ISSN 1864-0907
JUNI 2022

IT-BUSINESS

IT-SECURITY

CHANNEL GUIDE

VOGEL IT MEDIEN

FUJITSU

Microsoft HCI Lösungen für Ihre Kunden-projekte – aus einer Hand!

Rechenzentren nahtlos mit der Cloud verbinden

PRIMEFLEX for Microsoft Azure Stack HCI ist der schnellste und einfachste Weg, die Rechenzentren Ihrer Kunden mit Kapazitäten aus der Cloud zu erweitern. Viel Know-How, Trainings und neue Tools & Prozesse sorgen dafür, dass Sie auf Fujitsu zählen können und PRIMEFLEX Projekte jetzt einfacher umsetzen können.

Die Azure Stack HCI Show: Wissen schadet nicht!

Als offizieller Premium Sponsor empfehlen wir Ihnen die „Azure Stack HCI Show“ von Manfred Helber und Sven Langenfeld:

- Jeden zweiten Freitag, 12:00 bis 13:00 Uhr
- Insights rund um Azure Stack HCI, Windows Server, Azure Arc oder Azure Lighthouse

Azure Stack HCI Show

Weitere Informationen und den Link zur ASHCI Show:
www.fujitsu.com/de/channel-ashci/

Microsoft Azure

Azure. Invent with purpose.

Im Mittelpunkt der Digitalisierung steht Security

Sylvia Lösel,
Chefredakteurin IT-BUSINESS

BILD: KRAS99 - STOCK.ADOBE.COM

865.000 US-Dollar betrug 2021 die durchschnittliche Lösegeldsumme bei Ransomware-Angriffen. Eine Goldgrube für Hacker tut sich da gerade im Zuge der Digitalisierung vieler Unternehmen auf, die oft erst durch solche Vorfälle erkennen, wie wichtig ein durchgängiges Security-Konzept ist. Immer mehr Daten befinden sich im digitalen Kreislauf, immer mehr Geräte werden angeschlossen und durch die Einbindung von Cloud-Instanzen erhält der Unternehmens-Schutz zusätzliche Komplexität.

68.000 fehlende Security-Experten in Deutschland machen die Sache allerdings nicht einfacher. Denn wie soll man schützen, wenn es viel zu wenig Leute gibt, die sich um diesen Schutz kümmern können? Automatisierung, Vereinfachung und Management-Plattformen sollen Abhilfe schaffen, damit wenige Experten viel bewirken können.

38 Prozent der Industrieunternehmen planen, die Ausgaben für OT-Sicherheit deutlich zu erhöhen. Das zeigt: die Digitalisierung in der Industrie nimmt zu und sorgt für viele neue Security-Projekte im Channel. Umso besser, dass sich gerade neue VADs formieren und die Internationalisierung der Branche voranschreitet. Denn Security macht nicht an Grenzen halt.

Ich wünsche Ihnen
eine aufschlussreiche Lektüre!

sylvia.loesel@vogel.de

IT-BUSINESS CHANNEL GUIDE IT-Security

Lebensversicherung für Unternehmen
Mehr Daten, mehr Cloud, mehr Geräte – Unternehmen werden immer angreifbarer, ein Rundumschutz immer komplexer. Managed Security kann helfen. Doch auch Systemhäuser und Dienstleister müssen sich im Dickicht der Anbieter und Lösungen zurechtfinden. **6**

Eine neue Riege formiert sich
Distributoren aus dem In- und Ausland haben das Potenzial des Security-Markts erkannt. **14**

Managed Service Provider in Gefahr
Supply-Chain-Attacken auf MSPs haben eine verheerende Multiplikatorwirkung. **18**

Herausfordernde Netzwerksicherheit
Netzwerke sollten 24/7 überwacht werden und MSPs können dies gewährleisten. **26**

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

Christian Milde,
General Manager Central Europe

Branchenweiter Vorreiter für Transparenz und Zuverlässigkeit

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

kas.pr/vertrauen

kaspersky 25 years DREAM DIGITALLY. PROTECT FOR REAL.

So sicher wie in einer Glaskugel ist man in der hybriden IT-Welt selten.

BILD: ALPHASPIRIT - STOCK.ADOBE.COM

Vom Kostenfaktor zur Lebensversicherung

Die Digitalisierung sorgt für eine größere Angriffsfläche, die Cyberkriminelle gerne nutzen. Deshalb boomt IT-Security und zahlreiche neue Anbieter tummeln sich im Markt. Wo für sie und Partner die Reise hingeht, bleibt spannend.

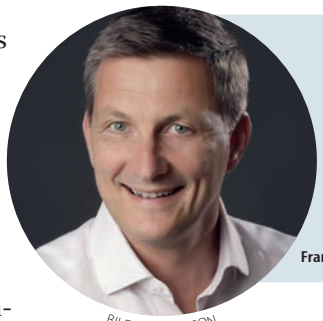


BILD: CYBEREASON

>> Security ist kein Firewall- oder Endpoint-, kein SASE und kein Zero-Trust-Problem, Security ist ein Data-Analytics-Problem.

Frank Kölmel, Vice President Central Europe bei Cybereason

„Früher hat man Security als Kostenfaktor gesehen. Aber zusehends verstehen Unternehmen, welchen Geschäftseinfluss ein Sicherheitsvorfall haben kann und Security wird mehr und mehr als ‚Versicherung' gesehen." Julien Antoine, CEO beim Distributor Infinigate, beschreibt treffend den Kulturwandel, der gerade in Unternehmen jeglicher Branche und Größe vor sich geht. Apropos Versicherung: In den vergangenen Jahren waren Cyberversicherungen ein gängiger Bestandteil des Risikomanagements vieler Firmen. Jetzt hat sich der Wind gedreht, denn die immense Ransomware-Angriffswelle und andere Sicherheitsbedrohungen haben dieses Geschäftsmodell der Versicherungsgesellschaften erheblich unter Druck gesetzt. Die Cyberkriminalitätszahlen, und damit auch die Schadenssummen, sind förmlich explodiert, wie Mohamed Ibbich, Director Solutions Engineering bei BeyondTrust weiß.

„Einerseits gibt es einen längst überfälligen Quantensprung bei der Digitalen Transformation, um den pandemiebedingt neuen Anforderungen gerecht zu werden, andererseits hat das auch einen Wettlauf auf Seiten der Cyberkriminellen ausgelöst, die sich die schlagartig vergrößerte Angriffsfläche zunutze machen." Und Marktforschungskollege Frank Dickson, Vice President bei IDC, ergänzt: „Einerseits verspricht Remote Work Flexibilität und Agilität, andererseits kann sie die Ursache von Security-Schwachstellen sein. Dies betrifft nicht nur Perimeter und Endpoints, sondern auch die größere Angriffsfläche in der Cloud." Das Wall Street Journal bezeichnete hybride Arbeitsplatzstrukturen sogar als „Cybersecurity-Alptraum". Dafür sorgen die sich ständig verändernde Mischung aus Büro- und Remote-Mitarbeitern, immer neue Geräte innerhalb und außerhalb der Unternehmensnetze sowie personelle Engpässe, um nur einen Bruchteil der Faktoren zu nennen, die die neue Welt so vulnerabel machen. Eine ISC-Studie weist für Deutschland aktuell 68.000 fehlende Security-Experten aus, 6.000 mehr als 2021. In der Folge leiden das Risiko-Assessment und -Management, das Patch-Management sowie das Wissen um potenzielle Bedrohungen. (siehe Grafik Seite 8).

All dies hat Folgen, erläutert Antoine. „Es ist daher Aufgabe des Channels, Kunden nicht nur in Bezug auf Technologie, sondern auch hinsichtlich der Sicherung von Geschäftsprozessen zu beraten." Die Distribution sieht er dabei natürlich als entscheidenden Akteur. Denn Distribution ist längst nicht mehr ausschließlich ein Produkt von A nach B zu bringen. „Es geht darum, Beschleunigung und Wachstum für Reseller und Hersteller zu schaffen" Wichtig ist, Wissen rund um Abonnements und Cloud aufzubauen und als Multiplikator zu agieren. Luca Brandi, EMEA Channel Sales Director bei Trellix, sieht das ähnlich: „Wir konzentrieren uns auf den SMB-Markt,

BILD: ADN

>> Durch die hohe Individualität des Angebots wird in dem Moment auch ein starrer Preisvergleich obsolet. Des Weiteren erreichen Partner eine engere Kundenbindung, haben sichere monatliche Einkünfte und generieren zudem zusätzliche Upsell-Möglichkeiten.

Michael Bölk, Leiter Professional Services DACH, ADN

denn die Digitalisierung ist gerade für alle Unternehmen ein heißes Thema." Die Distribution kennt dabei sowohl den jeweiligen Markt als auch die Hersteller. Für ihn ist klar: „Wir brauchen ein Ökosystem von Partnern, die in der Lage sind, Services anzubieten. Und wenn sie das noch nicht können, brauchen wir die Distribution, die ihnen dabei hilft – mit Beratung aber auch mit Services, die der Partner selbst nicht anbieten kann oder möchte." Neben den Leistungen der Distribution ist für den Channel aber noch ein weiterer Punkt entscheidend: Einfachheit. „Es geht nicht nur da-

DIE KONSEQUENZEN DES FACHKRÄFTEMANGELS

BILD: (ISC)2 CYBERSECURITY WORKFORCE STUDY, 2021

Die ISC-Studie Cybersecurity Workforce sammelte Umfragedaten von 4.753 Cybersicherheitsexperten, die in KMU und großen Organisationen in Nordamerika, Europa, Lateinamerika und Asien-Pazifik arbeiten.

rum, wer die beste Technologie hat, sondern auch, wer den schnellsten Marktzugang schafft. Dies wird umso wichtiger, je mehr Player sich im Security-Markt tummeln. Und das sind einige. Kamen in den vergangenen Jahren doch zu den traditionellen Anbietern zahlreiche Cloud-native Spezialisten hinzu, die alle ihre Marktnische und ihren Kundenkreis suchen. Ob SentinelOne, Cybereason, Crowdstrike oder ExtraHop – es ist eine echte Herausforderung, den Überblick über die Anbieter zu bewahren, geschweige denn über die Lösungen. Denn in Zeiten von Cloud- und Plattformdenken wird hier munter kombiniert. Die Plattform des Herstellers A mit Technologieschnittstellen zu Hersteller B. Am besten dann noch angereichert mit eigenen Services der Distribution oder der Partner selbst.

Dazu kommen zahlreiche Schlagworte, die im Markt herumschwirren, wie XDR, SASE, Zero Trust oder CASB. Nicht verwunderlich, dass Kunden überfordert sind und sich so gerne an Dienstleister und Systemhäuser wenden, um ihre Umgebungen abzusichern und die Verantwortung für Datenschutz und Security gerne an diese auslagern. Von Einfachheit kann in diesem Sammelsurium dann nur noch schwer die Rede sein. Wie sich der Markt gewandelt hat, beschreibt Frank Kölmel, General Manager EMEA bei Cybereason: „Security ist kein Firewall- oder Endpoint-, kein SASE- und kein Zero-Trust-Problem. Security ist ein Data-Analytics-Problem." Das hat Folgen. Von einer Hardware- und Produktlastigkeit geht die Reise zu Plattformen, Cloud-Security und Services. Als Partner habe man drei Grundbedürfnisse, wenn man auf Managed Security Services setze, erklärt Jens Pälmer, Channelchef bei Cybereason: „Man möchte schnell guten Service anbieten, den Aufwand und die Total Cost of Ownership reduzieren." Für Marktakteure ist deshalb die Herausforderung, Kunden und Partner „schnell mit auf die Reise zu nehmen und auch bei Kunden den Mehrwert aufzuzeigen", sagt Pälmer. Doch in die Cloud geht es nicht von heute auf morgen, sondern meistens ist es eine Reise, bei der die On-Premises-Welt mitbedacht werden muss. „Viele Hersteller haben Security-Lösungen für die Cloud, aber nicht für On-Prem. Denn konservative Mittelstandskunden benötigen genau so etwas. Das ist ein echter Türöffner für viele Partner," ist Pälmer sicher.

Dass Partner Unterstützung bei der Orientierung im Markt und beim Aufbau neuer Erlösmodelle benötigen, hat die Distribution erkannt. „Wir können dank der Ressourcen unseres Professional-Services-Teams technische Aufgaben so lange übernehmen, bis der Partner selbst fit ist. Beispiele dafür sind etwa die Full Managed Firewall für unsere Reseller und deren Endkunden, die wir mit Sonicwall oder Watchguard realisieren. Basierend auf den Lösungen der Hersteller Proofpoint, No Spam Proxy oder Hornetsecurity bieten wir Full Managed Mail Security an", beschreibt Michael Bölk, Head of Professional Services DACH bei ADN, die Herangehensweise.

Ähnlich sieht es bei Nuvias aus. Der Distributor bietet mit dem Managed-Services-Programm flexible Security-Dienstleistungen. „Die Angebote unterstützen Reseller bei Aufbau und Erweiterung ihrer Geschäftsmöglichkeiten und ergänzen deren bisherige Dienstleistungen", sagt Helge Scherff, Regional Vice President Central Europe bei Nuvias. Für Partner sieht Bölk weitere Vorteile: „Durch die hohe Individualität des Angebots wird in dem Moment auch ein starrer Preisvergleich obsolet. Des Weiteren erreichen Partner eine engere Kundenbindung, haben sichere monatliche Einkünfte und generieren zudem zusätzliche Upsell-Möglichkeiten." Einen weiteren Trend in der Partnerlandschaft beobachtet Patrick Pulvermüller, CEO bei Acronis, nämlich „eine zunehmende Vertikalisierung, um die Kundenbedürfnisse besser adressieren und sich selbst differenzieren zu können. Eine Digitalagentur hat ganz andere Datenmengen, ganz andere Proble-

Wie kann die Sicherheit und eine uneingeschränkte Konnektivität von Fabrikanalagen gewährleistet werden?

