

Hybrid/Multi-Cloud-Vernetzung

Secure Access Service Edge

**Out-of-Band-Verwaltung
für das SD-WAN**

**Cloud-basiertes
Netzwerk-Management**

**Mit Marktübersicht
SD-WAN-Lösungen**



**Cisco Meraki
Go Set im Test**
Wireless-Lösung
für das KMU

**Sicherheit beim
Edge Computing**
Größerer Blickwinkel
gegen diffuse Sicht

**Backup und
Archivierung**
Mit Marktübersicht
Backup-Lösungen

KOSTENFREIE
TEILNAHME



Datacenter
Symposium

23. SEPTEMBER 2021

H4 HOTEL MÜNCHEN
MESSE

Das Datacenter Symposium findet am 23. September 2021 wieder als Präsenz-event in München statt. Die Themen sind hochaktuell, denn besonders in der derzeitigen Situation haben sich **Datacenter** nicht nur als **Herz der Unternehmensprozesse**, sondern auch als unverzichtbare **Basis der Digitalisierung** beweisen müssen. Zum Beispiel mit der Verlagerung von Office-Arbeitsplätzen aus der Firma heraus kommen viele neue Herausforderungen hinzu. Mehr denn je sind zum Beispiel **Agilität** und **Flexibilität** gefragt, vielfach im Zusammenspiel mit Cloud-Lösungen. Die Standardfragen nach einem effizienten Einsatz von Kühlung/Klimatisierung und Strom haben dabei allerdings nichts von ihrem Stellenwert eingebüßt, legen vielmehr im Zeichen der Dekarbonisierung der Energieversorgung in ihrer Bedeutung noch einmal zu.

Zu den Highlights des DCS in München zählen unter anderem:

- Eine Keynote zur „Optimierung des Energieaufwandes im RZ durch intelligente IT-Infrastrukturen“,
- mehrere Vorträge zur Technikentwicklungen bei der RZ-Kühlung und Stromversorgung,
- die Diskussion des „Low Carbon“-Rechenzentrums“
- ein „Praxis-Ratgeber für Infrastruktur-Beschaffung und RZ-Betrieb“

Eine Veranstaltung von:

LANline
IT ■ Network ■ Datacenter



Weitere Infos, Agenda und Anmeldung finden Sie unter
www.datacenter-symposium.de

Sponsoren der LANline Datacenter Symposium München

Stand: 26.07.2021

AIRSYS

**BACH
MANN**
Wir power your life

BENDER
The Power in Electrical Safety

DC INTELLIGENCE
www.dc-intelligence.com



HUAWEI

RITTAL

sachsenkabel

Starline
A brand of legrand

STULZ
CLIMATE CONTROLS

tde
trans data elektronik GmbH

VERTIV

Wolkenbildung



Dr. Wilhelm Greiner,
Freier Mitarbeiter der
LANline

Bei dem Wort „Wolke“ bekommt der Mensch Assoziationen: Manche denken an Schäfchenwolken, manche an Dampfwolken und manche an die Cloud. Vielen kommen neuerdings vor allem die Regenwolken in den Sinn, die in Deutschland – wie auch in China oder Nordkorea – ganze Landstriche unter Wasser gesetzt haben, oder die Rauchwolken an der US-Westküste, die selbst im 4.000 Kilometer entfernten New York die Sonne verschleiern.

Und die Rauchmelder schrillen weiter: Während ich dieses Editorial schreibe (am 8. August) sind die Nachrichten voller dramatischer Szenen aus Griechenland, Italien und der Türkei, wo Waldbrände toben. Was angesichts der Horrorbilder aus beliebten Urlaubsregionen der Deutschen praktisch untergeht: Zugleich lodern 250 Waldbrände in Russland, unzählige mehr in Brasilien und im südlichen Afrika. Der Golfstrom fließt so langsam wie seit 1.600 Jahren nicht mehr, einer der gefürchteten Klima-Kipppunkte droht. Die Gletscher in den Anden schmelzen drastisch ab, Grönlands Gletscher sogar doppelt so stark wie früher ... Die Liste will kein Ende nehmen: Vieles, wovon die Klimaforschung seit Jahrzehnten warnt, tritt nun fast zeitgleich ein.

So wenig überraschend diese Entwicklungen eigentlich sein dürften, so sehr überrascht die träge Reaktion. Klimaforschende wie Stefan Rahmstorf fordern, die Politik müsse den Klimawandel endlich als Krise ernst nehmen. Passt aber gerade schlecht, es ist Wahlkampf, wer wird da schon ein ständig heißer werdendes Eisen anpacken? Die globale Klimakrise gerät so zum Provinzpolitikum.

Ohne politische Rahmensetzung sind die Pariser Klimaziele nicht zu schaffen, aber auch die Wirtschaft ist gefragt, nicht zuletzt die IT-Branche. Das energieeffiziente RZ zum Beispiel ist ein LANline-Dauerthema, doch es ist nur ein Aspekt von vielen: Wie kann man RZs klimagerechter bauen, obwohl es keinen „grünen Beton“ gibt? Wie können Unternehmen bei der Digitalisierung Ökonomie und Ökologie vereinen? Wie klimafreundlich sind Cloud-Services wirklich, und wie können Anwenderunternehmen das überprüfen? Wie kann umweltfreundliches digitales Arbeiten in Zukunft aussehen? Hier stehen uns spannende Diskussionen bevor – hoffentlich mit dem Effekt der Fort- und nicht der Lagerbildung.

Viel Neugier wünscht

All-in-One-System



DATACENTER INTELLIGENT ABSICHERN

Das All-In-One-System aus Monitoring, Access und PDU – bei dem alles zusammen passt



Schwerpunkt

Hybrid- und Multi-Cloud-Vernetzung

Stellt euch vor, es ist Cloud, und keiner geht hin. Noch vor zehn Jahren hätte dieser Satz bei manchem wohlwollendes Nicken oder verschmitztes Lächeln hervorgerufen. Heute hingegen wäre ein Leben ohne die Cloud schwer vorstellbar. Die sichere Anbindung an das Unternehmensnetz wie auch an die Cloud ist somit wichtiger als je zuvor.

Seite 34

Schwerpunkt

Backup und Archivierung

Mit der steigenden Relevanz von Daten sollte auch die Frage ihrer Sicherung stärker in den Vordergrund rücken. So unaufhaltsam sich die IT-Umgebung von Unternehmen verändert, so verändern sich auch die Anforderungen an die unternehmenseigene Backup- und Recovery-Strategie.

Seite 18

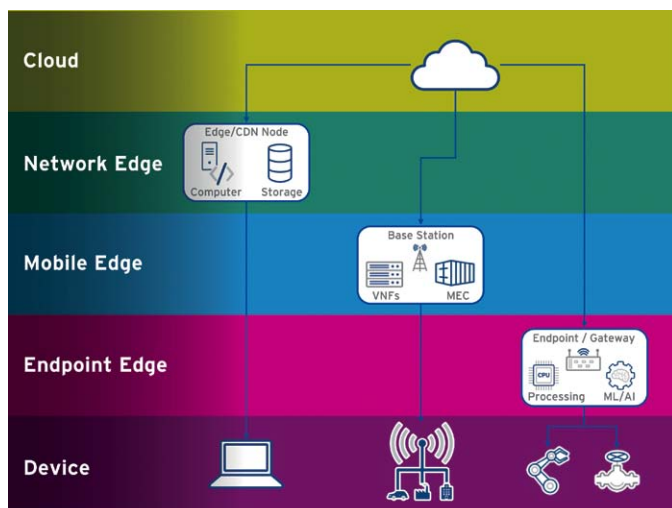


Produkte/Services

Praxistest Cisco Meraki Go Set

Das Set soll kleinen Unternehmen einen einfachen Einstieg in die sichere Vernetzung ermöglichen. Es besteht aus einem Secure Gateway, einem WLAN-Access-Point und einem LAN-Switch. Die Verwaltung erfolgt mit Hilfe einer App, die über die Meraki-Cloud auf die Geräte zugreift.

Seite 12



Technik

Security beim Edge Computing – Teil 2

Teil 1 dieses Beitrags in LANline 8/2021 reihte Edge Computing in die Liste der Begriffe ein, die beim Marketing-Buzzword-Bingo hoch im Kurs stehen. Das soll jedoch nicht darüber hinwegtäuschen, dass es auch viel inhaltliche Substanz gibt. Eine kritische Diskussion der Sicherheitsgrundsätze bis zum Endgerät steht noch aus.

Seite 32

Markt

Tech Day der LANline zur RZ-Kühlung: Richtig kühlen	6
Angriff auf Software-Provider Kaseya: Digitales Freibeutertum	8

Produkte/Services

Praxistest Cisco Meraki Go Set: Netzwerk-Komplettset	12
Test: Nutanix HCI: HCI-Plattform mit Hybrid-Cloud-Option	14

Schwerpunkt: Backup und Archivierung

Backup-Herausforderungen: Versicherung für das Unternehmensgedächtnis	18
Keine Lösung von der Stange: Techniken für eine Cyber-Recovery-Strategie	20
DSGVO-konforme Archivierung: E-Mail-Governance im Blick	22
BaaS, RaaS & DRaaS: Datensicherungsdienste für MSPs	24
Datensicherung für SaaS-Angebote: „One Size Fits All“ oder „Case by Case“?	26
Marktübersicht: Backup-Lösungen	28

Technik

Cybersecurity: OT und IT im Gleichschritt – Know-how bündeln	30
Security beim Edge Computing – Teil 2: Neues Bekanntes	32

Schwerpunkt: Hybrid- und Multi-Cloud-Vernetzung

Sicherheit in Zeiten der Hybrid Cloud: Dame, König, As, SASE	34
Monitoring des Applikationsverhaltens: Komplexe Multi-Clouds überwachen	37
Netzwerk-Management per Cloud: Vogelperspektive	39
SD-WAN mit Out-of-Band-Management: WAN der Enterprise-Klasse	41
Multi-Cloud-Architekturen: Resilienz und Innovation	43
Do it yourself vs. Managed Service: SASE verwalten per Co-Management	45
Marktübersicht: SD-WAN-Lösungen	44

News

Produktneuheiten und Aktuelles aus den Bereichen Netze, Daten- und Telekommunikation	28, 29, 44
---	------------

Rubriken

Editorial	3
IT Service Guide	47
Inserentenverzeichnis	49
Vorschau	50
Impressum	50

ALLE AUSGABEN ALS E-PAPER LESEN!



DIGITALE AUSGABEN AB SOFORT ERHÄLTICH.

shop.weka-fachmedien.de



Tech Day der LANline zur RZ-Kühlung

Richtig kühlen

Ein Rechenzentrum wandelt in großem Stil elektrischen Strom in Wärme um. Diesen Verlust möglichst gering zu halten und die Energie optimal für die Rechenkapazität zu nutzen, ist eine wichtige ökonomische, technische und im Zeitalter von allgegenwärtiger Digitalisierung und Klimawandel sogar eine gesellschaftspolitische Herausforderung mit vielen Facetten.

Beim ersten virtuellen „Tech Day“ der LANline im Juli stand das Thema RZ-Kühlung im Vordergrund. Bekanntlich ist dies der Teil der Datacenter-Infrastruktur, der am stärksten zum Energieverbrauch beiträgt und sich damit direkt als signifikanter Posten in jeder Betreiberrechnung niederschlägt. Rechenzentren energieeffizient zu betreiben und sie sowohl ökonomisch als auch ökologisch zu optimieren, heißt daher in erster Linie, die individuell optimale Kühlung zu finden. Hilfestellung dabei, zunächst einmal das passende Konzept für das Zusammenspiel von Cloud-, Colocation und eigenem Rechenzentrum zu finden, konnte Jürgen Strate, Direktor Sales & Strategic Business

Development, Site and Facilities Services bei IBM Deutschland und erfahrener RZ-Fachmann, in seinem Keynote-Vortrag leisten. Die Planung, der Bau, das Management und der Betrieb moderner Rechenzentren müssen heute mit adäquaten Konzepten und den passenden Werkzeugen erfolgen, wie Strate betonte. In die Strategie gehören jedoch auch Überlegungen zum Zusammenspiel mit hybriden Cloud-Strukturen. Laut Strate kann zeitgemäße Technik – beispielsweise in Form künstlicher Intelligenz – dabei helfen, die Anforderungen an Nachhaltigkeit und Energieeffizienz ebenso zu erfüllen wie normative und nicht zuletzt ökonomische Vorgaben. Die sich daraus ergebenden Hy-

brid-IT-Lösungsszenarien führen zu einer vernünftigen Roadmap-Planung und zu einer praxistauglichen Definition der Folgeaktivitäten. Bemerkenswert dieses Statement Strates dazu: „Es ist durchaus möglich, dass auch ein eigenes Rechenzentrum sich als optimale Lösung herausstellt.“

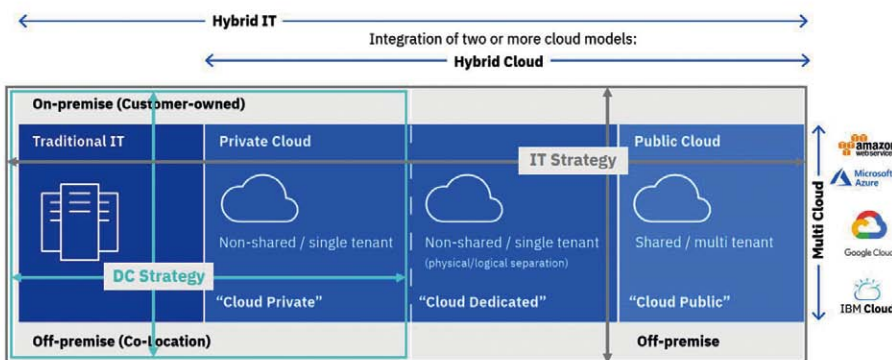
Offensichtlich gibt es innerhalb der RZ-Community ein ausgeprägtes Bewusstsein für diese Thematik, denn am LANline Tech Day nahmen insgesamt rund 170 Online-Besucher teil – als Zuhörer bei den Vorträgen, aber ebenso aktiv bei den anschließenden Diskussionen und in einer besonderen virtuellen Gesprächsrunde für alle per Video oder Telefon.

Welche Kühltechnik – und daraus abgeleitet, welche Geräteform – sich für ein bestimmtes RZ-Szenario am besten eignet, verdeutlichten Philipp Müller, Leiter Global Data Center Projects, und Michael Nicolai, Leiter Vertrieb IT Deutschland bei Rittal, in ihrem Online-Vortrag „Erfrischende Ideen für Ihr Rechenzentrum“. Mit der richtigen Größenauswahl der Kühlgeräte für den jeweiligen Einsatzzweck gelangt man schon sehr dicht an das individuelle Optimum, wie die beiden Rittal-Fachmänner eindrucksvoll vorrechnen konnten.

Zu den wichtigen Faktoren zählt außerdem zum Beispiel auch das passende Kühlmittel. Das Stichwort lautet F-Gas-Verordnung. Neben Kriterien wie der Klimaschädlichkeit kommt es hier unter anderem auch auf die Brennbarkeit oder Giftigkeit an.

Worauf in der Umsetzung solcher Projekte unter Praxisaspekten besonders zu achten hat, erklärten im dritten Vortrag des Tages Heiko Ebermann, Senior Program Manager Infrastructure Solutions, und Sascha Horn, Sales Engineer Thermal Management, beide von Vertiv. Unter anderem bei den immer mehr eingesetzten Edge-Anwendungen gibt es eine Vielzahl von unterschiedlichen Kühllösungen, die der Herausforderung durch sehr unterschiedliche Randbedingungen gerecht werden müssen. Neben Anwendungsbeispiele bot der Vortrag auch einen Ausblick auf die Zukunft mit einer Kombination aus flüssigkeitsgekühlten Servern und Luftkühlung.

Begriffsbestimmung DC-Strategie im Zeitalter von (Hybrid) Cloud



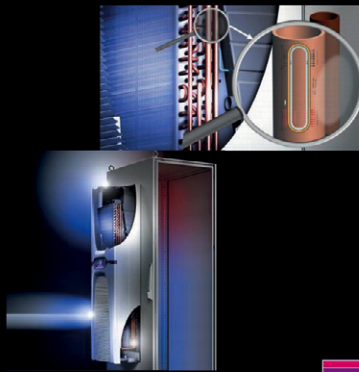
Wie ein gutes Konzept für das Zusammenspiel von Cloud-, Colocation und eigenem Rechenzentrum aussehen kann, erklärte Jürgen Strate, Direktor Sales & Strategic Business Development, Site and Facilities Services bei IBM Deutschland.

Bild: IBM

Klimatisierungsmethoden

Herausforderungen Kompressor vs. Heat Pipe

- Das Kühlgerät hat einen
 - **aktiven Kreislauf** mit einem Inverter-betriebenen Kompressor
 - und einem **passiven Kreislauf**, der aus einer Heat Pipe besteht.
- Ist die Temperatur auf der Rückseite des Servers höher als die Umgebungstemperatur des Racks, verdunstet das Kältemittel in der Heat Pipe und transportiert die Hitze nach außen durch Konvektion. Das Kühlmittel verflüssigt sich wieder. Nur die Lüfter arbeiten in diesem Betriebszustand.



Philipp Müller, Leiter Global Data Center Projects, und Michael Nicolai, Leiter Vertrieb IT Deutschland bei Rittal, gingen in ihrem Vortrag unter anderem auf verschiedene Kühltechniken ein. Bild: Rittal

Die abschließende Podiumsdiskussion („Rechenzentren in der Zwickmühle zwischen Leistungsanforderungen und Ressourceneinsparung – Was RZ-Kühlung als Beitrag leisten kann, ökonomische und ökologische Aspekte zu vereinen“), an der

neben allen Sprechern des Tages auch Thomas Wawra (DC Academy) teilnahm, griff unter anderem noch einmal die Frage auf, wie gut die Branche für die kommenden Aufgaben gerüstet ist. Technisch sei man auf Höhe der Zeit, so die einhellige

Meinung. Freikühlung – auch bei hohen Außentemperaturen – und Abwärmenutzung bieten zum Beispiel noch viel Potenzial. Auch wenn der Begriff derzeit etwas verpönt ist, sei allerdings durchaus mehr Lobbyarbeit der RZ-Branche sinnvoll. Ebenso sinnvoll – und auch da war man sich einig – ist die technische Weiterbildung und Wissensvermittlung auf Seiten der Anwender, also derjenigen, die schlussendlich alle Verantwortung tragen.

Die LANline-Veranstaltungsreihe Tech Days findet ab dem 9. September (Thema: RZ-Stromversorgung) auch weiter virtuell statt. Am 7. Oktober ist ein Tech Day zum Thema Single Pair Ethernet geplant. Daneben stehen mit dem Datacenter Symposium und dem Tech Forum zur Verkabelung ab dem 23. September auch wieder Präsenzveranstaltungen auf der Agenda.

Alle Informationen dazu gibt es auf lanline.de/events. Eine Registrierung ist bereits möglich und für Leserinnen und Leser kostenlos.

Dr. Jörg Schröper

Anzeige

Monitoring von Hybrid Cloud-Umgebungen

Hybrid-Cloud ist derzeit eines der Top-Themen in der IT. Es bezeichnet die gemeinsame Nutzung einer Private und der Public Cloud und – je nach Definition – auch die Einbeziehung lokaler IT-Komponenten. Genau wie in der lokalen IT gilt es auch bei Hybrid Cloud-Umgebungen Performance und Verfügbarkeiten ständig im Blick zu haben, um Ausfälle zu vermeiden und SLAs zu kontrollieren.

Dazu ist ein kontinuierliches und umfassendes Monitoring aller beteiligten Komponenten von grundlegender Bedeutung, sowohl in der Public oder Private Cloud als auch der IT-Infrastruktur vor Ort. Viele IT-Services und -Prozesse greifen auf Komponenten aus zwei oder allen drei Bereichen zu. Im Idealfall ist die eingesetzte Monitoring-Lösung in der Lage, sämtliche Bereiche abzudecken und übergreifende Services oder Prozesse entsprechend abzubilden. Allerdings sind die Anforderungen recht unterschiedlich:

1. Lokale IT

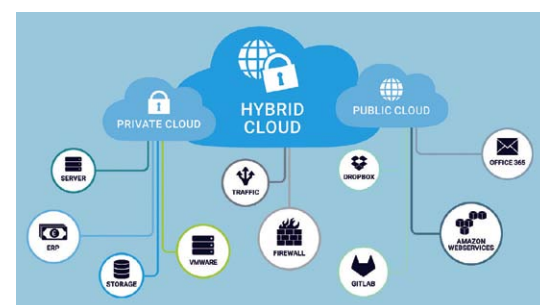
Hier spielt das Netzwerk die zentrale Rolle. Der Datentransfer aus der Cloud zum Nutzer muss stets gewährleistet sein. Natürlich muss auch die Infrastruktur vor Ort verfügbar und performant sein.

2. Private Cloud

In der Regel laufen hier Applikationen. Diese müssen ebenso überwacht werden wie die virtuellen Umgebungen, auf denen die Applikationen betrieben werden. Dazu kommt meist auch die darunter liegende Hardware, die als Basis unter der Private Cloud liegt. Auch die Datenspeicherung ist häufig in die Private Cloud ausgelagert und muss entsprechend überwacht werden.

3. Public Cloud

Die Möglichkeiten zur Überwachung der Public Cloud sind oft relativ begrenzt. Sie sind auf Tools des Cloud-Anbieters, wie etwa bei AWS auf Amazon CloudWatch beschränkt, um die Gesamtleistung der genutzten Cloud-Dienste zu überwachen.



Das Monitoring dient hier in erster Linie dazu, SLAs zu überwachen, um im Problemfall möglichst schnell mit dem Provider in Kontakt zu treten und SLA-Verstöße zu belegen. Paessler PRTG bietet die komplette Funktionalität zum zentralen Monitoring von Hybrid Cloud-Umgebungen ebenso wie der IT vor Ort. Mit PRTG sind Sie stets über alle Details informiert und im Bedarfsfall umgehend alarmiert. Sie definieren bereichsübergreifende Prozesse für einen zentralen Überblick über ihre gesamte IT. Kostenfreie 30-Tages-Test-Version <https://www.paessler.com/monitoring>

Angriff auf Software-Provider Kaseya

Digitales Freibeutertum

Im Zeitalter des Kolonialismus konnten Freibeuter wie Sir Francis Drake vom britischen Königshaus unbehelligt ihr Unwesen treiben, solange sie ihre Piraterie auf spanische und portugiesische Schiffe beschränkten und die heimischen unangetastet ließen. Ähnlich gehen heute russische Cybercrime-Organisationen wie REvil vor: Sie attackieren westliche, bevorzugt US-amerikanische Unternehmen und Organisationen mit Ransomware, halten sich aber wohlweislich von Russland und dessen Geschwisterstaaten fern.



