der Benutzer vertrauenswürdig ist und seine Identität mittels Authentifizierung bestätigt ist. Um beispielsweise zu entscheiden, welche Berechtigungen ein Benutzer erhält, muss zuerst seine Identität geklärt werden. Langwierige und komplexe Authentifizierungsprozesse sind dabei jedoch kontraproduktiv. Die Authentifizierung muss vielmehr benutzerfreundlich in etablierte Prozesse integriert werden. Wie die Praxis zeigt, werden Nutzer ansonsten sehr kreativ, zu hohe Sicherheitsanforderungen zu umschiffen. Zur Lösung dieser Spannung – Sicherheit versus Benutzerfreundlichkeit – haben sich risikobasierte Authentifizierungsverfahren bewährt.

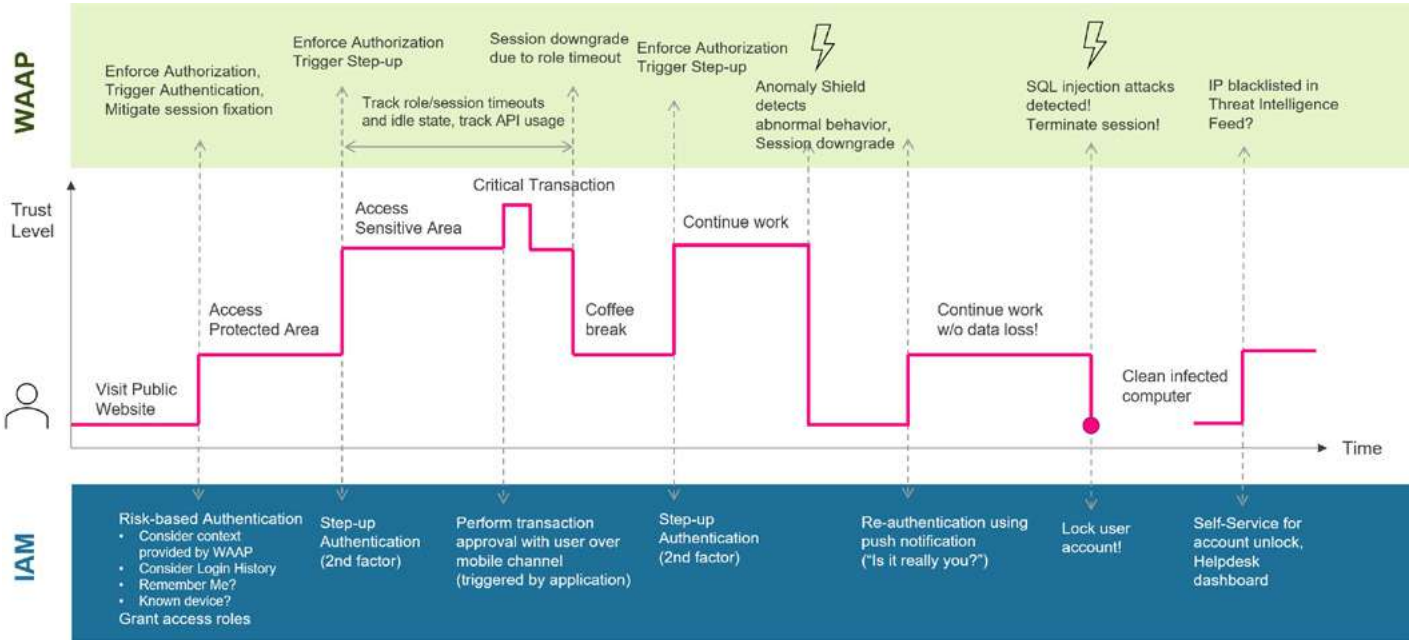
Risikobasierte Authentifizierung

Vertrauen ist nicht binär: Zwischen blindem Vertrauen und totalem Misstrauen gibt es beliebig viele Zwischenstufen. Welches Vertrauensniveau für einen digitalen Zugriff effektiv notwendig ist, hängt von der Risiko-Empfindlichkeit ab. Der Zugriff auf besonders sensible Daten setzt ein höheres Vertrauen voraus als der Download eines öffentlichen Dokuments von der Webseite. Bei der risikobasierten Authentifizierung (RBA) wird das Vertrauensniveau in die Entscheidung über die Häufigkeit und Stärke des Log-ins mit einbezogen.

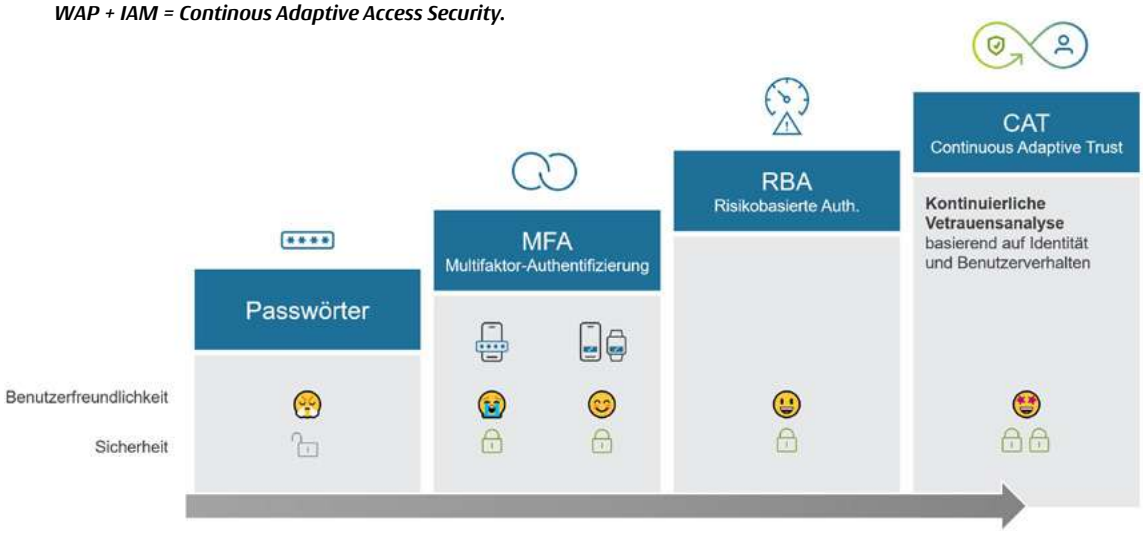
Statt also bei jedem Log-in einen zweiten oder gar dritten Faktor vom Benutzer einzufordern, wird der Kontext eines Zugriffs analysiert und mit vergangenen Sitzungen desselben Nutzers verglichen. Dabei wird berücksichtigt, in welchem Netz sich ein Benutzer befindet, von wo er sich einloggt oder welchen Browser er nutzt. Wenn sich zum Beispiel ein Benutzer von seinem gewohnten Arbeitsplatz im Intranet oder aus seinem Homeoffice anmelden möchte, kann auf den zweiten Faktor verzichtet werden. Mittels der Remember-Me-Funktion wird zudem die Benutzeridentität im Browser hinterlegt und bei künftigen Anmeldungen wiederverwendet.

Continuous Adaptive Trust

Vertrauen ist allerdings nicht konstant über die Zeit. Auch ein Vertrauensverlust zwischen zwei Menschen kommt oft schleichend. Das Vertrauen in eine Person kann sich ändern, wenn sich diese unerwartet oder verdächtig verhält. Auch in der digitalen Welt sollte das Vertrauen nicht nur beim Log-in beurteilt werden. Stattdessen muss das Verhalten eines Benutzers analysiert und das Vertrauen bei Bedarf angepasst werden. So wird bei längerer Inaktivität oder unüblichem



WAP + IAM = Continous Adaptive Access Security.



Continuous Adaptive Trust (CAT) analysiert das Vertrauensniveau kontinuierlich und passt es bei Bedarf an. Weil die Sicherheitsmechanismen tendenziell im Hintergrund bleiben, wird der Benutzerkomfort nicht merklich beeinträchtigt.

Verhalten das Vertrauensniveau reduziert. Falls es unter die Schwelle fällt, die für die aktuelle Anwendung festgelegt wurde, muss das Vertrauen wieder erhöht werden. Dazu braucht es eine vertrauensbildende Aktion wie einen erneuten Log-in mit zweitem Faktor oder das Lösen eines Captchas. Ein solcher „Vertrauensbeweis" kann auch verlangt werden, wenn eine kritische Funktion aufgerufen wird. Ein Beispiel dafür ist die Transaktionsbestätigung bei der Zahlung an einen neuen Empfänger.

Continuous Adaptive Trust (CAT) analysiert das Vertrauensniveau kontinuierlich und passt es bei Bedarf an. Weil die Sicherheitsmechanismen tendenziell im Hintergrund bleiben, wird der Benutzerkomfort nicht merklich beeinträchtigt. Dadurch entsteht eine Win-win-Situation: Wenn sich ein Kunde sicher fühlt, aber nicht durch mühsame Sicherheitsmaßnahmen belästigt, dann schafft das ebenfalls Vertrauen — dieses Mal von der anderen Seite. Mit Continuous Adaptive Trust kann die Identität kontinuierlich und zeitabhängig auf das gerade erforderlichen Risikoniveau geprüft werden.

Resumée

Die Welt der Applikationssicherheit wird immer komplexer. Unternehmen müssen für einen umfassenden Schutz ihrer Apps eine Vielzahl unterschiedlicher Hersteller für WAF, API Security (WAAP), Security in Container-Umgebungen, Threat Intelligence, Access Management und starke Authentifizierung konzertieren. Dies ist mühsam, teuer und fehleranfällig. Die gewonnene Agilität von DevOps-Prozessen geht damit schnell verloren oder die Security bleibt auf der Strecke. Lösungen, welche die einzelnen Domänen der Applikationssicherheit miteinander vereinen und verbinden können, bieten hier große Vorteile und machen Ansätze wie Continuous Adaptive Trust erst möglich. Die Komplexität wird vereinfacht und ein vollständiger Ansatz der Security wird ermöglicht. ■

Quellen:

[1] IDG Studie Application- und API-Security im Containerumfeld 2022 https://www.airlock.com/application-und-api-security-im-container-umfeld-2022

Gernot Bekk-Huber,
Senior Product Marketing Manager
bei Ergon

HZ212318 · ISSN 1868-5757 · www.datakontext.com Oktober/November 5/2022

IT-SICHERHEIT SPECIAL

Technologietrends: Reifeprüfung für die Sicherheit

Zaleman - stockadobe.com

OT- und IoT-Cyber Security:
Immer bedeutsamer für die Produktionsbranche

Ganzheitliche Endpoint Protection Platformen (EPP):
Ideal als Managed Services

Hochspezialisierte Cyber-Security-Dienstleistungen:
Incident Response, Aufbau von Frühwarnsystemen sowie Sicherheitsoptimierung durch Angriffssimulationen

DATAKONTEXT

Welche Technologien und Trends die IT-Security aktuell bestimmen

Reifeprüfung für die Sicherheit

Detection- und Response-Technologien, das heißt Technologien zur Erkennung, Bewertung und Reaktion auf Vorfälle, ganzheitliche Endpoint Protection Platformen (EPP) in Form von Managed Services, sowie hochspezialisierte Cybersecurity-Dienstleistungen prägen die IT-Sicherheitslandschaft im Jahr 2022. OT- und IoT-Cybersecurity werden als notwendiger Bestandteil der Wertschöpfungskette von Produktionsbetrieben und aufgrund von gesetzlichen Vorschriften immer bedeutsamer für die Produktionsbranche. Befeuert vom eklatanten Mangel an Cybersecurity-Spezialisten haben auch Schulungsplattformen zur Ausbildung von Cybersecurity-Spezialisten Hochkonjunktur.

Extended Detection und Response (XDR) und Managed Detection und Response (MDR) werden von sehr vielen Herstellern in den unterschiedlichsten Ausprägungen angeboten. Wegen der Vielzahl der Anbieter sprechen Experten von einem Käufermarkt. Aus Kundensicht wirkt sich diese Situation positiv auf die Marktpreise aus.

Detection- und Response-Technologien

XDR-Technologien lösen technologische Silos in Unternehmensstrukturen auf, da sie drei Grundtechnologien miteinander verbinden und auf diese Weise Synergien in der Entdeckung und Bewertung von Vorfällen schaffen:

- **Security Information and Event Management (SIEM)**
  Echtzeitanalyse von Informationen aus NDR- und EDR-Systemen mit Aufbereitung von Daten, damit Gegenmaßnahmen zur Risikoabwendung eingeleitet werden können.
- **Network Detection und Response (NDR)**
  NDR analysiert Datenströme im Netzwerk und schlägt bei ungewöhnlichem Datenverkehr Alarm, zum Beispiel Botnetz-Verkehr (Command und Control), Abfluss von sensiblen Unternehmensdaten (Data Exfiltration), Seitwärtsbewegungen von Angreifern (Lateral Movement) etc.

- **Endpoint Detection und Response (EDR)**
  Endgeräteforensik in Verbindung mit signaturbasierenden Endgerätesicherheitslösungen (klassischer AV-Schutz) mit der Möglichkeit, verseuchte Endgeräte in die Quarantäne zu schicken.

Unternehmen, die sich auf ihre Kernkompetenzen konzentrieren möchten und nicht auf technische Cybersecurity-Experten zugreifen können, bedienen sich Managed Detection und Response (MDR) Services. MDR-Services vereinigen menschliche Cybersecurity-Expertise mit Cybersecurity-Technologien. Es geht dabei um Vorfall-Reaktions-Dienstleitungen (Incident Response, kurz IR) mit oder für bestimmte XDR-Technologien.

In der Praxis gibt es MDR in zwei Ausprägungen:

1. MDR mit Incident Response für den eigenen XDR-Stack

2. MDR mit Incident Response einschließlich eines externen XDR-Stacks des Incident-Response-Anbieters. Sollte es keinen eigenen XDR-Stack, geben, kommt ausschließlich diese Variante in Frage.

Da mittelständische Unternehmen in der Regel keinen nennenswerten XDR-Stack haben, überwiegen hier MDR-Projekte mit Incident Response einschließlich eines externen XDR-Stacks.

Managed Endpoint Protection Services

Vor allem kleinere und mittlere Unternehmen greifen vermehrt auf Managed Endpoint Protection Services, um die IT-Gesamtkosten zu senken und die IT-Ressourcen zu optimieren, ohne dabei auf einen hohen IT-Grundschutz verzichten zu müssen.

Konsolidierung von verschiedenen IT-Sicherheitstechnologien

Aus den verschiedensten Gründen gibt es immer noch Unternehmen, die IT-Sicherheitstechnologien verschiedener Anbieter auf einem Endgerät nutzen. Bei der Analyse der eingesetzten IT-Sicherheitslösungen auf einem Endgerät lassen sich in der Regel drei der folgenden Lösungen finden:

1. Anwendungskontrolle
2. Endgeräteforensik (Endpoint Detection und Response)
3. Patchmanagement
4. Schnittstellenkontrolle
5. Schutz vor Malware (signaturbasiert)
6. Schwachstellenmanagement
7. Verhinderung von Datenklau (Data Leakage/ Loss Prevention)
8. Verschlüsselung von Daten

Durch die Konsolidierung aller Funktionalitäten in eine ganzheitliche und zentral verwaltbare Plattform lassen sich Kosten sparen, das Trouble Shooting der Supportabteilung optimieren und das Sicherheitsniveau verbessern.

EXKURS: THREAT INTELLIGENCE

Detection- und Response-Technologien können die Erkennungsrate von Cyberbedrohungen durch den Einsatz von Threat Intelligence (TI) signifikant erhöhen. Unter Threat Intelligence versteht man Informationen über Cybersecurity-Bedrohungen und Gefährdungspotenziale.

- Eine Cybersecurity-Bedrohung ist zum Beispiel eine Website mit einem Spionagetrojaner oder eine Darknet-Information über einen geplanten Cyberangriff.

- Informationen über Schwachstellen oder Informationen über gefährdete Branchen für einen bestimmten Angriff sind Beispiele für Cyber-Security-Gefährdungspotenziale.

Unternehmen vertrauen heute gern auf die Kombination von kostenfreier und kommerzieller Threat Intelligence. Bei der Nutzung von kommerzieller Threat Intelligence hat sich die Notwendigkeit herauskristallisiert, verschiedene Anbieter aus verschiedenen geografischen Regionen miteinander zusammenzuführen. Ein Threat-Intelligence-Mix aus unterschiedlichen Anbietern aus dem Westen (USA), Europa und Asien (Singapur) ist das Fundament für Risikomanagement bei dieser Technologie, denn nicht jeder Anbieter erkennt jede Bedrohung.

Mit Digital Risk Protection (DRP) hat sich eine neue Lösungskategorie im Threat-Intelligence-Bereich etabliert. DRP beschäftigt sich mit Bedrohungen, die aus der Interaktion von Web und sozialen Medien entstehen können:

- Identifizierung und Validierung von relevanten und realen Bedrohungsinformationen im Darknet und in sozialen Medien

- Schutz vor betrügerischen Inhalten und Falschinformationen

- Schutz vor modernen Bedrohungen gegen eine bestimmte Marke (VIPs, Firmenbrands)

Bei Identifizierung von relevanten Bedrohungsinformationen, betrügerischen Inhalten, Falschinformationen etc. können solche Inhalte mittels Take-Down-Services zum Schutz der Marke aus dem entsprechenden Forum entfernt werden.

Threat-Intelligence-Plattformen (TIP) sorgen für eine effektive Nutzung durch Visualisierung, Priorisierung und Orchestrierung der verschiedenen Threat-Intelligence-Anbieter. Dem Einsatz von Threat-Intelligence-Technologien werden sehr große Marktpotenziale zugesprochen. Sie sind eine wichtige Grundlage für den Aufbau von Cybersecurity-Frühwarnsystemen.

Was am Endpoint sonst noch wichtig ist

Garantie von hohen Endgeräteverfügarbeiten

Mindestens einmal im Jahr erleben Nutzer einen Blackout eines Laptops, einer Workstation oder, was eher selten ist, den Ausfall eines Servers. Ursachen dieser Blackouts sind zum Beispiel fehlerhafte Software-Updates, beim Surfen eingefangene Schadsoftware oder auch ein gezielter Angriff. Die Widerherstellung eines ausgefallenen Systems dauert in der Regel zwischen zwei und sechs Stunden. Für solche Ereignisse macht der Einsatz einer Disaster-Recovery-Lösung Sinn, da so das ausgefallende System in kürzester Zeit wieder lauffähig gemacht werden kann. Das sorgt für hohe Endgeräteverfügbarkeiten im Unternehmen.

Sicherung von sensible Unternehmensdaten

Unabsichtliche Löschung von Unternehmensinformationen, Systemabstürze oder gezielte Ransomware führen dazu, dass essentielle Daten nicht mehr verfügbar und somit nicht mehr für einen operativen Betrieb nutzbar sind. Durch den Einsatz einer modernen, Cloud-basierenden und DS-GVO-konformen Backup-Lösung gehören die genannten Herausforderungen der Vergangenheit an. Unternehmen verhindern im Falle eines Ransomware-Angriffs die Zahlung von Erpressungsgeldern für die Entschlüsselung der Daten – vorausgesetzt, die Backup-Strategie verhindert ein Verschlüsseln auch der Backups.

Managed Endpoint Protection Services helfen Unternehmen dabei, verschiedene IT-Security-Technologien in ein zentrales System zu konsolidieren, hohe Verfügarbeiten der Endgeräte zu garantieren und sensible Unternehmensdaten zu sichern.

Hochspezialisierte Cybersecurity-Services

Im Folgenden wird der Fokus auf Incident Response, Aufbau von Frühwarnsystemen sowie Sicherheitsoptimierung durch Angriffssimulationen gelegt. Auf andere Bereiche wird nicht eingegangen.

Der hohe Bedarf an hochspezialisierten Cybersecurity-Services spiegelt sich in der regelmäßig ansteigenden Anzahl von Anbietern wieder, die auf der Incident-Responder-Liste des BSI stehen. Lag im Janaur 2021 die Anzahl der qualifizierten APT-Response Dienstleiter bei 11, sind es im Juni 2022 bereits 32 Anbieter.

Dieser Anstieg von 190 Prozent in nur 18 Monaten lässt sich dadurch erklären, dass die Qualität und Komplexität der Cybersecurity-Angriffe während dieser Zeit immens zugenommen haben. Hinzu kommt, dass Corona die daraus resultierende Homeoffice-Pflicht in technischen Abteilungen und fehlende Cybersecurity-Kompetenzen den Anstieg zusätzlich gefördert haben.

Gemäß Best Practice sollen qualifizierte Incident-Response-Anbieter folgende Fähigkeiten und Qualifikationen vorweisen können:

- Durchführung eines Vorfalls-Reaktions-Grundlagenworkshops, in dem Nutzer lernen, effektiv auf die Incident-Response-Anforderungen zu reagieren, um so einen zeitlichen Vorteil bei der Inanspruchnahme der Incident-Response-Services zu haben
- Analyse, Ziel und Rekonstruktion eines erfolgten Cybersecurity-Angriffs
- Einleitung von Gegenmaßnahmen mit dem Ziel, die Hackergruppe zur Schadenbegrenzung dingfest zu machen und zu isolieren
- Überwachung eines wiederholten Cybersecurity-Angriffs durch dieselbe Hackergruppe 90 Tage nach dem ersten Angriff
- Wiederherstellung des Gerätezustands vor dem Cybersecurity-Angriff
- Aufbau eines Frühwarnsystems zur Erkennung künftiger Cybersecurity-Angriffsversuche
- Regelmäßige Angriffssimulation und Risk Assessments

Die wichtigsten spezialisierten Cybersecurity-Services

Frühwarnsystem zur Erkennung von Cybersecurity-Angriffen

Ein Frühwarnsystem soll Unternehmen in die Lage versetzen, einen bevorstehenden Cybersecurity-Angriff schnell zu erkennen und notwendige Gegenmaßnahmen zu ergreifen. Für den Aufbau eines Frühwarnsystems zur Erkennung von Cybersecurity-Angriffen werden folgende Bausteine benötigt:

- Cybersecurity-Analysten-Team für 24x7x365-Einsatz
- Threat-Intelligence-Technologien: höchste Effektivität bei Abbildung von Bedrohungsinformationen aus dem Westen, Europa und Asien

EXKURS: IDENTITY RISK ASSESSMENT

Durch einen Hack wurde in diesem Jahr aufgezeigt, dass Identity- und-Access-Management-(IAM-)Technologien kompromittierbar sind. Zur Aufdeckung dieser Risiken haben sich sogenannte Identity Risk Assessments sehr bewährt. Ein Identity Risk Assessment dauert zwei bis drei Stunden läuft folgendermaßen ab:

- Analyse, ob die Kombination eines Benutzernamens samt Passwort auf einem Endgerät auffindbar ist.
- Bei Identifizierung solch einer Kombination sollten diese Informationen augenblicklich auf dem Endgerät gelöscht werden.
- Angreifer können mit solchen Informationen beziehungsweise Benutzername-Passwort-Kombinationen eine „Firma lahmlegen", diese für Seitwärtsbewegungen missbrauchen oder im Darknet für viel Geld veräußern.

- Threat-Intelligence-Plattform: Orchestrierung der verschiedenen Threat-Intelligence-Technologien
- Branchenbezogene Cybersecurity-Bedrohungsanalysen, wenn die Angreifer bestimmte Branchen im Visier haben
- Individuelle Cybersecurity-Bedrohungsanalysen (maßgeschneiderte Threat Intelligence Reports)
- Einbindung aller Informationen über Bedrohungen in das zentrale SIEM
- Regelmäßige Übungen mit definierten Prozessen für den Ernstfall unter Einbindung von Management, Compliance-Beauftragten, Abteilungsleitern, Netzwerk- und Cybersecurity-Administratoren, SOC-Analysten etc.

Regelmäßige Angriffssimulation und Risk Assessments

Es ist eine Tatsache, dass Unternehmen hohe Investments in Cybersecurity-Technologien tätigen, aber aus Zeit- und Ressourcenmangel die Konfiguration der Technologien bei den Standardeinstellungen belassen. Aber auch bei regelmäßiger Anpassung der bestehenden Konfiguration gibt es keine Garantien, dass diese einem gezielten Cybersecurity-Angriff standhält. Aufgrund der Dynamik der Cybersecurity-Angriffe kann die heutige Konfiguration durch neu entdeckte Schwachstellen morgen schon veraltet sein.

Durch eine Angriffssimulation mit bekannter Malware oder neuen gezielten Angriffsmustern können aktuell vorhandene Schwachstellen sowie eine fehlerhafte oder unzureichende Konfiguration der eingesetzten Technologie frühzeitig erkannt und somit deren Effizienz in der Erkennung messbar optimiert werden (Cybersecurity-Improvement).

Ziele des durchgeführten Cybersecurity-Stresstests sind Netzwerk-, E-Mail- und Endgeräte-Sicherheitstechnologien. Des Weiteren liefern solche Stresstests auch Entscheidungshilfen dazu, ob eine wenig effektive Cybersecurity-Technologie besser gegen eine effektivere ausgetauscht werden sollte. Angriffssimulationen werden oft auch „Breach und Attack Simulation (BAS)" sowie „Security Validation" genannt.

OT- und IoT-Cybersecurity

Der Begriff „Operational Technology" (OT) bezieht sich auf die Methoden und Werkzeuge, die zum Schutz von Personal, Eigentum und Daten einer Organisation eingesetzt werden, die sich mit der Überwachung und/oder Steuerung von Maschinen, Anlagen und anderen mechanischen oder elektronischen Systemen beschäftigt. Digitale Risiken in produzieren-

den Unternehmen und an der Automatisierung teilhabenden Firmen zu verhindern, enden nicht damit, konventionelle IT-Systeme vor Cyberbedrohungen zu schützen.

Bild: Blue Planet Studio - stock.adobe.com

In der Vergangenheit galten industrielle Steuerungssysteme nicht als hohes Risiko für Cyberangriffe, da sie nicht mit Unternehmenssystemen oder dem Internet verbunden waren. Heute sind OT- und IoT-Systeme durch die Verwendung gemeinsamer Technologieplattformen, die gemeinsame Nutzung von IT- und IoT-Daten sowie cloudbasierte Anwendungen und Analysen zu einem primären Ziel für Bedrohungsakteure geworden.

Von CIOs und CISOs wird nun erwartet, dass sie die gesamte IT/OT-Landschaft schützen, einschließlich aller physischen Anlagen und industriellen Prozesse. Um dies zu erreichen, muss die OT- und IoT-Sicherheit Teil einer umfassenden digitalen Sicherheitsstrategie sein, die von einem kooperativen IT/OT-Team verwaltet wird. Auf Basis von Risikoabwägungen sollte eine Cybersecurity-Strategie für industrielle Steuerungssysteme (ICS), operative Technologien (OT), konvergierte IT-, OT- und IoT-Netze implementiert werden, die folgende Aspekte zwingend berücksichtigt:

- Einfache Identifizierung von OT- und IoT-Geräten im Unternehmensnetzwerk, um Risikoanalysen zu verbessern
- Schnelle Schwachstellenbewertung und Risikoüberwachung, damit Sicherheitsbedrohungen effektiver erkannt werden
- Umfassende Bedrohungsanalysen durch verhaltensbasierte Anomalie-Erkennung, signaturbasierte Bedrohungs-Erkennung und Asset Intelligence
- Modernes Dashboard- und Berichtswesen für die zügige Einleitung von Gegenmaßnahmen, um die Effizienz des OT-/IoT-Risikomanagement zu verbessern
- Integration in Protection (Firewall), Detection (SIEM, SOAR) und Response-Strategien
- Umfassende Technologiepartnerschaften zu Anbietern aus Cloud Service, OT-/IoT-Hersteller, Netzwerktechnologien etc.

Ausbildung von Cybersecurity-Spezialisten

Der gezielte Know-how-Transfer von Cybersecurity-Spezialwissen sowie die Ausbildung von Cybersecurity-Experten ist schon immer eine große Herausforderung für Unternehmen jeglicher Größe gewesen. Daher ist es wenig verwunderlich, dass sich der hohe Bedarf an Cybersecurity-Experten in über vier Millionen unbesetzten Cybersecurity-Stellen widerspiegelt.[1]

Damit der Nutzen der in den Unternehmen eingesetzten Cybersecurity-Technologien hochgehalten und gesteigert wird, ist es unabdingbar, dass es im Unternehmen Experten mit Cybersecurity-Fachwissen gibt. Der gezielte Know-how-Transfer von Cybersecurity-Spezialwissen sowie die Ausbildung von Cybersecurity-Experten sollte aus Ressourcengründen (Zeit, Kosten, Personal) unabhängig von Ort und Zeit sein. Dafür eignen sich am besten moderne und intuitive Cybersecurity-Trainingsplattformen, auf welchen sich theoretische Inhalte zu Cybersecurity-Themen vermitteln und praktische Übungen durchführen lassen, um das Gelernte anzuwenden.

Folgende Themen sollte eine Cybersecurity-Trainingsplattform für die individuelle Ausbildung mindestens abbilden: Cloud Security, Cybersecurity Essentials, Microsoft Security, SOC Analyst-Know-how, Threat Hunter Know-how sowie Web Application Security. Cybersecurity-Übungen mit Angriffs-Simulationen verbessern im Team eine zügige und kompetente Reaktion auf Cybervorfälle. ■

Quellen:

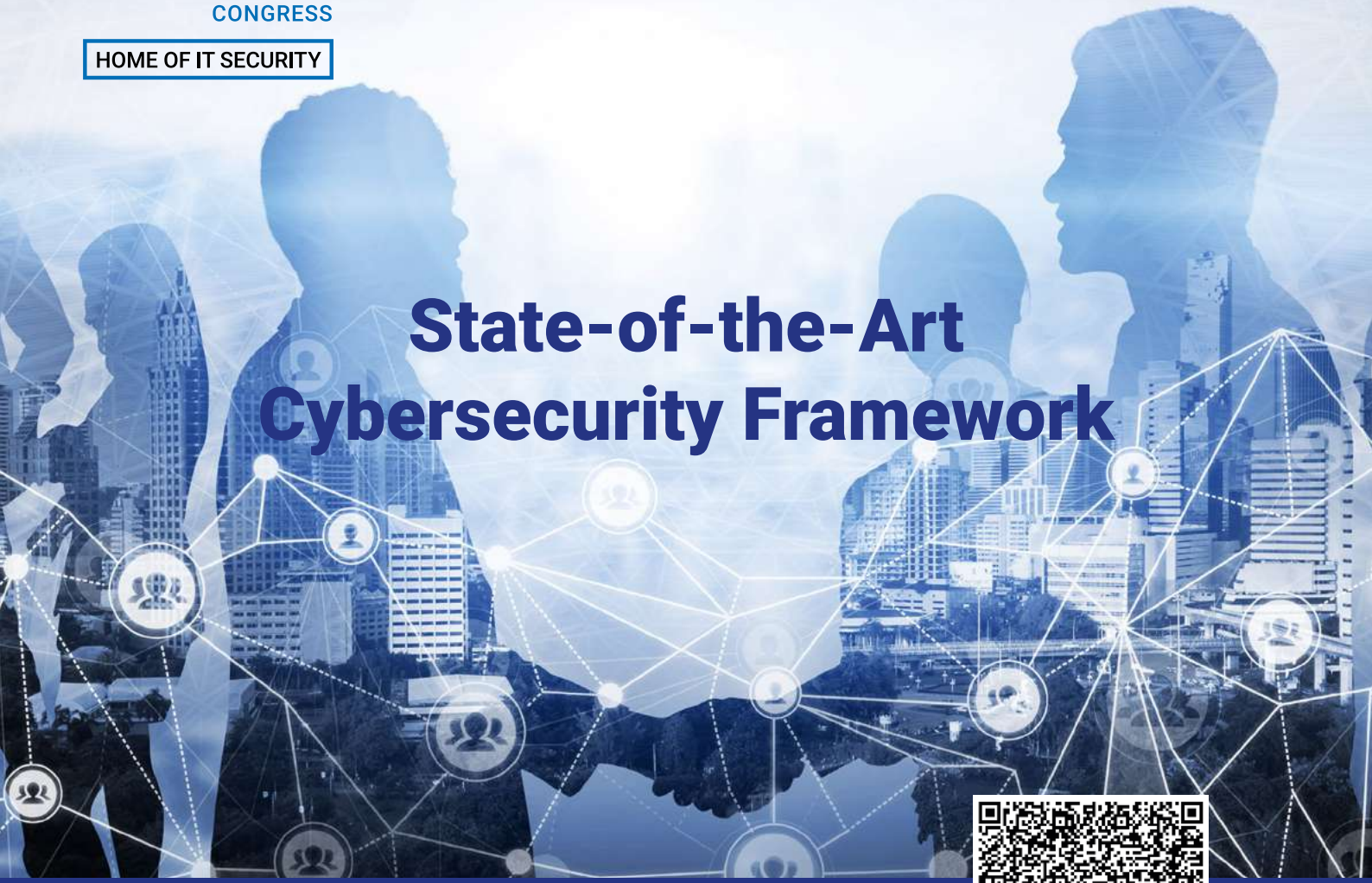
[1] International Information System Security Certification Consortium (ISC)

Tomé Spasov,
Geschäftsführender Gesellschafter
bei Ectacom

itsa EXPO CONGRESS

HOME OF IT SECURITY

ectacom



State-of-the-Art Cybersecurity Framework

Gratis-Ticket mit dem Code: **479752itsa22**

Wir freuen uns auf Ihren Besuch!