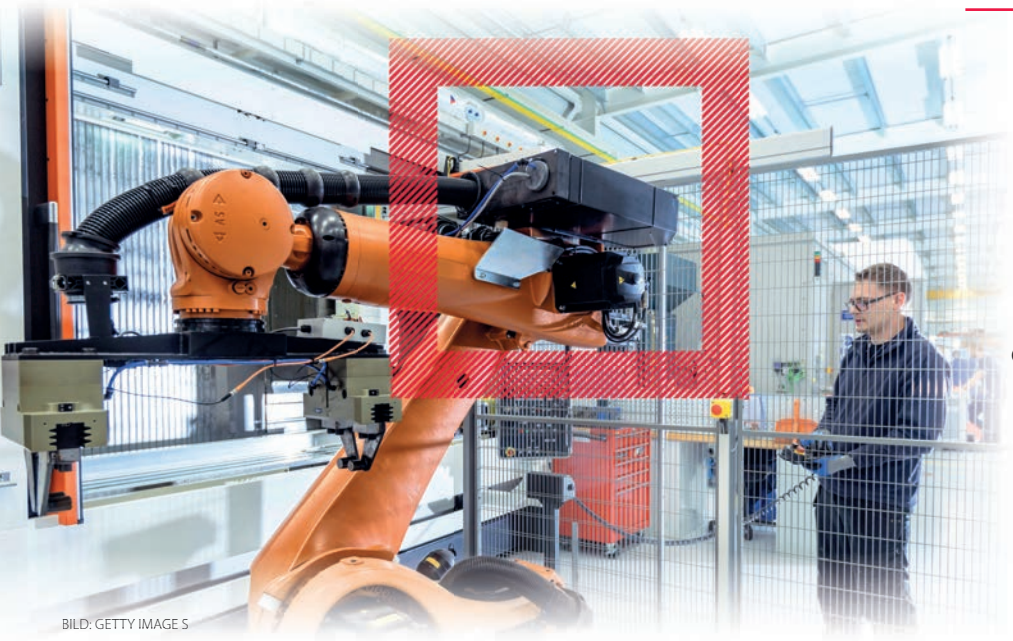


BILD: GETTY IMAGE S

Die Stichwörter Resilienz und IT-Sicherheit sind momentan aktueller denn je und überall zu lesen. Kein Wirtschaftszweig bleibt mehr von Ransomware Angriffen verschont. Und auch von veralteten und unsicher vernetzten Maschinen und Anlagen gehen Risiken aus. Doch solche Komponenten lassen sich durch ein Digitalisierungs- und Security-Retrofit sicher an aktuelle Infrastrukturen anbinden.

Egal von welchen Ecken die unerwünschten Gäste eindringen – wenn sie einmal drin sind, legen sie die gesamte IT-Landschaft lahm. Die Ausfälle reichen von nicht funktionierenden Softwaresystemen bis hin zum Stillstand kompletter Industrieanlagen. Nicht selten ist es der Fall, dass Bedrohungen von der Maschinenanlage direkt ausgehen, da veraltete Maschinen Betriebssysteme aufweisen, welche meist nicht mal mehr gepatched werden. Besonders auffällig war zuletzt das Netzwerkprotokoll SMB 1, welches bei Legacy-Fabrikanlagen eine Schwachstelle darstellte. Solch ein Einfallstor kann im gesamten Produktionsnetz als Vervielfältiger zu einem Produktionsstopp und damit verbundenen Einbußen führen. Organisationen sei damit dringendst geraten im Zuge einer Neuanschaffung auch ein Retrofit durchzuführen.

Am besten eignen sich hierfür Lösungen, die zum einen zukunftsfähige Funktionen für die OT-Welt und zum anderen sichere Maßnahmen für die IT-Welt mitbringen. Edge Computing ist die Technologie, welche in diesem Fall in Frage kommt. Mit secunet edge können beispielsweise mehrere Maschinen entweder direkt oder in einzelnen Zonen an die IT-Infrastruktur angebunden werden. Damit ist die OT-Seite von der IT-Seite abgeschirmt und Eindringlinge können sich nicht einfach verbreiten. Die Zonierung trägt aber nicht nur zu der Sicherheit bei, sondern ermöglicht auch eine zentrale Steuerung, gruppierte Rollouts oder System-Patches.

Auch Legacy-Anlagen profitieren von secunet

Das Schöne daran ist, dass dies auch nachgerüstet werden kann. Gerade zu der Pandemie haben noch einmal mehr Firmen von nachträglich angebunden Edge-Technologien profitiert. Fernwartung war ein beliebtes Beispiel. Keine Anfahrtskosten und zeitbegrenzte Zugriffe auf die Unternehmensinfrastruktur erwiesen sich als Vorteil.

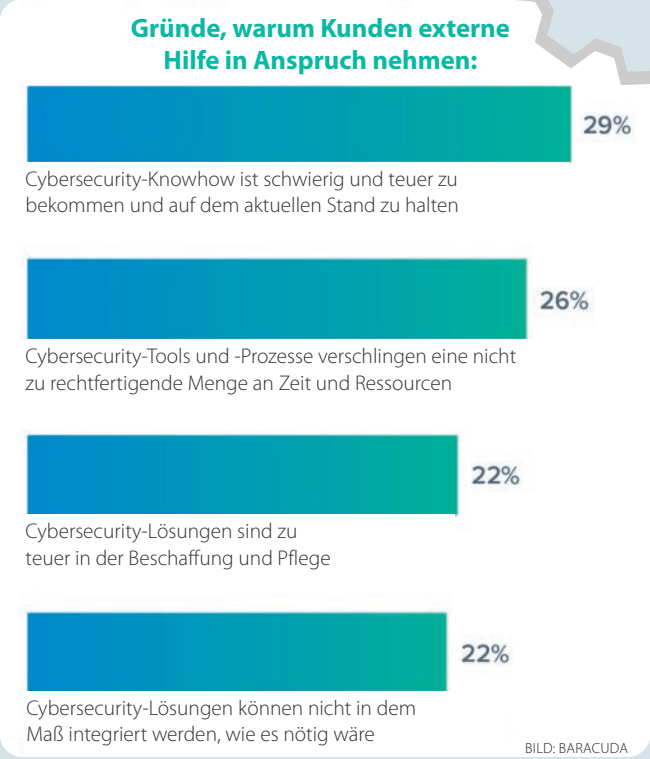
Legacy-Infrastrukturen mit neuen Komponenten nach dem Zero-Trust Ansatz zum Beispiel und der Aufbau von ganzheitlichen neuen Infrastrukturen schließen sich nicht aus. Für gewöhnlich ist ein kompletter Neuaufbau nicht realistisch. Zudem sind einige Neuheiten auf dem Markt noch in der Reifephase mit den damit verbundenen Betriebs- und Sicherheitsherausforderungen. Daher ist ein schrittweiser Umstieg der beste Weg. Die Lösung secunet monitor bietet hierfür eine Asset-Erkennungsfunktion an. Von physisch definierten Systemen und Netzwerken hin zu hoch virtualisierten Infrastrukturen. Mit secunet monitor kann mit dem tatsächlichen Netzwerkverkehr erkannt werden, welche Komponenten oder Ressourcen vorhanden sind. Mit Hilfe dessen können erste Schritte in Richtung Zero-Trust gegangen werden. Ein Beispiel könnte hier die Übersetzung von erlernten Zugriffsbeziehungen über die Firewall von Edge Appliances sein.

Egal von welchem Einfallstor die Ransomware nun in das Unternehmen gelangt - Fakt ist, dass sich Cyberbedrohungen weiterentwickeln und noch perfider, schneller oder häufiger werden. Dieser Herausforderung müssen wir uns stellen und die richtigen OT-Security-Anbieter auswählen. Erfahren Sie mehr über secunet edge bei Ihrem Distributor Tech Data.

Weitere Informationen
secunet - Tech Data Digital World (techdata-events.com)

STEIGENDE SECURITY-REGULIERUNGEN VERUNSICHERN UND UNTERSTÜTZUNG WIRD IMMER WICHTIGER

- MSPs erwarten für 2022 ein Umsatzwachstum von mehr als einem Drittel. Der durchschnittliche Umsatz in diesem Jahr wird bei 12,12 Millionen US-Dollar liegen.
- Im Jahr 2021 stammten 53 Prozent der Einnahmen aus Managed Services, für 2022 erwartet man einen Anstieg auf 63 Prozent.
- Für 2022 erwarten 94 Prozent der Befragten, dass ihr Service-Portfolio um durchschnittlich sechs Angebote wachsen wird. 2021 waren es durchschnittlich vier Services.
- Die Besorgnis der Kunden vor Cyberangriffen nimmt zu, gaben 80 Prozent der Befragten an.
- Nur 36 Prozent der befragten MSPs sind zuversichtlich, dass sie mit den Cybersecurity-Vorschriften auf dem Laufenden seien und sie einhielten. Weitere 36 Prozent glauben, dass es zu viele Vorschriften gebe.
- 89 Prozent sind der Meinung, dass ihre Unternehmen weitere Unterstützung und Schulungen zu Cybersecurity-Vorschriften benötigen.
- 98 Prozent der Befragten meinten, dass sie in mindestens einem Bereich zusätzliche Unterstützung durch einen Hersteller benötigen. Dazu gehörten die Planung der Reaktion auf Sicherheitsvorfälle für 44 Prozent, Hilfe bei bewährten Verfahren für hybrides Arbeiten für 50 Prozent und Marketingunterstützung für 44 Prozent der Befragten.



Wenn Sie an die Kunden Ihres Unternehmens denken: Aus welchen Gründen suchen Sie bei Cybersicherheit externe Hilfe?

me wie beispielsweise ein Retailer oder ein Industrieunternehmen", erläutert er. „Wir erwerben deshalb für unsere Lösung so viele Zertifikate wie möglich, um es Partnern möglichst einfach zu machen, diese beispielsweise auch in regulierten Bereichen einzusetzen und auf die Kundenbedürfnisse hin zuzuschneiden."

Und als ob diese Vielfalt noch nicht genug sei, kommt ein weiteres Spannungsfeld hinzu: Globalität und Regionalität. „Man merkt eine Entglobalisierung und eine Renationalisierung, was die Infrastruktur betrifft", stellt so auch Pulvermüller fest. „Unser Wettbewerbsvorteil ist, dass wir in 50 verschiedenen Regionen vertreten sind. Wir sind ein globales Unternehmen, das aber lokale Ausprägungen hat. Acronis hat inzwischen fast 50 Rechenzentren weltweit, jedes Quartal kommen fünf bis sechs neue Rechenzentrums-Lokationen hinzu, um Daten wirklich im jeweiligen Land halten zu können. Dieser Trend wird bleiben." Denn weder machen Cyberangriffe an Staatsgrenzen halt, noch beschränken sich Unternehmen auf ein Land. In einer globalisierten Welt muss auch eine Sicherheitsstrategie global gedacht werden. Dennoch gilt es, nationalstaatliche oder regionale Besonderheiten und Bedürfnisse hinsichtlich Datensouveränität, Gesetzesvorschriften und vielem mehr zu berücksichtigen.

Viel zu tun. Das ist auch im Channel zu spüren. Es bauen zahlreiche Dienstleister und Systemhäuser ihre Security-Einheiten deutlich aus und es drängen immer mehr Beratungsunternehmen in den Markt. Aktuellstes Beispiel: Materna, die gerade ein neues Systemhaus gegründet haben, das Sicherheitsbehörden mit schlüsselfertiger IT- und Rechenzentrums-Infrastruktur beliefert. Denn Sicherheit wird auch künftig ein Basis-Baustein sein, wenn IIoT und datengetriebene Geschäftsmodelle weiter an Relevanz gewinnen.

Mehr zu Managed Security:
www.it-business.de/Man-Sec

Autor:
Sylvia Lösel

terra
IT. MADE IN GERMANY.

TERRA CLOUD

IT-SECURITY
AUS EINER HAND

terra CLOUD

intel

Microsoft

DIE CHANNEL CLOUD

Das Thema Sicherheit wird bei uns groß-geschrieben, deshalb setzen wir auf unsere **Always-private-Strategie.**
Jede Infrastruktur beinhaltet eine Firewall, so dass ein privates Kundenetzwerk inklusive VLAN und IP zugrunde liegt.

Sicheres Netzwerk.

FWaaS
Ihre Firewall ist als monatliche Leistung virtuell oder als Hardware Appliance erhältlich.

Umfassender Virenschutz.

Antivirus Pro
Die Antivirus-Lösung für Ihre Cloud Server, lokalen Server sowie Endgeräte mit einer cloudbasierten Management Oberfläche.

Sicher unterwegs.

Mobile Security
Schließen Sie Sicherheitslücken von mobilen Endgeräten in Sekundenschnelle, mit Hilfe einer cloudbasierten und templatefähigen Lösung.

Sicher archivieren.

UMA as a Service
Innovative E-Mail Archivierung für kleine und mittelständische Unternehmen nach BSI-Norm.

B
Backup

Backup
Wissen, wo Ihre Daten liegen. Professionelles und automatisiertes Backup aus der TERRA CLOUD in Hüllhorst.

Microsoft Security
Ergänzen Sie Ihr Cloud Angebot durch Security Produkte aus dem Hause Microsoft. Mit Microsoft Defender for Business erhalten Sie Sicherheits-Software auf höchstem Niveau.

Erfahren Sie mehr zur TERRA CLOUD
Unseren TERRA CLOUD Vertrieb erreichen Sie unter:
Telefon: +49 5744.944 188 | E-Mail: cloud@wortmann.de
www.wortmann.de | www.terracloud.de

WORTMANN AG
IT. MADE IN GERMANY.