Am Freitagnachmittag des 2. Juli – also kurz vor dem Wochenende, auf das dieses Jahr der US-National-Feiertag am 4. Juli fiel – waren die Systeme von Kaseya, einem Anbieter von Fernwartungssoftware mit Sitz in Miami, Florida, Ziel eines Zero-Day-basierten Ransomware-Angriffs. Da Kaseya seine Software namens VSA vorrangig an MSPs (Managed Services Provider) liefert, die wiederum zahlreiche kleinere und mittelgroße Unternehmen betreuen, war das Schadenspotenzial enorm. Doch da Kaseya laut eigenen Angaben innerhalb einer Stunde nach der Warnmeldung vorsichtshalber den Zugriff auf die betroffene Software abschaltete, ließ sich der Auswirkungsradius eindämmen: Laut Bekunden des Anbieters waren nur rund 50 von mehr als 35.000 Kunden betroffen – damit aber nach Schätzung von Experten wie auch von Kaseya selbst bis zu 1.500 MSP-betreute Anwenderunternehmen, darunter auch diverse in Deutschland.

Laut Erkenntnissen des britischen Security-Providers Sophos nutzten die Angreifer eine Zero-Day-Schwachstelle aus, um aus der Ferne auf VSA-Server zuzugreifen. Es handelt sich also um einen sogenannten Supply-Chain-Angriff ähnlich dem, der letztes Jahr auf den US-Softwareanbieter

SolarWinds abzielte: Die Angreifer infizierten die Systeme eines IT-Ausrüsters, um dann über diesen „Umweg“ über die IT-Lieferkette Zugriff auf Anwenderunternehmen zu erhalten – bei SolarWinds damals auf diverse US-Behörden, im aktuellen Fall privilegierten Zugriff auf die Endgeräte zahlreicher Firmen zum Zweck der Erpressung. Ein VSA-Server dient zur Automatisierung von IT-Aufgaben wie etwa Software-Rollouts. „Als solches besitzt er ein hohes Maß an Vertrauen seitens der Kundengeräte“, erläutert Sophos. „Wenn der VSA Server infiltriert wird, wird jeder angeschlossene Client jede Aufgabe ausführen, die der VSA Server anfordert, ohne zu hinterfragen.“ Dies sei wahrscheinlich ein Grund, warum die Kriminellen Kaseya ausgewählt hatten.

„Wir sind zu 100 Prozent sicher, dass wir wissen, wie es passiert ist, und wir haben es behoben“, sagte Kaseya-CEO Fred Voccola kurz nach dem Vorfall gegenüber der US-Fernsehsendung „Good Morning America“. Offenbar konnten die Angreifer eine Zero-Day-Schwachstelle ausnutzen, kurz bevor Kaseya in der Lage war, sie zu schließen. Nach dem Abschalten der VSA-Server, so verkündete der Softwareanbieter, habe man sofort ein internes Incident-

Response-Team aufgestellt, um die Art des Angriffs zu ermitteln, und die zuständigen Behörden informiert. Das sind in den USA die Bundespolizei FBI als Strafverfolgungsbehörde und die CISA (Cybersecurity and Infrastructure Security Agency). Kaseya arbeite mit verschiedenen Behörden zusammen, neben dem FBI und der CISA auch mit dem Department of Homeland Security und dem Weißen Haus – ein Hinweis darauf, für wie brisant man in den USA den Angriff der offenbar russischen Freibeuter hält. Zudem hat das Softwarehaus die Fachleute von FireEyes Incident-Response-Team Mandiant hinzugezogen, um den Vorfall aufzuarbeiten.

Der israelische Security-Anbieter Check Point warnt, dass die Kriminellen längst nicht nur auf die USA zielen: In den vergangenen zwei Monaten habe das hauseigene Forscherteam 15 neue REvil-Angriffe pro Woche verzeichnet, die meisten davon in den USA, Deutschland, Brasilien und Indien. „Im Jahr 2021 wurden bereits Rekorde für Cyberangriffe gebrochen“, so Christine Schöning von Check Points deutscher Organisation: „Der Anstieg von Ransomware-Angriffen liegt bei einem Allzeithoch von 93 Prozent weltweit, der aller Attacken in der EMEA-Region bei 97 Pro-

Web-Seminare

Know-how für Experten

WEB-SEMINAR

Alles unter Kontrolle - Server und Netzwerke zentral überwachen und Ausfälle reduzieren

Mal ehrlich, hätten Sie nicht auch gerne ein zentrales Monitoring, das Ihnen jederzeit zeigt, dass alle Server, Applikationen usw. in Ihrem Netzwerk im grünen Bereich sind?

Erfahren Sie in unserem Live-Webinar, wie Sie ganz einfach

- ein Network Operations Center (NOC) aufbauen
- einen Überblick über den aktuellen Status Ihrer Server und virtuellen Umgebungen haben
- den Datenverkehr und weitere Netzwerkdaten überwachen
- aussagekräftige Übersichten zur Analyse erstellen
- Routineaufgaben automatisieren und proaktiv alarmiert werden

DIENSTAG

21.
SEP
2021

10:00 UHR

ManageEngine

MICRONOVA
Software und Systeme



Sascha Degenhardt ist seit vier Jahren bei der MicroNova AG tätig und betreut Themen rund um Netzwerk-Monitoring, ITSM und IT Security. In seiner Rolle als Software Consultant begleitet er Kunden über den kompletten Lebenszyklus hinweg, angefangen bei der Installation und Konfiguration, bis hin zu Beratung / Schulung und Support. Durch seine Ausbildung zum Fachinformatiker für Anwendungsentwicklung unterstützt er Kunden zudem bei der Entwicklung von Schnittstellenlösungen und beim Customizing unserer Produkte.



Jetzt kostenfrei anmelden unter:

lanl.in/micronova



Ansprechpartner
zum Thema Web-Seminare:
Robin Beilicke
rbeilicke@weka-fachmedien.de
Tel.: +49 89 25556 1340

zent, und das nur in den letzten zwölf Monaten. Noch nie gab es so viele Opfer von Ransomware-Angriffen, von denen ein unbekanntes Ausmaß nicht nur allein die USA betrifft, sondern vermehrt sind es auch europäische Unternehmen, die hier ins Visier geraten sind.“

Der Angriff auf Kaseya im Detail

Hintergründe und Details zum Angriff gibt es bei mehreren Security-Providern, darunter beim US-Anbieter Palo Alto Networks: „REvil hat sich zu einem der berüchtigtsten Ransomware-Betreiber der Welt entwickelt“, schrieb Unit 42, Palo Altos Analyseteam, in einem Report. Schließlich hatte REvil erst kurz zuvor elf Millionen Dollar vom weltgrößten Fleischverpackungsunternehmen JBS (mit Hauptsitz in Brasilien und zweitem Firmensitz in Dallas, Texas) erpresst.

Man sei REvil erstmals 2018 begegnet, als die Kriminellen mit der GandCrab-Gruppierung zusammenarbeiteten, um Ransomware durch Malvertising und Exploit-Kits zu verbreiten. „Diese Gruppe entwickelte sich zu REvil, wuchs und erwarb sich den Ruf, riesige Datensätze zu exfiltrieren und Lösegelder in Höhe von mehreren Millionen Dollar zu fordern“, so Palo Alto. „Sie gehört nun zu einer Elitegruppe von Cybererpresserbanden, die für den Anstieg der lähmenden Angriffe verantwortlich sind, die Ransomware zu einer der drängendsten Sicherheitsbedrohungen für Unternehmen und Nationen rund um den Globus gemacht haben.“

Als einer der bekanntesten RaaS-Anbieter (Ransomware as a Service) biete die kriminelle Gruppe anpassungsfähige Ver- und Entschlüsselungsprogramme, Infrastruktur und Dienste für die Verhandlungskommunikation sowie eine Leak-Site zur Veröffentlichung gestohlener Daten, wenn die Opfer die Lösegeldforderung nicht bezahlen. Dafür nehme REvil einen Prozentsatz des ausgehandelten Lösegeldpreises als Gebühr in Anspruch. Denn das Mittel der Wahl ist die sogenannte „doppelte Erpressung“: Erstens verschlüsselt der Angreifer Unternehmensdaten, sodass die Unternehmen nicht auf ihre Informationsbestände zugreifen und kritische Systeme nicht ver-

wenden können, und fordert Lösegeld für die Entschlüsselung. Zweitens stiehlt er aber auch Daten und droht damit, die Interna – darunter gegebenenfalls auch Börsenrelevantes – auf seiner Leak-Site zu veröffentlichen. Im ersten Halbjahr 2021 haben Kriminelle mit REvil nach Palo-Alto-Berechnungen im Schnitt rund 2,25 Millionen Dollar (in Bitcoins) erbeutet. Die Höhe der Lösegelder hänge von der Größe des Unternehmens und der Art der gestohlenen Daten ab. Dabei verdoppeln die Angreifer oft die Forderung, wenn die Opfer die vorgegebene Zahlungsfrist nicht einhalten. Bei der Höhe des Lösegelds ist die Erpressergruppe laut Experten allerdings verhandlungsbereit.

REvil-Bedrohungsakteure verwenden laut Palo Alto zuvor kompromittierte Zugangsdaten, um per RDP (Remote Desktop Protocol) aus der Ferne auf externe Ressourcen zuzugreifen. Eine weitere häufig beobachtete Taktik sei eine Infiltration mit Malware per Phishing. Man habe aber auch schon abweichende Angriffsvektoren beobachtet. Sobald die Kriminellen sich Zugang verschafft haben, nutzen sie laut den Experten in der Regel das Angriffswerkzeug Cobalt Strike, um sich in einer IT-Umgebung einzunisten, mitunter aber auch eine Remote-Control-Software wie ScreenConnect und AnyDesk. „Außerdem deaktivierten die Bedrohungsakteure häufig Antiviren- und Sicherheitsdienste sowie Prozesse, die ihre Anwesenheit in der Umgebung stören oder anderweitig aufdecken würden“, so die Security-Analysten. Danach verschaffen sich die Kriminellen laut Unit 42 Zugang zu zusätzlichen Konten, die über eine breitere Palette von Berechtigungen verfügen (Privileg-Eskalation), um sich weiter in der Umgebung des Opfers zu bewegen und ihre Mission auszuführen. Dazu komme oft Mimikatz zum Einsatz, um auf zwischengespeicherte Zugangsdaten auf dem lokalen Host zuzugreifen, oder aber das SysInternals-Tool procdump sowie Open-Source-Tools. In der letzten Angriffsphase gehe die Angreiferseite dazu über, Netzwerke zu verschlüsseln, Daten zu exfiltrieren und dann zu zerstören, um eine Wiederherstellung zu verhindern und die Analyse zu erschwe-

ren. Unit 42 hat zudem beobachtet, dass die Kriminellen diverse Verteidigungsmanöver (Evasion Techniques) nutzen, um einer Erkennung zu entgehen. Zudem lösche man, eine übliche Taktik, Schattenkopien von Windows-Systemen, offenbar auch, um die Wiederherstellung forensischen Beweismaterials zu verhindern.

Im Kaseya-Fall stellte die REvil-Gruppe ungewöhnlicherweise eine „Sammelforderung“ für die Freigabe verschlüsselter Daten in Höhe von 70 Millionen Dollar, später senkte sie die Forderung auf 50 Millionen. Kaseya verfügt laut Palo Altos Unit 42 über einen Entschlüsselungs-Key; ob eine Zahlung geleistet wurde, sei aber unbekannt. Seit Mitte Juli sind die REvil-Sites inklusive Bezahl- und Data-Leak-Seite allerdings offline. Die Hintergründe dieser Entwicklung sind unklar.

Palo Alto Networks rät IT-Organisationen, sich die Zeit zu nehmen, um zu lernen, was in ihren Umgebungen normal ist, um Anomalien bemerken zu können. Ebenso gelte es, die Verteidigungsmaßnahmen zu hinterfragen, nicht nur einmal, sondern routinemäßig immer wieder. Zu einer weiteren Verteidigungsmaßnahme, die insbesondere angesichts russischen Freibeutertums von Nutzen sein kann, rät Security-Blogger Brian Krebs. Es sei bei „praktisch allen Ransomware-Stämmen“ eine eingebaute Failsafe-Funktion festzustellen: „Sie lassen sich einfach nicht auf einem Microsoft-Windows-Computer installieren, auf dem bereits eine der vielen Arten virtueller Tastaturen installiert ist – beispielsweise Russisch oder Ukrainisch“, so Krebs.

Es könnte somit ratsam sein, Russisch als zusätzliche Tastatursprache auszuwählen – natürlich nicht anstelle von, sondern als Ergänzung zu durchdachten Security-Maßnahmen. Ob es einst half, unter britischer Flagge zu segeln, um Francis Drake & Co. fernzuhalten, ist fraglich – die Freibeuter dürften spanische Galeonen schon an der Bauform erkannt haben. Wenn hingegen heute das Hissen einer russischen Flagge auf der Computertastatur hilft – warum nicht? Aber man möchte sich zur Abwehr digitaler Piraten natürlich nicht gänzlich auf ein buntes Wimpelchen verlassen.

Dr. Wilhelm Greiner

Studie Digital Workplace

ab dem 16. September 2021

**Jetzt
Startdatum
vormerken!**

**Was folgt auf den
Homeoffice-Boom?**

Die vergangenen Monate haben unterstrichen, dass moderne, flexible Arbeitskonzepte nicht nur funktionieren, sondern vor allem auch eine effiziente Zusammenarbeit über verschiedenste Standorte hinweg ermöglichen können.

Doch entwickelt sich aus dem notgedrungenen Homeoffice-Boom auch eine langfristige Strategie, welche Technologien kommen dabei zum Einsatz und zielen Unternehmen tatsächlich auf die Gestaltung eines Digital Workplace ab?

Im kommenden September startet die gemeinsame Studie rund um den digitalen Arbeitsplatz. Wir freuen uns über Ihre Teilnahme.

Nur auf funkschau.de, ict-channel.com und lanline.de

funkschau

ICT
CHANNEL

LANline

WEKA Consulting

PLATIN-SPONSOREN



secunet

GOLD-SPONSOREN

ivanti] **pexip** [

BRONZE-SPONSOREN

byon **logitech**

STARFACE
COMFORTPHONING

Praxistest Cisco Meraki Go Set

Netzwerk-Komplettset

Das Meraki Go Set von Cisco soll kleinen Unternehmen einen einfachen Einstieg in die sichere Vernetzung ermöglichen. Das Set besteht aus einem Secure Gateway für die Internetanbindung sowie einem WLAN-Access-Point und einem LAN-Switch. Die Verwaltung erfolgt mit Hilfe einer Mobilgeräte-App, die über die Meraki-Cloud auf die Geräte zugreift.



Ciscos Meraki Go Set besteht aus einem Secure Gateway (Bild), einem WLAN-Access-Point und einem LAN-Switch.

Bild: Cisco

Die zunehmende Verlagerung von Services in die Cloud macht auch vor Netzwerk-Management-Lösungen nicht Halt. Neben einem flexiblen Zugriff, der von überall aus per Internet möglich ist, bieten über die Cloud bereitgestellte Services den Vorteil, dass ein Unternehmen sich nicht selbst um die für die jeweilige Anwendung benötigten Backend-Systeme kümmern muss. Cisco bietet mit Meraki Go ein Netzwerk-Komplettset für kleinere Unternehmen an, das man über die Cloud verwaltet. Die App für das Management ist für iOS und Android erhältlich. Sie verbindet sich mit der Meraki-Cloud, um auf diesem Weg mit den Geräten zu kommunizieren. Das Set enthält das Security-Gateway GX20, das über den WAN-Port die Internetanbindung herstellt und vier LAN-Ports bereitstellt, von denen einer PoE (Power over Ethernet) unterstützt. Für die Funkvernetzung stehen der Indoor-Access-Point GR10 und das Outdoor-Modell GR60 zur Verfügung. Die LAN-Switch-Modelle für das kabelgebundene Netz reichen von dem 8-Port-Switch GS110 über einen 24-Port-Switch bis zu ei-

nem Gerät mit 48 LAN-Ports. Alle Switches sind mit zwei zusätzlichen SFP-Uplink-Ports ausgestattet und auch als PoE-Version erhältlich.

Für den LANline-Test stellte Cisco ein Set mit dem GX20 Security Gateway, dem WLAN-AP GR10 und dem lüfterlosen 8-Port-Switch GS110 zur Verfügung. Da die Verwaltung über die Cloud erfolgt, muss der Anwender als erstes auf der Meraki-Go-Website ein Konto anlegen. Nach der Registrierung installierten wir die Meraki-Go-App auf einem iPhone und meldeten uns an. Um die Geräte in einen Cloud-Account aufzunehmen, scannt der Systemverwalter mit seinem Handy einfach den auf der Geräterückseite angebrachten QR-Code. Dadurch übertragen die Geräte automatisch die für das System-Management benötigten Daten wie zum Beispiel Modellname und MAC-Adresse in die Cloud. Nachdem wir die drei Geräte gescannt hatten, verbanden wir den LAN-Switch mit einem LAN-Port des Security Gateways und den WLAN-AP mit einem Port des LAN-Switches. In den Internet-Port des

Gateways steckten wir das LAN-Kabel zum DSL-Modem, das an eine 50/10-MBit/s-Leitung von 1&1 angeschlossen war, und schalteten die drei Geräte ein. In der App klickten wir auf den Such-Button, um unsere Meraki-Geräte über die Cloud zu finden. Die Suche blieb zunächst erfolglos, weil das Security-Gateway aufgrund der 1&1-Zugangsdaten, die dem Gerät noch nicht bekannt waren, keine Internetverbindung herstellen konnte. Bei DSL-Anschlüssen, bei denen die ISP-Login-Daten bereits im DSL-Modem hinterlegt sind, verbindet sich das Security-Gateway automatisch mit dem Internet und der Meraki Cloud. Im LANline-Testnetz ist das DSL-Modem jedoch ohne Zugangsdaten in einem Spezialmodus für PPPoE (Point-to-Point over Ethernet) konfiguriert. Nach kurzer Suche im Internet fanden wir den Hinweis, dass sich das Security Gateway lokal über eine minimalistische Web-GUI konfigurieren lässt, wenn ein Rechner an einem LAN-Port des Geräts hängt. Dies funktionierte, und wir konnten auf diesem Weg den Internet-Port vom Direktmodus auf PPPoE umstellen und unsere 1&1-Zugangsdaten eingeben. Danach verband sich das Gateway mit dem Internet und führte als erstes automatisch ein Software-Update durch. Auch der LAN-Switch und der WLAN-AP verbanden sich mit der Meraki-Cloud und aktualisierten ebenfalls selbsttätig ihre Firmware.

Die Einrichtung des Funknetzwerks erfolgt ebenfalls über die App. Unter Netzwerke zeigte sie das Standard-WLAN an, das Meraki heißt. Wir änderten den Namen und trugen ein Kennwort ein, das die WLAN-Clients beim Login angeben müssen. Man kann für den WLAN-Login auch einen QR-Code erzeugen, damit die Beschäftigten keine Zugangsdaten mehr eingeben müssen.

Anschließend konnten wir uns mit einem Notebook am WLAN anmelden. Mit `ipconfig /all` überprüften wir, welche IP-Adresse der Rechner erhalten hatte. Der WLAN-AP hatte eine IP-Adresse aus einem 10er-Netz zugewiesen. Die Meraki-Geräte und der am LAN-Switch angeschlossene Test-PC verwendeten dagegen das Netz 192.168.128.0. Daraufhin öffne-

ten wir in der App nochmals die WLAN-Einstellungen und sahen, dass standardmäßig der NAT-Modus eingeschaltet ist, der den WLAN-Clients eine IP-Adresse aus einem isolierten Gastnetz zuweist. Wir änderten das Setting auf den Bridge-Modus und starteten das für die WLAN-Tests genutzte Notebook neu. Diesmal erhielt es eine IP-Adresse aus dem LAN und konnte so mit dem am LAN-Switch angeschlossenen PC kommunizieren.

Abgesehen von den wenigen Konfigurationsparametern, die sich über die minimalistische Web-Konsole ändern lassen, erfolgt die komplette Verwaltung der Geräte mit der Meraki-Go-App. Hier lässt sich zum Beispiel einstellen, welche Anwendungen wie viel Bandbreite nutzen dürfen. Eine Auswahlliste mit 25 Kategorien vereinfacht die Konfiguration. Zudem steht eine manuelle Blacklist-Funktion zur Verfügung, um den Zugriff auf bestimmte Websites zu sperren. Auch Ausschlusszeiten, in denen das WLAN nicht verfügbar ist, lassen sich festlegen. Port-Forwarding macht ausgewählte Services unter einem bestimmten Port von außen erreichbar.

Um bei Störungen schnell Nachricht zu erhalten, empfiehlt es sich, in der App die Alarmierung per E-Mail- oder Push-Nachrichten zu aktivieren. Standardmäßig versendet das Tool Warnungen, sobald eine Hardware länger als fünf Minuten nicht mehr erreichbar ist. Man kann sich auch

Tested by



Cisco Meraki Go Set

<https://meraki.cisco.com>

- ✓ Gut aufeinander abgestimmtes Set für die Einrichtung lokaler LANs und WLANs inklusive sicherer Internetanbindung
 - ✓ Einfache Inbetriebnahme und Verwaltung über iOS- oder Android-App
 - ✓ Schnelle Registrierung der Geräte in der Meraki-Cloud per QR-Code-Scan
 - ✓ VLAN-Support auf allen Geräten, um sensible Bereiche besonders zu schützen
-
- ✗ Keine Web-Browser-Konsole für das Geräte-Management verfügbar

benachrichtigen lassen, wenn das Volumen des Internet-Traffics innerhalb eines bestimmten Zeitfensters den definierten Schwellenwert übersteigt. Um den Warnmechanismus zu testen, schalteten wir kurzerhand die Steckdosenleiste aus, an der die drei Meraki-Geräte angeschlossen waren. Nach gut fünf Minuten ging bei dem in der App hinterlegten E-Mail-Konto zu jedem Gerät eine Mail ein, dass das System nicht mehr zu erreichen ist. Als wir die Steckdosenleiste eine Stunde später wie-

der einschalteten, kamen erneut drei E-Mails mit der Meldung, dass die Geräte jetzt wieder online sind. Für den Zugriff auf die App lässt sich auch eine Multi-Faktor-Authentifizierung einrichten. Optional erhältlich ist ein Abo für das GX Security Gateway, die Ciscos SASE-Lösung (Secure Access Service Edge) Umbrella nutzt. Sie bietet unter anderem zusätzliche DNS-basierte Schutzmechanismen sowie Anti-Malware- und Anti-Phishing-Funktionen. Um in einem Meraki-Go-Netz ein neues VLAN hinzuzufügen, legt der Administrator zunächst auf dem GX-Security-Gateway ein neues Wired Network an und weist diesem eine IP-Adresse und eine VLAN-ID zu. Wird die Option „Secure this network“ aktiviert, erstellt das System automatisch Firewall-Regeln, um den Datenverkehr zwischen VLANs zu blockieren. Das Meraki Go Set überzeugte im Test durch einfache Inbetriebnahme und Verwaltung. Die Mobile App für iOS und Android ist übersichtlich gestaltet, wir fanden uns schnell darin zurecht. Der Umfang der konfigurierbaren Funktionen reicht allerdings nicht an Web-Browser-basierte Netzwerk-Management-Tools heran. Mit Straßenpreisen ab etwa 110 Euro für das Security-Gateway, 95 Euro für den Indoor-AP und 200 Euro für den 8-Port-PoE-Switch sind die Meraki-Produkte auch für kleine Geldbeutel erschwinglich.