Acronis | Cobalt | COFENSE | GROUP-IB

illusive | MANDIANT | NOZOMI NETWORKS | QuoLab

RANGEFORCE | sumo logic | WINMAGIC | ZEROFOX

Halle 7 - Standnummer 7-122

Starkes Interesse an EDR, Zero Trust und Made in EU

it-sa 2022: Drei aktuelle Trends bestimmen die IT-Security

Auf der Sicherheitsmesse it-sa stehen für gewöhnlich die technischen Neuentwicklungen im Kampf gegen Cyberkriminalität im Vordergrund. Doch in diesem Jahr bestimmen andere Faktoren den Takt. Die Auswahl der passenden Security-Philosophie steht ebenso im Vordergrund wie die Herkunft der Hersteller. Vor dem Hintergrund der aktuellen, weltpolitischen Ereignisse ist IT-Security mehr denn je Vertrauenssache.

Erfolgreiche Cyberangriffe auf Unternehmen erfolgen in den seltensten Fällen „Knall auf Fall", sondern sind das Resultat längerer und vor allem aufwendiger Vorbereitungen aufseiten der Angreifer. Je besser das anzugreifende Netzwerk jedoch abgesichert ist, desto intensiver müssen Cyberkriminelle nach Schwachstellen suchen. Das bedeutet für sie, vorab geeignete Wege finden zu müssen, um in der Zielorganisation eine Basis für einen Angriff zu schaffen. Insbesondere, wenn Advanced Persistent Threats und Zero-Day-Exploits ins Spiel kommen, stoßen jedoch klassische Sicherheitsprodukte an ihre Grenzen. Diese Gefahren sind selten direkt erkennbar, wie beispielsweise Malware, verraten sich aber im Laufe der Zeit über ihr Verhalten und ihre Arbeitsweise im Netzwerk.

TREND 1: Endpoint Detection and Response rückt ins Rampenlicht

Abhilfe schaffen Endpoint-Detection-and-Response-Lösungen, die das Schutzniveau deutlich erhöhen und IT-Security-Verantwortlichen eine umfassende Innenansicht ihres Netzwerks ermöglichen. Aber was bedeutet Detection und Response eigentlich in der Praxis? Zum einen soll damit der Endpoint geschützt werden („Detection"), auf dem die meisten Hacker-Aktivitäten stattfinden. Dort liegt ein Großteil der schutzwürdigen Daten vor, Passwörter, Bankdaten und viele andere sensible Informationen werden am Gerät eingegeben. Zum anderen beschreibt „Response", dass auf Anomalien sofort reagiert werden kann. Je nachdem kann das eine manu-

elle Reaktion eines IT-Sicherheitsexperten oder eine automatische, zuvor definierte Verhaltensweise sein.

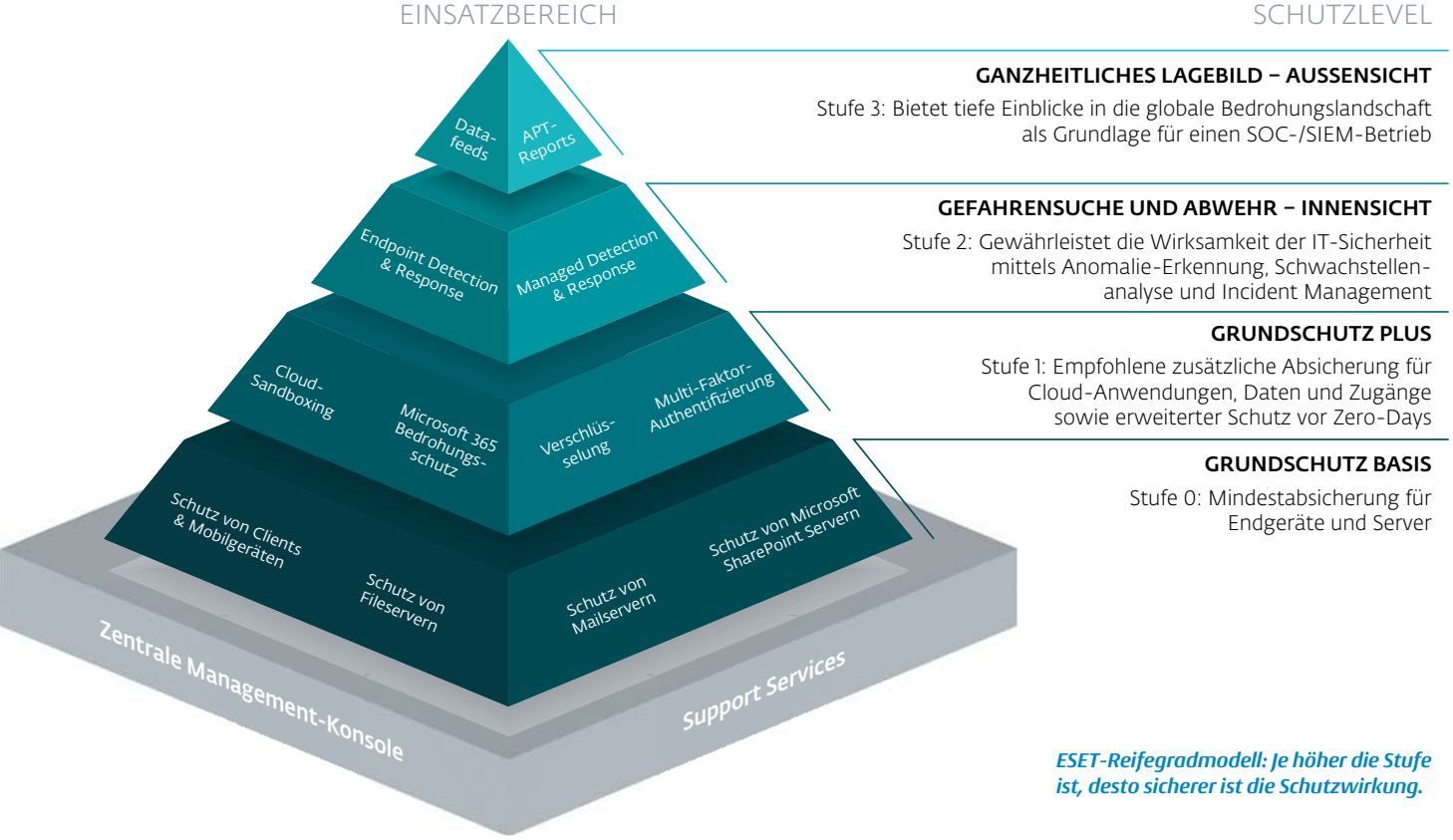
Und genau auf diese Veränderungen an Dateien, Protokollen und ausgeführten Diensten springen die EDR-Lösungen beinahe in Echtzeit an – und starten sofort die Überprüfung. Zudem bieten sie eine weitere wichtige Einsatzmöglichkeit: Anhand von EDR können nach einer Cyberattacke forensische Untersuchungen eingeleitet werden. Ähnlich wie etwa bei einem Mordfall werden möglichst viele Informationen gesammelt und „Alibis" – in diesen Fällen die ordnungsgemäßen Arbeitsweisen – überprüft. Administratoren erkennen so zuverlässig, wie der Angriff ablief, welche Schwachstellen konkret ausgenutzt und welche Veränderungen im Netzwerk vorgenommen wurden. Dazu kann der Verantwortliche auf Informationen von Reputationssystemen zurückgreifen und/oder anhand des MITRE ATT&CK Frameworks die Attacke nachvollziehen.

TREND 2: Von EDR zu Zero Trust ist es nur ein kurzer Schritt

Hinter Zero Trust steht die Idee einer konzeptionellen Leitlinie für alle IT-Security-Maßnahmen, die auf Vorsicht und Skepsis beruht. Es handelt sich also nicht um eine Blaupause für ein IT-Sicherheitssystem oder eine technisch ausgefeilte Security-Lösung. Laut Forrester beruht die Prämisse von Zero Trust darauf, keiner Entität zu vertrauen, weder intern noch extern. Mit anderen Worten: „Vertraue nie, überprüfe immer". Experten beschreiben Zero Trust als ein perimeterloses Modell. Dieses muss ständig aktualisiert werden, um Daten, Software und andere Anwendungen unabhängig von Nutzern, Standort oder Geräteart zu schützen. Ein wichtiger Bestandteil von Zero Trust ist dabei die kritische Sicht nach innen. Also, wer macht was und darf er oder sie das; womit dann wieder das Thema EDR ins Spiel kommt.

ArtemisDiana - stock.adobe.com

ESET hat ein Reifegradmodell entwickelt, das die unterschiedlichen Stufen und Maßnahmen von Zero Trust anschaulich darstellt. Der Ansatz besteht aus einer dreistufigen Pyramide. Je höher die Stufe ist, desto sicherer ist die Schutzwirkung – also „reifer". Das Modell startet mit der Basisstufe „Grundschutz Plus", die dem Prinzip des „Multi Secured Endpoint" (MSE) folgt. Im Zusammenspiel von Malwareschutz mit einer Festplattenverschlüsselungs- und Multi-Faktor-Authentifizierungslösung sowie Cloud Sandboxing, verwandeln Administ-



ESET-Reifegradmodell: Je höher die Stufe ist, desto sicherer ist die Schutzwirkung.

ratoren PCs und Laptops in gehärtete Endpoints. Diese Vorgehensweise eignet sich unabhängig vom individuellen Schutzbedarf für jede Organisation und sollte die Mindestanforderung jeder IT-Abteilung abbilden. Damit legen Netzwerkbetreiber einen wichtigen ersten Grundstein von Zero Trust Security. MSE sichert Endpoints weit besser ab als andere Systematiken zuvor. Und: Es spielt nun keine Rolle mehr, ob sich Gerät oder Anwender im IT-sicheren Bürogebäude befinden.

Daran schließen sich zwei Zero-Trust-Stufen mit weiter steigenden Security-Maßnahmen und -Diensten an. In der Ausbaustufe zwei spüren Endpoint-Detection-and-Response-Lösungen verdächtiges Verhalten und Sicherheitslücken im Netzwerk automatisch auf.

In der dritten Stufe des Modells kommen „Threat Intelligence Services" (TI) hinzu. Während EDR im Inneren nach Sicherheitsproblemen sucht, blickt (TI) nach außen. Ähnlich wie klassische Geheimdienste sammeln die Systeme Daten und Informationen aus unterschiedlichsten externen Quellen. Dies können beispielsweise Informationen zu Sicherheitsbedrohungen, wie Cyberangriffe, zu aktuell erkannten Schwachstellen in Software, wie Zero-Day-Threats, oder zu Sicherheitslücken von Hardwaresystemen sein.

TREND 3: Kunden bevorzugen „Made in EU"

Aufgrund der Ereignisse rund um die Ukraine hat definitiv ein Umdenken eingesetzt – und ein regelrechter „Run" auf Security-Unternehmen aus Europa begonnen. Natürlich sind die Qualität der IT-Sicherheitslösungen sowie die begleitenden Services immer noch die wichtigsten Faktoren bei der Auswahl des Herstellers. Aber: Immer mehr Unternehmen oder Verwaltungen hinterfragen die Herkunft der Sicherheitslösungen und schauen verstärkt auf das Label „Made in EU". Ihnen stellt sich zwangsläufig die Frage: Ist der Hersteller des Malware-Schutzes, den meine Organisation einsetzt, auch wirklich vollumfänglich vertrauenswürdig und vor allem für meine Sicherheit verlässlich? Wer garantiert mir, dass jeder Schadcode gefunden, Updates vollständig bereitgestellt und keine Hintertüren durch die Software geöffnet werden? Oder gar Regierungen im Hintergrund Druck ausüben und Backdoors einbauen lassen?

Die Herkunftsbezeichnung „Made in EU" steht für eine Top-Qualität und die Einhaltung strikter Vorgaben. Insbesondere im Bereich der IT-Security sind Unternehmen aus der Europäischen Union weltweit führend und bestechen zudem durch eines: Vertrauen der Kunden in die Technologie und den Schutz der Kundendaten. Mit diesem Vertrauenssiegel können sich europäische Hersteller von IT-Security-Lösungen von Mitbewerbern aus anderen Weltregionen abheben und zeigen, dass ihre Lösungen den strengen europäischen Datenschutzbestimmungen entsprechen. Das Siegel signalisiert nicht nur Vertrauen, sondern bringt Produkte und Technologien aus der EU in den Fokus von Wirtschaft und Government. So können beispielsweise Behörden bei Ausschreibungen davon ausgehen, dass eine mit dem Siegel „IT-Security made in EU" ausgezeichnete Lösung den in der EU geltenden Standards genügt. Organisationen und Anwender stellen damit sicher, dass sie auf die Leistungsfähigkeit und Zuverlässigkeit der gekennzeichneten Technologien und Lösungen ebenso vertrauen können wie auf deren bedingungslose Gesetzeskonformität. Denn mit diesem Siegel verpflichten sich Hersteller mit Hauptsitz in der EU freiwillig dazu, dass ihre Security-Lösungen vertrauenswürdig sind, strengsten Datenschutzauflagen entsprechen und keinerlei versteckte Backdoors enthalten.

Wenige Anbieter gehen sogar noch einen Schritt weiter und geben eine „No backdoor guarantee". Damit garantieren sie, dass bei der Entwicklung der Sicherheitssoftware keine „Hintertürchen" eingebaut werden, staatlich initiierte Malware ebenso abgewehrt wird wie anderer Schadcode und keine Ausnahmen beziehungsweise Zugeständnisse in puncto IT-Sicherheit auf Druck von Regierungen gemacht werden. ■

www.eset.de

it-sa 2022: Stand 7-530

Thorsten Urbanski,
IT-Sicherheitsexperte,
ESET Deutschland GmbH

HZ212318 · ISSN 1868-5757 · www.datakontext.com Oktober/November **5/2022**

IT-SICHERHEIT SPECIAL

Eugene Kaspersky, CEO und Firmengründer von Kaspersky, im Datenzentrum in Zürich

Managed Detection and Response (MDR)
Gut gewappnet gegen fortschrittliche Angriffe

Kampf gegen Cyberangriffe:
Threat Intelligence ist mehr als nur ein Buzzword

Sichere Digitalisierung:
Cybersicherheit muss auf den Prüfstand!

DATAKONTEXT

Wie Managed Detection and Response (MDR) vor komplexen Bedrohungen schützt

Gut gewappnet gegen fortschrittliche Angriffe

Zeit ist Geld – dieses altbekannte Sprichwort gilt auch im Fall eines Cyberangriffs. So zeigen aktuelle Kaspersky-Studien, dass die Zeit, die benötigt wird, um einen Cybersicherheitsvorfall zu erkennen, einen beträchtlichen Einfluss auf die Folgen eines Angriffs hat. Demnach erleiden mittelständische Unternehmen 17 Prozent geringeren finanziellen Schaden, wenn sie einen Angriff direkt erkennen (im Vergleich zu einer Erkennung nach einer Woche).[1] Im Jahr 2021 belief sich das durchschnittliche IT-Sicherheitsbudget auf jedoch nur 236.000 Euro bei kleinen und mittelständischen Unternehmen.[2]

Allzu oft denkt der Mittelstand leider noch, kein interessantes Ziel für Cyberkriminelle zu sein. Dem ist jedoch nicht so. Cyberkriminelle führen Angriffe durch, wenn es sich für sie lohnt, und dies ist unter anderem bei Ransomware oder Spyware der Fall, bei der Lösegeld zur Wiederherstellung von Daten gefordert wird, beziehungsweise die erbeuteten Informationen gegebenenfalls im Darknet verkauft werden. Solange die Kosten für die Planung und Durchführung eines Angriffs geringer sind als die potenziellen Einnahmen eines Angriffs, lohnt es sich für die Cyberkriminellen. Dabei ist die Größe des anvisierten Unternehmens zweitrangig, sodass auch mittelständische Unternehmen betroffen sind.

Sicherheit trotz begrenzter Unternehmensressourcen

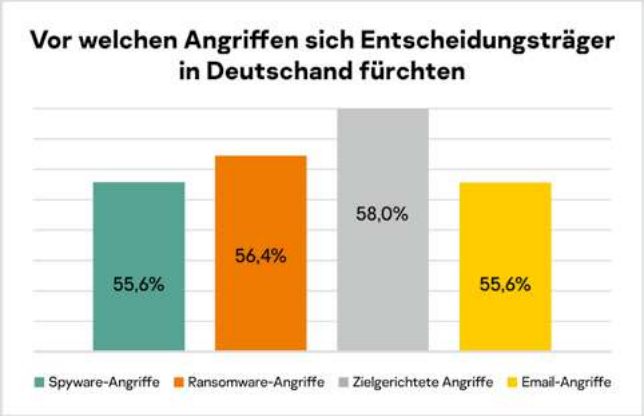
Um komplexe Angriffe abzuwehren, fehlen mittelständischen Unternehmen oftmals die Ressourcen – sowohl finanziell als auch personell. Der vorherrschende Fachkräftemangel trifft kleine und mittelständische Organisationen noch einmal stärker als Großunternehmen, die oft bessere Gehälter anbieten können, und fast die Hälfte aller Unternehmensentscheider kämpft zudem mit der Beschaffung finanzieller Mittel zur Verbesserung ihrer Cybersicherheit. Beides wird jedoch dringend benötigt, da die zunehmend komplexe Infrastruktur in Unternehmen entsprechende Schutzmaßnahmen verlangt. Als mögliche Lösung für dieses Dilemma entscheiden sich Firmen deshalb oft, ihre Cybersicherheitsabteilung an einen Dienstleister auszulagern. Damit handeln sie genau richtig, denn europäische Unternehmen, die auf externe Expertise setzen, sind besser geschützt: Sie werden mit fast zehn Prozent weniger Cybervorfällen konfrontiert.[3]

Threat Intelligence als Basis

Lagern Unternehmen ihre Cybersicherheit aus, sollten sie auf eine automatisierte und verwaltete Lösung in Form von Managed Detection and Response (MDR) setzen. Dabei geht es darum, Technologien, Lösungen und Dienstleistungen mit

Bild: Who is Danny - stock.adobe.com

menschlicher Expertise zu kombinieren, um Sicherheitsvorfälle zu analysieren, zu bewerten und entsprechend darauf zu reagieren. Hier ist es ausschlaggebend, dass die Lösung auf aktueller Threat Intelligence basiert. Denn durch einen steten Abgleich der Informationen können Taktiken, Techniken und Vorgehensweisen der Angreifer frühzeitig erkannt und somit Angriffe abgewehrt werden. Entsprechende Angriffsindikatoren sorgen dafür, dass selbst Bedrohungen abseits von Malware, die legitime Aktivitäten vortäuschen, erkannt werden.



Vor diesen Angriffen fürchten sich Entscheidungsträger in Deutschland.

Eine schnelle Erkennung und eine umfassende Reaktion auf Sicherheitsvorfälle sind heute entscheidend, um die Auswirkungen eines Angriffs möglichst gering zu halten. MDR ermöglicht eine umfassende Transparenz über alle Geräte im Unternehmensnetzwerk hinweg und bietet überlegene Abwehrmaßnahmen, sodass auch Unternehmen ohne die nötige interne Expertise vor komplexen Bedrohungen nachhaltig geschützt sind.

Wie finden Unternehmen den passenden MDR-Anbieter?

1. Starke Technologie:

Bei der Auswahl einer entsprechenden Lösung sollten Unternehmen mehrere Faktoren beachten, welche die eigenen Anforderungen und Bedürfnisse berücksichtigen. Die hinter einer Lösung stehende Technologie sollte umfassend schützen – auch ohne Beteiligung der externen Sicherheitsanalysten oder internen Cybersecurity-Mitarbeiter. Hierfür sind maschinelle Lernalgorithmen nötig, die bei der Alarmverarbeitung unterstützen. Da diese Automatisierung Routineaufgaben übernimmt, können sich die Sicherheitsanalysten mit ernst zu nehmenden Vorfällen viel früher befassen und so die Reaktionszeit auf einen Angriff reduzieren – bevor die Kompromittierung zum Problem wird.

2. Flexible Response-Optionen:

Welche Response-Fähigkeiten sind Teil des Anbieterportfolios? Idealerweise sind diese flexibel abrufbar und können mit zwei Optionen kombiniert werden: Entweder führt ein MDR-Team die Reaktionsmaßnahmen per Fernzugriff durch oder die internen Mitarbeiter können nach Anweisung und unter Verwendung eines bereitgestellten Toolstacks selbstständig reagieren. Letzteres ist oft zu Beginn einer Zusammenarbeit hilfreich, da ein Unternehmen meist sicherstellen möchte, dass die erhaltenen Empfehlungen auch gut funktionieren und die Besonderheiten des eigenen Netzwerks und der Geschäftsprozesse berücksichtigt werden. Außerdem ziehen es einige Unternehmen vor, bei Angriffen auf kritische Assets, beispielsweise Computer von Führungskräften, selbst aktiv zu werden.

3. Klar definierter Service 24/7:

Darüber hinaus sollte darauf geachtet werden, dass der Vertrag in den Service Level Agreements eine klare Reaktionszeit auf Vorfälle festlegt – abhängig von der zugewiesenen Priorität eines erkannten Vorfalls. Generell müssen MDR-Anbieter schnell auf Vorfälle reagieren können, und das rund um die Uhr.

4. Transparenz aus einer Hand:

Im Idealfall wählen Unternehmen einen Anbieter, der sowohl die technische als auch die menschliche Expertise miteinander vereint. Der Ansatz, einen einzigen, vertrauenswürdigen und transparenten Cybersecurity-Partner mit einer Open-Door-Policy zu beauftragen, der alles aus einer Hand liefern kann, zahlt sich aus. Neben der technischen Komponente einer robusten Managed-Detection-and-Response-Lösung[4] sollten demnach auch ein fachkundiges Verständnis, die Unterstützung durch die neuesten automatisierten Bedrohungsdaten sowie ein einheitliches Framework, das alle Aufgaben erfüllt, zum Repertoire des Partners zählen.

Entscheidungsträger in kleinen, mittleren und großen Unternehmen müssen Cybersicherheitsherausforderungen proaktiv angehen. Sie benötigen dafür aktuelles, fundiertes und umfassendes Wissen über globale Cyberbedrohungen und die Bedrohungslandschaft im Allgemeinen. Sie benötigen Unterstützung in Form der neuesten Bedrohungsinformationen aus der ganzen Welt, die dazu beitragen, eine Immunität auch gegen bisher unbekannte Bedrohungen aufrechtzuerhalten. Möglich wird dies durch ein einheitliches Framework, das ein integriertes Toolkit mit einer Bedrohungserkennung auf mehreren Ebenen verbindet. Konkret heißt das eine Kombination aus automatisierter Sicherheitslösung (Endpoint Detection and Response) und MDR, bei der externe Sicherheitsexperten Unternehmenskunden aktiv dabei unterstützen, Cyberangriffe so früh wie möglich zu erkennen und zu neutralisieren. ■

Quellenverweise

[1] https://www.kaspersky.com/blog/it-security-economics-2020-part-2/

[2] https://go.kaspersky.com/rs/802-IJN-240/images/Kaspersky_IT%20Security%20Economics_report_2021.pdf

[3] https://box.kaspersky.com/f/346436ee3a9e46159cb2/

[4] https://www.kaspersky.de/enterprise-security/managed-detection-and-response

Christophe Biolley,
Head of Presales Central Europe
bei Kaspersky

Interview: Vorausschauend statt reaktiv im Kampf gegen Cyberangriffe

Threat Intelligence ist mehr als nur ein Buzzword

Die Cyberbedrohungslandschaft verändert sich rasant und wird zunehmend komplexer. Technische Lösungen wie Endpoint-Security schützen vor unterschiedlichen Bedrohungen. Allerdings sollten diese dringend um die Komponente der menschlichen Expertise ergänzt werden. Das Buzzword der Stunde lautet Threat Intelligence (TI). Waldemar Bergstreiser, Head of Channel Germany bei Kaspersky, erklärt im Interview, welche Vorteile Threat Intelligence Unternehmen bietet und worauf sie bei der Auswahl eines Anbieters achten sollten.

Waldemar Bergstreiser, Head of Channel Germany bei Kaspersky (Foto: Kaspersky)

ITS: Herr Bergstreiser, Cyberkriminelle entwickeln ihre Taktiken und Methoden stets weiter und passen sie unter anderem an aktuelle Ereignisse an. Sicherheitslösungen schaffen hier Abhilfe – oder sollten es zumindest. Viele Anbieter bieten nun auch Threat Intelligence in ihrem Portfolio an. Worum handelt es sich dabei?

Waldemar Bergstreiser: Gelegentlich wird der Begriff „Threat Intelligence" mit anderen Begriffen zusammengeworfen oder gleichgesetzt – zum Beispiel „Bedrohungsdaten". Dabei handelt es sich aber nicht um dasselbe, auch wenn es einen Zusammenhang gibt. Bedrohungsdaten sind quasi eine Liste möglicher Bedrohungen. Dagegen wird bei Threat Intelligence das Gesamtbild betrachtet: Die Daten werden in einem breiteren Kontext analysiert. Auf dieser Grundlage lassen sich Entscheidungen zum weiteren Vorgehen treffen. So können Unternehmen mithilfe von Threat-Intelligence-Daten schnellere und fundiertere Sicherheitsentscheidungen fällen. Im Kampf gegen Cyberangriffe fördert TI vorausschauendes statt reaktives Verhalten, indem sie umfassende Einblicke in die Bedrohungslandschaft bietet. Das versetzt Unternehmen in die Lage, Risiken zu antizipieren. Heutzutage reicht ein reaktiver Ansatz für die Cybersicherheit einfach nicht mehr aus.

ITS: Das klingt alles sehr technisch. Das heißt Threat Intelligence ist nur für große Unternehmen mit einer eigenen Sicherheitsabteilung geeignet?

Waldemar Bergstreiser: Nein, Threat Intelligence kann jedes Unternehmen – unabhängig von der Größe – nutzen. Entweder verfügt das Unternehmen selbst über ein Sicherheitsteam, das weiß, wie es damit umgehen kann, oder man lagert TI über einen Managed-Detection-and-Response-Dienst aus. Diese Lösung bietet sich übrigens nicht nur für kleinere Unternehmen an. Threat Intelligence ist immer komplementär zur jeweiligen IT-Infrastruktur des Unternehmens. Es gibt jedoch zahlreiche unterschiedliche TI-Funktionen und eine große Vielfalt an verfügbaren Quellen und Diensten. Das macht es Unternehmen oft schwer zu verstehen, welche Lösung ihre Anforderungen abdeckt. Deshalb ist es wichtig, dass sich der Service individuell an die Bedürfnisse des Unternehmens anpassen lässt.

ITS: Nutzen denn Unternehmen Threat Intelligence bereits rege?

Waldemar Bergstreiser: Wir haben dazu aktuelle Zahlen der Finanzbranche in Deutschland [1], die einen guten Überblick bieten. Diese Unternehmen setzen fast durchgängig auf Threat-Intelligence-Services: Insgesamt nutzen 99 Prozent mindestens einen entsprechenden Dienst. Allerdings haben nicht alle Unternehmen die Services, die sie gern nutzen würden, auch wirklich im Einsatz. Mehr als die Hälfte gibt an, dass sich ihr Unternehmen mithilfe von Advanced-Persistent-Threat-(APT-)Reports über die neuesten Untersuchungen, Bedrohungskampagnen und Techniken von APT-Akteuren auf dem Laufenden hält. Über ein Viertel wünscht sich den Ein-

Weltweit anerkannte Bedrohungsjäger: das Global Research and Analysis Team (GReAT) von Kaspersky (Foto: Kaspersky)

satz solcher Reports. Nahezu die Hälfte greift auf Sicherheitsevaluierungen – etwa über das TIBER-Framework (Threat Intelligence-based Ethical Red Teaming) – sowie auf Tools zur Entdeckung zielgerichteter Attacken zurück. Mehr als ein Drittel (34 Prozent) ist der Auffassung, das eigene Unternehmen sollte solche technologischen Werkzeuge zukünftig einsetzen. Das Bewusstsein für die Bedeutung von Threat-Intelligence-Services scheint also in der Finanzbranche inzwischen recht hoch zu sein.

ITS: Was raten Sie Unternehmen, worauf sie bei der Auswahl eines Anbieters achten sollten?

Waldemar Bergstreiser: Um gegen Bedrohungen gewappnet zu sein, müssen Unternehmen durchgehend alle Assets im Blick haben. Generell sollten sie sich für einen Anbieter entscheiden, der das System rund um die Uhr überwacht und analysiert, damit er jederzeit Schwachstellen finden und sofort entsprechende Sicherheitsmaßnahmen einleiten kann. Außerdem sollte der Anbieter stets topaktuelle Untersuchungsdaten nahezu in Echtzeit bereitstellen.

Eine qualitativ hochwertige Threat Intelligence muss sich auf ein anerkanntes Expertenteam mit nachgewiesener Erfahrung in der Aufdeckung komplexer Bedrohungen stützen und sich reibungslos in die bestehenden Sicherheitsabläufe des Unternehmens integrieren können. Denn eine gute Threat Intelligence entlastet interne Cybersecurity-Abteilungen durch umfassende Automatisierungsmöglichkeiten; so können sich diese auf vorrangigere Ziele konzentrieren.

ITS: Kaspersky bietet ja auch entsprechende Threat-Intelligence-Dienste an, die auf jahrelanger Erfahrung beruhen …

Waldemar Bergstreiser: Genau, die Threat Intelligence von Kaspersky bietet Zugriff auf alle Informationen, die zur Abwehr von Cyberbedrohungen benötigt werden. Wir haben über 20 Jahre Erfahrung mit der Entdeckung und Analyse von Cyberbedrohungen, und unser Team aus internationalen Forschern und Analysten ist weltweit anerkannt. Mit Kaspersky Threat Intelligence [2] erhalten Unternehmen einen direkten Zugang zu technischer, taktischer, operativer und strategischer Threat Intelligence. Zum Kaspersky-Portfolio gehören unter anderem Threat Data Feeds, die Threat-Intelligence-Plattform CyberTrace, Threat Lookup, Threat Analysis mit einer Cloud Sandbox und Cloud Threat Attribution Engine sowie eine Reihe an Threat-Intelligence-Berichtsoptionen. Besonders interessant für Spezialisten sind unsere APT & Crimeware Reportings. Zusätzlich bieten wir den Service „Ask the Analyst", sodass sie bei Bedarf Experten von Kaspersky direkt um Rat fragen können. Sehr stolz sind wir außerdem auf die jüngste Kooperation zwischen Kaspersky und Microsoft, durch die unsere Threat Data Feeds jetzt in Microsoft Sentinel integriert sind.

ITS: Allerdings warnt das BSI vor dem Einsatz der Produkte. Was sagen Sie dazu?

Waldemar Bergstreiser: Die BSI-Warnung bezieht sich „nur" auf unsere Virenschutzprodukte und nicht auf die Threat-Intelligence-Dienste von Kaspersky. Und: wie eine Recherche des *Bayerischen Rundfunks* und *Der Spiegel* zeigen, spielten technische Argumente und Fakten keine Rolle bei der Warnung durch das BSI. Kaspersky hat dem BSI seit Februar umfangreiche Informationsangebote gemacht und es zu Tests und Audits eingeladen. Es ist unser Ziel, den langjährigen konstruktiven Dialog mit dem BSI fortzusetzen, um gemeinsam auf der Basis faktenbasierter Bewertungen für ein Höchstmaß an Cybersicherheit für die deutschen und europäischen Bürger sowie Unternehmen einzutreten.

ITS: Vielen Dank für das Gespräch!

Derzeit bietet Kaspersky Unternehmen unter dem Shortlink **kas.pr/threat-intelligence** einen kostenfreien Zugang zu seinen Threat-Intelligence-Services. Der Zugang wird zunächst für einen Monat gewährt.

Quellenverweise:

[1] https://kas.pr/h2ia

[2] https://www.kaspersky.de/enterprise-security/threat-intelligence

Interview: Eindeutige Bewertungskriterien für eine sichere Digitalisierung

Cybersicherheit muss auf den Prüfstand!

Eindeutige, nachprüfbare Bewertungskriterien tragen zu einer sicheren Digitalisierung bei. Vertrauen in Cybersicherheit ist nur durch maximale Transparenz und kontinuierliche Prozessüberprüfung möglich. Jochen Michels, Head of Public Affairs Europe bei Kaspersky, erklärt im Interview, wo sich Unternehmen in Sachen Bewertungskriterien orientieren können – auch an welchen neutralen Stellen, und was Kaspersky unternimmt, um Vertrauen aufzubauen und zu pflegen.

ITS: Herr Michels, Cybersicherheit gewinnt immer mehr an Bedeutung. Welche Kriterien muss digitale Sicherheitstechnologie erfüllen?