Wachstumsmarkt IT-Security

Die Zahl der Cyberangriffe in Deutschland steigt und damit auch die Relevanz der IT-Sicherheit. Der Bitkom rechnet 2022 mit Ausgaben von rund **6,8 Milliarden** Euro für Security-Hardware, -Software und -Services. Bis zum Jahr 2025 sollen diese auf bis zu **8,9 Milliarden** Euro ansteigen. Die Security-Ausgaben nehmen seit 2017 mit einer jährlichen Wachstumsrate von über **10 Prozent** zu.

BILD: STATISTA / BITKOM

BILD: CROCOTHERY - STOCK.ADOBE.COM

Unternehmen reagieren

Wegen steigenden IT-Sicherheitsvorfällen haben laut Eco – Verband der Internetwirtschaft, 54 Prozent der Unternehmen die Ausgaben für IT-Security erhöht.

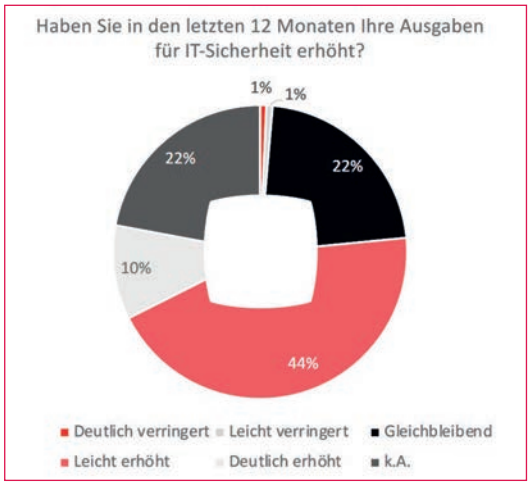


BILD: ECO – VERBAND DER INTERNETWIRTSCHAFT

IT-Sicherheit im Homeoffice? Egal!

Über ein Viertel der von Provectus Technologies und Splendid Research befragten Homeoffice-Arbeiter macht sich wenig bis gar keine Gedanken um die IT-Sicherheit beim mobilen Arbeiten.

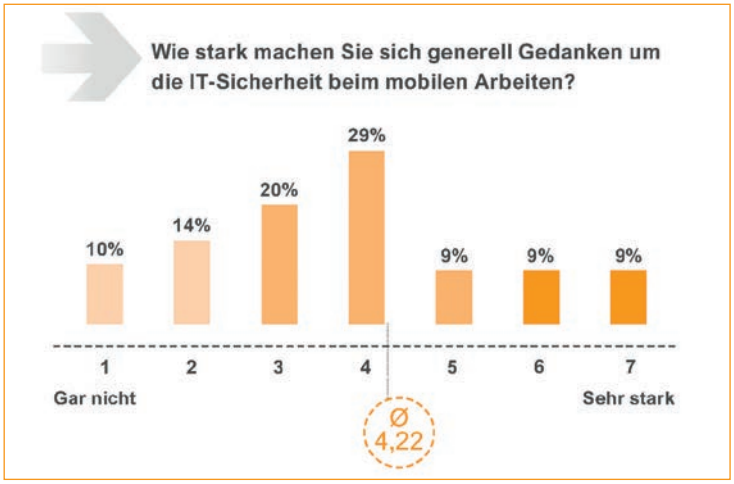


BILD: PROVECTUS TECHNOLOGIES

Alle Segmente wachsen

Information Security & Risk Management, Ausgaben Endverbraucher nach Segmenten, 2021-2024 (in Milliarden US-Dollar)

Marktsegment	2021	2022	2023	2024
Application Security	5,238	6,413	7,93	9,725
Cloud Security	1,062	1,425	1,958	2,66
Data Security	3,494	3,905	4,427	5,009
Identity Access Management	14,954	16,954	19,397	22,195
Infrastructure Protection	25,915	29,803	34,589	39,89
Integrated Risk Management	5,547	6,311	7,175	7,958
Network Security Equipment	18,084	19,761	21,518	23,192
Andere Information Security Software	2,556	2,681	2,878	3,13
Security Services	71,081	74,266	80,016	87,186
Consumer Security Software	6,844	6,878	7,151	7,505
Gesamt	**154,777**	**168,397**	**187,038**	**208,45**

Bis 2024 sollen die weltweiten Ausgaben für Sicherheit und Risikomanagement auf über **208 Milliarden** US-Dollar steigen, so die Prognosen von Gartner.

BILD: GARTNER

Cyberangriffe auf Unternehmen nehmen zu

Die Zahl der Cyberangriffe auf Unternehmen ist laut dem Security Navigator 2022 von Orange Cyberdefense in den vergangenen 12 Monaten um 13 Prozent gestiegen. Davon betroffen waren alle Unternehmensgrößen.

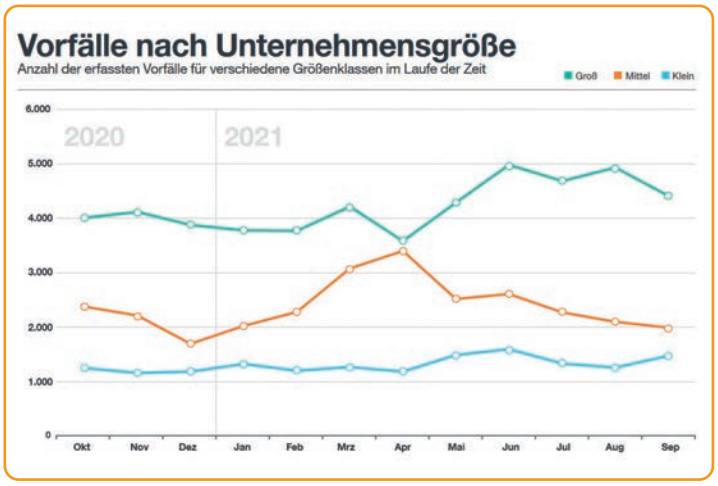


BILD: ORANGE CYBERDEFENSE

BILD: BERND ARNOLD

„Schnell wechselnde Cyber-Bedrohungen und ein falsches Vertrauen in den Cyber-Schutz schaffen ein enormes, oft verstecktes Geschäftsrisiko."

Dr. Sebastian Schmerl,
Director of Security Services für EMEA
bei Arctic Wolf

37 Prozent der von Arctic Wolf befragten IT-Entscheidungsträger und Führungskräfte glauben, dass **Cyberangriffe** überhaupt keine Gefährdung für ihr Unternehmen darstellen.

Es fehlt an Security-Fachkräften

Eine Umfrage von Arctic Wolf zeigt, dass viele der befragten IT- und Sicherheitsverantwortlichen mit erheblichen Hürden beim Rekrutieren neuer Teammitglieder konfrontiert sind. Dies hat zur folge, dass oftmals die IT-Security-Ziele der Unternehmen nicht erreicht werden können und sich das Cyberrisiko erhöht.

BILD: DUNCAN ANDISON - STOCK.ADOBE.COM

76 %

der Befragten erklärten, die größten Hürden beim Erreichen ihrer IT-Security-Ziele seien das Einstellen neuer Fachkräfte oder mangelnde Fachkenntnisse der bestehenden Mitarbeitenden.

44 %

der befragten Unternehmen verfügen über keine Mitarbeitenden, die Vollzeit oder primär mit dem Thema Cybersicherheit betraut sind

Ohne ein dediziertes Cyber-Security-Team oder Security Operations Center (SOC) wird das Thema IT-Sicherheit häufig noch immer vernachlässigt und ist nur eine von vielen Aufgaben der zuständigen Mitarbeitenden.

BILD: STATISTA / BITKOM

BILD: MICHELLE ALBERS - STOCK.ADOBE.COM

Eine neue Riege von VADs formiert sich

Bewegung in der Distribution: VADs wie Ebertlang und Prianto entwickeln ihr Security-Geschäft systematisch weiter, Newcomer wie Cyber Monks entstehen, und weitere Distributoren aus dem Ausland kommen in den deutschen Markt.

Internationale Gruppen wie Arrow, Exclusive, Infinigate, Nuvias und Westcon dominieren die Security-Distribution. Wer als Reseller oder MSP nach Produkten eines relevanten Herstellers sucht, wird garantiert bei mindestens einem dieser VADs fündig. Jenseits der Big Five agieren im deutschen Channel aber noch etliche andere Security-Spezialisten. Gerade in ihren Reihen tut sich momentan einiges. Angesichts des enormen Wachstumspotenzials verwundert die Aktivität nicht. So rechnet der Branchenverband Bitkom für das laufende Jahr damit, dass sich das Gesamtvolumen des deutschen Security-Markts erneut um knapp zehn Prozent erhöht, und zwar auf 6,8 Milliarden Euro. Sowohl VADs aus Deutschland als auch aus dem europäischen Ausland bringen sich derzeit im hiesigen Markt in Stellung.

Ein Beispiel dafür ist der Software-Distributor Prianto, zu dessen Portfolio seit jeher auch IT-Sicherheitsprodukte gehören. Im Februar dieses Jahres hat das Münchner Unternehmen eine dedizierte Business Unit für Cybersecurity ins Leben gerufen, die mit einem 13-köpfigen Team und 16 Anbietern an den Start ging. Zu den Herstellern zählen CyberRes, Flexera, Greenbone, Mateso oder Sailpoint. Seitdem ist das Angebot weiter gewachsen, unter anderem durch Neuverträge mit Cyfirma und Logpoint. Außerdem hat Prianto durch die Akquisition des Mitbewerbers ISP*D aus Poing im April einige Distributionsverträge mit Security-Anbietern, nicht zuletzt mit Bitdefender, übernommen. „Wir können mittlerweile die gesamte Range an Security-Technologien bereitstellen“, betont William Geens, Geschäftsführer des Unternehmens.

Ein ganzheitliches Security-Portfolio streben auch die Verantwortlichen bei Ebertlang an. Der Software-Spezialist aus Wetzlar vertreibt seit langem Sicherheitsprodukte, etwa von Anbietern wie Appriver, Eset oder Qbik. Dabei hatten die Hessen nicht den Anspruch, alle wesentlichen Disziplinen abzudecken. Vielmehr gab es bei ihnen eine gewisse Scheu vor Produktkategorien, die mit Hardware verbunden sind, wie etwa Firewalls. Der frühere Mailstore-Manager Philip Weber, der seit Februar 2021 als CEO an der Spitze von Ebertlang steht, möchte das Unternehmen nun im Security-Segment breiter aufstellen. Ein Schritt zum Ausbau des Portfolios war im Oktober 2021 die Übernahme des Würzburger Mitbewerbers 8Soft,

Der Markt für Security-Technologien wächst in Deutschland laut Branchenverband Bikom um knapp zehn Prozent. Daran partizipiert auch die Distribution.

BILD: MICHAEL TRAITOV - STOCK.ADOBE.COM

durch die Ebertlang zusätzliche Herstellerverträge, unter anderem mit Kaspersky, erworben hat. Aktuell vertreibt der VAD die Produkte von zehn Security-Anbietern. Da die Wetzlarer langjährige Erfahrung im Managed-Service-Geschäft besitzen, wollen sie sich Weber zufolge „frühzeitig mit den richtigen Lösungen für Managed Security Service Provider positionieren".

Unter der Marke Cyber Monks formierte sich im Herbst 2020 ein neuer VAD, der sich ebenfalls auf Managed Security Services fokussiert. Das Unternehmen wurde in Frankfurt / Main gegründet, und zwar von ehemaligen Führungskräften des Distributors Spectrami mit Sitz in Dubai, der sich zuvor aus Europa zurückgezogen hatte. Cyber Monks versteht sich in erster Linie als Enabler, der Systemhäuser in die Lage versetzt, ihre Kunden dauerhaft gegen Cyberbedrohungen zu schützen. Dazu erbringt das Unternehmen eine Reihe von Dienstleistungen, zu denen auch die Bereitstellung von Managed Services als Whitelabel gehört. Der VAD arbeitet mit etwa 15 Herstellern zusammen, darunter Eset und Tanium.

Einige Distributoren aus dem Ausland haben ebenfalls das Potenzial des deutschen Security-Markts erkannt. So nahm der italienische VAD Icos im Frühjahr 2021 hierzulande mit acht Herstellern den Betrieb auf. Im April dieses Jahres kaufte das Unternehmen aus Ferrara den Münchner Mitbewerber Brainworks, der auf Collaboration-, Netzwerk- und Sicherheitslösungen spezialisiert ist. Der erworbene Distributor soll in die deutsche Landesgesellschaft von Icos eingegliedert werden. Auch der Schweizer VAD Boll, nach eigenen Angaben im Heimatmarkt die Nummer eins im Security-Segment, kündigte im Februar dieses Jahres an, er plane, das Geschäft in Deutschland auszubauen. Die Eidgenossen sind seit drei Jahren mit einem Büro in Ulm vertreten und bieten dem Channel hierzulande die Produkte von acht Herstellern an. Darüber hinaus stieg im März 2021 die britische CMS-Gruppe beim Schorndorfer Distributor Sysob ein, der seither sein Security-Portfolio weiter verstärkt hat.