Christoph Lange/wg



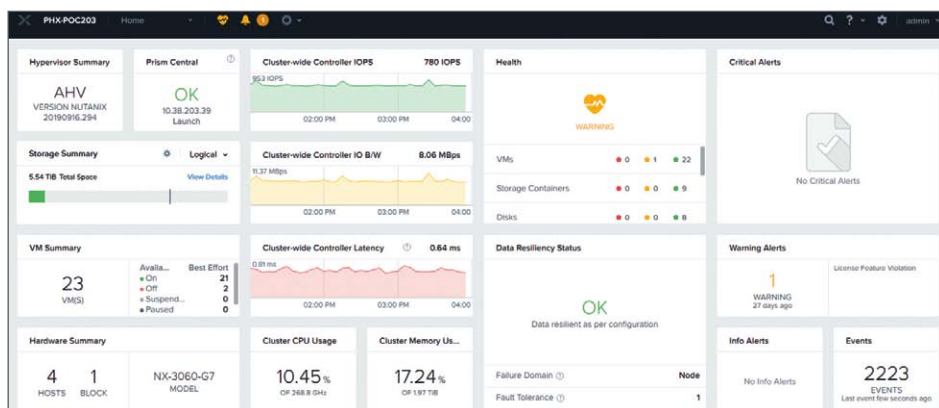
www.faberkabel.de

WIR BRINGEN
DIE ZUKUNFT
IN ROLLEN.

Im Test: Nutanix HCI

HCI-Plattform mit Hybrid-Cloud-Option

Die HCI-Lösung (Hyperconverged Infrastructure) von Nutanix stellt eine Virtualisierungsplattform bereit, die sich für die meisten Workloads eignet. Mit Nutanix Clusters on AWS lassen sich jetzt auch hybride Clouds unterstützen. Die Verwaltung aller Ressourcen erfolgt über die Management-Anwendung Prism Central.



Das Dashboard von Nutanix bietet einen schnellen Überblick zum aktuellen Zustand der HCI-Infrastruktur.

Bild: Christoph Lange

Das im Jahr 2009 gegründete US-amerikanische Unternehmen Nutanix zählt zu den Pionieren auf dem Markt für hyperkonvergente Infrastrukturlösungen (HCI). HCI-Plattformen bestehen aus einem ausfallsicheren Verbund von mehreren physischen Server-Systemen, die sowohl die CPU- und RAM-Ressourcen als auch die virtuellen und physischen Netzwerkverbindungen sowie die Storage-Kapazitäten für den Betrieb von virtuellen Rechnern bereitstellen. Anwendende können bei Nutanix frei wählen, ob sie für die Virtualisierung den hauseigenen lizenzfreien Hypervisor AHV (Acropolis), VMware ESXi oder Microsoft Hyper-V einsetzen wollen.

Der Hersteller hat eigene HCI-Komplettlösungen auf Basis von Supermicro-Servern im Portfolio. Von Nutanix zertifizierte Server-Hardware sowie schlüsselfertige HCI-

Appliances sind über Partner erhältlich. Bezüglich der Architektur hat Nutanix sich dazu entschieden, auf jedem physischen Host eine Controller-VM (CVM) mit dem Acropolis OS (AOS) zu implementieren, die den größten Teil der HCI-Funktionen steuert und dafür erheblich CPU- und RAM-Ressourcen benötigt. Bei VMware und bei Microsoft sind die HCI-Funktionen dagegen in das Hypervisor-Betriebssystem integriert, das direkt auf die Host-Ressourcen zugreift.

Mit Clusters on AWS bietet Nutanix die HCI-Plattform als schlüsselfertige Lösung an, die auf Hardware-Servern in der AWS-Cloud läuft. Für die Zukunft ist geplant, Nutanix Clusters auch in der Microsoft Azure-Cloud bereitzustellen. Den LANline-Test führten wir mit mehreren Nutanix-Clustern durch. Zum einen installierten wir

im LANline-Testlab mit der für Testzwecke kostenfreien Nutanix Community Edition einen 3-Node-Cluster, für den drei T640-Server von Dell zum Einsatz kamen. Das Setup führten wir per USB-Stick durch, auf den wir zuvor das Installations-Image aufgespielt hatten. Nach der Basisinstallation erfolgt die Konfiguration des Clusters. Für Testzwecke lässt sich auch ein 1-Node-Cluster mit nur einem physischen Host erstellen. Wir richteten einen 3-Node-Cluster ein, und die Setup-Routine installierte auf jedem Host eine Controller-VM. Anschließend konnten wir uns per Web-Browser über die virtuelle Cluster-IP-Adresse mit der Basis-Management-Konsole Prism Element verbinden. Um alle HCI-Funktionen verwalten zu können, ist eine zusätzliche virtuelle Appliance mit der Anwendung Prism Central erforderlich. Nachdem wir diese VM erstellt hatten, konnten wir mit dem Nutanix-Cluster im LANline-Testlab die HCI-Funktionen testen.

Außerdem führten wir die Tests per Remote-Zugriff auf einen 4-Node-Cluster durch, der in einem Rechenzentrum von Nutanix in den USA lief und für den LANline-Test exklusiv zur Verfügung stand. Zu diesem Cluster fügten wir zum Abschluss der Tests einen weiteren Nutanix-Cluster hinzu, der in der AWS-Cloud lief. Anschließend konnten wir die aus den zwei HCI-Clustern bestehende hybride Cloud über die Prism-Central-Konsole zentral verwalten.

Funktionsweise von Nutanix HCI

Die Virtualisierungsplattform von Nutanix bietet alle für einen ausfallsicheren Betrieb erforderlichen Funktionen. So lassen sich virtuelle Rechner im laufenden Betrieb zwischen den Cluster-Nodes verschieben. Beim Ausfall eines physischen Hosts lassen sich die VMs auf den anderen Knoten neu starten, wobei der Acropolis Dynamic Scheduler Service die Last automatisch gleichmäßig auf die Nodes verteilt. Cluster-Erweiterungen sind durch das Hinzufügen neuer Host-Systeme ebenfalls im laufenden Betrieb möglich. Die HCI-Software stellt die neuen Ressourcen automatisch zur Verfügung und führt ein Re-Balancing der Storage-Kapazitäten durch. Die Speicherkapazitäten verwaltet die Distributed

Storage Fabric (DSF) von Nutanix. DSF fasst alle in den physischen Hosts vorhandenen HDD- und SSD-Laufwerke zu einem großen Speicherpool zusammen. Bei Bedarf lassen sich auch mehrere Pools mit unterschiedlichen Charakteristiken einrichten. DSF führt standardmäßig ein Thin Provisioning durch. Die Storage-Zugriffe erfolgen effizient, indem die CVM des Cluster-Nodes, auf dem die VM gerade läuft, alle Lesezugriffe immer lokal ausführt. Wenn eine CVM ausfällt, laufen die VMs des betroffenen physischen Nodes ohne Unterbrechung weiter.

DSF unterstützt Storage-Policies, die sich auf Basis von sogenannten Storage-Containern zuweisen lassen. Ein Container ist eine logische Gruppierungsebene, der man VMs oder einzelne vDisks zuordnen kann. Mit einer Policy lässt sich zum Beispiel festlegen, ob die Daten einer VM komprimiert und dedupliziert sein sollen und welches Redundanzverfahren zum Einsatz kommt.

Nutanix verwendet standardmäßig den Redundanzfaktor RF=2, was bedeutet, dass jeder Datenblock auf zwei Nodes gespeichert ist. Dies schützt vor dem Ausfall eines Laufwerks oder eines physischen Hosts. Mit RF=3 legt die Software jeden Block auf drei Cluster-Nodes ab, womit auch bei einem gleichzeitigen Ausfall von zwei Hosts keine Daten verloren gehen. Zum Schutz vor Standortausfällen hat Nutanix eine asyn-

chrone Replikation auf Basis von VM-Snapshots implementiert. Damit lassen sich die Replica-VMs schnell online bringen, wenn das primäre RZ ausfällt. Nutanix verwendet ressourcenschonende Redirect-on-Write-Snapshots und unterstützt eine One-to-One- und One-to-Many-Replikation. Das kürzeste Replikationsintervall beträgt eine Minute, Nutanix bezeichnet dies als Near-Sync.

Die HCI-Software unterstützt zudem verschiedene Scale-out-Storage-Services. Mit den File-Services lassen sich SMB- und NFS-Shares bereitstellen. Bei Nutanix Objects handelt es sich um eine Object-Storage-Lösung mit S3-kompatiblen Rest API. Nutanix Volumes ist ein Block-Level-Service für iSCSI.

Die Netzwerkvirtualisierung mit Nutanix AHV funktioniert ähnlich wie die Distributed Virtual Switches von VMware und lässt sich für alle Cluster-Nodes zentral konfigurieren. Nutanix bietet mit Flow eine eigene Netzwerksicherheitslösung an, die eng in AHV und Prism Central integriert ist. Sie stellt eine Netzwerkvisualisierung und Automatisierungsfunktionen bereit. Flow unterstützt zudem eine Mikrosegmentierung mit Hilfe einer verteilten Firewall, um VMs auf einer granularen Ebene zu schützen. Eine Verschlüsselung der gespeicherten Daten ist ebenfalls möglich.

Die Nutanix-Plattform umfasst auch Werkzeuge für die Workflow-Orchestrierung

und Automatisierung. Mit Calm lassen sich eigene Projekte individuell oder auf Basis von Blueprints erstellen, um die für Services oder Applikationen benötigte Infrastruktur automatisiert bereitzustellen.

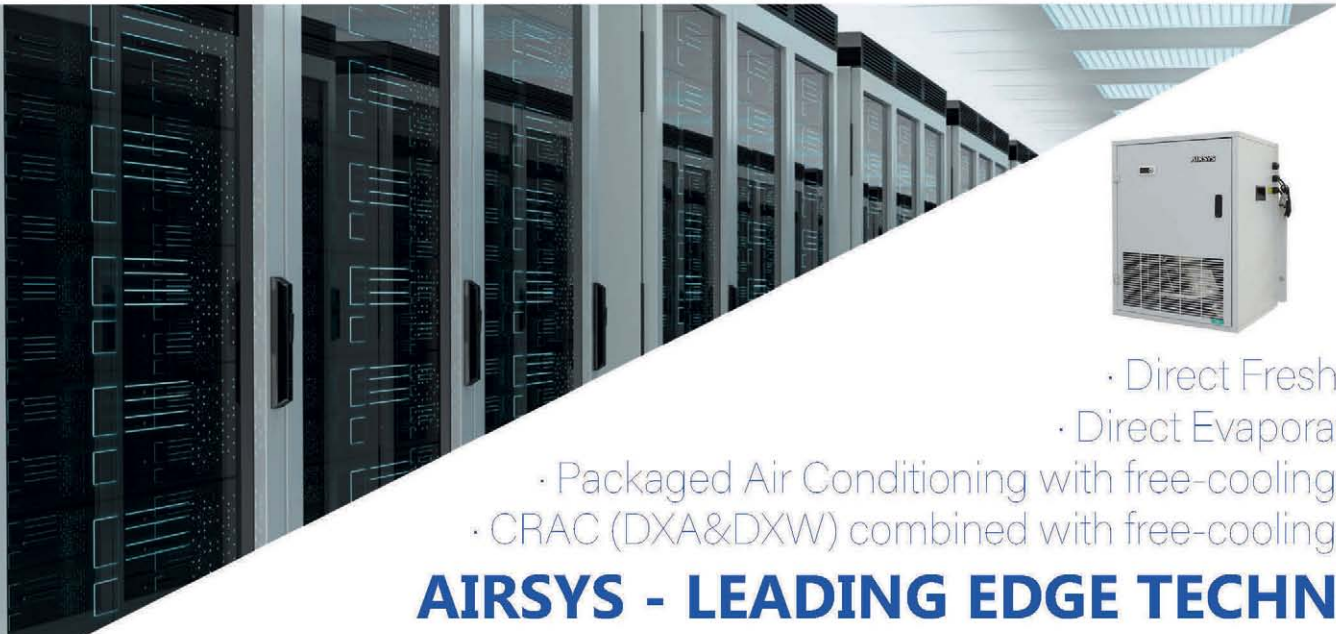
Tools für die Automatisierung

Die Pro-Version von Prism bietet zusätzlich das Machine-Learnig-Tool X-Fit und das Automatisierungswerkzeug X-Play zum Ausführen von Runbooks. X-Fit dient unter anderem zur Erkennung von Anomalien und ineffizienter Ressourcennutzung und liefert die Grundlage für Forecast-Berechnungen mit „Was wäre wenn“-Szenarien, um Infrastrukturveränderungen akkurat planen zu können. Mit Tools wie Terraform oder Ansible lässt sich Nutanix auch gut in große Automatisierungsumgebungen integrieren.

Für die Verwaltung von Kubernetes-Clustern bietet Nutanix mit Karbon eine eigene Lösung an. Auch das Datenbank-Management lässt sich mit der HCI-Lösung vereinfachen, zum Beispiel indem Datenbanken lokal repliziert und zusätzlich asynchron in die Cloud übertragen werden. Für das Lifecycle-Management (LCM) findet sich ein Tool in Prism Element und eine zweite Software in der Prism-Central-Konsole. Mit LCM kann der Systemverwaltende sowohl hardwarebezogene Komponenten wie BIOS, Firmware und Treiber aktualisieren als auch die verschiedenen

AIRSYS

www.air-sys.eu
anfragen@air-sys.eu



- Direct Fresh Air Cooling
- Direct Evaporative Cooling
- Packaged Air Conditioning with free-cooling technology
- CRAC (DXA&DXW) combined with free-cooling technology

AIRSYS - LEADING EDGE TECHNOLOGY

Nutanix-Anwendungen auf den neuesten Stand bringen. Der Hersteller arbeitet bereits daran, die zwei LCM-Tools in einer Anwendung zusammenzuführen.

Nutanix HCI im Testbetrieb

Mit dem Nutanix-Cluster im LANline-Testlab führten wir unter anderem einen Ausfalltest durch. Zunächst importierten wir über die Prism-Central-Konsole eine ISO-Datei mit Windows Server 2019 als Image-File. Dann erstellten wir eine neue VM, banden die Image-Datei an und starteten das Setup von WS2019. Die IT-Administration muss für die Installation von Windows-VMs eine zweite Image-Datei mit den Virt-IO-Treibern von Nutanix anbinden und im Windows-Setup den passenden Storage-Controller-Treiber laden, damit die vDisk erkennbar ist. Nachdem wir WS2019 erfolgreich installiert hatten, zogen wir bei dem physischen Host, auf dem die VM lief, das Stromkabel ab. Daraufhin startete einer der anderen beiden Nodes die VM innerhalb von wenigen Minuten automatisch neu.

Damit wir auf den von Nutanix bereitgestellten 4-Node-Cluster zugreifen konnten, installierten wir auf einem Testnotebook den VPN-Client Pulse Secure und konfigurierten die Web-Adresse des Nutanix-Portals. Der Client stellte anschließend erfolgreich eine Verbindung her, und wir konnten uns an der Prism-Management-Konsole anmelden. Das Dashboard der Prism-Konsole liefert einen guten Überblick zum aktuellen

Tested by


IT • Network • Datacenter

Nutanix HCI

<https://www.nutanix.com/de>

- ✓ Leistungsfähige, einfach skalierbare HCI-Infrastruktur
- ✓ Umfangreiches Werkzeugset für Automatisierung, Workflow-Orchestrierung, Forecast-Analysen und Mikrosegmentierung
- ✓ Einfach zu bedienende Management-Konsole, die alle HCI-Cluster zentral verwalten kann
- ✓ Mit Nutanix Clusters on AWS lässt sich eine Hybrid Cloud schnell implementieren

✖ Für das Lifecycle-Management sind bislang zwei verschiedene Tools nötig

Zustand der HCI-Umgebung. Die Navigation zu den verschiedenen Konfigurationsbereichen erfolgt mit Hilfe einer übersichtlichen Menüstruktur, in der wir uns schnell zurechtgefunden haben.

Die Testumgebung enthielt schon startbereite Image-Dateien für Windows und Linux, mit denen eine neue VM in wenigen Minuten betriebsbereit ist. Wir erstellten damit zunächst eine neue WS2016-VM und konnten uns nach etwa drei Minuten daran anmelden. Um zusätzlich eine VM mit WS2019 aufzusetzen, kopierten wir zunächst per WinSCP mit dem SFTP-Pro-

tokoll eine Windows-2019-ISO-Datei vom LANline-Testnetz in die Testumgebung in den USA. Anschließend erzeugten wir damit in Prism Central eine Image-Datei, banden diese an die neu erstellte VM an und installierten dann in der VM erfolgreich das WS2019-Betriebssystem.

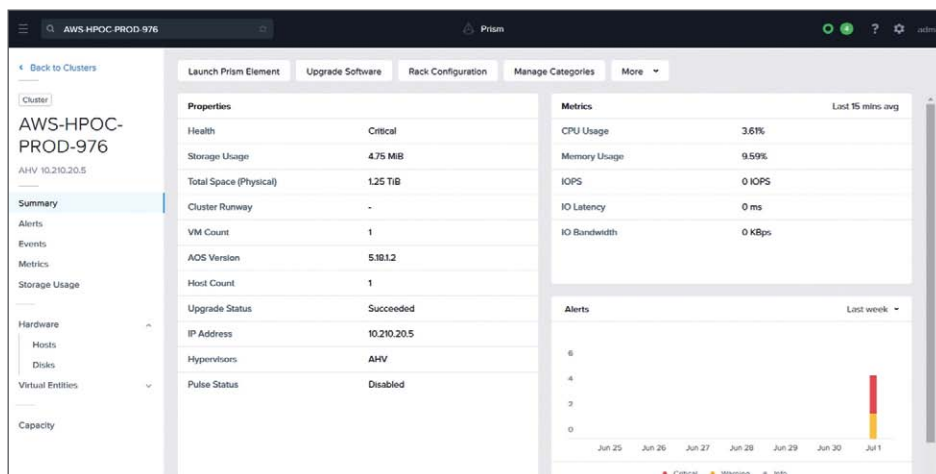
Zum Abschluss der Tests fügten wir in der Prism-Central-Konsole einen neuen Nutanix Cluster on AWS hinzu. Die von AWS für die Provisionierung benötigten Informationen waren bereits zuvor in der Testumgebung hinterlegt. Anschließend konnten wir den AWS Cluster über Prism Central verwalten. VMs lassen sich mit Hilfe eines DR-Szenarios auf Basis von Snapshots und Planned Failover zwischen der AWS-Cloud und der Private Cloud beliebig verschieben. Dafür wären jedoch zusätzliche Konfigurationen erforderlich gewesen, die den zeitlichen Rahmen des LANline-Tests gesprengt hätten.

HCI-Lösung mit Automatisierung und Hybrid-Cloud-Option

Die HCI-Lösung von Nutanix stellt auf Basis von Standard-Server-Hardware eine leistungsfähige Virtualisierungsplattform zur Verfügung, die sich für die meisten Workloads gut eignet. Ein Cluster lässt sich per Hinzufügen von Hardware-Nodes, deren Ressourcen automatisch in den Verbund eingefügt werden, ohne großen Aufwand skalieren. Die Verwaltung der kompletten HCI-Infrastruktur erfolgt über die einfach zu bedienende Prism-Central-Konsole. Für die Bereitstellung und einen sicheren Betrieb von Applikationen stehen nützliche Tools für Workflow-Automatisierung, Forecast-Analysen, Kubernetes-Container und Netzwerk-Mikrosegmentierung bereit.

Mit Nutanix Clusters on AWS bietet der Hersteller zudem die Möglichkeit, die im eigenen RZ betriebene Private Cloud zu einer Hybrid Cloud zu erweitern. Ein Vorteil dieser Lösung besteht darin, dass sich alle Nutanix-Cluster über die Prism-Central-Konsole von einer Stelle aus verwalten lassen. Die Preise für Nutanix HCI sind projektabhängig und auf Anfrage beim Hersteller und seinen Partnern erhältlich.

Christoph Lange/am



Nutanix Clusters on AWS lassen sich zur eigenen HCI-Umgebung hinzufügen, womit eine Hybrid Cloud entsteht.

Bild: Christoph Lange



digital solution days

**KOSTENLOSE
TEILNAHME**



Die digital solution days sind die virtuelle Veranstaltungsreihe von ICT CHANNEL, funkschau und Smarthouse Pro rund um die entscheidenden **Themen und Entwicklungen** der ICT-Landschaft

Ob **Professional Displays** oder **Education**, ob **Multi Cloud**, **Storage**, **Agiles IT-Management** oder **Smart Home**. Hier finden Reseller, Systemhäuser, IT-Consultants und -Dienstleister an mehreren Terminen im Jahr die perfekte Plattform, um sich mit Anbietern sowie Experten auszutauschen, sich zu vernetzen und zu informieren – hoch interaktiv und stets praxisnah.