Jochen Michels: Für eine angemessene Sicherheit müssen Sicherheit, Verfügbarkeit, Verarbeitungsintegrität, Vertraulichkeit und Datenschutz risikobasiert betrachtet und erfüllt sein. Auditierungen und Zertifizierungen nach anerkannten Industriestandards helfen Kunden und Partnern, eine fundierte Kaufentscheidung zu treffen.

Jochen Michels, Head of Public Affairs Europe bei Kaspersky

ITS: Können Sie Beispiele nennen?

Jochen Michels: Hier gibt es zum Beispiel die Richtlinien des vom American Institute of Certified Public Accounts (AICPA) entwickelten Standards Service Organization Control 2 (SOC 2).[1] 2019 wurden die Entwicklungs- und Freigabeprozesse der Kaspersky-AV-Datenbasen nach diesen Vorgaben auditiert. Dieses Jahr gab es eine erneute Zertifizierung der jetzt aktuellen Prozesse, durchgeführt von einer der vier großen Wirtschaftsprüfungsgesellschaften. Anfang 2022 wurde das Informationssicherheits-Managementsystem nach ISO 27001:2013 durch die unabhängige Zertifizierungsstelle TÜV AUSTRIA zertifiziert.

ITS: IT-Sicherheit beruht auf Vertrauen und Transparenz. Welche Maßnahmen ergreift Kaspersky dafür?

Jochen Michels: Kaspersky hat seit vielen Jahren umfassende Maßnahmen ergriffen, um technologisch, organisatorisch und strukturell so transparent wie möglich zu sein. Die Verarbeitung und Speicherung von Bedrohungsdaten erfolgt in hochsicheren Rechenzentren in der Schweiz, also einem Land mit hohen Datenschutzstandards. Für Kunden, Partner und Regierungsorganisationen haben wir weltweit verschiedene Transparenzzentren eröffnet. Dort können der Quellcode der Software, die Software-Updates und die Regeln zur Bedrohungserkennung eingesehen und analysiert werden! Weitere nachprüfbare Bewertungskriterien finden Sie auf unserer Website ***kas.pr/vertrauen***.

ITS: Wie können sich Unternehmen vor Cyberbedrohungen schützen?

Jochen Michels: Wichtig ist eine individuelle Risikoanalyse und darauf aufbauend die angemessene Gestaltung der IT-Sicherheitsarchitektur. Dabei sind nicht nur technische Fragen zu beantworten, sondern auch organisatorische und Fragen der Mitarbeiterqualifikation. Sind intern nicht die erforderlichen Ressourcen vorhanden, ist externe Unterstützung durch geschulte Experten in den Bereichen Threat Hunting, Malware-Analyse, Reverse Engineering, Forensik, Incident Response und Notfallplanung erforderlich.

Mitarbeiter sollten sich in regelmäßigen praxisnahen Security-Awareness-Trainings mit typischen Angriffsszenarien auseinandersetzen. Im Rahmen der Kaspersky Automated Security Awareness Platform (ASAP) können diese auf ***kas.pr/asap-some*** derzeit kostenfrei an einem Online-Kurs rund um den sicheren Umgang mit sozialen Medien und Social Engineering teilnehmen.

Des Weiteren sollten die Organisationen Zugriff auf aktuelle Bedrohungsdaten haben, damit sie stets über die neuesten Taktiken und Methoden von Cyberkriminellen informiert sind. Kaspersky unterstützt Institutionen etwa durch sein Threat-Intelligence-Netzwerk, das detaillierte Einblicke liefert. Kaspersky Threat Intelligence (TI) ermöglicht durch die Zusammenarbeit mit unserem weltweit führenden Branchen- und Analystenteam neueste, zuverlässige Informationen über neue Malware- und Bot-Bedrohungen. Derzeit stellen wir unter ***kas.pr/threat-intelligence*** einen kostenfreien Zugang bereit. Durch einen solchen mehrstufigen Ansatz können Unternehmen ein hohes Sicherheitsniveau erreichen.

ITS: Vielen Dank für das Gespräch!

Quellen:

[1] https://us.aicpa.org/interestareas/frc/assuranceadvisoryservices/aicpacybersecurityinitiative

“Tue, was du sagst und sage, was du tust – Kaspersky ist und bleibt transparent und sicher.”

Waldemar Bergstreiser,
Head of Channel Germany, Kaspersky

Branchenweiter Vorreiter für Transparenz und Zuverlässigkeit

Seit Jahren legen wir Quellcode, Updates, Threat Detection Rules, Daten, Engineering-Praktiken und mehr in unseren Transparenzzentren offen. Transparenzzentren bestehen aktuell in der Schweiz, Spanien, Malaysia, Singapur, Japan, den USA und Brasilien.

kas.pr/vertrauen

kaspersky 25 years YOUR PROTECTION IS OUR PRIORITY

Warum Managed Service Provider auch IT-Sicherheit anbieten sollten

Outsourcing als Strategie gegen komplexe Security

Neben der schieren Masse und „Qualität" der Angriffe macht den Unternehmen auch die wachsende Komplexität ihrer eigenen Angriffsflächen zu schaffen. Durch Cloud, Hybrid Work oder IoT vergrößert sich die Zahl der potenziellen Schwachstellen enorm. Alles ist irgendwie mit allem vernetzt und hängt voneinander ab. Und die Angreifer nutzen immer intelligentere Methoden, um Netzwerke, IT-Systeme oder Maschinen zu attackieren. Wie also die IT vereinfachen? Nicht nur Unternehmen selbst stellen sich zunehmend diese Frage. Auch Managed Service Provider müssen die enorme Komplexität von IT-Systemen und Security-Herausforderungen ihrer Kunden reduzieren.

Einfach war früher. Seit Cyberangriffe mit voller Wucht und mit wechselnden Methoden auf die Unternehmen hereinbrechen, fühlen sich Security-Teams wie Hamster im Laufrad. Sie schließen Sicherheitslücken und decken sich mit immer mehr neuen Sicherheitstools ein, wie die steigenden Ausgaben für IT-Sicherheit zeigen. Und am Ende werden sie doch Opfer eines Angriffs.

Angriffe im Stundentakt

Ein Blick auf nur ein paar Meldungen im Sommer 2022 reicht, um das Ausmaß zu erahnen. Ein Automobilzulieferer meldet im August, innerhalb von zwei Wochen von drei verschiedenen Ransomware-Banden angegriffen worden zu sein. Zwei der Angriffe erfolgten innerhalb von nur zwei Stunden. Der eigentliche Einbruch in die Systeme des Unternehmens lag Monate zurück und erfolgte aufgrund einer Fehlkonfiguration der Firewall.

Cisco bestätigte im August einen Einbruch in sein Netzwerk, bei dem der Angreifer einen Mitarbeiter durch Voice-Phishing dazu brachte, einen bösartigen Push für die Multi-Faktor-Authentifizierung (MFA) zu akzeptieren. Die Verletzung führte dazu, dass sich die Cyberangreifer Zugang zum Virtuellen Privaten Netzwerk (VPN) des Unternehmens verschafften und Dateien aus dem Netzwerk entwendeten.

Der Nürnberger Elektronikhersteller Semikron meldet einen Ransomware-Angriff, der zu einer teilweisen Verschlüsselung der IT-Systeme und Dateien geführt habe. Die

Industrie- und Handelskammern waren Ziel eines massiven Cyberangriffs, weswegen deren Internetangebote nicht erreichbar waren und digitale Servicedienstleistungen nicht zur Verfügung standen. Oder medi, Hersteller von medizinischen Hilfsmitteln, meldet einen Cyberangriff, weswegen die Bayreuther Firma IT-Systeme heruntergefahren hat und „nur sehr stark eingeschränkt erreichbar" war.

Gefangen im Hamsterrad

Woran liegt es, dass sich Security-Teams wie Hamster fühlen, obwohl 2021 die Ausgaben für IT-Security in Deutschland laut IDC auf ein neues Allzeithoch von 6,2 Milliarden Euro gestiegen sind? Und obwohl inzwischen in größeren Unternehmen weit mehr als 20 verschiedene Security-Tools im Einsatz sind.

Die Antwort: Die Vielfalt an Tools macht IT- und Security-Teams gleich zweifach zu schaffen. Durch digitale Transformation mit Virtualisierung, Software Defined Infrastructure, Multi Cloud, Remote Work oder Internet of Things steigt die Komplexität der IT-Infrastruktur und mit ihr auch die Security-Aufgaben. Wenn alles miteinander vernetzt ist und immer mehr Mitarbeiter von überall auf Software und Daten zugreifen können, entstehen unzählige Schwachstellen und damit Angriffspunkte auf die IT-Systeme. 29 Prozent der Befragten einer Cybersecurity-Umfrage von IDC in Deutschland bewerten daher das Thema „Sicherheitskomplexität" als größte IT-Sicherheitsherausforderung – noch vor den eigentlichen Angriffsformen wie Ransomware, Phishing oder Advanced Persistent Threats.

Wie reagieren die Unternehmen auf diese Herausforderung? Noch glauben laut IDC-Umfrage rund 66 Prozent der Befragten daran, dass sie aus eigener Kraft und ohne externe Dienstleister und Experten, IT-Sicherheitsbedrohungen bewältigen könnten. Sie investieren in alles, was der Security-Markt hergibt: von IAM-Lösungen über SASE, Cloud Security Posture Management bis hin zu forensischen Analysetools.

Teurer Tool-Schrott landet auf dem Abstellgleis

Nicht immer laufen die Anschaffungen zugunsten des dringend notwendigen Zusammenspiels. Manche Tools landen daher teuer bezahlt schon nach kurzer Zeit auf dem Abstellgleis. Andere Tools werden nicht mehr genutzt, da niemand sie richtig anwenden kann. Und einige Security-Teams verzweifeln, da sie so viele Alerts auf den Tisch bekommen, dass sie nicht hinterherkommen, sie zu bewerten, geschweige denn bei Bedarf Maßnahmen einzuleiten.

So langsam scheint sich aber die Meinung zu ändern, wie sich mit wachsender Bedrohung und fehlendem Fachwissen den Security-Herausforderungen begegnen lässt. Die Entwicklung ist vergleichbar mit dem Trend hin zu Managed Services. Die Ergebnisse einer IDC-Umfrage zeigen, dass Unternehmen anstelle eines Best-of-Breed-Ansatzes – also kaufen, was der Markt hergibt, zunehmend auf ein Security-Ökosystem umschwenken – Plattformen und Outsourcing an Managed (Security) Service Provider (MSSP).

Expertenmangel und Skaleneffekte als Chance für MSSP

Für die MSSP entwickeln sich dadurch neue Wachstumschancen. Nachdem Cloud Computing und Software as a Service das Ende des Outsourcings einzuläuten schienen, spielen den MSSP jetzt die Themen Komplexität und Fachkräftemangel zunehmend in die Karten. Die Unternehmen kommen nicht mehr hinterher, für die Vielfalt an IT- und Security-Aufgaben die passenden Fachkräfte zu bekommen. Die MSSP haben den Vorteil, dass sie gleichzeitig für mehrere Kunden IT- und Security-Systeme managen können und von Skalen- und Kompetenzeffekten profitieren. Daher denken inzwischen 43 Prozent der für die IDC-Deutschland-Studie befragten Unternehmen daran, auch Security-Aufgaben an einen MSSP outzusourcen.

Doch sind Security-Kompetenzen den klassischen Managed Service Providern nicht automatisch in die Wiege gelegt. Auch sie müssen ihr Security-Know-how weiter ausbauen. Sie selbst verzeichnen Cyberangriffe, und Hacker versuchen in die IT-Systeme ihrer Kunden einzudringen. In ihrer Rolle als Service-Provider mehrerer Unternehmen könnten die MSPs jedoch von einem erheblichen Vorteil profitieren, wenn sie Security-Aufgaben in ihr Portfolio integrieren. So wäre ein erheblicher Anteil klein- und mittelständischer Unternehmer bereit, ihren MSP zu wechseln, wenn der neue MSP eine geeignete Cyber-Security-Lösung mitanbieten würde. Genauso viele würden aus diesem Grund erstmals in Erwägung ziehen, einen Managed Service Provider zu beauftragen.

Cyber Protection für Managed Services

Bisher fußte die „Security-Taktik" von MSPs meist auf einer Backup- und Wiederherstellungsstrategie. „Lieber Kunde, mach dir keine Sorgen, wenn du Opfer eines Cyberangriffs wirst, stellen wir dir deine Systeme und Daten wieder aus dem Backup her." Cyberkriminelle wissen das aber längst und löschen beispielsweise bei Ransomware-Angriffen auch die Backup-Dateien. Allein aus diesem Grund kommt den MSP eine zusätzliche Aufgabe zu. Sie sollten ihre Managed Services um Security zu einem Cyber-Protection-Angebot erweitern, der Backup, Disaster Recovery, KI-basierten Malware-Schutz, Remote-Unterstützung und Cyber Security in ein einziges, schnelles, effizientes und zuverlässiges Tool integriert. ■

Christian Anding,
Regional Marketing Manager DACH,
Acronis Germany

PKI, Kryptologie, X.509-Zertifikate und Cybersicherheit

Warum Vertrauensbildung ein Update braucht

Ein Geschäftsvorfall im Zusammenhang mit Zertifikaten verursacht laut Ponemon & Gartner etwa drei bis fünf Millionen Euro Schaden pro Jahr. Ein Unternehmen erlebt typischerweise drei bis fünf Vorfälle pro Jahr. Zertifikate haben offensichtlich ein Problem. Sie werden von vielen Stellen ausgegeben. Damit ein Zertifikat als gültig betrachtet wird, muss der Nutzer der Zertifizierungsstelle vertrauen. In Webbrowsern sind aus diesem Grund schon viele Zertifizierungsstellen als vertrauenswürdig eingestuft. Allerdings sind viele dieser Firmen und Organisationen den meisten Anwendern unbekannt. Der Anwender delegiert somit sein Vertrauen an den Hersteller der Software. Leider ist das nicht das einzige Problem.

Praxis und Umgang mit Zertifikaten sind lange etabliert, entsprechen aber nicht mehr den aktuellen Anforderungen. Ein zweites Problem neben der Delegation von Vertrauen ist, dass dem Zertifikat selbst nur schwer anzusehen ist, wie sicher die bei seiner Ausstellung und Veröffentlichung eingesetzten Verfahren sind und für welche Anwendungen das Zertifikat überhaupt geeignet oder vorgesehen ist. Der Anwender müsste dafür die entsprechenden Dokumentationen der Zertifizierungsstelle, die Certificate Policy (CP) und das Certification Practice Statement (CPS), lesen, deren Inhalte durch RFC 3647 allgemein vorgegeben sind. Bei hohen Sicherheitsanforderungen können qualifizierte Zertifikate verwendet werden, deren Aussteller gesetzlich vorgeschriebenen Sicherheitsvorgaben und staatlicher Aufsicht unterliegen.

Standards bei Zertifikaten

Am weitesten verbreitet ist der Standard X.509 der internationalen Fernmeldeunion. X.509 ist ein ITU-T-Standard für eine Public-Key-Infrastruktur zum Erstellen digitaler Zertifikate. In der elektronischen Kommunikation finden X.509-Zertifikate Anwendung bei den TLS-Versionen diverser Übertragungsprotokolle, wie zum Beispiel beim Abruf von Webseiten mit dem HTTPS-Protokoll, oder zum Unterschreiben und Verschlüsseln von E-Mails nach dem S/MIME-Standard.

- Detaillierungen der Standards werden über die Public Key Infrastructure Standards (PKCS #1-15) definiert.
- ISO 7816 definiert zwei verschiedene Formate für sehr kompakte Zertifikate, die von Chipkarten interpretiert und geprüft werden können (Card Verifiable Certificates (CV-Zertifikate)). CV-Zertifikate kommen zum Beispiel beim Extended Access Control für elektronische Reisepässe und dem deutschen Personalausweis sowie bei der elektronischen Patientenkarte und dem elektronischen Heilberufsausweis zum Einsatz.
- Im Zahlungssystem EMV wird ein besonders kompaktes Zertifikatsformat verwendet.
- Für die Verkehrstelematik, konkret für die Kommunikation mit Kraftfahrzeugen, sind in IEEE 1609.2 und ETSI TS 103 097 spezielle Zertifikatsformate definiert. IEEE 1609.2 definiert auch ein Datenformat für Sperrlisten.

Eine Public Key Infrastructure (PKI) zur Herausgabe von Zertifikaten umfasst folgende Bestandteile:

- ***Digitale Zertifikate:***
  Digital signierte elektronische Daten, die sich zum Nachweis der Echtheit von Objekten verwenden lassen.
- ***Zertifizierungsstelle (Certificate Authority, CA):***
  Organisation, die das CA-Zertifikat bereitstellt und die Signatur von Zertifikatsanträgen übernimmt.
- ***Registrierungsstelle (Registration Authority, RA):***
  Organisation, bei der Personen, Maschinen oder auch untergeordnete Zertifizierungsstellen Zertifikate beantragen können. Diese prüft die Richtigkeit der Daten im gewünschten Zertifikat und genehmigt den Zertifikatsantrag, der dann durch die Zertifizierungsstelle signiert wird. Bei einer manuellen Prüfung wird diese durch den Registration Authority Officer durchgeführt.

- ***Zertifikatsperrliste (Certificate Revocation List, CRL):***
  Eine Liste mit Zertifikaten, die vor Ablauf der Gültigkeit zurückgezogen wurden. Gründe sind die Kompromittierung des Schlüsselmaterials, aber auch die Ungültigkeit der Zertifikatsdaten (zum Beispiel E-Mail) oder das Verlassen der Organisation. Eine Zertifikatssperrliste hat eine definierte Laufzeit, nach deren Ablauf sie erneut aktualisiert erzeugt wird. Anstatt der CRL kann auch eine Positivliste, die sogenannte White-List, verwendet werden, in die nur alle zum aktuellen Zeitpunkt gültigen Zertifikate eingetragen werden. Prinzipiell muss eine PKI immer eine Zertifikatsstatusprüfung anbieten. Hierbei können jedoch neben der CRL (Online Certificate Status Protocol) oder der White-List) als Offline-Statusprüfung auch sogenannte Online-Statusprüfungen wie OCSP (oder SCVP (Server-based Certificate Validation Protocol)) zum Einsatz kommen (siehe Validierungsdienst). Online-Statusprüfungen werden üblicherweise dort eingesetzt, wo die zeitgenaue Prüfung des Zertifikats wichtig ist, zum Beispiel bei finanziellen Transfers etc.

- ***Verzeichnisdienst (Directory Service):***
  Ein durchsuchbares Verzeichnis, das ausgestellte Zertifikate enthält, meist ein LDAP-Server, seltener ein X.500-Server.

- ***Validierungsdienst (Validation Authority, VA):***
  Ein Dienst, der die Überprüfung von Zertifikaten in Echtzeit ermöglicht wie OCSP oder SCVP.

- ***Dokumentationen:***
  Eine PKI führt eines oder mehrere Dokumente, in denen die Arbeitsprinzipien der PKI beschrieben sind. Kernpunkte sind der Registrierungsprozess, die Handhabung des privaten Schlüssels, die zentrale oder dezentrale Schlüsselerzeugung, der technische Schutz der PKI-Systeme sowie eventuell rechtliche Zusicherungen. In X.509-Zertifikaten kann das CPS in den Extensions eines Zertifikats verlinkt werden. Die nachfolgend aufgeführten Dokumente sind teilweise üblich.

- ***CP (Certificate Policy):***
  In diesem Dokument beschreibt die PKI ihr Anforderungsprofil an ihre eigene Arbeitsweise. Es dient Dritten zur Analyse der Vertrauenswürdigkeit und damit zur Aufnahme in den Browser.

- ***CPS (Certification Practice Statement):***
  Hier wird die konkrete Umsetzung der Anforderungen in die PKI beschrieben. Dieses Dokument beschreibt die Umsetzung der CP.

- ***PDS (Policy Disclosure Statement):***
  Dieses Dokument ist ein Auszug aus dem CPS, falls das CPS nicht veröffentlicht werden soll.

Problembereiche

Probleme wurden beispielsweise durch einen Vorfall deutlich, bei dem VeriSign auf die Firma Microsoft ausgestellte Zertifikate an Personen ausgab, die sich fälschlicherweise als Microsoft-Mitarbeiter ausgegeben hatten. Mit diesen Zertifikaten hatten die Betrüger nun einen augenscheinlich vertrauenswürdigen Beleg dafür, dass sie zur Firma Microsoft gehörten. Es wäre zum Beispiel möglich gewesen, Programmcode im Namen von Microsoft zu signieren, so dass er von Windows-Betriebssystemen ohne Warnung installiert würde. Obwohl diese Zertifikate sofort widerrufen wurden, nachdem der Fehler bemerkt wurde, stellten sie doch weiterhin ein Sicherheitsrisiko dar, da die Zertifikate keinen Hinweis darauf enthielten, wo ein möglicher Widerruf zu finden ist. Dieser Fall ist ein Zeichen dafür, dass man sich nicht immer auf die Vertrauenswürdigkeit von Zertifikaten und die Sorgfalt von Zertifizierungsstellen verlassen kann.

Die Sperrung eines Zertifikats ist nur dann effektiv, wenn bei der Prüfung aktuelle Sperrinformationen vorliegen. Zu diesem Zweck können Zertifikatsperrlisten (CRL) oder Onlineprüfungen (zum Beispiel OCSP) abgerufen werden.

Das Gartner Institut hat eine Studie zu diesem Thema durchgeführt und eine Vielzahl von Themen identifiziert. Laut dieser Studie werden für 58 Prozent der Angriffe Zertifikate genutzt. Ebenfalls werden in Unternehmen fast alle Sicherheitsprodukte und -mechanismen über zertifikatsbasierte Methoden abgesichert. Somit bekommt das Zertifikat eine unternehmenskritische Bedeutung. Bekannt sind unter anderem folgende Problembereiche: Gültigkeitsdatum, Verschlüsselungsmethode und Stärke, Hashgenerierung, Aussteller, Nutzungsrechte/Privilegien, Schlüsselablageorte, Schlüsselspeicher.

Ausblick auf Alternativen

Durch die laufende technische Entwicklung gibt es verschiedene Versuche, den Einsatz einer PKI durch andere Konzepte zu ersetzen. Beispiele dafür sind:

- ***SPKI (Simple Public Key Infrastructure)***
  SPKI soll die den alten X.509-Standard ablösen und Zertifikate vielseitiger gestalten. Dabei wird besonderer Wert auf die Art der Autorität, die durch ein Zertifikat übertragen wird, gelegt.

- ***SDSI (Simple Distributed Security Infrastructure)***
  SDSI ist wie SPKI ein Ansatz zur Verbesserung des alten X.509-Standards. Es ist das Konzept, das am stärksten mit dem alten Standard bricht, da es keine Certificate Revocation Lists mehr verwendet. Es wird bei diesem Konzept besonderer Wert auf Benutzergruppen und die Vergabe von Zugriffsrechten für World-Wide-Web-Objekte gelegt. ■

Dr. Alexander Löw,
Geschäftsführung/Owner
Data-Warehouse GmbH

IT-Sicherheit neu gedacht – integrierte Cyber Protection

Daten mit einer einzigen Lösung vor allen Bedrohungen schützen

Einzelne Backup- und Antivirus-Lösungen reichen heutzutage für den zuverlässigen Schutz gegen Cyberbedrohungen fast nicht mehr aus, denn im Angriffsfall müssen alle Lösungen nahtlos zusammenarbeiten und einfach zu handhaben sein. Neue Strategien und Lösungen machen aus IT-Security-Silos integrierte Lösungen, die IT-Dienstleister entlasten und Unternehmen sicher vor Cybercrime und Datenverlust schützen.

Christian Anding, info@acronis.com

Schutz der Geschäftsdaten: Regeln für erfolgreiche Backups

Jedes Backup ist zwar besser als gar kein Backup, dennoch sind nicht alle Backup-Geräte und -Technologien gleich und bieten auch nicht die gleiche Schutzwirkung. Aus diesem Grund ist es für optimalen Schutz am sichersten, Daten nach der 3-2-1-Regel zu sichern:

- Speichern von mindestens drei Kopien der Daten
- Speichern von Daten in mindestens zwei unterschiedlichen Formaten (zum Beispiel Festplatte, Cloud).
- Speichern einer Kopie an einem anderen Standort (zum Schutz vor beispielsweise physischen Katastrophen)

Kombiniert man nun noch die Backups mit IT-Security-Tools, bietet sich ein anspruchsvoller Schutz. Da leider oft eine unzureichende Integration beider Komponenten besteht, entstehen System-Performance-Probleme und Prozesskonflikte. Genau das sollte man vermeiden, denn im Ernstfall kommt es besonders auf eine schnelle Reaktionsfähigkeit an.

Neue Szenarien erfordern einen neuen Ansatz

Da heute auch kleine und mittlere Unternehmen (KMU) ein leichtes Ziel sind, entscheiden sich bereits viele Unternehmen für einen Managed Service Provider (MSP), der ihre IT-Anliegen übernimmt und die Sicherheit ihrer Workloads und Systeme gewährleistet. Doch auch viele MSPs haben Schwierigkeiten, den neuen Bedrohungen einen Schritt voraus zu bleiben. Ein neuer Ansatz ist erforderlich, der Cyber Security, Data Protection und Endpunktschutz-Verwaltung integriert und dabei strenge Kontrollen und funktionsübergreifende Automatisierung bietet. Cyber Protection integriert also Backup, Disaster Recovery, Malware-Schutz, Remote-Unterstützung und Cyber Security in ein einziges, schnelles, effizientes und zuverlässiges Tool.

Acronis Cyber Protect

Dank der Integration und Automatisierung von Acronis Cyber Protect Cloud können Unternehmen leicht und ohne Komplexität ihre gesamten Daten umfassend schützen. Unternehmensdaten können auf Wunsch Datenschutzkonform in über 45 Acronis-eigenen Datenzentren, zum Beispiel in Deutschland, Österreich und der Schweiz, gesichert werden. Die integrierte Lösung bietet die wichtigsten IT-Sicherheitsfeatures über eine Konsole:

- **Endpoint Security**
  Anti-Ransomware-Protection, Antimalware, Anti-Virus, E-Mail-Security und vieles mehr

- **Backup und Recovery**
  Minimiert Datenverluste in der Infrastruktur und Workloads. Safe Recovery ermöglicht das Scannen von Backups mit den neuesten Anti-Malware-Definitionen. Forensik Backups erleichtern spätere Analysen nach einem Vorfall.

- **Verwaltung**
  Zentrales Protection-Management. Bewertung von Systemschwachstellen und Sicherheitslücken in Systemen. Überblick dank Monitoring- und Berichtsfunktionalitäten.
- **Disaster Recovery**
  Spezielle Wiederherstellungsoption, die über eine Offsite-Recovery-Site die Hochverfügbarkeit von geschäftskritischen Daten und Systemen sicherstellt.
- **File Sync & Share**
  Unternehmensinhalte jederzeit, von überall und mit jedem Gerät erstellen und sicher teilen.
- **Nahtlose Integrationen und Automatisierung**
  Administrativen Aufwand minimieren, da Integrationen in gängige Systeme (wie RMM- und PSA-Tools, Webhosting-Verwaltungskonsolen und Abrechnungssysteme) bestehen.

Security Checkliste für Unternehmen

Speziell für Unternehmen mit überschaubaren IT-Budgets und -Mitarbeitern hat Acronis eine **Security-Checkliste** entwickelt, mit der Interessierte einfach und schnell ihre eigene Cyber Protection bewerten und planen können. Mehr Informationen und ein Live Demo zu **Acronis Cyber Protect** finden sich auf der Herstellerwebseite. ■

Acronis auf der it-sa 2022

Vom **25. bis 27. Oktober** zeigt Acronis in **Halle 7** auf **Stand 320** die komplette Bandbreite der Acronis Cyber-Protection-Lösungen und demonstriert wichtige Trends der IT in drei inspirierenden Vorträgen.

Für ein **Gratis-Ticket** oder auch einen Gesprächstermin können sich Interessierte **hier** kostenfrei registrieren.

Mehr dazu hier

Acronis

Security Awareness als Schutzschild gegen Cyberangriffe

Cyberattacken sind aktuell das Risiko Nummer 1 für Unternehmen. Seit der Pandemie haben die Angriffe durch Cyberkriminelle deutlich zugenommen. Dabei erfolgen 85 Prozent der Attacken über den Menschen und nicht über die Maschine.

Neben technischen Maßnahmen ist es essenziell, jeden einzelnen Mitarbeiter zu einer „menschlichen Firewall" auszubilden. Nur wenn die Sicherheitslücke „Mensch" erkannt wird, kann ein ganzheitliches IT-Sicherheitskonzept funktionieren. Mitarbeiter müssen in der Lage sein, Cyberangriffe zu erkennen und sich richtig zu verhalten – und zwar unabhängig davon, ob die Angreifer per Phishingmail, Telefon, SMS oder gar vor Ort im Unternehmensgebäude versuchen, ihr Opfer in die Falle zu locken, um Zugang zu wertvollen Unternehmensdaten zu erhalten.

IT-Sicherheit betrifft also alle Mitarbeitenden und jede Abteilung.

Wie werden Angestellte zum Abwehrschirm gegen Cyberangriffe?

Der beste Schutz: Schulung der Belegschaft

Besonders wirkungsvoll sind interaktive Security-Awareness-Kampagnen mit kurzen E-Learning-Einheiten und zusätzlichen Phishing-Simulationen. Bedarfsgerechte Inhalte erhöhen die Akzeptanz und den Erfolg der Trainingsmethode nachweislich – insbesondere im Hinblick auf den Zeit- und somit auch den Kostenaufwand.

Was beinhaltet eine Security-Awareness-Kampagne?

Eine erfolgreiche Security-Awareness-Kampagne entwickelt die Mitarbeiter zum aktiven Mitglied der Verteidigung. Eine Kombination aus relevanten kurzen Online-Trainings und simulierten Phishing-Angriffen in wiederkehrenden Rhythmen sind der Schlüssel zum Lernerfolg und der Trainingsakzeptanz.

E-Learning Module

Nach einem ersten kurzen Assessment zur Eruierung des Kenntnisstands werden interaktive E-Learning-Module mit zielgerichteten, rollenbasierten und abwechslungsreichen Inhalten angeboten. Das hat den Vorteil, dass jeder das Training erhält, das für ihn von inhaltlicher Relevanz ist.

Die Mitarbeiter werden dadurch weder über- noch unterfordert und erhalten das für sie wichtige Wissen. Die Akzeptanz der Trainings ist bei den Mitarbeitern dadurch sehr hoch.

Wichtig sind immer wiederkehrende kleine Trainingseinheiten, die den Mitarbeitern häppchenweise angeboten werden. Dadurch sind sie dauerhaft wachsam, und der Blick für drohende Gefahren wird geschärft. Die kurzen E-Learning-Einheiten sind damit auch leicht in den „Arbeitsalltag" zu integrieren.

Phishing Simulationen

Parallel werden simulierte Phishing-Angriffe durchgeführt. Diese Attacken werden im Kampagnenverlauf immer schwieriger und münden bei sehr exponierten Mitarbeitern in eigens recherchierten Spear-Phishing-Angriffen mit persönlich zugeschnittenen Inhalten.

Analyse

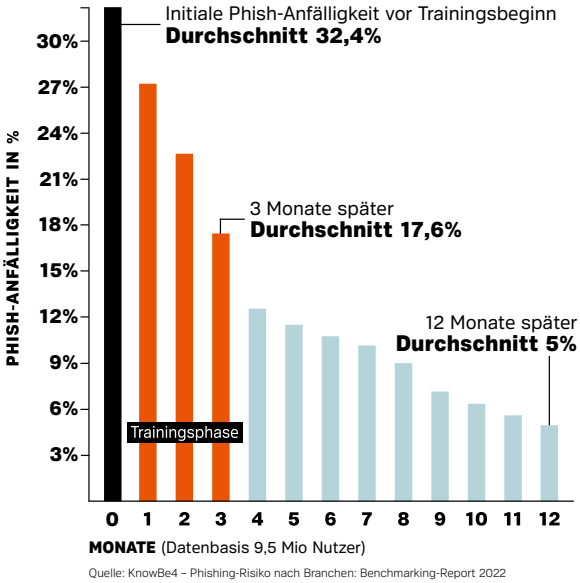
Während der Kampagnenlaufzeit wird das Trainings- und Phishingverhalten in anonymen Gruppen analysiert, um die Kampagneninhalte äußerst feingranular und bedarfsgerecht auszurichten.

Die Mitarbeiter werden durch ihr neu erlerntes Verhalten als „Last line of defense" gestärkt, und das Sicherheitsrisiko „Mensch als Eintrittspforte" wird nachweislich gesenkt.

Wie wird eine nachhaltige Sensibilisierung erreicht?

Trainingserfolg nach drei Monaten - Fehlerrate um fast 50 Prozent gesenkt

Jeder dritte ungeschulte Mitarbeiter fällt auf Cyberattacken herein. Die Häufigkeit des Fehlverhaltens kann durch eine Security-Awareness-Kampagne in nur 90 Tagen um etwa die Hälfte – auf nur 17,6 Prozent – reduziert werden. Bei konsequenter Umsetzung des Trainings sinkt der Wert nach einem Jahr auf durchschnittlich 5 Prozent.



