it security

Detect. Protect. Respond.
Januar/Februar 2023

MODERNE VPN-LÖSUNGEN

Zero Trust & SASE-Strategien

Bernd Nüßlein, NCP engineering GmbH

Cyber-Resilience
ab Seite 10

CASB, SSE, SASE
Next Generation

CYBER-ATTACKEN
Hilft ein Threat Navigator?

MITRE ATT&CK
Wo stehen wir heute?

Künstliche Intelligenz

Fluch oder Segen?

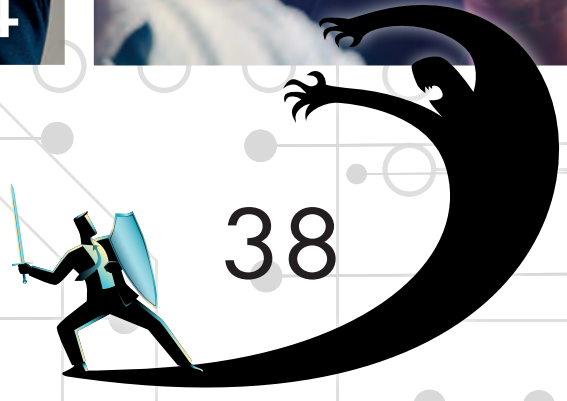
Mehr Infos dazu im Printmagazin

SCAN ME

itmanagement

und online auf **www.it-daily.net**

Inhalt



COVERSTORY

IT SECURITY

Ganzheitliche IT-Security-Konzepte im Fokus

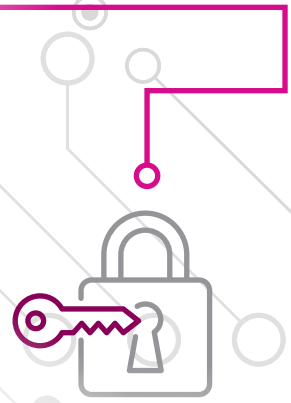
MODERNE VPN-LÖSUNG, ZERO TRUST UND SASE-STRATEGIEN

In der IT-Sicherheit wandelt sich der Blick der Security-Verantwortlichen. Der Trend geht weg von einzelnen Tools hin zu vollumfänglichen IT-Security- & Cloud-Konzepten. Diese Entwicklung ist auch für den Nürnberger Enterprise-VPN-Anbieter NCP von großer Bedeutung. Darüber sprach Ulrich Parthier, Publisher it security mit Bernd Nüßlein, Vice President Sales & Marketing bei NCP in Nürnberg.

Ulrich Parthier: *Hallo Herr Nüßlein, kommen wir gleich zur Einstiegsfrage. Können auch Sie bei ihren Kunden einen geänderten Blickwinkel auf die IT und die IT-Sicherheitsgefahrenlage feststellen?*

Bernd Nüßlein: Hallo Herr Parthier. ja das können wir so bestätigen. Wenn es früher noch darum ging, dass man einzelne Lösungen haben musste, um von einer sicheren IT zu sprechen, sind heute eine ganze Vielzahl von Schritten nötig, um Hackern das Handwerk zu legen. Dabei ist ein ganzheitlicher Ansatz sehr wichtig, denn es nützt nichts, nur die richtigen Lösungen zu haben, sie müssen am Ende auch perfekt ineinandergreifen.

SECURE



ACCESS

Ulrich Parthier: *In den vergangenen Jahren haben immer mehr Unternehmen ihre Anwendungen in die Cloud verschoben. Das erfordert natürlich auch einen Strategiewechsel bei den IT-Security Anbietern. Sehen Sie diese Wechsel auch bei ihren Kunden und den Toolanbietern im Allgemeinen?*

Bernd Nüßlein: Selbstverständlich gehen auch unsere Kunden und Partner diesen Weg – der eine mehr, der andere weniger schnell.

Ulrich Parthier: *Und wie lautet die NCP-eigene Antwort auf diese Frage? Welche Rolle spielt die Cloud in ihrer Lösungsstrategie?*

Bernd Nüßlein: Wir müssen darauf vorbereitet sein. Unsere Produkte müssen in die neuen Konzepte integrierbar sein. In Bezug auf die Cloud müssen wir natürlich die Trends beobachten und dort, wo es sinnvoll erscheint, neue Technologien aufgreifen.

Ulrich Parthier: *Können Sie dies etwas näher erläutern?*

Bernd Nüßlein: Das Thema „Cloud" hat in den letzten Jahren dazu beigetragen, dass IT-Security-Netzwerke immer flexibler und digitaler werden. Technologien und Standards wie SASE, Single Sign On, SD-WAN oder Zero Trust erweitern die Möglichkeiten des modernen Remote Access. Gleichzeitig steigen durch die fortschreitende Vernetzung aber auch die potenziellen Angriffsvektoren. Daher müssen Cloud-Lösungen in Unternehmen genauso lückenlos abgesichert werden wie eine On-Premises-Infrastruktur. Wir entwickeln dazu moderne VPN-Lösungen, die alle Anforderungen von Anwendern, Unternehmen und Providern gleichermaßen erfüllen und in jedes dieser Technologie-Konzepte eingebaut werden können!

Ulrich Parthier: *SD-WAN wird derzeit auch viel in Unternehmen eingeführt. Wie integriert sich ein VPN von NCP als Beispiel hier in einen software-definierten Netzwerk-Verbund?*

Bernd Nüßlein: Ein SD-WAN (Software Defined Area Network) ist im Grunde ein verzweigtes Computernetzwerk, das beispielsweise weit verteilte Standorte eines Unternehmens auf intelligente Weise miteinander verbindet. Ein solcher Zusammenschluss aus vielen Standorten und Netzwerken benötigt ein sehr hohes Sicherheitsniveau. Diese Absicherung übernehmen in einem SD-WAN die softwarebasierten IPsec-VPN-Produkte von NCP.

Der nötige Schutz gelingt durch die Kombination eines NCP Virtual Secure Enterprise VPN Servers (SES/vSES) als

Gateway und des NCP Secure Enterprise Managements (SEM) als Management-System. Hierbei liegt das Gateway in der Cloud aber nicht direkt im Internet, sondern bildet hinter der Firewall eine abgesicherte Umgebung direkt auf dem Server. Über die Management-Umgebung regeln Sie anschließend die komplette, sicherheitstechnische Administration im SD-WAN. Dies reicht von der User- und Geräte-Authentisierung, über Firewall-Konfigurationen und zentrales Update-Management bis hin zu Multifaktor-Authentifizierung oder Endpoint Policy Checks, die jeden Login-Versuch und das dazugehörige Endgerät auf seine Sicherheit hin überprüfen.

Ulrich Parthier: *Es ist sicher nicht einfach, neue Architekturkonzepte zu integrieren. Wie gelingt NCP dies beim SASE-Ansatz?*

Bernd Nüßlein: Unter SASE (Secure Access Service Edge) versteht man ein Architekturkonzept, das WAN-Services und Security-Funktionen wie Zero Trust oder VPNaaS (VPN as a Service) in einer cloudbasierten Lösung kombiniert. Die gemanagten Enterprise-Lösungen von NCP stellen dem SD-WAN den passenden IT-Security-Mitspieler an die Seite. Als 100 Prozent softwarebasiertes VPN-Produkt lässt sich unsere Lösung komplett flexibel in der Cloud betreiben und übernimmt fortan die verschlüsselte Datenübertragung zur Firmenzentrale. Jeglicher Datenverkehr wird über einen IPsec-basierten Tunnel übertragen, wodurch neben umfassender Sicherheit auch die maximale Geschwindigkeit für den Transfer sichergestellt wird.

Ulrich Parthier: *Ein großes Thema in Unternehmen ist das des Single Sign On, kurz SSO. Damit kann ein Benutzer nach einer einmaligen Authentifizierung an einem Arbeitsplatz auf alle Rechner und Dienste, für die er lokal berechtigt ist, vom selben Arbeitsplatz aus zugreifen. Welchen Part übernimmt NCP in einer SSO-/SAML-Konfiguration?*

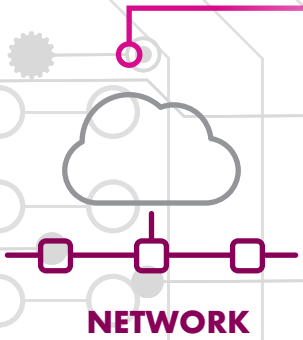
Bernd Nüßlein: Benutzerfreundlichkeit steht bei NCP seit jeher im Fokus aller Produkte. SSO haben wir seit Jahren bei unseren Lösungen im Einsatz – ist also nichts Neues.

Die Security Assertion Markup Language (SAML) ist ein offener Standard, der die Verwendung und Verifizierung von Anmeldeinformationen für mehrere Webseiten erlaubt. Mit SAML kann sich ein Nutzer mit nur einem Login-Datensatz in verschiedene webbasierte Anwendungen einwählen und die Verwaltung mehrerer Anwender entfällt. Hier nutzen wir das SSO in einem neuen Kontext und Verbinden es mit der Forderung, dass nach der Anmeldung die verschiedenen Datenströme getrennt werden können.

Das NCP-Gateway und -Management bilden hierbei gewissermaßen das Eingangstor für den Cloud-Remote-Access über SAML. Unsere Lösung übernimmt in diesem Prozess die Rolle eines Authentication Providers (AP). Wurde die Login-Anfrage des Nutzers am SSO-Portal geprüft und genehmigt, baut der NCP-Client anschließend einen VPN-Tunnel auf. Dieser Zugang gilt fortan für alle internen Dienste, während externe Cloud-Anwendungen dynamisch über Funktionen wie den NCP VPN-Bypass oder Application Based Tunneling am Tunnel vorbeigeleitet werden können. Und dank IPsec-Verschlüsselung sind alle Verbindungen zur Firmenzentrale bestens abgesichert. Dies ist ein klarer Vorteil und Security-Pluspunkt von NCP gegenüber vielen anderen Zero-Trust-Anbietern.

Ulrich Parthier: *Zero-Trust-Konzepte haben in den letzten Monaten verstärkt Einfluss auf die Planung bei IT-Security-Verantwortlichen gehalten. Wie sind sie hier aufgestellt und wie integrieren sie sich in solche Konzepte?*

Bernd Nüßlein: So ist es. Zero Trust bezeichnet einen allgemeinen IT-Sicherheitsansatz, der Nutzern nach einem



> ALS 100 PROZENT SOFTWAREBASIERTES VPN-PRODUKT LÄSST SICH UNSERE LÖSUNG KOMPLETT FLEXIBEL IN DER CLOUD BETREIBEN UND ÜBERNIMMT FORTAN DIE VERSCHLÜSSELTE DATENÜBERTRAGUNG ZUR FIRMENZENTRALE.
>
> **Bernd Nüßlein, Vice President Sales & Marketing, NCP engineering GmbH, www.ncp-e.com**

Least-Privilege-Prinzip kein blindes Vertrauen mehr ausspricht. Stattdessen erhält der Anwender nur Zugriff auf die Daten, die er für seine aktuelle Arbeit benötigt.

Die softwarebasierten Lösungen für sichere Datenkommunikation von NCP verfolgen diesen Ansatz bereits seit Jahren: Im Gegensatz zu herkömmlichen Standard-VPN-Lösungen bieten wir mehr als nur eine abgesicherte Verbindung zum Firmenserver, sondern setzen auf vollumfängliche Netzwerksicherheit.

Deshalb möchten wir uns auch von diesen Standardlösungen distanzieren und mit dem Vorurteil über VPN aufräumen. Viele ziehen den Schluss, dass VPN tot sei beziehungsweise, dass die Technologie veraltet und überholt sei. Moderne VPN-Lösungen machen eine Zero-Trust-Strategie aber besser und sicherer.

So können IT-Administratoren im NCP Secure Enterprise Management (SEM) unter anderem die Zugriffsrechte von Nutzergruppen und einzelnen Anwendern granular konfigurieren. Auf diese Weise fügt sich unsere Lösung mit ihrer zentralen Administration der Nutzerzugriffe nahtlos in den Zero-Trust-Leitgedanken ein.

Ulrich Parthier: *Nehmen wir an, Unternehmen schlagen den von Ihnen vorgezeichneten Weg zu einem ganzheitlichen IT-Security und Cloud-Ansatz ein und setzen einen Zero Trust-Ansatz um. Was bedeutet das für das IT-Sicherheitsniveau?*

SERVICE

FRAMEWORK

Bernd Nüßlein: Das Sicherheitsniveau sollte bei den richtigen Komponenten in diesen Security-Ansätzen ein weit Höheres sein, als es die sogenannten All-In-One-Anbieter propagieren. Denn kein Anbieter kann behaupten, er hätte die perfekte Zero-Trust-Lösung. Zero Trust ist ein Konzept und kein einzelnes Produkt.

Ulrich Parthier: *Zusammengefasst, niemand sucht mehr nach Einzellösungen und verteilten Features, sondern nach kompletten Lösungen. Weg vom Silogedanken hin zu 360 Grad-Lösungen. Ist das richtig so?*

Bernd Nüßlein: Exakt, dementsprechend entwickeln wir auch unsere strategische Ausrichtung weiter: Weniger Fokus auf einzelne Features, sondern lösungsorientiert. Unternehmen haben Herausforderungen/Zielsetzungen bei ihrer IT-Security – wie können wir diese individuellen Ansprüche als Gesamtlösung optimal ergänzen und verbessern?

Ulrich Parthier: *Sie haben gerade die Bereiche Sales und Marketing intern neu strukturiert. Was ist der Hintergrund und wie lauten hier ihre Ziele?*

Bernd Nüßlein: Zum einen haben die Neustrukturierung personelle Veränderungen notwendig gemacht. Zum anderen war es unserer Geschäftsleitung ein Anliegen, die Bereiche in ein und dieselben Hände zu legen und so die Ziele und Ausrichtung von Vertrieb und Marketing noch enger zusammenwachsen zu lassen. Hierbei muss es gelingen den Unternehmen, die noch auf der Suche nach den passenden Bausteinen für ihr IT-Konzept sind, die richtigen Argumente pro NCP an die Hand zu geben. Ich freue mich, dass ich dieses Vertrauen bekommen habe.

Ulrich Parthier: *Der Wechsel vom klassischen Hersteller hin zum lösungsorientierten Anbieter, wie kann der gelingen?*

Bernd Nüßlein: So viel muss sich gar nicht verändern, denn die Produkte, die wir heute haben, erfüllen schon jetzt die Kriterien für eine moderne VPN-Lösung, die Zero Trust oder SASE-Strategien verbessern. Wir müssen nur den Fokus in der öffentlichen Wahrnehmung verändern und verdeutlichen, dass wir als deutscher Hersteller von High-Level-Security ein wichtiger Baustein in diesen Konzepten sind.

Ulrich Parthier: *Welche Auswirkungen wird das auf ihre Partner und die Partnerstruktur haben?*

Bernd Nüßlein: Sowohl unsere Partner als auch Kunden können sich sicher sein, dass sie mit NCP einen verlässlichen und starken Anbieter für die Zukunft haben. Dies belegen die zahlreichen Gespräche der vergangenen Wochen und Monate. Einen deutlichen Schritt nach vorne machen wir dabei insbesondere mit unseren großen OEM-Partnern, deren Bedarf rasant nach oben geht. Gleichzeitig kommen neue Anfragen von MSSP´s (Managed Security Service Providern), die unsere ganzheitliche Enterprise- und vom BSI zugelassene VS-NfD Lösung als Service anbieten möchten. Wir werden hier, denke ich, ebenfalls noch neue Partnerschaften hinzugewinnen.

it security: *Herr Nüßlein, wir danken für das Gespräch!*

Sicherheit von A bis Z

UNTERNEHMEN BRAUCHEN STIMMIGE IT-KONZEPTE WIE SASE ODER ZERO TRUST!

Cybersicherheit war schon immer eine heikle Sache. Speziell für Unternehmen gewinnt dieses Thema jedoch zunehmend an Bedeutung. Egal, ob es um die Bestellung von Waren, die Absprache mit Lieferanten und Kunden oder die interne Datenkommunikation der Mitarbeiter geht: Ohne ein entsprechend hohes Level an IT-Security machen sich Firmen angreifbar und können nicht dauerhaft produktiv bleiben.

Wie brisant diese Thematik ist, verdeutlichen auch die Zahlen der vergangenen Jahre. So hat sich die Cyber-Bedrohungslage zuletzt so stark angespannt wie noch nie zuvor. Laut dem Bundesamt für Sicherheit in der Informationstechnik (BSI)[1] wurden allein im Jahr 2021 insgesamt 15 Millionen Meldungen zu Schadprogramm-Infektionen an deutsche Netzbetreiber übermittelt. Im gleichen Zeitraum wurden auch 20.174 Schwachstellen in Software-Produkten bekannt – ein Zuwachs von 10 Prozent gegenüber dem Vorjahr.

Entwicklungen wie diese sorgen dafür, dass sich Unternehmen ihrer eigenen „Cyber-Verwundbarkeit" immer mehr bewusstwerden. Und spätestens, wenn man selbst zum Opfer einer Cyberattacke geworden ist, stellt sich in vielen Betrieben die entscheidende Frage: Wie sichere ich meine IT-Security wirklich verlässlich ab? Oft beschäftigt man sich dann das erste Mal mit aktuellen Technologien und Standards aus dem Cybersecurity-Umfeld, die zunehmend auf dem Vormarsch sind. Dabei kristallisiert sich schnell heraus, dass man den eigenen IT-Security-Flickenteppich nicht nur mit einzelnen Features stopfen möchte, wie man es vielerorts zu Beginn der Corona-Pandemie beobachten konnte. Vielmehr suchen Unternehmen nach kompletten Security-Lösungen, die in ihrem individuellen Fall von A bis Z für Sicherheit sorgen.

Moderne Technologien für moderne Unternehmen

Zu den beliebtesten Fundamenten für eine moderne Security-Infrastruktur zählen SD-WAN und SASE. Unter einem SD-WAN (Software Defined Area Network) versteht man im Grunde ein weit verzweigtes Computernetzwerk, mittels dem zum Beispiel die Standorte eines Unternehmens miteinander verbunden werden können. Ein solcher Zusammenschluss benötigt natürlich ein sehr hohes Sicherheitsniveau, um das Netzwerk sicher vor Angreifern zu machen. Diese Absicherung können in einem SD-WAN beispielsweise softwarebasierte VPN-Lösungen übernehmen. Auf diesem Prinzip baut SASE (Secure Access Service Edge) weiter auf. Bei diesem Architekturkonzept werden WAN-Services und Security-Funktionen direkt zusammen in einer cloudbasierten Komplettlösung kombiniert, was die Einstiegshürde für interessierte Unternehmen merklich senkt.

Durch die aktuelle Bedrohungslage hat zuletzt vor allem ein IT-Security-Konzept immer weiter an Bedeutung gewonnen: Zero Trust. Hier wird die Herangehensweise, nach der Netzwerkinfrastrukturen gewöhnlich aufgebaut sind, komplett umgekehrt. Sämtliche Datenzugriffe folgen bei Zero Trust einem „Least privilege"-Prinzip. Hierbei wird Nutzern und ihren Endgeräten kein blindes Vertrauen mehr ausgesprochen, sondern nur noch Zugriff auf die Daten gewährt, die für die aktuelle Arbeit nötig sind. Um dies zu bewerkstelligen, prüft das System bei jedem Datenzugriff im Hintergrund, ob der Anwender überhaupt zum Zugriff berechtigt ist. Auf diese Weise lässt man

Cyber-Angreifern nur wenig Spielraum, da selbst ein erfolgreicher Angriff nur Zugang zu einem sehr kleinen Teil des gesamten Firmennetzwerks ermöglichen würde. Damit unbefugte Zugriffe jedoch möglichst komplett verhindert werden, muss natürlich insbesondere der Login-Aspekt einer Zero-Trust-Infrastruktur bestens abgesichert sein.

Dabei hat es oberste Priorität, dass bisherige Login-Mechanismen durch Multifaktor-Authentifizierung (MFA) abgelöst werden. Schließlich spielt MFA eine tragende Rolle im Zero-Trust-Prinzip und stellt nicht zuletzt eine der effizientesten Methoden dar, um die eigenen Zugänge effektiv vor Angreifern zu schützen. Dies ist besonders für Ansätze wie Zero Trust, bei denen sich die Anzahl der Passwörter eines Nutzers in Grenzen hält, von großem Nutzen. Gerade im Firmenkosmos erfreuen sich auch komplexere Protokolle wie SAML immer größerer Beliebtheit, mit denen die Verwendung von Anmeldeinformationen für mehrere Webseiten möglich wird. Nach dem Prinzip des Single Sign On (SSO) muss sich der User dann ebenfalls nur ein Passwort merken, mit dem er sich einmal authentifiziert und anschließend – ganz im Sinne des Zero-Trust-Gedanken – auf alle Portale und Webseiten zugreifen kann, die er für seine Arbeit benötigt.

Ein gemeinsamer Nenner

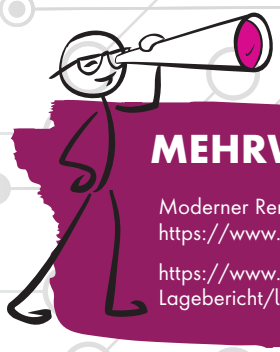
Die moderne Welt der IT-Sicherheit bietet also viele Möglichkeiten, sich vor ungebetenen Gästen zu schützen. Doch bei aller Security darf die tägliche Arbeit der Nutzer nicht durch immer neue Technologien und IT-Anwendungen eingeschränkt werden. Daher suchen Unternehmen nach IT-Security-Lösungen, die fortschrittliche Technik mit einer hohen Usability vereinen. Deshalb sollte im Zuge einer SASE-/Zero-Trust-Strategie zwingend eine moderne Lösung wie die VPN-Technologie von NCP eingesetzt werden.