Digital Solution Day
**CYBER
SECURITY**
23.09.2021

Digital Solution Day
**DIGITAL
WORKPLACE**
21.10.2021

ICT
CHANNEL

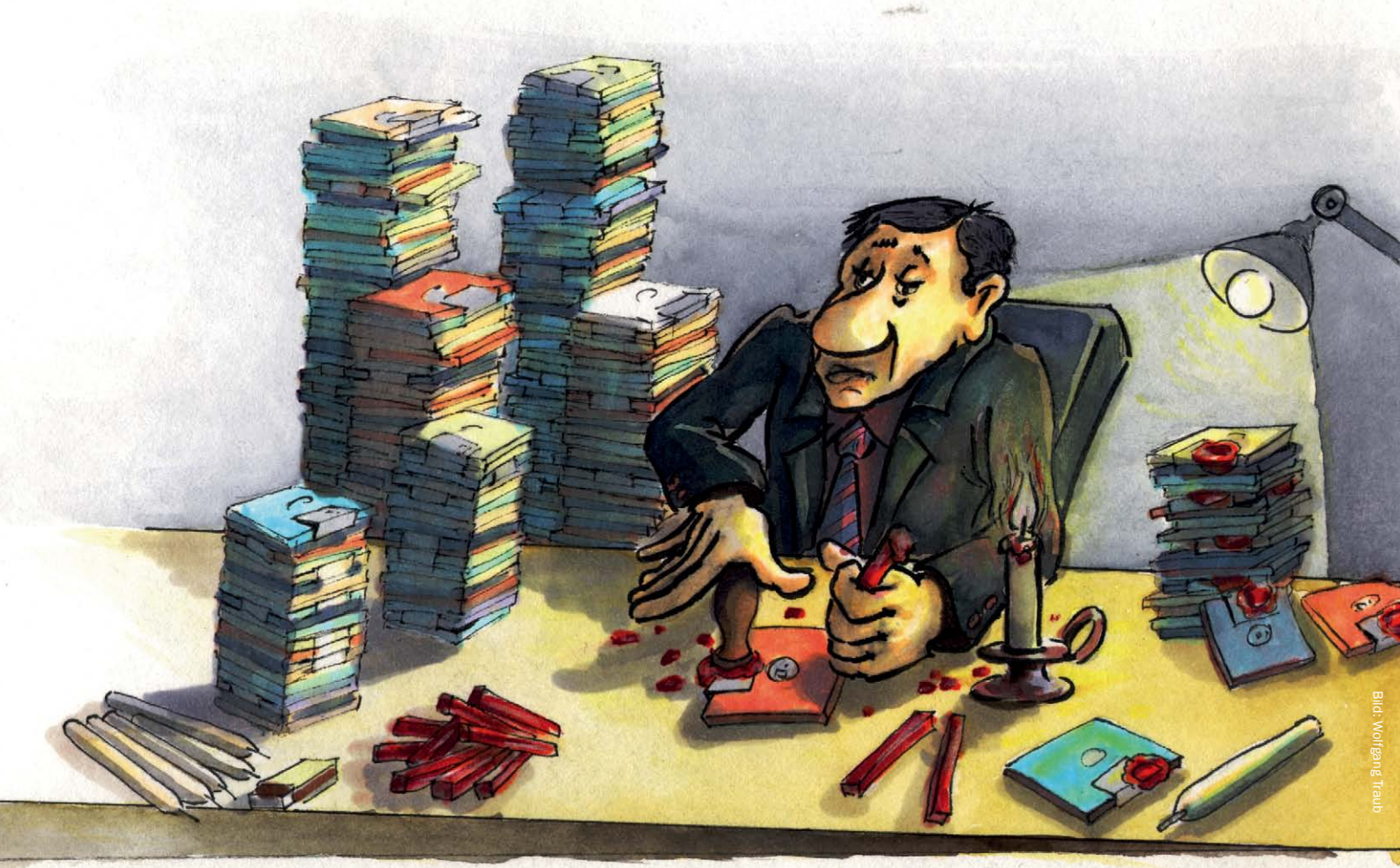
funkschau

SMARTHOUSEPRO

digitalsolutiondays.de

Backup-Herausforderungen begegnen

Versicherung für das Unternehmensgedächtnis



Bildlich gesprochen sind die Datenspeicher eines Unternehmens so etwas wie ein Gedächtnis. Und genau wie bei einem Gedächtnisverlust verlieren Unternehmen mit ihren Daten auch die Fähigkeit, sich zu orientieren und zurecht zu kommen. Mit der steigenden Relevanz von Daten sollte auch die Frage ihrer Sicherung stärker in den Vordergrund rücken. So unaufhaltsam sich die IT-Umgebung von Unternehmen verändert, so verändern sich auch die Anforderungen an die unternehmenseigene Backup- und Recovery-Strategie. Diverse Herausforderungen beeinflussen zusätzlich, wie und was Unternehmen sichern und im Ernstfall wiederherstellen müssen.

Zunächst müssen Unternehmen die Vorgaben erfüllen, die der Gesetzgeber für den Umgang mit Daten stellt. Gleich mehrere nationale und internationale Richtlinien und Gesetze regeln von der Datenverarbeitung bis hin zur Archivierung nahezu alles. Mit GDPdU (Grundsätze zum Datenzugriff und zur Prüfbarkeit digitaler Unterlagen), GoBD (Grundsätze zur ordnungsmäßigen Führung und Aufbewahrung von Büchern, Aufzeichnungen und Unterlagen in elektronischer Form sowie zum Datenzugriff) und der DSGVO (Datenschutz-Grundverordnung) seien hier nur die wichtigsten erwähnt. Zu diesen gesetzlichen

Vorgaben kommen noch die internen Compliance-Richtlinien hinzu.

Fehlende Backups von Cloud-Diensten

Leider hat sich die Fehlannahme weit verbreitet, dass die Microsoft-365-Suite, die unter anderem die beliebten Kollaborationslösungen Outlook und Teams beinhaltet, von Haus aus gesichert sei. Wenn schon Public-Cloud-Anbieter eine grundlegende „Disaster Recovery“, also die Systemwiederherstellung nach Totalausfällen bieten, bedeutet das nicht, dass sie automatisch Backups genutzter Dienste erstellen. Die Wiederherstellungszusage bezieht sich lediglich auf den Ausfall der eigenen Rechenzentren im Falle eines Hardwareversagens oder höherer Gewalt. Auf die konkreten Recovery-Anforderungen einzelner Unternehmen bieten sie per Standard keine Antwort. Die Anbieter operieren meist auf der Grundlage der geteilten Verantwortung, was heißt, dass sie die grundsätzliche Ausfallsicherheit ihrer Dienste garantieren, während der Nutzende selbst für das individuelle Backup der Dateien und Applikationen Sorge tragen muss.

Aktuelle Herausforderungen

Hybride IT-Landschaften: In vielen Unternehmen führte die Corona-Pandemie dazu, dass eine Umstellung von nahezu der gesamten Belegschaft zeitweise oder dauerhaft auf Remote Work erfolgte. Sind auch vor der Pandemie schon viele Systeme in eine Form von Public oder Private Cloud gewandert und somit in der Theorie Remote-fähig, stellte der flächendeckende Test des verteilten Arbeitens die Unternehmens-IT vor ungeahnte Herausforderungen. Angestellte, die nicht in den Büroräumen des Unternehmens arbeiten, müssen weiterhin täglich Dateien speichern, Veränderungen in Datenbanken und anderen Datenressourcen vornehmen. Somit benötigen sie weiterhin sicheren Fernzugriff auf eine Vielzahl von Unternehmensressourcen.

Mangelhafte Lösungen: Wie in jedem anderen Segment auch, sehen sich Unternehmen mit einer Unzahl an Anbietern und Lösungen konfrontiert. Nicht selten lassen sich Unternehmen von Buzzwords

oder Versprechungen einer Hochglanz-Roadmap blenden, deren Funktionen man dann doch nie umsetzt. Somit stehen sie häufig mit einer Backup- und Recovery-Lösung da, die viele ihrer Anforderungen nicht erfüllt und Lücken in ihrer Datensicherung offenlässt. Kommt es einmal zum Anwendungsfall, lassen sich Backups allzu oft nicht wiederherstellen, weil sie nicht funktionieren. Dies hätten routinemäßige Tests der Backups verhindern können. Die Nutzung der über hybride Cloud-Umgebungen verteilten Dienste und Speicher führt nicht selten dazu, dass Unternehmen gleich mehrere Backup-Lösungen im Einsatz haben. So entsteht ein Flickenteppich von Backups mit neuen Datensilos.

Fehlende Ressourcen: Viele Unternehmen sparen am falschen Ende und kündigen die Update-Verträge ihrer Backup-Anbieter. Hat man die regelmäßige Wartung und Aktualisierung des Systems lange genug vernachlässigt, kommt ein Ernstfall dem entsprechenden Unternehmen wesentlich teurer zu stehen als der Einfluss des Updatevertrags auf die Betriebskosten. Mit dem Datenwachstum und der Abhängigkeit der Unternehmen von ihrer IT steigt auch die Verantwortung und Anforderung an die IT-Abteilungen. Dies spiegelt sich zumeist nicht in den Budgets oder der Personaldecke wider. Es fehlt an Know-how und Fachleuten wie etwa Backup-Experten, aber auch an klaren Vorgaben aus den Führungsetagen.

Backup- und Recovery-Ratschläge

1. Um sowohl eine geeignete Backup- und Recovery-Strategie zu entwickeln als auch die passende Lösung auszuwählen, lautet die simple Empfehlung, einen klaren Anforderungskatalog zu erstellen. Mag dieser Rat für jede Art von IT-Ausschreibung gelten, nehmen sich im hektischen Tagesgeschäft immer noch viel zu wenige Unternehmen Zeit dafür. Doch eine vor schnell eingeführte Lösung, die sich nach kurzer Zeit als ungenügend herausstellt, strapaziert ohnehin schmale Budgets unnötig. Um die Anforderungen zu erfassen, geht es zunächst um eine Bestandsaufnahme: Wo erfolgt die Erzeugung und Spei-

cherung der Daten und wie kritisch sind die zu speichernden Daten? Aus dieser Bestandsaufnahme lassen sich die Anforderungen an die zukünftige Lösung klar ermitteln und dem Anbieter ermöglichen, ein realitätsnahes Angebot zu erstellen.

2. Backup as a Service (BaaS) ist ein vielversprechender Trend, der Backup und Recovery als Managed Service bereitstellt. BaaS erlaubt es Unternehmen, bedarfsgerecht skalierbare Backup-Kapazitäten vorzuhalten und die Kosten dafür vorausschauend zu planen. Automatisierte Backup-Tests garantieren die Integrität und Konsistenz der Backups. Auch wenn der Trend zur Cloud ungebrochen ist, erkennen die Hersteller an, dass Unternehmen auf unabsehbare Zeit in einer hybriden IT-Welt arbeiten werden. Deshalb bieten sie die wahlweise Speicherung in der Cloud, On-Premise und entsprechend der Workloads und sichern On-Premise-Daten auf Wunsch zusätzlich in der Cloud. SLAs (Service-Level-Agreements) lassen sich mit Cloud-basierten BaaS-Diensten wahrscheinlicher einhalten, etwa dank der quasi unbegrenzten Kapazität der dahinterstehenden Rechenzentren. Ausfallzeiten lassen sich minimieren und einen Großteil der Backup- und Recovery-Strategie auslagern, indem die Einhaltung rechtlicher Vorgaben durch integrierte Features vereinfacht ist.

3. (Ausnahmsweise) auf einen einzigen Anbieter setzen: Wie weiter oben geschildert, sind Unternehmen, die zwei oder mehr Backup- und Recovery-Anbieter im Einsatz haben, stärker bedroht. Dies liegt nicht zuletzt an der fehlenden Kommunikation der Lösungen untereinander. Auf der Grundlage des Anforderungskatalogs sollte die Wahl auf den Anbieter fallen, der alle Punkte bereits jetzt erfüllen kann und bestenfalls noch Raum für Entwicklung bietet. Auch wenn das Risiko eines Vendor-Lock-ins hierbei steigt, überwiegen dennoch die Vorteile einer einheitlichen Lösung.

Oliver Kolb und Marcel Teupe/am

Oliver Kolb ist Business Development Manager Commvault, und Marcel Teupe ist Sales Consultant bei ADN.

Keine Lösung von der Stange

Techniken für eine Cyber-Recovery-Strategie

Cyber Recovery ist ein wichtiger Teil der Business Continuity und dürfte wohl die einzig wirksame Versicherung für Unternehmen sein, um sich vor den Auswirkungen einer Ransomware-Attacke zu erholen. Cyber Recovery beschreibt spezielle Schutzkonzepte gegen Cyberangriffe auf Backup-Systeme, ist jedoch kein Standardprodukt, das man einfach installieren kann. Es ist Teil einer umfassenden Strategie, die mehr als nur die IT-Abteilung im Unternehmen einbezieht.

Cyber Recovery ist ein Teil der Business-Continuity-Strategie, die je nach Unternehmensgröße und Komplexität der Infrastruktur einen nicht unerheblichen Aufwand bedeutet. Diese Strategie besteht im Wesentlichen aus sechs Phasen: Planung, Teamdefinition, Informationsaufbereitung, Technikauswahl und Implementierung und vor allem Tests.

Planung: Die Planung der Cyber Recovery setzt voraus, dass die Unternehmen neben der Wichtigkeitsbewertung unterschiedlicher Abteilungen genau wissen, welche Systeme welche Priorität haben. In einer komplexen Umgebung ist bei einem Recovery-Fall nicht davon auszugehen, dass sich alle Systeme gleichzeitig wiederherstellen lassen.

Eine Priorisierung und die Abhängigkeiten der Systeme voneinander sind entscheidend, um im Notfall den Geschäftsbetrieb schrittweise wieder anzufahren – die kritischen Systeme zuerst, im Anschluss folgen alle anderen.

Cyber-Recovery-Team: Die beste Planung hilft nichts, wenn im Notfall die eine Hand nicht weiß, was die andere tut. Daher ist es wichtig, ein Team und dedizierte Verantwortlichkeiten zu definieren. Nur so lassen sich komplex aufgebaute oder verteilte Rechenzentren mit den Daten der Cyber-Recovery-Backups schnell wieder hochfahren.

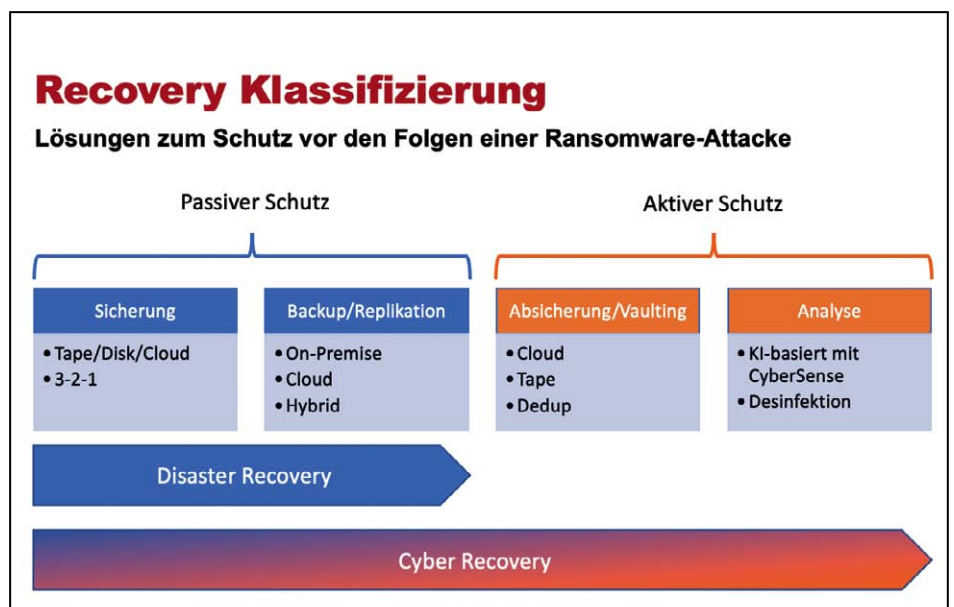
Informationen zur Infrastruktur: Entscheidend für Cyber Recovery ist das Wissen über die Infrastruktur. Welche Server, welche Datenbanken, welche Applikationen sind für das Unternehmen besonders wichtig, und vor allem: wer ist der Spezialist für diese Systeme? Sind externe Dienstleister hinzuzuziehen, weil diese bestimmte Systeme betreiben? Dazu gehören Managed-Service-Provider (MSPs) und Cloud-Anbieter ebenso wie interne Spezialisten, die beispielsweise das Indus-

trial Internet of Things (IIoT) für die Produktion im Unternehmen beherrschen.

Technikauswahl implementieren und testen: Die passende Technik für Cyber Recovery müssen Verantwortliche individuell für die IT-Struktur des Unternehmens auswählen. Ist die passende Technik implementiert, kommt ein besonders wichtiger Teil des Cyber-Recovery-Plans: das Testen. Ohne Tests können Unternehmen nicht sicherstellen, dass die eingesetzte Technik und das Team auch tatsächlich in der Lage sind, in einem Notfall die Daten und Applikationen in geplanter Zeit wiederherzustellen. Im Zweifel hat man viel Budget und Ressourcen investiert, und schlussendlich scheitert die Umsetzung an einer Kleinigkeit, die man ohne vorherige Tests leicht übersieht.

Mittel zur Realisierung

Cyber Recovery ist dann wichtig, wenn die Security-Systeme einen Ransomware-Angriff nicht abwehren oder vereiteln konnten. Gemeinhin haben die meisten Unternehmen eine gute und funktionierende Backup-Strategie, die unter normalen Umständen, beispielsweise bei einem Hardwarefehler oder beim unbeabsichtigten Löschen von Daten sehr gut hilft, die Informationen wiederherzustellen. Moderne Ransomware ist jedoch Tage und Wochen vor der eigentlichen Verschlüsselungsatta-



Klassifizierung von Disaster Recovery und Cyber Recovery.

Bild: MTI Technology

cke im Firmennetz und hat dort auch die Backups im Visier. Es ist also das primäre Ziel, die Backups vor einer Verschlüsselung zu schützen.

Eine wirksame Methode ist das Klassifizieren der Backups in den passiven Datensatz für klassisches Disaster Recovery und den aktiven Datenschutz für Cyber Recovery. Für Disaster Recovery sieht das 3-2-1-Backup-Prinzip vor, drei Kopien der Daten auf zwei unterschiedlichen Medienformaten zu speichern sowie eine Kopie extern. Die ersten beiden Kopien dienen dem schnellen Recovery, da sich diese von im Netzwerk befindlichen Speichern sehr schnell wiederherstellen lassen. Die dritte externe Kopie schützt Daten vor einer größeren Katastrophe beispielsweise einem kapitalen Brand. Jedoch befinden sich alle Kopien aktiv im Netzwerk und sind für die Ransomware erreichbar.

Erst wenn man diesem Prinzip eine weitere eins hinzufügt (3-2-1-1), die für eine zusätzliche für Ransomware unerreichbare Kopie der Daten steht, ist man auch gegen Verschlüsselung der Backups geschützt. Ab hier findet die aktive Datensicherung für Cyber Recovery statt. Dafür existieren Lösungen wie beispielsweise mit Tape, Disk oder über die Cloud.

Drei Lösungsvarianten

Bei der Tape-basierten Lösung etwa mit dem Active Vault Tresor von Quantum er-

folgt das Anlegen einer sicheren „Air Gap“-Kopie der Daten. Die Daten lassen sich innerhalb der Library in ein sicheres Archiv exportieren – die Active-Vault-Partition (AV). Diese AV-Partition bildet einen sicheren Speicherort, auf den die Ransomware nicht zugreifen kann, denn die Tapes liegen in Archiv-Slots ohne Zugriff durch die Backup-Software.

Die Variante unter Einbindung der Cloud erfordert Techniken, die vor Ransomware schützen und ein schnelles Cyber Recovery garantieren. Dies können Unternehmen beispielsweise mit CloudBoost Appliances, Data Domain und Networker von Dell realisieren. Die Daten lassen sich über Networker auf Data Domain sichern. Damit sind sie im Netzwerk noch in Reichweite der Ransomware. Der entscheidende Schritt erfolgt mit einem Storage Clone und einer CloudBoost Appliance. Die Appliance kopiert die Backup-Daten in die Cloud und dort auf einen Object Storage mit Objektsperre. Mit Hilfe von Object Lock lassen sich die Objekte mit der WORM-Methode (Write Once, Read Many) speichern. Diese Objektsperre verhindert, dass sich Objekte für einen bestimmten Zeitraum oder auf unbestimmte Zeit löschen oder überschreiben lassen. Diese Sperre dient der Einhaltung regulatorischer Anforderungen, oder um eine zusätzliche Schutzebene gegen Objektänderungen und -lösungen einzurichten, was

schlussendlich auch die Verschlüsselung durch eine Ransomware verhindert.

Die dritte Lösungsvariante, ausschließlich unter Einsatz von Disk, baut auf eine physische Unterbrechung der Speichersysteme auf. Dabei erfolgt eine automatisierte Herstellung der Netzwerkverbindung zwischen der Produktionsumgebung und der Datensicherung einmal pro Tag. Die Backup-Daten der Produktionsumgebung lassen sich innerhalb kurzer Zeit in einen ansonsten vom Netz getrennten Cyber-Recovery-Tresor schreiben und dort komplett isoliert in einen Daten-Reinraum übertragen.

Fazit

Die Herausforderung bei Cyber Recovery besteht darin, die Daten und Systeme nach ihrer Wichtigkeit für das Unternehmen zu bewerten und im Anschluss die passende Cyber-Recovery-Infrastruktur zu wählen. Auf Speicher spezialisierte Dienstleister können helfen, diesen Prozess anzustoßen, ihn mit viel Erfahrung zu durchlaufen und die individuell passende Lösung zu finden. Entscheidend dabei ist, dass der Dienstleister eine große Auswahl im Portfolio führt, denn eine „One Size Fits All“-Lösung gibt es für Cyber Recovery nicht.

Robert Meiners/am

Robert Meiners ist Business Development and Partner Manager bei MTI Technology.



KIOXIA

Next Gen Data Center NVMe™ PCIe® 4.0 SSDs



DSGVO-konforme Archivierung

E-Mail-Governance im Blick

Viele Unternehmen und zuvorderst ihre Betriebsräte und Datenschutzbeauftragten haben oft Bedenken, wenn es um die Archivierung von E-Mails geht. Schließlich sind darin personenbezogene Daten enthalten. Jedoch gibt es Aufbewahrungs- und Archivierungspflichten, an die sich Unternehmen auch im Sinn der Revisionssicherheit halten müssen. Dieser scheinbare Widerspruch lässt sich durch eine datenschutzkonforme E-Mail-Archivierungsstrategie lösen.

Mittlerweile ist die europäische Datenschutz-Grundverordnung (DSGVO) seit etwas über drei Jahren in Kraft. Dennoch herrscht vielerorts noch Unsicherheit, was die Umsetzung im eigenen Unternehmen angeht – besonders dann, wenn die Vorgaben der DSGVO scheinbar mit anderen Regularien kollidieren.

Revisionssicherheit und Datenminimierung

Grundsätzlich sind die meisten deutschen Unternehmen nach steuer- und handelsrechtlichen Vorgaben dazu verpflichtet, jedwede externe Korrespondenz, in der es um Vorbereitung, Abwicklung, Abschluss und Annullierung einer geschäftlichen Aktivität geht, für einen bestimmten Zeitraum aufzubewahren. Darunter fallen beispielsweise Rechnungen, Verträge, Zahlungsbelege sowie Auftrags- und Reklamationschreiben. Die Aufbewahrungspflicht gilt auch dann, wenn die Inhalte in elektronischer Form, wie also zum Beispiel als E-Mail, vorliegen.