Quelle: KnowBe4 – Phishing-Risiko nach Branchen: Benchmarking-Report 2022

Minimaler Aufwand für wirksame Cybersicherheit - Security Awareness as a Service

Die Bereiche IT oder IT-Security sind vor allem im Mittelstand tendenziell eher unterbesetzt, sodass oftmals nicht genügend Personal zur Verfügung steht. Ein Dienstleister wie Cyber Samurai kann hier mit zusätzlicher Manpower professionell zur Seite stehen.

Security-Awareness-Spezialisten haben den Vorteil, dass sie sich mit den einzusetzenden Tools, Trainings und aktuellen Angriffen umfassend auskennen. Sie können Security-Awareness-Kampagnen sehr viel schneller, effizienter und kostengünstiger umsetzen und das Risiko für einen Cyberangriff nachweislich senken. Mit Security Awareness as a Service erreichen Sie mit minimalem Aufwand eine nachhaltige und wirksame Cyber Awareness.

Der IT-Security Dienstleister Cyber Samurai GmbH hat sich auf eine moderne, nachhaltige und wirksame Schulung der Belegschaft im Security-Awareness-Bereich spezialisiert. Die Cyber Samurais stehen bei der Auswahl der passenden Tools und Herangehensweise zur Seite und führen Trainings- und Phishing-Kampagnen in mittelständischen Unternehmen sowie internationalen Konzernen durch.

Security Awareness als Full-Service-Dienstleistung entlastet unternehmenseigene Ressourcen, erhöht die Effizienz und steigert nachweislich die Sicherheit.

Stärken Sie Ihre menschliche Firewall in nur vier Schritten:

1) **Baseline Phishing-Test durchführen:**
   Dieser Test wird im Vorfeld zu den Trainings durchgeführt. Er dient als Kennzahl für das Gefährdungspotenzial der Belegschaft.

2) **Nutzer durch zielgerichtete Trainingsmodule schulen:**
   Interaktive und kurze Online-Module schulen die Belegschaft bedarfsgerecht und rollenbasiert.

3) **Nutzerverhalten durch simulierte Phishing-Angriffe testen:**
   Simulierte Phishing-Angriffe testen punktuell das Nutzerverhalten und zeigen, ob die Lerninhalte erfolgreich angewendet werden.

4) **Ergebnisse analysieren:**
   Analysen zeigen auf, wie die Belegschaft auf Trainings und Phishing-Tests reagiert und der Lernfortschritt voranschreitet. Durch transparente Kennzahlen können Folgemaßnahmen eingeleitet werden.

Ihre Vorteile mit Cyber Samurai

Die Cyber Samurai GmbH versteht sich im übertragenen Sinn als „Dienender" und „Beschützender" vor den Herausforderungen der Digitalisierung. Sie bietet Ihnen einen Full-Service bei der Planung, Umsetzung und Dokumentation von Security-Awareness-Kampagnen.

Ihre Vorteile:

- Experten-Know-how hinsichtlich marktführender Tools
- Professionelle Kampagnenplanung je nach Kenntnisstand
- Erfahrenes Projektmanagement samt transparentem Reporting
- Bedarfsgerechte, multilinguale Trainingsinhalte
- Zeit-, Ressourcen und Kostenersparnis im Kampagnenverlauf

IT-Security-Dienstleistungen:

- Kostenfreie Erstberatung
- Interaktive Security Awareness Kampagnen
- Simulierte Phishing-Tests
- IT-Security-Checks
- Livehacking, Cyber-Security-Vorträge und -Webinare
- Vulnerability Scans & Pentesting
- ISMS Tool Implementierungen
- Network Detection and Response

Wir beraten Sie, wie Sie eine nachhaltige und wirksame Security-Awareness-Kampagne in Ihrem Unternehmen umsetzen. Sprechen Sie uns an. ■

https://cyber-samurai.net

Mehr dazu hier

CYBER SAMURAI
WE SERVE AND PROTECT

PKI, Kryptologie, X.509-Zertifikate und Cybersicherheit

Ein Geschäftsvorfall mit Zertifikaten verursacht etwa drei bis fünf Millionen Dollar Schaden pro Jahr (Quelle Ponemon & Gartner). Ein Unternehmen erlebt typischerweise drei bis fünf Vorfälle. Stellen Sie sich vor, Sie könnten nur einen davon verhindern! Oder besser gleich alle?

Hintergrund

Zertifikate werden von vielen Stellen ausgegeben. Damit ein Zertifikat als gültig betrachtet wird, muss man der Zertifizierungsstelle vertrauen. In Webbrowsern sind aus diesem Grund schon viele Zertifizierungsstellen als vertrauenswürdig eingestuft. Allerdings sind viele dieser Firmen und Organisationen den meisten Anwendern unbekannt. Der Anwender delegiert somit sein Vertrauen an den Hersteller der Software.

Ein weiteres Problem ist, dass dem Zertifikat selbst nur schwer anzusehen ist, wie sicher die bei seiner Ausstellung und Veröffentlichung eingesetzten Verfahren sind und für welche Anwendungen das Zertifikat überhaupt geeignet oder vorgesehen ist. Der Anwender müsste dafür die entsprechenden Dokumentationen der Zertifizierungsstelle, die Certificate Policy (CP) und das Certification Practice Statement (CPS), lesen, deren Inhalte durch **RFC 3647** allgemein vorgegeben sind. Bei hohen Sicherheitsanforderungen können qualifizierte Zertifikate verwendet werden, deren Aussteller gesetzlich vorgegebenen Sicherheitsvorgaben und staatlicher Aufsicht unterliegen.

Problembereiche

Probleme wurden beispielsweise durch einen Vorfall deutlich, bei dem **VeriSign** auf die Firma Microsoft ausgestellte Zertifikate an Personen ausgab, die sich fälschlicherweise als Microsoft-Mitarbeiter ausgegeben hatten. Mit diesen Zertifikaten hatten die Betrüger nun einen augenscheinlich vertrauenswürdigen Beleg dafür, dass sie zur Firma Microsoft gehörten. Es wäre zum Beispiel möglich gewesen, Programmcode im Namen von Microsoft zu signieren, sodass er von Windows-Betriebssystemen ohne Warnung installiert würde. Obwohl diese Zertifikate sofort widerrufen wurden, nachdem der Fehler bemerkt wurde, stellten sie doch weiterhin ein Sicherheitsrisiko dar, da die Zertifikate keinen Hinweis darauf enthielten, wo ein möglicher Widerruf zu finden ist. Dieser Fall ist ein Zeichen dafür, dass man sich nicht immer auf die Vertrauenswürdigkeit von Zertifikaten und die Sorgfalt von Zertifizierungsstellen verlassen kann.

Die Sperrung eines Zertifikats ist nur dann effektiv, wenn bei der Prüfung aktuelle Sperrinformationen vorliegen. Zu diesem Zweck können **Zertifikatsperrlisten** (CRL) oder Onlineprüfungen (beispielsweise **Online Certificate Status Protocol** – OCSP) abgerufen werden.

Das Gartner-Institut hat eine Studie zu diesem Thema durchgeführt und eine Vielzahl von Themen identifiziert. Laut dieser Studie werden für 58 Prozent der Angriffe Zertifikate genutzt. Ebenfalls werden in Unternehmen fast alle Sicherheitsprodukte und -mechanismen über zertifikatsbasierte Methoden abgesichert. Somit bekommt das Zertifikat eine unternehmenskritische Bedeutung. Bekannt sind unter anderem folgende Problembereiche: Gültigkeitsdatum, Verschlüsselungsmethode und Stärke, Hashgenerierung, Aussteller, Nutzungsrechte/Privilegien, Schlüsselablageorte, Schlüsselspeicher.

Standards bei Zertifikaten

Am weitesten verbreitet ist der Standard **X.509** der **internationalen Fernmeldeunion.** X.509 ist ein ITU-T-Standard für eine Public-Key-Infrastruktur zum Erstellen digitaler Zertifikate. In der elektronischen Kommunikation finden X.509-Zertifikate Anwendung bei den TLS-Versionen diverser Übertragungsprotokolle, wie zum Beispiel beim Abruf von Webseiten mit dem HTTPS-Protokoll, oder zum Unterschreiben und Verschlüsseln von E-Mails nach dem S/MIME-Standard.

- Detaillierungen der Standards werden über die Public Key Infrastructure Standards (PKCS #1–15) definiert.
- **ISO 7816** definiert zwei verschiedene Formate für sehr kompakte Zertifikate, die von Chipkarten interpretiert und geprüft werden können (**Card Verifiable Certificates** (CV-Zertifikate)). CV-Zertifikate kommen zum Beispiel beim Extended Access Control für **elektronische Reisepässe** und den **deutschen Personalausweis** sowie bei der **elektronischen Patientenkarte** und dem **elektronischen Heilberufsausweis** zum Einsatz.
- Im Zahlungssystem **EMV** wird ein besonders kompaktes Zertifikatsformat verwendet.
- Für die **Verkehrstelematik,** konkret für die Kommunikation mit **Kraftfahrzeugen,** sind in IEEE 1609.2 und ETSI TS 103 097 spezielle Zertifikatsformate definiert. IEEE 1609.2 definiert auch ein Datenformat für Sperrlisten.

Automatisierung und Management

Trotz des Einsatzes von unterschiedlichen Sicherheitstechnologien, wie Firewalls, Vulnerability-Scanner, SIEM etc., werden Unternehmen zunehmend Opfer von erfolgreichen Cyberattacken. Analysiert man die Angriffs-Vektoren, zeigt sich, dass viele erfolgreiche über Missbrauch von Identitäten und Zertifikate erfolgen.

PCert ermöglicht einen automatisierbaren, vollständigen Überblick über die unternehmensinterne IT-Vertrauens-, Crypto- und X.509-Zertifikatslandschaft. Dadurch lassen sich Risiken identifizieren oder eventuell auftretende Probleme frühzeitig und präventiv lösen.

Die Lösung unterstützt sowohl mittlere wie auch große Unternehmensnetzwerke und bietet zusätzlich wissensbasierte, servicegestützte Entscheidungshilfen an. Hier hat bisher eine Unterstützung in den wichtigsten Aspekten Identifizierung, Sammlung, Bewertung gefehlt. Da es in den existierenden Umgebungen bereits massive Probleme gibt, werden mit der Einführung weiterer Digitalisierung wie Internet of Things (massiv vernetzte Umgebungen) und Supply-Chain-Sicherheit diese Probleme wachsen. Die jederzeit drohende Schwächung zurzeit genutzter Crypto-Maßnahmen durch Softwarefehler und/oder schwache Schlüssel und Methoden erfordert außerdem eine schnelle Reaktion innerhalb des Unternehmens und damit

eine Crypto-Agilität, um auf diese Bedrohung zu reagieren. Ohne Automatisierung des gesamten IT-Trust-Bereichs werden alle Sicherheitsmaßnahmen unnötig geschwächt. Ebenfalls ist eine anstehende Migration zu Post Quantum sicheren Verschlüsselungsmethoden vorzubereiten.

Dieses Thema ist nicht mehr manuell zu lösen, deswegen setzt hier PCert an. Um den Überblick über die interne Struktur zu bekommen, gibt es zwei Ansätze:

1. Der Anwender erlaubt nur vertrauenswürdige Software zur Installation und bekommt von der Herstellerfirma eine Zertifikatsübersicht.

2. Der Anwender verifiziert die Zertifikatslandschaft mit einer automatisierten Softwarelösung und definiert seine Vertrauenslandschaft selbst.

Beide Ansätze erfordern Kenntnis der vollständigen Vertrauenslandschaft ohne Silos von Hersteller oder Zulieferer.

Unsere langjährige Erfahrung in der Erstellung von militärischen und luftfahrttechnischen Softwareprodukten sowie Certificate Authorities und Public-Key-Infrastrukturen ist in die Entwicklung von PCert eingeflossen und dadurch wurde auf höchstmögliche Softwarequalität geachtet. Zusätzlich wurde ein weites Spektrum von Sicherheitsrichtlinien von Anfang an in die Produkte mit einbezogen, sodass bei Bedarf eine herausragende Sicherheit auch auf staatlichem Level mit minimalen Aufwendungen erreicht werden kann.

PCert entdeckt Ihre Computer-Vertrauensbeziehungen (Krypto-Assets wie X.509, SSH, PGP, Keystores) und unterstützt Sie dabei, sie gemäß Ihren Unternehmensregeln unabhängig von Einzelpersonen und Silos zu verwalten und Ihren Cybersicherheitsansatz (SOC, CIT) mit einer neuen leistungsstarken Cybersicherheitsfähigkeit zu stärken.

PCert-Scanner

Ermöglicht Ihrem Unternehmen das Sammeln und Überwachen alle X.509-Zertifikate, Keystores (+Schlüssel) auf Ihren Computern (bis zu 400k pro Gerät), Servern (bis zu 200k pro Gerät) oder anderen Geräten.

Verschaffen Sie sich einen unternehmensweiten Überblick und Risikobewertung für die Einhaltung gesetzlicher Vorschriften (zum Beispiel SOX, ISO 27.001) oder bereiten Sie die Neugestaltung Ihrer Vertrauenslandschaft (beispielsweise PKI, HSM) vor.

PCert AIO-Plattform

Sammelt alle Scan-Ergebnisse, generiert eine unternehmensweite Übersicht, setzt Policies durch, tauscht, verknüpft und registriert Zertifikate mit den Geräten, bietet Management und Verifikation Ihrer IT-Trust Landscape und hilft Ihnen, auch unbekannte Cyberrisiken oder Schwachstellen zu verstehen und Eindringlinge zu erkennen. ■

Mehr dazu hier

Über Data-Warehouse:

Die Data-Warehouse GmbH ist seit 1987 am Markt erfolgreich tätig und hat sich zu einem Systemhaus mit eigenem Produktportfolio im Bereich gesamtheitliches, qualitätsgesichertes Informationsmanagement, Logistik- und Prozessoptimierung, gesamtheitliche Sicherheitsstrategie und Datenschutzberatung entwickelt.

Wir schaffen auf Wunsch ein hocheffizientes IT-Umfeld mit minimalem Consultingbedarf und produktneutraler Beratung. Unsere Bandbreite umfasst alle Tätigkeiten von der klassischen Beratung über den Aufbau von IM-Strategien über die Optimierung existierender Lösungen (Prozesse, Architekturen), Datenkonsolidierung, bis hin zur Umsetzung und dem Betrieb.

Im Hochsicherheitsumfeld bieten wir Erfahrungen in Projekten zum Beispiel mit nationalen und internationalen Partnerschaften (zum Beispiel Airbus, ESG und weitere) auf erfolgreiche Unterstützung von Kunden wie Airbus, BAESystems, Alenia, CASA, der Luftwaffe, Heer, Marine und dem österreichischen Bundesheer zurückgreifen. Unsere Services werden weltweit in jeder Projektgröße angeboten.

Unsere Strategie unterstützt die Philosophie der agilen, individuellen Lösungsfindung und ist seit Jahrzehnten in der Industrie bewährt bei der Durchführung von Informationskonsolidierungen, Prüfung und Etablierung von Computersicherheit, schrittweisen Ablösung von IT-Systemen, Unterstützung von ERP-Systemen, Qualitätssicherung von Daten und Informationen, Aufbau von zentralen Informationssystemen und automatisierter Langzeitarchivierung. Durch eigene hocheffiziente Produktlinien im Bereich Datenmanagement, Cybersicherheit und Softwareentwicklung können (fast) alle Themenbereiche individuell mit standardisierter Plattform und minimalem Aufwand gelöst werden.

Produkte:

IQIMS-OC für die transparente, revisions- und rechtssichere Speicherung von Informationen. Ermöglicht iterative und evolutionäre, hocheffiziente und langfristig aktuelle Lösungen, bei gleichzeitiger Senkung von IT-Kosten, Entlastung des eigenen IT-Personals, transparente Einbindung in IT-Landschaften (ERP/SinN), Minimierung der Programmierung und Abhängigkeiten.

IQIMS Ebus-J: Vollständige ausgereifte 4 GL zur aufwandsminimierten, iterativen crossplattformkompatiblen Produktion von Softwarelösungen mit eigener Datenbank. Schnell erlernbare Programmiersprache (BASIC) für sichere, schnelle auch komplexe Lösungen in C, Java, n-tier Java, HTML. Einbindung von beliebigen Bibliotheken, DB. Keine Exportbeschränkungen durch Drittstaaten da „Made in Bavaria".

Tixxle: Mobile Collaboration & Kommunikationslösung (Notizzettel für das Internet), Verbindung mobiler zu stationärer Kommunikation usw.

PCert: Mandantenfähiger Key- und Zertifikatsscanner zur Auditierung des Unternehmens. Unternehmensweite Sammlung, Analyse und Auswertungen, Detektion und Identifikation ungültiger, doppelter Zertifikate als Schwachstelle. Unterstützung der Compliance, Risk und Unternehmenssicherheit.

Referenzen: z.B. Dt. Luftwaffe, Österr. Bundesheer, Eurofighter GmbH, NATO, Airbus , Airbus DS, Cassidian Cyber Security, Dt. Post, EV Group, 1&1 AG, IKK,KZV, Telefonica O2, Dt. Börse AG, Dresdner Bank AG und viele mehr.

Endpoint Detection and Response erreicht den Mittelstand

ESET KOMMT HACKERN UND SCHWACHSTELLEN FRÜHZEITIG AUF DIE SPUR

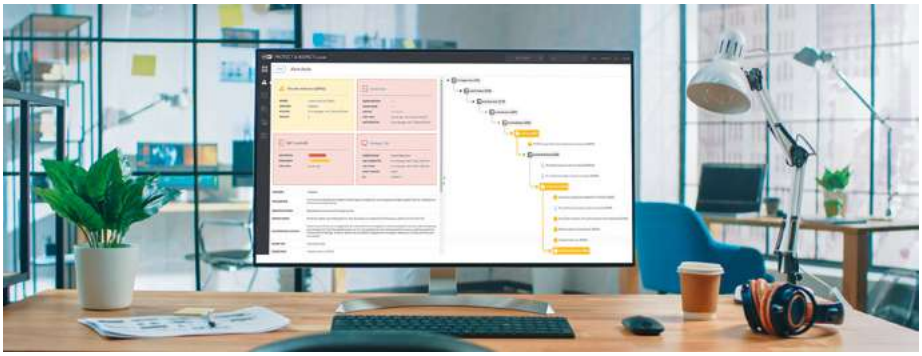
Im Zeichen der Digitalisierung müssen Organisationen mehr denn je über die Vorgänge in ihrem Netzwerk informiert sein. Nur so lassen sich Angriffe von außen abwehren, interne Sicherheitslücken identifizieren oder erfolgreiche Hackerangriffe in Echtzeit erkennen und aufarbeiten. Endpoint-Detection-and-Response-Tools unterstützen die IT-Security-Teams von immer mehr KMU.

Erfolgreiche Cyberangriffe auf Unternehmen erfolgen in den seltensten Fällen „Knall auf Fall", sondern sind das Resultat längerer und vor allem aufwendiger Vorbereitungen aufseiten der Hacker. Je besser das anzugreifende Netzwerk jedoch abgesichert ist, desto intensiver müssen Cyberkriminelle nach Schwachstellen suchen. Das bedeutet für sie, vorab geeignete Wege zu finden, um in der Zielorganisation eine Basis für einen Angriff schaffen zu können. Insbesondere, wenn Advanced Persistent Threats und Zero-Day-Exploits ins Spiel kommen, stoßen jedoch klassische Sicherheitsprodukte an ihre Grenzen. Diese Gefahren können zwar selten direkt, wie beispielsweise Malware, aber umgehend als Anomalie im Netzwerk erkannt werden.

Endpoint Detection and Response

Abhilfe schaffen Endpoint-Detection-and-Response-(EDR-)Lösungen wie ESET Inspect, die das Schutzniveau deutlich erhöhen und IT-Security-Verantwortlichen eine umfassende Innensicht ihres Netzwerks ermöglichen. Aber was bedeutet Detection und Response eigentlich in der Praxis? Zum einen soll damit der Endpoint geschützt werden („Detection"), auf dem die meisten Hacker-Aktivitäten stattfinden. Dort liegt ein Großteil der schutzwürdigen Daten vor bzw. werden am Gerät zum Beispiel Passwörter oder Bankdaten eingegeben. Zum anderen beschreibt „Response", dass auf Anomalien sofort reagiert werden kann. Je nachdem kann das eine manuelle Reaktion eines IT-Sicherheitsexperten oder eine automatische, zuvor definierte Verhaltensweise sein.

Und genau auf diese Veränderungen an Dateien, Protokollen und ausgeführten Diensten springen die EDR-Lösungen beinahe in Echtzeit an – und können sofort überprüft werden. Zudem bieten sie eine weitere wichtige Einsatzmöglichkeit: Anhand von EDR können nach einer Cyberattacke forensische Untersuchungen eingeleitet werden. Ähnlich einem Mordfall in bekannten Krimis werden möglichst viele Informationen gesammelt und Alibis – in diesen Fällen die ordnungsgemäßen Arbeitsweisen – überprüft. Administratoren erkennen dann zuverlässig, wie der Angriff ablief,



welche Schwachstellen konkret ausgenutzt und welche Veränderungen im Netzwerk vorgenommen wurden. Dazu kann der Verantwortliche auf Informationen von Reputationssystemen wie ESET LiveGrid zurückgreifen und/oder anhand des MITRE ATT&CK Frameworks die einzelnen Phasen einer Attacke umgehend einordnen.

Managed Detection and Response

Aufgrund der Vielschichtigkeit und der Komplexität der Materie kamen EDR-Lösungen bislang nur in Großkonzernen zum Einsatz, in denen die IT-Abteilungen entsprechende Ressourcen und Know-how mitbringen. Dies ändert sich gerade gravierend: Mittelständische Unternehmen nutzen verstärkt die Möglichkeit, EDR in ihren Netzen einzusetzen. Sie greifen dabei auf eine stetig wachsende Anzahl von Dienstleistern zurück, die mit dem sogenannten Managed Detection and Response (MDR) ihre Expertise als Service anbieten. Dieser Bereich steht noch am Anfang und bietet gerade deshalb viel Potenzial für den Channel.

Gleichzeitig werfen auch IT-Sicherheitshersteller ihren Hut in den Ring. Beispielsweise steigt ESET ab 2023 mit eigenen MDR-Services in den Markt ein. Unter der Bezeichnung ESET Endpoint Detection and Response bietet der Sicherheitsspezialist seine Dienstleistung in den drei Stufen „essential", „advanced" und „ultimate" an. Mit umfassenden, auf den tatsächlichen Bedarf der Kunden zugeschnittenen MDR-Services stärkt ESET die Schutzmechanismen der Unternehmens-IT. Dreh- und Angelpunkt ist dabei die eigene EDR-Lösung ESET Inspect. Die Services verfolgen einen ganzheitlichen Security-Ansatz, der effektive Hilfe bei der Untersuchung von Vorfällen sowie eine ausführliche Analyse potenziell schädlicher Dateien bietet. Darüber hinaus wird eine optimale Anpassung an die Bedürfnisse der Organisation gewährleistet. So werden mögliche Einfallstore frühzeitig erkannt und zuverlässig geschlossen.

Extended Detection and Response

Sicherheitsexperten schwören auf die erweiterte Form von Endpoint Detection and Response: Extended Detection and Response (XDR). Diese besondere Variante bezieht Daten nicht nur von Endpoints, sondern auch von vielen weiteren Informationsquellen in seine Analysen mit ein. Dies können im „einfachen" Fall Daten aus Netzwerken, E-Mails oder der Cloud-Sandbox sein. Besonders wertvoll wird XDR dann, wenn Telemetriedaten aus weiteren Quellen wie Cloud-Anwendungen, SIEM (Security Information and Event Management), SOAR (Security Orchestration and Response) oder RMM (Remote Monitoring and Management) verarbeitet werden.

Für die gewinnbringende Auswertung aller Daten benötigt XDR zum einen eine leistungsfähige EDR-Lösung und zum anderen eine Security-Plattform, die mit der nötigen Performance und einem ausgefeilten Know-how aus Einzelinformationen Übersichten, Problemlösungen und Security-Aktionen generieren kann. Mit ESET Inspect und der ESET PROTECT-Plattform steht Kunden und Dienstleistern ein leistungsfähiges XDR-Duo zur Verfügung. ■

Mehr dazu hier

Digital Security
Progress. Protected.

ESET 100% Made in EU IT-Security

IT-Sicherheit ist Vertrauenssache

„Eine No-Backdoor-Garantie ist für uns selbstverständlich – denn: Als IT-Sicherheitshersteller aus der EU stehen wir zu 100 % hinter den demokratischen Werten der Europäischen Union."

– Holger Suhl, Country Manger DACH, ESET Deutschland GmbH

www.eset.de/itsa

Stand 7-530

25.-27. Oktober in Nürnberg

itsa EXPO CONGRESS

Cybersecurity-Expertise von macmon secure auf der it-sa: Stand 224, Halle 7

Zero Trust Network Access – Übersicht und Kontrolle lokaler Netzwerke und Cloud-Infrastrukturen

Personenbezogene Daten wie Name oder E-Mail-Adresse sind ein lukratives Ziel von Cyberkriminellen. Homeoffice und Digitalisierung bieten neue Angriffsmöglichkeiten. Durch Diebstahl, Spionage und Sabotage entsteht der deutschen Wirtschaft jährlich ein Gesamtschaden von 223 Milliarden Euro, die Dunkelziffer ist hoch. Fundierte Abwehrstrategien präsentiert macmon secure, gemeinsam mit Partnern, auf der diesjährigen it-sa in Nürnberg.

Cyberkriminelle überall aktiv – lokal und in der Cloud

Externe Netzwerkzugriffe auf Unternehmensressourcen sind heutzutage Normalität. Geräte werden weltweit genutzt und können überall und zu jeder Zeit direkt auf Cloud-Dienste, E-Mail-Applikationen und andere potenziell vertrauliche Unternehmensressourcen zugreifen. Kriminelle können somit an unterschiedlichen Stellen ansetzen, um ihre Ransomware in Unternehmen, Betrieben, Institutionen oder Behörden zu platzieren. Hier schiebt das **Sicherheitskonzept Zero Trust** einen starken Riegel vor. Es fußt auf der Philosophie, weder einem Gerät noch einem Benutzer einen Vertrauensvorschuss zu geben, bevor eine **sichere Authentifizierung** erfolgt ist. Mit ZTNA ist es möglich, die Datensicherheit nachhaltig zu gewährleisten und modernen Anforderungen an die Netzwerksicherheit zu entsprechen.

„Wir erwarten während der it-sa hohe Besucherzahlen an unserem Stand, denn wir verzeichnen eine weiterhin steigende Nachfrage nach unseren Sicherheitslösungen bei Kunden, Channel Partnern und Interessenten. Wir haben eine valide Marktstudie durchgeführt, um unsere Eindrücke mit konkreten Zahlen zu untermauern. Fazit: Der Einsatz von NAC-Lösungen wurde bei zwei Drittel der Befragten noch nicht realisiert, obwohl ein Viertel aller Sicherheitsvorfälle im Netzwerk der befragten Unternehmen stattfand“, erläutert Christian Bücker, Business Director, macmon secure.

Ganzheitliche Sicherheitskonzepte mit NAC und SDP sind notwendig

Das Zero-Trust-Konzept basiert auf Restriktion und Monitoring. Bereits seit 2003 trägt macmon secure mit seiner **Network-Access-Control-Lösung (NAC)** diesem Ansatz Rechnung. Dieser erlaubt nur definierten Geräten Zugang zum Netzwerk, ganz gleich, ob iPads, Laptops oder medizintechnische Geräte. IT-Administratoren wissen jederzeit, welche Endgeräte im lokalen Netzwerk angemeldet sind, und können diese dank der kompletten **Netzwerk-Übersicht** permanent identifizieren und effizient überwachen. Jedes Endgerät, welches im jeweiligen Netzwerk nichts zu suchen hat, erhält von vornherein keinen Zugriff. Die unbefugte Nutzung der IT-Systeme ist damit nahezu ausgeschlossen.

Mit **macmon SDP** dehnte der IT-Sicherheitsexperte den Schutz lokaler Netzwerke durch **macmon NAC** auf sämtliche Cloud-Dienste aus. Im Unterschied zu klassischen VPNs authentifizieren sich bei Secure Defined Parameter (SDP) sowohl der Benutzer als auch der Agent am Controller. Dieser arbeitet hochgesichert in einem ISO-27001-zertifizierten Rechenzentrum in Berlin. Ist die Authentifizierung erfolgreich, teilt er dem Agenten mit, ob der jeweilige Nutzer Zugriffsrechte auf die Unternehmensressourcen hat und welche das sind. Jeder einzelne Zugriff – egal ob im Firmennetzwerk oder in der Cloud – wird geprüft. Es gibt keinen Vertrauensvorschuss.

Als DSGVO-konforme Lösung, gehostet in einer deutschen Cloud mit Fokus auf einfache Bedienung und Nutzung, ist dieses skalierbare Sicherheitsangebot einzigartig. ■

www.macmon.eu

Mehr dazu hier

macmon intelligent einfach

Bild: greenbutterfly/Shutterstock

AIRLOCK®
SECURE ACCESS HUB

Besuchen Sie uns auf der it-sa 2022
Halle 7A
Stand 111

Die Zukunft der Applikationssicherheit

Agil und benutzerfreundlich

Auf unserem Kongress am **26. Oktober** können Sie in hilfreichen Vorträgen erfahren, wie sich die Welt der **Applikationssicherheit** durch neue Technologien und Ansätze für höhere Agilität und Benutzerfreundlichkeit **verändert** hat.

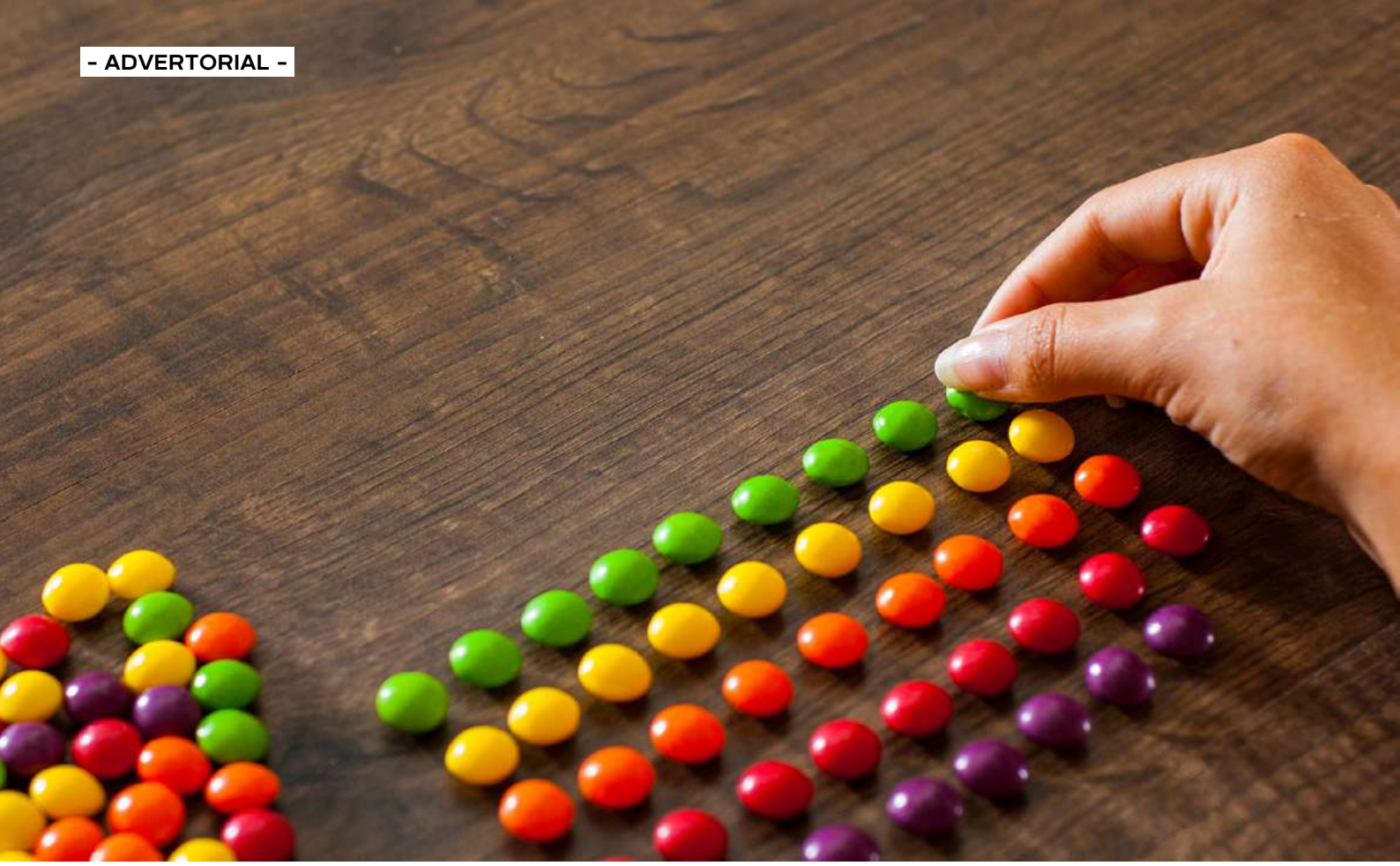
Simon Hülsbömer, Senior Project Manager Research Studienprojekte in der Marktforschung von CIO, CSO und COMPUTERWOCHE, gibt spannende Einblicke, wie **deutsche Unternehmen** auf die Veränderungen bereits reagiert haben, auf welchem **Status** sie stehen und welche nächsten Schritte geplant werden.