Der Clou: Die zu 100 Prozent softwarebasierte NCP-Lösung kann sowohl On Premises als auch im Rechenzentrum bei Managed (Software) Service Providern zum Einsatz kommen. Diese Funktionsweise macht die NCP-Produkte von Natur aus cloudfähig, wodurch sie lückenlos in SASE-, SSE-, Zero-Trust- und SD-WAN-Konzepte integriert werden können. Den Ansatz des nutzerbasierten Datei- und Anwendungszugriffs verfolgt NCP zudem bereits seit vielen Jahren. In der Praxis funktioniert dies mithilfe granular definierter Firewall-Regeln. Der Administrator konfiguriert im NCP Secure Enterprise Management (SEM), welchen Nutzern oder Nutzergruppen welche Zugriffsrechte gewährt werden. Ergänzt wird die Lösung durch Funktionen wie Application based Tunneling oder VPN-Bypass, wodurch auch ganze Netzbereiche bei Bedarf am Tunnel vorbeigeleitet werden können. So bleibt beispielsweise eine im Firmennetz befindliche Telefonanlage weiterhin nutzbar, während diese bei einigen Zero-Trust-fähigen Produkten in der Cloud stehen müsste.

Auf diese Weise werden moderne VPN-Lösungen ein wertvoller Teil hochkomplexer Technologiekonzepte wie SASE, SSE oder Zero Trust und liefern gleichzeitig bedeutende Vorteile in Form von anwenderfreundlicher Bedienung und einfacher Administrierung. Firmen sparen sich außerdem mehrere Einzelanwendungen, indem sie eine vielseitige VPN-Lösung als Ergänzung in ihr Sicherheitskonzept einbauen, die ihre individuellen Security-Bedürfnisse erfüllt. So trägt NCP den Gedanken einer modernen, allumfassenden Netzwerksicherheit in modernen Technologien weiter, wodurch am Ende auch OEM-Partner profitieren. Nicht umsonst bezeichnet Aryaka im Zusammenhang mit ihrer SD-WAN-Lösung die VPN-Produkte von NCP als „the industry's most flexible VPN solution."

www.ncp-e.com

Quelle: 1 BSI - Die Lage der IT-Sicherheit in Deutschland 2022



MEHRWERT

Moderner Remote Access von NCP:
https://www.ncp-e.com/de/loesungen/cloud-vpn/

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

Eine Veranstaltung von itsecurity & it-daily.net
Das Online-Portal von itmanagement & itsecurity

SAVE THE DATE

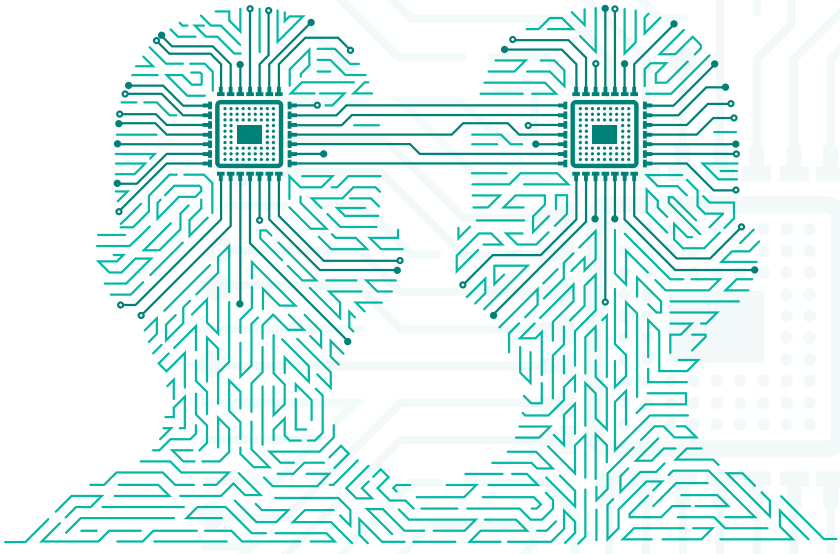
CYBERSECURITY
DIE GEFAHR AUS DEM OFF

Digitalevent
22. März 2023

#cybersec23

SCAN ME

https://www.it-daily.net/cybersecurity/



Cyber-Resilience

UNTERNEHMENSWEITE STRATEGIE ERFORDERLICH

Täglich finden Cyberangriffe statt, die Einfluss auf alle Unternehmensbereiche haben. Managementsysteme für Information Security, Business Continuity, Krisenmanagement und eine technische Absicherung der IT stellen dabei zwar starke Security-Maßnahmen dar, reichen für einen effektiven Rundumschutz jedoch nicht aus. Wie Unternehmen Cyber-Resilience erreichen können und welche besondere Rolle der Faktor Mensch dabei spielt, erläutert Florian Goldenstein, Manager IT Security Consulting & CISO, Konica Minolta Deutschland im Interview.

it security: *Herr Goldenstein, der Begriff Cyber-Resilience ist in aller Munde. Was verbirgt sich konkret dahinter?*

Florian Goldenstein: Cyber-Resilience bedeutet, dass Unternehmen auch in Krisenlagen handlungsfähig bleiben und ihr Geschäft weiterführen können. Das umfasst nicht nur einzelne, sondern sämtliche, für die Unternehmensführung relevante, Geschäftsbereiche und alle Mitarbeitenden. Denn nur, wenn alle an einem Strang ziehen, lässt sich IT-Sicherheit im Unternehmen gewährleisten. Das haben die letzten Jahre gezeigt, die von der Corona-Pandemie, der Finanzmarkt- und Energiekrise und geopolitischen Ereignissen geprägt waren. Im Zuge der Pandemie mussten im Frühjahr 2020 viele Arbeitgeber ihre Mitarbeitenden von jetzt auf gleich ins Homeoffice schicken. Das war für die IT-Abteilungen eine große Herausforderung, denn darauf war niemand vorbereitet. Bis Konzepte und Infrastrukturen an die neuen Anforderungen angepasst werden konnten ist einige Zeit vergangen. Das haben Kriminelle genutzt. Während der Fokus früher auf dem Betrieb der IT-Infrastruktur und weniger auf der Sicherheit lag, ist die Relevanz durch die bestehenden Sicherheitslücken mittlerweile deutlich gestiegen. Doch auch mit zunehmendem Fokus auf Cybersecurity, haben viele Unternehmen in diesem Punkt noch immer Nachholbedarf.

it security: *Wie können IT-Abteilungen ihre Infrastruktur zu einer nachhaltig sicheren IT-Landschaft entwickeln?*

Florian Goldenstein: Das geht nur mit effektiven Cyber-Resilience-Konzepten, die Angriffen auf die Infrastruktur trotzen und einen laufenden Betrieb auch im Angriffsfall ermöglichen. Nur so ist es möglich, Mitarbeitende und Kunden langfristig vor Datenmissbrauch, Industriespionage oder Malware zu schützen. Neben der passenden Sicherheitsstruktur und einer aktuellen Hardware spielt dabei auch der Faktor Mensch eine wichtige Rolle.

it security: *Was sind die wichtigsten Bestandteile dieser Konzepte?*

Florian Goldenstein: Cyber-Resilience ist eine Prozesskette aus fünf Phasen: „Identifizieren", „Schützen", „Detektieren", „Reagieren" und „Wiederherstellen". Im Rahmen eines Managementsystems kommt noch die „Kontinuierliche Verbesserung" hinzu. Sie rundet das Thema mit Lernprozessen ab. Diese Phasen müssen geplant und auf die Anforderungen der Informationssicherheit, die Unternehmensziele sowie die Geschäftsstrategie und das Risiko einer

PLUS

Im Whitepaper „Update für die menschliche Firewall" zeigt Konica Minolta anhand von Praxisbeispielen, wie wichtig Sensibilität für Informationssicherheit ist und wie Unternehmen mit „Security by Design" den Grundstein für eine gelungene Digitalisierung legen.

www.konicaminolta.de/sensibilisierung

außerplanmäßigen Betriebsunterbrechung ausgerichtet werden.

it security: *Wie integrieren Unternehmen solche Cyber-Resilience-Konzepte?*

Florian Goldenstein: Im Idealfall ist Cyber-Resilience ein Managementsystem, das stetig verbessert wird. Basis hierfür ist eine unternehmensweite Strategie, die durch das Risikomanagement gestützt ist und von sämtlichen Mitarbeitenden auf allen Hierarchieebenen getragen wird. Ein solches Managementsystem funktioniert aber nur dann, wenn ein organisatorischer, technischer und verhaltensorientierter Dreiklang besteht.

it security: *In den letzten Jahren waren Mitarbeitende häufig das erste Ziel einer Attacke. Welche Gründe gibt es Ihrer Meinung nach hierfür?*

Florian Goldenstein: Das liegt an zwei Faktoren: Einerseits mussten sie in vielen Unternehmen innerhalb kürzester Zeit den Umgang mit neuen Technologien, Arbeitsweisen und Prozessen lernen. Das hat einige überfordert, andere waren dadurch oftmals unachtsam. Außerdem ist vielen Mitarbeitenden nicht umfassend bewusst, dass das Thema Informationssicherheit auch sie betrifft – und zwar in vielen Situationen am Arbeitsplatz. Nicht jeder widersteht der Versuchung, einen herumliegenden USB-Stick in den Port seines Rechners zu stecken. Eine vermeintlich vom Vorgesetzten verschickte, „dringende" E-Mail wird ebenso schnell geöffnet. Man muss die alltäglichen Prozesse sehr genau überdenken, um Cyberangriffen keine Chance zu geben. Deshalb ist es so wichtig, die Menschen im Unternehmen für das Thema zu sensibilisieren und einen unachtsamen Umgang der Mitarbeitenden mit Daten zu verringern. Vor diesem Hintergrund haben Cyber-Schulungen eine elementare Bedeutung, da letztlich alle

CYBER-RESILIENCE BEDEUTET, DASS UNTERNEHMEN AUCH IN KRISENLAGEN HANDLUNGSFÄHIG BLEIBEN UND IHR GESCHÄFT WEITERFÜHREN KÖNNEN.

Florian Goldenstein, Manager IT Security Consulting & CISO, Konica Minolta Deutschland, www.konicaminolta.de

im Unternehmen die Grundlagen der Informationssicherheit kennen und täglich leben müssen.

it security: *Stichwort „Social Engineering": Die Methoden der Bedrohungsakteure, um das Vertrauen von Personen zu erlangen und letztlich auszunutzen, sind hoch professionell. Wo liegen die Angriffsvektoren?*

Florian Goldenstein: Kriminelle machen sich menschliche Züge wie Hilfsbereitschaft, Angst oder Pflichtbewusstsein zunutze. Das funktioniert im Bereich Spear-Phishing sehr effektiv. Es handelt sich dabei um den gezielten Versand einer E-Mail, die zum Anklicken eines Links, zur Eingabe von Passwörtern oder dem Preisgeben von Informationen auf einer fingierten Oberfläche auffordern. Ebenfalls kommt Telefon-Spoofing häufig zum Einsatz. Dabei rufen Kriminelle Mitarbeitende an und fälschen die übermittelte Rufnummer. Der Effekt: Die angerufene Person geht davon aus, dass der Anruf aus dem eigenen Unternehmen käme und gibt im Gespräch vertrauliche Informationen preis.

Seit langem aktuell und immer wiederkehrend ist der CEO-Fraud: Hierbei werden gezielt ausführende Personen eines Unternehmens angegriffen. Kriminelle geben sich als Führungskräfte oder Management einer Firma aus. Um einen vorgeblichen Geschäftsablauf nicht zu behindern, bitten sie um Reaktion und weisen auf die Dringlichkeit hin. Das kann beispielsweise eine eilig zu tätigende Express-Überweisung sein. Deshalb ist es so wichtig, zu sensibilisieren und auf allen Ebenen zu trainieren.

it security: *Reichen Schulungen und Trainings für einen wirksamen Schutz aus?*

Florian Goldenstein: Die menschliche Firewall ist die wichtigste im Unternehmen. Hierzu bieten wir die Mitarbeiter-Sensibilisierung „as a Service" an, um auch die menschliche Firewall regelmäßig zu trainieren. Sie darf aber nicht die einzige Maßnahme zur Gefahrenabwehr darstellen. Wir unterstützen unsere Kunden daher aktiv mit Managed Services, die viele Bereiche und auch Security abdecken, beispielsweise mit Monitoring, Patch-Management oder Backups. Zudem bieten wir auch Managed Firewalls und Endpoint Protection an, denn die Sicherheit der Endgeräte – an jedem Ort – ist ein zentrales Thema. Damit legen wir den Grundstein für sichere hybride Arbeitsmodelle und eine sichere Unternehmens-IT.

it security: *Herr Goldenstein, wir danken für das Gespräch.*

THANK YOU

IT-Security-Trends

WAS 2023 WICHTIG WIRD

DURCH DIE DIGITALE TRANSFORMATION SIND DATEN HEUTE DAS WERTVOLLSTE GUT DAS UNTERNEHMEN BESITZEN, GLEICHZEITIG SIND DIE DATEN GRÖSSEREN RISIKEN AUSGESETZT ALS JEMALS ZUVOR.

Audra Simons, Senior Director of Global Products, Global Governments and Critical Infrastructure, Forcepoint, www.forcepoint.com

Die Finanzbranche rüstet sich gegen synthetischen Betrug, die aktuellen Krisen produzieren neue Insider-Risiken und Unternehmen wollen die IT-Sicherheit vereinfachen: Diese Trends werden die IT-Security im Jahr 2023 und darüber hinaus prägen.

Synthetische Identitätsdiebstähle nehmen weiter zu. Bei dieser Methode kombinieren Kriminelle gestohlene Informationen mit gefälschten persönlichen Angaben und erschaffen daraus betrügerische Identitäten, mit denen sie Konten eröffnen, Kredite beantragen und im Internet einkaufen. Um dieses Problem in den Griff zu bekommen, werden Banken, Kreditgeber und Gläubiger künftig von den Antragstellern Scans oder Fotos ihrer Pässe oder Ausweise verlangen müssen, um damit ihre Identitäten zu verifizieren. Dabei handelt es sich um Millionen von Dokumenten, die sie online entgegennehmen – und jedes dieser Dokumente ist ein potentieller Träger von Schadsoftware.

Bei der Abwehr dieser Gefahr kann ihnen die neuartige Sicherheitstechnologie Zero Trust Content Disarm and Reconstruction (CDR) helfen, die einen ganz anderen Ansatz verfolgt als herkömmliche Systeme wie Firewalls, Virenscanner oder Sandboxes. Sie durchsuchen Dokumente anhand von Signaturen nach Schadsoftware und finden deshalb nur bösartigen Programmcode den sie bereits kennen. Da Cyberkriminelle ihre Malware permanent modifizieren, sind sie immer einen Schritt voraus. Sobald eine neue Variante bekannt wir, aktualisieren IT-Sicherheitsanbieter zwar ihre Systeme, aber in diesem Zeitfenster gelingt es Angreifern immer wieder, ihre Schadsoftware an den Sicherheitssystemen vorbeizuschmuggeln.

Zero Trust CDR geht davon aus, dass grundsätzlich kein Dokument vertrauenswürdig ist und sucht deshalb erst gar nicht nach Malware. Stattdessen extrahiert sie aus den Dokumenten die Informationen, bei denen schädliche Inhalte garantiert ausgeschlossen sind und erstellt daraus in Sekundenschnelle neue, voll funktionsfähige Dateien, die vollständig frei von ausführbarem Code sind und dadurch auch keine Schadsoftware enthalten können. Zero Trust CDR alleine wird synthetischen Identitätsbe-

trug natürlich nicht gänzlich verhindern können. Aber es kann zumindest dafür sorgen, dass die zur Verifizierung von Identitäten gesammelten Dokumente sicher sind.

Politische Verhärtung erhöht Insider-Risiken

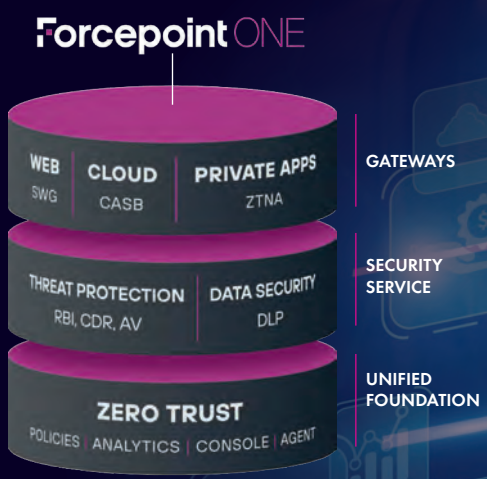
Die aktuellen Krisen führen zu einer zunehmenden Politisierung von Bürgern. Desinformationen haben dabei sogar teilweise eine regelrechte Verhärtung der Positionen und eine Radikalisierung zur Folge. Für Unternehmen entstehen daraus neue potenzielle Risiken durch Innentäter. Mitarbeiter könnten aus politischen Motiven heraus versuchen, geistiges Eigentum zu stehlen oder sensible Informationen zu exfiltrieren.

Um dieser neuen Herausforderung zu begegnen, werden Unternehmen Systeme für eine kontinuierliche Verhaltensüberwachung einführen. Der Schlüssel zum Erfolg liegt dabei in der Flexibilität der Systeme. Das Verhalten der Mitarbeiter kann sich im Lauf der Zeit ändern. Je nachdem, wie sich ihre Ansichten und Überzeugungen entwickeln, können sie nach und nach zu einem Sicherheitsrisiko werden. Die Systeme zur Überwachung von Insider-Risiken müssen flexibel genug sein, solche manchmal schleichenden Entwicklungen zu registrieren. Sie sollten es Unternehmen ermöglichen, Schwankungen in den Verhaltensmustern von Nutzern zu überwachen und mit ihrem Ausgangsverhalten zu vergleichen.

Aktuell werden solche Systeme hauptsächlich dazu verwendet, um festzustellen, ob ein Nutzer auf ungewöhnliche Weise auf Informationen zugreift. Angesichts der neuen Insider-Risiken werden Unternehmen sie künftig aber dafür einsetzen, ungewöhnliche Verhaltensmuster zu erkennen, die weit über den Zugriff auf Unternehmensdaten und -systeme hinausgehen. Mit kontinuierlicher Verhaltensüberwachung können sie beispielsweise feststellen, ob sich ein Nutzer von seinen Kollegen oder seiner Arbeit abwendet, oder ob er anfängt, ungewöhnlich große Datenmengen zu horten. Solche Erkenntnisse können Hinweise darauf liefern, dass ein User ein potenzielles Insider-Risiko darstellt. Selbstverständlich müssen solche Systeme mit den Betriebsräten abgestimmt sein. Zudem müssen sie durch eine anonymisierte Erfassung der Nutzerdaten für Datenschutzkonformität sorgen.

Unternehmen transformieren ihre IT-Sicherheit

Zur Bereitstellung von Anwendungen nutzen Unternehmen zunehmend hybride Multi-Cloud-Umgebungen, die mehrere Public Clouds, Private Clouds und On-Premises-Installationen kombinieren. Mit herkömmlichen IT-Sicherheitsarchitekturen können sie den Schutz dieser komplexen Landschaften nicht effizient managen. Diese Architekturen sind in der Regel ein Flickenteppich aus losgelösten Insellösungen, die von verschiedenen Anbietern stammen und separate Managementoberflächen mit eigener Logik haben. Die Folge ist nicht nur eine komplizierte und aufwändige Verwaltung, sondern auch Inkonsistenz. Sicherheitsteams können häufig keine identischen Sicherheitsrichtlinien einrichten und müssen sich mit Policies zufriedengegen, die lediglich ähnlich sind.



Unternehmen werden 2023 verstärkt auf integrierte All-in-One-Plattformen für IT-Sicherheit setzen. (Quelle: Forcepoint).

Unternehmen werden deshalb daran gehen, ihre IT-Sicherheit zu transformieren und auf integrierte, Cloud-basierte All-in-One-Plattformen aus der Hand eines einzigen Anbieters umsteigen. Mit solchen Komplettlösungen können sie künftig sämtliche Vorgaben mit einem einzigen Satz an Sicherheitsrichtlinien über die komplette IT-Landschaft hinweg durchsetzen und in einer einzigen Managementkonsole zentral verwalten. Dabei werden sie verstärkt auf Plattformen setzen, die einen datenzentrierten Ansatz verfolgen. Durch die digitale Transformation sind Daten heute das wertvollste Gut das Unternehmen besitzen, gleichzeitig sind die Daten durch hybride Arbeitsmodelle, mobiles Arbeiten und BYOD größeren Risiken ausgesetzt als jemals zuvor.

Diese Anforderungen machen Data Loss Prevention (DLP) zu einer Schlüsseltechnologie. DLP-Lösungen sind in der Lage, schützenswerte Informationen zu identifizieren und Aktionen mit hinterlegten Richtlinien abzugleichen. Registrieren sie Verstöße gegen die Vorgaben, machen sie die Mitarbeiter darauf aufmerksam. Moderne adaptive Systeme reagieren dabei jedes Mal mit Schutzmaßnahmen, die dem Kontext angemessen sind. So verhindern sie den ungewollten Abfluss von Daten, ohne die Produktivität der Mitarbeiter unnötig einzuschränken. Deshalb werden vor allem IT-Security-Plattformen erfolgreich sein, die Technologien Secure Web Gateway (SWG), Cloud Access Security Broker (CASB), Advanced Threat Protection (ATC) und Zero-Trust-Funktionen mit DLP integrieren. Solche Komplettlösungen ermöglichen es Unternehmen, ihre Daten über sämtliche Anwendungen und Endgeräte inklusive BYOD-Geräte hinweg zu schützen.

Audra Simons

IT-Sicherheit 2023

MASSNAHMEN GEGEN CYBERERPRESSUNG

Gute Vorbereitung ist das A und O im Kampf gegen Cyberkriminalität. Dabei stehen Unternehmen auch in diesem Jahr wieder vor einigen Herausforderungen. Denn IT-Strukturen werden in Zeiten zunehmender Digitalisierung immer vielseitiger, komplexer und damit auch anfälliger für Cyberangriffe.