Diese Archivierungsvorgaben sind für Unternehmen in Deutschland in den sogenannten Grundsätzen zur ordnungsmäßigen Führung und Aufbewahrung von Büchern, Aufzeichnungen und Unterlagen in elektronischer Form sowie zum Datenzugriff (GoBD) geregelt. In Österreich und

der Schweiz gibt es vergleichbare Anforderungen. Diese Vorgaben gelten prinzipiell für alle Daten, die für die Besteuerung relevant sind. Dies umfasst unter anderem folgende Bereiche:

- Bücher und Aufzeichnungen, Inventare, Jahresabschlüsse, Lageberichte, die Eröffnungsbilanz sowie die zu ihrem Verständnis erforderlichen Arbeitsanweisungen und sonstigen Organisationsunterlagen,
- die empfangenen Handels- oder Geschäftsbriefe,
- Wiedergaben der abgesandten Handels- oder Geschäftsbriefe,
- Buchungsbelege und
- sonstige Unterlagen, soweit sie für die Besteuerung von Bedeutung sind.

Dadurch entsteht ein hohes Aufkommen an Daten, die Unternehmen revisionssicher archivieren sollten. Demgegenüber steht der Datenschutzgrundsatz der Datenminimierung, der besagt, dass man personenbezogene Daten nur in dem Umfang und für die Dauer erheben darf, wie sie auch zur Erreichung des jeweiligen Zwecks gebraucht sind. Einfach auf Verdacht alle E-Mails dauerhaft zu speichern, ist dementsprechend keine Lösung und auch nicht rechtskonform. Die Löschung von E-Mails sollte gemäß der Datenschutz-Grundverordnung nach Ablauf spezifi-

scher Fristen oder auf Wunsch betroffener Personen erfolgen. Hier zeigt sich schon, dass Systeme für Backup und Datensicherung den komplexen Anforderungen nicht gerecht werden können, da diese nicht für die revisionssichere und datenschutzkonforme Speicherung von – in diesem Fall – E-Mails konzipiert sind.

Was eine E-Mail-Archivierungslösung leisten muss

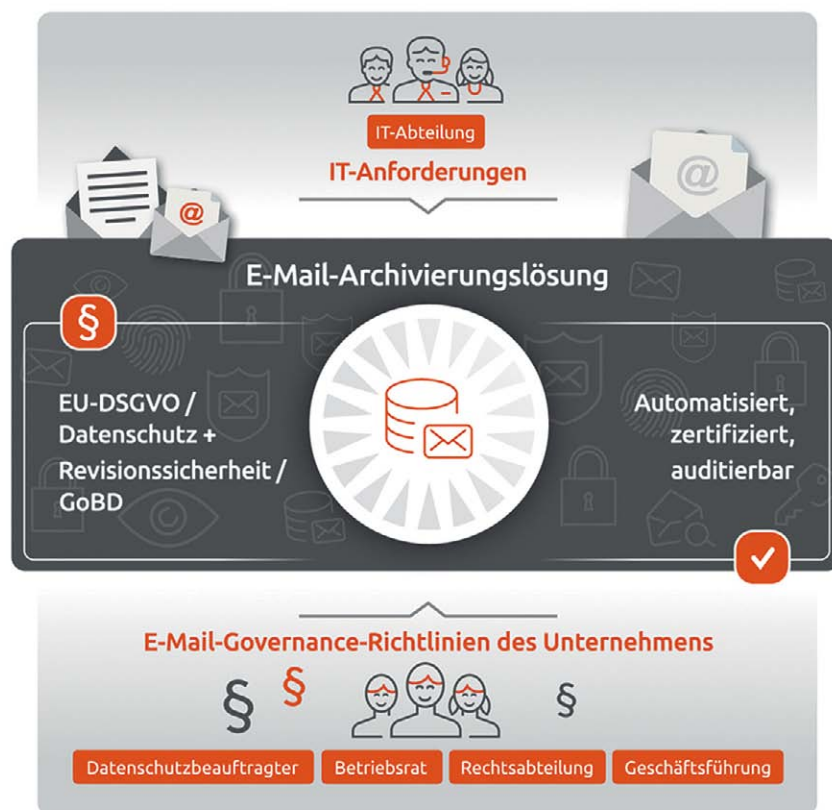
Es gibt eine Reihe von Vorgaben, die eine rechtssichere Archivierungslösung unter anderem erfüllen sollte:

- Vollständigkeit der relevanten Dokumente (E-Mails und Dateianhänge),
- Unveränderbarkeit und Schutz vor Manipulation,
- nachvollziehbare Aufbewahrungsrichtlinien,
- Protokollierung von Änderungen (Audit Log),
- Exportmöglichkeiten in Standardformate (etwa EML, MSG und PST) sowie
- Zugriffsmöglichkeiten für externe Auditoren (zum Beispiel Betriebsprüfer).

Die meisten dieser Anforderungen sind durch die Revisionssicherheit getrieben. Das heißt, die Lösung und der von ihr verwaltete Datenbestand sollten einerseits einer Prüfung durch das Finanzamt standhalten. Auf der anderen Seite unterstützen bestimmte Funktionen einer professionellen E-Mail-Archivierung die Compliance hinsichtlich der DSGVO-Vorgaben. Nach Artikel 15 haben betroffene Personen beispielsweise ein Auskunftsrecht über ihre durch das entsprechende Unternehmen gespeicherten personenbezogenen Daten.

Um dem nachzukommen, sollten Unternehmen, so trivial das auch klingen mag, zunächst selbst wissen, welche Daten über die betreffende Person gespeichert sind. Außerdem müssen diese Daten bei Bedarf zeitnah auffindbar und exportierbar sein. Eine gute E-Mail-Archivierung bietet daher eine volle Durchsuchbarkeit des E-Mail-Archivs auf Unternehmensebene und Exportmöglichkeiten in Standardformate. Die gleichen Mechanismen unterstützen die Einhaltung weiterer DSGVO-Vorgaben wie das Recht auf Löschung (Artikel 17 DSGVO) oder das Recht auf Daten-

Spannungsfeld E-Mail-Archivierung in Unternehmen



Eine E-Mail-Archivierungslösung kann die Anforderungen der IT und die Governance-Richtlinien des Unternehmens vereinen.

Bild: MailStore

übertragbarkeit (Artikel 20 DSGVO). Weiterhin empfiehlt es sich, dass das Unternehmen die jeweilige Rechtsgrundlage berücksichtigt, bevor es personenbezogene Daten speichert und diese im nächsten Schritt verarbeitet.

Worauf Unternehmen bei der Implementierung achten sollten

Unternehmen, die nach einer E-Mail-Archivierungslösung suchen und Bedenken hinsichtlich der Datenschutzkonformität haben, können sich zunächst an Zertifizierungen unabhängiger Stellen orientieren. Obwohl es bislang noch keine explizite DSGVO-Zertifizierung der EU oder einer anderen offiziellen Stelle gibt, sind unabhängige Prüfungen durch Datenschutzexperten eine Hilfe, um IT-Entscheidern und Datenschutzbeauftragten bei der Auswahl einer entsprechenden Lösung zusätzliche

Sicherheit zu verleihen. Entsprechende Nachweise und Prüfberichte sollten auf Anfrage von Herstellern beziehungsweise IT-Systemhäusern zu erhalten sein.

Praxistipp: Häufig gibt es Bedenken von Seiten des Datenschutzbeauftragten oder des Betriebsrats. Daher sollten IT-Verantwortliche die Datenschutzbeauftragten und den Betriebsrat entsprechend frühzeitig als relevante Stakeholder bei der Auswahl einer E-Mail-Archivierungslösung involvieren.

Bevor es an die Umsetzung einer E-Mail-Archivierungslösung auf technischer Ebene geht, gilt es, vorab interne Rahmenbedingungen abteilungsübergreifend zu definieren und zu dokumentieren. Darin kann beispielsweise das Verbot privater E-Mail-Korrespondenz über die vom Unternehmen bereitgestellten E-Mail-Konten

können Unternehmen zudem gesondert behandeln, beispielsweise wenn darüber die Kommunikation der HR-Abteilung mit Bewerbern oder zwischen dem Betriebsarzt und den Beschäftigten läuft. Bei der Ausgestaltung solcher internen Richtlinien ist es ratsam, unbedingt die Rechtsabteilung miteinzubeziehen und diese Richtlinien schriftlich festzuhalten. Ihre Einhaltung sollte darüber hinaus einer regelmäßigen Überprüfung unterlaufen.

Schaut man nun auf die technische Ebene der Lösung, die vor allem die IT-Abteilung betrifft, geht es auch darum, welche Möglichkeiten ein Tool für die Definition von Aufbewahrungsrichtlinien bietet. Insbesondere sollten Aufbewahrungsrichtlinien GoBD-konform definiert sein und gleichzeitig die Anforderungen aus der Datenschutzgrundverordnung unterstützen. Beispielsweise lässt sich über solche Richtlinien eine Mindestaufbewahrungsdauer definieren. Nach Ablauf dieser Frist kann entweder auf direktem Wege eine automatisierte Löschung erfolgen, oder der berechtigte Administrator löscht E-Mails manuell auf Basis unternehmensinterner Vorgaben.

Fazit

Der Datenschutz und die revisionssichere Archivierung von E-Mails müssen keinen Widerspruch bedeuten. Richtig aufgesetzt können leistungsfähige Archivierungslösungen die Einhaltung der DSGVO-Anforderungen an das E-Mail-Management unterstützen.

Leistungsstarke Such- und Exportfunktionen sorgen dafür, dass Unternehmen geforderte Daten schnell und unkompliziert finden und zum Beispiel betroffenen Personen, Auditoren etc. unverzüglich zur Verfügung stellen können. Backup-Lösungen sind für diesen Einsatzzweck nicht gedacht. Für Unternehmen sind die E-Mail-Archivierung und das Backup sich ergänzende Aspekte und sollten stets zusammen im Einsatz sein, da auch Archive von Systemausfällen betroffen sein können.

Roland Latzel/am

Roland Latzel ist Director of Marketing bei MailStore Software.

BaaS, RaaS & DRaaS

Datensicherungsdienste für MSPs

Außen simpel, innen komplex – so lässt sich der Trend der vergangenen Jahre in der Enterprise-IT auf den Punkt bringen. Was die Endanwender in Unternehmen im Alltag zu sehen bekommen und nutzen, ist grundsätzlich nur ein Bruchteil dessen, was die dahinterliegende Infrastruktur ausmacht.

Diese Infrastruktur ist gekennzeichnet von zunehmend vielschichtigen Technik-Stacks, aufbauend auf Virtualisierung, Cloud Computing und Storage- sowie Security-Layern. Hinzu kommen noch On-Premise-Hardware und Legacy-Anwen-

dungen. Für Managed-Service-Provider (MSPs) ist diese Entwicklung ein Segen. MSPs können Unternehmen helfen, die wachsende Komplexität der IT zu planen, verlässlich zu betreiben und den hausinternen IT-Abteilungen bisweilen lästige Rou-

tineaufgaben abnehmen. Eine essenzielle Aufgabe dieser Art ist das Daten-Management und hier besonders die Datensicherung. Groß angelegte Cyberangriffe sind nur die prominentesten Bedrohungen. Im Alltag geht es zunehmend auch um die Sicherung von Produktivität und den Schutz vor allzu menschlicher Vergesslichkeit und Unachtsamkeit.

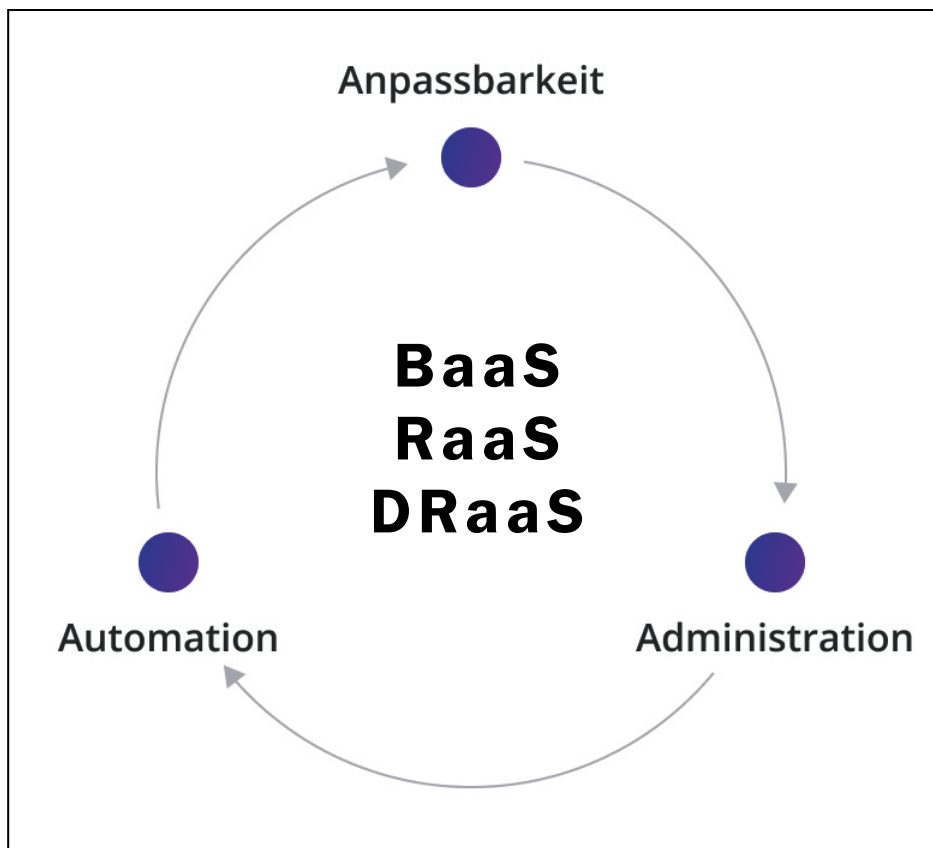
Für MSPs steckt in Backup, Replication und Disaster Recovery as a Service (BaaS, RaaS und DRaaS) viel Potenzial, zumal sich sehr viele Standardprozesse der Datensicherung automatisieren lassen. Mit dem Grundgedanken der „Versicherung“ gegen Datenverlust und Produktivitätseinbrüche lässt sich Datensicherung als Dienstleistung recht einfach verkaufen. Damit sich BaaS, RaaS und DRaaS aber auch in großem Maßstab profitabel betreiben lassen, muss sich ein Managed-Service-Provider über eine Vielzahl von Faktoren im Klaren sein, die Einfluss auf den wirtschaftlichen Betrieb einer Datensicherungslösung in Multi-Tenant-Umgebungen haben. Man sollte sich des Umstands bewusst sein, dass die namhafteste Lösung dabei nicht zwangsläufig die Beste sein muss.

Handreichung für die Tool-Auswahl

Bei der Tool-Auswahl hilft eine kleine Eselsbrücke aus den drei „A“: Anpassungsfähigkeit, Administration und Automatisierung sowie aus den zugehörigen Checklistenfragen.

Anpassungsfähigkeit: Die IT-Infrastruktur der Unternehmen gibt weitgehend vor, was die BaaS-Lösung können muss. Entsprechend flexibel und vielfältig einsetzbar sollte die zum Einsatz kommende Software sein. Zum Start der Evaluation ist die Frage nach der Betriebsumgebung relevant: Lässt sich die Software für virtuelle Server mit Microsoft Hyper-V oder VMware vSphere genauso einsetzen, wie für physische Server in einer On-Premise-Welt? Außerdem sollte man der Frage nachgehen, wie die Lösung mit Microsoft 365 und Azure zurechtkommt und wie mit AWS und Google Cloud.

Ein weiterer Punkt ist das Betriebssystem, auf dem die IT-Infrastruktur laufen soll.



Anpassbarkeit, Administration und Automation ergeben zusammen eine wirtschaftliche Lösung für MSPs.

Bild: Nakivo

Windows-Server und Linux-Maschinen stellen einen Standard dar, aber auch AWS Linux AMI oder der Einsatz auf Virtual Appliances sind möglich. Und schließlich haben auch die zu sichernden Anwendungen einen Einfluss auf den geforderten Funktionsumfang. Angesichts der eingangs beschriebenen zunehmenden Komplexität von IT-Infrastrukturen mit immer häufiger einem hybriden Cloud/On-Premise/Virtual-Charakter lohnt dort ein besonders genauer Blick auf die Anbieter und ihre Fähigkeit, eng an neuen Entwicklungen zu bleiben. Ist sie beispielsweise in der Lage, Microsoft-365-Instanzen sowie deren Unteranwendungen wie Exchange, Teams, SharePoint und OneDrive zu sichern und feingranular bis auf Objektebene im Self-Service wiederherzustellen? Ebenso sind Anhaltspunkte zu infrastrukturelevanten Anwendungen wie dem VMware Cloud Director von Bedeutung. Für die Feature-basierte Evaluation der verfügbaren Backup-und-Recovery-Lösungen empfiehlt sich die Entwicklung eines detaillierten Pflichtenhefts. Mit seiner Hilfe können MSPs Featuresets vergleichen und die Funktionen entsprechend ihres anvisierten Kundenklientels gewichten.

Administration: Für MSPs zählen neben der Kernfunktionalität einer Backup- und Recovery-Lösung noch weitere administrative Faktoren. Mehrmandantenfähigkeit (Multi-Tenancy) gehört hier ganz oben auf die Liste. Denn schließlich wollen MSPs für möglichst viele Unternehmen eine gemeinsame Infrastruktur bereitstellen, die dann den jeweiligen Service-Levels entsprechend und sicher separiert den Anwenderunternehmen zur Verfügung stehen kann.

Da nicht jedes Unternehmen die gleichen Anforderungen an Datensicherungskapazitäten hat, hilft eine Funktion zur Ressourcenallokation bei der effizienten Administration von Multi-Tenant-Instanzen. Administrationsteams sollten den Mandanten spezifische Hosts, Cluster, Virtual Machines, Backup Repositories und Transporter zuweisen sowie eine rollenbasierte Zugriffskontrolle und Rechte im Self-Service-Portal implementieren können. Ein regelmäßig vorkommendes Ärgernis für

die Remote-Administration durch MSPs ist die Notwendigkeit, für die Verbindung zu den hauseigenen Systemen der Mandanten VPN-Verbindungen konfigurieren und unterhalten zu müssen. Funktioniert das VPN aus welchem Grund auch immer nicht, leidet die Service-Qualität, weil sich beispielsweise Item-Level-Recovery-Aufgaben unnötig verzögern. Dann können alternative Verbindungen, wie zum Beispiel „Direct Connect for MSPs“ aus dem Hause Nakivo, helfen, die ohne ein VPN auskommen und über einen definierten Port eine durch ein Verschlüsselungszertifikat abgesicherte Direktverbindung schaffen. Ein oft wenig beachteter Aspekt der Administration von Backup-Angeboten ist das Lizenz-Management und die damit einhergehenden Kosten. Dabei kann es gerade im Managed-Services-Umfeld den Unterschied zwischen angemessener Gewinnmarge der Services und Verlustgeschäft ausmachen. Schließlich liegt es in der Natur moderner IT-Infrastrukturen, dass sie sehr schnell und sehr dynamisch wachsen und schrumpfen können. Das Lizenzmodell des Softwareanbieters sollte diese Dynamik mitgehen und sich flexibel an die Auftragslage anpassen können. Bei Microsoft-365-Backups beispielsweise sind Pro-User-Lizenzen üblich, für Server- oder VM-Backups erfolgt die Abrechnung häufig in CPU-Sockets oder in Workloads. Damit ein MSP Softwarelizenzen flexibel an seine Kunden vergeben kann, bietet sich ein „Licence Pooling and Delegation“-System an. Dieses stellt sicher, dass die Kosten für die Lizenzierungseinheiten berechenbar bleiben, während man die Lizenzen selbst nach Bedarf unkompliziert an neue oder expandierende Kunden vergeben kann.

Automatisierung: Fachwissen ist stets begrenzt, doch das MSP-Geschäft soll skalieren – der Schlüssel zum profitablen Betrieb von Backup- und Recovery-Services liegt schon deshalb auch im dritten Erfolgsfaktor, der Automatisierung. Ihre Aufgabe: Administratoren nach dem Prinzip „Set and Forget“ von wiederkehrenden Routinejobs zu befreien und dabei die Datensicherung so verlässlich wie möglich sicherzustellen. Automatisierung beginnt

bei der Datenklassifizierung, die Teil jeder Backup-Strategie sein sollte. Stunden- oder gar minutenaktuelle Produktionsdaten benötigen dicht getaktete RPOs (Recovery Point Objective), archivierungspflichtige Altdaten nicht.

Manche Datenbanken ändern sich ständig, manche Exchange-Instanzen nur ab und zu. Wenn die Backup-Software eine Konfiguration von Backup-Plänen nach Anwendungs- oder Dateityp und nach Filterkriterien wie „zuletzt geändert vor ... Minuten“ erlaubt, ist schon die Basis gelegt. Die klassifizierten Daten fließen dann in passende Zeitpläne, die die nach MSP-Service-Level gebuchten RPOs und RTOs (Recovery Time Objective) abbilden. Was einmal läuft, muss ein Administrator so schnell nicht mehr anfassen. Läuft das Backup, ist die regelmäßige Prüfung der tatsächlichen Wiederherstellbarkeit der Backups ein weiteres Einsatzgebiet für die Automatisierung.

Fazit

Oberflächlich betrachtet mögen Backup und Replikation eher zu den Standarddienstleistungen von Managed-Service-Providern gehören. Doch sollte dieser Überblick zu einer systematischen, bedarfsorientierten und an Administratorproduktivität und Wirtschaftlichkeit ausgerichteten Auswahl einer MSP-fähigen Software gezeigt haben, dass es sich lohnt, ins Detail zu gehen. Denn ist eine Lösung erst einmal im Einsatz, sind Kurskorrekturen nur mit erheblichem Aufwand umzusetzen.

Gerade weil Datensicherung eine unverzichtbare Standardanwendung ist, für die Anwenderunternehmen jedoch aus eben dem Commodity-Argument heraus besonders preissensibel sind, ist das 3-A-Prinzip für die Softwareauswahl zu guter Letzt auf die Wirtschaftlichkeit ausgerichtet. Hier verhält es sich am Ende wie so häufig im IT-Geschäft: Die ideale Lösung, die alle erforderlichen Kriterien erfüllt, gibt es nicht. Wohl aber gibt es eine bestmögliche.

Sergei Serdyuk/am

Sergei Serdyuk ist Vice President of Product Management bei Nakivo.

Datensicherung für SaaS-Angebote

„One Size Fits All“ oder „Case by Case“?

Unternehmen müssen dafür sorgen, dass ihre kritischen Anwendungen nicht anfällig für Datenverluste sind. Doch es gibt einiges zu beachten, wenn es darum geht, Unternehmensdaten in Office 365 und anderen SaaS-Anwendungen zu sichern.

Während der COVID-19-Pandemie gab es ein immenses Wachstum bei der Nutzung von SaaS-basierten Diensten wie Office 365. Dies hat Unternehmen nicht nur dazu veranlasst, ihre Cloud-Strategie zu überdenken, sondern auch die Sicherheit der Daten, sobald sie sich in der Cloud befinden. Ransomware-Angriffe und Phishing-Versuche nahmen erheblich zu – in einer Zeit der allgegenwärtigen Verunsicherung. Oft nutzen die Angreifer E-Mails als Angriffsvektor, um sich Zugang zu eigentlich sicheren Daten zu verschaffen. Google Cloud berichtete über 18 Millionen Malware- und Phishing-E-Mails im Zusammenhang mit COVID-19 innerhalb von nur einer Woche.