Mehr unter:
www.it-business.de/-a-1024671/

Autor: Michael Hase

DIE INTERNATIONALISIERUNG DER SECURITY-DISTRIBUTION

In der Security-Distribution setzte vor mehr als zehn Jahren die erste Welle der Internationalisierung ein. Im Zuge dessen gaben hiesige Spezialisten ihre Unabhängigkeit auf und schlossen sich europa- oder weltweit agierenden Gruppen an, die auf diese Weise ihr Geschäft auf den deutschen Markt ausdehnten. So kaufte die internationale Westcon Group Mitte 2011 den Paderborner VAD Entrada. Exclusive Networks aus Frankreich übernahm Anfang 2012 den Distributor TLK mit Hauptsitz in Münster. Der britische Security-Spezialist Wick Hill, bis dahin nur in Deutschland und UK aktiv, verschmolz im Frühjahr 2017 mit Zycko zur Nuvias Group. Mit Icos, Boll und CMS expandieren nun weitere Distributoren aus dem Ausland, die freilich nicht die Marktmacht der zuvor genannten Gruppen haben, nach Deutschland.
Andere VADs aus dem hiesigen Markt wie Computerlinks oder Infinigate trieben die Internationalisierung aus eigener Kraft voran. Bereits in mehr als 20 Länder inner- und außerhalb Europas aktiv, wurde Computerlinks im Herbst 2013 vom nordamerikanischen Distributor Arrow übernommen und ging in dessen Organisation auf. Die Schweizer Infinigate Group, die in Deutschland den größten Anteil ihrer Einnahmen erzielt, expandierte seit 2008 außerhalb der DACH-Region und ist heute in elf europäischen Ländern präsent.

Überschreibverbot für Ransomware

Dateien verschlüsseln, umbenennen und die Quelldatei löschen – Erpresser, die so weit ins System eingedrungen sind, machen das automatisiert und perfide.

BILDER: RAWF8 - STOCK.ADOBE.COM

Der Schadcode von Ransomware ist wahrlich fies. Er nimmt sich Dateien, verschlüsselt diese, benennt sie dabei um und löscht dann die Ursprungsdatei. Schaden lässt sich begrenzen, indem Verschlüsselungsversuche Alarme auslösen. Außerdem können mit der Snaplock-Funktion Dateien so abgespeichert werden, dass diese nicht löschbar, beziehungsweise nicht überschreibbar sind. Das spielt insbesondere im Backup- oder Archivierungs-Kontext eine Rolle. Denn wird auf Sicherungsdateien zurückgegriffen, die womöglich schlafenden Ransomware-Code enthalten, hat sich der Admin quasi selbst ausgetrickst. Die Höhe einer durchschnittlichen Lösegeldzahlung betrug im Jahre 2021 laut Palo Alto Networks übrigens rund 865.000 US-Dollar pro Vorfall. Keine Frage: Vor diesem Hintergrund sollte Ransomware-Schutz keine Frage des Budgets sein.

Die Zunahme von Ransomware-Angriffen hat längst dazu geführt, dass die meisten Anbieter von Backup- und Wiederherstellungs-Lösungen inzwischen die Erstellung unveränderlicher Zweitkopien durch WORM-fähigen (Write Once, Read Many) Speicher unterstützen. Aus solchen Speichermedien heraus ist es Ransomware also technologiebedingt nicht möglich zu verschlüsseln, umzubenennen und Ursprungsdateien zu löschen. Allerdings muss schlafender Ransomware-Schadcode durch gezielte Scans danach und durch eine Notfallstrategie mit ausreichend zurückliegenden Backups verhindert werden, damit Systeme auch wiederhergestellt werden können.

IT-Verantwortlichen im KMU-Umfeld ist mitunter nicht klar, dass eine reine Spiegelung des Systems keine adäquate Backup-Strategie für ein drohendes Ransomware-Szenario darstellt. Bei einem gespiegelten System hat man das Problem quasi doppelt, beziehungsweise mehrfach. Vielmehr ist es nötig, Backups so zu erstellen, dass auf frühere Stände der Daten ohne das Ransomware-Problem zurückgegriffen werden kann. In der Praxis bieten sich hier die am häufigsten unterstützten Cloud-Speicher-Ziele an: Amazon Simple Storage Service (Amazon S3) und Azure Blob Storage. Beide können mit besagten Unveränderlichkeitsrichtlinien ausgestattet werden und passen gut in die 3-2-1-Backup-Regel. Diese fordert eine dreifache Kopie mit zwei Speichertechnologien und eine davon außer Haus gelagert. Der dahinter stehende Object Storage bietet etliche Vorteile. Extrem große, unstrukturierte Datenmengen lassen sich mit dieser Systematik sinnvoll organisieren, ablegen und bearbeiten. Der Clou ist die gewonnene Flexibilität: Weil die Datenspeicherung über eine Standardschnittstelle abläuft, können die Daten nach Bedarf zusätzlich On-Premises vorgehalten werden, beispielsweise auf einer I/O-starken Appliance.

Der Begriff „Ransomware“ kombiniert das englische Wort „ransom“ für „Lösegeld“ mit „ware“ aus Software.

Autor: Dr. Stefan Riedl

Penetration Testing der fortgeschrittenen Art

Durch Penetration Tests erhalten Unternehmen ein realistisches Bild der Angreifbarkeit ihrer IT-Infrastrukturen. Synack bietet eine Penetration-Testing-Lösung an, die das Optimum an Technologie mit einem weltumspannenden Spezialisten-Netzwerk vereint.

Synack hievt Penetration Testing auf ein neues Niveau.

BILD: GORODENKOFF PRODUCTIONS OU

Schwachstellen treten in jedem IT-System auf, von der einzelnen Applikation bis zu ganzen Netzwerksegmenten. Traditionell nutzt man zum Aufspüren von Sicherheitslecks sogenannte Vulnerability-Scanning-Werkzeuge. Diese liefern als Resultat ihrer Prüftätigkeit regelmässig eine Liste der erkannten Schwachstellen und klassifizieren sie dabei nach Schweregrad. Vulnerability Scanning ist bei allen größeren Unternehmen Usus und unterstützt das Patch Management massgeblich.

Penetration Tests greifen tiefer

Ein Scan auf bekannte Schwachstellen zeigt jedoch nicht das gesamte Bild, das ein Angreifer von der fraglichen Infrastruktur erlangt. Vulnerability Scanning deckt nur bereits bekannte Sicherheitslecks ab, die sich automatisiert erkennen lassen. Alle anderen Methoden, die Cyberkriminelle für ihre Attacken nutzen, werden nicht erfasst. Denn auch wenn die gesamte Infrastruktur auf aktuellem Stand mit Sicherheitsupdates versorgt ist, können Angreifer auf vielfältige Hacking-Tools und -Methoden zurückgreifen – man denke beispielsweise an Schwachstellen, für welche es noch keine Patches gibt.

Penetration Tests gehen einen Schritt weiter. Auch dabei wird die Infrastruktur zunächst per Vulnerability Scan auf Schwachstellen abgecheckt. Danach jedoch kommt der Mensch ins Spiel: Spezialisierte «White Hat»-Hacker versuchen im Auftrag ihrer Kunden, die Schwachstellen aktiv auszunutzen (natürlich ohne tatsächlich Schaden anzurichten) und liefern einen detaillierten Bericht über die in der Realität erfolgreichen Angriffsmethoden.

Plattformgestützter Managed Service

IT-Dienstleister, die Penetration Testing anbieten, offerieren diesen Service normalerweise als einzelne, zeitlich begrenzte Maßnahme und greifen für die Durchführung meist auf eine relativ kleine Zahl von Experten zurück.

Die technische Basis der Synack-Lösung ist eine Plattform, bestehend aus dem KI-gestützten Vulnerability Scanner Hydra, der Machine Learning Engine Apollo und dem Secure Testing Gateway LaunchPoint. Letzterer kommt dann zum Einsatz, wenn interne Systeme geprüft werden sollen. Die Plattform bietet dem Kunden jederzeit Zugriff auf die laufend aktualisierten Testresultate. Synack verfolgt das Ziel, für Kunden regelmäßige Penetration-Tests auszuführen. Im Speziellen für Applikationen, die sehr häufig aktualisiert werden und besonders geschäftskritisch sind. Dies im Gegensatz zum möglicherweise nur einmal jährlich erhältlichen Report beim Einsatz eines konventionellen Pentest-Anbieters. Anders ausgedrückt: Synack offeriert Penetration Testing nicht nur in Form von einmaligen Testprojekten, sondern auch als Managed Service mit kontinuierlicher Überprüfung der infrage stehenden Infrastrukturen.

Technologie und menschliche Intelligenz vereint

Die Technik ist allerdings nicht alles, was Synack auszeichnet. Sie liefert nur die Basis für das weitergehende Testen. Denn noch wichtiger ist das globale Netzwerk von über 1600 White-Hat-Hackern aus mehr als 80 Ländern, genannt Synack Red Team (SRT), die im Crowdsourcing-Modell die Infrastrukturen der Synack-Kunden auf Herz und Nieren testen. So wird es möglich, dass an einem Penetration Test üblicherweise mehrere hochkarätige Spezialisten beteiligt sind – dies mit einem hohen Grad an Internationalität.

Das breit aufgestellte Know-how und die je nach Weltgegend unterschiedlichen Hacking-Methoden ergeben ein realistisches Gesamtbild über die tatsächliche Angreifbarkeit. Die Mitglieder des SRT werden selbstverständlich auf Fähigkeiten und Vertrauenswürdigkeit geprüft, bevor sie mit der Arbeit beginnen dürfen. Zusammen mit der innovativen Technologieplattform ergibt sich ein skalierbarer Penetration-Testing-Service, der das Beste aus künstlicher und menschlicher Intelligenz vereint.

SYNACK: DIE HIGHLIGHTS

- Intelligente Testplattform
- Kundenportal mit aktuellen Informationen
- Globales Netzwerk von mehr als 1600 White-Hat-Hackern
- **Discover:** Vulnerability Discovery über 14 Tage
- **SmartScan:** Vulnerability Assessment 24/7/365
- **Certify:** Penetration Testing über 14 Tage
- **Synack365:** Penetration Testing 24/7/365
- Unterstützt Compliance nach PCI, OWASP Top 10 und NIST 800-53

BOLL Europe GmbH,

Ringstraße 3, 89081 Ulm
Tel. +49 731 850 748 23
info@boll-europe.com
www.boll-europe.com

BILD: GANGISKHAN - STOCK.ADOBE.COM

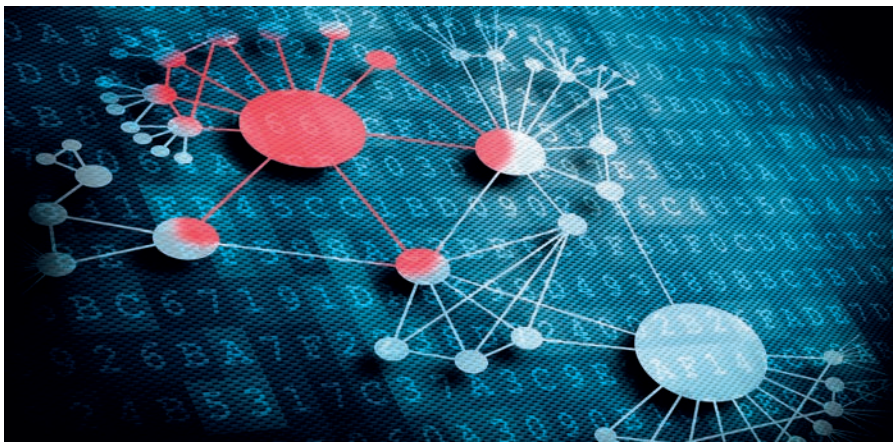
Cyberkriminalität: MSPs sind beliebtes Ziel

90 Prozent der Managed Service Provider (MSP) wurden in den vergangenen 18 Monaten Opfer einer Cyberattacke. Die Zahl der Angriffe hat sich fast verdoppelt; mit schwerwiegenden Auswirkungen.

Managed Service Provider (MSP) geraten immer häufiger ins Visier von Kriminellen. Die Attacken auf MSPs sind meist sehr zielgerichtet und technisch ausgefeilt. Es scheint, als hätten Service Provider in kriminellen Kreisen eine Art prominenten Stellenwert erlangt. Aufgrund der hohen Dichte an sensiblen Kundendaten kann man sie in Bezug auf das Schadenspotenzial durchaus mit kritischen Infrastrukturen vergleichen. Für Systemhäuser und andere Anbieter von MSP-Leistungen heißt das, dass sie sich auf immer mehr Infrastruktur-Attacken einrichten müssen.

Das bestätigen auch aktuelle Zahlen: Der diesjährige Report „State of the Market: The New Threat Landscape" von Coleman Parkes Research im Auftrag von N-able (ehemals Solarwinds MSP) zeigt auf, dass MSPs ihre Kunden als primäres Ziel für Cyberkriminelle rasant überholen. Demnach sind 90 Prozent der befragten MSPs in den vergangenen 18 Monaten Opfer von Cyberangriffen geworden. Ebenso viele verzeichneten eine steigende Anzahl von Angriffen, die sie pro Monat abwehren mussten. Im Durchschnitt ist die Zahl der abgewehrten Attacken von sechs auf elf gestiegen.

„MSPs haben während der Pandemie unermüdlich gearbeitet, um zu gewährleisten, dass ihre Unternehmenskunden auch unter den veränderten Bedingungen online und vernetzt bleiben können", betont Dave MacKinnon, Chief Security Officer bei N-able. „Aber genauso hart arbeiten die Cyberkriminellen daran, die Veränderungen für ihre Zwecke auszunutzen. Um ihre Kunden und sich selbst zu schützen, müssen MSPs erkennen, wie sich die Bedrohungslandschaft weiterentwickelt – nicht nur um die erforderlichen Maß-



Supply-Chain-Attacken auf Managed Service Provider haben eine verheerende Multiplikatorwirkung.

BILD: FOTOGESTOEBER - STOCK.ADOBE.COM

nahmen zu treffen, sondern auch um die enormen Chancen zu nutzen, die sich aus der verbesserten Security ergeben."