In einem Anwendungsbeispiel der V-Bank erfahren Sie, wie das Unternehmen in eine agile **Welt mit agiler Security** aufgebrochen ist.

Abschließend rückt die Identität in den Mittelpunkt der Applikationssicherheit: Das Prinzip von **Continuos Adaptive Trust** wird vorgestellt, die Vorteile dieses Ansatzes sowie die technologischen Anforderungen werden erklärt.

Registrieren Sie sich gleich und erhalten Sie ein **kostenloses Ticket:**

airlock.com/itsa
Kostenloses itsa Ticket und Anmeldung zum Kongress



So gelingt Unternehmen die Workflow-Automatisierung des E-Mail-Verkehrs

Den Kommunikationskanal E-Mail mit all seinen technischen und organisatorischen Herausforderungen unter Kontrolle zu behalten, stellt höchste Anforderungen an IT-Verantwortliche. Mit der Predelivery Logic bietet Retarus hier eine innovative Lösung, mit der E-Mails nach individuellen Regeln analysiert, optimiert oder umgeleitet werden. Der Service leistet als Teil der Retarus Secure Email Platform einen entscheidenden Beitrag zur Automatisierung und Beschleunigung von Geschäftsprozessen.

Unternehmen mit komplexen E-Mail-Infrastrukturen müssen heute häufig eine immer größere Menge an Nachrichten sinnvoll verwalten und absichern. Denn E-Mails sind nicht nur integraler Bestandteil jedes digitalen Arbeitsplatzes, sondern auch vieler unternehmenskritischer Geschäftsprozesse. E-Mail-Kommunikationslösungen aus der Cloud bieten dabei einen klaren Wettbewerbsvorteil für Unternehmen. Hier kommt die Retarus Secure Email Platform in Spiel. Sie bietet nicht nur Schutz vor Cyberangriffen, beispielsweise durch die frühzeitige Erkennung unbekannter Bedrohungen sowie Lösungen für Verschlüsselung und Archivierung, sondern auch innovative Infrastruktur-Services wie die Predelivery Logic. Mit der Predelivery Logic erhalten Unternehmen einen Werkzeugkasten, der es IT-Verantwortlichen ermöglicht, ihren E-Mail-Verkehr auf Basis selbst definierter Regeln zu kontrollieren, zu organisieren oder anzupassen. So werden beispielsweise eingehende E-Mails, noch bevor sie an die eigene Infrastruktur zugestellt werden, automatisch nach individuellen Regel-

werken weiterverarbeitet. Folglich verfügen IT-Verantwortliche wieder über mehr Ressourcen, Innovationen voranzutreiben, die sich positiv auf Geschäftsprozesse und -umsatz auswirken.

Umfassende Kontrolle des eingehenden E-Mail-Verkehrs

Mit der Predelivery Logic von Retarus lässt sich der eingehende E-Mail-Verkehr automatisiert und effizient kontrollieren. Flexible Kombinationsmöglichkeiten aus Bedingungen und Aktionen ermöglichen beim Definieren der Regelwerke nahezu unbegrenzte Einsatzszenarien. Dabei spielt es keine Rolle, ob das Unternehmen seine E-Mail-Infrastruktur On-Premises oder in der Cloud betreibt. Der Service spielt sogar gerade in hybriden Umgebungen seine Vorteile voll aus. Mit der Predelivery Logic werden E-Mails schon zum Zeitpunkt der Interaktion mit der Retarus Enterprise Cloud auf Ebene des Secure Email Gateways weiterverarbeitet. Dies ermöglicht maximale Flexibilität, die serverseitige oder auf einzelne Postfächer beschränkte lokale Regelwerke nicht bieten können. Denn wenn sich die E-Mail erst einmal in der eigenen IT-Landschaft befindet, lassen sich viele Sicherheitsregeln und -maßnahmen nicht mehr umsetzen.

Innovative Vorselektion anhand Sprache und Inhalt

Der Funktionsumfang der Retarus Predelivery Logic reicht deutlich über den einer Policy Engine hinaus. Denn neben einem User-abhängigen Routing von E-Mails an bestimmte Server beziehungsweise Standorte des Firmennetzes oder Tochterfirmen liefert die Predelivery Logic einen entscheidenden Beitrag, um Geschäftsprozesse zu automatisieren. Es ist beispielsweise möglich, E-Mails anhand ihres Inhalts oder ihrer Sprache zu verarbeiten. So lassen sich etwa Nachrichten an Funktionspostfächer automatisch vorsortieren. Die E-Mail wird dann direkt an die Server der richtigen Landesgesellschaft oder an die zuständige Abteilung eines Unternehmens geroutet, sobald sie empfangen wird. Durch die automatische Vorselektion (etwa an info@- oder support@-Adressen) profitieren beispielsweise Contact Center von einer deutlich effizienteren E-Mail-Bearbeitung. Darüber hinaus ist es möglich, E-Mails vollautomatisch und regelabhängig zu verändern – vom Umschreiben der Adresse bis hin zum Hinzufügen eines Schlagworts in der Betreffzeile.

Automatische Isolierung basierend auf GeoIP

Zusätzlich erlauben es die Regelwerke der Predelivery Logic, E-Mails nach landesspezifischer Herkunft („Source IP Country") zu identifizieren und entsprechende Maßnahmen automatisch einzuleiten, beispielsweise wenn seitens des Unternehmens aufgrund der aktuellen politischen Lage der Bedarf entsteht, alle Nachrichten aus bestimmten Regionen oder Ländern vorsorglich zu isolieren – sei es aus reinen Sicherheitserwägungen oder auch aufgrund interner Compliance-Vorgaben. Je nach Konfiguration lassen sich Nachrichten beispielsweise in die User-Quarantäne leiten oder komplett blockieren.

Professionelle Kommunikation über den Outbound-Kanal

Mit der Retarus Predelivery Logic lassen sich individuelle Regelwerke nicht nur für eingehende Nachrichten, sondern auch für den Outbound-Kanal festlegen. Ob Spin-off von Tochtergesellschaften, Carve-out, Zukäufe, Fusionen oder schlicht ein Rebranding – idealerweise sollen Mitarbeiter bereits zum Stichtag unter dem richtigen Firmennamen auftreten. Mit der Predelivery Logic lassen sich beispielsweise die Unternehmensbezeichnung oder -Domain überprüfen. Fehlerhafte oder nicht aktuelle Firmennamen werden automatisiert umgeschrieben. Auf diese Weise treten Mitarbeiter gegenüber Kunden und Partnern stets professionell in Erscheinung, sei aus Marketing- oder aber aus juristischen Gründen. Zusätzlich lässt sich per Retarus Email Live Search Monitoring der Weg einer Nachricht durch die gesamte Verarbeitungskette nachvollziehen. Wie bei anderen Regeln der Retarus Predelivery Logic können Administratoren die Richtlinien jederzeit individuell anpassen und beispielsweise das Rewriting nur für bestimmte Abteilungen oder einzelne Benutzer vornehmen lassen.

Umfassender Support und höchste Datenschutz-Standards

Retarus stellt die Predelivery Logic als zentralen Self-Service über das webbasierte Enterprise Administration Services (EAS) Portal bereit. Alle Regeln lassen sich dort transparent über einen Editor anlegen, verändern und priorisieren. In die eigentliche E-Mail-Infrastruktur des Unternehmens wird dazu nicht eingegriffen. Darüber hinaus stehen die Retarus-Experten Kunden bei der Umsetzung individueller Regeln für eine effiziente E-Mail- und Workflow-Automatisierung per 24/7-Support in der jeweiligen Landessprache beratend zur Seite. So lassen sich Probleme durch Zeitmangel oder noch unklare Organisationsstrukturen vermeiden und auch vorübergehende Maßnahmen schnell und mit geringem Aufwand umsetzen. Die Fehleranfälligkeit manueller Eingriffe reduziert sich dadurch deutlich. Auch hinsichtlich Datenschutzes, gesetzlichen Vorgaben und Compliance sind Unternehmen, die auf die Retarus Secure Email Platform setzen, auf der sicheren Seite. Denn Retarus setzt gezielt auf Local Processing, verarbeitet alle Daten in selbst betriebenen, auditierbaren Rechenzentren und erfüllt neben branchenspezifischen Standards und DS-GVO-Vorgaben auch höchste Compliance-Anforderungen. ■

Sie sind neugierig geworden und wollen mehr über die Retarus Secure Email Platform und die Predelivery Logic erfahren? Dann besuchen Sie Retarus auf der diesjährigen it-sa in Nürnberg in Halle 7, am Stand 502.

www.retarus.de

Mehr dazu hier

retarus

Bild: pavel siamionov - stock.adobe.com

Managed Detection and Response:

r-tec vereint modernste Technik mit Expertenwissen

Der Managed Detection and Response Service des Wuppertaler IT-Spezialisten r-tec vereint ein automatisch arbeitendes Next-Generation-SIEM-System mit einer manuellen Expertenanalyse. Im Angriffsfall steht den Kunden außerdem ein Incident-Response-Team zur Seite, das für die schnelle Wiederherstellung des Normalbetriebs sorgt.

Für die meisten Cyberkriminellen stellen klassische Security-Information-and-Event-Management-Systeme (SIEM) längst keine ernst zu nehmenden Gegner mehr dar. In immer kürzeren Abständen entwickeln sie neue Angriffsmuster und Tools, mit deren Hilfe klassische SIEM-Lösungen ohne großen Aufwand überlistet werden können. Das Problem besteht darin, dass die Systeme bei der Suche nach Bedrohungen ausschließlich auf Use Cases setzen. Damit lassen sich allerdings nur Bedrohungen identifizieren, nach denen auch explizit gesucht wird; neue und komplexe Angriffsmuster fallen hingegen unentdeckt durchs Raster.

r-tec verbindet Next-Generation-SIEM-System mit manueller Analyse

Um ein hohes Sicherheitsniveau zu erreichen, benötigen Unternehmen stattdessen mehrstufige Angriffserkennungssysteme, die verschiedene Präventionsmethoden miteinander kombinieren. Wie eine effektive Angriffserkennung aussieht, zeigt der Managed Detection and Response Service (MDR) der r-tec IT Security GmbH. Dieser vereint modernste Technik mit dem Know-how erfahrener IT-Sicherheitsexperten.

Dabei kommt ein Next-Generation-SIEM-System zum Einsatz, das nicht mit einem starren Regelwerk, sondern mit einer verhaltensbasierten Anomalieerkennung arbeitet. Mittels Machine Learning lernt das System das Verhalten von Nutzern und Geräten im Unternehmensnetzwerk kennen und leitet aus den gewonnenen Erkenntnissen ein Normalverhalten ab. Auch das Verhalten von Gruppen und Beziehungen innerhalb des Netzwerks kann überprüft werden. Das heißt, die technischen Komponenten analysieren nicht nur einzelne Logquellen oder verknüpfte Events, sondern das Gesamtverhalten des jeweiligen Unternehmens. Anschließend können Abweichungen und somit auch bis dahin unbekannte Angriffsmuster zuverlässig identifiziert werden.

Verhaltensbasierte Umgebungsprüfung versus Use-Case-Einsatz

Unternehmen profitieren außerdem von einer enormen Zeitersparnis. „Im Vergleich zu herkömmlichen SIEM-Systemen verursacht das von uns eingesetzte Next Generation SIEM nur einen minimalen Einrichtungsaufwand, da Use Cases und Regelwerke nicht händisch an das jeweilige Unternehmen angepasst werden müssen", erklärt r-tec-Geschäftsführer Dr. Stefan Rummenhöller. „Stattdessen erlernt unser Next-Generation-SIEM-System im Rahmen einer sechs- bis achtwöchigen Anlernphase automatisch den Normalzustand." Alle dafür benötigten Daten werden mithilfe von Site-Kollektoren aus den Logquellen des Kunden gesammelt und verschlüsselt in eine Cloud übertragen.

„Da immer wieder neue Angriffsmuster in der IT-Welt auftauchen, müssen herkömmliche SIEM-Lösungen ständig mit Use Cases gefüttert werden", gibt Stefan Rummenhöller zu bedenken. „Dies führt wiederum zu einem Anstieg der Alarme und Fehlermeldungen, die Unternehmensmitarbeiter analysieren, einstufen und bearbeiten müssen. Ab einem bestimmten Zeitpunkt ist die Masse an Meldungen allerdings kaum noch händelbar." Beim Einsatz eines Next-Generation-SIEM-Systems sei das regelmäßige Einpflegen von Use Cases aufgrund der verhaltensbasierten Umgebungsüberprüfung nicht mehr notwendig. „Daher bietet diese moderne Form der Angriffserkennung Unternehmen die Möglichkeit, Ressourcen und Kosten zu sparen."

Dr. Stefan Rummenhöller

Fachkundige Experten beurteilen Anomalien

Werden Anomalien erkannt, leitet das System diese an das r-tec-MDR-Expertenteam weiter, das die betreffenden Events manuell untersucht und klassifiziert. „Eine vollständig autonome Angriffserkennung, die in erforderlichem Maße auf einen Angriff reagieren kann, gibt es derzeit nicht", erläutert Rummenhöller. „Selbst wenn ein Unternehmen über die beste technische Lösung verfügt, sollte auf eine Qualifizierung durch sachkundige Spezialisten nicht verzichtet werden."

Identifizieren die Experten einen Security Incident, bestimmen sie im nächsten Schritt dessen Kritikalität. Besteht ein hohes Risiko, werden anschließend alle relevanten Personen über den Vorfall informiert, sodass schnellstens geeignete Maßnahmen ergriffen werden können.

Durch die Kombination aus technischer Lösung und manueller Expertenanalyse gelingt es r-tec letztlich, auch neue Angriffsversuche aufzudecken, die von herkömmlichen IT-Security-Komponenten nicht erkannt werden können.

Da Managed Detection and Response als Full-Managed-Service angeboten wird, entsteht für Kunden bei der Angriffserkennung nur ein geringer Aufwand. r-tec übernimmt von der Implementierung der technischen Komponenten über die Anomaliequalifizierung bis hin zur Erstellung von Maßnahmenempfehlungen alle anfallenden Aufgaben.

Incident Response Service hilft bei der Angriffsbewältigung

Auch im Angriffsfall können sich Unternehmen auf das r-tec-Team verlassen. Im MDR-Service ist nämlich ein Incident Response Service inbegriffen. Das heißt, auf Wunsch unterstützen die Experten ihre Kunden außerdem bei der Angriffsbewältigung. Sie kümmern sich unter anderem um die Eindämmung von Attacken sowie um die Wiederherstellung des Normalzustandes im jeweiligen Betrieb. „Unser MDR-Team informiert nach der Identifikation eines Angriffs sofort das Incident-Response-Team, das innerhalb garantierter Reaktionszeiten zur Verfügung steht", erklärt der r-tec-Geschäftsführer. „Möchten unsere Kunden diesen Service in Anspruch nehmen, definieren wir bereits bei der Implementierung gemeinsam sinnvolle Meldewege und legen fest, wie im Angriffsfall agiert werden soll. So können wir bei Bedarf schnell reagieren."

In Kombination mit dem Incident Response Service stellt Managed Detection and Response eine umfassende Lösung dar, mit deren Hilfe das Wuppertaler Unternehmen seine Kunden in jeder Phase eines Angriffs unterstützt. Kunden erhalten somit alle MDR-Leistungen aus einer Hand.

MDR-Service für aktuelle und zukünftige Herausforderungen

Da die Lösung komplett aus der Cloud betrieben wird, lässt sich die Angriffserkennung zudem ganz unkompliziert an die individuellen Bedürfnisse des jeweiligen Unternehmens anpassen. Falls nötig, können zusätzliche Produkte aus der Cloud hinzugebucht werden. Auf diese Weise lässt sich das System in Zukunft kostengünstig auf neue Entwicklungen einstellen. Betrieben wird der Cloud-Service in einem DS-GVO-konformen Rechenzentrum.

„Wir sorgen dafür, dass Unternehmen für den Ernstfall gerüstet sind – und es in Zukunft auch bleiben", verspricht Stefan Rummenhöller. „Da unser MDR-Team sämtliche IT-Sicherheitsherausforderungen löst, können sich unsere Kunden ohne Ablenkung um ihr Kerngeschäft kümmern. Um die Konsequenzen einer möglichen Attacke müssen sie sich keine Sorgen machen." ■

Weitere Informationen zum r-tec-MDR-Service finden Sie im Internet unter
www.r-tec.net/mdr

Mehr dazu hier

r-tec cyber security

IT-SICHERHEIT
Mittelstandsmagazin für Informationssicherheit und Datenschutz

Thapana_Studio - stock.adobe.com

Besuchen Sie uns!

auf der it-sa 2022

Halle 6 **Stand Nr. 6-101**

Software Bill of Materials

REZEPTUR FÜR MEHR CODE-SICHERHEIT

IT-Sicherheit beginnt auf Codeebene. Um die Software-Supply-Chain transparenter und Anwendungen sicherer zu machen, müssen Entwickler bei der Verwendung von Open-Source-Software-(OSS-)Komponenten genau Buch führen. Gut, dass mit der Software Bill of Materials (SBOM) dafür bereits ein Template bereitsteht.

Bild: Ratul Ghosh/Unsplash

Bei der Software-Entwicklung ist es ein bisschen wie beim Kochen: Verschiedene Codezeilen und Komponenten werden miteinander vermischt, bis am Ende eine neue Anwendung entsteht. Die richtige Rezeptur ist entscheidend – nicht nur für die Performance, sondern auch für die Sicherheit. Immerhin stammen die Zutaten aus verschiedenen Quellen, enthalten versteckte „Zusatzstoffe", oder gelten als „hoch verarbeitete Lebensmittel". Von Informationen über „Herkunftsland", „biologischer Anbau" und „Fairtrade" ganz zu schweigen. In der Lebensmittelindustrie gibt es immer wieder Versuche, die Kennzeichnung auf Verpackungen zu verbessern und Lieferketten rückverfolgbar zu machen. Wie steht es aber um die Sicherheit und Transparenz im Software-Code?

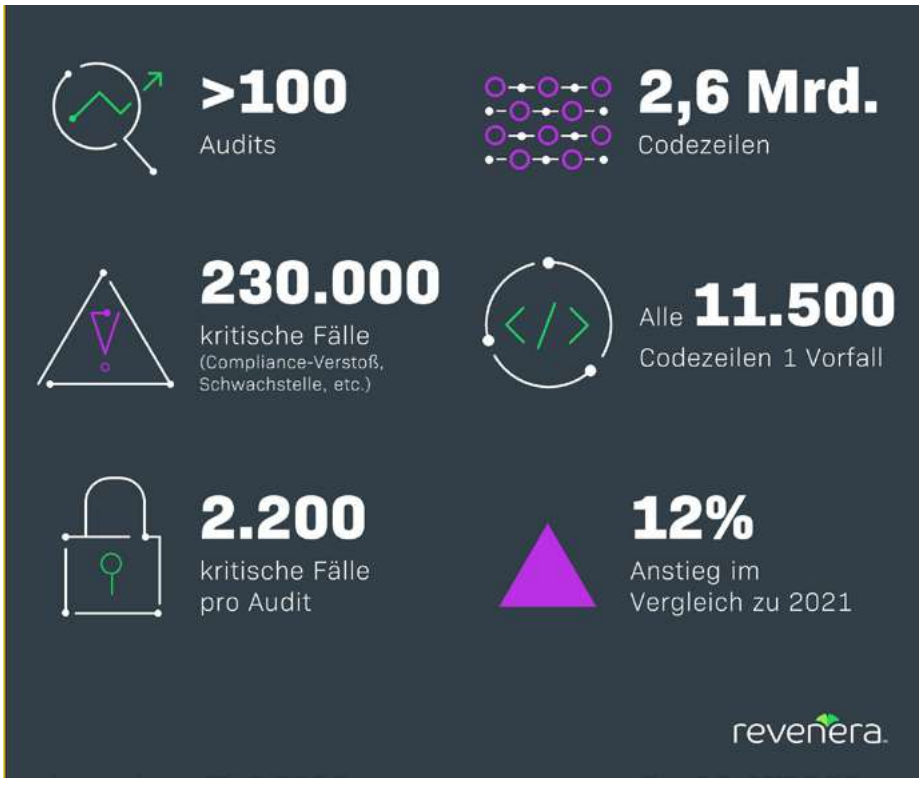
SICHERHEITSRISIKO VON OPEN SOURCE SOFTWARE (OSS)

Wäre Software ein Rezept, stände Open Source ganz oben auf der Einkaufsliste. Open-Source-Software-(OSS-)Komponenten machen bis zu 80 Prozent des Codes in kommerziellen Anwendungen aus. Kaum ein Entwicklerteam, das nicht auf bestehende Komponenten zurückgreift, um schneller und effektiver zu arbeiten. Dabei bleibt die Dokumentation der Bausteine leider oft außen vor. Finden sich dann zu einem späteren Zeitpunkt Schwachstellen oder Lizenzverstöße, lässt sich nur sehr schwer zurückverfolgen, wo und wie der betroffene Code in die Software Supply Chain gelangt ist und welche Anwendungen betroffen sind.

Unternehmen fehlt es an Transparenz: Im Rahmen von Software-Audits wertete Revenera mehr als 2,6 Milliarden Codezeilen aus und entdeckte dabei insgesamt 230.000 kritische Fälle. Im Durchschnitt stießen die Analysten alle 11.500 Codezeilen auf einen Compliance-Verstoß, eine Sicherheitsschwachstelle oder Ähnliches. Das eigentlich Fatale: 83 Prozent der in den Audits aufgedeckten Risiken war den Unternehmen im Vorfeld der Untersuchung nicht bekannt. Oder um beim Vergleich zu bleiben: Vielen wurde ein Gericht vorgesetzt, von dem nicht einmal der Koch den Großteil seiner Zutaten kannte.

SBOM: STÜCKLISTE FÜR DIE SOFTWARE-INDUSTRIE

In den letzten Jahren hat sich die Softwarebranche daher gezwungenermaßen mit der Verbesserung der Open-Source-Governance auseinandergesetzt. Im Mittelpunkt vieler Compliance-Programme steht dabei die Software Bill of Materials (SBOM). Die SBOM bezeichnet die vollständige Dokumentation aller in einer Software eingesetzten Code-Komponenten einschließlich Lizenzierung, Versionen und Herkunft. Dabei geht es nicht nur darum, die einzelnen Komponenten zu kennen, sondern auch deren Zusammensetzung – angefangen bei Paketen und Abhängigkeiten über Binärdateien ohne Manifest-Dateien, Multimedia-Dateien, Bilder/Icons, Codecs und Copy/Paste-Codes bis hin zu den von Entwicklern genutzten Source Libraries und Drittanbieter-Bibliotheken.



Grafik aus dem Open Source Report 2022 (Quelle: Revenera)

SICHERHEIT ALS WETTBEWERBSFAKTOR

Software-Anbieter, denen ein solcher Einblick in den eigenen, intern entwickelten Code fehlt, müssen über kurz oder lang mit fehlendem Kundenvertrauen sowie Wettbewerbsnachteilen rechnen. Schon jetzt pochen viele Unternehmen beim Kauf von Softwareprodukten auf die Offenlegung des Codes. Oft wird die SBOM sogar als Teil der Service-Level-Verträge (SLAs) vertraglich festgesetzt. Wer als Anbieter mit der US-Regierung Geschäfte machen will, muss seit Mai 2021 eine Software-BOM für jedes Produkt bereitstellen. Die EU-Kommission geht mit ihrer Open-Source-Software-Strategie 2020–2023 in eine ähnliche Richtung. Und auch einflussreiche Branchenverbände und Behörden, wie die FDA (The Food and Drug Administration) in den USA sowie die GENIVI Alliance und die Automotive Grade Linux (AGL), machen sich für die SBOM stark.

Angetrieben wird diese Entwicklung vor allem durch die Flut von Cyberattacken, bei denen Angreifer versuchen, über die Codeebene Systeme zu infiltrieren. Open-Source-basierte Schwachstellen wie Log4Shell haben eindrücklich verdeutlicht, dass Softwarelieferketten geschützt und überwacht sein wollen. So hatten allein im letzten Jahr fast zwei Drittel (64 Prozent) der Unternehmen mit Angriffen auf die Softwarelieferkette zu kämpfen.

VIER BEST PRACTICES BEI DER SBOM-ERSTELLUNG

Die gute Nachricht: Das Framework rund um die automatisierte und kollaborative Erstellung der Software-BOM verbessert sich zunehmend. Eine wichtige Anlaufstelle ist zum Beispiel das ISO-zertifiziert OpenChain-Project. Anerkannte

Standardformate (zum Beispiel SPDX, CycloneDX, SWID) helfen Entwicklern darüber hinaus, Informationen einheitlich zu dokumentieren und zu teilen. Darüber hinaus sollten Unternehmen einige grundlegende Best Practices in den Erstellungsprozess von SBOM implementieren.

1. Automatisierung und Zusammenarbeit

Ein zentrales Kriterium der SBOM ist ihre Aufbereitung. Der Datensatz sollte nicht nur formal und abfragbar, sondern auch maschinenlesbar sein. Der Grund: Nur so lässt sich die nötige Automatisierung beim Erstellen sowie beim Durchsuchen einer SBOM realisieren. Softwareprodukte sind komplex und legen mit jeder neuen Version und jedem neuen Update an Code-Umfang zu. Wer sich hier manuell an das Auflisten von Code-Fragmenten und Abhängigkeiten macht, läuft nicht nur Gefahr, kontinuierlich einen Schritt hinter dem aktuellen Entwicklungsstand der Anwendung zu bleiben. Es passieren auch Fehler.

Entwicklerteams mangelt es schlichtweg an Ressourcen. Zudem fehlt es oft an spezifischem Wissen, was die Open Source-Lizenzierung und sichere Codierungsverfahren angeht. Entwickler sind zudem nicht im Alleingang für die Software-BOM verantwortlich. Im Gegenteil, die Software-BOM setzt die Mitarbeit von Rechtsexperten, Produktmanagern und Sicherheitsteams voraus. Automatisierte Software Composition Analysis-Tools unterstützen diesen kollaborativen Ansatz, scannen den Code, gleichen die gefundenen Komponenten mit externen Quellen (zum Beispiel Open-Source-Wissensdatenbanken) ab und erstellen eine detaillierte Auflistung für alle Stakeholder.

2. Kontinuierliche Überprüfung und Aktualisierung

Selbst bei vollständiger Automatisierung braucht die Erstellung einer SBOM Zeit. Die Aktualisierung der Software-Stückliste wird daher von den wenigsten Anbietern täglich durchgeführt, sondern erfolgt in regelmäßigen Abständen und/oder zu bestimmten Anlässen (zum Beispiel Veröffentlichung einer Schwachstelle, neues Release). Wie häufig es zu SBOM-Updates kommt, hängt sowohl von der Anwendung selbst, als auch vom Unternehmen ab. Wichtige Faktoren sind unter anderem die Anzahl der Releases, die Größe des IT-Portfolios, die vorhandenen Ressourcen sowie die SBOM-Expertise. Auch mit dem Kunden vertraglich vereinbarte Services sowie Compliance-Richtlinien sind entscheidend.

SBOM Kreislauf (Quelle: Revenera)

Wie oft auch immer Unternehmen ihre Software-Stücklisten aktualisieren, in jedem Fall heißt es, klare Prozesse und Best Practices bezüglich der Rollenverteilung und der Terminierung zu definieren und zu implementieren. Die SBOM sollte dabei weniger als Ad-hoc-Instrument verstanden werden, sondern als fester Bestandteil der Entwicklungsarbeit bzw. der IT-Sicherheit.

3. Zentralisierte Teams: OSPO und OSRB

Um ein entsprechendes, SBOM-konformes Framework aufzustellen, braucht es dezidierte Teams in Unternehmen. Im sogenannten Open Source Program Office (OSPO) beispielsweise arbeiten Vertreter aus den Bereichen Recht, Technik, Produkt und Sicherheit zusammen, um ganzheitliche Strategien intern zu implementieren (Inbound-Use-Case) und Code innerhalb von Open-Source-Projekten in die Community einzubringen (Outbound-Use-Case).

Die Aufgabe von Open Source Review Boards (OSRB) besteht darin, diese Prozesse kontinuierlich zu verfeinern. Gemeinsam mit dem Entwicklungsteam wird daran gearbeitet, die Nutzung von Open Source und Drittanbieter-Code zu dokumentieren und zu überwachen. Auch hier sollten idealerweise Stakeholder aus den jeweiligen Rechts-, Entwicklungs-, Sicherheits-, IT- und Führungsteams zusammenkommen.

4. Integration in die Threat Intelligence

Die Software-BOM versteht sich als Sicherheitsinstrument und sollte dementsprechend in die unternehmensübergreifende IT-Sicherheit integriert werden. Das gilt insbesondere für die Threat Intelligence. Bekanntgewordene Schwachstellen, geleakte Code-Fragmente und im Darknet angebotene Exploits stellen unmittelbare Bedrohungen für Anwendungen dar. Software-Anbieter müssen im Ernstfall in der Lage sein, das Risiko für ihre eigenen Produkte einzuschätzen. Die SBOM liefert hier die Informationsgrundlage für einen schnellen Abgleich. Sind Anwendungen betroffen, schlagen die Systeme automatisch Alarm und helfen in der Regel auch, Maßnahmen zur Mitigation (zum Beispiel Patches) zu priorisieren und durchzuführen. Gleichzeitig können Software-Anbieter ihre Kunden informieren und besorgte Anfragen bezüglich möglicher Sicherheitsrisiken souverän beantworten. ■

NICOLE SEGERER,
VP of Product Management & Marketing, Revenera
(Foto: Nicole Segerer)

Phishing gefährdet Unternehmen in Deutschland

ES KOMMT AUF DIE MENSCHLICHE FIREWALL AN

Phishing ist zu einer enormen Bedrohung für die deutsche Wirtschaft geworden. Wer seine Mitarbeiter nachhaltig vor den Risiken gefälschter E-Mails schützen will, braucht eine IT-Sicherheitsstrategie, welche die drei zentralen Bausteine einer Sicherheitskultur integriert: Mindset – Skillset – Toolset.

Nach einer Studie des Bitkom-Digitalverbands nutzt ein Großteil der Cyberkriminellen den „Faktor Mensch" als vermeintlich schwächstes Glied der Sicherheitskette aus.[1] Immer häufiger werden die Social-Engineering-Angriffe, die auf die Manipulation der Beschäftigten zielen, von hochprofessionellen Betrügerbanden ausgeführt. Sie geben sich in raffiniert gefälschten E-Mails als Vorgesetzte, Kollegen oder Geschäftspartner aus, um die Mitarbeiter zur Preisgabe vertraulicher Daten, zu Klicks auf schädliche Links und Dateianhänge oder zu Überweisungen auf falsche Konten zu verleiten. Nicht selten dient ein geglückter (Spear)-Phishing-Angriff für die Cyberkriminellen als Auftakt, um in das gesamte Unternehmensnetzwerk einzudringen.

Mit einer IT-Sicherheitskultur, die dem Dreiklang „Mindset – Skillset – Toolset" folgt, können Unternehmen einen nachhaltigen Schutzwall gegen die immer ausgeklügelteren Phishing-methoden errichten. Ganz oben auf der Agenda sollte eine grundlegende Verhaltensänderung der Mitarbeiter stehen.

MINDSET: MITARBEITER ZUM UMDENKEN MOTIVIEREN

So meinen viele Beschäftigte noch immer, sich blind auf die IT-Sicherheitstechnik verlassen zu können, und klicken empfangene E-Mails bedenkenlos an. Doch Vorsicht: Obwohl es den IT-Abteilungen heute gelingt, täglich Millionen betrügerischer Mails abzufangen, landen doch etliche im Posteingang von Mitarbeitern. Daher müssen die Nutzer erkennen, wie wichtig ihre Rolle als menschliche Firewall ist.

Dies geschieht am wirksamsten im Rahmen gezielter Informationskampagnen, die vom Management, den Führungskräften und IT-Sicherheitsverantwortlichen getragen und über unterschiedliche Kanäle verbreitet werden: zum Beispiel in Team-Meetings, Videos und Rundmails. Dabei sollten die Mitarbeiter anhand konkreter Zahlen und Fakten sowie bekanntgewordener Sicherheitsvorfälle in der eigenen Branche ein Bewusstsein für die Gefahren von Phishingangriffen entwickeln. So verlor zum Beispiel der österreichisch-chinesische Maschinenbauer FACC rund 43 Millionen Euro, als die Buchhaltung auf mehrere gefälschte E-Mails des angeblichen Firmenchefs hereinfiel und wiederholte Überweisungen auf ausländische Konten vornahm.