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) zeigte erst kürzlich im Lagebericht zur IT-Sicherheit 2022 schwarz auf weiß: Die IT-Sicherheitslage spitzt sich zu – die Gefahr, Opfer von Cyberangriffen zu werden, war noch nie so hoch wie jetzt.

Ransomware stellt dabei die größte Bedrohung für die IT-Sicherheit deutscher Unternehmen dar. Die Trends für die IT-Sicherheit 2023 weisen deshalb gezielt auf Maßnahmen gegen Cybererpressung hin.

Hier sind die sieben wichtigsten Entwicklungen, die Unternehmen zum Thema IT Security für 2023 im Blick behalten sollten:

#1 Kritische Infrastruktur im Fokus

Ein Blick in die Medienlandschaft zeigt: Kritische Infrastrukturen sind immer häufiger das Ziel von Cyberattacken. Aktuell weist nichts darauf hin, dass beispielsweise Angriffe auf das Gesundheitswesen oder die Energieversorgung 2023 abnehmen werden. Im Gegenteil: Sie werden häufiger und gezielter.

Der Grund ist ein Trend hin zu „Cybercrime as a Service" (CaaS). Besonders „Ransomware as a Service", also Erpressersoftware, die für Attacken vermietet wird, wird immer häufiger für präzise Angriffe auf lukrative Ziele eingesetzt. Die kritische Infrastruktur ist dabei besonders anfällig und schutzbedürftig.

#2 Neue Regulierungen implementieren

In den vergangenen Jahren wurden national und international einige Gesetze und Regulierungen auf den Weg gebracht, bei denen jetzt die Umsetzungsphase beginnt. Dazu gehören zum Beispiel:

- die NIS-2-Richtlinie für EU-Mitgliedsstaaten mit strengeren Überwachungsmaßnahmen und Meldepflichten
- der Gesetzesentwurf zum European Cyber Resilience Act (CRA) für die Cybersicherheit internetfähiger Geräte und Produkte
- die EU-Verordnung zur Radio Equipment Directive (RED), die zur Cybersicherheit bei allen Wireless-Geräten (Smartphones, Tablets oder Smartwatches) verpflichtet

Dabei gilt: Selbst ist die Frau oder der Mann. Unternehmen müssen auf eigene Faust prüfen, ob sie betroffen sind. Falls

ja, müssen sie überlegen, wie sie ihre IT-Sicherheit möglichst effizient und kostengünstig anpassen können.

#3 Mehr Cyber Resilienz: Widerstandsfähigkeit stärken

Der Begriff Cyber Resilienz drückt aus, wie widerstandsfähig ein Unternehmen gegen Attacken von Cyberkriminellen ist – und ob es handlungsfähig bleibt, selbst wenn die Attacke erfolgreich ist. Es geht also um einen Notfallplan, der die sogenannte Business Continuity aufrecht und die wirtschaftlichen sowie finanziellen Verluste in Grenzen hält.

Grundlage für eine gute Cyber Resilienz ist es, dass alle im Unternehmen die Bedrohungen und eigenen Schwächen verstehen. Unternehmen können an diesem Punkt zum Beispiel mit IT-Notfallplänen und Übungsszenarien (Disaster-Recovery-Tests) effektiv vorsorgen. Reaktionen auf Angriffe sollten geplant und immer wieder geübt werden, sodass im Ernstfall alle Mitarbeiter und Mitarbeiterinnen vorbereitet sind.

#4 Zero Trust wird zum Must-have

Das Zero-Trust-Modell an sich ist nicht neu. Neu ist, dass Zero Trust durch den Fokus auf Homeoffice und Software as a Service zum neuen Standard und Must-have für Unternehmensnetzwerke wird. IT-Analysten und -Analystinnen sind sich dabei einig, dass Zero Trust künftig der einzig funktionierende Sicherheitsansatz sein wird. Unternehmen mit ausgereiftem Zero-Trust-Konzept sind deutlich besser in der Lage, Bedrohungen zu erkennen und darauf zu reagieren. Es findet also ein Paradigmenwechsel statt, der sich erheblich auf die IT-Sicherheitsarchitektur von Firmen auswirkt.

Das Zero-Trust-Modell basiert auf dem Grundsatz „never trust, always verify". Das heißt, alle Geräte, Dienste, Benutzer und Benutzerinnen – egal ob intern oder extern – werden grundsätzlich mit Misstrauen behandelt. Netzwerke müssen nicht mehr nur nach außen, also an den Netzwerkgrenzen, abgesichert werden. Sicherheitssysteme werden im gesamten Netzwerk benötigt.

Für IT-Sicherheitsverantwortliche bedeutet das, dass sie 2023 auf mehrschichtige Zero-Trust-Architekturen für Datenschutz und Cybersicherheit umstellen sollten. Dafür die technischen Weichen im Unternehmen zu stellen, kann herausfordernd und zeitintensiv sein. Eine Cloud-basierte Zero Trust Platform wie zum Beispiel von DriveLock, die mit Endpoint Security und Endpoint Protection Unternehmensdaten, Endgeräte und IT-Systeme nach modernsten Standards schützt, vereinfacht die Umstellung erheblich.

#5 Sicherheitsrisiken automatisch priorisieren

Cyber Resilienz erfordert auch eine neue Denkweise im Umgang mit Schwachstellen in der IT-Sicherheit. Es ist wichtig, dass Unternehmen im ersten Schritt alle Sicherheitslücken kennen. Um zu wissen, wo welche Gefahren lauern, sind regelmäßige Penetrationstests, laufendes Patch-Management und kontinuierliche Checks durch IT-Sicherheitsexperten und -expertinnen eher Pflicht als Kür.

Sind die Gefahren bekannt, versuchen viele Unternehmen, alle Probleme gleichzeitig zu lösen. Das ist aber nicht (mehr) zielführend. Der Trend geht stattdessen zu einem modernen Schwachstellenmanagement, das Sicherheitslücken automatisch analysiert und vor allem priorisiert. So ist der Blick immer auf die Schwachpunkte gerichtet, von denen die größte Gefahr ausgeht.

Eine solche risikobasierte Priorisierung bietet einen deutlich besseren Schutz

Foto: istockphoto/metamorworks

TOP 3-BEDROHUNGEN JE ZIELGRUPPE

Staat & Verwaltung
Ransomware
APT
Schwachstellen
Offene oder falsch konfigurierte Online-Server

Wirtschaft
Ransomware
Schwachstellen
Offene oder falsch konfigurierte Online-Server
IT-Supply-Chain

Gesellschaft
Identitätsdiebstahl
Sextortion
Fake-Shops im Internet

Quelle: bsi.bund.de

gegen Cyberkriminelle – erfordert aber auch eine grundlegend neue Vorgehensweise und die Unterstützung von erfahrenen Cybersecurity-Experten und -Expertinnen

#6 Mit smarten Tools gegen den Fachkräftemangel

Immer mehr Sicherheitsteams haben mit personellen Problemen zu kämpfen. Der IT-Fachkräftemangel wird immer sichtbarer: Eine aktuelle Bitkom-Studie zeigt, dass in Deutschland aktuell 137.000 IT-Experten und -Expertinnen fehlen. Das sind rund 10 Prozent mehr als 2019. Bei der Cybersicherheit ist die Personallücke verglichen mit 2021 sogar um fast 53 Prozent gewachsen. Das Ergebnis: überlastete und unterbesetzte IT-Sicherheitsteams, die zwangsläufig Fehler machen und weniger gut für Angriffe gerüstet sind. Vor allem kleinere und mittlere Unternehmen geraten verstärkt ins Visier von Cyberkriminellen.

In Zukunft werden Verantwortliche für die IT-Sicherheit Technologien neu bewerten und nach umfassenden Lösungen suchen müssen, mit denen sie ihre Prozesse effizienter machen können. Es braucht Tools und Plattformen, die viele Aufgaben automatisiert übernehmen und damit dünn besetzten Teams den Rücken freihalten. Der Security Service von DriveLock beispielsweise ist von Experten:Innen gemanagt, sofort einsatzbereit, ressourcenschonend, individualisierbar und maximal sicher.

#7 Anwendungsfreundliche Security in der Cloud

IT-Umgebungen werden in unserer hybriden Arbeitswelt mit verschiedensten Endgeräten, Videochats und Remote Work immer komplexer. Mehr und mehr Services wandern von On-Premises in die (Hybrid) Cloud. Viele Unternehmen werden 2023 ihre bisherige IT-Infrastruktur evaluieren und einsatzbereite Cloud-native Technologien noch mehr und vor allem strategischer einsetzen.

Mit diesem Wandel steigen auch die Anforderungen an die IT-Sicherheit. Cloud-basierte Services erfordern besondere Schutzmaßnahmen wie Confidential Computing oder hybride Firewalls. Die Kunst dabei: maximale Sicherheit für alle Geräte innerhalb eines Netzwerks zu garantieren, ohne dass die Cybersecurity-Lösungen die Nutzer:Innen im Arbeitsalltag behindern.

DriveLock hat sich Nutzerfreundlichkeit groß auf die Fahnen geschrieben und arbeitet kontinuierlich daran, die tägliche Nutzung der Lösung für Admins sowie Anwender:Innen zu vereinfachen. Zum Beispiel mit einem Self-Service-Portal, mit intelligenter Applikationskontrolle oder durch die Integration von Microsoft BitLocker Management in DriveLock.

www.drivelock.com

PLUS

IT-Sicherheit in kritischen Infrastrukturen
Lesen Sie mehr dazu in unserem Whitepaper
https://www.drivelock.com/de/lp-wp-kritis

Sicher arbeiten vom Bilderbuchstrand

SECURITY-AWARENESS-MANAGEMENT IM DIGITALEN ZEITALTER

Bei Sonnenaufgang mit nackten Füßen über lauwarmen Sand schreiten und anschließend vom klimatisierten Co-Working-Space die Kollegschaft im Online-Meeting begrüßen. Traumhaft, oder?

Im Windschatten der Pandemie locken viele Hotels mit höhenverstellbaren Tischen, Highspeed-Internet und Meerblick. Ein Paradigmenwechsel des modernen Arbeitens, „New Work". Neben Selbstverwirklichung und Potenzialentfaltung rücken auch Informationssicherheitsrisiken in den Mittelpunkt. Kritisch sind Zugriffe auf Kundschaftsdaten oder Firmennetzwerke über ungesichertes WiFi.

Schockierende 71 Prozent der befragten Führungskräfte aus der Informationssicherheit gaben in einer Forrester-Umfrage an, sie hätten nur einen geringen oder gar keinen Einblick in die Absicherung der Remote-Arbeitsplätze ihrer Angestellten.

Informationssicherheit muss Teil der Unternehmensphilosophie werden. Der erste Schritt zur Absicherung der Remote-Workforce ist eine Zero-Trust-Sicherheitsarchitektur. Dabei werden jegliche Zugriffsversuche von allen Geräten, Anwendungen, Netzwerken und Usern überwacht.

Ein weiterer Eckpfeiler ist ein kompetentes Security-Awareness-Management. Der Phishing-Attack-Simulator von Increase Your Skills beispielsweise hilft Unternehmen dabei, Angestellte gegen Social Engineering-Angriffe widerstandsfähig zu machen. Zur Auswahl stehen verschiedene, individuell erstellte Angriffsszenarien oder bereits vorhandene branchenspezifische Szenarien. Das Reporting-Modul wertet die Daten aus und gibt Aufschluss über den aktuellen Stand. Somit werden nicht nur Schwachstellen im Unternehmen analysiert, sondern langfristig auch sensible Unternehmensdaten und finanzielle Werte geschützt.

Mehr Infos und weitere Produkte für ein höheres Schutzniveau finden Sie unter:
https://increaseyourskills.com/

Praxisbuch ISO/IEC 27001
– Management der Informationssicherheit und Vorbereitung auf die Zertifizierung, Michael Brenner u.a.; Carl Hanser Verlag GmbH & Co. KG; 11-2022

PRAXISBUCH ISO/IEC 27001

MANAGEMENT DER INFORMATIONSSICHERHEIT UND VORBEREITUNG AUF DIE ZERTIFIZIERUNG

Informationen zählen zum wertvollsten Kapital vieler Unternehmen. Egal ob Kunden-, Lieferanten-, Produkt-, Produktions- oder Mitarbeiterdaten – gerät davon etwas in falsche Hände, ist oft das Überleben des Unternehmens gefährdet. Wenn Sie in Ihrem Unternehmen Verantwortung für Informationssicherheits-Themen übernehmen, müssen Sie sich mit der ISO/IEC 27001 auseinandersetzen. Ein dieser Norm entsprechendes Informationssicherheits-Managementsystem ist zunehmend Voraussetzung für die Erfüllung von Kunden-Anforderungen sowie gesetzlicher und behördlicher Vorgaben, unter anderem im Rahmen des IT-Sicherheitsgesetzes.

In diesem Buch erhalten Sie die optimale Unterstützung für den Aufbau eines wirksamen Informationssicherheits-Managementsystems. Die Autoren vermitteln zunächst das notwendige Basiswissen zur ISO/IEC 27001 sowie zur übergeordneten Normenreihe ISO/IEC 27000 und erklären anschaulich die Grundlagen von Informationssicherheits-Managementsystemen.

Im Hauptteil des Buches finden Sie alle wesentlichen Teile der DIN ISO/IEC 2700:2022. Die Autoren geben Ihnen hilfreiche Erläuterungen dazu und wertvolle Praxistipps, die Ihnen bei der Umsetzung der Norm in Ihrem Unternehmen helfen.

IT-Security Herausforderungen 2023

KOMPLEXITÄT WÄCHST WEITER

IDC hat im September 2022 branchenübergreifend Security-Verantwortliche befragt, um detaillierte Einblicke in die Herausforderungen beim Aufbau und Betrieb von IT-Security-Konzepten zu erhalten. Man stellte fest, dass die Komplexität der Sicherheits-Lösungen im zweiten Jahr in Folge am häufigsten als Herausforderung genannt wurde. Deshalb ist es wichtig, bei der Auswahl von IT-Partnern auf die Kompatibilität der ausgewählten Lösungen zu achten, denn Stand-Alone-Lösungen erhöhen den Administrationsaufwand und senken die Effizienz.

Fachkräftemangel ist Engpassfaktor

Fast zwei Drittel der Befragten verzeichnen bereits einen akuten Security-Fachkräftemangel, oder erwarten diesen für das kommende Jahr. Deshalb sind Lösungen bei IT-Teams beliebt, die den Administrationsaufwand komplexer Netzwerke reduzieren. Florian Renner, Chief Information Officer, ist für alle Netzwerkthemen bei Hagleitner Hygiene International GmbH verantwortlich. Die besondere Herausforderung seiner Aufgabe liegt im ständigen Wandel und wachsender Komplexität des expandierenden Unternehmens mit den bekannten Herausforderungen an Zugangskontrolle und zeitfressender Administration des Endgeräte-Managements im Netzwerk. Renner: „Durch den Einsatz von macmon Network Access Control können wir in unserem Team zwischen 5 bis 10 Prozent Arbeitszeit einsparen. Und da der Faktor Zeit bei uns der limitierende Faktor ist, stellt das für unser Team einen signifikanten Mehrwert dar."

PLUS

Anwenderberichte aus der Praxis: **www.macmon.eu/loesungen/kunden**

Industrie erwartet Anstieg der Cyber-Angriffe

Mehr als die Hälfte der Befragten der IDC-Studie ist besorgt über die aktuelle Risikolage. 43 Prozent der Betriebe verzeichneten in den letzten 12 Monaten eine Zunahme der Cyberangriffe und für die Zukunft erwarten 51 Prozent einen weiteren Anstieg. 47 Prozent der befragten Organisationen passen wegen der geopolitischen Folgen des Ukraine-Kriegs ihre Cyberbereitschaft und -verteidigung an. Gut wer vorausschauend gehandelt hat und, wie der Schokoladenhersteller Ritter Sport, bereits sein Netzwerk absichert. Allein in der Firmenzentrale arbeiten über 1.000 Mitarbeiter, insgesamt rund 1.700 Menschen an neun Standorten, deren Endgeräte und ihre Aktivitäten im Firmennetzwerk sicher überwacht werden müssen, denn die Prozesse rund um die Produktion müssen reibungslos funktionieren. Michael Jany, Teamleitung Infrastruktur und Security: „Ziel unseres NAC-Projektes war eine komplette und sichere Überwachung und die Gewährleistung der Basissicherheit des Firmen-Netzwerkes, bei 3.400 Netzwerkknoten eine zentrale Aufgabe, um den IT-Betrieb störungsfrei zu managen.

KRITIS sollen in Zukunft besser geschützt werden

Energie, Trinkwasser, das Verkehrssystem - diese Bereiche zählen zur kritischen Infrastruktur. Die Bundesregierung hat sich zum Ziel gesetzt, diese stärker zu schützen. Zu diesem Zweck hat das Bundeskabinett im Dezember 2022 die Eckpunkte des sogenannten KRITIS-Dachgesetzes verabschiedet. Mit dem Gesetz will die Bundesregierung auf Vorfälle in den vergangenen Monaten reagieren. Außerdem sollen dadurch die Vorgaben der Richtlinie zur Resilienz kritischer Einrichtungen (CER) umgesetzt werden. Die CER-Richtlinie ist als Komplementärgesetzgebung zur ebenfalls überarbeiteten Netzwerk- und Informationssicherheits-Richtlinie (NIS2) angelegt, die Cybersicherheits-Vorgaben für kritische Infrastrukturen neu fasst und ebenfalls im kommenden Jahr in deutsches Recht umgesetzt werden soll.

Finanzwesen & Versicherungen

Banken, Kreditinstitute, Finanzdienstleister und Versicherungsunternehmen gehören zu den Institutionen mit den höchsten Anforderungen an die Informationssicherheit. Die wachsende Verwundbarkeit und Gefahr erhöht den Handlungsdruck für ein aktives IT-Sicherheitsmanagement im Finanz- und Versicherungswesen. Cyberexperten und Bankaufseher befürchten infolge des Ukraine-Krieges verstärkt Attacken

russischer Hacker auf Finanzinstitute. In gut jedem dritten Fall kämen Schadprogramme zum Einsatz, mit denen Hacker Computer und Daten verschlüsseln und Geld verlangen, um sie wieder freizugeben. Jeder zweite erpresste Finanzdienstleister hat bereits einmal Lösegeld gezahlt, zeigen Analysen des britischen IT-Anbieters Sophos. Im Durchschnitt wird ein Lösegeld von mehr als 800.000 Dollar fällig – üblicherweise zu begleichen in Bitcoins. Die meisten Banken und Finanzinstitute arbeiten heute mit hybriden Lösungen, einem Mix aus traditionellen IT-Systemen und Cloud-Applikationen. Die Kombination von NAC und Secure Defined Perimeter (SDP) bietet dafür einen optimalen Schutz, eine hohe und globale Verfügbarkeit, flexible und anpassbare Umsetzung von Compliance Vorgaben und die Erfüllung von Nachweispflichten gemäß ISO, PCI oder auch DSGVO-Vorgaben.

Öffentliche Verwaltungen im Visier von Datendieben

Behörden beherbergen eine Fülle an sensiblen Daten. Gleichzeitig müssen diese flexibel für die verschiedenen Fachverfahren nutzbar sein – auf unterschiedlichen Geräten und an multiplen Standorten. In einer Kommunalverwaltung arbeitet man mit äußerst sensiblen persönlichen Daten der Einwohner, die ein lukratives Ziel für Cyberkriminelle darstellen. Allein die Stadtverwaltung Bochum verzeichnet nach eigenen Angaben täglich 10.000 Angriffsversuche auf die Computersysteme der Verwaltung.

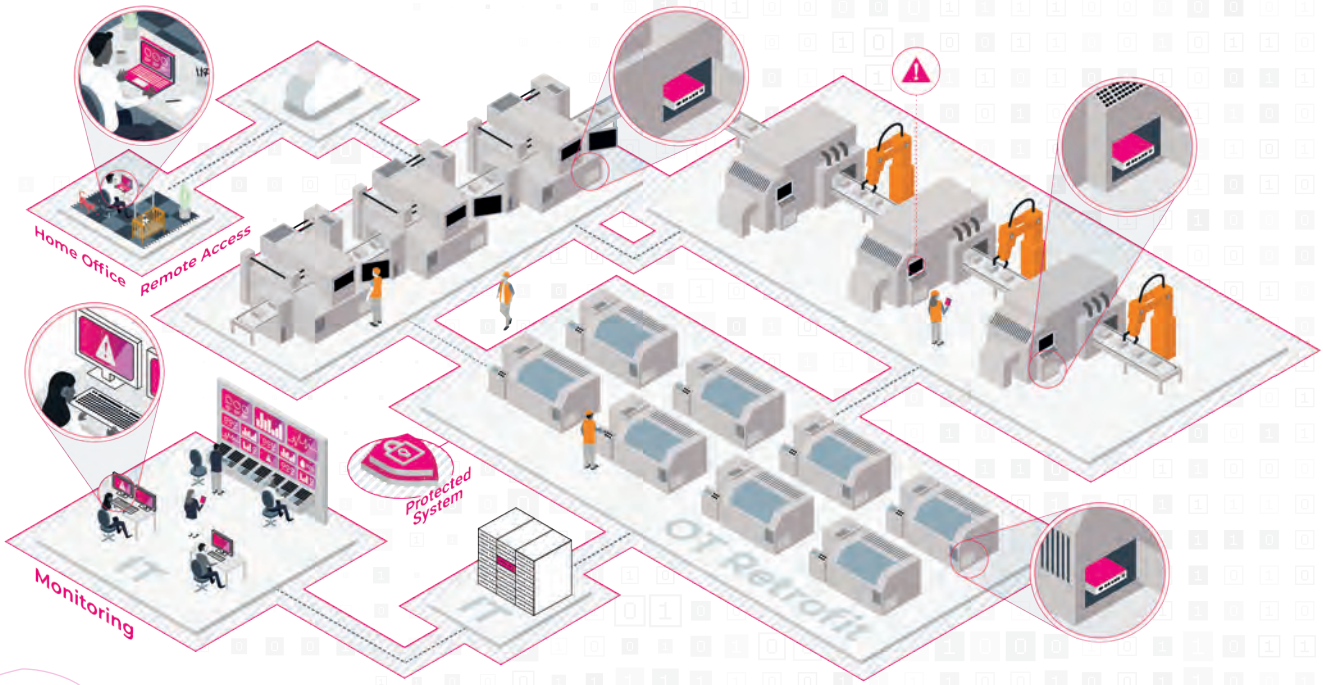
Ebenfalls finden sich in den Netzwerken der Behörden Informationen zu kritischen Infrastrukturen, wie Daten der Energieversorger oder des öffentlichen Transportwesens. Durch den Einsatz einer NAC-Lösung wissen IT-Administratoren jederzeit, welche Geräte sich im Netzwerk befinden, können sie effizient und komfortabel überwachen und kontrollieren.