Die Auswirkungen von Cyberangriffen sind dabei weitreichend: Mehr als die Hälfte der befragten MSPs geben an, dass ein Cyberangriff zu finanziellen Verlusten (58%) und Geschäftsunterbrechungen (56%) geführt hat. Viele gaben zudem an, dass sie Geschäftseinbußen (46%), Auswirkungen auf ihren Ruf (45%) und sogar einen Vertrauensverlust bei ihren Kunden (28%) erfahren haben. Zwar sind die Budgets der MSPs immerhin um durchschnittlich 5 Prozent gestiegen, allerdings konzentrieren sich die Dienstleister bei der Investition der zusätzlichen Mittel auf Schlüsselbereiche wie Datenschutz, Cloud-Security und den Schutz der Infrastruktur.

Laut der Studie ist die Automatisierung von Schlüsselfunktionen entscheidend, um gegen Cyberkriminelle vorzugehen. Am häufigsten setzen MSPs automatisierte Backups ein, um das Geschäft ihrer Kunden zu schützen. Sie kommen bei 85 Prozent aller Befragten zum Einsatz. Doch nehmen nicht nur die Cyberangriffe auf Service Provider zu: 82 Prozent der Security-Dienstleister haben der Studie zufolge auch einen Anstieg der Angriffe auf ihre Kunden verzeichnet. Seit der Pandemie wurden durchschnittlich 14 Angriffe pro Monat verhindert, vor der Pandemie lag dieser Wert noch bei acht Angriffen pro Monat.

Kleine und mittlere Unternehmen (KMU) haben selbst den Ernst der Lage erkannt und müssen nicht erst durch den MSP von Sicherheitsinvestitionen überzeugt werden. So planen der Studie zufolge weltweit sieben von zehn eine Erhöhung ihres Sicherheitsbudgets. Der Anteil derer, die nicht aufstocken, behält größtenteils das bisherige Budget bei; nur 2 Prozent erwägen Kürzungen. Die Budget-Erweiterungen betragen im Durchschnitt sieben Prozent und sind somit erheblich. KMU möchten dabei ihre zusätzlichen Mittel vorrangig in Datensicherheit und Cloud-Sicherheit investieren.

Mehr zu Managed Security:
www.it-business.de/-a-1112180

Autor:
Sarah Böttcher

SUPPLY-CHAIN-ANGRIFFE HABEN ERST BEGONNEN

Supply-Chain-Attacken halten die ITK-Welt in Atem. Ein prominentes und aktuelles Beispiel ist die Log4j-Schwachstelle in den Apache Logging Services. Große Supply-Chain-Hacks mussten bereits Solarwinds und Kaseya verzeichnen. Angriffe auf Software-Lieferketten haben schwerwiegende und weitreichende Folgen. Da sie nicht auf ein einzelnes Unternehmen abzielen, lassen sie sich schwerer erkennen und verhindern. Cyberkriminelle attackieren hierbei nicht die IT-Umgebung eines Unternehmens, sondern sie schleusen Viren oder schadhaften Code über eine Lieferkette (Supply Chain) oder einen Anbieter in den Quellcode einer Anwendung ein. Software-Hersteller sind sich der Malware nicht bewusst. So sind auch deren Kunden ahnungslos und installieren, updaten oder nutzen die Drittanbieter-Software weiterhin. Die Malware erreicht so eine Vielzahl von Unternehmen. Supply-Chain-Angriffe können aber auch über Hardware in Form von physischen Geräten wie USB-Keylogger oder über die Firmware erfolgen.
Ist ein MSP von einer Supply-Chain-Attacke betroffen, entsteht eine verheerende Multiplikatorwirkung, durch den Cyberkriminelle auch sofort Zugriff auf die Daten der Endkunden erhalten. Deshalb sind gerade Managed Service Provider ein beliebtes und lukratives Ziel.

BILD: GORODENKOFF - STOCK.ADOBE.COM

OT-Security: Die Suche nach dem Königsweg

Der Schutz vor Cyberattacken auf KRITIS und Industrie muss intensiviert werden. Wie kann der ITK-Channel in der OT-Security Fuß fassen? So wie IT und OT konvergieren, müssen auch die Security-Lösungen zusammenfinden.

„Die Zeitenwende, die wir erleben, erfordert deutliche Investitionen in unsere Cyber- und Informationssicherheit. Das hat besondere Priorität für uns", sagte Bundesinnenministerin Nancy Faeser bei der Vorstellung des neuen „Digitalpolitischen Programms". Vertreter der Security-Branche, wie der Bundesverband IT-Sicherheit e.V. (Teletrust), sehen einen konkreten Handlungsbedarf gerade bei Kritischen Infrastrukturen und der Industrie. Cyberangriffe in der Ukraine haben gezeigt, dass kritische Infrastrukturen und industrielle Netzwerke zunehmend in den Fokus politisch motivierter Cyberattacken geraten, so Teletrust. Entsprechend fordert der Verband unter anderem die wirksame Absicherung der Industrieproduktion und digitaler Industrie-Netzwerke, einschließlich Logistik und Supply Chain, sowie eine Verbesserung des Qualifizierungsniveaus des Personals in Bezug auf IT-/OT-Sicherheit. Aufgaben und mögliche Projekte für Security-Hersteller und den Security-Channel gibt es damit genug, gerade auch im Bereich der Operational Technology (OT).

Der Bedarf an OT-Security steigt gegenwärtig besonders an. Doch ein Thema ist die Sicherheit im Umfeld von Industrie 4.0 schon seit langem. Die Hemmnisse für den Einsatz von Industrie-4.0-Anwendungen haben sich in den vergangenen Jahren praktisch nicht verändert, so eine Umfrage des Bitkom. Die größten Herausforderungen waren und sind fehlende finanzielle Mittel (77 %), Anforderungen an den Datenschutz (61 %) und an die IT-Sicherheit (57 %) sowie der Fachkräftemangel (55 %). Offensichtlich ist es nicht einfach, dem Bedarf an OT-Security gerecht zu werden.

Der entscheidende Schritt für Ramsey Hajj, Global Industrial IIoT/ICS Leader bei Deloitte, ist, dass nicht nur IT und OT technisch zusammenwachsen, sondern dass auch die Teams für IT-Sicherheit und OT-Sicherheit miteinander sprechen und arbeiten. „Zum Beispiel könnte eine Änderung in einem Herstellungsprozess eine Cyber-Schwachstelle öffnen, über die die IT-Leute Bescheid wissen und die sie beheben müssen, bevor der Prozess implementiert ist", begründet Hajj die notwendige Kooperation. Überträgt man diesen Gedanken auf die Anbieter und Dienstleister aus der IT-Sicherheit, sollten auch diese mit OT-Anbietern und -Dienstleistern kooperieren. Die Lösungen und Services benötigen entsprechende Schnittstellen und gemeinsame Management-

Cyberattacken zielen meist auf digitale Daten ab, auch und gerade bei Industrieunternehmen, so eine Umfrage des Digitalverbands Bitkom. Die Folge: Security für OT (Operational Technology) wird immer wichtiger.

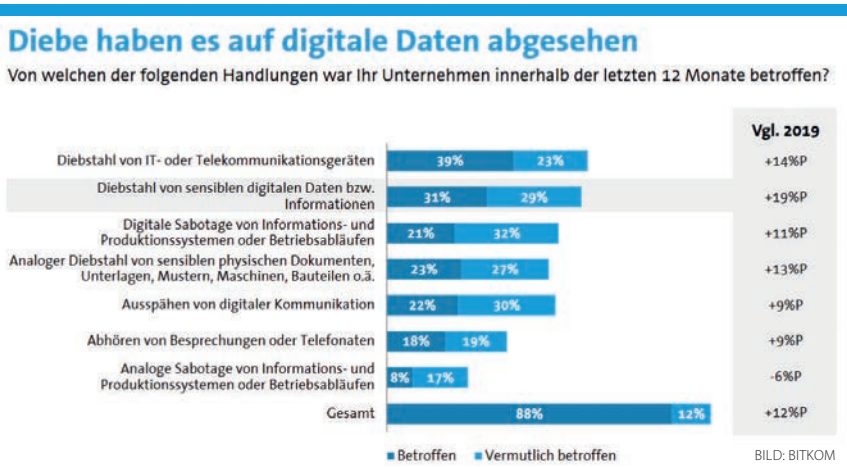


BILD: BITKOM

Tools und Dashboards. Solche spezialisierten Lösungen bieten zum Beispiel Tenable.ot, Forescout OT-Security, Claroty Platform, Darktrace Industrial Immune System und Nozomi Networks Guardian.

Partnerschaften von OT-Security-Anbietern mit Security-Dienstleistern, MSSPs und Distributoren sind keine Seltenheit mehr. „Cyberbedrohungen und gezielte Angriffe können schwerwiegende Auswirkungen auf kritische Infrastrukturen haben“, erläutert Denis Ferrand-Ajchenbaum, VP Global Vendor Alliances and Business Development, Exclusive Networks. „Der dynamische Vernetzungsprozess macht die Produktion flexibler und schneller. Dadurch entstehen neue Geschäftsmodelle, aber gleichzeitig auch neue Angriffspunkte für Cyberkriminelle“, weiß Dr.-Ing. Stefan Rummenhöller, Geschäftsführer des Wuppertaler IT-Sicherheitsspezialisten R-tec. „Wir sind bestrebt, unsere Cyberfähigkeiten weiterzuentwickeln und die Zusammenarbeit mit Technologiepartnern ist ein Schlüsselelement“, sagt Phil Jones, Head of Services bei Airbus CyberSecurity.

OT-Sicherheit ist ein weites Feld. Eine Priorisierung erscheint deshalb sinnvoll. Die Security-Experten von KPMG nennen drei Bereiche, die zuerst angegangen werden sollten: Endpunktschutz von OT-Ressourcen, Perimeter-Firewalls um OT-Assets herum und Netzwerksegmentierung, innerhalb von OT und zwischen OT/IT. Daneben sollten Unternehmen die Sichtbarkeit von OT-Netzwerken frühzeitig implementieren und eine Überwachung des OT-Netzwerks auf bekannte Bedrohungen oder verdächtiges Verhalten ermöglichen. Idealerweise sollten diese Technologien in das bestehende Überwachungs- und Reaktions-Framework integriert werden, also in ein bestehendes SOC (Security Operations Center) und Incident Response-Team, so KPMG.

Die Marktforscher von Gartner berichten, dass 38 Prozent der Industrieunternehmen die Ausgaben für OT-Sicherheit im Jahr 2021 um fünf bis 10 Prozent erhöhen wollten, weitere 8 Prozent um mehr als 10 Prozent. Laut Gartner reicht dies jedoch möglicherweise nicht aus, um der jahrelang zu geringen Investition in diesem Bereich entgegenzuwirken. Trotz der hohen Risiken im Operational-Technology-Bereich sind Projekte für OT-Security keine Selbstläufer. Neben der Suche nach geeigneten Partnern müssen auch die Kunden überzeugt werden.

Autor:
Oliver Schonscheck

NEUE CYBER-SECURITY-STRATEGIEN FÜR SMART MANUFACTURING

Das Beratungshaus Deloitte empfiehlt für die Verbindung von IT- und OT-Sicherheit:

- Schaffung eines Production Security Operations Center: Use Case Design auf Basis bestehender IT Standard Use Cases (z. B. BruteForce und DoS, Suspicious User Behavior, Inappropriate Credential Usage)
- Design eines Incident-Handling-Prozesses für die Zusammenarbeit zwischen IT und OT
- Neugestaltung der Sicherheitsorganisation, um OT-Security in die globale Struktur der Organisation zu integrieren.
- Security by Design sowie Risiko- und Schwachstellenanalyse für Smart Products
- Secure Life Cycle Development (SLCD) für Smart Products
- Schaffung eines Security Frameworks und eines erhöhten Datenschutz-Bewusstseins bei Mitarbeitern, Kunden und Anwendern

ISX2022

IT-Security Conference

» 22. JUNI HAMBURG
» 6. JULI GARCHING & DIGITAL

www.isxconference.de
JETZT ANMELDEN!

IT-SECURITY IN THE **NEW**

Unter diesem Motto erwarten Dich hochkarätige Speaker und brandaktuelle Themen, welche Dich und Dein Unternehmen im Kampf gegen Cyberangriffe voranbringen und Antworten bieten!

Prof. Dr. Peter Bräutigam Noerr

Prof. Dr. Marco Gercke
Cybercrime Research Institute

Stefan Strobel
cirosec

Florian Oelmaier
Corporate Trust

TRIFF DIESE KEYNOTE-SPEAKER IM JUNI & JULI

» HIER GEHT ES ZUR ANMELDUNG FÜR DEN 22. JUNI & 6. JULI

ISXQIV/22

IT-Security Virtual Conference

» 23.NOVEMBER VirtCon

www.isxconference.de

SAVE THE DATE!

CYBERCRIME WORLD

» **HIER GEHT ES ZUR VORANMELDUNG FÜR DEN 23. NOVEMBER**

Eine Veranstaltung der VOGEL IT AKADEMIE

BILD: ADAM121 - STOCK.ADOBE.COM

Mehr Homeoffice braucht mehr IT-Security

Die Corona-Pandemie hat den Weg für moderne Arbeitsmodelle geöffnet. Gleichzeitig verschärfen sich Cyberangriffe in Deutschland zunehmend. Gefährdet die Freiheit der Arbeitswelt nun die IT-Sicherheit der Unternehmen?