Wenn neue SaaS-Anwendungen zum Einsatz kommen, sollten Unternehmen eine Strategie haben, um die damit verbundenen nativen Cloud-Daten zu schützen und das Risiko eines Datenverlusts zu mindern. Eine häufig übersehene Herausforderung ist dabei die Verwaltung des „Shared Responsibility“-Modells, also der geteilten Verantwortung bei der Cloud-Nutzung. So ist beispielsweise Microsoft für die Aufrechterhaltung der Betriebszeit seiner Infrastruktur verantwortlich. Für den Schutz der Anwendungsdaten und die Wiederherstellung im Bedarfsfall liegt die Verantwortung jedoch beim Anwenderunternehmen. Eine Studie von Veritas gibt jedoch zu bedenken, dass 76 Prozent der Verantwortlichen in den Unternehmen davon ausgehen, dass die Verantwortung für Compliance und Datenschutz vollständig beim

Cloud-Betreiber liegt. Ein weiterer wichtiger Aspekt ist die Data Governance. In vielen Branchen gibt es spezifische Vorgaben zu Datenschutz und Datensicherheit, die ein Dienst wie Office 365 nicht automatisch umsetzen kann. Mit der massiven Verlagerung zu Telearbeit in Kombination mit zunehmenden Cyberangriffen ist der Schutz von Daten zu einer entscheidenden Herausforderung geworden.

Backup-Management in der Cloud

Entscheidend für die Datensicherung in der Cloud ist die „Ease of Operation“, also die Einfachheit der Umsetzung. Ein gängiges, aber sicherheitstechnisch anspruchsvolles Verfahren ist die Sicherung von der Cloud in die Cloud. Es ist nicht so einfach, verschiedene Geolokationen als Speicherziele festzulegen, ohne dass dabei eine Sicherung aus der Cloud heraus erfolgt, denn sonst entsteht ein Bruch. Für das Backup-Management ist es nicht praktikabel, auf Insellösungen zu setzen. Die meisten Unternehmen wollen keine Tools nutzen, die jeweils nur für eine Umgebung funktionieren, also etwa nur für Datenbanken oder Dateispeicherung. Dieser Ansatz kann schnell sehr komplex sein, vor allem wenn die Cloud als Komponente dazukommt. Langfristig praktikabel sind hochgradig automatisierte Ansätze, die On-Premise, Office 365, Multi-Cloud etc. mit einem Tool auf einer Plattform nutzbar machen. Office 365 in seiner nativen Form ist beispielsweise für die Archivierung eher rudi-

mentär aufgestellt. So sind nicht viele Funktionen für diesen Zweck verfügbar. Eine Frage – vor dem Hintergrund verschärfter Datenschutzbestimmungen wie durch die DSGVO – ist, was mit Backup-Daten geschieht. So soll etwa das „Recht auf Vergessenwerden“ gewährleisten, dass persönliche digitale Daten nicht dauerhaft zur Verfügung stehen. Bei Office 365 findet diese Frage so gut wie gar keine Berücksichtigung. Microsoft delegiert hier viel Verantwortung an seine Nutzenden. Diese müssen sich umfassend informieren und vorbereiten, um all ihrer Verantwortung gerecht zu werden.

Für die Datensicherung in Office 365 und anderen SaaS-Angeboten gibt es keine klare Antwort auf die Frage „Case by Case“ oder „One Size Fits All“. Die Wahrheit liegt wie so oft irgendwo dazwischen. Die Datensicherung in Office 365 und bei SaaS generell sollte dabei aber jedenfalls an drei Merkmalen ausgerichtet sein:

Automatisierung: Angesichts einer wachsenden Komplexität vieler IT-Umgebungen und dem nicht nachlassenden Mangel an IT-Fachleuten ist eine weitreichende Automatisierung nahezu unerlässlich. Ein effizienter Automatisierungsplan erfordert einen Restful-API-Ansatz. Dabei ist es gleichgültig, ob PowerShell, Curl oder Python zum Einsatz kommt, denn sie alle nutzen die gleichen Aufrufe für die gleichen Aufgaben.

Simplifizierung: Schon die Implementierung einer entsprechenden Lösung sollte einfach sein, um beim Umstieg keine Verzögerungen oder Fehler zu verursachen. So sollte es beispielsweise ein Auto-Discovery aller Mailboxen und aller Datenbanken geben, das mittels SLAs die täglichen Backup-Jobs steuert.

Orchestrierung: Diese ist das oberste Gebot bei der Einführung von Backup-Lösungen. Es muss die Gestaltung logischer Abläufe erfolgen, die eine sinnvolle Reihenfolge bei der Wiederherstellung großer Datenmengen sicherstellt.

Am einfachsten und auch praktikabelsten sind Lösungen, die SLA-basiertes Backup und Recovery für Office 365 ermöglichen. SLA-basierte Konzepte erlauben unterschiedliche Maßgaben für unterschiedli-

che Mitarbeitergruppen – und dies über Cloud und On-Premise hinweg. SLA-basiertes Gruppen-Management, also auch von Office-365-Nutzenden, ist ebenso wichtig und praktisch wie eine automatisierte Backup-Verschlüsselung bei Office 365. Anderenfalls haben Unternehmen bei einem erfolgreichen Angriff auf die Cloud schlechte Karten, wenn Kriminelle beispielsweise das Backup verschlüsseln.

Eine moderne Cloud-fähige Backup-Lösung baut auf nativen Tools der Cloud-Betreiber mit eingebauter Backup- und Recovery-Automatisierung auf. So lassen sich der Schutz vor Datenverlusten und eine optimierte Verwaltung von SaaS-Anwendungen gewährleisten. Eine zentralisierte Verwaltung ermöglicht konsistente, SaaS-basierte Backups im Falle von Microsoft für Exchange Online, OneDrive, SharePoint und Teams über ein einziges, intuitives Dashboard. Problemlose Offline-Backups sorgen dafür, dass wichtige Daten sicher, leicht auffindbar und immer zu-

gänglich sind. Einzelne E-Mails oder ganze OneDrive-Ordner lassen sich mit nur drei Klicks an jedem beliebigen Ziel wiederherstellen. Granulare Wiederherstellung an jedem beliebigen Zielort und das einfache Auffinden von Daten mit globaler Echtzeitsuche sind entscheidend, um Datenverluste zu vermeiden und Ausfallzeiten zu minimieren. Benutzende können Daten auf Dateiebene finden, um Datenverluste schnell zu beheben und die Geschäftskontinuität sicherzustellen.

Das automatisierte Management im großen Maßstab sorgt dafür, dass Unternehmen manuelle Prozesse rationalisieren und automatisieren können. Durch Automatisierung entfällt die manuelle Job-Planung, während sich die Richtlinienverwaltung für Zehntausende von Anwendern optimieren lässt. Die automatische Skalierung von Ressourcen ermöglicht einen nahtlosen Betrieb im großen Maßstab. Management und Reporting lassen sich über On-Premise und die Cloud hinweg mit einer einzi-

gen Softwareplattform zentralisieren. Eine automatisierte Richtlinienzuweisung mit einer leistungsstarken SLA-Engine ermöglicht die Einhaltung zuvor festgelegter RPOs (Recovery Point Objectives) für große SaaS-Umgebungen.

Sicheres Daten-Handling

Die SaaS-Datensicherung muss keinen weiteren komplizierten Management-Aufwand oder zusätzliche Komplexität bedeuten. Im Gegenteil: Mit einer modernen Backup-Lösung für SaaS-Daten ergeben sich vielmehr entscheidende Vorteile, um den Verwaltungsaufwand zu verringern. Der Einsatz einer modernen Cloud-fähigen Daten-Management-Plattform gibt Unternehmen somit die Gewissheit, dass ihre kritischen Daten sicher, vorschriftsmäßig gespeichert und jederzeit zugänglich sind.

Achim Freyer/am

Achim Freyer ist Regional Director Central and Eastern Europe bei Rubrik.

ONE STULZ. ONE SOURCE.



STULZ steht für Klimatechnologien auf höchstem Niveau.

Ob maßgeschneidert oder standardisiert, ob Rechenzentrum oder Industrieanwendung, ob Kaltwassersatz oder Software; vertrauen Sie auf STULZ für Ihr betriebssicheres Klima.

STULZ – alles aus einer Hand.

www.stulz.de

Pure Storage: FlashStack im As-a-Service-Angebot

Flexible Modernisierung der IT

Pure Storage hat den weiteren Ausbau seines Abonnement-Service-Portfolios bekanntgegeben. Mit FlashStack, das jetzt als Service bereitsteht, sollen Unternehmen die KI-basierte Infrastruktur von Pure Storage und Cisco mit einem flexiblen IT-Verbrauchs- und Nutzungsmodell verwenden können. Für Anwendungen, die auf Kubernetes laufen, berechne Portworx Cloud Consumption Kosten nach den tatsächlichen Nutzungsstunden. FlashStack von Pure Storage und Cisco ist eine KI-basierte und softwaredefinierte Dateninfrastruktur, die On-Premise- und Multi-Cloud-Landschaften integriert. Einzeln skalierbar und ganzheitlich verwaltet, bie-

tet FlashStack eine Komplettlösung für kritische Anwendungen, die immer betriebsbereit und zukunftssicher ist, so das Versprechen. Mit vorab getesteten, validierten Referenzarchitekturen für gängige Workloads sollen Unternehmen den Zeitaufwand und das Risiko für die Bereitstellung und Verwaltung reduzieren können. Durch die Bereitstellung eines modernen Betriebsmodells helfe FlashStack Unternehmen, den geschäftlichen Anforderungen voraus zu sein und Anwendungen und Daten vor Ort, am Edge oder in der Cloud zu sichern. Portworx ermögliche es Anwendenden, ihre Enterprise-Anwendungen in jeder Cloud und jedem Rechen-

zentrum mit der gewohnten Performance, Sicherheit und Datensicherheit zu betreiben und konsistent zu skalieren. Da Cloud-native Anwendungen, die auf Kubernetes laufen, sehr dynamisch sind, ist die Abschätzung der genauen Anzahl von Servern, die für den Betrieb von Anwendungen auf Kubernetes nötig sind, eine große Herausforderung, die zu einer Überbereitstellung und höheren Kosten führt, so der Hinweis von Pure Storage. Um diese Herausforderung zu lösen, führt Portworx ein flexibles Modell ein, das es Anwenderunternehmen laut Pure Storage ermöglicht, den Verbrauch von Portworx an die Auf- und Abskalierung ihrer Anwendun-

gen anzupassen. Bisher kauften Unternehmen eine oder mehrere Jahreslizenzen von Portworx, die sich jeweils auf einem einzelnen Server betreiben ließen. Wenn sie jedoch über die Anzahl der erworbenen Lizenzen hinaus skalieren wollten, mussten sie den Vertrieb kontaktieren, um zusätzliche Lizenzen zu erwerben. Mit der neuen flexiblen Preisgestaltung erwerben Anwender eine Anzahl von Stunden, anstatt eine Lizenz, die an einen einzelnen Server gebunden ist. Diese Stunden können Anwenderunternehmen über das Jahr hinweg in beliebigem Umfang verbrauchen, je nachdem, wie viele Server nötig sind, so die abschließende Anbieterangabe. am

Marktübersicht: Backup-Lösungen

Hersteller/Anbieter	Web
Acronis	www.acronis.com
Arcserve	www.arcserve.com
Ashampoo	www.ashampoo.com
AWS	www.aws.amazon.com
Barracuda Networks	www.barracuda.com
Carbonite	www.carbonite.com
Cohesity	www.cohesity.com
Commvault	www.commvault.com
Dell Technologies	www.delltechnologies.com
Fujitsu	www.fujitsu.com
GCP	cloud.google.com
HPE	www.hpe.com
HYCU	www.hycu.com
IBM	www.ibm.com/de-de
Ionos	www.ionos.de
Langmeier	www.langmeier-software.com
MailStore	ww.mailstore.com
Microsoft Azure	www.azure.microsoft.com
MTI Technology	de.mti.com
Nakivo	www.nakivo.com

Hersteller/Anbieter	Web
NetApp	www.netapp.com
Netgear	www.netgear.com
NovaStor	www.novastor.de
Nutanix	www.nutanix.com
Oracle	www.oracle.com
Pure Storage	www.purestorage.com
Qnap	www.qnap.com
Quantum	www.quantum.com
Rubrik	www.rubrik.com
SEP	www.sepsoftware.com
SoftwareOne	www.softwareone.com
Starline	www.starline.de
Strato	www.strato.de
Synology	www.synology.com
Unitrends	www.unitrends.com
Veeam	www.veeam.com
Veritas	www.veritas.com
Wasabi	www.wasabi.com
Waxar	www.waxar.eu
Zerto	www.zerto.com

Thomas-Krenn bietet Cloud-Dienste an Vor-Ort-Server flexibel ergänzen

Der Server-Hersteller Thomas-Krenn bietet ab sofort auch Cloud-Dienste an. Die „Thomas-Krenn-Cloud“ kombiniere IaaS- und PaaS-Angebote (Infrastructure und Platform as a Service) mit ausgewählten Cloud-basierten Applikationen. Zielgruppe sind mittelständische Unternehmen oder IT-Dienstleister, die ihre Server vor Ort kurzfristig oder perma-

nent durch ein beliebig skalierbares virtuelles Datacenter ergänzen wollen. Laut Hersteller verbindet die Cloud einfache Administrierbarkeit über ein intuitives Web-Interface mit hoher Flexibilität. So sollen Hardwareprofile bei virtuellen Servern für bestmögliche Performance und Kompatibilität zu bestehenden Applikationen sorgen. Beim Storage seien

drei Speed-Klassen bis hin zu fünffacher SSD-Geschwindigkeit möglich. Neben virtuellen Servern, Storage und Netzwerken sind Datenbank-Dienste (Microsoft SQL Server, PostgreSQL, MySQL/MariaDB) und die Key Value Stores Redis und Memcached als PaaS verfügbar, so die weitere Angabe. Als schlüsselfertige Applikationen bietet Thomas-Krenn un-

ter anderem das Video-Konferenzsystem Jitsi, die Datei-Synchronisations-Plattformen Nextcloud und Cloudplan oder das Mailarchiv Benno an.

Die Cloud basiert auf der Plattform des Kölner Unternehmens Gridscale. Die Dienste seien in Hochleistungsrechenzentren an zwei verschiedenen Standorten in Deutschland gehostet, so Thomas-Krenn. am

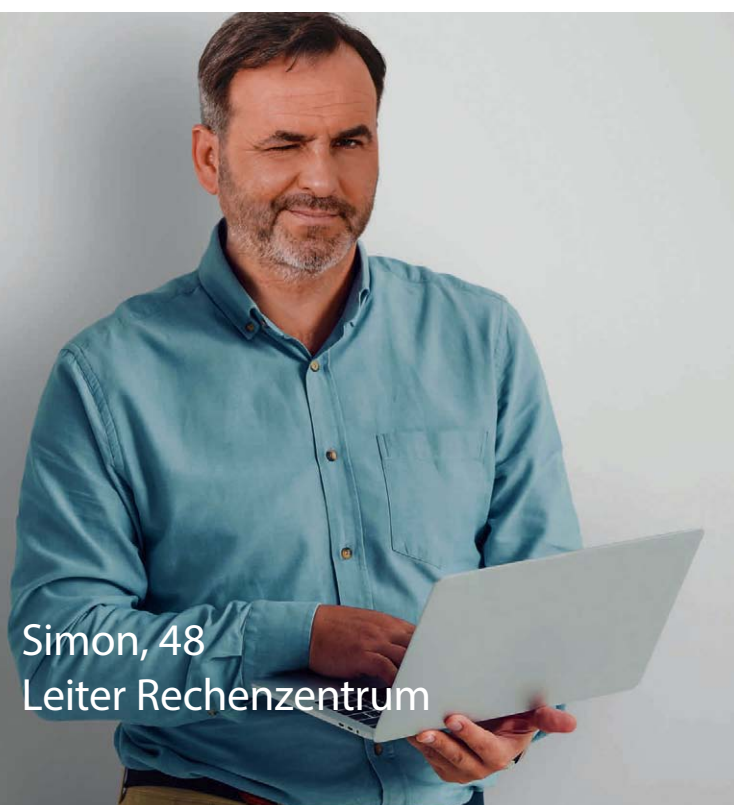
Meshcloud launcht Open-Source-Anwendung Collie Cloud-Aktivitäten im Überblick behalten

Der Multi-Cloud-Spezialist Meshcloud launchte sein CLI-Tool (Command Line Interface) Collie für Cloud-Teams. Damit stellt das Frankfurter Startup eine Open-Source-Anwendung zur Verfügung, die Unternehmen einen besseren Überblick über ihre Cloud-Landschaft verschaffen soll. Als Open-Source-Lösung ist Collie kostenfrei auf GitHub unter der Apache License 2.0

erhältlich und innerhalb von ein paar Minuten ohne langwieriges Setup nutzbar, so das Meshcloud-Versprechen. Das Tool zielt darauf ab, Cloud-Verantwortlichen Kontrolle und Übersicht über ihre Infrastruktur zu geben. Ein Vorteil der Anwendung sei unter anderem, einen generellen Überblick über aktuelle Cloud-Umgebungen (AWS, Azure und Google Cloud) zu erhalten. Da-

rüber hinaus ermögliche das Tool den Überblick über die Kosten aktueller Umgebungen und über die Zugriffsrechte in Cloud-Umgebungen. Zur Umsetzung einer konsistenten Cloud-Tagging-Strategie sollen Nutzende außerdem von einer Übersicht und Analyse von Cloud-Tags profitieren. Das Tool richtet sich laut Meshcloud-Bekunden an individuelle Enterprise-Architekten und

Cloud-Plattform-Spezialisten, die sich einen transparenten Überblick über ihre Cloud-Landschaft verschaffen wollen. Damit sei Collie auch geeignet für kleinere Unternehmen, die sich eine leichtgewichtige Cloud-Governance aufbauen wollen. Collie ergänzt Mesh-Stack, eine Plattform für Cloud-Foundation-Teams, soll aber auch unabhängig davon nutzbar sein. am



Simon, 48
Leiter Rechenzentrum

Energiebegeistert



Steckt voller Zuverlässigkeit.
#WePowerYourDataCenter

Finden Sie Ihre ideale PDU auf
www.bachmann.com

**BACH
MANN**
We power your life.

Cybersecurity: OT und IT im Gleichschritt

Know-how bündeln

Cyberkriminelle haben die Operational Technology (OT) als lukratives Angriffsziel entdeckt. Viele Betriebe sind auf die Bedrohung nur wenig vorbereitet. Dies gilt vor allem, weil IT- und OT-Verantwortliche unterschiedliche Sichtweisen haben.

Es kann jeden treffen – im Mai war Colonial Pipeline dran, der Betreiber der größten Treibstoff-Pipeline in den USA. Hacker platzierten eine Schadsoftware, die die Computersysteme verschlüsselte und den Betrieb der Pipeline störte. Damit hatten sie Erfolg. Colonial zahlte fünf Millionen Dollar, damit die Angreifer das System wieder entsperren.

Angriffe mit Ransomware oder anderen Strategien auf Industrieanlagen oder kritische Infrastrukturen passieren täglich, und sie dürften häufiger werden. Die Industrie digitalisiert ihre Geschäftsprozesse entlang der gesamten Wertschöpfungskette, von der Virtualisierung im Produktentstehungsprozess über flexiblere Service- und Geschäftsmodelle bis zu neuen Herstellungsverfahren wie Additive Manufacturing. Durch die Anbindung der Produktionsanlagen und Maschinen an interne Systeme zur Produktionssteuerung oder immer mehr auch an die Cloud steigt das Risiko für Malware und Cyberangriffe.

Verfügbarkeit ist alles

Noch etwas spielt den Angreifern in die Hände: Zwischen den Verantwortlichen für IT und OT gibt es in vielen Unternehmen eine tiefe Kluft, der eine versteht nicht, was der andere sagt und umgekehrt. Dies beginnt damit, dass IT- und OT-Verantwortliche die drei Säulen von Cybersecurity – Verfügbarkeit, Integrität, Vertraulichkeit – unterschiedlich gewichten. Während für IT-Experten die Vertraulichkeit einen hohen Stellenwert genießt, ist sie den Verantwort-

lichen im Produktionsumfeld ziemlich gleichgültig. Für sie zählen nur drei Aspekte: Verfügbarkeit, Verfügbarkeit und Verfügbarkeit. Die Produktion darf niemals stillstehen, außer in geplanten Wartungsfenstern, die bei Anlagen in der Prozessindustrie, also bei der kontinuierlichen Fertigung etwa von Chemikalien, nur alle paar Jahre anstehen. Die Maxime aus der IT-Welt, Patches möglichst schnell innerhalb von Tagen einzuspielen, ist deshalb bei Produktionsleuten völlig unbekannt.

Dennoch ist den Beteiligten bewusst, dass dies nicht für immer so bleiben kann. Schließlich hat sich durch die Vernetzung von Maschinen untereinander und zunehmend über die Automatisierungspyramide hinweg mit der Office-IT die Angriffsfläche vergrößert, ebenso das Risiko, sich Malware einzufangen, die sich durch das Netzwerk gräbt. An dieser Stelle gibt es die nächste Diskrepanz. Wenn die IT von Vernetzung spricht, meint sie meist sternförmige Netzwerktopologien, die von Switches koordiniert werden. Dort sind Anbieter wie Cisco, HP oder Fortinet die Platzhirsche. Anders in der OT: Dort dominieren Ringtopologien, Feldbusse und Echtzeit-Netzwerke. Den Markt dominieren Siemens, Hirschmann, Phoenix-Contact und andere, mit denen die IT selten zu tun hat. Die Vorliebe für Ringtopologien in der OT rührt daher, dass dort Latenzen und natürlich die Verfügbarkeitsanforderungen sehr kritisch sind. Der Datenaustausch etwa mit einem Roboter muss auf Millisekunden genau sein, Laufzeitverzögerun-

gen können ihn aus dem Takt bringen. IT- und OT-Experten sprechen also eine unterschiedliche Sprache und haben völlig unterschiedliche Vorstellungen von der Cybersecurity. Angesichts zunehmender Attacken etwa mit Ransomware fühlen sich die IT-Leute in Unternehmen in der Pflicht, ihren OT-Kollegen die Gefahren zu erklären und Lösungsvorschläge zu machen. Dies kann von ihnen jedoch schnell als oberlehrerhaft aufgefasst und abgeblockt werden. Das Totschlagargument der OT lautet dann: Die Produktion sorgt für den Umsatz des Unternehmens, nicht die IT.