Bei der Auswahl einer NAC-Lösung bietet sich eine herstellerunabhängige Sicherheitslösung an, die eine zuverlässige Überwachung auch von Netzen mit unterschiedlichsten Netzwerkkomponenten bietet.

ZTNA - Vertraue niemandem, verifiziere jeden

Die ZTNA-Philosophie bietet den Rahmen für einen intelligenten und einfachen Schutz für Netzwerke und Cloud. techconsult veröffentlichte im Juli 2022 eine mit macmon secure erstellte Studie über Cyber-Security in deutschen Unternehmen: So geben 46 Prozent der Unternehmen an, in den nächsten zwei Jahren Zero Trust einzuführen. Durch Diebstahl, Spionage und Sabotage entsteht der deutschen Wirtschaft jährlich ein Gesamtschaden von 223 Milliarden Euro, die Dunkelziffer ist hoch. Homeoffice und Digitalisierung bieten neue Angriffsmöglichkeiten, ganzheitliche Sicherheitskonzepte mit NAC und SDP sind deshalb notwendig. Das Konzept basiert auf Restriktion und Monitoring. Zusätzlich zur Sicherung lokaler Netzwerke wird der Schutz auf sämtliche Cloud-Dienste ausgeweitet. Im Unterschied zu klassischen VPNs authentifizieren sich bei Secure Defined Parameter (SDP) sowohl der Benutzer als auch der Agent am Controller. 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.

Christian Bücker | www.macmon.eu



IT-Sicherheitsgesetz

WIE DER INDUSTRIELLE MITTELSTAND PROFITIEREN KANN

Unternehmensprozesse werden nicht nur komplexer, sie werden auch digitaler. So ist die Kommunikation zwischen Maschinen inzwischen eher die Regel als die Ausnahme. Das Problem: Wachsende Ansprüche an die Cybersicherheit überfordern viele Unternehmen. Laut der Studie „Cybersecurity in Deutschland 2022", die das Research- und Beratungshaus International Data Corporation (IDC) in Zusammenarbeit mit secunet umgesetzt hat, sehen Firmen in Deutschland die Sicherheitskomplexität (27 %), Datenschutz/Privacy (21 %), Cybersecurity-Personal-/Fachkräftemangel (19 %) und die Sicherheit von vernetzten Umgebungen (18 %) als die größten Herausforderungen bei ihrer IT-Sicherheit. Fast zwei Drittel (61 %) gaben außerdem an, bereits einen akuten Fachkräftemangel zu haben oder erwarten ihn für 2023.

Das führt dazu, dass an vielen Stellen nicht genügend in die Cybersicherheit investiert wird. Die Bundesregierung hat das mittlerweile erkannt und mit dem IT-Sicherheitsgesetz 2.0 moderne Leitlinien für die IT-Sicherheit geschaffen. Es bietet Unternehmen Orientierungshilfe – egal, ob sie rechtlich davon betroffen sind oder nicht.

Das IT-Sicherheitsgesetz: Keine Pflicht, aber Vorbild für die Industrie

Das IT-Sicherheitsgesetz (IT-SiG) ist seit 2015 eines der entscheidenden Gesetze, mit denen die Bundesregierung Behörden und die Bevölkerung vor Cyberangriffen und ihren Folgen schützen will. Betroffen sind vor allem Betreiber Kritischer Infrastrukturen (KRITIS) in den Bereichen Energie, Wasser, Ernährung, Informationstechnik und Telekommunikation, Transport und Verkehr sowie Gesundheit. Mit Inkrafttreten des IT-SiG 2.0 im Jahr 2021 sind der Sektor Siedlungsabfälle und alle so genannten „Unternehmen im besonderen öffentlichen Interesse" (UBI) hinzugekommen. Diese Unternehmen werden zur strukturellen Modernisierung ihrer Cybersicherheitskonzepte verpflichtet. Angefangen bei durchdachten Netzwerkstrukturen, die Risiken bereits von vornherein berücksichtigen, umfasst dies auch eine systematische Ordnung der

Netzwerkzugänge und geeignete Mittel zur frühzeitigen Angriffserkennung.

Alles Themen und Herausforderungen, die auch in der Industrie bekannt sind. Denn die fortschreitende Automatisierung und maschinelle Kommunikation im Industriellen Internet der Dinge (IIoT) stellen auch hier hohe Ansprüche an die Cybersicherheit. Doch fehlen gerade mittelständischen Unternehmen oftmals das Know-how und das Fachpersonal, um im Schadensfall vorbereitet zu sein und schnell reagieren zu können. Deshalb empfiehlt es sich auch für sie, sich an den Standards des IT-SiG zu orientieren. Dies bietet gleich mehrere Vorteile:

1. **Effektivität:** Die umgesetzten Maßnahmen sind transparent, messbar und alltagserprobt.

2. **Planbarkeit:** Die Maßnahmen werden für mehrere Jahre und aufeinander aufbauend strukturiert, sodass Unternehmen Budgets frühzeitig definieren und verbindlich planen können. So werden Cybersicherheitsprojekte nicht zum „Fass ohne Boden".

3. **Versicherbarkeit:** Cybersicherheitsmaßnahmen dienen der Risikominimierung, können jedoch keinen einhundertprozentigen Schutz bieten. Für den Schadensfall lohnt sich deshalb eine Cyber-Versicherung. Diese greift aber nur, wenn gewisse Mindeststandards eingehalten werden.

Wie sichere ich meine Produktionsumgebung ab?

Die Basis für Cybersicherheit bildet eine Ist-Analyse. Anhand dieser lassen sich sinnvolle Maßnahmenpläne ableiten. secunet, IT-Sicherheitspartner der Bundesrepublik Deutschland, berät Unternehmen über alle Aspekte der Cybersicherheit hinweg und unterstützt diese bei der Implementierung einer professionellen und individuellen Sicherheitsinfrastruktur. In drei Schritten werden dabei zunächst bestehende Systeme, darunter auch veraltete Legacy-Geräte, vollständig erfasst. Auf Basis dessen werden Risiken bestimmt, bewertet und Anforderungen festgestellt. Im zweiten Schritt werden die passenden Maßnahmen definiert, die zur notwendigen Sicherheit der vernetzten Systeme führen. Dabei spielt auch das sogenannte Retrofitting eine Rolle, das Vernetzen bestehender und teilweise veralteter Maschinen und Anlagen. Abschließend werden die Übertragungswege zwischen Maschine und Verarbeitungsort abgesichert. Dabei handelt es sich oftmals um hybride Infrastrukturen, beispielsweise der eigenen Infrastruktur oder der Cloud. Auch kann der Einsatz einer vertrauenswürdigen „Private Cloud" sinnvoll sein, um die Vorteile der zuvor genannten Betriebsarten zu kombinieren und zudem die Datenhoheit zu behalten.

Ganzheitliche IT-Sicherheit

Neben den Maßnahmen zur Absicherung der Produktions- und Prozessumgebung braucht es ein ganzheitliches Cybersicherheitskonzept, welches das Gesamtunternehmen betrachtet. Die häufigsten Risiken, insbesondere für produzierende Unternehmen, kommen dabei aus den Bereichen, die mit dem Internet kommunizieren, also von außen erreichbar sind. Dazu zählen unter anderem der Office-Bereich oder externe Zugänge wie beispielsweise Fernwartungszugänge verschiedener Maschinen- und Anlagenhersteller.

Durch sogenannte Penetrationstests können einzelne Systeme oder Infrastrukturen auf Sicherheitslücken untersucht werden. Anhand der Ergebnisse werden im Anschluss daran effektive Maßnahmen für einen wirksamen Schutz abgeleitet. Diese beginnen bei präventiver „Basis-Security" wie Optimierungen der Firewalleinstellungen, Netzwerksegmentierungen oder Zugriffsberechtigungen. Auch Awareness-Schulungen gehören dazu, die Mitarbeiter und Führungskräfte für das Thema Cybersecurity sensibilisieren. Nicht zu vernachlässigen ist das Thema „Disaster Recovery", also das Wiederherstellen des Geschäftsbetriebs nach einem Sicherheitsvorfall. Hier sind automatisierte und funktionierende Backup-Systeme essentiell.

Eine weitergehende Maßnahme ist das sicherheitstechnische Abkoppeln veralteter Maschinen von der vernetzten Infrastruktur durch die Nutzung von gehärteten Industrial PCs („Secure Edge"). Die Maschine ist so nur noch indirekt angebunden und kann von außen nicht erkannt und kompromittiert werden. Dies trägt dazu bei, Angriffe zu erschweren und Risiken zu reduzieren. Angriffserkennungssysteme ermöglichen das frühzeitige Erkennen eines Vorfalls. Je kürzer die Erkennungszeit, desto effektiver können Schäden eingedämmt werden. Dies setzt voraus, dass das System genutzt werden kann und Reaktionsmaßnahmen und Verantwortlichkeiten vorab definiert sind. Auch hierbei bietet das IT-SiG 2.0 eine Orientierungshilfe für den effektiven Aufbau und Einsatz solcher Systeme.

Cybersecurity als Erfolgsfaktor

Langfristig können nur jene Unternehmen wettbewerbsfähig bleiben, denen es gelingt, zusätzliche Mehrwerte der Digitalisierung zu schaffen und gleichzeitig einen wirksamen Schutz vor Cyberattacken sicherzustellen. Dies trägt zudem dazu bei, die Laufzeit der Investitionsgüter zu verlängern und zum Beispiel alte Maschinen länger in Betrieb zu halten. Gerade dann entpuppt sich eine sichere und zuverlässige IT-Infrastruktur als Investition in die Zukunft.

Udo H. Kalinna | www.secunet.com

Ethisches Hacking

DER NÄCHSTE SCHRITT IHRER SICHERHEITSREISE?

1983 rief das Technologieunternehmen Hunter & Ready die erste als Bug Bounty verstehbare Initiative ins Leben. In einer cleveren Marketingkampagne mit Wortspiel wurde jeder Person, die einen Bug im hauseigenen Betriebssystem VRTX (Versatile Real-Time Executive) findet, ein Volkswagen Käfer versprochen. Wer einen Software-Bug fand, konnte also seinen eigenen Käfer (Bug) erhalten.

Die Anzeige lautete: „Es gibt jedoch einen Haken. Da VRTX das einzige Mikroprozessor-Betriebssystem ist, das vollständig mit Silikon versiegelt ist, wird es nicht einfach sein, einen Bug zu finden."

Hunter & Ready erhielten an diesem Tag ihre erste Lektion in Sachen Crowdsourced Security: Unterschätze niemals die Power der Gemeinschaft! Insgesamt wurden sieben Bugs in dem System gefunden. Die Hacker entschieden sich jedoch für die Geldprämie, nicht für das Auto.

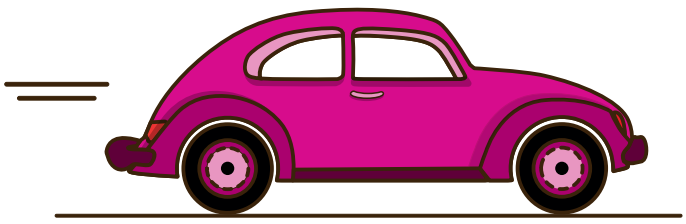
Crowdsourced Security

Damit war der Startschuss für einen neuen Ansatz bei Sicherheitstests gefallen. Heute verdienen ethische Hacker und Hackerinnen auf der ganzen Welt durch Bug Bountys genug Geld, um davon leben zu können. Laut Intigritis Ethical Hacker Insights Report 2022 erwägen 66 Prozent der Befragten, sich in Vollzeit dem ethischen Hacking zu widmen.

Crowdsourced Security hat sich seit den Tagen interner Bug Bountys rasant weiterentwickelt. Die „Power der Gemeinschaft" lässt sich heute auf verschiedene Weise nutzen. Es gibt zahlreiche Lösungen, die den unterschiedlichen Anforderungen gerecht werden.

Dabei gelten drei Schlüsselfaktoren, die hilfreich sind, um sich für die geeignete Crowdsourcing-Lösung zu entscheiden: Zeit, Budget und der Zugang zur Community.

Jede Lösung bietet Vorteile bei mindestens zwei der Schlüsselfaktoren. Werfen wir einen genaueren Blick auf die vorhandenen Möglichkeiten.



Private und öffentliche Bug-Bounty-Programme

Während öffentliche Bug Bountys möglicherweise die bekannteste Lösung in Sachen Crowdsourced Security darstellen, sind sie nicht für alle Unternehmen gleich gut geeignet. Für Start-ups, die noch am Beginn ihrer Sicherheitsreise stehen, könnte ein öffentliches Bounty-Programm zum Beispiel zu viel Aufmerksamkeit erregen.

Hier kommen private Bug-Bounty-Programme zum Zuge. Die gezielte Auswahl bestimmter Sicherheitsexperten und -expertinnen bietet mehr Kontrolle. Private Programme eignen sich hervorragend, um mit ethischem Hacking zu starten oder neuere Assets zu testen.

Egal, ob man sich für eine öffentliche oder private Lösung entscheidet, Bug-Bounty-Programme sind individuell anpassbar. Der Umfang, das Budget und die Sichtbarkeit lassen sich auf die jeweiligen Bedürfnisse abstimmen.

Zudem sind Bug Bountys sehr kosteneffizient und daher auch für kleinere Budgets eine geeignete Lösung. Während sie zwar länger als Penetrationstests brauchen, um Ergebnisse zu liefern, profitieren die Assets von der Überprüfung durch eine Vielzahl an HackerInnen innerhalb der Gemeinschaft.

Penetrationstests als Service

Generell haben sich Penetrationstests gewissermaßen als separate Lösung zu Bug Bountys etabliert. Ein Pentest ist eine zeitlich begrenzte, simulierte Attacke auf ein Asset, bei dem häufig eine bestimmte Methode verwendet wird.

Beim Bug-Bounty-Programm handelt es sich hingegen um einen kontinuierlichen Prozess, bei dem Schwachstellen über einen längeren Zeitraum hinweg gemeldet werden. Ein Pentest wird zwar schneller durchgeführt, bietet jedoch nur eine Momentaufnahme eines bestimmten Assets zu einer bestimmten Zeit.

CROWDSOURCED SECURITY HAT SICH IMMENS WEITERENTWICKELT UND BIETET MITTLERWEILE PASSENDE LÖSUNGEN FÜR JEDEN ANSPRUCH.

Stijn Jans, CEO, Intigriti, www.intigriti.com

Angelehnt an das allgegenwärtige „Software as a Service"-Modell (SaaS), liefert Pentesting as a Service (PTaaS) skalierbare und kosteneffiziente Pentests, die den administrativen Aufwand reduzieren und Schwachstellenmeldungen in einem zentralisierten Portal anbieten.

Einige Bug-Bounty-Plattformen bieten mittlerweile erweiterte PTaaS-Services an, die auf den Fähigkeiten der Experten und Expertinnen innerhalb ihrer Gemeinschaft basieren – so auch Intigritis hybrides Pentesting.

Um auf die drei Schlüsselfaktoren zurückzukommen: PTaaS ist dann besonders sinnvoll, wenn man schnelle Resultate braucht, aber nur ein begrenztes Budget hat. Im Gegensatz zu öffentlichen Bug-Bounty-Programmen wird nicht auf die gesamte Gemeinschaft zurückgegriffen. Da der Umfang meist geringer ist und sehr spezifische Methoden notwendig sind, bietet eine große Gemeinschaft den geeigneten Pool, um spezialisierte Hacker oder Hackerinnen zu finden, die die gewünschten Fähigkeiten mitbringen.

Live-Hacking-Events

Eine weitere Lösung sind Live-Hacking-Events. Sie eignen sich besonders für alle, die eine tiefgehende Sicherheitsüberprüfung benötigen, die schnell Ergebnisse liefern muss.

In diesem Fall treffen sich ausgewählte HackerInnen zu dem Event und arbeiten gemeinsam an Angriffsstrategien. Innerhalb dieser intensiven Testperiode können zahlreiche Schwachstellenmeldungen generiert werden. Außerdem demonstrieren Unternehmen damit, dass sie eine progressive Haltung gegenüber ihrer Sicherheit einnehmen. Da der Schwerpunkt auf der Schnelligkeit liegt und die besten HackerInnen zum Einsatz kommen, sind diese Events jedoch meist kostspieliger als die anderen Lösungen.

Crowdsourced Security hat sich immens weiterentwickelt und bietet mittlerweile passende Lösungen für jeden Anspruch. Cyberkriminelle greifen auf alle möglichen Strategien zurück, was zu stetig steigenden Bedrohungen führt.

Der Einsatz ethischer HackerInnen bietet dank zahlreicher verfügbarer Lösungen eine hervorragende Möglichkeit, diesen Bedrohungen einen Schritt voraus zu sein. Unternehmen, die gerade ihr Sicherheitsbudget für das nächste Jahr planen, seien die Worte von Espen Johansen, Security Director der Softwarefirma Visma, ans Herz gelegt: 1 Dollar Investition in ein Bug-Bounty-Programm bedeutet 10–100 Dollar Ersparnis zu einem späteren Zeitpunkt.

Stijn Jans

Wie sicher ist https?

INNOVATIONEN SIND EN VOGUE, AUCH BEI HACKERN

Die Threat Labs von WatchGuard Technologies haben ihren neuen Internet Security Report (ISR) veröffentlicht. In diesem werden in gewohnter Weise die wichtigsten Malware-Trends sowie aktuell relevante Angriffsmethoden auf Netzwerke und Endpunkte ausführlich beschrieben.

Die Erkenntnisse der Forscher des WatchGuard Threat Labs zeigen, dass die größte Malware-Bedrohung für das dritte Quartal 2022 ausschließlich über verschlüsselte Verbindungen verschickt wurde. Ebenso konnten vermehrt Angriffe auf ICS- und SCADA-Systeme verzeichnet werden. Auch Computerspieler sind gefährdet, denn bei einer Minecraft-Cheat-Engine wurde eine bösartige Nutzlast entdeckt. Der ISR enthält darüber hinaus eine Vielzahl weiterer Informationen und Beispiele zur gegenwärtigen Bedrohungslage.

Fazit der Forscher: Man kann gar nicht oft genug betonen, wie wichtig die Inspektion von HTTPS-Verbindungen ist. Unternehmen sollten die entsprechende Sicherheitsfunktion unbedingt aktivieren – selbst wenn es einige Anpassungen und Ausnahmeregeln erfordert. Denn der Großteil der Malware kommt über verschlüsseltes HTTPS. Wird dieser Angriffsvektor nicht überprüft, steht Bedrohungen jeglicher Art Tür und Tor offen. Auch sollte sich das Augenmerk verstärkt auf Exchange-Server und SCADA-Managementsysteme richten. Sobald für diese ein Patch zur Verfügung steht, ist es wichtig, dieses Update sofort einzuspielen und die Anwendung zu aktualisieren. Angreifer profitieren von jedem Unternehmen, das Schwachstellen noch nicht gefixt hat.

Die überwiegende Mehrheit der Malware kommt über verschlüsselte Verbindungen

Obwohl die Malware „Agent.IIQ" in der Zeit von Juli bis September 2022 den dritten Platz in der regulären Top-10-Malware-Liste belegte, landete sie auf Platz 1 der Aufstellung für verschlüsselte Schadsoftware. Denn alle Agent.IIQ-Erkennungen wurden in HTTPS-Verbindungen gefunden. Wie die Analysen zeigen, kamen 82 Prozent der gesamten Malware über gesicherte Verbindungen, aber nur 18 Prozent unverschlüsselt. Wird der HTTPS-Datenverkehr auf der Firebox nicht überprüft, ist es sehr wahrscheinlich, dass ein großer Teil der Malware unentdeckt bleibt. In diesem Fall können Unternehmen nur darauf hoffen, dass ein wirksamer Endpunktschutz implementiert ist, um wenigstens die Chance zu haben, die Malware an einer anderen Stelle der sogenannten Cyber Kill Chain abzufangen.

ICS- und SCADA-Systeme sind weiterhin beliebte Angriffsziele

Neu in der Liste der zehn häufigsten Netzwerkangriffe im dritten Quartal 2022 ist eine Attacke vom Typ SQL-Injection, die gleich mehrere Anbieter traf. Eines dieser Unternehmen ist Advantech, dessen WebAccess-Portal den Zugriff auf SCADA-Systeme einer Vielzahl von kritischen Infrastrukturen ermöglicht. Ein weiterer schwerwiegender Angriff im dritten Quartal, der ebenfalls zu den Top 5 der einschlägigen Netzwerkbedrohungen gehörte, betraf die U.motion Builder-Software von Schneider Electric, Version 1.2.1 und früher. Dies ist ein deutlicher Hinweis darauf, dass Angreifer weiterhin aktiv versuchen, Systeme zu kompromittieren, wo immer dies möglich ist.