Um solche Horrorszenarien zu vermeiden, sollten die Unternehmen eindringlich an die Eigenverantwortung und Selbstwirksamkeit der Beschäftigten appellieren. Sie dürfen keinesfalls Angst vor Spear Phishing entwickeln, sondern müssen lernen, dass ihr Einsatz und ihre Aufmerksamkeit mitentscheidend für das Funktionieren des gesamten Unternehmens sind. Dies betrifft auch die achtsame Nutzung von Social-Media-Kanälen, wie eine Studie der Technischen Universität (TU) Darmstadt und IT-Seal zeigt.[2] Danach nutzen Cyberkriminelle verstärkt persönliche Daten, die die Mitarbeiter in den sozialen Netzwerken zugänglich machen, zum Aufbau gezielter Spear-Phishing-Mails. Ziel der Informationskampagne ist es, das richtige Mindset zu schaffen und die Mitarbeiter so auf die folgenden Security-Awareness-Trainings vorzubereiten.

SKILLSET: SCHNELLE ENTSCHEIDUNGEN FÖRDERN

Awareness-Trainings entfalten dann ihre größte Wirkung, wenn sie theoretische Präsenzschulungen, E-Learnings und Webinare mit praxisnahen Spear-Phishing-Simulationen kombinieren. Diese verwenden echte Unternehmens- und Mitarbeiterinformationen, um reale Angriffe nachzustellen. Doch statt am Haken der Betrüger landet der Mitarbeiter auf einer interaktiven Erklärseite, wo er Hinweise auf die Merkmale der gefälschten E-Mail erhält: von Buchstabendrehern in der Adresszeile über Fake-Subdomains bis hin zu zweifelhaften Links.

Simulierte Spear-Phishing-Angriffe nutzen den „Most teachable Moment" eines Mitarbeiters, indem sie ihn im richtigen Moment über sein potenziell schadhaftes Verhalten aufklären. Das stärkt sein schnelles, intuitives Entscheidungsvermögen und bewirkt, dass er künftig vorsichtiger mit eingehenden E-Mails umgeht. Um einen nachhaltigen Lerneffekt zu erzielen, sollten die Spear-Phishing-Simulationen kontinuierlich wiederholt und an die aktuellen Angreifermethoden angepasst werden.

Zudem hat es sich als vorteilhaft erwiesen, dass die simulierten Phishingattacken am individuellen Schulungsbedarf der Mitarbeiter ausgerichtet werden und eine kennzahlenbasierte Dokumentation der Lernfortschritte erlauben. Diese Kennzahlen dienen der Ermittlung des Sicherheitsbewusstseins der Mitarbeiter und können sich beispielsweise danach richten, wie die Mitarbeiter auf Phishing-Simulationen verschiedener Schwierigkeitsgrade reagieren. Die Unternehmen können damit jederzeit feststellen, wo Defizite und Handlungsbedarfe bestehen und weitere Schulungsmaßnahmen abgeleitet werden sollten.

TOOLSET: INNOVATIVE SICHERHEITSTECHNIK NUTZEN

Wer den Phishing-Angreifern noch deutlicher Paroli bieten möchte, sollte ergänzend auf geeignete IT-Sicherheitswerkzeuge setzen – neben 2- oder Multi-Faktor-Authentifizierung (2FA/MFA) bieten sich Password Manager an, die einfach zu integrieren sind und eine zentrale Speicherung und Verwaltung digitaler Identitäten erlauben. Damit lässt sich verhindern, dass die Mitarbeiterinnen und Mitarbeiter aus Bequemlichkeit immer die gleichen Log-in-Daten für alle wichtigen Konten wählen. Gelingt es Spear-Phishing-Angreifern, ein bestimmtes Passwort zu stehlen, stehen ihnen nicht mehr automatisch alle anderen Nutzerkonten offen, wenn ein Password Manager im Einsatz ist.

Einen weiteren Schutz vor Spear-Phishing-Betrügern können spezielle Tools zur Erkennung und Meldung zweifelhafter E-Mails bieten. Ein Beispiel bieten sogenannte Reporter Buttons, die direkt in Microsoft Outlook integrierbar sind. Erhalten Nutzer eine verdächtige E-Mail, lässt sich damit per Knopfdruck prüfen, ob diese auch tatsächlich das Werk von Betrügern ist. Sind sich die Mitarbeiter dann immer noch unsicher, können sie diese E-Mail per zweitem Knopfdruck zur Analyse an die IT-Sicherheitsverantwortlichen weiterleiten. Wird die E-Mail dann tatsächlich als gefälscht identifiziert, wird sie unverzüglich gesperrt. Das reduziert die Gefahrenquellen, während die IT-Sicherheitsverantwortlichen einen fundierten und fast tagesaktuellen Überblick über die Phishing-Bedrohungslage im Unternehmen erhalten.

FAZIT

Mindset – Skillset – Toolset: Mit dieser Kombination aus didaktischen, organisatorischen und technischen Maßnahmen können die Unternehmen ein Bollwerk gegen die wachsenden (Spear)-Phishing-Gefahren errichten. Sie setzen bei einer der größten Schwachstellen in der Sicherheit eines Unternehmens – den Mitarbeiterinnen und Mitarbeitern – an und nutzen ergänzende IT-Sicherheitstechnik. ■

Quellen

[1] *Bitkom: „Wirtschaftsschutz 2021", 5. August 2021*

[2] *Anjuli Franz und Evgheni Croitor, Technische Universität (TU) Darmstadt: „Who bites the Hook? Investigating Employees' Susceptibility to Phishing: A randomized Field Experiment", 2021*

DAVID KELM,
Mitgründer und Geschäftsführer der IT-Seal GmbH

Endpunkthärtung und -absicherung in einer sich verändernden Bedrohungslandschaft

WAS AUF DIE GERÄTELAND-SCHAFT ZUKOMMT

Es ist unmöglich, über die Cyber-Bedrohungslandschaft zu sprechen, ohne auf geopolitische Situationen einzugehen. Das bringt ein großes Maß an Ungewissheit mit sich, welche die aktuellen Ereignisse begleitet. Es ist unklar, wie lange die derzeitigen Umstände andauern werden oder welche dauerhaften Auswirkungen eine komplizierte geopolitische Situation haben kann. Klar ist aber: Es wird neue Gefahren geben. Und: Unternehmen sollten sich darauf vorbereiten.

Viele Entwickler von Sicherheitslösungen haben es sich zum Ziel gesetzt, mit den wichtigsten Trends Schritt zu halten und verwertbare Informationen zu gewinnen. Nach aktuellen Erkenntnissen zeichnet sich eine Reihe von Trends in der Cyber-Bedrohungslandschaft ab.

Möglicher Anstieg von Ransomware-Angriffen inmitten wirtschaftlicher Instabilität:
Da die EU als primäre Reaktion auf Russlands Einmarsch schwere Sanktionen gegen russische Interessen verhängt haben, könnte die daraus resultierende wirtschaftliche Instabilität zu mehr Ransomware-Angriffen auf Organisationen innerhalb der EU führen. Das FBI hat Russland als „freizügiges Umfeld für Cyberkriminelle" bezeichnet und davor gewarnt, dass es zu einer „möglichen Zunahme von Cyberbedrohungen" durch Hacker kommen könnte, die mit Unterstützung Russlands operieren.

Aufkommen neuer zerstörerischer Malware:
In einem kürzlich erschienenen Artikel von *Deep Instinct* heißt es, dass die russischen Cyberaktivitäten in den Wochen vor der Invasion darauf abzielten, „Chaos zu stiften und die Kommunikation innerhalb der ukrainischen Regierung und der militärischen Institutionen zu stören". Dazu gehörte auch der Einsatz einer neuen Malware namens HermeticWiper, die Festplatten löscht (zusammen mit weitverbreiteten DDoS-Angriffen und Webdefacements). In den darauffolgenden Wochen sind mindestens zwei neue zerstörerische Malware-Familien aus dem Konflikt hervorgegangen, die von neuartigen Infektionsvektoren und unterstützender Malware begleitet werden, welche die erfolgreiche Auslieferung der zerstörerischen Payloads sicherstellen sollen.

Phishing und andere Betrugsmaschen nutzen den Konflikt aus:
Wie bei allen öffentlichkeitswirksamen Ereignissen in der Welt (einschließlich Cyberangriffen) nutzen Bedrohungsakteure schnell die verfügbaren Informationen und die öffentliche Unsicherheit, um überzeugende Phishing-Köder und Social-Engineering-Kampagnen zu entwi-

ckeln. Die Motive solcher Kampagnen variieren zwischen Spionage, Diebstahl von Zugangsdaten und Finanzbetrug.

Potenzieller „Spillover" von Cyberaktivitäten, die EU-Ziele betreffen:
Die Cybersecurity and Infrastructure Security Agency (CISA) und andere multinationale Cyberagenturen haben wiederholt ihre Besorgnis darüber geäußert, dass sich die in Russland und der Ukraine beobachteten Cyberaktivitäten über die Konfliktzone hinaus ausbreiten und Organisationen in den USA, der EU oder westlichen Gebieten beeinträchtigen könnten.

Die Beteiligung von Hacktivisten erhöht das Risiko:
Hacktivistische Handlungen in geopolitischen Konflikten laufen Gefahr, von beiden Seiten falsch zugeordnet zu werden, als staatlich geförderte, feindliche Aktivitäten interpretiert zu werden und die Spannungen ungewollt zu verschärfen. Hacktivismus (auch wenn er noch so gut gemeint ist) kann die kinetischen Aktivitäten auf dem Schlachtfeld eskalieren lassen und die Risiken im Cyberspace erhöhen – eine Tatsache, die Menschenleben fordern, kritische Infrastrukturen zerstören oder zu Vergeltungsmaßnahmen führen kann, die sich gegen diejenigen Nationen richten, von deren Staatsgebiet die Angriffe ausgehen. Ein aktuelles Beispiel, das dieses Phänomen verdeutlicht, ist das Bekanntwerden von Conti-Daten (einschließlich des Quellcodes). Diese wurden von einem ukrainischen Hacktivisten aus der Ransomware-Gruppe gestohlen – als Reaktion auf Contis öffentliches Versprechen, Russland in dem Konflikt zu unterstützen. Der Code von Ransomware ist schon früher durchgesickert, wie zum Beispiel bei der Babuk-Ransomware, und hat zur Wiederverwendung und Modifizierung der Ransomware durch neue Bedrohungsakteure geführt. Dies ist auch hier ein echtes Risiko.

Auch wenn vieles des bisher gesagten mit den Cyberauswirkungen eines bestimmten geopolitischen Konflikts zusammenhängt, prognostizieren Experten mehrere Gefahren, die sich schon bald auf die Cyberbedrohungslandschaft auswirken werden. Einige davon haben bereits begonnen, sich bemerkbar zu machen. Organisationen sollten sich auf Folgendes einstellen:

- anhaltende Beeinflussungskampagnen und Versuche von staatlich unterstützten Akteuren, sichere Kommunikationskanäle auszuschalten, auf die sich die Öffentlichkeit für eine zuverlässige Kommunikation verlässt
- kritische Infrastrukturen im Visier von Angriffen
- steigende Kraftstoff-/Energiepreise, wirtschaftliche Instabilität und Cyberversicherungen, die weniger abdecken und mehr verlangen
- vermehrte Angriffe auf Open-Source-Bibliotheken und -Pakete sowie andere Technologien, die in Lieferketten enthalten sind
- Ransomware:
  - zunehmende Ransomware-Aktivitäten, wobei der Schwerpunkt wieder auf Verbrauchern, KMU und mittelständischen Unternehmen liegt
  - zunehmende Konzentration von Cyberkriminellen (mit Ransomware und BEC an der Spitze) auf SaaS- und Cloud-Technologie
  - Die Veröffentlichung des Conti-Quellcodes könnte zu neuen Varianten führen, die von neuen Akteuren genutzt werden, wie es bei der Veröffentlichung des Codes der Babuk-Ransomware der Fall war.
  - Entstehen neuer, lose verbundener Hackergruppen, wie im Russland/Ukraine-Krieg beobachtet
- das wahrscheinliche „Durchsickern" von Malware, die in Konflikten eingesetzt wird, in die Hände von Cyberkriminellen, die sie nach eigenem Gutdünken verändern und umfunktionieren können – und umgekehrt
- Zunahme von mehrgleisigen Cyberangriffen, wie zum Beispiel Ransomware-Angriffe in Kombination mit Beeinflussungskampagnen, DDoS, zerstörerische Malware, Operationen unter falscher Flagge etc.

In dieser sich schnell verändernden Landschaft ist das, was Sicherheitsverantwortliche heute tun, entscheidend für die Bereitschaft und Reaktionsfähigkeit im Fall eines Cyberangriffs. Branchenunabhängig sollten alle Unternehmen ihre IT-Infrastruktur so ausstatten, dass das Risiko und die Angriffsfläche reduziert werden.

WARUM ENDPUNKTHÄRTUNG UND -VORBEREITUNG SO WICHTIG SIND

Der beste Zeitpunkt, um Asset-Management und Patching-Workflows einzurichten, war gestern. Der zweitbeste Zeitpunkt ist heute. Während sich viele Angreifer derzeit auf Systeme in Ländern konzentrieren, die in einen aktiven militärischen Konflikt verwickelt sind, haben Forscher und Spezialisten für Bedrohungsdaten auf einen wahrscheinlichen Anstieg der Cyberkriminalität hingewiesen, da die Auswirkungen von Sanktionen im Zusammenhang mit diesen Konflikten zu wirtschaftlicher Unsicherheit in verschiedenen Teilen der Welt führen. Unternehmen sollten diese Zeit unbedingt nutzen, um Lücken in der Patch-Verwaltung für Betriebssysteme und Tools von Drittanbietern zu schließen und ihre Richtlinien zu optimieren, um Ihre Angriffsfläche zu verringern.

Höchste Priorität haben die Beseitigung von Abdeckungs- und Sichtbarkeitslücken, die Behebung von Patch-Fehlern und die Aktualisierung von Drittanbieter-Software. Die aktuelle Bedrohungslandschaft toleriert keine Endgeräte, die länger als 30 Tage nicht upgedatet wurden. Sicherheitsverantwortliche sollten diese Gelegenheit nutzen, um alle Systeme, einschließlich Server und Workstations, auf den neuesten Stand der Betriebssystem-Patches und der Software von Drittanbietern zu bringen.

In der unmittelbaren Zukunft sollte den folgenden Maßnahmen Vorrang eingeräumt werden:

- Beantragung einer Notfall-Änderungsgenehmigung, um verpasste Patches schnellstmöglich aufzuspielen
- Einsatz einer Patch-Management-Lösung oder Behebung von Patch-Fehlern
- Patches für das Betriebssystem aufspielen
- Aktualisieren der Software von Drittanbietern
- Entfernung von nicht autorisierter, inaktiver oder nicht unterstützter Software
- Anwendung von Richtlinien zur Reduzierung der Angriffsfläche
- Sicherstellen, dass Pläne zur Reaktion auf Vorfälle von den genutzten Tools unterstützt werden
- Warnungen und Anweisungen des BSI beachten und unverzüglich umsetzen ■

ZAC WARREN,
Senior Director Cybersecurity Advisory EMEA bei Tanium

Datenschutz im Unternehmen

ALLER GUTEN DINGE SIND DREI

IT-Sicherheit ist untrennbar mit dem Thema Datenschutz verbunden: Daten aller Art sind mittlerweile die Basis von Prozessen und Entscheidungen in Unternehmen. Zum Schutz personenbezogener Daten gilt es zudem, die Prozesse konform zur DS-GVO zu gestalten. Viele kleine und mittlere Unternehmen zeigen in beiden Bereichen noch Nachholbedarf. Sie sollten drei Dinge beachten, um den Datenschutz im eigenen Unternehmen zu stärken.

Besonders kleine und mittlere Unternehmen (KMU) stehen oft vor dem Problem, dass ihnen das notwendige Fachwissen zu Datenschutz- und IT-Sicherheitsthemen fehlt oder Fachpersonal nur schwer am Arbeitsmarkt zu bekommen ist. Zur Unterstützung können sie auf unabhängige Berater und externe Datenschutzbeauftragte zurückgreifen. Aber auch Unternehmen selbst können Einiges tun, um eine gute Basis für Datenschutz und IT-Sicherheit zu schaffen. Sie beruht auf drei Elementen: Menschen, Prozessen und Technologie.

MITARBEITENDE WEITERBILDEN

Der erste Schritt, um das Thema Datenschutz im eigenen Unternehmen voranzutreiben, ist eine entsprechende Sensibilisierung der eigenen Mitarbeitenden. Sie müssen geschult werden, damit sie sich darüber im Klaren sind, was personenbezogene Daten sind und wie mit diesen umgegangen werden muss. Es sollte auch klar sein, welche Strafen bei Missachtung der DS-GVO drohen. Datenschutz muss zu einem festen Bestandteil der Unternehmenskultur werden. Besonders dort, wo vermehrt mobiles Arbeiten zum Berufsalltag zählt, gilt, dass die Belegschaft ausreichend für Datenschutz und IT-Sicherheit sensibilisiert sein muss. Die Angriffsmöglichkeiten auf sensible Unternehmensdaten sind durch das Homeoffice deutlich gewachsen.

Unternehmen ab einer gewissen Größe müssen einen Datenschutzbeauftragten benennen, der sowohl intern als auch extern gegenüber Behörden als Ansprechpartner dient. Dabei muss es sich allerdings nicht zwingend um ein Mitglied der eigenen Organisation handeln, auch Externe können diese Aufgabe übernehmen. So bieten unabhängige Prüforganisation den Unternehmen nicht nur ausführliche Schulungen für ihre Belegschaft an, sondern stellen auch externe Datenschutzbeauftragte.

PROZESSE GESTALTEN

Im zweiten Bereich geht es um die Betrachtung der Abläufe und Prozesse innerhalb der Organisation, bei denen personenbezogene Daten, etwa von Kunden oder Beschäftigten, verarbeitet werden. Beispielsweise werden personenbezogene Daten häufig über die Webseite des Unternehmens verarbeitet. Dort werden Daten von Besuchern unter anderem mittels Cookies erfasst – regelmäßig erfordert dies die Zustimmung des Nutzers. Das Unternehmen ist dazu verpflichtet, sich diese Zustimmung über ein Cookie-Banner einzuholen, das bei dem ersten Besuch der Webseite angezeigt wird. Was genau das Banner an Informationen für den Nutzer enthalten muss und ab wann eine Einwilligung rechtens ist, wird durch die DS-GVO vorgegeben. Ebenso ist bestimmt, wie im Anschluss mit den Daten umgegangen werden darf. Wer hier Fehler vermeiden will und kein geeignetes Fachpersonal zur Verfügung hat, sollte auf die Hilfe unabhängiger Experten zurückgreifen.

Mobiles Arbeiten gewinnt weiter an Bedeutung. Auch mit Blick hierauf ergeben sich neue Anforderungen für den Datenschutz im Unternehmen: Mit Mitarbeitenden im Homeoffice sollte der Abreitgeber idealerweise eine Vereinbarung treffen, die alle im Einzelfall zutreffenden Pflichten und Schutzvorkehrungen dokumentiert. In diesem Vertrag können dann auch Abwehrmaßnahmen und Kontrollrechte festgelegt sein.

TECHNISCHE INFRASTRUKTUR INTELLIGENT NUTZEN

Der dritte Eckpfeiler des Datenschutzes ist die IT-Infrastruktur, die innerhalb des Unternehmens eingesetzt wird. Dabei steht die Technologie zum Speichern und Verschlüsseln personenbezogener Daten besonders im Fokus. Welchen Anforderungen die IT-Abschirmung laut DS-GVO dabei gerecht werden muss, ergibt sich aus einer objektiven Bewertung der Daten, die verarbeitet werden. Grundsätzlich gilt: Je sensibler die Daten sind, umso besser müssen sie durch technische Maßnahmen geschützt werden. Besonders drei Aspekte sollten hierbei berücksichtigt werden: Die Vertraulichkeit, die Integrität und die Verfügbarkeit von Daten – in der IT-Sicherheit auch als C.I.A.-Triade bekannt (Confidentiality, Integrity, Availabilty). Es muss sichergestellt sein, dass Daten für unbefugte Personen unzugänglich sind, dass Daten nicht unbefugt verändert werden können und dass Daten nicht verloren gehen.

Zur Gewährleistung dieser Anforderungen sollten die verwendeten IT-Systeme regelmäßig geprüft werden – so lässt sich sicherstellen, dass keinerlei Datenschutzvorfälle geschehen, weil Sicherheitslücken übersehen wurden. Viele unabhängige Prüfstellen bieten entsprechende Untersuchungen und Zertifizierungen an. Immer wichtiger werden internetfähige Geräte und Systeme. Als Teil des stetig wachsenden Internet of Things (IoT) sind sie Schnittstellen nach außen, dadurch wächst auch die Verletzbarkeit für Angriffe von außen. Entsprechend arbeiten Gremien von Behörden sowie unabhängige Prüfstellen daran, Normen und Standards für IoT-Geräte zu etablieren, damit sich einheitliche Sicherheitsstandards durchsetzen.

Mobiles Arbeiten muss bei der Betrachtung der IT-Infrastruktur und IT-Sicherheit ebenfalls Berücksichtigung finden. Konkret bedeutet das: Keine Nutzung privater Endgeräte, alle Arbeitsrechner dürfen nur über ein Virtual Private Network (VPN) auf die Firmensysteme und Infrastruktur zugreifen und durch Sicherheitslösungen geschützt sein. Dabei ist es essenziell, dass private und geschäftliche Daten strikt getrennt werden.

DATENSCHUTZ SCHAFFT VERTRAUEN

Datenschutz ist ein wichtiger Grundstein für das Vertrauen der Kunden, Mitarbeitenden und Geschäftspartner in ein Unternehmen. Es reicht aber nicht, gesetzliche Richtlinien und Anforderungen einzuhalten, auch die notwendige Transparenz bei Sammlung und Verarbeitung der personenbezogenen Daten muss gewährleistet sein. Die drei Elemente eines guten Datenschutzkonzepts – der Mensch, die Prozesse und die Technik – dienen Unternehmen dabei als Orientierung. ■

STEFFEN REIMANN,
Produkt- und Partnermanager,
TÜV SÜD Akademie

Wie Unternehmen die Multicloud-Herausforderung in den Griff bekommen

GEFAHR FEHLKONFIGURATION

Ein typisches Cloud-Szenario umfasst heute oft mehrere hundert Services und Plattformen, die darüber hinaus ständig weiterentwickelt werden. Unzählige Konfigurationsmöglichkeiten erhöhen hier Risiken für die IT-Sicherheit. Bereits ein Konfigurationsfehler kann zur Exposition vertraulicher Daten oder zu schweren Sicherheitsproblemen mit rechtlichen und finanziellen Auswirkungen führen. Solche Fehlkonfigurationen in cloudbasierten Services oder Anwendungen können die Organisation anfällig für Cyberangriffe machen, da sie sich ihrer Angriffsflächen oftmals nicht bewusst sind.

Mehr und mehr Organisationen stellen ihre IT-Architektur auf die Nutzung von Multicloud-Umgebungen um – nicht zuletzt, um einen Vendor Lock-in zu verhindern. Die Analysten von KPMG stellten diesen Trend bereits 2020 fest, denn 87 Prozent der dort befragten Großunternehmen ab 2.000 Mitarbeiter richteten ihre Strategie entsprechend aus. Bei der Umstellung auf Multicloud-Umgebungen und cloudnative Services fällt es vielen Unternehmen jedoch schwer, den Überblick zu behalten, speziell auch über die verschiedenen Konfigurationen. Unklare Zuständigkeiten, mangelnde Transparenz und die allgemeine Komplexität der Cloud tragen dazu bei, die effektive Absicherung und die sichere Konfiguration der IT-Assets und -Ressourcen zu erschweren. Nicht umsonst ist die überwältigende Mehrzahl aller erfolgreichen Angriffe auf Cloud-Services nicht auf Schwachstellen in den Services selbst beziehungsweise ihrer Infrastruktur zurückzuführen, sondern auf intern verursachte Fehlkonfigurationen.

HERAUSFORDERUNGEN DURCH CSPM ABFANGEN

Cloud Security Posture Management (CSPM) unterstützt Organisationen dabei, nicht nur den Überblick zu bewahren, sondern bereits ab

der Entwicklungsphase Fehlkonfigurationen zu vermeiden. CSPM-Lösungsansätze helfen, die wichtigsten Herausforderungen wie Komplexität, Datenabfluss und Compliance der Infrastrukturen zu adressieren. Inkonsistente Sicherheitsausstattungen und Mindestanforderungen in den unterschiedlichen Phasen des Software-Entwicklungszyklus und mehreren Cloud-Umgebungen verkomplizieren die Steuerung und die Kontrolle von Sicherheitsmaßnahmen. Parallel zur Ransomware-Bedrohung hat sich auch die Bedeutung von Governance, Risk und Compliance (GRC) in den Unternehmen entwickelt. Hier steht und fällt das Risikomanagement von Cybergefahren mit den Fähigkeiten und Erfahrungen der Mitarbeitenden sowie deren Einfluss auf die Geschäftsführungsebene.

Fehlkonfigurationen von Cloud-Anwendungen zählen zu den häufigsten Ursachen für ungewollten Datenabfluss. Sie kosten die Organisationen nicht nur viel Zeit und Geld, sondern können auch den Ruf beschädigen, wenn es zu einem Cybersicherheitsvorfall mit Datenverlust kommt. Ein Beispiel sind die nach einem Ransomware-Vorfall mit doppelter Erpressungsmethode veröffentlichten Kundeninformationen zu Verträgen, personenbezogenen Daten sowie Unternehmensinterna. Die dezentrale Bereitstellung von Anwendungen für unterschiedliche Standorte und User-Gruppen erschwert zudem ihre einheitliche Absicherung unter Einhaltung aller geltenden Vorschriften wie der DS-GVO, bei KRITIS dem IT-Sicherheitsgesetz 2.0 sowie zahlreichen branchenspezifischen oder international geltenden Anforderungen.

Die folgenden sieben Faktoren helfen den Verantwortlichen dabei, die für sie richtige CSMP-Lösung auszuwählen:

1. Ermittlung
Die Bestandsermittlung aller Assets und deren Inventarisierung ist die Grundvoraussetzung vor der Auswahl eines Ansatzes. In Multicloud-Implementierungen wird diese Art Informationen jedoch oftmals in Silos vorgehalten. Unabhängig vom Cloud-Anbieter ist eine einheitliche Datenerfassung ein Muss, und die Auswahl eines Anbieters mit einer agentenlosen Architektur gewährleistet eine schnelle und umfassende Erkennung.

2. Priorisierung
Bei der Risikobewertung sollte eine klare Prioritätensetzung erfolgen im Einklang mit der Risikotoleranz der Organisation. Die Verantwortlichen müssen sicherstellen, dass die Lösung kontextabhängig arbeitet und die Aufmerksamkeit auf die Dinge lenkt, die am wichtigsten sind, basierend auf dem Bedrohungsniveau, der jeweiligen Industrie und der Sensibilität der Umgebung.

3. Konformität
Das Augenmerk sollte darauf gelegt werden, dass die Lösung mit einem Klick Berichte zum Nachweis der Konformität mit gängigen Datenstandards wie PCI, DSS, NIST und anderen bereitstellen kann. Damit entfällt der komplexe manuelle Aufwand des Sammelns von Daten und der Erstellung von Reports.

4. Optimierung
Die Lösung sollte in der Lage sein, eine Schritt-für-Schritt-Anleitung mit relevanten und umsetzbaren Handlungsanweisungen zu liefern – aufbauend auf der Diagnose. Allzu oft entdecken Tools ein Problem, ohne einen entsprechenden Plan zur Behebung zur Verfügung zu stellen, wodurch sich die Komplexität der Fehlerbehebung erhöht.

5. Integration
Eine Integration von IDE-Plattformen, DevOps-Tools und Code-Repositories hilft dabei, Probleme auf Code-Ebene bereits in der Generierungsphase zu erkennen. Es ist einfacher, Fehler frühzeitig zu beheben, bevor sie in der Produktionsphase erkannt werden. Die Devise sollte „Vorbeugen" lauten und nicht „nachträgliches Beheben von Fehlkonfigurationen".

6. Konsolidierung
Zur Komplexitätsreduktion bietet sich die Konsolidierung von IT-Umgebungen an, was gleichzeitig zu einer besseren Interoperabilität beiträgt. Sicherheitslösungen wie Cloud Infrastructure Entitlement Management (CIEM), Data Loss Prevention (DLP) oder das Scannen auf Schwachstellen können dazu in einer einzigen Plattform zusammengeführt werden. Damit steht Security-Analysten eine Übersicht aus einer Bandbreite an Datenquellen auf einen Blick zur Verfügung.

7. Automation
Wert sollte ebenfalls auf die Automatisierung und „Selbstheilung" zur Fehlerbehebung gelegt werden. Der Fachkräftemangel sowie die sich stetig verändernde Bedrohungslandschaft erfordern den Einsatz von KI, um die beschriebenen Prozesse so weit wie möglich zu automatisieren.

FAZIT: CSPM ALS TEIL VON CNAPP

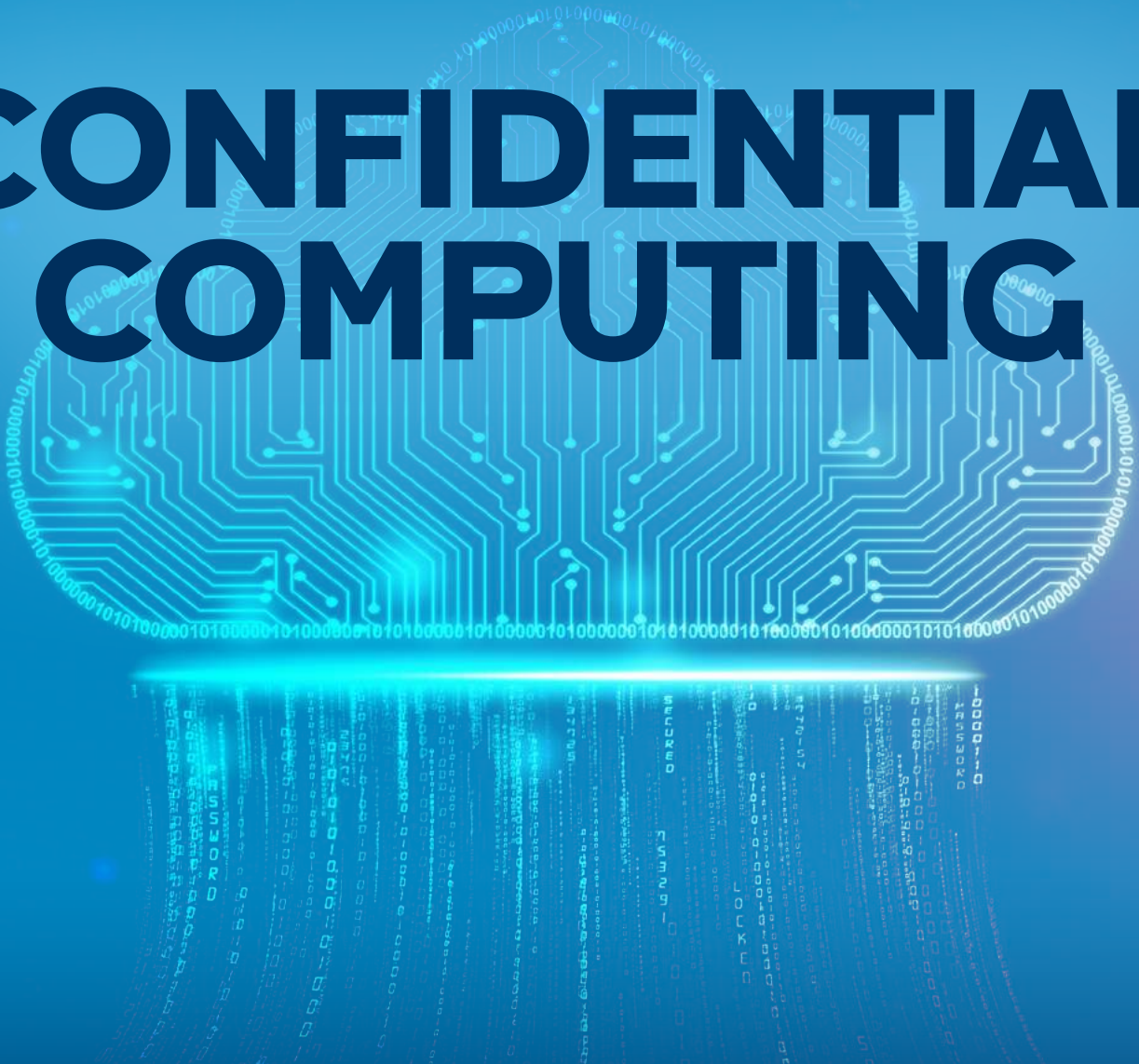
Eine umfassende Cloud Native Application Protection-Plattform (CNAPP) unterstützt Organisationen durch Erkennen, Priorisieren und Beheben von Risiken in Cloud-Infrastrukturen und nativen Anwendungsbereitstellungen in allen Multicloud-Umgebungen.