Unterschiedliche Sprachen

Um den Knoten zu durchschlagen, richten einige Unternehmen Schnittstelleneinheiten ein, die zwischen IT und OT vermitteln. Erfahrungsgemäß funktioniert dies meist gut. In solchen Zirkeln müssen beide Seiten aufeinander zugehen. Die OT muss sich öffnen und ihr Know-how preisgeben. Die IT muss die funktionale Sichtweise der OT akzeptieren und ihr Know-how entsprechend anpassen. Wenn die OT zum Beispiel einen Server aufsetzt, sollte sie die IT dazu holen und ein Sicherheitskonzept erstellen, das für beide passt und bei dem die IT-Kollegen nicht die Hände über dem Kopf zusammenschlagen.

Die IT und die Security-Abteilungen können auch ein wichtiger Partner sein bei Verhandlungen mit den Lieferanten von Steuerungen und Anlagen. Fragt man OT-Leute, warum sie eine Anlage so und nicht anders vernetzen, kommt als Antwort meist: Weil es der Hersteller so vorgibt oder man es immer schon so gemacht hat. Angesichts neuer Bedrohungen ist dies jedoch unbefriedigend. Die IT kann kritisch hinterfragen und die Hersteller zusammen mit dem Einkauf dazu verpflichten, mehr für eine moderne Cybersicherheit zu tun, damit sich die OT-Kollegen nichts aufzwingen lassen.

Malware schon bei Auslieferung

Dies gelingt allerdings leider nicht immer. Bei Spezialanlagen gibt es mitunter nur einen Anbieter und der Betreiber hat keine Wahl, was gefährlich sein kann. Es gab

Fälle, bei denen sich Malware bereits vor Auslieferung in einer Maschine eingenistet hatte. Abhilfe schaffen Lösungen, die Anlagen vor Inbetriebnahme überprüfen und das Normalverhalten der Anlage überwachen und Alarm schlagen, wenn es zu verdächtigen Abweichungen kommt.

Dies greift dann jedoch nur bei neuen Anlagen. Was macht man mit den alten Maschinen, die oft 20 Jahre oder länger ihren Dienst tun und nun plötzlich zur Vernetzung nachgerüstet werden? Dann empfiehlt sich eine Netzwerksegmentierung. Dabei trennt man Teile einer Produktion je nach Risikolevel, Kritikalität und Betriebsmodell von anderen Systemen ab und wendet separate Sicherheitsstrategien an. Dazu müssen der Aufbau im Detail und die Kommunikation der Anlage bekannt sein. Nicht nur Hersteller und Betreiber einer Anlage sind gefordert. Für eine hohe Security müssen vielmehr auch die Instandhalter mit ins Boot. Bei Fernwartung greifen sie über eine VPN-Verbindung meist auf einen Jump-Server zu. Über solche Verbindungen gelingt es Hackern bisweilen, Schad- und Spionagesoftware zu platzieren, die dann ganze Anlagen und Werke befallen kann, insbesondere wenn der Zugriff auf den Jump-Server oder die VPN-Authentifizierung nur schwach geschützt ist. Um solche Risiken zu vermindern, ist eine bessere Architektur nötig. Aber wie könnte die aussehen? Manche Security-

Dienstleister empfehlen dazu ein Audit mit einem Penetrationstest, der Schwachstellen in der IT- und OT-Infrastruktur aufdecken soll. Vermutlich findet man jede Menge Schwachstellen, doch der Erkenntnisgewinn ist gering, insbesondere, wenn keine Security in die OT-Systeme implementiert ist. Viel besser ist es, erst einmal Basismaßnahmen umzusetzen und diese dann mit einem Audit zu prüfen.

Nur schützen, was man kennt

Startpunkt für eine bessere OT-Security ist eine höhere Sichtbarkeit in den OT-Netzen. Oft wissen die Unternehmen gar nicht, welche Detailkomponenten sie in den Anlagen haben, welche Softwareversionen sie nutzen, welche Daten sie austauschen und welche Verbindungen nach außen zu Drittfirmen bestehen. Doch was nicht bekannt ist, kann man auch nicht schützen. Die Kenntnis der eingesetzten Softwareversionen, Kommunikationsbeziehungen, externen Zugriffe, Zonierungen im Netzwerk und einiges mehr ist die Grundlage jeder Cybersecurity-Strategie. NTT Data empfiehlt zum Beispiel ein Cybersecurity-Framework, das aus vier Schritten besteht: technische Analyse, Bewertung, Umsetzung und Sicherung.

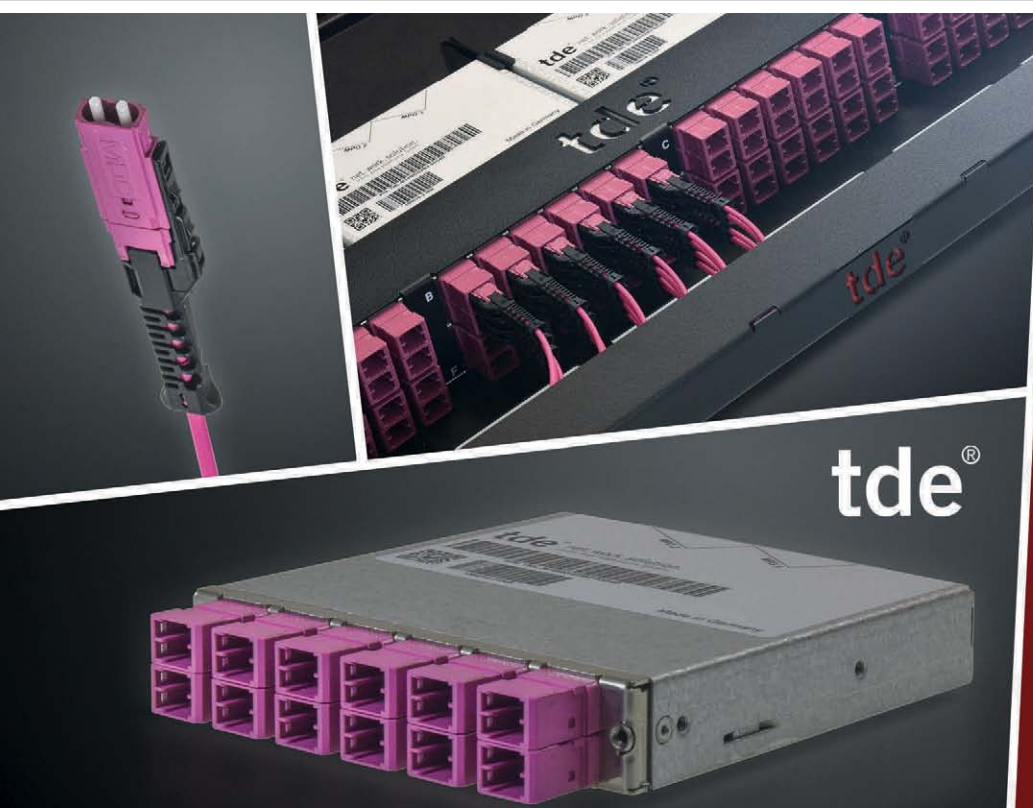
Viele Unternehmen, die nach Unterstützung für OT-Security fragen, haben bereits einen Sicherheitsvorfall hinter sich oder kennen Unternehmen in ihrem Umfeld, die

so einen Vorfall hatten. Das Bewusstsein ist in den letzten Jahren gestiegen und die Unternehmen sind motiviert, mehr für die Security zu tun. Die Unternehmen fühlen sich allerdings oft überfordert und wissen nicht, wo sie beginnen sollen. Dann ist ein strukturiertes Vorgehen gefragt, das dem Unternehmen Orientierung gibt. NTT Data erarbeitet mit dem Anwender zusammen ein Sicherheitskonzept, technische und organisatorische Lösungen und begleitet ihn später bei der Umsetzung und beim Betreiben der Sicherheitsmaßnahmen. Dabei geht es nicht um maximale Sicherheit, sondern um die für dieses Unternehmen passende Sicherheit. Viele Unternehmen denken dabei nur an Ransomware, die in den Medien großes Echo findet, vergessen jedoch, dass sie jede Menge Know-how haben, das für Wettbewerber interessant sein könnte. Vor allem das Wissen, wie man ein Produkt herstellt, ist mehr wert als viele denken. Dieses Wissen steckt in der OT, zum Beispiel in den Steuerungen.

Das Fazit lautet also: Cybersecurity in Produktionsanlagen ist kein optionales Feature, sondern ein absolutes Muss – und zum Glück auch kein Hexenwerk, wenn man sich an Grundregeln hält und mit kompetenten Partnern zusammenarbeitet.

Christian Koch/jos

Christian Koch ist Vice President Cybersecurity und Lead für IoT/OT bei NTT Data DACH.



tML® mit MDC

384

Fasern auf einer
Patch-Höheneinheit

www.tde.de

Security beim Edge Computing – Teil 2

Neues Bekanntes

Teil 1 dieses Beitrags in LANline 8/2021 reihte Edge Computing in die Liste der Begriffe ein, die beim Marketing-Buzzword-Bingo derzeit hoch im Kurs stehen. Dies soll jedoch nicht darüber hinwegtäuschen, dass es auch viel inhaltliche Substanz gibt. Eine Diskussion der Sicherheitsgrundsätze steht noch aus.

Ein wichtiger Aspekt ist der Einsatz am Netzwerkrand mit im Gegensatz zu vielen Cloud-Anwendungen geringen Latenzwerten. Für diesen Bereich sind – wie in Teil 1 dieses Artikels bereits angedeutet – Hardwareplattformen verfügbar, die ihre Funktionen und Leistung lokal bereitstellen. Kombiniert mit einem Dienst wie Greengrass steht einem Entwickler also eine sehr potente Hardwareplattform kombiniert mit einer umfangreichen Ablaufumgebung und Management-Backend zur Verfügung, die bei Bedarf auch transparent Ressourcen der Cloud nutzt. Dieser beeindruckende, aber dennoch komplexe Stack macht einige Use Cases jedoch überhaupt erst möglich und wirtschaftlich sinnvoll. Die Argumentation sollte jedoch nicht den Eindruck erwecken, dass Amazon und Nvidia in dem Umfeld die einzigen Player sind. Schaut man sich moderne Autos an, so findet man eine fast identische Architektur vor, nur stammen die Komponenten dort von anderen Anbietern oder sind vom Hersteller selbst entwickelt. Die Spannweite an Implementierungsmöglichkeiten ist also enorm.

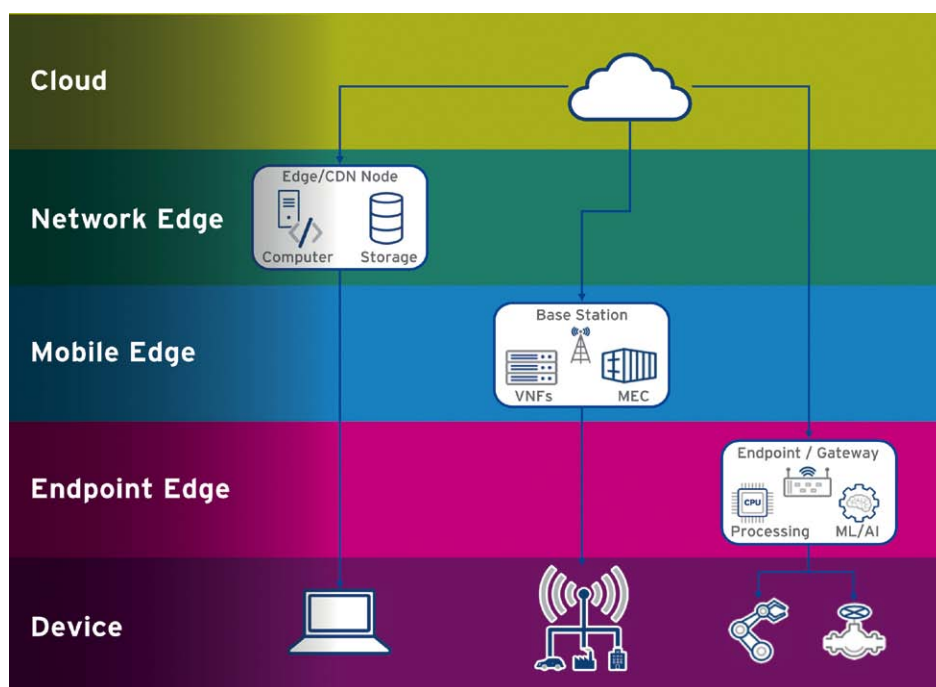
Mobile Edge Computing

Eine dritte Spielart des Edge Computings findet sich im Umfeld der Mobilfunknetze – insbesondere bei 5G. Mobile Edge Computing oder auch Multi-Access Edge Computing ist eine von der ETSI definierte Netzwerkarchitektur, die im Bereich der Mobilfunknetze die Cloud-Computing-artige Ausführung von Funktionen am (Mo-

bilfunk-)Netzwerkrand (etwa der Basisstation) erlaubt.

Während bei früheren Mobilfunkgenerationen wie LTE die Netze sehr statisch waren und Netzwerkfunktionen von dedizierten Hardwareinstanzen übernommen wurden,

Firewalls) sind durch VNFs (Virtualized Network Functions) ersetzt. Gerade der letzte Aspekt hat auch für Nicht-Mobilfunkbetreiber eine extreme Relevanz, erlaubt er doch, Netzwerkfunktionen direkt am Sendemast oder deutlich näher am Subscriber zu implementieren. Einige Netzbetreiber bieten sogar bereits Dienste an, bei denen man als Kunde eigene Funktionen mit NFV (Network Function Virtualization) direkt im Core-Netz des Betreibers schaffen kann. Dies ist sicher nichts, was Firmen für wenige unkritische Netzwerkfunktionen aufsetzen oder bezahlen wollen. Wenn man das Konzept der klassischen CDNs jedoch weiterentwickelt (etwa für Video-Streaming-Dienste), könnten lokale Edge Server noch näher an die Subscriber rücken – sozusagen bis in die Basisstation. Funktionstechnisch sind diese VNF-Instanzen in virtuellen Maschinen abgebildet. Die Plattformen reichen von kommerziell (etwa



Die verschiedenen am Edge Computing beteiligten logischen und technischen Schichten.

Bild: Trend Micro

zeichnet sich 5G durch eine durchgehende Virtualisierung aller beteiligten Komponenten aus. Statische Netzwerkkonfigurationen sind durch die automatische Provisionierung von Netzwerkstrukturen via SDN (Software-Defined Networking) ersetzt. Proprietäre Netzwerkhardware (etwa

VMware vCloud VNF) bis hin zu Open Source (etwa OPNFV auf Basis von OpenStack/KVM). Um hohe Durchsätze zu ermöglichen und die Ressourcen zu optimieren, kommen darüber hinaus noch Techniken (zum Beispiel DPDK) zum Einsatz, die das Netzwerkpaket-Handling optimieren

oder in geeignete Hardware auslagern. Aber auch von der Verwaltungsseite erfordern SDN und NFV ein Umdenken. Vereinfacht gesagt lautet das Ziel: null manuelle Interaktion. Pfade werden automatisch konfiguriert (SDN) und Instanzen automatisch bei Bedarf an entsprechenden Stellen hoch- und heruntergefahren (NFV). Dies geht sogar so weit, dass einige Router-Hersteller jetzt in der Lage sind, VNF-Instanzen auf Routern selbst zu betreiben. Letztendlich entscheidet also ein Operator (auch wieder eine automatische Funktion) darüber, was wann wo hochzufahren oder zu konfigurieren ist.

Gerade in diesem Umfeld ist es noch wichtiger, sich von der Idee des „Server-Streichelns“ zu verabschieden. Server – oder Dienste – sind nun massenhaft wie Vieh organisiert – und werden nicht wie Haustiere gestreichelt („Pet vs. Cattle“).

Dies gilt auch, wenn die Details zunächst sehr komplex klingen und auf den ersten Blick zu komplex für Enterprise-Netze erscheinen. Letztlich ist das Betriebsmodell von 5G nicht auf Telkos/Carrier limitiert. Vielmehr liefert das Netz-Betriebskonzept von 5G eine Art Blaupause für zukünftige Netzdesigns. So wie das Thema Virtualisierung und Overlay-Netze nach und nach in kleinere Umgebungen diffundiert ist, gehen Experten davon aus, dass das Netzbetriebs- und Architekturkonzept von 5G aufzeigt, wie zukünftige Netze zu designen und zu betreiben sind – unabhängig von der Branche.

Edge Computing Security

Bei all diesen schönen neuen Edge-Computing-Techniken stellt sich zwangsläufig auch die Frage nach Sicherheit. Leider sind Antworten ähnlich diffus wie die Definition von „Edge Computing“. Letztlich hilft es, sich im Einzelfall die Implementierung anzuschauen, um mögliche Ansatzpunkte zu sehen.

Das Ausführen von Funktionen am Network Edge ist technisch nicht weit von „Serverless“ entfernt. Im konkreten Fall lässt sich also nur das schützen, worauf man als Kunde Zugriff hat – bei Serverless also ausschließlich auf den Programmcode, der abläuft. Abgesehen vom Monito-

ring lässt sich Security also nur als integraler Bestandteil des ausgeführten Codes einbringen. Dienste, Libraries oder Sicherheitsfunktionen müssen die Beteiligten also gewissermaßen während der Entwicklung „einbrennen“ (lassen).

Beim Edge Computing am Endpoint tut sich bisweilen das größte Problem von allen auf: Wenn man nicht gerade einen Full-Service-Dienstleister hat, bleiben der Aufbau eines sehr komplexen Dienste-Stacks über die Cloud sowie Kommunikation und Endpunkt am Anwenderunternehmen selbst hängen. Der Nutzer sieht sich also mit einer beliebig komplexen Aufgabe aus Absicherung von Workloads (in der Cloud), Services, Identity- und Access-Management, Verschlüsselung (Transport und Storage), PKI, FOTA, Firmware-Integrität und vielem mehr konfrontiert.

Technisch bedeutet dies also mindestens Workload Security (Server, VM, Container, Serverless), Communication Security (Netzwerk, FW, IPS, QoS, Routing, LB/GLB) und Embedded Security (Identität, FOTA, (De-)Provisionierung). Dies gilt selbst dann, wenn er auf bestehende Plattformen und SDKs aufbaut. Dann bleibt mindestens die Security des eigenen Codes als eigene Aufgabe übrig. Das Thema ist also beliebig komplex.

Bei der Implementierung von Mobile-Edge-Computing-Diensten stellt sich die Situation (nur) auf den ersten Blick sehr einfach dar. Das Paketierungsformat ist eine VM, und Aufgabe dieser VM ist es, Netzwerkinhalte zu untersuchen, zu filtern und zu verändern. Auf den zweiten Blick ergeben sich jedoch auch in diesem Umfeld massive Herausforderungen, die VM sicher zu halten – seien es die Third-Party-Dienste und die Services, die man auf der VM ausführt, natürlich jedoch auch der eigene Code. Die Integration in das Provisions- und Konfigurations-Framework des jeweiligen Telekommunikationsanbieters kommt hinzu, zumal es dort leider auch keinen echten Standard gibt.

Fazit

Edge Computing (in welcher Form auch immer) bringt aus Security-Sicht einige Herausforderungen mit sich, denen sich alle Be-

teiligten stellen müssen. Eine Seite ist sicher der Abschied von liebgewonnenen Best Practices. Es gilt, sich geistig davon zu verabschieden, dass sich Security im Nachhinein schon „irgendwie anbauen“ lässt. Was bei lokalen Diensten und Netzwerken noch machbar war, ist bei modernen Umgebungen einfach nicht mehr möglich, schon in Ermangelung einer Basis, an die der Anbau erfolgen könnte. Vielmehr muss Security von Anfang an bei der Entwicklung mit eingeplant und eingebunden sein. Dies bedeutet jedoch leider auch, dass sich Security-Verantwortliche mehr mit Technik und Vorgehensweisen auseinandersetzen müssen, die bisher eher im Bereich der Softwareentwicklung zu suchen waren.

Die andere Seite ist die Verwaltung von Sicherheitsfunktionen. Die manuelle Verwaltung von einzelnen Sicherheitsfunktionen ist (vor allem bei einer großen/variablen Anzahl von Edge-Computing-„Dingen“) einfach nicht mehr machbar. In diesem Kontext ist auch die Verwaltung zahlreicher Devices über eine Management-Lösung oft noch „manuell“. Zugespielt lässt sich formulieren: „Wenn der Regelbetrieb vorsieht, dass ein Mensch Dinge ändert, dann gibt es noch Automatisierungspotenzial.“ Dies ist etwa mit der Codifizierung von Konfigurations- und Sicherheitsoptionen (Stichwort „Everything as Code“) adressierbar. Eine andere Möglichkeit stellen „Operators“ dar – dort ist auch das Wissen/Vorgehen eines menschlichen Administrators in Code gegossen, der dann automatisch reagieren kann. Dies ermöglicht den menschlichen Verantwortlichen, sich auf das zu konzentrieren, was sich nicht automatisieren lässt.

Im Gegenzug gewinnt die Branche allerdings womöglich eine ganze neue Art von Security, die fast vollständig automatisiert in Dienste eingebaut ist und den Regelbetrieb gewährleistet. Die Menschen sind dann frei, das zu tun, was ihnen keine Maschine abnehmen kann: unvorhergesehene Dinge kreativ und „um die Ecke denkend“ zu behandeln.