Schwachstellen in Exchange-Servern stellen weiterhin ein Risiko dar

Die jüngste CVE-Schwachstelle (CVE-2021-26855), die das Threat Lab entdeckte, betrifft die Remote-Code-Ausführung (RCE) von Microsoft Exchange Server bei On-Premise-Servern. Diese RCE-Schwachstelle, die eine CVE-Bewertung von 9,8 erhielt, wurde bekanntermaßen bereits ausgenutzt. Das Datum und der Schweregrad dieser Sicherheitslücke lassen ebenfalls aufhorchen, da es sich um eine von der Gruppe HAFNIUM ausgenutzte Schwachstelle handelt. Auch wenn die meisten der betroffenen Exchange-Server inzwischen gepatcht worden sein dürften, sind manche noch gefährdet und das Risiko besteht weiter.

Bedrohungsakteure, die es auf Nutzer kostenloser Software abgesehen haben

Der Trojaner Fugrafa lädt Malware herunter, die bösartigen Code einschleust. Die WatchGuard-Analysten untersuchten eine Variante, die in einer Cheat-Engine für das beliebte Spiel Minecraft gefunden wurde. Die Datei, die hauptsächlich auf Discord geteilt wurde, gibt vor, die Minecraft Cheat Engine Vape V4 Beta zu sein – aber das ist nicht al-

les, was sie enthält. Agent.FZUW weist einige Ähnlichkeiten mit Variant.Fugrafa auf, doch anstatt sich über eine Cheat-Engine zu installieren, scheint die Datei selbst geknackte Software zu enthalten. Im konkreten Fall zeigten sich zudem Verbindungen zu Racoon Stealer: Dabei handelt es sich um eine Kryptowährungs-Hacking-Kampagne, mit der Kontoinformationen von Kryptowährungsdiensten entwendet werden.

LemonDuck-Malware ist jetzt mehr als ein Cryptominer

Auch wenn die Zahl der blockierten oder verfolgten Malware-Domänen im dritten Quartal 2022 zurückgegangen ist, lässt sich unschwer erkennen, dass die Zahl der Angriffe auf ahnungslose Nutzer weiterhin hoch ist. Mit drei Neuzugängen in der Liste der Top-Malware-Domains – zwei gehörten zu ehemaligen LemonDuck-Malware-Domains und der dritte war Teil einer Emotet-klassifizierten Domain – gab es mehr neue Malware-Sites als üblich. Dieser Trend wird sich im Hinblick auf die Kryptowährungslandschaft voraussichtlich weiter verstärken, da Angreifer nach neuen Möglichkeiten suchen, um Nutzer zu täuschen. Ein wirksames Mittel dagegen ist ein aktiver Schutz auf DNS-Ebene. Damit können die Systeme der Benutzer überwacht und Hacker daran gehindert werden, Malware oder andere ernsthafte Probleme in das Unternehmen einzuschleusen.

JavaScript-Verschleierung in Exploit-Kits

Die Signatur 1132518 – als Indikator für JavaScript-Verschleierungsangriffe auf Browser – war der einzige Neuzugang in der Liste der am weitesten verbreiteten Signaturen für Netzwerkangriffe. JavaScript ist seit längerem ein gängiger Angriffsvektor und Cyberkriminelle verwenden immer wieder JavaScript-basierte Exploit-Kits, unter anderem für Malvertising und Phishing-Angriffe. Im Zuge verbesserter Verteidigungsmechanismen der Browser intensivieren auch Angreifer ihre Bemühungen, bösartigen JavaScript-Code zu verschleiern.

Anatomie der standardisierten Adversary-in-the-Middle-Angriffe

Die Multifaktor-Authentifizierung (MFA) ist zwar unbestreitbar eine immens wichtige Maßnahme im Zuge von IT-Sicherheit, aber auch kein Allheilmittel. Bestes Beispiel dafür sind der rasche Anstieg und die Kommerzialisierung von Adversary-in-the-Middle (AitM)-Angriffen. Die Untersuchung des Threat Labs zeigt, wie böswillige Akteure sich auf immer ausgefeiltere AitM-Techniken umstellen. Ähnlich wie beim zunehmend frequentierten Ransomware-as-a-Service-Angebot hat auch die Veröffentlichung des AitM-Toolkits namens EvilProxy im September 2022 die Einstiegshürde für entsprechend ausgeklügelte Angriffe erheblich gesenkt. Deren Abwehr kann nur durch die Kombination aus technischen Tools und einer Sensibilisierung der Benutzer erfolgreich aufgegleist werden.

Malware-Familie mit Verbindungen zu Gothic Panda

Bereits im Bericht des Threat Labs für das zweite Quartal 2022 fiel die Sprache auf Gothic Panda – eine Cyberspionage-Gruppe mit enger Verbindung zum chinesischen Ministerium für Staats-

GERÄTE MIT APT BLOCKIERER

50,3 %
der Malware war **Zero Day** Malware

49,7 %
der Malware war bekannte Malware

Quelle: watchguard.com/security-report

sicherheit. Interessanterweise enthält die Top-Liste der verschlüsselten Malware für das dritte Quartal eine Malware-Familie namens Taidoor, die nicht nur von Gothic Panda entwickelt wurde, sondern auch nur von Angreifern einschlägig chinesischer Herkunft eingesetzt wurde. Während sich die entsprechende Malware bisher in der Regel auf Ziele in Japan und Taiwan konzentrierte, wurde das analysierte Generic.Taidoor-Beispiel vor allem bei Organisationen in Frankreich gefunden – möglicherweise ein klarer Hinweis auf einen spezifischen, staatlich gesponserten Cyberangriff.

Neue Ransomware- und Erpressergruppen in freier Wildbahn

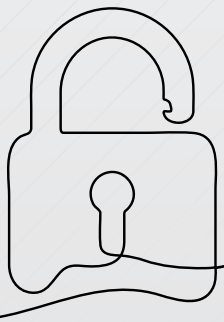
Ab sofort widmet sich das WatchGuard Threat Lab noch stärker dem Aufspüren von Ransomware-Initiativen. Dafür wurden die zugrundeliegenden Threat-Intelligence-Möglichkeiten gezielt erweitert. Im dritten Quartal 2022 führt LockBit die Liste mit über 200 einschlägigen Vorfällen an – fast viermal mehr als die Ransomware-Gruppe Basta, die von Juli bis September 2022 am zweithäufigsten von sich reden machte.

Die vierteljährlichen Forschungsberichte von WatchGuard basieren auf anonymisierten Firebox-Feed-Daten von aktiven WatchGuard-Fireboxen, deren Besitzer sich für die Weitergabe von Daten zur direkten Unterstützung der Forschungsarbeit des Threat Labs entschieden haben. Im dritten Quartal blockierte WatchGuard insgesamt mehr als 17,3 Millionen Malware-Varianten (211 pro Gerät) und mehr als 2,3 Millionen Netzwerkbedrohungen (28 pro Gerät). Der vollständige Bericht enthält Details zu weiteren Malware- und Netzwerktrends aus dem 3. Quartal 2022, empfohlene Sicherheitsstrategien, wichtige Verteidigungstipps für Unternehmen aller Größen und Branchen und vieles mehr.

www.watchguard.de

Status der IT-Security

DEUTSCHE UNTERNEHMEN KÖNNEN CYBERBEDROHUNGEN NUR BEDINGT ABWEHREN

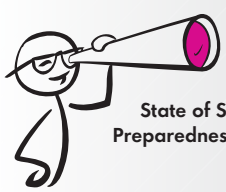


Ivanti hat die Ergebnisse der internationalen Studie „State of Security Preparedness 2023" veröffentlicht. Demnach sind deutsche Unternehmen nur bedingt in der Lage, Angriffe wirksam abzuwehren. Vor allem in den Bereichen Patch Management und der Absicherung gegen Angriffe über die Supply Chain gibt es größte Lücken.

Zweifel am Sicherheitskonzept

Viele deutsche Entscheider haben erhebliche Zweifel an ihren Sicherheitskonzepten. Jeder zehnte Manager ist davon überzeugt, dass sein Unternehmen einen schwerwiegenden Sicherheitsvorfall innerhalb der nächsten 12 Monate nicht verhindern oder stoppen kann. Damit sind die Bedenken bei deutschen Unternehmenslenkern so hoch wie in keinem anderen Land.

Diese Zweifel wirken sich auch auf die Unternehmensfinanzen aus: 9 von 10 Firmen haben bereits Rücklagen für Ransomware-Zahlungen und Kosten im Angriffsfall gebildet. Auch in diesem Punkt stehen deutsche Entscheider unangefochten an der Spitze der betrachteten Länder. Knapp die Hälfte des jährlichen Cyber-Budgets (49 %) fließt in solche Rücklagen, der Rest in Security-Tools und -Teams (43 %) sowie in Cyberversicherungen (6 %).



PLUS

State of Security Preparedness 2023

Cyberbewusstsein in der Führungsetage? Fehlanzeige

Interessanterweise sind es vor allem die C-Entscheider selbst, die es an der nötigen Portion Cyberbewusstsein mangeln lassen. Im Vergleich zu ihren Mitarbeitern im Büro werden sie etwa dreimal so häufig Opfer von Phishing-Angriffen.

Eher irritierend wirkt vor diesem Hintergrund eine Aussage der Leitungsebene zu den Gründen für die fehlende Cyber-Exzellenz des eigenen Unternehmens. Für mehr als 1/3 von ihnen (38 %) spielt ein zu großer Verlass in die eigene Belegschaft dafür eine zentrale Rolle. Ebenfalls bemängelt 1/3 der C-Ebene, dass das Sicherheitstraining für Mitarbeiter ineffizient oder unvollständig sei.

Sorgenkind Patch Management

Insgesamt verdeutlicht die Studie, dass deutsche Unternehmen zwar Vieles daran setzen, sich gegen Cyberangriffe zu wappnen, das Gros der Firmen kämpft aber immer noch mit einer reaktiven Checklisten-Mentalität. Am deutlichsten zeigt sich dies in den Prozessen der Security-Teams selbst, vor allem im Schwachstellen-Management. Heute gilt es, diejenigen Sicherheitslücken zu schließen, von denen ein tatsächliches Risiko für das individuelle Unternehmen ausgeht. Doch anstatt Schwachstellen risikobasiert zu priorisieren, versuchen deutsche Security-Teams immer noch möglichst alle Schwachstellen abzuarbeiten. Zur Verdeutlichung: Zwar geben 9 von 10 Sicherheitsexperten an, dass sie über eine Methode zur Priorisierung verfügen, doch bestätigen sie auch, dass alle Arten von Schwachstellen für sie einen gleich hohen Stellenwert haben. Im Enderfolg vergeuden sie so wertvolle Zeit, die Cyber-Angreifer ausnutzen.

Allerdings: Auf dem Weg zu einem risikobasierten Patch-Management sind deutsche Security-Teams schon einen Schritt weiter als der internationale Durchschnitt. So fokussieren sich bereits 48 Prozent der IT-Sicherheitsteams auf Angriffsvektoren, die aktiv ausgenutzt werden, als auf die jeweils neuesten Schwachstellen. Weltweit sind es durchschnittlich nur 31 Prozent.

www.ivanti.com

C-ENTSCHEIDER UND MANGELNDES SICHERHEITSBEWUSSTSEIN:

2/3 wurden im vergangenen Jahr per Phishing attackiert

1/3 hat auf Scam- und Phishing-Mails geklickt oder Zahlungen geleistet

37% haben ein Arbeitspasswort mit einer Person außerhalb des Unternehmens geteilt

71% nutzen Passwörter, die älter als ein Jahr sind

1/3 verwendet für unterschiedliche Zugänge oder Geräte das gleiche Passwort

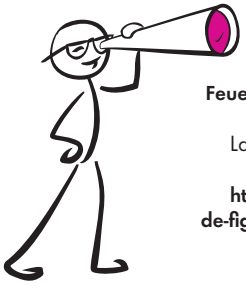
Feuer mit Feuer bekämpfen

AKTUELLE STUDIE ZUR GLOBALEN CYBERSICHERHEITSLAGE

Mit dem Report "Feuer mit Feuer bekämpfen" hat Fastly gerade eine aufschlussreiche Studie zur globalen Cybersicherheitlage in Unternehmen veröffentlicht. Im Interview erklärt Chief Product Architect Sean Leach die wichtigsten Erkenntnisse der Befragung von über 1400 IT-Entscheidern.

it security: *Herr Leach, die Cyber-Bedrohungslage scheint sich derzeit stark zu verändern. In den Medien häufen sich Berichte über immer ausgeklügeltere Cyber-Attacken, Datendiebstähle, und Unternehmen, die Opfer digitaler Erpressung werden. Müssen wir besorgter sein als noch vor ein paar Monaten?*

Sean Leach: Nicht wirklich. Natürlich entwickeln sich Angriffsmethoden weiter, neue Schwachstellen tauchen auf. Und wenn besonders prominente Unternehmen oder wichtige Verwaltungsbehörden von Attacken betroffen sind, macht das Schlagzeilen. Aber Angst ist wie so oft ein schlechter Ratgeber. Tatsächlich ist es so, dass Unternehmen und Organisationen, die die Grundlagen der Cybersicherheit richtig umsetzen, die meisten der gängigen Bedrohungen in der Regel problemlos abwehren können.



PLUS

Feuer mit Feuer bekämpfen

Laden Sie sich die Studie hier herunter:
https://learn.fastly.com/de-fighting-fire-with-fire.html

it security: *Welche Strategie ist die Sinnvollste, um sich effektiv zu schützen?*

Sean Leach: Mit einer Kombination aus bekannten Strategien und richtig umgesetzten Abwehrmechanismen wie etwa einer nicht SMS-basierten Zwei-Faktor-Authentifizierung, strengen Autorisierungsregeln, Rate Limiting zur Kontrolle von ein- und ausgehenden Anfragen und umfassenden Mitarbeiterschulungen sind Sicherheitsteams gut aufgestellt. Dies steht im Gegensatz zu der weit verbreiteten Ansicht, dass „mehr und neu" die Antwort auf Cyber-Bedrohungen sei und auch automatisch mehr Sicherheit bringe. Das ist eines der Ergebnisse unserer neuen Studie.

it security: *Reden wir über diese Analyse: Woher kam die Studienausrichtung?*

Sean Leach: Ihre Eingangsfrage hat es ja schon anklingen lassen: Seit Jahren wird die Cybersicherheitslandschaft als zunehmend komplexer gezeichnet und wahrgenommen. Außerdem werden die Auswirkungen für Unternehmen immer dramatischer, wenn sie nicht bereit oder in der Lage sind, mit den sich entwickelnden Bedrohungen Schritt zu halten. Aus Angst vor möglichen Einfallstoren kaufen die Security-Verantwortlichen deswegen so viele Sicherheitstools, wie es ihr Budget erlaubt. Was unsere Erfahrung aus Gesprächen mit Kunden aber auch zeigt:

Die alltägliche Arbeit wird nicht von einer sich entwickelnden Bedrohungslage bestimmt und die größten Bedenken von IT-Sicherheitsverantwortlichen gehen oft auf bekannte Ursachen zurück. Wir wollten daher das Szenario der zunehmenden Komplexität auf den Prüfstand stellen. Um zu verstehen, welche Herausforderungen, Faktoren, Entwicklungen und Trends die Cybersicherheit heute beeinflussen, entstand eine globale Umfrage unter mehr als 1.400 IT-Entscheidungsträgern in großen Unternehmen aus verschiedenen Branchen in Nordamerika, Europa und dem Asien-Pazifik-Raum. Darunter auch über 200 aus der DACH-Region.

it security: *Was sind Ihre Schlüsselergebnisse?*

Sean Leach: In der Studie zeigte sich, dass Unternehmen angesichts des zunehmenden Drucks anscheinend Komplexität der Einfachheit vorziehen. Statt effizienter Lösungen sehen wir oft den Aufbau übermäßig komplexer Cybersicherheitsumgebungen, die immer mehr Ressourcen binden. Dabei vernachlässigen sie einfache Schritte und Grundlagen, die das Fundament einer starken Cybersicherheitsstrategie bilden.

it security: *Was bedeutet das genau in Zahlen?*

Sean Leach: Über ein Drittel der Befragten (35 Prozent) in der DACH-Region geht davon aus, dass Phishing-Versuche in den nächsten zwölf Monaten die größte Bedrohung für die Cybersicherheit in ihrem Unternehmen darstellen werden, gefolgt von Malware (26 Prozent) sowie Datenschutzverletzun-

gen und -verlusten (25 Prozent). 69 Prozent erhöhen die Investitionen in die Cybersicherheit, um sich auf künftige Sicherheitsrisiken vorzubereiten. Das ist grundsätzlich positiv zu bewerten. Im Durchschnitt sind jedoch nur 59 Prozent der Cybersicherheits-Tools vollständig implementiert und aktiv, was ein klares Zeichen dafür ist, dass viele IT-Leiter ihr Vertrauen in eine Fülle von Tools und Technologien setzen und dann auf das Beste hoffen.

Eine weitere Herausforderung im deutschsprachigen Raum stellt das in den letzten zwei Jahren alltäglich gewordene Homeoffice-Konzept dar. Fast die Hälfte (48 Prozent) der Befragten geht davon aus, dass Cyberangriffe auf Remote-Mitarbeiter in den nächsten zwölf Monaten zu den Hauptbedrohungen für die Cybersicherheit gehören werden. Hinzu kommt, dass in der IT-Branche ein zunehmender Fachkräftemangel herrscht. Der Kampf um (Security-)Talente hat sich dabei durch neue Technologien noch verschärft. 54 Prozent geben an, dass die Verbesserung der Cybersicherheitsfähigkeiten durch Schulungen und/oder die Gewinnung von Talenten hohe Priorität für das nächste Jahr hat. Weitere 39 Prozent planen, das Thema Cybersicherheit „zugänglicher" zu machen, um eine bessere, unternehmensweite Cyber-Hygiene zu fördern.

it security: *Das Fachkräfteproblem wird sich nicht über Nacht lösen lassen – worauf sollten sich Sicherheitsteams also konzentrieren?*

Sean Leach: Da haben Sie Recht. Deswegen werden sich Unternehmen bei der Überprüfung ihrer Sicherheitsabläufe und -technologien die Frage stellen müssen: Sollten wir diese selbst verwalten oder ist es für uns sinnvoller, sie an spezialisierte Sicherheitsanbieter auszulagern? Und wenn es um die Wahl der richtigen Tools geht, sollten drei entscheidende Kriterien berücksichtigt werden: Benutzerfreundlichkeit, Observability und Kompatibilität.

IT-SECURITY-ENTSCHEIDER SOLLTEN AUF EFFIZIENZ SETZEN STATT AUF ÜBERMÄSSIG KOMPLEXE CYBERSICHERHEITSUMGEBUNGEN ZU VERTRAUEN.

Sean Leach, Chief Product Architect, Fastly, www.fastly.com

it security: *Können Sie auf diese drei Aspekte näher eingehen?*

Sean Leach: Nun, grundsätzlich müssen die Tools einfach zu bedienen sein. So ergab unsere Studie, dass 39 Prozent aller eingesetzten Sicherheitstools in Deutschland so eingestellt sind, dass sie Bedrohungen über lange Zeiträume im „Monitoring-Modus" nur protokollieren und nicht tatsächlich blockieren und damit keinen wirklichen Schutz bieten. Dies hat nach unseren Ergebnissen zwei Gründe: Zum einen gaben die Befragten an, dass 38 Prozent der erkannten Meldungen sich als Fehlalarme herausstellen. Zum anderen fanden wir heraus, dass die Angst, einen legitimen Nutzer zu blockieren, oft größer ist als die Angst, von einem böswilligen Akteur kompromittiert zu werden.

Ein weiterer wichtiger Faktor ist Observability. Sicherheitstools müssen Fachleuten klar verwertbare Einblicke liefern. Unternehmen, die wenig oder keinen Zugang zu diesen Informationen haben und Daten mehrerer Sicherheitslösungen nicht gesammelt betrachten können, werden in ihrer Sicherheitsstrategie gehindert. Einfach ausgedrückt: Wenn Sie nicht wissen, wovor Ihre Tools Sie schützen, können Sie nicht wissen, was Sie tun müssen, um geschützt zu bleiben.

Zuletzt müssen die Sicherheitslösungen leicht in bestehende Systeme integrierbar sein. Hierzu ergaben unsere Untersuchungen, dass sich durchschnittlich 41 Prozent der auf Netzwerk und Anwendungen ausgerichteten Cybersicherheitslösungen in ihrer Funktionalität überschneiden. Das ist ein deutlicher Hinweis darauf, dass Unternehmen eine Reihe von Tools kaufen, die gar nicht für eine sinnvolle Zusammenarbeit ausgelegt sind.

Entscheidend für eine zuverlässige und effiziente Cybersicherheitsarchitektur ist die Kombination dieser Faktoren.

it security: *Herr Leach, wir danken Ihnen für das Gespräch.*

MITRE ATT&CK

WO STEHEN WIR HEUTE?

Die Zahl der Cyberangriffe steigt und steigt. Die aktuelle Bedrohungslage rund um den Ukraine Konflikt hat gerade das Thema Nation-State Attacks weiter befeuert. So richten sich diese Angriffe nicht exklusiv gegen die ukrainische Infrastruktur, sondern bedrohen auch die Ukraine unterstützende Unternehmen im Westen. Wie soll man darauf reagieren? Wie soll man wissen, welche Aktoren und welche Maßnahmen für das eigene Unternehmen relevant sind?

Im Jahr 2019 haben wir auf it-daily.net einen Artikel zum MITRE ATT&CK Framework veröffentlicht der dargestellt hat, was das Framework ist und wie es uns in der Cyber Sicherheit hilft. Viel ist seitdem passiert und auch das Framework hat sich massiv weiterentwickelt. Es ist an der Zeit, die Änderungen zu beleuchten und das Framework in den Kontext der heutigen Bedrohungslage zu setzen.

CYBER SICHERHEITSTEAMS GEHEN HEUTE VIEL STRUKTURIERTER VOR UND DIE STÄNDIG WEITER ENTWICKELTE ATT&CK MATRIX WIRD ZU IMMER MEHR UND IMMER STRUKTURIERTEN SICHERHEITSTESTS FÜHREN.