Kein Stau auf dem Arbeitsweg, eine Stunde länger Schlafen und mehr Ruhe bei der Arbeit. Das sind nur ein paar der Vorteile von Homeoffice. Und deutsche Arbeitnehmer wollen diese beibehalten. Während der vergangenen beiden Jahre war die Arbeit von Zuhause ein wichtiges Mittel, um die Ausbreitung des Coronavirus einzudämmen. Nun kehrt der Alltag schrittweise zurück. Doch das Homeoffice bleibt. In Sachen Sicherheit herrscht jedoch noch Nachholbedarf, denn die Umstellung auf Remote-Work und damit einhergehend die Einführung von Collaborations-Tools geschah bei vielen Unternehmen ad hoc. Die IT-Sicherheit ist oft nicht mit den schnellen Anpassungen und Umstrukturierungen mitgewachsen. Diese Versäumnisse müssen nun dringend aufgeholt werden.

Einfallstor für Hacker sind noch immer die Mitarbeiter, die nun vermehrt von überall aus arbeiten und sich über diverse Netzwerke mit unterschiedlichen Devices ins Firmen-Netz einwählen. Dieses Szenario stellt IT-Security-Verantwortliche vor diverse Herausforderungen, wie Calgar Colkusu, Commercial Security Sales Executive DACH Business Development bei Lenovo, erläutert: „Bei einer immer mobiler werdenden Belegschaft müssen IT-Abteilungen dennoch die Kontrolle behalten und gleichzeitig auf die Privatsphäre der Mitarbeiter achten sowie Datenschutzbestimmungen im Blick haben. Am Ende des Tages muss aber auch die Usability gegeben sein – Sicherheitskonzepte müssen idealerweise im Hintergrund funktionieren und einfach zu administrieren sein."

Und die Liste der zu beachtenden Punkt bei Remote Security ist lang, weiß Ben Kröger, Technische Leitung Cyber Security bei Axians IT-Security. Denn die Remote-Arbeit erweitert nicht nur die Bedrohungsoberfläche, sondern schafft auch völlig neue Angriffsflächen. So ist ein weiterer potenzieller Bereich etwa die Perimeter-Sicherheit, da Mitarbeiter von teils persönlichen, nicht vertrauenswürdigen Geräten über das heimische WLAN auf Collaboration-Tools und kritische Geschäftsanwendungen zugreifen. Dabei reichen bestehende Remote- und VPN-Lösungen für einen umfangreichen Schutz oft nicht mehr aus. Unternehmen müssen ihre Security-Strategie entsprechend anpassen und zu einer grenzübergreifenden Security-Architektur wechseln, um die Geschäftskontinuität weltweit zu ermöglichen.

BILD: AXINS

Ben Kröger, Technische Leitung Cyber Security, Axians IT Security

Die wichtigste Grundlage für Remote Security ist: Bei der hybriden Nutzung müssen zuerst alle technischen und vor allem organisatorischen Schutzmaßnahmen besonders strikt eingehalten werden.

BILD: INDEVIS

Wolfgang Kurz, Geschäftsführer und Founder, Indevis

Der Fachkräftemangel macht es gerade Mittelständlern schwer, Experten zu gewinnen, die sich fachgemäß um die Remote-Security kümmern.

BILD: INFOSYS

Vishal Salvi, Chief Information Security Officer & Head of Cyber Security Practice, Infosys

Für die IT-Sicherheit des modernen Arbeitsplatzes müssen sich Unternehmen mit SASE befassen, einem in der Cloud bereitgestellten Service, der Sicherheit am Rande des Netzwerks bietet.

Bei der Absicherung von Heimarbeitsplätzen gibt es zwei unterschiedliche Ansätze: Über ein Virtual Private Network (VPN) oder Zero Trust. „VPNs schaffen einen Schutzwall um das Netzwerk, der es authentifizierten Benutzern und Geräten ermöglicht, das Netzwerk zu durchqueren und problemlos auf Ressourcen zuzugreifen“, erklärt Vishal Salvi, CISO & Head of Cybersecurity Practice bei Infosys. Jedoch wird autorisierten Nutzern blind vertraut. Das kann zu einer Gefahr werden. Ein Zero-Trust-Ansatz, wie der Name schon andeutet, traut hingegen erst einmal niemanden. So wird bei Zero Trust zunächst jeder Benutzer und jedes Gerät einzeln überprüft, bevor der Zugriff auf eine bestimmte Anwendung gewährt wird. Des Weiteren wird entgegen zum VPN auch kein „vertrauenswürdiges“ Netzwerk erstellt. Auf was nun setzen?

„Beide Modelle haben Vor- und Nachteile“, sagt Kröger. Standard sei dem Technischen Leiter zufolge eine Lösung via Remote Access VPN für den Zugang zu Unternehmensressourcen und ein Zero-Trust-Ansatz für Cloud Services. Es sind jedoch weitere Varianten möglich, wie virtuelle Desktops, wenn Mitarbeiter beispielsweise ihre eigenen Geräte verwenden. Auch Kombinationen mit Remote Access VPNs via SSL zu virtuellen Desktops seien denkbar.

Für Wolfgang Kurz, Geschäftsführer bei Invedis führt hingegen an Zero Trust sowie dem Architektur-Konzept SASE (Secure Access Service Edge) langfristig kein Weg vorbei. „In verteilten Netzwerken ist es schlichtweg zu ineffizient, den gesamten Traffic über VPN zu routen. Klüger ist es, Security an den Endpoint oder in die Cloud zu verlagern, um sichere Direktverbindungen zwischen Anwendungen aufzubauen.“ Für ihn hat der klassische VPN Zugang ausgedient. „Künftig arbeiten User transparent in unterschiedlichsten Applikationen vollkommen unabhängig vom Zugangsweg“, prognostiziert der Geschäftsführer.

Mehr unter:
www.it-business.de/-a-1108119/
Autor:
Ann-Marie Struck

BILD: LENOVO

Caglar Colkusu, Commercial Security Sales Executive DACH Business Development, Lenovo

Security-Konzepte müssen ganzheitlich gedacht werden.

BILD: MEDROCKY - STOCK.ADOBE.COM

Mammutaufgabe Netzwerksicherheit

Das Netzwerk ist die grundlegende Struktur, die alle Systeme miteinander verbindet. Dementsprechend wichtig, aber auch aufwendig, ist die Absicherung der Infrastruktur.

Keinen Urlaub, keine Feiertage und keine Pausen gibt es für die IT-Sicherheit. Deshalb sind Unternehmen gut darin beraten, die eigene IT-Landschaft rund um die Uhr zu überwachen oder überwachen zu lassen. „Vor zehn Jahren war die Frage noch, ob man angegriffen wird, vor vier Jahren fragte man sich noch, wann man angegriffen wird, und heute geht es darum, welche Angriffe laufen gerade, welche Malware ist im Netz und welcher Schaden ist bereits entstanden", sagt Steffen Brieger, Director Vendor Management beim Distributor Nuvias.

Vor allem für Service Provider ist hier ein rentables Geschäftsfeld entstanden. Denn selten können Unternehmen genügend eigene Ressourcen aufbringen, um ein 24/7-Monitoring zu gewährleisten. „Security spielt im Netzwerk eine immense Rolle und ist fast Teil jeden Projektes", bestätigt Alexander Ernst, Director Network & Communication bei Cancom. Naheliegend ist es, beides enger miteinander zu verweben. Doch „Sicherheitslösungen werden leider immer noch oft getrennt vom Netzwerkaufbau gesehen", sagt Jörn Kraus, Manager Presales beim Distributor Westcon Deutschland. Eine Integration kann schnell zur Mammutaufgaben werden. Denn jede Komponente, die im Netzwerk enthalten ist, und jedes Gerät, das angebunden wird, muss geschützt werden: Daten, mobile Endgeräte, Server und Applikationen, Zweigstellen und Homeoffices, aber auch hybride, private, öffentliche Infrastrukturen sowie solche am Netzwerkrand.

Mit einem entsprechenden Zoo an Sicherheitslösungen für das Netzwerk kommen Neukunden zu Controlware, sagt Rolf Bachmann, Senior Business Development Manager bei dem IT-Dienstleister. „Jeder unserer Kunden hat schon vor der Zusammenarbeit mit uns etwas für seine Netzwerksicherheit getan. Die Herausforderung besteht darin, das ideale Sicherheitskonzept für jedes Unternehmen zu finden. Denn es gibt nicht die eine richtige Lösung, die für alle passt."

Wer allerdings keinen Kompromiss zwischen Netzwerkleistung und Sicherheit machen will und es möglichst kosten- und ressourcengünstig braucht, kann über SASE nachdenken: Secure Access Service Edge beschreibt keine konkrete Lösung, sondern ein Architekturmodell, bei dem Netzwerkfunktionen und Sicherheitsservices

BILD: PINKEYES-STOCK.ADOBE.COM - [M] CARIN BOEHM

Lait dem BSI wurden im vergangenen Jahr pro Tag 322.000 neue Varianten von Schadprogrammen bekannt. Die größte Angriffsfläche für Hacker sind allerdings Netzwerke und Infrastrukturen.

nicht mehr getrennt eingesetzt werden, sondern integriert sind. Gartner hat den Begriff erstmals 2019 definiert und empfiehlt, die Sicherheitsleistungen als Software as a Service aus der Cloud zu beziehen, was günstiger ist als Hardware anzuschaffen. Setzt man dann noch auf Managed Services, spart man auch an eigenem Personal. Auf der Netzwerkseite gehören zu dem Gartner-Konzept SD-WAN, WAN Optimization, QoS, Routing, SaaS Acceleration und Content Delivery/Caching. „Diese Möglichkeiten, ein Netzwerk zu designen, sind erst mal nicht neu", erklärt Bachmann. Auch die Security Services, mit denen Unternehmen das Netzwerk aufrüsten sollten, um eine SASE-Architektur zu erstellen, sind größtenteils nicht neu. Dazu gehören Secure Web Gateway, CASB, ZTNA/VPN, FWaaS, Remote Browser Isolation sowie Ver- und Entschlüsselung. Neu ist Bachmann zufolge, dass diese Services für ein SASE-Modell aus der Cloud bezogen werden.

Für die Dienstleister, die mit dem Kunden die Architektur entwickeln, geht es nun darum, den „Zoo an Sicherheitslösungen" und die Netzwerkfunktionen unter einen Hut zu bekommen und beides auf einer zentralen Plattform verwaltbar zu machen. In diesem Prozess kann es vorkommen, dass ein Hersteller ausgetauscht wird und eine neue Sicherheitslösung, die besser in das SASE-Konzept passt, muss an die Plattform angebunden werden. Dafür gibt es mehrere Möglichkeiten.

So ausgefeilt diese Prozesse auch sein mögen, sie haben einen Nachteil: Die Security-Leistungen werden im Nachgang implementiert. Dadurch können an den Schnittstellen Sicherheitslücken entstehen. Besser ist es für Unternehmen, unabhängig vom Netzwerkmodell, ein Konzept zu wählen, bei dem die Sicherheit nativ in die Netzwerklösungen eingebunden ist. Hierbei hat sich in Unternehmen die Entwicklungsmethode „DevSecOps" etabliert. Diese agile Arbeitsweise soll die Zusammenarbeit zwischen Entwicklern, dem operationalen IT-Team und dem Sicherheitsteam eines Unternehmens und somit die Lösung selbst verbessern. In der Praxis bedeutet das, dass sowohl die Betriebsabteilung wie auch die Security-Experten am Entwicklungsprozess einer Applikation beteiligt sind.

Die Idee entstand durch die mit der DSGVO im Mai 2018 einhergegangenen schärferen Datenschutzgesetze, bringt aber weitere Vorteile als „nur" die Sicherheit. Dynamische Entwicklungsansätze und eine DevOps-Kultur gehören heute zu den Faktoren für den Geschäftserfolg. Denn durch die Zusammenarbeit der Experten aus bisher separaten Abteilungen, können sie die Markteinführungszeit neuer Software verkürzen und so auf Veränderungen schneller reagieren. Nimmt man nun die IT-Sicherheit als grundlegenden Bestandteil mit in die Softwareentwicklung auf, sparen sich die Teams die rückwirkende Beseitigung von Schwachstellen und spätere Änderungsschleifen, da sie Sicherheitsscans nicht mehr nur punktuell, sondern zu verschiedenen Zeiten der Entwicklungsphase durchführen können.

Eine Methode, die der Sicherheit guttut, jedoch die Nachfrage nach Fachkräften und die Anforderungen an diese weiter in die Höhe treibt. Denn die Agilität soll die Effizienz erhöhen, was allerdings die Entwickler unter Zeitdruck setzt. Trotzdem werden Sicherheits- und Netzwerkteams künftig enger zusammenarbeiten müssen, um Netzwerke und Infrastrukturen noch besser abzusichern. Vielleicht kommt „DevNetSecOps" als nächster Entwicklungsschritt, bei dem DevSecOps-Team noch die Netzwerkexperten beitreten. Als notwendigster nächster Schritt steht jedoch die Automatisierung von Betriebsabläufen der Netzwerksicherheit an, um die Mitarbeiter zu entlasten. „Durch eine Kombination aus fortschrittlichen Technologien, mehr Rechenleistung, Künstlicher Intelligenz, Maschinellem Lernen und Prozess Automation entstehen ganz neue Potenziale, um Sicherheitsrisiken zu minimieren", ist sich Brieger sicher.

Mehr unter:
www.it-business.de/-a-1089280/

Autor:
Melanie Staudacher

Windows 11: Fensterputz für mehr Sicherheit

Windows 11 bekommt zusätzliche Security-Features. Sie erfordern aktuelle Hardware und auch die PC-Hersteller müssen mitziehen.