Durch proaktive Identifizierung und Korrektur von Fehlkonfigurationen in IaaS und PaaS trägt die CSPM als Bestandteil zur Reduzierung von Risiken sowie Gewährleistung der Konformität mit allen geltenden Vorschriften in AWS, Azure und Google-Cloud-Plattform bei und unterstützt die Aufrechterhaltung eines robusten Sicherheitsstatus. Ein solches Vorgehen unterstützt bei der Umsetzung von IT-Sicherheits- und Compliance-Maßnahmen durch Abgleich mit vordefinierten Richtlinien. Diese Richtlinien decken ein breites Spektrum von Standards und Best Practices ab. Unternehmen müssen auf ihrem Weg in die Multicloud die IT-Sicherheit von Anfang an mitdenken, um gefährliche Konfigurationsfehler zu vermeiden. ■

MARTYN DITCHBURN,
Director of Transformation Strategy bei Zscaler

IT-Sicherheit und Datenschutz in der Cloud

CONFIDENTIAL COMPUTING



Daten sind heute die Schlüsselkomponente in der Wertschöpfung. Ihre sichere und vertrauenswürdige Verarbeitung sind daher essenziell – auch in Cloud-Infrastrukturen, die per se erst einmal nicht vertrauenswürdig sind. Während die Daten und der Code der sie verarbeitenden Anwendung hier in gespeicherter Form und bei der Übertragung in der Regel verschlüsselt sind, liegt beides während der Verarbeitung von Anwendungen in einer Cloud-Infrastruktur im Klartext vor und ist somit angreifbar. Auf der Basis von Sicherheitsfunktionen in der CPU sorgt Confidential Computing dafür, dass Anwendungen mit Code und Daten auf Cloud-Infrastrukturen in isolierter und verschlüsselter Form in sicheren Enklaven verarbeitet werden. Die Inhalte der Anwendung in einer Enklave werden so vor unbefugtem Zugriff durch Systemadministratoren und weiteren Personen, die prinzipiell Zugriff auf die Cloud-Infrastruktur haben, geschützt. Technik unterstützt auf diese Weise die sichere und vertrauenswürdige Umsetzung des Datenschutzes.[1]

Vertrauenswürdigkeit ist das Schmiermittel der modernen IT sowie der Digitalisierung. Das Vertrauen von Unternehmen in Cloud-Anwendungen ist heute jedoch noch eher gering – aus Angst, dass Unbefugte Zugriffe auf vertrauliche Daten und den Code einer Anwendung in der Cloud erlangen könnten.

Der Code ist das Softwareprogramm, mit dem die Daten in der Anwendung verarbeitet werden. Bei der Betrachtung moderner Software-Stacks ist festzustellen, dass die Anwendungen meist in virtuellen Maschinen laufen, die häufig in Cloud-Infrastrukturen gehostet werden. Im Rahmen dieser Konfigurationen werden die Daten während der Verarbeitung im Hauptspeicher nicht geschützt. Prinzipiell können sie somit zum Beispiel durch gezielte Angriffe – etwa solche, die Schwachstellen ausnutzen oder einen sogenannten Seitenkanal-Angriff – gezielt ausgelesen werden, da die Daten im Klartext verarbeitet werden.

Mit Confidential Computing besteht die Möglichkeit, diesen und anderen Angriffen effektiv entgegenzuwirken. Die Daten und der Code werden in einer sogenannten Trusted Execution Environment (TEE) geschützt verarbeitet, die eine sichere beziehungsweise vertrauenswürdige Laufzeitumgebung für Anwendungen zur Verfügung stellt. Enklaven stellen dabei eine Realisierungsform von TEE dar. Die grundsätzliche Idee hierbei ist, die Angriffsfläche sehr stark zu reduzieren. Die Anzahl der erzeugbaren Enklaven kann beliebig groß sein, steht aber in Abhängigkeit zur Performance der eingesetzten CPU. Enklaven können auch miteinander kommunizieren, zum Beispiel wenn eine Webserver-Enklave ein Datenbank-Enklave nutzt.

In Abbildung 1 ist die prinzipielle Einbindung von Enklaven als TEEs dargestellt. Es ist zu erkennen, dass nur der nicht geschützte Teil der Anwendungen Zugriff auf die ihnen zugeordneten Enklaven mit dem geschützten Teil der Anwendung (Code und Daten) haben. Die Nutzerinteraktion erfolgt über die Anwendung außerhalb des TEEs. Es ist außerdem zu erkennen, dass die Enklaven stark voneinander isoliert sind und es keine ungewollten Kommunikationskanäle zwischen ihnen gibt. Um Confidential Computing umsetzen zu können, werden CPUs mit erweiterten Sicherheitsfunktionen benötigt, die

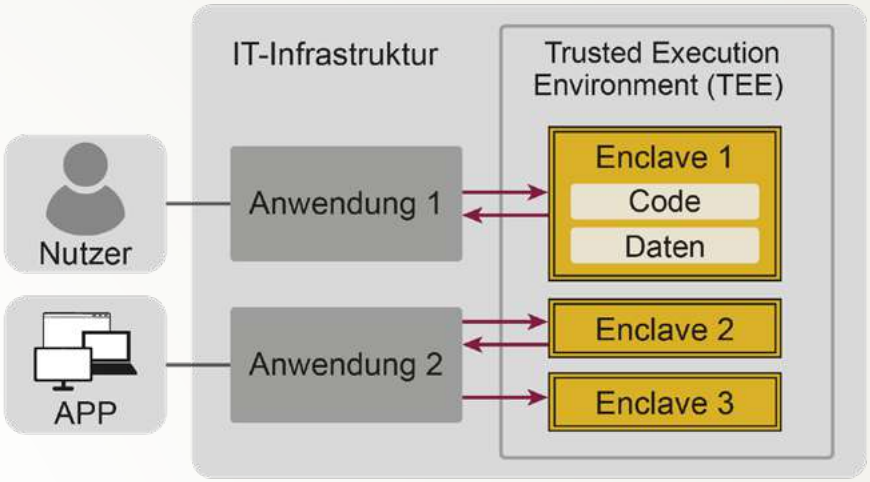


Abbildung 1: Trusted Execution Environment/Enklave

für die Sicherheit und Vertrauenswürdigkeit der Enklaven verantwortlich sind und sie umsetzen.

CONFIDENTIAL COMPUTING AUF DEM PUNKT

Confidential Computing ist ein wichtiger und zukunftsorientierter Aspekt in der IT-Sicherheit, der aus dem Bedarf der Interaktion zwischen verschiedenen IT-Umgebungen hervorgegangen ist. Mithilfe von Confidential Computing ist es möglich, remote die Daten und den Code einer Anwendung vertrauenswürdig im verschlüsselten Zustand als Enklaven auf einem fremden IT-System wie Cloud-Infrastrukturen sicher zu verarbeiten. Alle dafür notwendigen Sicherheitsfunktionen sind in der CPU implementiert. Damit haben Hacker, Malware und Insider mit kriminellen Absichten keinen Einfluss mehr auf die Sicherheit der Anwendung in der Cloud. Folglich muss dem Cloud Provider nicht mehr vertraut werden, sondern nur noch der CPU mit ihren Sicherheitsfunktionen und dem eigenen Code in der Enklave.

Confidential Computing erfüllt zwei wesentliche Sicherheitsaspekte:

- Zum einen wird der Stand der Technik in Bezug auf Datenschutzanforderungen bei der Nutzung von Cloud-Anwendungen automatisch erfüllt.
- Zum anderen ist Confidential Computing Teil des Zero-Trust-Prinzips, bei dem das Sicherheitsparadigma lautet: „Vertraue nie, überprüfe immer“ (siehe dazu zum Beispiel den Absatz „Remote Attestation“).

Unterschiedliche Hersteller haben eigene Confidential-Computing-Lösungen auf dem Markt gebracht: **ARM mit TrustZone, Intel mit SGX** (SoftwareGuard Extension) und der Intel Management Engine sowie **AMD mit SP** (Secure Processor) und Secure Encrypted Virtual Machines. Allerdings ist Intel SGX im Bereich Confidential Computing zurzeit die vorherrschende Lösung am Markt und soll als Basis für weitere Betrachtungen dienen.

INTEL SGX

Intel SGX wurde von Intel mit Mikroprozessoren der sechsten Generation im Jahre 2015 eingeführt. Intel SGX steht für Software Guard Extension und ist eine Erweiterung der x86-Architektur, die es erlaubt, sichere Enklaven zu erstellen und zu verwalten. Remote Attestation, Sealing, Runtime Speicher-Verschlüsselung und Isolierung gehören zu den Kernfunktionen von SGX.

Problematisch bei einer lokal nicht zur Verfügung stehenden und nicht durch TEEs geschützten, vertrauenswürdigen Ausführungsumgebung ist die mangelnde Kontrolle über potenzielle Angriffe. Dies ist ein wichtiger Punkt, da es eine Vielzahl von Angriffsflächen gibt – zum Beispiel das Betriebssystem, den Hypervisior oder die virtuellen Maschinen. Das Ziel von SGX ist, den Bereich, auf dem Angriffe auf die Inhalte einer Enklave ausgeübt werden können, so klein wie möglich zu halten.

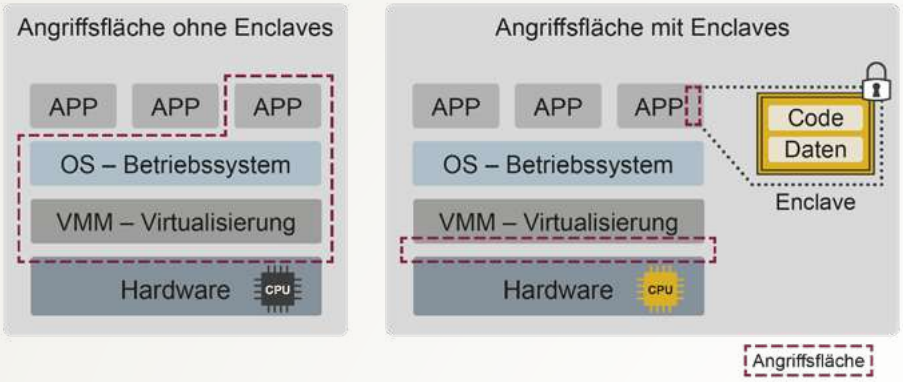


Abbildung 2: Angriffsflächen mit und ohne Confidential Computing

In Abbildung 2 werden die Angriffsflächen von normalen Software-Stacks ohne Confidential Computing parallel zu den Software-Stacks mit Confidential Computing dargestellt. Es ist zu erkennen, dass ohne Confidential Computing der gesamte Bereich zwischen einer App und der zugrunde liegenden Hardware angegriffen werden kann. Da die Software des Betriebssystems sowie für die Virtualisierung von Anwendungen sehr umfangreich ist und rein statistisch gesehen sehr viele Softwarefehler vorhanden sind, können über die dadurch vorhandenen Softwareschwachstellen immer wieder erfolgreiche Angriffe umgesetzt werden.

Dies wird mit der Verwendung von Confidential Computing verhindert, da die Anwendung direkt in einer Enklave mit der Unterstützung von Sicherheitsfunktionen in der CPU isoliert vom Rest der IT-Infrastruktur läuft und die Daten verschlüsselt sind. Damit werden die Angriffsfläche auf den Code und die Daten in der Anwendung deutlich reduziert. Die Schwachstellen des Betriebssystems, der Virtualisierung und der Anwendung haben keinen Einfluss auf den Inhalt der Enklave, weil alles verschlüsselt, isoliert und verifiziert wird.

Das bedeutet, Enklaven können weder durch Software- noch Hardware-Debugger analysiert werden. Im zugewiesenen Arbeitsspeicher einer Enklave werden nur verschlüsselte Daten abgelegt. Der Schlüssel wird regelmäßig neu generiert und innerhalb der CPU sicher gespeichert. Auf die isolierten Daten kann nur der Code zugreifen, der in der Enklave erhalten ist und über Attestation verifiziert wird. Selbst privilegierte Prozesse haben während der Verarbeitung keinen Zugriff auf die Daten.

Bei der Umsetzung der Confidential Computing IT-Sicherheitsarchitektur muss lediglich noch dem eigenen Code in der Enklave (den Programmierern oder der Software-Hersteller) und der CPU (dem Hersteller Intel) vertraut werden. Durch die redundante Nutzung verschiedener Cloud-Anbieter ist es zusätzlich möglich, auch die Verfügbarkeit eigenständig zu managen.

VERTRAUENSWÜRDIGE CPU

Die CPU stellt die Basis für die Umsetzung von Enklaven der Confidential Computing Idee dar. In der Intel-CPU sind ein Hardware-Sicherheitsmodul und weitere IT-Sicherheitsfunktionen implementiert, auf deren Basis sicher und vertrauenswürdig Enklaven umgesetzt werden. Die Sicherheitsfunktion der CPU lässt sich grob in drei Bereiche aufteilen:

- Attestation gegenüber dritten Parteien (Integrität, Vertrauenswürdigkeit)
- Verschlüsseln der Daten (Vertraulichkeit)
- Beobachten/Messen der Enklaven (Vertrauenswürdigkeit)

Weitere Sicherheitsfunktionen sind Key-, Memory- und Cache-Management. Thread Control Structure und Handling Hardware Exception gehören ebenfalls dazu.

KEY MANAGEMENT UND VERSCHLÜSSELUNG

Bei der Herstellung einer CPU werden von Intel im Produktionsprozess zwei sogenannte Device Root Keys erstellt. Diese haben verschiedene Funktionen und werden direkt in der Intel-CPU gespeichert, um damit Kryptografie-basierte Sicherheitsfunktionen umsetzen zu können.

Root Provisioning Key (RPK)

Der Root Provisioning Key wird von Intel nach dem Zufallsprinzip generiert. Den öffentlichen Schlüssel speichert Intel in einer Datenbank, damit dieser zur Verifizierung von SGX-Prozessoren und von Zertifikaten im Attestationsprozess verwendet werden kann. Bei der Remote Attestation kommt der RPK zum Einsatz, um mit dem geheimen Schlüssel einen Report und die Antwort auf die Challenge zu signieren.

Root Sealing Key (RSK)

Der Root Sealing Key wird im Produktionsprozess bei Intel nach dem Zufallsprinzip in der CPU generiert und abgespeichert. Dabei wird für jede CPU ein einzigartiger Schlüssel generiert. Er ist somit vertraulich. Die meisten Schlüssel, die von Intel SGX verwendet werden, sind vom RSK auf der Basis einer Schlüsselhierarchie abgeleitet, daher kann keine andere Instanz diesen kennen. Aus diesem Grund ist es wichtig, dass der jeweilige Schlüssel vertraulich behandelt wird und der CPU zur Verfügung steht. Hier muss Intel vertraut werden, dass der RSK nicht anderweitig verwendet wird, denn es ist schwer nachprüfbar, ob die generierten Schlüssel wirklich unabhängig und einzigartig sind. Wenn Intel einen guten Zufallsgenerator verwendet und die Schlüssellängen dem Stand der Technik genügen, stellt dieser Sicherheitsaspekt jedoch kein Risiko dar.

VERSCHLÜSSELUNG

Intel SGX ist so designt, dass nur die CPU selbst als vertrauenswürdig einstuft ist, weil diese die Basis für die Sicherheit der Enklave darstellt. Für die hardwareseitige Zugriffskontrolle verfügt die CPU über eigens entwickelte Befehle, um eine sichere Laufumgebung zu schaffen. Diese CPU-Befehle verhindern das ungewollte Laden von Daten oder Code. Diese liegen in eigens dafür gewidmeten DRAM-Bereichen, die von der CPU verschlüsselt werden. Nachdem eine Enklave einmal gestartet wurde, läuft diese hardwareseitig in einem besonderen Modus, der von allen anderen Prozessoren stark isoliert ist.

ATTESTATION

Ein wichtiges Konzept von Confidential Computing ist die Attestation. Allgemein beschreibt Attestation den Prozess, mit dem sich die Vertrauenswürdigkeit einer (fremden) IT-Infrastruktur feststellen lässt. Im Kontext von Confidential Computing heißt dies, dass mit Attestation die Vertrauenswürdigkeit einer Enklave bescheinigt

werden kann, wenn sie auf einer fremden IT-Infrastruktur verarbeitet wird, oder zwei Enklaven miteinander in diese kommunizieren. Es ist so möglich festzustellen, ob die entsprechenden Daten und der Code in der Enklave nicht manipuliert und damit original sind. Im Folgenden werden zwei Varianten der Attestation beschrieben. Zum einen die Local Attestation und zum anderen die Remote Attestation.

Local Attestation

Local Attestation beschreibt den Prozess, wenn zwei Enklaven auf derselben Cloud-Infrastruktur laufen. Ziel ist es, ein Vertrauensverhältnis zwischen zwei lokalen Enklaven aufzubauen. Die zu prüfende Enklave erstellt dabei einen Report und signiert diesen mit ihrem privaten Schlüssel, der in der CPU gespeichert ist.

Die andere Enklave kann nun mit dem passenden öffentlichen Schlüssel der prüfenden Enklave diese Signatur verifizieren. Zwischen den Enklaven ist bereits eine sichere Verbindung, zum Beispiel basierend auf dem Diffie-Hellman-Verfahren, hergestellt worden.[2] Der Report beinhaltet den Hashwert des Codes und der Daten in der Enklave, ihre Konfiguration sowie weitere Attribute.

Remote Attestation

Mit Remote Attestation kann die Vertrauenswürdigkeit eines sich auf einer fremden IT-Infrastruktur befindlichen Enklave festgestellt werden, zum Beispiel einer in der Cloud laufenden Enklave, bevor mit dieser Daten und Code verarbeitet werden. Es wird also überprüft, ob die richtige Anwendung auf der richtigen Cloud-Infrastruktur läuft. Die benötigten Schlüssel für die Attestation werden bei der CPU-Herstellung von Intel generiert. Für die Remote Attestation ist es zum einen möglich, den Intel-Attestierungsdienst zu verwenden und zum anderen, einen eigenen Attestierungsdienst aufzubauen.

In Abbildung 3 ist der Ablauf von Remote Attestation bei Confidential Computing schemenhaft dargestellt. Im ersten Schritt (1) wird von der prüfenden Instanz eine Challenge an die Anwendung gesendet, um zu überprüfen, ob die richtige Anwendungs-Enklave auf der richtigen IT-Infrastruktur läuft. Die Anwendung gibt die Challenge an die Anwendungs-Enklave weiter (2). Die Challenge dient dem Zweck, zu beweisen, dass die betreffende Anwendungs-Enklave nicht manipuliert wurde (Daten und Code). Außerdem wird von der Anwendungs-Enklave ein

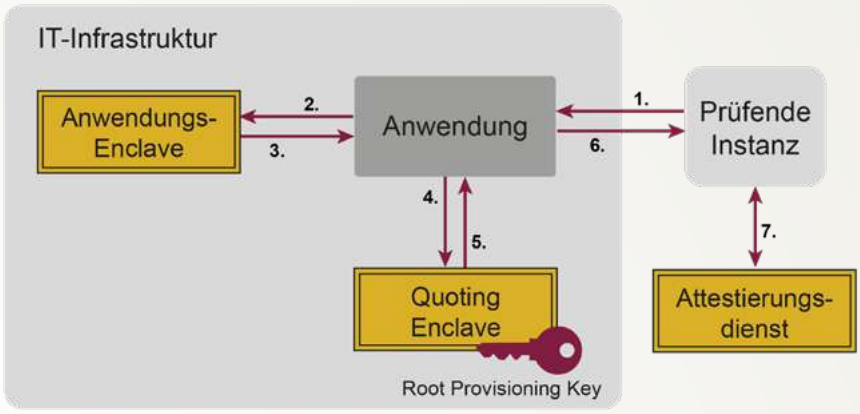


Abbildung 3: Remote Attestation bei Confidential Computing

Report erstellt, mit dem der Code, die Daten, die Konfiguration und weitere Attribute der Anwendungs-Enklave überprüft werden können.

In Schritt (3) sendet die Anwendungs-Enklave die Antwort der Challenge und den Report an die Anwendung. Diese schickt die Informationen an die sogenannte Quoting Enklave. Dies ist eine von Intel bereitgestellte Enklave, die als vertrauenswürdiger Zwischenhändler fungiert. Der von der Anwendungs-Enklave erstellte Report und die Lösung der Challenge wird nun zur Quoting Enklave gesendet (4) und dort mit dem geheimen Teil des Root Provisioning Keys, der sicher in der CPU gespeichert ist, signiert. Das Ergebnis ist nun der sogenannte Quote, ein Zertifikat. Der Quote wird über die Anwendung (5) zur Verifikation an die zu überprüfende Instanz gesendet (6). Die überprüfende Instanz verwendet den von Intel bereitgestellten Attestierungsdienst oder einen selbst gehosteten, um die Quote-Signatur der Quoting Enklave zu verifizieren. Der Attestierungsdienst hat Zugriff auf die Datenbank, in der alle öffentlichen Schlüssel der Root Provisioning Key aller Intel-CPUs gespeichert sind. Dies wird dadurch ermöglicht, da Intel bei der Produktion den Schlüssel generiert und den öffentlichen Teil in einer Datenbank abspeichert. Anschließend checkt die überprüfende Instanz den Inhalt des Reports und stellt sicher, dass die erwartete Antwort auf die Challenge enthalten ist.[2], [3]

SGX HARD- UND SOFTWARE

Damit Confidential Computing in Betrieb genommen werden kann, müssen verschiedene Parteien innerhalb der IT-Infrastruktur zusammenarbeiten. Die User Runtime stellt in diesem Kontext das Bindeglied zwischen der eigentlichen Hardware und den Enklaven dar. Die User

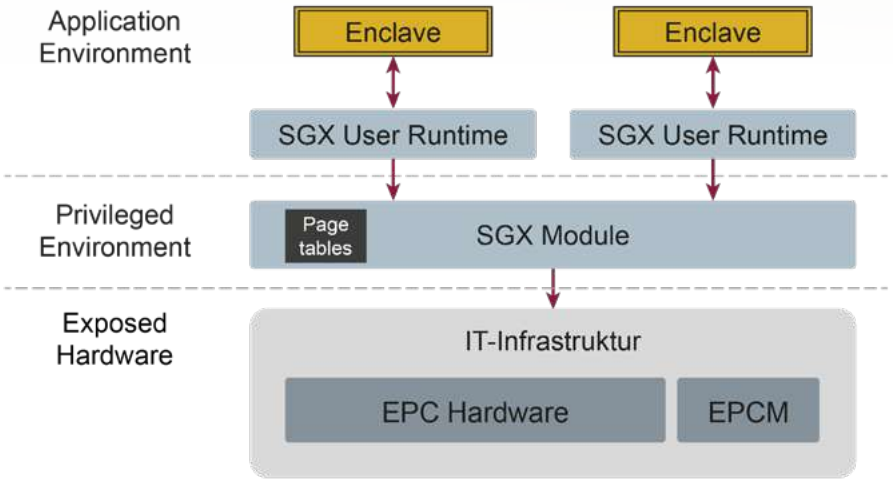


Abbildung 4: SGX Hardware/Software

Runtime umfasst den erweiterten Befehlssatz, der unbedingt vonnöten ist, denn dadurch kann die IT-Infrastruktur angesprochen werden. Die IT-Infrastruktur beinhaltet EPC (Enklave Page Cache) sowie EPCM (Enklave Page Cache Map), beides Ausschnitte aus dem Arbeitsspeicher. Abbildung 4 zeigt den Zusammenhang zwischen Middleware, Soft- und Hardware.

PERFORMANCE VON CONFIDENTIAL COMPUTING

Um die Praxistauglichkeit von Confidential Computing auszutesten, wurden zum Beispiel von USENIX – dem Verband von Ingenieuren, Systemadministratoren und Softwareentwickler, die sich hauptsächlich mit der Weiterentwicklung des Unix-Betriebssystems beschäftigen – verschiedene Performance-Tests durchgeführt [4]. Bei der Durchführung der Tests wurde einerseits der Focus auf **Prozessorzeit** in Relation zum **Durchsatz** (Requests), andererseits auf die **Latenz** gelegt. Die Prozessorzeit bezeichnet in modernen IT-Systemen die Zeit, die vergeht, während die CPU einen Thread ausführt. In vielen modernen Softwarelösungen spielen die genannten drei Kenngrößen eine wichtige Rolle.

Bei diesem Test wurden verschiedene Containerumgebungen überprüft. Der Performance-Test ergab, dass durch dem Einsatz von Enklaven zwar ein Teil der verfügbaren Performance verloren geht, aber da dadurch die Sicherheit, Vertrauenswürdigkeit sowie der Datenschutz deutlich erhöht werden, ist dies als akzeptabel zu beurteilen.

PERSPEKTIVEN VON CONFIDENTIAL COMPUTING

Confidential Computing verspricht sehr gute Zukunftsaussichten im Cloud-Computing-Umfeld. Insbesondere wenn sensible Unternehmensdaten in der Cloud verarbeitet werden sollen, kann mittels Confidential Computing eine hohe Sicherheit und Vertrauenswürdigkeit bereitgestellt werden. Zudem werden die einschlägigen Datenschutzanforderungen durch die Nutzung von Confidential Computing erfüllt. Ein weiterer Vorteil ist, dass in der Enklave Daten analysiert werden können, ohne dass diese erkennbar und nutzbar sind, was für die Analyse von personenbezogenen Daten sehr hilfreich sein kann.

Confidential Computing trägt dazu bei, dass das Vertrauen der Unternehmen in die diversen am Markt existierenden Cloud-Dienste gesteigert wird, da Anwendungen in Enklaven auch während der Verarbeitung geschützt sind und vertrauenswürdig ausgeführt werden. Das Risiko, dass Unbefugte sich Zugriff zu Unternehmensdaten oder den Code verschaffen können, lässt sich sehr stark reduzieren.

Das Hauptanwendungsfeld der Intel SGX liegt im Serverbereich von Cloud-Infrastrukturen. Dies ist auch daran zu erkennen, dass Intel SGX nicht mehr auf CPUs verfügbar ist, die für Endanwender konzipiert sind, also in PCs oder Notebooks. Andere Hersteller bieten ebenfalls Confidential Computing an, zum Beispiel AMD mit Secure Encrypted Virtualization (SEV) – eine Technologie, die es ermöglicht, verschlüsselte virtuelle Maschinen (VMs) zu hosten.

ZUSAMMENFASSUNG

Sobald sich ein Unternehmen entscheidet, seine Daten in der Cloud zu verarbeiten, sollte die Sicherheit und Vertrauenswürdigkeit der Daten und des Codes bei der Verarbeitung von Anfang an mitberücksichtigt werden. Bei der IT-Sicherheitsarchitektur von Confidential Computing werden auf der Basis von Sicherheitsfunktionen in der CPU Daten und Code einer Anwendung in einer Enklave verschlüsselt und mit Attestation die Vertrauenswürdigkeit einer Enklave überprüft. Dadurch wird sichergestellt, dass nur gewünschte Daten genutzt werden und der richtige Code in der Enklave ausgeführt wird.

Auch die Verfügbarkeit von Intel SGX und anderen Lösungen am Markt ist ein Argument für Confidential Computing. Fast jeder Cloud-Anbieter hat Confidential Computing auf Basis von Intel SGX in seinem Produktportfolio, sodass es hier eine große Auswahl gibt. Außerdem haben die Performance-Tests gezeigt, dass die gewonnenne Sicherheit keinen unverhältnismäßigen Tribut fordert. Confidential Computing hilft, die Sicherheit und Vertrauenswürdigkeit von Cloud-Diensteanbietern deutlich zu erhöhen und den Datenschutzanforderungen zu genügen. ■

LUKAS DEMMING
studiert im Master Internet-Sicherheit an der Westfälischen Hochschule Gelsenkirchen und beschäftigt sich im Rahmen des Studiums mit Confidential Computing.

JAN ROTTHUES
studiert im Master Internet-Sicherheit an der Westfälischen Hochschule Gelsenkirchen und beschäftigt sich im Rahmen des Studiums mit Confidential Computing

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

Literatur

[1] *N. Pohlmann: „Cyber-Sicherheit – Das Lehrbuch für Konzepte, Mechanismen, Architekturen und Eigenschaften von Cyber-Sicherheitssystemen in der Digitalisierung". 2. Auflage, Springer Vieweg Verlag, Wiesbaden 2022*

[2] *Overview of Intel SGX – Part 1, SGX Internals, Juli 2018. Adresse: https://blog.quarkslab.com/overview-of-intel-sgx-part-1-sgx-internals.html*

[3] *Systems Software & Security Lab from Georgia Institute of Technology. https://sgx101.gitbook.io/sgx101/sgx-bootstrap/attestation*

[4] *Secure Linux Containers with Intel SGX, Marz 2016. Adresse: https://www.usenix.org/system/files/conference/osdi16/osdi16-arnautov.pdf*

Hybrider Datenschutz-Kongress

DATENSCHUTZ – GESTALTUNGSAUFTRAG IM ZEITALTER DER DIGITALISIERUNG

46. DAFTA & 41. RDV-Forum

Jetzt anmelden: **datakontext.com/dafta-2022**

GDD Gesellschaft für Datenschutz und Datensicherheit e.V.

DATAKONTEXT

Der Data Act als Turbo für datengetriebene Geschäftsmodelle

POTENZIALE VON UNTERNEHMENSDATEN AUSSCHÖPFEN

Mit dem Entwurf der Europäischen Kommission zum Data Act soll die europäische Datenstrategie weiter ausgebaut werden. Der freie Verkehr von Daten, der mit dem Verordnungsentwurf angekurbelt werden soll, ist von besonderer Wichtigkeit, denn mit ihm geht die Sicherung des digitalen Wandels einher. Derzeit wird trotz der Unmengen an Daten, die täglich generiert werden, nur ein Bruchteil des daraus resultierenden Potenzials ausgeschöpft. Der Data Act soll insofern zu einem besseren Zugang zu Daten beitragen und damit datengetriebene Geschäftsmodelle und Innovation vorantreiben. Welche Regelungen der Data Act vorsieht, welche Herausforderungen sich ergeben können und was er für den Datenschutz und die Unternehmenspraxis bedeutet, beleuchtet folgender Beitrag.

Der Vorschlag zum Data Act (deutsch Datengesetz) ist in Form einer EU-Verordnung ausgestaltet. Europäische Verordnungen entfalten – im Gegensatz zu europäischen Richtlinien – unmittelbare Wirkung in den EU-Mitgliedstaaten, ohne dass es einer Umsetzung durch die einzelnen Mitgliedstaaten bedarf. Der Vorschlag der Verordnung harmonisiert Vorschriften für den fairen Zugang zu und der Nutzung von Daten. Damit soll er als „zweite Säule" der europäischen Datenstrategie gelten, deren Ziel es ist, durch neue Regelungen das wirtschaftliche Potenzial der wachsenden Datenmenge besser zu nutzen und einen wettbewerbsfähigen Datenmarkt zu fördern.

Als „erste Säule" wird der Data Governance Act verstanden, welcher am 23. Juni 2022 in Kraft getreten ist und nach einer Nachfrist von 15 Monaten ab September 2023 gilt. Dieser umfasst Regelungen zur Datenverwaltung – er dient also der Schaffung von Prozessen und Strukturen, um die Generierung von Daten und deren Verkehr zu ermöglichen, unter anderem durch Einführung von Datenvermittlungsdiensten. Während der Data Governance Act also Verfahren schafft, die die gemeinsame Nutzung von Daten durch Unternehmen, Einzelpersonen und den öffentlichen Sektor erleichtern, wird im Data Act geklärt, wer unter welchen Bedingungen einen Mehrwert aus Daten schaffen kann.

Der Gesetzesentwurf des Data Act sieht Regelungen vor, die klären sollen, wer unter welchen Bedingungen einen Mehrwert aus Daten schaffen kann, wobei Fairness zentraler Faktor ist. Konkret soll es darum gehen, dass unter anderem Nutzende von vernetzten Geräten, Maschinen oder sonstigen Produkten, wie in den Bereichen Internet of Things (IoT), Industrial Internet of Things (IIoT) oder Connected Cars, darüber entscheiden können, wie mit den gewonnenen Daten umgegangen werden soll, an deren Entstehung sie mitgewirkt haben.

Damit umfasst der Data Act unter anderem Regeln für die Nutzung von Daten, die solche vernetzten Geräte, Maschinen und Produkte generieren. Nutzende können dabei Unternehmen als auch Verbraucher sein. Der Data Act soll es den Nutzenden ermöglichen, diese Daten auszuwerten und unter bestimmten Bedingungen an Dritte weiterzugeben. Unter Daten werden darunter sowohl personenbezogene als auch nicht personenbezogene Daten verstanden, womit der Anwendungsbereich des Data Act klar über den der DS-GVO hinausgeht. Der Zugang zu Daten und deren Nutzung soll zwischen Unternehmen sowie zwischen Unternehmen und Behörden erleichtert werden.

Angestrebt ist zudem ein ausgewogenes Verhältnis zwischen dem Recht auf Zugang zu Daten und Anreizen für Investitionen in Daten. Die Regelung des Zugangs und der Nutzung industrieller Daten, also gerade auch nicht personenbezogener Daten, durch Verbraucher und Unternehmen ist insofern Kernelement des Entwurfs („Accessability by Design"). Ebenso soll durch den Entwurf und die entsprechenden Regelungen die Eröffnung eines Wettbewerbsmarktes für Daten geschaffen werden.