Till Jäger, Leader Sales, SOC Prime, https://socprime.com/

Von V4 zu V12

So war zum Zeitpunkt unseres oben genannten Artikels die Version 4 aktuell, heute sind wir bei Version 12 angekommen. Neben vielen Änderungen im Detail, ist die PRE-ATT&CK Matrix in die Enterprise Matrix integriert worden, neben den Standard Plattformen auch Cloud, Network und Containers hinzugekommen, sowie eine neue Matrix für ICS (Industrial Control Systems) entstanden. Aus Sicht der Threat Detection Industry oder der Sicherheitsanalysten, ist sicher eine der wesentlichen Verbesserungen die Ausgliederung von Datenquellen in eigene Objekte.

Während vor drei Jahren das MITRE ATT&CK Framework („die Matrix") für

PRE-ATT&CK

Priority Definition
- Planning, Direction
- Target Selection
- Information Gathering
- Technical, People,Organizational
- Weakness Identifikation
- Technical, People, Organizational
- Adversary OpSec
- Establish & Maintain Infrastructure
- Persona Development
- Build Capabilities
- Test Capabilities
- Stage Capabilities

ENTERPRISE ATT&CK

Initial Access
Execution
Persistence
Privilege Escalation
Defense Evasion
Credential Access
Discovery
Lateral Movement
Collection
Exfiltration
Command and Control

Die sieben Stufen des Cyber Attack Lifecycle, heute bekannt als die Cyber Kill Chain, erstmalig verbreitet von Lockheed Martin.

viele Sicherheitsverantwortliche noch eine mehr oder weniger theoretische Referenzarchitektur war, hat die praktische Umsetzung in freien sowie kommerziellen Produkten in den letzten Jahren massiv Fahrt aufgenommen.

Die Nutzung von MITRE ATT&CK hat einen deutlichen Wendepunkt erreicht. Während ein Großteil der Anwender ATT&CK zumindest einsetzt, um die eigene Abwehrfähigkeit zu dokumentieren, ist sie bei einem steigenden Anteil nunmehr auch ein fester Bestandteil der Sicherheitsstrategie geworden.

Auch hat sich rund um das Framework ein veritables Geschäft mit Trainings entwickelt. MITRE selbst, über die Foundation MITRE-Engenuity, spielt mit dem „MITRE ATT&CK Defender" Kursen ebenfalls auf dem Spielfeld mit.

Keine 100prozentige Sicherheit

Allerdings sollte gerade bei der Bezeichnung „Framework" immer beachtet werden, dass es sich nicht um ein vollständiges Rahmenwerk aller möglichen Angriffsvektoren handelt.

MITRE ATT&CK basiert letztendlich auf veröffentlichten, dokumentierten Vorfällen. Jedoch wird nur ein kleiner Teil der Vorfälle öffentlich gemeldet. Obwohl die Informationen in der Matrix die meisten TTPs (Tactics, Techniques and Procedures) abdecken könnten, wird dies nie dem Anspruch an Vollständigkeit gerecht. Darüber hinaus ist eine komplette Abdeckung aller TTPs auch technisch nicht möglich.

Dennoch bietet ATT&CK stand heute eines der umfangreichsten Werke an und ist nicht nur deswegen in der Branche zum de-facto Standard geworden.

ATT&CK ist eine Wissensdatenbank für gegnerische Taktiken und Techniken, die auf realen Beobachtungen basieren. Sicherheitsverantwortliche sollten sie als solches einsetzen und nicht als etwas betrachten, das es zu 100% abzudecken gilt.

Typische Anwendungsfälle:

Grundlegende Ausrichtung / Richtlinie der Cybersicherheitsstrategie

CISOs und andere Sicherheitsverantwortliche nutzen zunehmend ATT&CK um die Sicherheitsstrategie des Unternehmens daran auszurichten.

Anreichern von Warnungen im SOC / Alert-Triage

ATT&CK gibt den SOC Teams wichtige Hinweise nach welchen Indikatoren zu suchen ist, um eine Warnung besser zu klassifizieren und die gesamte Breite des Angriffs aufzudecken

Analyse & besseres Verständnis der TTPs (Taktiken, Techniken und Verfahren) der Angreifer

So interessieren sich zum Beispiel Behörden oder behördennahe Unternehmen im Besonderen für nationalstaatliche Bedrohungen wie etwa APT29. Die in MITRE ATT&CK als Bedrohungsgruppen (Threat Groups) bezeichneten Akteure sind, soweit die Information verfügbar, den jeweiligen Industriezweigen zugeordnet, so dass der Sicherheitsanalyst sich vorrangig auf die Bedrohungsgruppen konzentrieren kann, die den spezifischen Industriezweig im Fokus haben (zum Beispiel APT28, APT29 – Behörden & Militär, APT41 – Gesundheitssektor/Telekom/Spieleindustrie, APT34 – Oil & Gas Sektor).

Anreichern der Bedrohungsinformation bestehender Technologien

Werkzeuge nutzen ATT&CK zunehmend zwecks Anreicherung der produzierten Informationen. Reports werden danach ausgerichtet.

Analyse der Fähigkeiten von Sicherheitswerkzeugen

Vor dem Hintergrund der derzeitigen Einsparmaßnahmen, die auch vor der Cyber Security Industrie nicht halt macht, nutzen immer mehr Unternehmen das Rahmenwerk, um vorhandene Tools und Technologien in Ihren Abwehr Fähigkeiten abzubilden und mögliche Überschneidungen (und natürlich auch Lücken) aufzudecken. Dadurch lässt sich effektiv die Landschaft an Sicherheitswerkzeugen im Unternehmen optimieren, sowie deren Einsatz gegenüber dem Management besser argumentieren und dokumentieren.

SOC Assessments

Assessments bestehender SOCs orientieren sich zunehmend an ATT&CK und

nutzen dies um Lücken in der Abwehr oder auch in bestehenden Prozessen zu dokumentieren und zu optimieren.

SIEM Rule Mapping

Ein sehr populärer Anwendungsfall betrifft die Welt der SIEM (Security Information & Event Management) Systeme. Während vor einigen Jahren die vom Hersteller mitgelieferten Regeln noch als „der Standard" angesehen wurden, gehen Unternehmen heute deutlich analytischer vor. So wird immer häufiger das MITRE ATT&CK Framework genutzt um die für das jeweilige Unternehmen relevanten Akteure zu ermitteln, diese dann auf die verfügbaren Log Quellen abzubilden und den dafür relevanten „Detection Content" individuell zu beziehen und ausrollen. Das SIEM wird dadurch von einem generischen zu einem individuell zugeschnittenen Werkzeug. Ein Anbieter, der sich sehr früh mit diesem Thema auseinandergesetzt hat, ist die mittlerweile marktführende Plattform von SOC Prime (siehe Kasten).

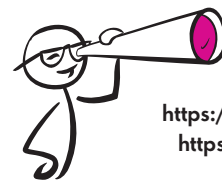
Wo geht die Reise hin? Ein Blick in die Zukunft

Cyber Sicherheitsteams gehen heute viel strukturierter vor und die ständig weiter entwickelte ATT&CK Matrix wird zu immer mehr und immer strukturierten Sicherheitstests führen. So ist die Matrix heute bereits der Goldstandard bei SOC Assessments. Die weitere Verbreitung von „Detection as Code" sowie auch von anderen Werkzeugen wie Red Teaming Tools verleihen der Matrix weiteren Vortrieb. Startups im Sicherheitsumfeld kommen um eine Unterstützung von ATT&CK nicht herum und bewerben dies aktiv. Basierend auf dem Erfolg von MITRE ATT&CK werden CISOs und SOC-Teams offener für andere MITRE-Projekte wie MITRE D3fend (A Knowledge Graph of Cybersecurity Countermeasures) und MITRE Engage (ein Framework für die Planung und Diskussion von gegnerischem Engagement und Operationen).

Till Jäger

SOC PRIME

- SOC Prime betreibt eine weltweite Plattform für kollaborative Cyberabwehr und transformiert die Erkennung von Bedrohungen auf globaler Ebene. Angetrieben von seiner Detection-as-Code-Plattform, die die Zusammenarbeit einer globalen Cybersicherheits-Community fördert, kuratiert die Lösung das weltweit größte Repository für Erkennungsinhalte, das über 200.000 Erkennungsalgorithmen basierend auf dem Sigma-Regelstandard aggregiert.
- Die Plattform bietet die aktuellsten Sigma-Regeln neben innovativen Tools für Bedrohungserkennung, Bedrohungssuche, Streaming von Erkennungsinhalten und SOC-Management bei gleichzeitiger Integration mit über 25 SIEM-, EDR- und XDR-Plattformen.
- Die Crowdsourcing-Initiative von SOC Prime, das Threat Bounty Program verbindet 600 Forscher und Threat Hunter aus der ganzen Welt, die Sigma- und YARA-Regeln erstellen, sie täglich mit Branchenkollegen teilen und ihre Beiträge monetarisieren. Die Plattform verbindet Sicherheitsexperten weltweit und stellt sicher, dass relevante Sigma-Regeln für jede kritische Bedrohung innerhalb von 24 Stunden oder weniger bereitgestellt werden.
- Die branchenweit erste Suchmaschine für Cyber-Bedrohungen bietet kostenlosen und sofortigen Zugriff auf Kontextinformationen, einschließlich Tags, MITRE ATT&CK- und CTI-Referenzen, CVE-Beschreibungen und aufschlussreichere Metadaten, die sicherstellen, dass jeder Sicherheitsfachmann relevante Informationen und Sigma-Regeln zu Cyber-Bedrohungen sofort finden kann um diese auf seine individuelle Sicherheitsinfrastruktur anzuwenden.
- Der kollaborative Cyber-Defense-Ansatz bewältigt die Herausforderung des Talentmangels mit seinem Quick Hunt-Modul, das es jedem ermöglicht, auch ohne Erfahrung auf diesem Gebiet ein Threat Hunter zu werden. Teams können automatisch nach den neuesten Bedrohungen in ihrer SIEM- oder EDR-Umgebung suchen, mit Top-Trend Threat Hunt Anfragen, die von der Empfehlungsmaschine basierend auf Information der Branchenkollegen vorgeschlagen werden. Das Continuous Content Management (CCM) / Outpost-Modul von SOC Prime ermöglicht das Streamen der aktuellsten Erkennungen, die als Inhaltslisten organisiert sind, direkt in ihre Umgebung.



MEHR WERT

https://attack.mitre.org
https://bit.ly/3Z11Tz1

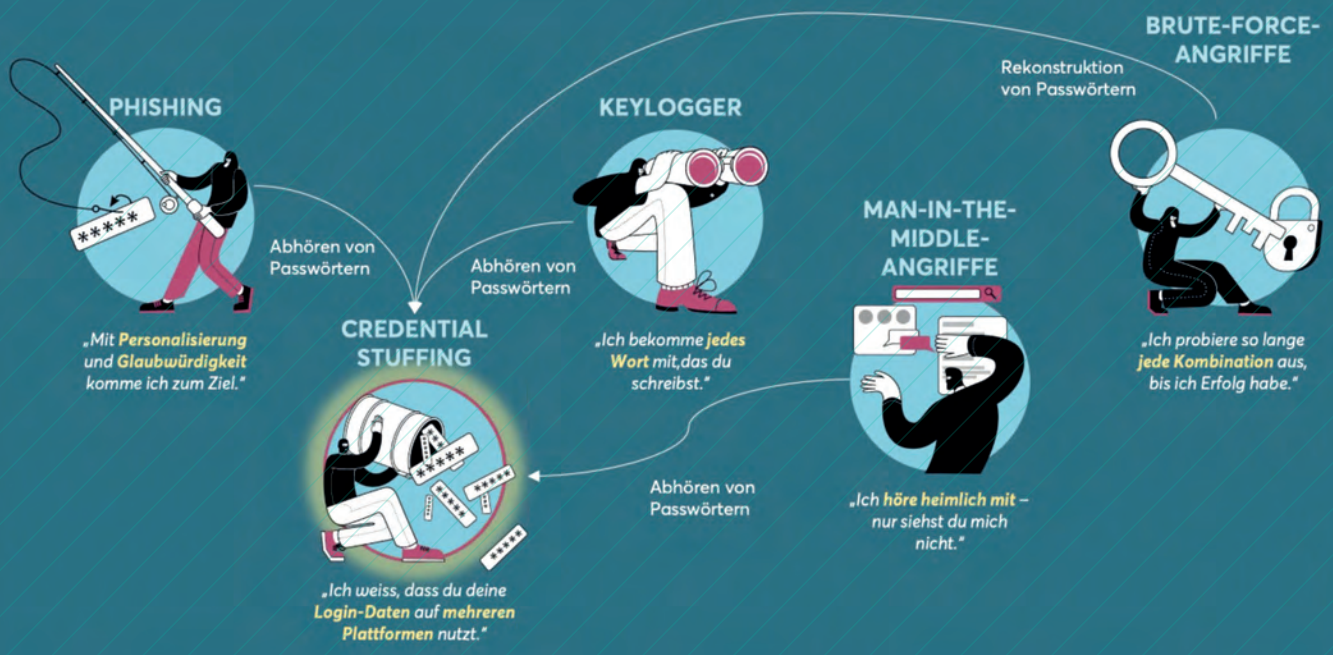
Einträgliches Business

ACCOUNT TAKEOVER

Die feindliche Übernahme von Benutzerkonten hat sich zu einem einträglichen Geschäft für Cyberkriminelle entwickelt. Durch die Nutzung des Internets und der zunehmenden Digitalisierung ist das Angriffsspektrum weit gefasst: es reicht von E-Mails, über die sozialen Netzwerke und den Online-Shops branchenübergreifend in alle Bereiche des täglichen Lebens. Das Account Takeover ist dementsprechend ein attraktiver Businesszweig für das organisierte Verbrechen geworden und Zugangsdaten sind die Basis, die sie benötigen, um bestehende Benutzerkonten zu übernehmen (engl. Account-Takeover). Nachfolgend die fünf erfolgreichsten Angriffsvektoren, die Nevis identifiziert hat.

www.nevis.net

DIE 5 ANGRIFFSVEKTOREN



Quelle: Nevis Security GmbH

Cyber-Attacken: Was hilft ein Threat Navigator?

INNOVATIVES CLIENT VISIBILITY-TOOL HILFT, DAS RISIKO VON CYBERANGRIFFEN ZU MINIMIEREN

Mit dem Threat Navigator erhalten Organisationen eine grafische Übersicht ihrer vorhandenen Sicherheitsmaßnahmen und können so besser einschätzen, wie gut sie vor den neuesten Angriffstechniken geschützt sind. Einziger Wermutstropfen: das Tool ist nicht stand-alone verfügbar, denn der Threat Navigator ist eine Kerkomponente des MDR (Managed Detection and Response) -Portals von Kudelski Security und in Fusion Detect integriert, das die Grundlage der hauseigenen XDR-Architektur darstellt.

Bei Managed-Detection-and-Response-Services wird die Angriffserkennung in der Regel mit einem Reaktionsservice kombiniert. Der Vorteil: als Service muss man als Unternehmen kein eigenes Expertenteam vorhalten.

Was unterscheidet XDR von EDR und MDR? EDR bezeichnet die endpunktbasierte Detektion und Reaktion, MDR die gemanagte Erkennung und Reaktion und XDR die erweiterte Erkennung und Reaktion auf Cybervorfälle.

Anwender erhalten damit automatisierte Empfehlungen, wie sie Bedrohungen in ihrem Umfeld besser erkennen können.

Herausforderungen

Cyberangriffe werden bekanntlicherweise immer häufiger und raffinierter. Gleichzeitig fordern Führungskräfte und Vorstände von ihren Sicherheitsteams, dass sie die Sicherheitslage klar kommunizieren. Eine der Herausforderungen für Sicherheitsteams ist die richtige Einschätzung und Kommunikation der Risiken und Möglichkeiten, um die modernen Bedrohungen und Angreifer zu erkennen. Mit dem Tool erhält man ein tieferes Verständnis darüber, welche Daten und Sicherheitstools notwendig sind, um die für ihre Branche bekannten Angreifer besser zu identifizieren.

DER THREAT NAVIGATOR ERMÖGLICHT UNSEREN KUNDEN, RISIKEN BESSER ZU VERSTEHEN UND ABWEHRMASSNAHMEN ZU PRIORISIEREN.

Jacques Boschung, Head of Kudelski Security, www.kudelskisecurity.com

Threat Navigator ist Teil der breit angelegten, auf dem Cyber Fusion Center basierenden MDR-Strategie von Kudelski Security, die Technologie, Dienstleistungen und hochoptimierte Prozesse und Verfahren kombiniert, die für jeden Kunden individuell angepasst werden. Dadurch werden bestehende MDR-Funktionen erweitert, die das bekannte MITRE ATT&CK-Framwork nutzen. Außerdem erhalten Sicherheitsverantwortliche durch die Analysen mit einer Bedrohungsmodellierung einen sofortigen Überblick über ihre Sicherheitsabdeckung.

Die Ergebnisse werden nach Relevanz gestaffelt und bieten Einblicke und Empfehlungen bezüglich der wichtigsten Sicherheitslücken. Damit können Kunden eine umfassende und rund um die Uhr aktive Strategie zur Erkennung und Abwehr von Bedrohungen implementieren, die auch Pläne zur Risikominimierung und Schwachstellenverwaltung umfasst. Unterstützt wird diese Strategie durch Threat Intelligence, Threat Hunting, effiziente Tools und Expertise in den Bereichen digitale Forensik und Incident Response (DFIR).

Die Vorteile der dynamischen Oberfläche im Überblick:

- Abgleich der aktuellen Sicherheitsabdeckung mit dem MITRE ATT&CK-Framwork, das besonders die für die jeweilige Branche relevanten Bedrohungsakteure sowie ihre Techniken priorisiert.

- Umfangreiche Wissensdatenbank mit Erkenntnissen zu Bedrohungsakteuren (einschließlich der verwendeten Techniken und angegriffenen Branchen), umfangreiche Informationen über MITRE ATT&CK-Techniken sowie Sicherheitsdaten, die von Fusion Detext, der Grundlage der XDR-Architektur, erfasst werden.

- Empfehlungen und Berichte mit vollständigen Listen priorisierter Angriffstechniken sowie Exportfunktionen.

- Für zukünftige Versionen sind branchenspezifische Funktionen geplant, um Verteidigungsstrategien zu verbessern und regelmäßig Sicherheitsempfehlungen zu geben, während sich die Bedrohungslage sowie das Cloud- und Hybrid-Unternehmensumfeld verändern.

Visualisieren, Priorisieren, Beseitigen

Die proaktive Erkennung von Bedrohungen hängt davon ab, herauszufinden, welche Bedrohungen für das jeweilige Unternehmen relevant sind, in welchem Umfang sie bereits abgedeckt sind und welche Maßnahmen man ergreifen sollte, um die Lücken zu schließen. Das Threat Navigator-Tool basiert auf dem MITRE ATT&CK-Framework und einer individuellen Bedrohungsmodellierung. Es ist vollständig in das Kundenportal von Kudelski Security integriert.

Methodik

Das Onboarding mit dem Managed Detection and Response Service von Kudelski Security ist aus gutem Grund sehr gründlich. Je mehr Informationen über das Unternehmen vorliegen, desto genauer ist das zu erstellende Bedrohungsmodell.

Definition des Cybersecurity-Bedrohungsmodell

Die Erstellung eines umfassenden Bedrohungsmodells – basierend auf der jeweiligen Angriffsfläche, den Business- und IT-Security-Experten und den potenziellen Bedrohungsakteuren – ist entscheidend, um zu verstehen, wie das Unternehmen angegriffen werden kann. Das ist der erste Schritt, um kritische Sicherheitslücken in ihrer Transparenz und Abdeckung aufzuzeigen.

Effektiv verteidigen

Ziel muss es sein, Abdeckungslücken durch priorisierte ATT&CK-Techniken automatisch zu erkennen und zu schließen. Das Threat Navigator-Tool verfolgt keinen „Alles-auf-einmal"-Ansatz, sondern hebt die Angriffstechniken hervor, die für das Unternehmen höchste Priorität haben. Durch die Zusammenführung von Datenquellen aus der jeweiligen Umgebung mit verfügbaren Erkennungsregeln und kontextbezogenen Informationen über die jeweilige Branche sowie geografische Informationen hebt der Threat Navigator die fünf wichtigsten empfohlenen Techniken für die Unternehmen hervor, um ATT&CK-Abdeckungslücken zu schließen. Die nächsten empfohlenen Angriffstechniken sind ebenfalls dokumentiert.

Datenanforderungen für die Erkennung von Angriffstechniken

Sobald die Unternehmen wissen, mit welchen Angriffstechniken ihr Unternehmen konfrontiert ist, hilft eine Daten-Checkliste dabei, das Rauschen zu reduzieren und die erforderlichen kritischen Daten zu definieren. Das Ziel ist

WIR GLAUBEN, DASS DIE TRANSPARENZ UND DAS WISSEN, DAS WIR IN UNSEREM KUNDENPORTAL ZUR VERFÜGUNG STELLEN, EIN ENTSCHEIDENDER VORTEIL FÜR UNTERNEHMEN IST.

Olivier Spielmann, First Vice President, Global Managed Detection & Response, Kudelski Security, www.kudelskisecurity.com

eine kontinuierliche, auf Bedrohungen ausgerichtete Verteidigung, um ihre allgemeine Sicherheitslage zu stärken.

Priorisierung von Angriffsabwehrmaßnahmen
Nachdem die Grundlagen geschaffen wurden, ist der Threat Navigator ein nützliches Tool, das Anwendern hilft, Prioritäten für ihre Abwehrmaßnahmen zu setzen. Sobald sie ein klares Bild von der Art der Angriffe haben, mit denen sie konfrontiert sind, können sie sich überlegen, wie sie ihre wichtigen Ressourcen am besten schützen.