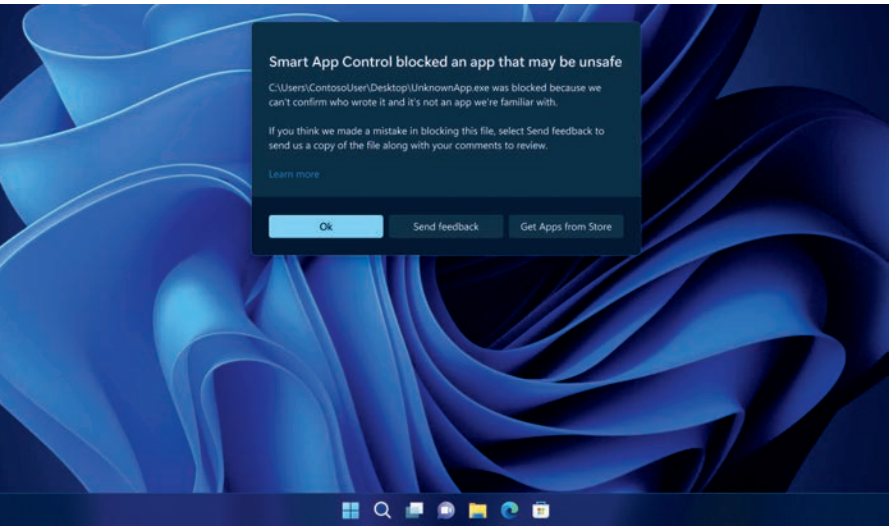


BILD: MICROSOFT

Eines der Ziele von Microsoft mit der Einführung von Windows 11 ist eine höhere Sicherheit, die gerade durch das immer weiter verbreitete hybride Arbeiten notwendig ist. Denn wenn Mitarbeiter nicht in der geschützten Unternehmensumgebung am Rechner sitzen, sondern im Homeoffice oder unterwegs sind, dann muss das Betriebssystem besser gegen digitale Angriffe jeder Art gewappnet sein. Eine Neuerung ist die Smart App Control. Sie soll laut Microsoft eine erhebliche Ausweitung des Sicherheitsmodells von Windows 11 bringen, das bisher vor der Ausführung unbekannter oder unsignierter Applikationen warnt. Die im Kern des Betriebssystems verankerte Funktion soll mit der Hilfe von Code Signing und Machine Learning in der Microsoft Cloud nur das Ausführen von Anwendungen zulassen, die als sicher eingestuft sind. Allerdings lässt sich Smart App Control nicht in einer bestehenden Windows-11-Installation nachrüsten, sondern erfordert eine Neuinstallation.

Im Defender SmartScreen wurde der Schutz vor Phishing-Angriffen mit dem letzten Windows-11-Update weiter verbessert und warnt nun auch vor der Eingabe von Passwörtern in möglicherweise schädlichen Applikationen. Mit Personal Data Encryption kommt ein besserer Schutz gespeicherter Daten durch die Authentifizierung des Nutzers mittels Windows Hello for Business zum Einsatz. Auf Secured-Core-PCs mit erweiterter Sicherheit durch Dynamic Root of Trust for Measurement (DRTM), einem aktivierten System Management Mode, Memory Access Protection und Hypervisor-Protected Code Integrity überwacht die Funktion Config Lock über MDM-Richtlinien die Integrität von Registrierungsschlüsseln. Allerdings sind diese Technologien nur auf einer Reihe relativ neuer Business-Notebook zu finden.

Als Ablösung für den TPM 2.0 hat Microsoft einen eigenen Security-Prozessor entwickelt, der bereits in der aktuellen Xbox and in den Azure-Sphere-IoT-Chips zum Einsatz kommt. Im Gegensatz zum TPM 2.0 soll er direkt in Prozessoren integriert werden und damit einen Schutz gegen Manipulationen bieten. Pluton ist so sicher gegen ein direktes Abgreifen der Kommunikation wie bei über SPI angebundenen TPMs oder gegen das Ausnutzen von Software-Bugs bei Firmware-TPMs (fTPM). Auch Firmware-Updates für Pluton kommen direkt von Microsoft und sollen so schnell und sicher geliefert werden. Bei den neuen AMD-Ryzen-6000-CPUs ist der Chip schon an Bord, bei Intels Alder Lake und Qualcomms Snapdragon-SoCs für Notebooks noch nicht. Daher zeigen Hersteller wie Dell und Lenovo derzeit leider noch keine Bereitschaft, ihn auch zu nutzen. Acer hat dagegen angekündigt, die nächste Generation des Business-Notebooks Travelmate P4 and des Convertibles Travelmate Spin P4 mit aktiviertem Pluton-Chip in den dort verwendeten AMD-Ryzen-6000-Pro-CPUs auszuliefern.

Mehr unter:
https://www.it-business.de/acer-notebook/
Autor:
Klaus Länger

Nachhaltig und sicher in die Zukunft

Mit **Microsoft Windows 11 Pro** auf **Premium. Renewed. Hardware.**

Fujitsu Lifebook U758 Touch

Premium. Renewed. Hardware.

Intel Core i5 8250U bis 3.40, 16GB RAM, 256GB M.2 SSD, 39,6cm (15.6“) **Full HD Touchdisplay** mit Webcam, WLAN, **4G LTE** & Bluetooth

Windows 10 Pro 64Bit oder Windows 11 Pro 64Bit, G DATA Internet Security Multi-Device mit 1 Jahr Premium Support & Updates, Acronis True Image RETEQ Edition

100+ verfügbar

~~499,00 €~~

je **398,40 €**

Bestellungen **vertrieb@gsd.eu** oder **+49 89 800 695 -195**

Unsere Partner:

Microsoft AUTHORIZED Refurbisher

Microsoft Partner Gold OEM Silver OEM

Windows

G DATA TRUST IN GERMAN SICHERHEIT

Acronis

GSD® THE EXPERT IN IT-REMARKETING

Gesetz zur Software-Updatepflicht

Die neuen Regeln zur Software-Updatepflicht von digitalen Produkten kommen Verbrauchern zugute. Es bleibt aber vor allem abzuwarten, für welchen Zeitraum Updates eingefordert werden können.

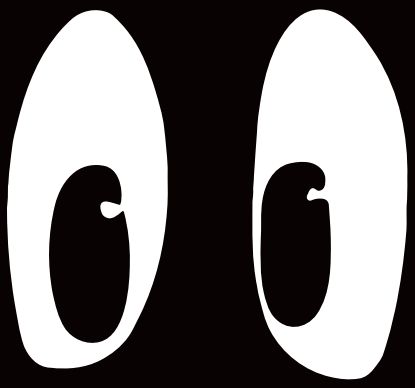
BILD: EVERYTHINGPOSSIBLE - STOCK.ADOBE.COM

Als sich Polit-Deutschland im Sommer 2021 schon im Wahlkampffieber befand, hat die Große Koalition als eine ihrer letzten Amtshandlungen eine wichtige EU-Richtlinie in nationales Recht überführt: Das Gesetz zur Regelung des Verkaufs von Sachen mit digitalen Elementen und anderer Aspekte des Kaufvertrages, verpflichtet Unternehmen, die Produkte mit Software verkaufen, dafür Updates anzubieten, solange „der Verbraucher Aktualisierungen aufgrund der Art und des Zwecks der Sache erwarten könne". Zu diesen Produkten zählen also Smartphones und andere Handys, aber auch Smartwatches, Fitnesstracker, Kühlschränke mit Bildschirmen und Bluetooth sowie persönliche, digitale Assistenten wie Google Home, der Apple HomePod oder Amazons Echo.

Bislang war die Rechtsprechung restriktiv: Selbst gegen den Verkauf eines Smartphones eines chinesischen Herstellers, welches noch nie ein Sicherheitsupdate erhalten hatte und zum Zeitpunkt des Verkaufs etliche ernste Sicherheitslücken aufwies, konnte vor der Rechtsänderung vor Gericht nichts unternommen werden. Dies ändert sich jetzt grundlegend. Verbraucher haben nun Gewährleistungsrechte, die deutlich umfassender sind als zuvor. Konkret können sie durch die neuen Regeln Schadensersatzansprüche geltend machen, ihren Vertrag vorzeitig beenden oder einen Preisnachlass erzielen, wenn der Verkäufer die Regeln nicht erfüllt: Sie müssen stets dafür sorgen, dass ihre Produkte dank der Updates nach Vertragsvereinbarung nutzbar bleiben – dazu zählen auch Updates, die die Sicherheit des jeweiligen Produkts betreffen.

Die Dauer der Updatepflicht hängt von der Art des Produkts und der Art des Vertrages ab: Wird zum Beispiel für die Nutzung einer App eine regelmäßige Vergütung verlangt, besteht die Updatepflicht für die volle Laufzeit des Vertrages. Beim Kauf eines smarten Devices kommt es mutmaßlich auf den zu erwartenden Lebenszyklus des Produktes an. Bei einem günstigen Gerät mit einem geringen Risikopotenzial (etwa einem Fitnessarmband) kann man gut argumentieren, dass die Updatepflicht die Gewährleistungszeit nicht übersteigt. Bei einem teureren Gerät, welches man sich für eine längere Zeit anschafft, kann man besser für eine längere Updatepflicht argumentieren. Teilweise wird vertreten, dass das Konzept der „Abschreibung" herangezogen werden kann: Demnach muss eine Updatepflicht gelten, bis der Wert einer Sache buchhalterisch abgeschrieben ist. Ob dieses für Unternehmen erdachte Konzept, auf Verbraucherverträge angewendet werden kann, bleibt fraglich. Klar ist: Bei teuren Hochrisikogeräten, wie etwa einem Herzschrittmacher, dürfte eine lange Updatedauer anzunehmen sein, die deutlich über die übliche Gewährleistungsfrist hinausgeht.

Autor:
Dr. Lutz Keppeler ist Anwalt und Salaried Partner bei der Anwaltssozietät Heuking Kühn Lüer Wojteke



STROM WEG –
DATEN WEG?

KLIMANEUTRAL
CO_2
CLIMATE NEUTRAL

Der USV-Hersteller mit 36 Monaten Garantie

Telefon: 089-242 39 90-10
info@online-usv.de • www.online-usv.de

ONLINE™
USV · SYSTEME AG
Luise-Ullrich-Straße 8 • 82031 Grünwald

BILD: JENNY STURM - STOCK.ADOBE.COM

Der Notruf der Krankenhäuser

Die Pandemie hat zu großen Veränderungen im Gesundheitswesen geführt: Neue digitale Arbeitspraktiken sind in die Krankenhäuser eingezogen. Damit gestiegen ist die Gefahr von Datendiebstahl, Erpressung durch Ransomware und im schlimmsten Fall lebensgefährlichen Eingriffen in die Medizintechnik.

Das Herz moderner Krankenhäuser und Uni-Kliniken, und damit ein hochkritischer Bereich, ist die OT/IT-Konnektivität, also die Koppelung von medizinischen Geräten mit IT-Infrastrukturen. Ein Beispiel zur Verdeutlichung: Das Bild eines MRT-Scanners wird über einen Bildschirm gesichtet und per Mail an einen externen Facharzt zur weiteren Begutachtung versandt – und in Zukunft vielleicht sogar live gestreamt an eine Medizinkoriphäe in der Ferne, die bei einer OP am Herzen assistiert. Klassische OT-Geräte verlassen ihre Sicherheitszone in dem Moment, wo Daten für klassische IT-Anwendungen zur Verfügung gestellt werden. „Hier ist auch das Tor für Angreifer, die sich damit Zugriff auf Geräte verschaffen können. Man möchte sich gar nicht vorstellen, welch gravierende Auswirkungen es hat, wenn beispielsweise die Dosis der radioaktiven Substanz bei den Szintigraphien oder Chemotherapie-Dosen per Angriff erhöht werden. Daher ist es essentiell, die Sicherheit von OT und IT-Schnittstellen abzusichern“, erklärt Santosh Wadwa, Head of Product Channel Sales, Central Europe bei Fujitsu.

„Egal ob Infusionspumpen oder Röntgengeräte: Sicherheit nur zum Zeitpunkt des Verkaufs zu gewährleisten, reicht nicht aus, denn die Geräte befinden sich viele Jahre im Einsatz und brauchen daher auch regelmäßig ein Sicherheitsupdate. Das ist die große Aufgabe für Hersteller“, erklärt Eckhart Traber von Lancom Systems, einem Anbieter für sichere Netzwerklösungen. Der Knackpunkt sind geradezu urzeitliche Standards, mit denen Röntgengeräte und Co. heute noch arbeiten. Digital Imaging and Communications in Medicine (DICOM) beispielsweise ist ein Standard aus den 1980er-Jahren, sowohl für die Speicherung als auch für die Übertragung medizinischer Bilddaten. Internisten benutzen den Standard beim Ultraschall, in der Kardiologie werden Aufnahmen der Koronarangiographien im DICOM-Standard gespeichert. Health Level 7 (HL7) ist neben DICOM ein weiterer internationaler Standard aus dem letzten Jahrhundert, um den Austausch klinischer und administrativer Daten zwischen medizinischen Anwendungen zu regeln. Um 2010 wurde HL7 durch Fast Healthcare Interoperability Resources (FHIR) ergänzt. FHIR öffnet die Tür zu mobilen Geräten, Apps und Wearables. In der Praxis scheitert die Implementierung von Sicherheitsmechanismen zum einen daran, dass die Produkte keine oder veraltete Standards nutzen. Zum anderen fehlt es an Zertifizierungen, um Medizingeräte sicherheitstechnisch up to date zu halten. Zudem werden weder Transport-Layer-Security (TLS) noch digitale Signaturen eingesetzt. Klini-

ken verwalten also historisch gewachsene Technikstrukturen, die mit der zunehmenden digitalen Vernetzung der Kliniken und Praxen kaum Schritt halten.