Ziel des Data Act ist es also, Fairness in Bezug auf Daten zu schaffen, Rechte der Nutzenden transparent zu machen, ihnen die Ausübung der Rechte zu erleichtern sowie eine Kohärenz zwischen Zugriffsrechten zu gewährleisten – und das sowohl für die Privatwirtschaft als auch den öffentlichen Sektor.

WANN KOMMT DER DATA ACT ZUR ANWENDUNG?

Der sachliche Anwendungsbereich des Data Act betrifft Regelungen über die Bereitstellung von Daten, die bei der Nutzung eines Produkts oder verbundenen Dienstes erzeugt werden. In Art. 2 Data Act-E findet sich eine Reihe von Begriffsdefinitionen, die die Elemente des sachlichen Anwendungsbereiches definieren und damit auch näher abgrenzen. Daten sind gemäß Art. 2 Data Act-E „jede digitale Darstellung von Handlungen, Tatsachen oder Informationen, sowie jede Zusammenstellung solcher Handlungen, Tatsachen oder Informationen, auch in Form von Ton-, Bild- oder audiovisuellem Material".

Während IoT- oder IIoT-Geräte, also Produkte, die durch ihre vernetzten Funktionen Daten über unter anderem die Umgebung erlangen, erzeugen oder sammeln können, unter die Verordnung fallen sollen, sind beispielsweise Tablets, Smartphones, Kameras, Webcams oder Textscanner von ihr ausgeschlossen. Gravierender Unterschied und Grund dafür ist, dass für Letztere ein menschlicher Beitrag zur Generierung von Daten notwendig ist, während dies bei den zuerst genannten

Während IoT- oder IIoT-Geräte, also Produkte, die durch ihre vernetzten Funktionen Daten über unter anderem die Umgebung erlangen, erzeugen oder sammeln können, unter die Verordnung fallen sollen, sind beispielsweise Tablets, Smartphones, Kameras, Webcams oder Textscanner von ihr ausgeschlossen.

Geräten vollständig automatisiert möglich ist. Hinsichtlich virtueller Assistenten, die häufig in Smart-Home-Umgebungen mit IoT eng zusammenspielen, aber nicht in direkter Verknüpfung mit einem Produkt stehen, fordert die Verordnung ihre Geltung ein. Hier müssen Unternehmen dann aber genau differenzieren, für welche Daten der Data Act Anwendung finden kann. Dies soll nur für diejenigen Daten gelten, die aus der Interaktion zwischen dem Nutzenden und dem Produkt über den virtuellen Assistenten stammen. Vom virtuellen Assistenten erstellte Daten, die nicht mit der Verwendung eines Produkts zusammenhängen, sind nicht Gegenstand des Data Act. Für Unternehmen ist es daher entscheidend, welche Produkte sie herstellen, anbieten oder gar selbst nutzen, um von den einzelnen Rechten des Data Act profitieren zu können.

WEN ADRESSIERT DER DATA ACT?

In Art. 1 Abs. 2 Data Act-E wird festgelegt, für wen die Verordnung gelten soll. Das sind:

- Hersteller von Produkten und Erbringer verbundener Dienste, die in der Union in Verkehr gebracht werden,
- Nutzende solcher Produkte oder Dienste,
- Dateninhaber, die Datenempfängern in der Union Daten bereitstellen,
- unter bestimmten Voraussetzungen öffentliche Stellen und Organe, Einrichtungen und sonstige Stellen der Union, sowie
- Anbieter von Datenverarbeitungsdiensten, die Kunden in der Union solche Dienste anbieten.

Eine der zentralen Pflichten des Data Act ist die in Art. 3 Data Act-E geregelte Pflicht der Zugänglichmachung von bei der Nutzung von Produkten oder verbundenen Diensten erzeugten Daten.

Unter Nutzenden eines Produkts fallen juristische wie auch natürliche Personen, also zum Beispiel Unternehmen oder Verbraucher, soweit diese das Produkt gekauft, gemietet oder geleast haben. Von einer Nutzung soll nach Maßgabe der Verordnung dann ausgegangen werden, wenn die Risiken und Vorteile der Verwendung des vernetzten Produkts den Nutzenden betreffen.

Für Kleinstunternehmen oder kleine und mittlere Unternehmen (KMU) ist eine Privilegierung in Art. 7 Abs. 1 Data Act-E vorgesehen, wonach die Pflichten des Kapitel II (Datenweitergabe von Unternehmen an Verbraucher und zwischen Unternehmen) diese nicht treffen sollen.

WELCHES SIND DIE WICHTIGSTEN REGELUNGEN DES DATA ACT?

Für den B2C- und B2B-Bereich hält Kapitel II des Data Act-E wichtige Regelungen bereit, welche die Datenweitergabe von Unternehmen an Verbraucher und zwischen Unternehmen betreffen. Dieses Kapitel enthält vor allem Rechte, die Nutzenden eines Produkts oder verbundenen Dienstes zukommen und von ihnen geltend gemacht werden können.

Eine der zentralen Pflichten des Data Act ist die in Art. 3 Data Act-E geregelte Pflicht der Zugänglichmachung von bei der Nutzung von Produkten oder verbundenen Diensten erzeugten Daten. Insbesondere Art. 3 Abs. 1 Data Act-E nimmt den Gedanken des Access by Design auf. Mit dieser Vorschrift soll insofern dem Ziel der Datenwirtschaft Rechnung getragen werden, weil die Zugänglichmachung von Daten als Grundpfeiler für den freien Verkehr von Daten dient.

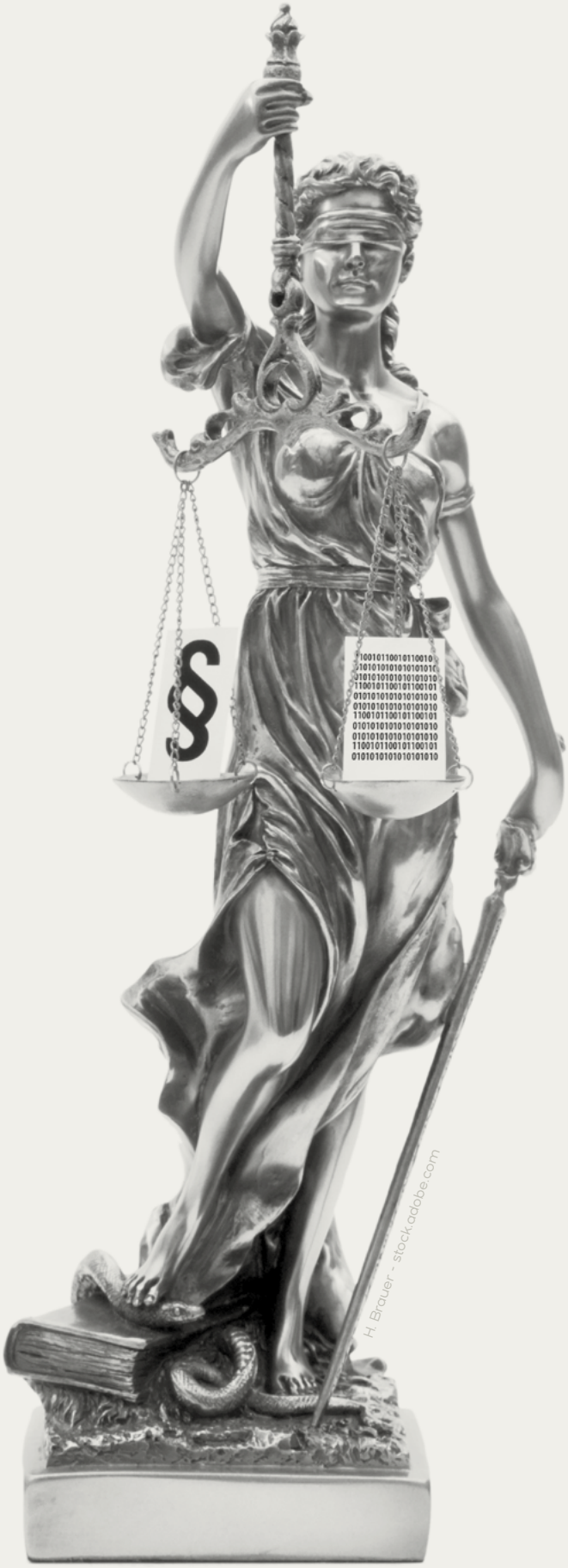
Im direkten Anschluss, in Art. 3 Abs. 2 Data Act-E, findet sich eine weitere wichtige Regelung für Verbraucher: die vorvertragliche Informationspflicht vor dem Abschluss eines Kauf-, Miet- oder Leasingvertrages für zum Beispiel ein IoT-Produkt. Die transparente Darstellung relevanter Informationen soll ebenfalls zum Fairnessfaktor beitragen, bürdet den anbietenden Unternehmen jedoch auch weitere Pflichten auf.

Eine weitere wesentliche Norm stellt Art. 4 Data Act-E dar, der das Recht der Nutzer auf Zugang zu den bei der Nutzung von Produkten oder verbundenen Diensten erzeugten Daten sowie das Recht auf deren Nutzung regelt. Dieses Recht zielt darauf ab, dem Nutzenden transparent seine Zugänglichkeitsrechte zu eröffnen und dabei aber den fairen Wettbewerb nicht aus dem Blick zu verlieren, in dem auch Regelungen zu Geschäftsgeheimnissen oder Entwicklung von Produkten mitbedacht wurden. In Art. 4 Abs. 6 Data Act-E wird außerdem geregelt, dass nicht personenbezogene Daten, die bei der Nutzung eines Produktes oder verbundenen Dienstes erzeugt werden, nur auf Grundlage einer vertraglichen Vereinbarung mit dem Nutzer verarbeitet beziehungsweise genutzt werden dürfen.

Auch Art. 5 Data Act-E nimmt den Verkehr der Daten nochmals in den Blick und regelt die Herausgabe der Daten an Dritte, der auf Verlangen eines Nutzenden gefolgt werden muss.

In Kapitel IV, welches Regelungen zu missbräuchlichen Klauseln in Bezug auf den Datenzugang und die Datennutzung zwischen Unternehmen bereithält, ist insbesondere auf Art. 13 Data Act-E hinzuweisen. Dieser regelt den Umgang mit missbräuchlichen Vertragsklauseln in Bezug auf den Datenzugang und die Datennutzung, die gegenüber einem Kleinstunternehmen oder einem kleinen oder mittleren Unternehmen (KMU) einseitig auferlegt werden. Es handelt insoweit um eine wettbewerbs- beziehungsweise kartellrechtliche Komponente des Data Act. Die vereinbarten Vertragsklauseln sollen für das regelmäßig strukturell unterlegene KMU nicht bindend sein und die Fairness in der Datenwirtschaft und auf dem Markt vorantreiben. In Art. 13 Abs. 2–4 Data Act-E findet sich eine Definition zur Missbräuchlichkeit und AGB-ähnliche Regelbeispiele, wann eine Vertragsklausel als missbräuchlich zu verstehen ist beziehungsweise sein kann. Zur Erleichterung der Umsetzung der Vorschriften aus dem Data Act soll die Europäische Kommission Mustervertragsbedingungen erarbeiten, wie Art. 34 Data Act-E vorsieht.

Eine weitere bedeutende Regelung, um die Ziele des Data Act erreichen zu können, sind die Vorschriften zur Interoperabilität (Kapitel VIII), welche als verbindliche regulatorische Vorgaben zur Festlegung europäischer Standards fungieren. Der Entwurf des Data Act verlangt, dass Dienste mit offenen Standards und Schnittstellen kompatibel sein müssen, um so die Interoperabilität zwischen den Diensten zu erhöhen. Dadurch soll die Erleichterung des Wechsels zwischen Cloud- und Edge-Diensten erreicht werden, wobei der Zugang zu wettbewerbsfähigen und interoperablen Datenverarbeitungsdiensten ein zentrales Anliegen für eine florierende Datenwirtschaft ist.



In diesem Zusammenhang sind auch die Vorschriften zur Erleichterung des Wechsels zwischen Anbietern von Cloud-Diensten zu sehen. Es sollen nach dem Kapitel VI des Data Act-E, das den Wechsel zwischen Datenverarbeitungsdiensten regelt, unter anderem keine Hindernisse beim Anbieterwechsel bestehen. Weiterhin sind beispielsweise auch Höchstgrenzen bei Kündigungsfristen (vgl. Art. 23 Abs. 1 lit. a Data Act-E) vorgesehen.

Der Entwurf des Data Act sieht außerdem Regelungen vor, die den Zugang zu Daten, die im Besitz des Privatsektors sind, durch Behörden zu gewissen Zwecken ermöglichen.

Als Sanktionsmittel, die bei Verstößen gegen den Data Act zum Einsatz kommen können, verweist der Entwurf zum Data Act zum Teil (vergleiche zum Beispiel Art. 33 Abs. 3 Data Act-E) auf die Regelungen der DS-GVO zu den allgemeinen Bedingungen für die Verhängung von Geldbußen sowie auf die dort genannten Beträge für Geldbußen.

WIE IST DAS VERHÄLTNIS ZWISCHEN DATA ACT UND DS-GVO?

Das Verhältnis zur DS-GVO nimmt der Data Act in Art. 1 Abs. 3 Data Act-E in den Blick und stellt klar, der Data Act grundsätzlich nicht die Anwendbarkeit der DS-GVO berührt. Hier muss zunächst festgehalten werden, dass die DS-GVO die Regulierung personenbezogener Daten betrifft, wohingegen der Data Act gerade auch nicht personenbezogene Daten mit einbezieht. Zudem liegt der Fokus der DS-GVO unter anderem darin, mögliche Rechtsgrundlagen für die Verarbeitung personenbezogener Daten zu schaffen. Auch wenn der Data Act vertragliche Regelungen als Datenverarbeitungsgrundlagen berücksichtigt, ist das Anliegen dieses Entwurfs in erster Linie, den Verkehr und die Zugänglichmachung nicht personenbezogener Daten zu ermöglichen und nicht Rechtsgrundlagen für deren Verarbeitung zu erschaffen.

Bei der Nutzung eines Produkts oder verbundenen Dienstes können allerdings auch Daten erzeugt werden, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen (und damit personenbezogene Daten darstellen). Die Verarbeitung solcher Daten unterliegt weiterhin den Vorschriften der DS-GVO, auch wenn personenbezogene und nicht personenbezogene Daten häufig in einem Datensatz untrennbar miteinander verbunden sind. Daraus dürften sich auch eine Menge offener Abgrenzungsfragen zum Anwendungsbereich der jeweiligen Vorschriften ergeben.

Für Unternehmen, die unter den Anwendungsbereich des Data Act fallen, ist von großer Bedeutung, wann eine spezielle Rechtsgrundlage notwendig wird, etwa

Gemäß der DS-GVO gilt das Recht auf Datenportabilität nur für personenbezogene Daten, die auf der Grundlage bestimmter Rechtsgrundlagen mithilfe von automatisierten Verfahren verarbeitet werden. Mit dem Data Act wird dieses Recht auf vernetzte Produkte ausgeweitet …

um das Recht auf Zugang zu gewähren. Fordert ein Nutzender, der zugleich die betroffene Person ist, sein Zugangsrecht ein, so steht ihm dieses ohne Weiteres zu. Anders ist dies hingegen, wenn ein Unternehmen die auch personenbezogenen Daten einem Dritten, zum Beispiel einem anderen Unternehmen, zugänglich machen will. Hier muss unbedingt zusätzlich das Erfordernis einer Rechtsgrundlage nach Art. 6 DS-GVO beachtet werden. Insofern muss bei Auslegung und Anwendung des Data Act immer auch die DS-GVO im Blick behalten werden, was ebenfalls zu komplexen rechtlichen Einordnungsfragen führen dürfte.

Aus Art. 1 Abs. 3 Data Act-E lässt sich zumindest in Bezug auf das Recht der Datenübertragbarkeit nach Art. 20 DS-GVO erkennen, dass dieses Recht durch den Data Act erweitert wird. Gemäß der DS-GVO gilt das Recht auf Datenportabilität nur für personenbezogene Daten, die auf der Grundlage bestimmter Rechtsgrundlagen mithilfe von automatisierten Verfahren verarbeitet werden. Mit dem Data Act wird dieses Recht auf vernetzte Produkte ausgeweitet, damit Verbraucher Zugriff auf alle von ihrem Produkt erzeugten sowohl personenbezogenen als auch nichtpersonenbezogenen Daten haben und diese weitergeben können. Generell spricht die Kommission davon, dass der Vorschlag im Einklang mit der DS-GVO stehen soll, die bestehenden Rechte jedoch ergänzt.

WAS MÜSSEN UNTERNEHMEN NUN BEACHTEN?

Der Data Act hat das grundsätzliche Potenzial, wichtige Ziele im EU-Binnenmarkt zu erreichen und eine breitere Verwendung von erhobenen Daten zu ermöglichen. Der bisherige Entwurf bildet hierfür eine erste Grundlage. In der Praxis könnten sich jedoch einige gewichtige Herausforderungen bei der Anwendung des Data Act ergeben, etwa die Schwierigkeit von Unternehmen zu beurteilen, ob ihre Produkte vom Anwendungsbereich des Data Act umfasst sind oder aber wie das komplexe Zusammenspiel mit den Vorgaben der DS-GVO beachtet werden kann. Deshalb empfiehlt es sich, dass Unternehmen frühzeitig die Vorgaben des Data Acts beachten und die vorgesehenen Regelungen evaluieren.

AUSBLICK

Der Entwurf wurde im Februar 2022 durch die Europäische Kommission vorgelegt. Das Konsultationsverfahren vor dem Europäischen Wirtschafts- und Sozialausschuss wurde bis Mai 2022 durchgeführt. Derzeit liegt die Verordnung dem Europäischen Parlament und dem Rat vor, wobei der Zeithorizont bis zu einer Entscheidung noch offen ist. Die aktuelle Tschechische Ratspräsidentschaft hat im Juli 2022 einen ersten Kompromissvorschlag vorgelegt, der die Grundlage für die Diskussionen im Rat liefern soll. Dabei wurde unter anderem eine Angleichung an die auf der DS-GVO basierenden Definitionen, umfassendere Ausnahmeregelungen für mittlere Unternehmen, eine striktere Trennung zwischen den Bestimmungen zur Regelung der Beziehungen zwischen Unternehmen und Kunden sowie zusätzliche Schutzmaßnahmen für Geschäftsgeheimnisse und ein Verbot von „dark patterns“ vorgeschlagen. Ob der Data Act in seiner aktuell vorliegenden Fassung so Geltung erlangen wird, bleibt daher vorerst mit Spannung abzuwarten. ■

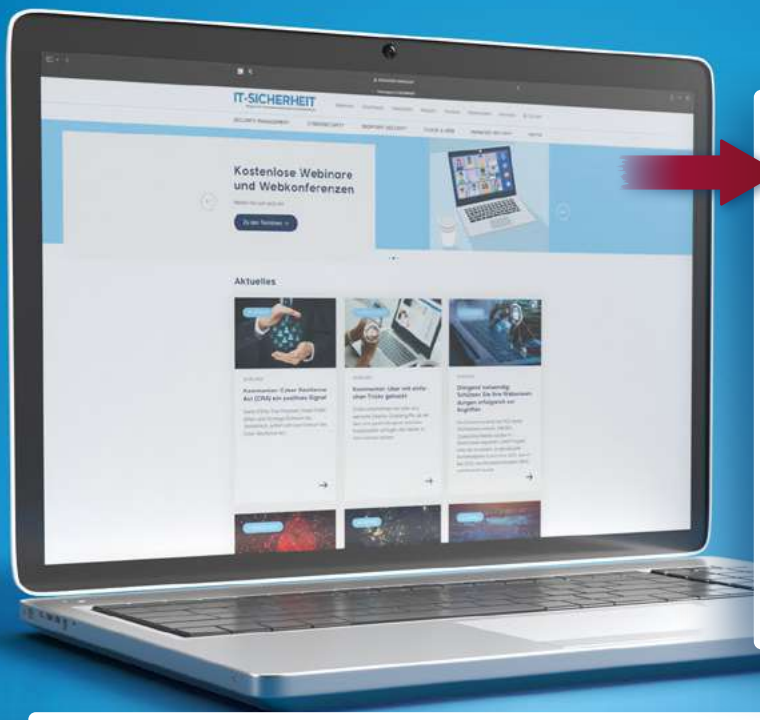
Foto: Kanzlei SRD

JAN O. BAIER,
Rechtsanwalt, Associated Partner, Fachanwalt für Urheber- und Medienrecht, ist spezialisiert auf das Urheber-, Medien-, IT-, Datenschutz- und Wettbewerbsrecht sowie den gewerblichen Rechtsschutz. Er berät Unternehmen zu rechtlichen und strategischen Fragen der Digitalisierung und ist überdies ein geschätzter Ansprechpartner bei der Vertragsgestaltung im Medienbereich, für IT-Projekte, Cloud Computing und SaaS. Auch zu Fragen von IT-Wartungsverträgen und Lizenzverträgen verfügt er über eine ausgewiesene Expertise.

www.srd-rechtsanwaelte.de

DR. SEBASTIAN SCHNEIDER
ist Legal Consultant bei der ISiCO Datenschutz GmbH und ist spezialisiert auf EU- und Datenschutzrecht. Ein Fokus seiner beratenden Tätigkeit liegt in den Bereichen Digital Compliance und Health Data. Als Datenschutzexperte betreut er nationale und internationale Mandanten bei der datenschutzkonformen Umsetzung (digitaler) Geschäftsmodelle.

www.isico-datenschutz.de



Das Webportal von IT-SICHERHEIT

IM WEB GEHT'S WEITER!

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

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

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

Die drei Schlüssel zu Business-Resilienz

WIDERSTANDSFÄHIGKEIT STÄRKEN

Inflation, unterbrochene Lieferketten und massive Umbrüche in der Arbeitswelt haben das Bewusstsein dafür geschärft, dass sich die Geschäftswelt immer schneller auf Veränderungen einstellen muss. Das erfordert neue Konzepte, um sich frühzeitig darauf vorzubereiten. Um die Widerstandsfähigkeit von Unternehmen zu stärken, sind drei Bausteine essenziell.

www.itsicherheit-online.com/Dell-2022-05

Tim van Wasen,
Geschäftsführer von Dell Technologies in Deutschland
(Foto: Dell Technologies)

Der Datenlebenszyklus als Sicherheitsmodell

BESSERE SICHT IM INFORMATIONSDSCHUNGEL

Im Zuge der Digitalisierung sind für Kriminelle nicht nur Wertsachen wie Bargeld, Schmuck und Gold, sondern auch Daten eine gut verwertbare Beute. Für Unternehmen ist der Schutz derselben ein schwieriges Unterfangen. Denn im Gegensatz zu physischen Gütern müssen sich Daten in der Regel frei zwischen Kunden und Partnern bewegen können. Sie benötigen daher Schutzmaßnahmen, die in einer Vielzahl von möglichen Szenarien zuverlässig greifen, ohne jedoch die Unternehmensprozesse, von denen sie Bestandteil sind, sowie alle daran Beteiligten, zu beeinträchtigen. Das Modell des Datenlebenszyklus kann dabei unterstützen, lückenlose Sicherheit über alle Verarbeitungsprozesse hinweg zu etablieren.

www.itsicherheit-online.com/HelpSystems-2022-05

Michael Kretschmer,
Vice President DACH, HelpSystems
(Foto: HelpSystems)

Wenn Hacker Benutzer mit MFA-Anfragen bombardieren

BEST PRACTICES GEGEN MFA-PROMPT-BOMBING-ATTACKEN

MFA Prompt Bombing ist eine relativ einfache, aber effektive Angriffsmethode, die darauf abzielt, Zugang zu einem System oder einer Anwendung zu erhalten, die durch Multi-Faktor-Authentifizierung (MFA) geschützt ist. Der Angreifer sendet dabei in kurzer Zeit eine Vielzahl an MFA-Genehmigungsanfragen an einen Benutzer, in der Hoffnung, dass das Opfer durch die Anfragen so überfordert ist, dass es schließlich aufgibt und unwissentlich dem Angreifer Zugang gewährt. Für eine höhere Erfolgsquote wird der Angreifer den Benutzer in den meisten Fällen zu einem ungünstigen Zeitpunkt herausfordern, zum Beispiel spät in der Nacht.

www.itsicherheit-online.com/Silverfort-2022-05

Haiko Wolberink,
Vice President of Sales EMEA, Silverfort
(Foto: Silverfort)

VORSCHAU Ausgabe 6|22 DEZEMBER/ JANUAR

KONTINUIERLICHE RISIKOBEWERTUNG

Kaum ein Unternehmen wurde bisher von Cyberangriffen verschont. Dabei ist es schon lange nicht mehr entscheidend, wie groß oder aus welcher Branche ein Unternehmen ist. Für die zuständigen Chief Information Officer (CISO) ist klar, mögliche Angriffe müssen proaktiv angegangen werden. Eine kontinuierliche Risikobewertung ist somit wichtiger denn je, aber gleichzeitig umso schwieriger geworden. Es stellt sich daher die Frage: Wie sollten CISOs diese angehen und was muss unbedingt beachtet werden?

MOBILE ANWENDUNGEN: WIE ENTWICKLER IHRE APPS BESSER SICHERN KÖNNEN

Mobile Apps speichern viele persönliche Informationen wie Fotos, Aufnahmen, Notizen, Zahlungs- und Kontodaten oder Standortdaten. Entsprechend wird erwartet, dass mobile Anwendungen und Dienste diese Informationen sicher aufbewahren, schützen und verantwortungsvoll verarbeiten. Die Geräte- und Betriebssystemhersteller stellen dazu viele innovative Technologien bereit, die kombiniert mit bewährten Methoden und effizienten Werkzeugen leistungsstarke Schutzmaßnahmen bilden können.

Weitere geplante Themen:

- **Security Management:** Awareness messbar steigern
- **Container:** temporär aber mit hohem Schutzbedarf

... und vieles mehr.

IN UNSEREM VERLAG ERSCHEINEN AUSSERDEM NOCH FOLGENDE ZEITSCHRIFTEN

IT-SICHERHEIT
Magazin für Informationssicherheit und Datenschutz

Verlag:
DATAKONTEXT GmbH
Standort Frechen
Augustinusstr. 11 A · 50226 Frechen
www.datakontext.com

Chefredaktion:
Stefan Mutschler (S.M.)
E-Mail: stefan-mutschler@t-online.de

Redaktion:
Dr. Peter Münch (P.M.),
Dr. jur. Martin Zilkens (M.Z.),

Online-Redaktion:
Jessica Herz
Leitung Online
herz@datakontext.com
+49 2234 98949-80
Lisa Bieder
Silvia Klüglich
Chiara Schönbrunn

Herausgeberbeirat:
Prof. Dr. Michael Backes, Prof. Dr. jur. Dirk-M. Barton, Walter Ernestus, Prof. Dr. Nikolaus Forgó, Prof. Dr. Rainer W. Gerling, Dr. Jan-Peter Ohrtmann, Prof. Dr. Norbert Pohlmann, Dr. jur. Martin Zilkens

Gründer: † Bernd Hentschel

Grafik/Layout/Satz:
Michael Paffenholz
Tel.: +49 173 8382572
E-Mail: michael.paffenholz@gmx.de

Objekt- und Anzeigenleitung:
Wolfgang Scharf
Tel.: +49 2234 98949-60
E-Mail: wolfgang.scharf@datakontext.com
zzt. gilt die Anzeigenpreisliste Nr. 27

Vertrieb/Herstellung:
Dieter Schulz
Tel.: +49 2234 98949-99
dieter.schulz@datakontext.com

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

Erscheinungsweise: sechs Ausgaben
Alle Preise verstehen sich inkl. MwSt. Der Abonnementpreis wird im Voraus in Rechnung gestellt. Das Abonnement verlängert sich zu den jeweils gültigen Bedingungen um ein Jahr, wenn es nicht mit einer Frist von 8 Wochen zum Ende des Bezugszeitraumes gekündigt wird.

Erscheinungsweise, Bezugspreise und -bedingungen:
Abonnement und Bezugspreis beinhalten die Print-Ausgabe sowie eine Lizenz für das Online-Archiv. Die Bestandteile des Abonnements sind nicht einzeln kündbar. Der Preisanteil des Online-Archivs ist auf der Abonnementrechnung separat ausgewiesen.

Aboservice:
Hüthig Jehle Rehm GmbH, München,
Tel.: +49 89 21 83-7110

Druck: Grafisches Centrum Cuno GmbH & Co. KG, Calbe (Saale)

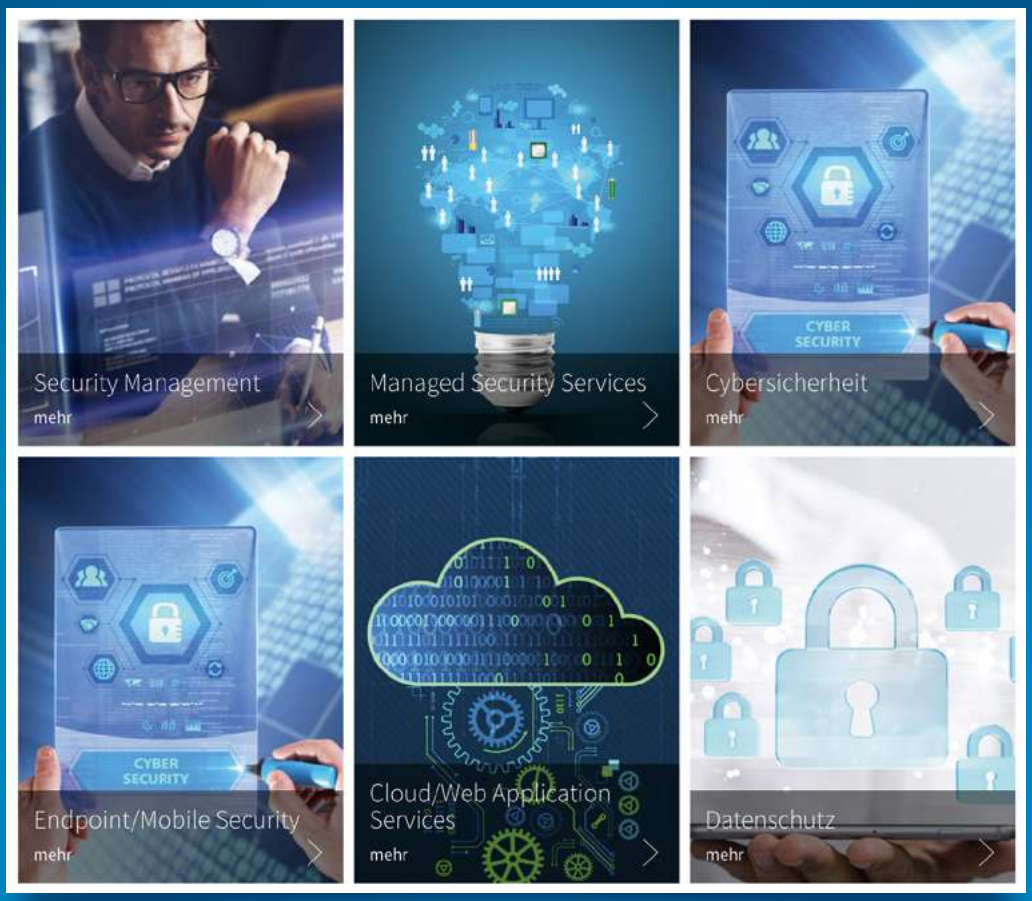
Beilagen: DATAKONTEXT GmbH, Frechen

Titelbild: LastPass

Fotos: Firmenbilder; DATAKONTEXT; (anttoniart, blackboard, Daniel Berkmann, Gorodenkoff, mchlskhrv, H. Brauer, lassedesignen, nb_factory, NeoLeo, Noah 9000, Passatic, peach_adobe, phonlamaiphoto, terovesalainen, tete_escape, tomasknopp, vladgrin) - stock.adobe.com; Ratul Ghosh/ unsplash, florian krumm/unsplash

28. Jahrgang 2022 · ISSN: 1868-5757

Der neue Themenguide IT-Sicherheit



www.itsicherheit-online.com/themen

Wir bedanken uns bei unseren Partnern:

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

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

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

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

Jetzt mitmachen und Firmenpartner werden:

wolfgang.scharf@datakontext.com

DATAKONTEXT

Cyber-Security-Zertifizierungen von TÜV SÜD.

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

- ISO/IEC 27001 Zertifizierung
- ISO/IEC 20000-1 – Zertifiziertes Service-Management (in der IT)
- Zertifizierung nach IT-Sicherheitskatalog
- KRITIS – Nachweis über angemessene IT-Sicherheit nach §8a BSIG
- TISAX® – Der Nachweis für IT-Sicherheit in der Automobilbranche
- ISO 22301 – Business Continuity Management (BCM)
- ISO/IEC 27701 – Privacy Informationssicherheits-Managementsystem (PIMS)

www.tuvsud.com/cyber-security-zertifizierungen

TÜV SÜD Management Service

Mehr Wert.
Mehr Vertrauen.

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

TÜV®