Die Prioritätensetzung konzentriert sich auf drei Bereiche:

1. Die Bedrohungsakteure – und die von ihnen verwendeten Techniken – die am ehesten auf die Branche des jeweiligen Unternehmens abzielen
2. Die Daten, die von ihren Sicherheitstechnologien stammen
3. Die von Kudelski Security gepflegten Erkennungsregeln

Die Aggregation dieser Daten ermöglicht es zu verstehen, wo die Sicherheitslücken liegen und welche fünf Lücken am dringendsten geschlossen werden müssen.

Externe Daten einbinden
Anwender können den Threat Navigator zusätzlich mit Daten aktualisieren, die außerhalb der Kudelski Security MDR Services vorliegen. Sie können Datenquellen als „abgedeckt" markieren, wenn sie eine Quelle selbst überwachen oder wenn ein anderer Anbieter diese Informationen für sie bereitstellt.

Ein Security Detection Engineering Team pflegt die Erkennungen „als Code". Das bedeutet, dass die Informationen aus dem Threat Navigator genutzt werden, um Entwicklungen zu verstehen und Erkennungsaktivitäten entsprechend immer wieder neu zu priorisieren. Das geht soweit, Erkennungen automatisch der Kunden-Infrastruktur bereitzustellen soweit die Technologien unterstützt werden. Das bedeutet, dass die globale Sichtbarkeit immer berücksichtigt wird, wenn eine neue Erkennungslogik geändert wird.

THREAT HUNTING

Unter Threat Hunting versteht man die proaktive Suche nach Cyber-Bedrohungen, die unentdeckt in einem Netzwerk lauern. Die Cyber-Bedrohungsjagd gräbt tief, um böswillige Akteure in Ihrer Umgebung zu finden, die an Ihren ursprünglichen Endpunkt-Sicherheitsmaßnahmen vorbeigeschlüpft sind.
Nachdem sich ein Angreifer eingeschlichen hat, kann er monatelang unbemerkt in einem Netzwerk verbleiben, während er heimlich Daten sammelt, nach vertraulichem Material sucht oder sich Anmeldeinformationen verschafft, mit denen er sich seitlich in der Umgebung bewegen kann.
Wenn es einem Angreifer gelungen ist, sich der Erkennung zu entziehen und ein Angriff die Verteidigungsmaßnahmen eines Unternehmens durchdrungen hat, verfügen viele Unternehmen nicht über die fortschrittlichen Erkennungsfunktionen, die erforderlich sind, um zu verhindern, dass die fortschrittlichen, dauerhaften Bedrohungen im Netzwerk verbleiben. Aus diesem Grund ist die Bedrohungsjagd ein wesentlicher Bestandteil jeder Verteidigungsstrategie.

Threat Detection

Im Allgemeinen lassen sich alle Bedrohungserkennungen in vier Hauptkategorien einteilen: Konfiguration, Modellierung, Indikator, und Bedrohungsverhalten. Jede Kategorie kann unterschiedliche Anforderungen und Ansätze unterstützen, je nach den geschäftlichen Anforderungen. Wenn das Ziel ist, neuartige Angriffe zu finden und man bereit ist, einen erheblichen Aufwand zu betreiben, dann ist die Modellierung ein guter Ansatz. Wenn das Ziel darin besteht, ähnliche Angriffe mit weniger Aufwand zu finden, dann ist die Analyse des Bedrohungsverhaltens der richtige Ansatz.

Threat Intelligence

Darunter versteht man den Prozess der Identifizierung und Analyse von Cyberbedrohungen. Dabei werden als „Threat Intelligence" entweder die Daten selbst bezeichnet, die über eine potenzielle Bedrohung erfasst werden, oder der Prozess der Erfassung, die Verarbeitung und die Analyse dieser Daten, um sich ein umfassendes Bild von einer Bedrohung zu machen. Threat Intelligence-Daten werden zunächst gesichtet und im Kontext untersucht, um Probleme zu identifizieren und für jedes aufgespürte Problem eine spezifische Lösung zu entwickeln.

Threat Modeling

Bei Threat Modeling (Bedrohungsmodellierung) handelt es sich um eine sehr bewerte konzeptionelle Analysetechnik mit deren Hilfe sich potentielle Schwachstellen (bzw. Risken) bereits frühzeitig bei der Entwicklung von Anwendungen oder Diensten identifizieren und hierfür erforderliche Maßnahmen ableiten lassen.

DATENSICHERHEIT

SO SCHÜTZEN UNTERNEHMEN IHRE SENSIBLEN UND GESCHÄFTSKRITISCHEN DATEN

Betriebliche Informationsflüsse erfolgen heute zunehmend digital – und die Menge der verarbeiteten Daten steigt dabei täglich an. Für Unternehmen wächst damit auch die Gefahr, ins Visier von Cyberkriminellen zu geraten. Wie das Bundeskriminalamt im Bundeslagebild Cybercrime verlauten ließ, hat die Zahl erfasster Cyberstraftaten mit 146.363 Delikten im Jahr 2021 eine Rekordmarke erreicht. Einer Studie zufolge haben Cyberangriffe bei 90 Prozent der befragten deutschen Unternehmen seit Beginn der COVID-19-Pandemie sogar noch zugenommen.

Und hier liegt das Problem, denn eben genau wegen der Pandemie wurden bei fast allen Unternehmen Sicherheitsprojekte auf Eis gelegt – ein äußerst gefährliches Wagnis.

Um die Sicherheit von Daten zu gewährleisten, bedarf es einer ausgeklügelten Strategie, die nicht nur die rechtlichen Anforderungen abdeckt, sondern auch für das Unternehmen gangbar ist. Hier heißt es, Maßnahmen einzuführen, die es gestatten, sensible Informationen schnell, bequem und ohne Risiken auszutauschen. Zudem gilt es sicherzustellen, dass ausschließlich berechtigte Personen darauf zugreifen können.

WHITEPAPER DOWNLOAD

Das Whitepaper umfasst 35 Seiten und steht kostenlos zum Download bereit.
www.it-daily.net/Download

Das vorliegende Whitepaper gibt Ihnen deshalb Hilfestellung zu folgenden Fragen:

- Was ist Datensicherheit und welche gesetzlichen Grundlagen gibt es dazu?
- Welche Risiken ergeben sich aus mangelnder Datensicherheit?
- Welche Maßnahmen für Datensicherheit gibt es?
- Wie sieht Datensicherheit in der Praxis aus?
- Welche hochsicheren Datenraumlösungen gibt es?

Flankiert wird dies mit nützlichen Checklisten und wertvollen Tipps.

Converged Endpoint Management

ANTWORTEN AUF DIE FRAGEN EINER IMMER KOMPLEXEREN IT-BEDROHUNGSLANDSCHAFT

Nicht nur das Volumen an Cyberangriffen hat im vergangenen Jahr zugenommen, die Angriffe werden auch immer komplexer. So unterteilt der Data Breach Investigations Report 2022 von Verizon die Angriffe in mehrere übergeordnete Kategorien ein.

Die vier hervorstechendsten sind Folgende:

Hacking – Gezielte Angriffe auf IT-Systeme (Backdoor, Web Applications, DoS etc.)

Malware – Schadcode, der Änderungen am IT-System vornimmt (Ransomware, Backdoor, manipulierte Software Updates und Downloader)

Social Engineering – Täuschung und Manipulation von Mitarbeitern, um Zugriff auf die IT-Infrastruktur zu erlangen (Phishing, Emails, Social Engineering etc.)

Missbrauch – Die Verwendung von Privilegien und Rechten im Widerspruch zum ursprünglich formulierten Zweck

Jede dieser Angriffswege nutzt unterschiedliche Schwachstellen in der IT-Sicherheitsstrategie des Opfers aus. Die meisten Sicherheitslösungen konzentrieren sich jedoch auf eine bestimmte Angriffsstrategie und können daher keinen vollumfänglichen Schutz garantieren. Hinzu kommt, dass die neue Arbeitswelt durch Home-Office und Fernzugriff auf Firmendaten die Situation noch komplexer gemacht hat. Die Masse an neuen Endgeräten im Firmennetz sowie die Implementation einer Vielzahl heterogener Softwarelösungen haben ein schwer manage- und überwachbares IT-Ökosystem geformt.

> ES GIBT VIELE ANGRIFFSWEGE, ABER ALLE NUTZEN UNTERSCHIEDLICHE SCHWACHSTELLEN IN DER IT-SICHERHEITSSTRATEGIE DER OPFER AUS.
>
> **Zac Warren,**
> **Chief Security Advisor EMEA, Tanium,**
> **www.tanium.com**

Unübersichtliche Endpoint-Landschaft

Eine verteilte Belegschaft, naürlich auch pandemie-begünstigt durch das Home Office, bedeutet einen gewissen Grad an Kontrollverlust - nicht unbedingt über die Belegschaft, sondern über die Vielzahl von unsichtbaren und ungeschützten Endpunkten in der IT-Infrastruktur von Unternehmen. Daten von Tanium zeigen, dass in 94 Prozent der Organisationen mindestens 20 Prozent der Endgeräte ungeschützt sind. Hinzu kommt, dass die Daten immer mehr in fest verschlossenen Silos fragmentiert werden, was eine rechtzeitige Reaktion auf Vorfälle erschwert.

Insofern stellt Converged Endpoint Management (XEM) einen Paradigmenwechsel in der IT-Sicherheit dar. Die richtige Antwort auf die wachsende Zahl von Sicherheitsproblemen besteht nicht darin, die Zahl der Lösungen für jedes IT-Ökosystem zu erhöhen. Das Gegenteil ist der Fall: Mangelnde Kompatibilität und fehlende Synergien führen dazu, dass dieser Ansatz der IT-Sicherheitslage eines Unternehmens mehr schadet als nützt.

Fast die Hälfte der Befragten der Foundry's „Security Priorities Study" (45 Prozent) gab an, dass sie innerhalb des letzten Jahres mindestens vier neue Sicherheitslösungen zu ihrem IT-Arsenal hinzugefügt haben. Ein heutiges Unternehmen verfügt im Durchschnitt über 43 separate IT-Sicherheits- und Sicherheitsmanagement-Tools in seiner Infrastruktur, die häufig von verschiedenen Abteilungen betrieben werden. Dies schafft eine hochexplosive Mischung aus Undurchsichtigkeit und Unsicherheit, die CIOs und CISOs gleichermaßen Kopfzerbrechen bereitet.

Die Lösung: XEM

Converged Endpoint (XEM) Management wirkt diesen Tendenzen entgegen und beseitigt die Hauptursache für die meisten der heutigen IT-Vorfälle: Mangelnde Endpunkttransparenz und

schlechtes Patch-Management. XEM bietet den Sicherheitsspezialisten einen konsolidierten und hoch automatisierten Überblick über alle Endpunkte in der IT-Infrastruktur ihres Unternehmens. Es verkürzt die Reaktionszeit bei Sicherheitsverletzungen und ermöglicht eine schnelle und fundierte Reaktion, um eine Kompromittierung des Unternehmensnetzwerks durch Cyberkriminelle zu verhindern.

XEM entwirrt die verstreute IT-Infrastruktur in einer Welt verteilter Belegschaften und gibt dem Sicherheitspersonal die Kontrolle zurück, die es während einer langen Zeit der Fernarbeit sukzessive verloren hatte. Converged Endpoint Management ist in der Lage auf verschiedenen Plattformen oder in verschiedenen Softwareumgebungen reibungslos zu funktionieren. Die plattformübergreifende Kompatibilität ist ein zentraler Bestandteil der Kontrolle und Verwaltung verteilter IT-Systeme und das Fundament von XEM.

Automatisch und flexibel

Insofern bietet XEM Echtzeit-Sicherheit und passt sich an ein heterogenes IT-Ökosystem an.

Den besten Schutz bieten Lösungen, die nicht erst auf Vorfälle reagieren müssen, sondern die Sicherheit durch einen ständigen Abgleich zum optimalen System-Zustand generieren.

Durch den Einsatz von Künstlicher Intelligenz und Machine Learning kann die bestmögliche und stabilste Konfiguration vom Unternehmensnetz und all seiner Komponenten – vom zentralen Server bis hin zum entlegendsten Endpunkt – ermittelt werden. Dadurch können Abweichungen im laufenden Betrieb schnell erkannt, analysiert und bei Bedarf behoben werden.

Die riesige Menge an digitalen Prozessen kann jedoch unmöglich manuell abgearbeitet werden. Selbst eine gut ausstaffierte IT-Abteilung kann nicht jede einzelne Veränderung im System beobachten und verfolgen. Hier kommt die besondere Stärke von intelligenten und selbstlernenden Algorithmen zum Tragen. Durch die Zusammenführung aller relevanten Kriterien wie die Gesamtheit der im Firmennetz befindlichen Endpunkte, sowie deren Software- und Updatestatus auf einer zentralen Plattform, können einzelne Verantwortungsträger und Spezialisten informierte Entscheidungen in Echtzeit treffen – ganz ohne die dafür relevanten Informationen in Handarbeit zusammentragen zu müssen.

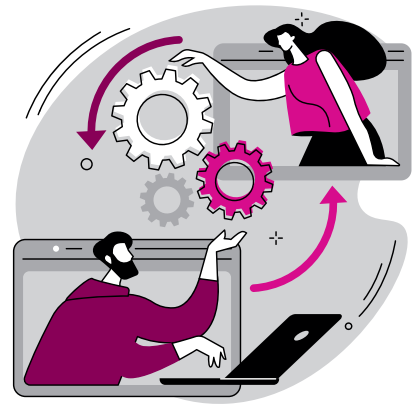
Die Vorteile von XEM auf einen Blick:

- CIOs können alle Endpunkte in wenigen Arbeitsschritten patchen und konfigurieren
- CISOs können Schwachstellen in Echtzeit erkennen und unternehmensweit beheben
- Infrastrukturteams können Cloud-Migrationen in Wochen anstatt in Jahren durchführen
- Der Einkauf kann erkennen, ob sie Software lizenzieren, die sie nicht benötigen
- Datenverwalter können sensible Daten in großem Umfang aufspüren und entfernen
- Auditoren können nachverfolgen, ob das Unternehmen Vorschriften und Compliance einhält.

Converged Endpoint Management ist die maßgeschneiderte Antwort auf ein täglich wachsendes Datenaufkommen kombiniert mit der Aufweichung klassischer Strukturen der Büroarbeit. Es stellt IT-Sicherheitsverantwortliche und Techniker vor eine große Belastungsprobe. Ein stetiger Zufluss neuer Endpunkte wird von einer – teils automatisch generierten – Datenflut flankiert und droht die begrenzte Anzahl an qualifiziertem Fachpersonal zu überfordern. Um mit dieser erhöhten Taktung im Tagesgeschäft mitzuhalten, ohne Burnouts bei Mitarbeitern oder Sicherheitslücken im System in Kauf nehmen zu müssen, benötigt es eine Abkehr von althergebrachten Methoden und eine Zuwendung zu Lösungen, die den Anforderungen der Zeit gewachsen sind.

XEM ist nicht weniger als ein Paradigmenwechsel und bietet die maßgeschneiderten Antworten auf die Fragen einer hochfrequenten und komplexen digitalen Gegenwart.

Zac Warren



Resilient Zero Trust

SCHRITT FÜR SCHRITT ZU MEHR SICHERHEIT

Es gibt viele Interpretationsvarianten für einen bestehenden Namen und immer wieder tauchen neue Begriffe auf. Zero Trust ist ein häufiger, oft unterschiedlich interpretierter Begriff. Zero-Trust-Architekturen und Zero-Trust-Network-Access werden so beispielsweise oft miteinander verwechselt.

Während ZTNA ein notwendiges Element jedes Zero-Trust-Sicherheitsansatzes ist, reicht ZTNA allein nicht aus, um Zero-Trust-Ziele zu erreichen. Es muss Teil eines integrierten Ansatzes sein.

In einem neuen Report von Absolute Software wird der Aufbau einer Grundlage für eine vollständige, integrierte Zero-Trust-Architektur erörtert. Wenn diese Puzzleteile für die Architektur richtig zusammengesetzt werden, können sie einen Großteil der Probleme lösen, die von Experten des 451 Research-Institutes genannt wurden.

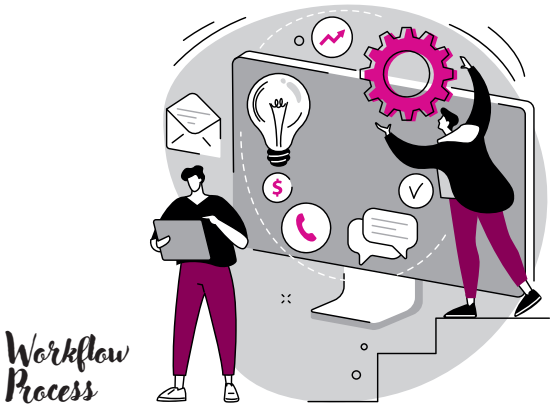
Anforderungen

Erik Hanselman, Principal Research Analyst, 451 Research, Teil von S&P Global Market Intelligence, schreibt in dem Bericht: Damit eine Zero-Trust-Umgebung wirklich belastbar ist, muss sie Endpunktsicherheit, sichere Zugriffsfunktionen, Netzwerktransparenz und -verwaltung in einem integrierten System zusammenführen. Viele Zero-Trust-Ansätze verknüpfen diese Elemente zwar, integrieren sie aber nicht wirklich. Eine integrierte Umgebung kann die Situationswahrnehmung verbessern, indem sie alle Aspekte der Geräte, ihrer Aktivitäten, des Netzwerkverkehrs und der Sichtbarkeit von Bedrohungen auf hoher Ebene zusammenführt. Zusammengenommen ist dies eine Kombination, die besser in der Lage ist, Angriffe abzuwehren und schneller eine Sanierung durchzuführen, wenn sie doch auftreten. Auf diese Weise können Unternehmen die Vorteile nutzen, die ein echtes, widerstandsfähiges Zero-Trust-System verspricht.

DIE TOP 10, DIE IT-SICHERHEITSVERANTWORTLICHEN KOPFSCHMERZEN BEREITEN.

Source: 451 Reserch's Voice of the Enterprise: Information Security, Workloads & Key Projects 2021

Was sind die drei größten Probleme Ihrer Organisation in Bezug auf die Informationssicherheit?



barkeit, Personalmanagement, Malware und Ransomware sowie Budget. Im Falle eines Angriffs wollen Unternehmen sicherstellen, dass Geräte, Systeme und Daten den Mitarbeitern so schnell wie möglich zur Verfügung gestellt werden.

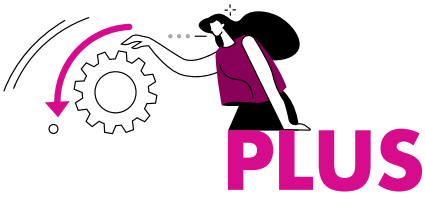
Wie in dem Bericht hervorgehoben wird, kann die Selbstheilung schneller erfolgen, wenn die Ausfallsicherheit in die Geräte eingebettet ist, so dass die Mitarbeiter schneller wieder produktiv arbeiten können.

Hanselman weist auch darauf hin, dass es zwar eine Vielzahl von Sicherheits- und Risikoproblemen gibt, mit denen Unternehmen zu kämpfen haben, dass aber Resilient Zero Trust viele der von Sicherheits- und Risikofachleuten am häufigsten angeführten Probleme lindert. Dazu gehören der Umgang mit Benutzerverhalten, Cloud-Sicherheit, Datenschutz, Phishing, Endpunktsicherheit, Fernzugriff, Sicht-

Definition und Umsetzung

Absolute Software ist ein Pionier, der nicht nur das Konzept des „Resilient Zero Trust" definiert, sondern auch die gesamte Palette der dafür erforderlichen Funktionen bereitgestellt hat. Es ist deutlich geworden, dass weit verteilte, hybride Arbeitsumgebungen auf Dauer Bestand haben werden. Daher suchen Unternehmen nach Sicherheitsansätzen, die Endpunkt- und Zugriffsbewertungen vollständig integrieren, um sicherzustellen, dass die Zero-Trust-Prinzipien bei jedem Schritt vollständig angewendet werden. Die Fähigkeit, Sichtbarkeit und Selbstheilung vom Endpunkt bis zum Netzwerkrand zu ermöglichen, bedeutet für die Unternehmen ein Mehr an Sicherheit.

Ulrich Parthier



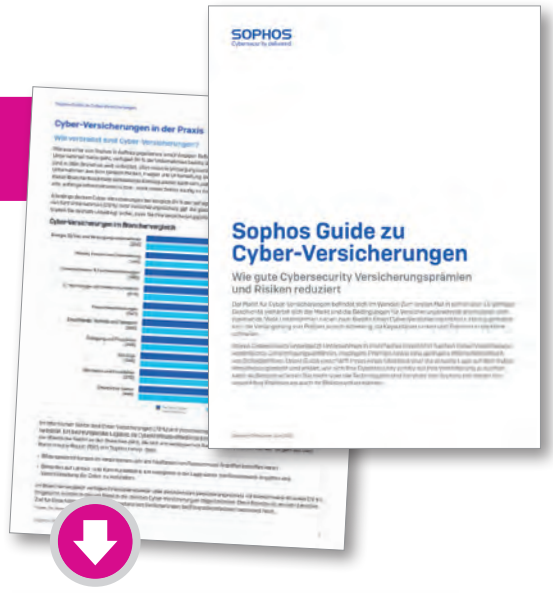
www.absolute.com/go/reports/451-research-resilient-zero-trust/

GUIDE ZU CYBER-VERSICHERUNGEN

WIE GUTE CYBERSECURITY VERSICHERUNGSPRÄMIEN UND RISIKEN REDUZIERT

Der Markt für Cyber-Versicherungen befindet sich im Wandel: Zum ersten Mal in seiner über 15-jährigen Geschichte verhärtet sich der Markt und die Bedingungen für Versicherungsnehmer erschweren sich zusehends. Viele Unternehmen haben zwar bereits einen Cyber-Versicherungsschutz. Häufig gestaltet sich die Verlängerung von Policen jedoch schwierig, da Kapazitäten sinken und Prämien in die Höhe schnellen.