Um Krankenhäuser besser vor diesen Cyberangriffen zu schützen, wurde das Verbundprojekt „MITSicherheit.NRW" der FH Münster, der Ruhr-Universität Bochum und Medizintechnikunternehmen ins Leben gerufen, mit dem Ziel, Penetrations-Tests zur Identifizierung von Sicherheitslücken in Krankenhäusern zu entwickeln. Für medizinische Geräte gab es bislang nämlich noch keine zuverlässigen Scanner. Das Ergebnis waren der Scanner „MedVAS", der einen Verwundbarkeitsscan der IT-Infrastruktur in Krankenhäusern bei laufendem Betrieb ermöglicht, sowie die Testumgebung „MedFUZZ" für die medizinischen Standardprotokolle DICOM und HL7, mit der Medizintechnikunternehmen Sicherheitslücken oder Instabilitäten der eigenen Software testen können. Die Falle für Penetrations-Tests in Kliniken besteht darin, dass die Scans nicht komplett vollautomatisch funktionieren. In der Praxis bedeutet das, dass die jeweilige IT-Abteilung eine gut gepflegte Dokumentation der genutzten IP-Adressen und Ports benötigt. Gerade bei Protokollen, die in der Praxis keine standardisierten TCP-Ports verwenden wie beispielsweise HL7, ist die Konfiguration der zu scannenden Ports essenziell für einen aussagekräftigen Sicherheitsbericht. Auch DICOM-Server sind schwer zu identifizieren, wenn sie nur mit fest konfigurierten IP-Adressen kommunizieren.

Nicht leichter wird es für die IT-Sicherheit aufgrund der verschiedensten Datenquellen – angefangen bei Bestellformularen über Röntgenbilder bis hin zur Kardiografie. Es ist für IT-Verantwortliche daher wichtig, einen genauen Überblick zu behalten, wo welche Daten abgelegt und gespeichert sind. Oft fehlt dieser, weil Daten auf verschiedenste Infrastrukturen und Datensilos verstreut und in eigenen Datenstrukturen abgelegt sind. Diese werden wiederum ihrerseits mit eigenen isolierten Programmen gesichert, weiß man bei Veritas Technologies, einem globalen Anbieter für Datensicherung. Die Punktlösungen überlappen sich teilweise oder lassen Lücken in der Abdeckung, die man erst dann entdeckt, wenn Daten korrumpiert wurden oder verloren gehen.

Bei Cortex Xpanse, einer globalen Plattform zur Verwaltung von Angriffen, beispielsweise stellt man in der Regel fest, dass Kunden über mindestens 30 Prozent mehr Assets verfügen, als ihnen bewusst ist. Mit zunehmender Komplexität steigt natürlich auch die Angriffsfläche. Da das Gesundheitswesen ein begehrtes Ziel ist, werden diese Gelegenheiten wahrscheinlich entdeckt und ausgenutzt, wenn sie nicht erkannt und abgesichert werden.

Absicherung allein reicht aber nicht. Ergänzend zu den IT-Sicherheitslösungen braucht jedes Krankenhaus und jede Uni-Klinik eine Notfallplanung – eine große Herausforderung für viele Häuser. „Trotz aller technischen Möglichkeiten ist es immer noch das bekannte Katze-Maus-Spiel in der IT-Security. Jedes Unternehmen sollte den Ernstfall durchspielen - eine Notfallplanung mithilfe eines Notfallhandbuchs ist daher unabdingbar" weiß Oliver Lorenz, Geschäftsführer und zertifizierter Datenschutzbeauftragter (DEKRA) bei Kelobit IT Experts. Systemhäuser können bei der IT-Dokumentation mit angeschlossenem Notfallhandbuch gute Hilfestellung geben. Doch Sicherheit kostet nicht nur Geld, sondern braucht auch Personal. Schwachstellen- und Patchmanagement sowie eine grundsätzliche Aktualisierung oder Modernisierung der Krankenhaus-IT ist keine kleine Aufgabe. Krankenhäuser haben also viele Baustellen. Die IDC Health Insights European Survey vom Februar 2022 zeigt, dass die Sicherheit der Patientenversorgung und die Qualitätssicherung, die Ermöglichung integrierter Pflegemodelle und die operative Effizienz, die wichtigsten Geschäftsbereiche für europäische Gesundheitsorganisationen im Jahr 2022 sind. Für Systemhäuser bieten sich daher viele Chancen.

Alles rund ums Thema Healthcare dann in unserem Sonderheft, das der Ausgabe 12 beiliegt.

Autor:
Sophia Kessler

BILD: FUJITSU

Santosh Wadwa, Head of CCD & Channel Sales Central Europe bei Fujitsu

„Es ist essentiell, die Sicherheit von OT- und IT-Schnittstellen abzusichern."

BILD: STANISLAW PANOW

Stanislaw Panow, geschäftsführender Gesellschafter bei Netcos

„Es fehlen Personal und Prozesse, um die Systeme aktuell zu halten. Gleichzeitig wird in weitere, neue Systeme investiert, die mit neuen Schnittstellen und neuen Schwachstellen den Risikofootprint vergrößern. Hier fehlt es grundsätzlich an Übersicht und IT-Governance. Mit KnowHow und Ressourcen können Systemhäuser dazu beitragen, diese Gaps zu schließen und Risiken zu minimieren."

IT-BUSINESS

Vogel IT-Medien GmbH
Max-Josef-Metzger-Straße 21, 86157 Augsburg
Tel. 0821/2177-0, Fax 0821/2177-150
eMail: it-business@vogel.de
www.it-business.de

Geschäftsführer:
Werner Nieberle, Günter Schürger

Co-Publisher: Lilli Kos (-300)
(verantwortlich für den Anzeigenteil)

Chefredaktion: Sylvia Lösel (sl)

Chef vom Dienst: Heidi Schuster (hs)

Chefreporter: Michael Hase (mh)

Leitender Redakteur: Dr. Stefan Riedl (sr)

Redaktion: Sarah Böttcher (sb), Klaus Länger (kl), Melanie Staudacher (ms), Ann-Marie Struck (amy),

Weitere Mitarbeiter dieser Ausgabe:
Sophia Kessler (sk)

Dr. Lutz Keppeler

Oliver Schonschek (os)

Account Management:
Besa Agaj, Hannah Lamotte, Stephanie Steen
eMail: media@vogel.de

Anzeigendisposition:
Alexandra Breuer, Denise Falloni (-202)

Grafik & Layout: Carin Boehm, Udo Scherlin, Johannes Rath

Titelbild: Daniel Berkmann / Skellen / Alex - stock.adobe.com / [M] Udo Scherlin

EBV: Carin Boehm

Anzeigen-Layout:
Carin Boehm, Udo Scherlin, Johannes Rath

Leserservice / Mitgliederbetreuung:
Sabine Assum (-194), Fax (-228)
eMail: vertrieb@vogel.de

Fragen zur Abonnement-Rechnung:
DataM-Services GmbH
97103 Würzburg
Tel.: 0931/4170-462 (Fax -494)
eMail: vogel-it@datam-services.de

Druck:
Vogel Druck- und Medienservice GmbH
Leibnizstr. 5
97204 Höchberg

Vogel IT-Medien, Augsburg, ist eine 100prozentige Tochtergesellschaft der **Vogel Communications Group**, Würzburg, einem der führenden deutschen Fachinformationsanbieter mit 100+ Fachzeitschriften, 100+ Webportalen, 100+ Business-Events sowie zahlreichen mobilen Angeboten und internationalen Aktivitäten. Seit 1991 gibt Vogel IT-Medien Fachmedien für Entscheider heraus, die mit der Produktion, der Beschaffung oder dem Einsatz von Informationstechnologie beruflich befasst sind. Dabei bietet er neben Print- und Online-Medien auch ein breites Veranstaltungsportfolio an.

Die wichtigsten Angebote des Verlages sind **IT-BUSINESS, eGovernment Computing, Healthcare Computing, BigData-Insider, Blockchain-Insider, CloudComputing-Insider, DataCenter-Insider, Dev-Insider, IP-Insider, Security-Insider** und **Storage-Insider.**

Der nächste Channel Guide „Cloud & Virtualisierung“ erscheint am 26. September 2022.

BILD: © DANIEL BERKMANN / SKELLEN / NATALYA YUDINA - STOCK.ADOBE.COM / [M] UDO SCHERLIN

Cloud Computing und Virtualisierung gehen Hand in Hand im As-a-Service-Zeitalter. IT-Dienstleister, Managed Service Provider und Cloud Consultants sind die Protagonisten der neuen Computing-Ära. Welche Möglichkeiten es gibt, in diesem Umfeld IT-Knowhow in bare Münze zu verwandeln, erfahren Sie im Channel Guide „Cloud & Virtualisierung“.

Redaktionell erwähnte Unternehmen

Firma	Seite
8Soft	14
Acer	28
Acronis	6
ADN	6
Airbus CyberSecurity	20
Amazon	30
AMD	28
Apple	30
Appriver	14
Arrow	14
Artic Wolf	12
AWS	16
Axians IT-Security	24
BeyondTrust	6
Bitdefender	14
Bitkom	12, 14, 20
Boll	14
Brainworks	14
Cancom	26
Claroty	20
CMS	14
Coleman Parkes Research	18
Computerlinks	14
Controlware	26
Crowdstrike	6
Cyber Monks	14
Cyberdefense	12
Cybereason	6
CyberRes	14
Cyfirma	14
Darktrace	20
DEKRA	32
Dell	28
Deloitte	20
Ebertlang	14
Eco – Verband der Internetwirtschaft	12
Entrada	14
Eset	14
Exclusive Networks	14, 20
ExtraHop	6
Flexera	14
Forescout	20
Fujitsu	32
Gartner	12, 20, 26
Google	30
Greenbone	14
Hornetsecurity	6
Icos	14
IDC	6, 32
Infinigate	6, 14
Infosys	24
Intel	28
Invedis	24
ISC	6
Kaseya	18
Kaspersky	14
Kelobit IT Experts	32
KPMG	20
Lancom Systems	32
Lenovo	24, 28
Logpoint	14
Mailstore	14
Materna	6
Mateso	14
Microsoft	16, 28
N-able	18
Netcos	32
No Spam Proxy	6
Nozomi Networks	20
Nuvias	6, 14, 26
Palo Alto Networks	16
Prianto	14
Proofpoint	6
Provectus Technologies	12
Qbik	14
R-tec	20
Sailpoint	14
SentinelOne	6
Solarwinds	18
Sonicwall	6
Spectrami	14
Splendid Research	12
Sysob	14
Tanium	14
Teletrust	20
Tenable	20
TLK	14
Trellix	6
Veritas Technologies	32
Watchguard	6
Westcon	14, 26
Wick Hill	14
Zycko	14

Inserenten

Firma	Seite
BOLL Engineering AG	17
Fujitsu Technology Solutions GmbH	2
GSD Remarketing GmbH & Co. KG	29
Kaspersky Labs GmbH	5
MR Datentechnik Vertriebs und Service GmbH	35
ONLINE USV-Systeme AG	31
Tech Data GmbH & Co. OHG	9
Vogel IT-Akademie	22, 23
WORTMANN AG	11
Zyxel Networks A/S	36

<online qualifiers>
06. Juli - 17. August

JETZT ANMELDEN

<finale challenge>
09. - 11. September

Join the community on discord

2022

DEUTSCHLANDS
BESTER HACKER
DEINE HACKING CHALLENGE

<hast du das zeug zu>

deutschlands bestem hacker? »

Bereits 2020 starteten die Veranstalter mit der Suche nach „Frankens Bester Hacker“ und erweiterten die Ausschreibung 2021 auf „Bayerns Bester Hacker“. Die Teilnehmerzahlen übertrafen alle Erwartungen und das Feedback zum Event war gigantisch. Daher wird die Challenge 2022 nun auf ganz Deutschland ausgedehnt! Die Schirmherrschaft übernimmt in diesem Jahr Judith Gerlach, Bayerische Staatsministerin für Digitales.

DeutschlandsBesterHacker

Infos & Anmeldung unter deutschlands-bester-hacker.de

<supporter>

IT-BUSINESS · INFINIGATE Adding Value to Distribution · FUJITSU · SOPHOS · THALES Building a future we can all trust · whitelisthackers · RAZER · AeroCool · veeam · NZXT · Sharkoon · CSF Cyber Security Fairevent · BUNDESVERBAND DIGITALE SICHERHEIT · IHK für Oberfranken Bayreuth · HACKER SCHOOL · MR Datentechnik

ZYXEL
NETWORKS

Höhere Erkennungsrate von Bedrohungen.

Effizientes Netzwerk-management

Durch die Integration der USG FLEX-Serie in die Nebula-Cloud-Networking-Lösung, verfügen Administratoren nun über ein zentrales, standort-unabhängiges Tool.

Multilayer-Schutz mit hoher Zuverlässigkeit

Die USG FLEX-Serie ist mit Multilayer-Schutz gegen zahlreiche Bedrohungsarten konzipiert. Zu den internen Schutzfunktionen gehören Application Intelligence und Web Filtering.

Leistungs-zuwachs bis zu 500%

Die neu konzipierte Plattform kann eine Verbesserung der Firewall-Leistung bis zu 125 % erreichen. Zusätzliche UTM-Leistung konnte bis zu 500% gesteigert werden.

Einfaches Lizenzierungs-modell

Basic, Plus und Pro-Lizenzen. Einfach und verständlich. Durch die zusätzlichen Plus-Lizenzen passt sich der Schutz an Unternehmen, verschiedenster Größe an.

JUST PROTECT

Durch die Management-Funktionen von Nebula mit ganzheitlichem Sicherheitskonzept und umfassendem Schutz für Unternehmensnetzwerke können unsere Kunden ihre Zusammenarbeit optimieren.

Erfahren Sie hier mehr über **Nebula Together**

www.zyxel.de | Tel.: +49 (0)2405-690968 | E-Mail: sales@zyxel.de | Zyxel Networks A/S | Adenauer Straße 20/B2, 52146 Würselen