Der Guide verschafft Ihnen einen Überblick über die aktuelle Lage auf dem Cyber-Versicherungsmarkt und erklärt, wie sich Ihre Cybersecurity positiv auf Ihre Versicherung auswirken kann. Außerdem erfahren Sie mehr über die Technologien und Services von Sophos, mit denen Sie sowohl Ihre Prämien als auch Ihr Risiko senken können.



WHITEPAPER DOWNLOAD

Das Whitepaper umfasst 10 Seiten und steht kostenlos zum Download bereit.
www.it-daily.net/Download

CASB, SSE, SASE

UND WAS KOMMT DANACH?

Die Verbreitung von SaaS in Unternehmen hat in den letzten Jahren rasante Ausmaße angenommen. Dieser Trend hat zwar die Produktivität der Benutzer und die Flexibilität des Unternehmens erheblich gesteigert, gleichzeitig aber auch neue Möglichkeiten für Datenschutzverletzungen und Gefährdungen eröffnet. Die Experten bei Palo Alto Networks haben sie näher mit den Ursachen beschäftigt.

Der „Schlüsselfertig"-Aspekt von Software-as-a-Service (SaaS) ist für Unternehmen verlockend, aber er kann letztlich trügerisch sein, wenn Sicherheitsrisiken eingeführt werden, die den Nutzern nicht bewusst sind.

Die Experten sehen daher im SaaS Security Posture Management (SSPM) eine zunehmend wichtige Entwicklung, um die Sicherheitsrisiken in SaaS-dominierten Umgebungen einzudämmen.

Ein großes Unternehmen verwendet in der Regel 100 oder mehr zugelassene SaaS-Anwendungen. Jede dieser Anwendungen verfügt über eigene Einstellungen, Funktionen, Versionen und Updates. Selbst wenn jede sanktionierte Anwendung zu einem bestimmten Zeitpunkt ordnungsgemäß konfiguriert ist, können Angreifer immer noch nach Sicherheitslücken suchen, die durch eine neue Funktion oder eine von einem Anwendungsadministrator vorgenommene Konfigurationsänderung entstehen.

Wenn dann noch eine neue SaaS-Anwendung ohne vorherige Genehmigung und Kontrolle zum bestehenden Portfolio sanktionierter Anwendungen hinzugefügt wird, müssen sich die Sicherheitsteams mit einer ganzen Reihe neuer blinder Flecken in der Sicherheit auseinandersetzen. Alles in allem ist jede SaaS-Anwendung – unabhängig vom Grad der Nutzung und des Schutzes – immer noch anfällig für Sicherheitslücken.

SaaS-Schwachstelle

Gartner hat vorausgesagt, dass mehr als 99 Prozent der Sicherheitsverletzungen in der Cloud auf vermeidbare Fehlkonfigurationen oder Fehler der Endbenutzer zurückzuführen sind. Heute werden SaaS-Fehlkonfigurationen schnell zu einer der Hauptursachen für Datenschutzverletzungen bei SaaS-Anwendungen. Zunächst gilt es zu klären, warum herkömmliche CASBs (Cloud Access Security Brokers) bei diesem Problem versagt haben.

Old School CASB

Herkömmliche CASBs sind so konzipiert, dass sie sensible Daten zunächst mit einer Data Loss Prevention (DLP)-Einheit schützen. Das Problem bei diesem „Schutz der Daten zuerst"-Ansatz ist,

SERVICE

SECURE

dass der Großteil der SaaS-Angriffsfläche übersprungen wird – die Angriffsfläche, die die Sicherheit und Integrität der SaaS-Anwendung selbst darstellt. Sich auf den Schutz der Daten zu konzentrieren und dabei die Sicherheit der Anwendung selbst zu vernachlässigen, ist, als würde man auf einem rissigen Fundament bauen. Die Anwendung selbst sollte zuerst vor Schwachstellen geschützt werden, damit sie zuverlässig alle Sicherheitsgarantien, einschließlich der Datensicherheit, bieten kann.

Wenn eine SaaS-Anwendung aufgrund einer durch eine Fehlkonfiguration verursachten Schwachstelle beeinträchtigt wird, wirkt sich dies negativ auf die Gesamtsicherheit aus, so dass die Daten der Anwendung dem Risiko einer Verletzung ausgesetzt sind. Um dieses Problem zu lösen, hat sich das SaaS Security Posture Management (SSPM) schnell zu einem grundlegenden Instrument zum Schutz der Sicherheitslage von SaaS-Anwendungen entwickelt.

Was sind einige der wichtigsten SaaS-Herausforderungen, die SSPM für die SaaS-Sicherheit in Unternehmen so wichtigmachen?

Herausforderung: Die sichere Konfiguration von Tausenden von Einstellungen für Hunderte von genehmigten SaaS-Anwendungen ist keine leichte Aufgabe.

Sicherheitsteams haben bereits damit zu kämpfen, mit der ständig steigenden Nutzung von genehmigten SaaS-Anwendungen im Unternehmen Schritt zu halten. Dabei müssen sie auch sicherstellen, dass jede SaaS-Anwendung sicher konfiguriert ist. Um dies zu erreichen, müssen die Sicherheitsteams die Grundlagen verstehen. Erstens gibt es zu viele Anwendungen und jede Anwendung hat Dutzende bis Hunderte von Einstellungen, die sich auf die Sicherheit auswirken. Zweitens müssen alle Einstellungen jeder Anwendung verstanden und korrekt eingestellt werden, damit sie mit den Branchen- und Unternehmensrichtlinien übereinstimmen. Drittens müssen die Sicherheitsteams die Risiken verstehen, die selbst dann bestehen, wenn eine Einstellung versehentlich falsch konfiguriert wurde.

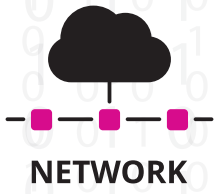
Eine beliebte Videokonferenz-App ist dafür ein gutes Beispiel. Die Anwendung scheint recht einfach zu sein, verfügt aber in Wirklichkeit über mehr als 50 Einstellungen, die sich auf die Sicherheit auswirken können – von Passwortanforderungen für Meetings bis hin zu Einstellungen für die Freigabe von Aufzeichnungen. All diese Einstellungen müssen von verschiedenen Abschnitten der Verwaltungskonsole aus verstanden werden und erstrecken sich über mehrere, verschiedene Dokumentationen.

Herausforderung: Die Behebung von Sicherheitsfehlkonfigurationen in SaaS ist schwierig – sie zu beheben ist noch schwieriger.

SaaS-Anwendungen werden in der Regel nicht nur von einem, sondern von vielen Beteiligten im gesamten Unternehmen genutzt und betrieben. Während sich diese Teams darauf konzentrieren, das Unternehmen zu unterstützen und die Zusammenarbeit zu verbessern, sind sich nicht alle von ihnen über die Sicherheitsauswirkungen der zahlreichen Einstellungen der Anwendung im Klaren, insbesondere, wenn Änderungen an der Anwendung ohne das Wissen der anderen vorgenommen werden. Darüber hinaus können die Beteiligten leicht neue SaaS einführen und zum De-facto-Eigentümer werden, obwohl sie möglicherweise nicht über das Fachwissen verfügen, um eine sichere Bereitstellung zu gewährleisten.

Letztendlich führt die mangelnde Koordination zwischen den Beteiligten aus verschiedenen Geschäftsbereichen, der IT, den Infosec- und GRC-Teams zu einer sogenannten Konfigurationsabweichung.

Das Ergebnis ist ein ineffizienter, zeitaufwändiger und langfristig nicht skalierbarer Sanierungsansatz, da immer mehr SaaS-Anwendungen für die Unternehmensnutzung zugelassen werden. Wenn Sicherheitsadministratoren keinen Einblick in die Änderungen an den Sicherheitseinstellungen einer SaaS-Anwendung haben, ist die Identi-



fizierung von Fehlkonfigurationen mit der Suche nach einer Nadel im Heuhaufen vergleichbar, und sie können die Sicherheit der Anwendung nicht gewährleisten. Sie müssen dann manuelle Anwendungsbewertungen durchführen, um nach der Möglichkeit einer Fehlkonfiguration zu suchen. Wie nicht anders zu erwarten, ist der Audit-Prozess langsam und mühsam und bietet nur punktuelle Einblicke, wenn Hunderte von sanktionierten Anwendungen betroffen sind.

Um ein Beispiel zu nennen: Wenn eine Person für eine Anwendungsbewertung eine Woche benötigt, würde es bei 200 Anwendungen 200 Wochen dauern, um eine vollständige Bewertung aller Anwendungen vorzunehmen. Selbst wenn vier Personen jeden Tag eine Anwendungsbewertung durchführen würden, würde dies ein ganzes Jahr dauern. Bis dieses Team alle Anwendungen durchgesehen hat, muss es diesen Zyklus noch einmal wiederholen, da diese Audits nur eine punktuelle Bewertung darstellen. Wenn sich etwas ändert, würde InfoSec das erst im nächsten Überprüfungszyklus herausfinden.

Es erübrigt sich zu sagen, dass es heute keine effiziente Lösung gibt, die den SaaS-Bewertungsprozess über mehrere Anwendungen hinweg automatisiert und gleichzeitig die Prüfung kontinuierlich überwacht.

Herausforderung: Die Sicherung von SaaS unterscheidet sich von der Sicherung herkömmlicher Software.

Das SaaS-Modell hat viele Vorteile gegenüber herkömmlicher Software, denn es bietet sofortige globale Verfügbarkeit und automatische Updates auf die neuesten und besten Funktionen. Doch genau diese Eigenschaften machen sie auch zu einer Herausforderung für die Sicherheit. Während herkömmliche Software im Rechenzentrum bereitgestellt wird, sind SaaS-Anwendungen direkt über das Internet zugänglich, was die Gefahr von Fehlkonfigurationen deutlich erhöht.

Es gibt ein gutes Beispiel, bei dem eine beliebte Anwendung zur Problemverfolgung den Benutzern die Option bot, ihre Dashboards mit „allen" zu teilen, was fälschlicherweise als „alle im Unternehmen" interpretiert wurde, während es in Wirklichkeit „alle im Internet" waren.

Upgrades für herkömmliche Software werden direkt vom IT-Team überwacht und durchgeführt. SaaS-Anwendungen hingegen aktualisieren sich dynamisch selbst, um neue Funktionen und Merkmale hinzuzufügen. Die häufigen Aktualisierungen verbessern die Funktionalität der Anwendung, beeinträchtigen aber auch ihre Sicherheit. Wenn eine SaaS-Anwendung angepasst wird, bieten ihre Einstellungen außerdem nicht mehr das erforderliche Sicherheitsni-

veau, was zu Konflikten mit den Compliance- und Sicherheitsrichtlinien des Unternehmens führt. Und es ist nicht nur so, dass Anpassungen zu Sicherheitslücken führen – oft sind auch die Standardeinstellungen nicht gut genug. IT-Teams in Unternehmen sollten sich an die Kerndevise von „Zero Trust" halten und niemals davon ausgehen, dass die SaaS-Anwendung standardmäßig sicher ist.

SSPM-Ansatz als nächste Stufe

Bei zeitgemäßem SSPM geht es darum, über die Einhaltung von Vorschriften hinauszugehen und alle Einstellungen zu untersuchen, die sich auf die Sicherheitslage der Anwendung auswirken. Dieser Sicherheitsansatz bietet einen vollständigen Überblick über alle Einstellungen, die sich auf die Sicherheit der Anwendung auswirken, ermöglicht eine Behebung mit nur einem Klick und verhindert das Abdriften. Darüber hinaus sollte sich SSPM nicht auf eine Handvoll Anwendungen beschränken, denn alle können ein Risiko für das Unternehmen darstellen.

Next level IT Security

Aber aufgepasst: CASB ist nur ein Teilaspekt innerhalb der IT-Security-Strategie. CASB steht auch nicht im Gegensatz zu SASE (Secure Access Service Edge), sondern ist ein Teil einer SASE-Architektur.

Gartner prägte den Begriff erstmals im Juli 2019. Näher ausgeführt haben die Analysten ihn dann in ihrem „The Future of Network Security is in the Cloud" betitelten Bericht. Seitdem wird SASE als die nächste Transformation für Unternehmensnetzwerke und deren Sicher-

FRAMEWORK

ACCESS

heit bezeichnet. Die Architektur verspricht, bestehende Technologien besser nutzen zu können. Dazu werden Netzwerk- und Sicherheitsbereiche in einem einzigen, globalen Cloud-Dienst zusammengeführt.

SASE kombiniert SD-WAN, Secure Web Gateway, Zero Trust Network Access, Firewall as a Service und Cloud Access Security Broker (CASB). Das SD-WAN sorgt dafür, dass Daten aufvdem schnellsten Weg ans richtige Ziel kommen. Greift der Endpunkt auf Cloud Services zu, schützt das Secure Web Gateway vor Gefahren aus dem Internet. Dafür setzt es zum Beispiel URL- und Web-Traffic-Filter, Anwendungskontrollen und Anti-Malware-Funktionen ein.

Firewall as a Service kontrolliert den Traffic, der nicht Web-basiert ist, während Zero Trust Network Access es ermöglicht, granulare Zugangskontrollen umzusetzen. Über einen sicheren, verschlüsselten Tunnel erhalten Nutzer nur Zugriff auf Anwendungen, wenn sie berechtigt sind. Mit dem CASB können Unternehmen zudem Schatten-IT vermeiden und sicherstellen, dass Anwender nur freigegebene Cloud Services nutzen.

Eine SASE-Plattform enthält nicht immer alle der genannten Komponenten – das muss sie auch nicht, da sich die einzelnen Services teilweise im Funktionsumfang überschneiden.Jeder Anbieter hat außerdem seine Stärken, je nachdem was sein Kerngebiet ist. Einige Hersteller sind zum Beispiel im Secure Web Gateway führend. Palo Alto Networks etwa punktet vor allem mit starken Next Generation Firewall- und ZTNA-Funktionen und bietet eine sehr gute SD-WAN-Komponente.

Natürlich gibt es am Markt zahlreiche Anbieter im Markt wie etwa Forcepoint, Zscaler, Akamai, Cisco, Cato Networks, Netskope, Versa oder Sast Solutions/Pathlock.

Ein Schmanckerl bietet Netskope mit einem kostenloses SASE-Assessment an, das in nur fünf Minuten abgeschlossen ist – mehr erfahren Sie unter www.netskope.com/sase-assessment.

Fazit

Zusammen bilden CASB (Cloud Access Security Broker), DLP (Data Loss Prevention), SWG (Secure Web Gateway) und ZTNA (Zero Trust Network Access) eine Einheit. Das verbindende Element sind das A wie Access und das Z wie Zero Trust-Gedanke, manchmal auch als perimeterlose Sicherheit bezeichnet. Es besagt, vertraue niemandem ungeprüft zu keiner Zeit. Entscheidend ist, dass niemand einen Vertrauensvorschuss für einen Zugriff erhält. Aufgrund von Kriterien wird das Vertrauen „erarbeitet“ und in einem Zero Trust-Modell mit der Anwenderidentität verknüpft, um Zugriff zu gewähren. Applikationen können sich somit überall befinden, ob im Internet, in der Private Cloud und oder im Rechenzentrum. Für private Applikationen wendet man zusätzlich das Prinzip des „Least Privilege‘“ an, also Zugriff auf Basis granularer Regeln und Rollen.

Und noch etwas: Die Konzentration dieser Aspekte auf einen Anbieter bietet eher Vorteile wie etwa ein effizientes Traffic Routing, weniger Ausschlüsse, ein verbessertes Monitoring und Troubleshooting. Dadurch wird auch die Erstellung von Sicherheitsrichtlinien vereinfacht sowie validere Metriken für Security-Management, Auditing, Governance und ein mehr an Transparenz erreicht.

Dem hat auch die Gartner Group Rechnung getragen und einen neuen Quadranten erschaffen. Er heißt Security Service Edge (SSE) und fasst alle Sicherheitskomponenten unter einem Dach zusammen. Gleichzeitig schließt er die netzwerkbezogenen Komponenten wie etwa SD-WAN, aus. Beide zusammen ergeben dann das SASE-Modell.

Ulrich Parthier

ABWEHR AKTIVIEREN

DATENSICHERHEIT IN HYBRIDEN ARBEITSUMGEBUNGEN

In unserer digitalen Welt müssen Unternehmen sich vor Cyberangriffen und dem Verlust wertvoller Daten schützen. Die Arbeit von CISOs ist anspruchsvoller denn je. Die Daten stehen als wertvolles Gut im Mittelpunkt. Das neue Normal im Zeitalter der Daten stellt Unternehmen vor die Frage, wie sie sensible Daten über den gesamten Lebenszyklus sowohl innerhalb als auch außerhalb des eigenen Firmennetzwerks im mehrdimensionalen Datenraum schützen. Unternehmen benötigen eine IT-Sicherheitslösung, die für die heutige Arbeit mit Daten geeignet ist. Eine IT-Sicherheitsplattform, die konsistent alle sensiblen Daten erkennt und schützt, unabhängig davon, wo sich diese befinden oder wie sie sich bewegen. Prävention ist immer besser als Intervention.

In diesem Whitepaper möchten wir Ihnen zeigen, welche Herausforderungen es heute für den Schutz der Daten gibt und wie ineinander verzahnte Sicherheitskontrollen entlang der Kill Chain ansetzen, um Datenverlust bereits im Vorfeld zu verhindern. Wir stellen Ihnen acht wichtige Schritte vor, die zu effektiverer Sicherheit in Ihrem Unternehmen führen.

www.it-daily.ner/download

WHITEPAPER DOWNLOAD

Das Whitepaper umfasst 10 Seiten und steht kostenlos zum Download bereit.
www.it-daily.net/Download

IMPRESSUM

Geschäftsführer und Herausgeber:
Ulrich Parthier (08104-6494-14)

Chefredaktion:
Silvia Parthier (-26)

Redaktion:
Carina Mitzschke (nur per Mail erreichbar)

Redaktionsassistenz und Sonderdrucke:
Eva Neff (-15)

Autoren:
Christian Bücker, Andrew Howard, Till Jäger, Stijn Jans, Udo H. Kalinna, Sean Leach, Carina Mitzschke, Silvia Parthier, Ulrich Parthier, Audra Simons, Oliver Spielmann, Zac Warren

Anschrift von Verlag und Redaktion:
IT Verlag für Informationstechnik GmbH
Ludwig-Ganghofer-Str. 51, D-83624 Otterfing
Tel: 08104-6494-0, Fax: 08104-6494-22
E-Mail für Leserbriefe: info@it-verlag.de
Homepage: www.it-daily.net

Alle Autoren erreichen Sie über die Redaktion.Wir reichen Ihre Anfragen gerne an die Autoren weiter.

Manuskripteinsendungen:
Für eingesandte Manuskripte wird keine Haftung übernommen. Sie müssen frei sein von Rechten Dritter. Mit der Einsendung erteilt der Verfasser die Genehmigung zum kostenlosen weiteren Abdruck in allen Publikationen des Verlages. Für die mit Namen oder Signatur des Verfassers gekennzeichneten Beiträge haftet der Verlag nicht. Die in dieser Zeitschrift veröffentlichten Beiträge sind urheberrechtlich geschützt. Übersetzung, Nachdruck, Vervielfältigung sowie Speicherung in Datenverarbeitungsanlagen nur mit schriftlicher Genehmigung des Verlages. Für Fehler im Text, in Schaltbildern, Skizzen, Listings und dergleichen, die zum Nichtfunktionieren oder eventuell zur Beschädigung von Bauelementen oder Programmteilen führen, übernimmt der Verlag keine Haftung. Sämtliche Veröffentlichungen erfolgen ohne Berücksichtigung eines eventuellen Patentschutzes. Ferner werden Warennamen ohne Gewährleistung in freier Verwendung benutzt.

Layout und Umsetzung: K.design | www.kalischdesign.de
mit Unterstützung durch www.schoengraphic.de

Illustrationen und Fotos:
Wenn nicht anders angegeben: shutterstock.com

Anzeigenpreise:
Es gilt die Anzeigenpreisliste Nr. 30.
Preisliste gültig ab 1. Oktober 2022.

Mediaberatung & Content Marketing-Lösungen it management | it security | it daily.net:
Kerstin Fraenzke, 08104-6494-19,
E-Mail: fraenzke@it-verlag.de
Karen Reetz-Resch, Home Office: 08121-9775-94,
E-Mail: reetz@it-verlag.de

Online Campaign Manager:
Roxana Grabenhofer, 08104-6494-21,
grabenhofer@it-verlag.de
Marena Avila (nur per Mail erreichbar),
avila@it-verlag.de

Objektleitung:
Ulrich Parthier (-14),
ISSN-Nummer: 0945-9650

Erscheinungsweise: 6 x pro Jahr

Verkaufspreis: Einzelheft 20 Euro
Jahresabopreis 100 Euro (Inland), 110 Euro (Ausland)
Probeabo 20 Euro für 2 Ausgaben
PDF-Abo 40 Euro für 6 Ausgaben

Bankverbindung:
VRB München Land eG,
IBAN: DE90 7016 6486 0002 5237 52, BIC: GENODEF10HC

Beteiligungsverhältnisse nach § 8, Absatz 3 des Gesetzes über die Presse vom 8.10.1949: 100 % des Gesellschafterkapitals hält Ulrich Parthier, Sauerlach.

Abonnementservice:
Eva Neff,
Telefon: 08104-6494 -15,
E-Mail: neff@it-verlag.de

Das Abonnement ist beim Verlag mit einer dreimonatigen Kündigungsfrist zum Ende des Bezugszeitraumes kündbar. Sollte die Zeitschrift aus Gründen, die nicht vom Verlag zu vertreten sind, nicht geliefert werden können, besteht kein Anspruch auf Nachlieferung oder Erstattung vorausbezahlter Beträge.

Unternehmen leben länger mit

IT-Security Schutzmaßnahmen

SCAN ME

Mehr Infos dazu im Printmagazin

itsecurity

und online auf **www.it-daily.net**