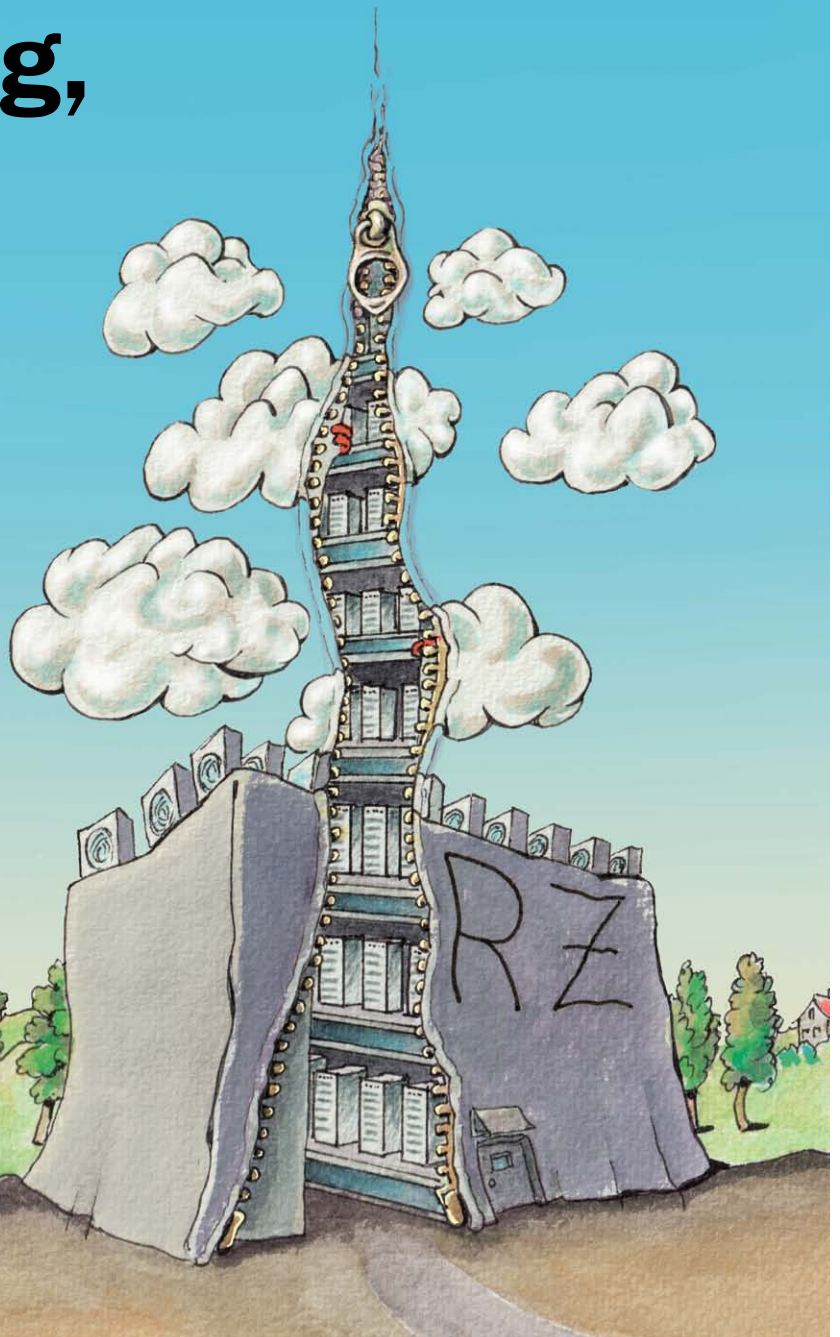
Udo Schneider/jos

Udo Schneider ist Security Evangelist bei Trend Micro.

Sicherheit in Zeiten der Hybrid Cloud

Dame, König, As, SASE

Stellt euch vor, es ist Cloud, und keiner geht hin. Noch vor zehn Jahren hätte dieser Satz bei manchem wohlwollendes Nicken oder verschmitztes Lächeln hervorgerufen. Heute hingegen wäre ein Leben ohne die Cloud schwer vorstellbar: Privat hängen wir am Tropf von Netflix, YouTube, Facebook und Instagram, während die Unternehmen in Pandemiezeiten vielen Beschäftigten spontan das Heimoffizierspatent verliehen und die Produktivität mit Cloud-Services wahrten, nicht zuletzt dank Videoconferencing mittels Zoom & Co. Die sichere Anbindung an das Unternehmensnetz wie auch an die Cloud ist somit wichtiger als je zuvor.



Einst – die Graumelierten oder aber dezent Colorierten werden sich erinnern – herrschte beim Thema Weitverkehrsnetz zumindest in größeren, geografisch verteilten Unternehmen ein regelrechter Hype um die Standortvernetzung per MPLS: Multiprotocol Label Switching erlaubte es seit Ende der 1990er-Jahre, die veralteten, überteuerten und vorrangig auf Sprachkommunikation ausgelegten Stand-

leitungen abzulösen. Es ermöglichte die QoS-gesicherte (Quality of Service) verbindungsorientierte Datenkommunikation zwischen Niederlassungen und der Zentrale, selbst die Vollvermaschung der Standorte war in greifbare Nähe gerückt (obschon ein teures Hobby). Der Siegeszug folgte: Laut dem Analystenhaus Research and Markets lag das globale Marktvolumen für Managed-MPLS-Services

2019 bei 48,6 Milliarden Dollar, bis 2025 soll es auf über 70 Milliarden klettern. Aber die Gloriole des MPLS-Hypes ist längst verblasst: Nicht nur raubten 20 Jahre Fortschritt beim IP-Routing dem MPLS einige seiner Performance-Vorteile; zugleich ließ der schleichende, aber kontinuierliche Siegeszug der Public Cloud die Vernetzung im Unternehmen deutlich komplizierter geraten, als es der Begriff

„Standortvernetzung“ einst vermuten ließ. Zugriff auf Applikationen ist längst nicht mehr gleichbedeutend mit Zugriff auf das Unternehmens-RZ. Vielmehr fordern heute Beschäftigte, wo immer sie arbeiten, zugleich performanten Zugang zu jener wachsenden Fülle von Cloud-Services, die sie für ihre Arbeit benötigen.

Laut „Cloud-Monitor 2021“ von Bitkom und KPMG, vorgestellt im Juni, nutzen inzwischen 82 Prozent der deutschen Unternehmen Cloud-Services, 46 Prozent beziehen diese aus der Public Cloud (36 Prozent meinen also mit „Cloud“ ihre eigene „Private Cloud“ oder eine „Hosted Private Cloud“). Doch beim Zugriff auf die Public Cloud – oder extern gehostete Private-Cloud-Ressourcen – ist der Kommunikationspfad über das Unternehmens-RZ ein Umweg, der aufgrund unnötig aufgeblähter Latenz viel Zeit und Geld sowie Nerven der Belegschaft kostet. Natürlich lassen sich mit Richtlinien punktuelle Direktverbindungen zu Web- und Cloud-Services (Internet Breakouts) definieren. Das kostet allerdings ebenfalls viel Zeit und Geld – sowie diesmal die Nerven des Netzwerkteams.

Standleitung, MPLS, Cloud, SD-WAN

Vor diesem Hintergrund hat sich das „softwaredefinierte“ Weitverkehrsnetz (Software-Defined Wide Area Network, SD-WAN) vor ein paar Jahren den Hype-Heiligenschein geschnappt. Der Begriff „Software-Defined“ ist auf den ersten Blick irreführend: Alles in der IT ist letztlich „softwaredefiniert“, wäre doch jede Hardware ohne passende Software nur Elektroschrott. Auch MPLS-Netze arbeiten nicht „hardwaredefiniert“, machen doch die MPLS-Labels nicht „Klonk!“, wenn sie runterfallen. Der Begriff „SD-WAN“ jedoch soll aussagen: Dynamische Softwaresteuerung gestaltet das Weitverkehrsnetz so flexibel, wie man dies von virtualisierten Servern und Storage-Geräten oder containerisierten Applikationen her kennt. Ein Hauptvorteil des SD-WANs liegt somit darin, dass sich echtzeitnah steuern, automatisieren und optimieren lässt, wer von wo aus mit welcher QoS auf welche IT-Ressourcen zugreifen darf.



„Wir beobachten, dass Unternehmen von der Best-of-Breed- zur Best-of-Suite-Technologie übergehen“, berichtet Verizon-Mann Alistair Neil.

Bild: Verizon Enterprise Solutions

Wie wichtig flexible Steuerung der Unternehmensvernetzung sein kann, hat die Pandemie gezeigt: Heutzutage kann sich der Ort, von dem aus Beschäftigte arbeiten, schnell ändern – Lockdowns führten international zu einer regelrechten Völkerwanderung an heimische Schreib- oder Küchentische. Zugleich ist der Bestand an Applikationen und Cloud-Services ein bewegliches Ziel: Vor wenigen Jahren war zum Beispiel Zoom noch ein Videokonferenzanbieter aus der zweiten Reihe, doch während der Lockdowns mauserte sich das Unternehmen trotz anfangs durchaus bedenklicher Security- und Datenschutz-mängel zur allseits bekannten Marke – und die Arbeitspsychologie nennt das verbreitete Phänomen einer Erschöpfung aufgrund nicht enden wollender serieller Videokonferenzen heute „Zoom Fatigue“. Eine dynamische Landschaft geschäftsrelevanter Cloud-Services wird künftig normal sein, ebenso das flexible, zumindest zeitweise verteilte Arbeiten: Nicht nur, dass angesichts einer schleppend verlaufenden Impfkampagne die Überwindung von COVID-19 in weite Ferne rückt und Epidemiologen längst davon ausgehen, dass Corona künftig endemisch (also alltäglich) sein wird wie etwa die Grippe –

vielmehr hat sich in der Pandemie auch gezeigt, dass Remote Work in deutlich mehr Fällen ohne Produktivitätsverlust möglich und damit praktikabler ist, als mancher zunächst dachte (sofern ein Unternehmen seine Heimoffiziere weder in die soziale Isolation noch in die Zoom-Erschöpfung treibt).

Hinzu kommt, dass zahllose Unternehmen dieser Tage alles ans Internet hängen, was nicht niet- und nagelfest ist (Stichwort „Digitalisierung“) – und dann das Niet- und Nagelfeste ebenso (Stichwort „Internet of Things“). Dieser Trend erfordert wiederum eine flexibel per Software steuerbare Vernetzung der Maschinen, Anlagen und sonstiger „Dinge“. Der Nährboden für einen florierenden SD-WAN-Markt ist also vorhanden. So geht das erwähnte Analystenhaus Research and Markets davon aus, dass das SD-WAN-Segment von 1,4 Milliarden Dollar 2020 bis 2030 auf stolze 43 Milliarden erblühen wird – ein jährliches Durchschnittswachstum von 38,6 Prozent.

Was leider ebenfalls wächst, ist das Sicherheitsrisiko, das die eskalierende Vernetzung – softwaredefiniert oder nicht – mit sich bringt: So berichtete der Branchenverband Bitkom Anfang August, dass Datendiebstahl, Spionage und Sabotage der deutschen Wirtschaft inzwischen jährlich einen Gesamtschaden von 223 Milliarden Euro zufügen. Fast neun von zehn Unternehmen (88 Prozent) seien 2020/2021 Ziel von Angriffen gewesen. Security erweist sich damit endgültig als drängendste Baustelle des allgegenwärtigen Digitalisierungsprojekts.

Sicher, Zugang, Service, Rand

Da wundert es nicht, dass sich im ewigen Hype-Staffellauf letzthin ein Security-Konzept die aktuelle Aureole geschnappt hat: „Secure Access Service Edge“ taufte das Analystenhaus Gartner vor ziemlich genau zwei Jahren (im August 2019) in seinem Papier „The Future of Network Security Is in the Cloud“ das jüngste Ferkelchen, das es seither durch das digitale Dorf treibt. Der Begriff klingt zunächst nach einer etwas lieblosen Aneinanderreihung der englischen Wörter für „sicher“,

„Zugang“, „Dienst“ und „(Netzwerk-) Rand“, ergibt aber im Englischen das Akronym (die als Wort aussprechbare Abkürzung) „SASE“. Das klingt so ähnlich wie das englische Wort „sassy“ (frech, vorlaut), was irgendjemand im Hause Gartner wohl witzig fand.

SASE ist keine neue Technologie, sondern beschreibt ein Vernetzungskonzept, bei dem Cloud-basierte Netzwerk- und Sicherheitsangebote (Network as a Service, Network Security as a Service) zusammenwachsen. Auf Netzwerkseite sind dies vorrangig SD-WAN, aber auch Content Delivery Networks (CDNs) und WAN-Optimierung, auf Security-Seite vor allem Dienste wie Secure Web Gateway (SWG), Cloud Access Security Broker (CASB), Firewall as a Service (FWaaS) und Zero-Trust Network Access (ZTNA), der KI-gestützt dauerüberwachende Nachfolger traditioneller VPN-Technik. Gartner geht davon aus, dass SASE-Anbieter sämtliche Komponenten per Cloud bereitstellen (auch wenn SD-WAN-Optimierung meist ein lokales Endgerät erfordert). Zugleich liege ein großer Vorteil des Konzepts darin, dass der Umstieg auf SASE eine Konsolidierung der Security-Anbieter erlaubt. Das Problem: Derzeit bilden sich die Angebote noch rasant aus und unterscheiden sich folglich in Breite wie auch Tiefe deutlich – siehe dazu die laufende LANline-Testserie zu SASE-Lösungen. Damit befinden wir uns mal wieder in jener Hype-Phase, in der jeder Anbieter sich die Gloriole so zurechtbiegt, dass sie ihm wie angegossen passt.

Die Konsolidierung von SD-WAN und Cloud-basierter Security zu einem Angebot aus einer Hand hat insbesondere für kleinere und mittelgroße Unternehmen einen sofort ersichtlichen Reiz. Und so prophezeien Auguren auch dem SASE-Markt eine strahlende Zukunft: Das Analystenhaus Dell'Oro sieht das Segment bis 2024 mit einer jährlichen Rate von 116 Prozent anwachsen, dann soll der SASE-Umsatz weltweit bei 5,1 Milliarden Dollar liegen. In Pandemiezeiten hat das Konzept sogar deutlich stärker Fahrt aufgenommen, als selbst die Gartner-Analysten dies erwartet hatten: Das Ferkel fegt im Schweinsga-



„Auch reine SD-WAN-Lösungen entwickeln sich weiter und erhalten zusätzliche Sicherheitsfunktionen“, so Simon Pamplin von der HPE-Tochter Aruba Silver Peak.

Bild: Aruba Silver Peak

lopp durchs Dorf. Und so mussten die Analysten ihre „strategischen Planungsannahmen“ deutlich nach oben korrigieren: Statt in fünf bis zehn Jahren werde SASE nun schon in zwei bis fünf Jahren Akzeptanz finden. Im März dieses Jahres hieß es auf Gartner's Blog, bis 2025 sollen mindestens 60 Prozent der Unternehmen eine SASE-Strategie inklusive Zeitplan vorweisen können.

Das Analystenhaus rät IT-Teams deshalb zu den folgenden vier Maßnahmen:

- ZTNA als Ergänzung zu oder aber als Ersatz für die Bestands-VPNs für Remote-Beschäftigte, insbesondere bei hohem Risiko,
- Inventarisierung von Geräten und Verträgen für den mittelfristigen Ausstieg aus lokaler Zweigstellen-Hardware und den Wechsel zu Cloud-basierter Bereitstellung von SASE-Funktionen,
- Konsolidierung von Anbietern bei der Erneuerung von Verträgen für SWGs, CASBs und VPNs zugunsten konsolidierter Angebote sowie
- aktive Beteiligung an Initiativen zur Modernisierung oder Transformation von Zweigstellen und MPLS-Offloads, um Cloud-basierte Security-Edge-Services in die Projektplanung zu integrieren.

Da der SASE-Markt gerade heftig fluktuiert, herrscht Uneinigkeit, ob und wie schnell SASE klassische SD-WAN-Lösungen ersetzen kann. „Auch reine SD-WAN-Lösungen entwickeln sich weiter und erhalten zusätzliche Sicherheitsfunktionen“, sagt zum Beispiel Simon Pamplin von Aruba Silver Peak. „Die Kombination aus integrierter Sicherheit in reinen SD-WAN-Lösungen und Best-of-Breed-Sicherheit auf Cloud-Basis wird in den nächsten Jahren das vorherrschende Konzept für Kunden sein.“ Doch die Bedeutung des „Best of Breed“-Ansatzes als Alternative zum SASE-idealtypischen „Alles aus einer Hand“ ist umstritten. Alistair Neil von Verizon Enterprise Solutions zum Beispiel berichtet: „Die meisten ‚SASE‘-Programme sind nicht so ganzheitlich wie die ursprüngliche Definition. Wir beobachten, dass Unternehmen von der Best-of-Breed- zur Best-of-Suite-Technologie übergehen. Eine integrierte Lösungssuite ist wichtiger als die besten 30 Einzelkomponenten.“

Arbeit, Zukunft, Büro, Klima

Noch ist unklar, wie schnell sich SASE hierzulande etablieren wird. Fest steht: Die nahtlose Integration von Vernetzung und Security muss rasch voranschreiten. Denn die Arbeitswelt der Zukunft wird verteilter und dynamischer sein, als uns lieb ist. Hier schlägt neben der Digitalisierung und der Pandemie auch der Klimawandel mit Wucht zu: Nicht nur aus Produktivitäts- oder Gesundheits-, sondern auch aus Klimaschutzgründen werden viele Unternehmen künftig oft auf Präsenzpfligt im Büro verzichten. Denn wenn sicheres, performantes Arbeiten von überall aus möglich ist, schaden Pendelfahrten und Bürotürme nur der Ökobilanz. Zugleich werden Unternehmen bei Auswahl und Nutzung der Cloud-Services den Energieverbrauch zum Kernkriterium machen müssen. Vielleicht stellen manche sogar fest, dass nicht alles per Videokonferenz besprochen sein muss – oft genügt eine Message, E-Mail oder ein Telefonat. Das vermeidet Zoom Fatigue und schon die Umwelt. Stellt euch vor, es ist Zoom, und keiner geht hin.

Dr. Wilhelm Greiner

Monitoring des Applikationsverhaltens

Komplexe Multi-Clouds überwachen

Eine wachsende Zahl von Unternehmen verteilt Workloads auf AWS, Microsoft, Google und andere Cloud-Provider, um Abhängigkeiten zu vermeiden und die Resilienz kritischer Geschäftsprozesse zu steigern. Dieser Trend zur Multi-Cloud verschärft die Herausforderungen für bereits stark belastete Sicherheitsteams: Komplexe Interdependenzen zwischen Cloud-Komponenten vergrößern die Angriffsfläche, während gleichzeitig die Sichtbarkeit der Gesamtinfrastruktur schwindet. Zudem fehlen Fachkräfte, während spezifisches Cloud- und Security-Know-how schnell veraltet.

Sicherheitshersteller haben ihre weit verbreiteten Konzepte und Toolsets nicht für die Elastizität und Komplexität moderner Multi-Clouds entwickelt. Das macht sich jetzt in mehrfacher Hinsicht bemerkbar: Isolierte Punktlösungen haben eine begrenzte Perspektive und führen zu Informationssilos. Der Wechsel zwischen den einzelnen Konsolen ist aufwendig und lie-

fert trotzdem keine übergreifende Sichtbarkeit. Der fehlende Kontext führt zu einer Flut einzelner Alarme ohne sinnvolle Priorisierung.

Hinzu kommt die Regelfixierung: Die vorausschauende Definition von Regeln war jahrzehntelang das A und O der IT-Sicherheit. Dynamische Cloud-Umgebungen erfordern heute aber eine permanente Anpassung

dieser starren Regelsätze. Multi-Clouds vervielfachen den Aufwand, denn Sicherheitsverantwortliche müssen vergleichbare Services unterschiedlicher Provider einzeln auf Regelkonformität prüfen (zum Beispiel AWS Cloud Formation, Azure Resource Manager und Google Cloud Deployment Manager).

Architekturbedingt haben traditionelle Sicherheitsansätze zudem Schwierigkeiten mit bestimmten Cloud-Aktivitäten. Network-Intrusion-Detection-Systeme erkennen zum Beispiel keinen Datenverkehr zwischen Containern auf derselben EC2-Instanz. Ein weiteres Problem bilden Micro-Services, Daten-Caches und temporäre IP-Adressen, die nur wenige Minuten aktiv sind und dann wieder verschwinden.

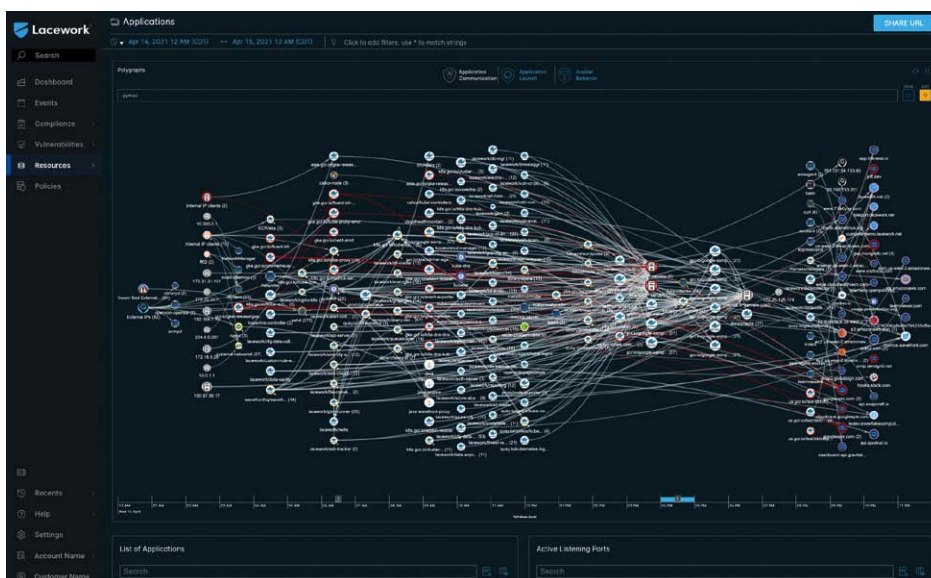
Regelloser Schutz mit Machine Learning

Eine neue Generation Cloud-nativer Sicherheitslösungen will jetzt die Komplexitätsspirale durch ML- (Machine Learning) und KI-gestützte Verfahren entschärfen. Das Versprechen lautet: umfassende Sichtbarkeit aller Cloud-Aktivitäten bei vollständiger Automation.

Im Wesentlichen kann man zwischen zwei Ansätzen unterscheiden: heuristischem und verhaltensbasiertem Machine Learning. Allerdings trennen selbst Hersteller die beiden Begriffe nicht immer eindeutig und bieten Lösungen, die oft Eigenschaften beider Ansätze aufweisen. Die Mehrzahl der heute verfügbaren Sicherheitslösungen mit ML tendiert aber eindeutig zur Heuristik. Dieser Ansatz durchsucht identifizierte Angriffe nach ähnlichen Mustern und sammelt Erkenntnisse für vergleichbare Events in der Zukunft. Besonders effektiv ist diese Methode bei Varianten bekannter Angriffe.

Wenn völlig unbekannte Zero-Day-Bedrohungen auftauchen, stößt heuristisches Machine Learning an Grenzen. Die typischen False-Positive-Raten sind in einfacheren Umgebungen akzeptabel, führen aber in komplexen Multi-Cloud-Umgebungen mit vielen Millionen Events zu Problemen.

Verhaltensbasiertes ML verwendet eine andere Herangehensweise: Hier wird fort-



ML-basierte Monitoring-Lösungen überwachen das Verhalten von Applikationen und Prozessen. So schaffen sie den Überblick selbst über komplexe Umgebungen.

Bild: Lacework

laufend der Normalzustand der individuellen Multi-Cloud-Umgebung analysiert. Dazu gehören die Aktivitäten aller Cloud-Entitäten, zum Beispiel Anwender, Workloads und Applikationen. Vor diesem Hintergrund treten Anomalien deutlich hervor. Ob eine Angriffsvariante erstmals auftaucht oder bereits bekannt ist, spielt keine Rolle. Weil die Technologie den Normalzustand erlernt, kann sie viele reguläre Aktivitäten im Cloud-Datacenter als Bedrohung ausschließen. Das reduziert die Zahl der False Positives selbst in komplexen Umgebungen.

Bestimmung der Baseline durch Prozessfokus

Für die Praxistauglichkeit verhaltensbasierter Cloud-Sicherheit ist entscheidend, ob und wie exakt sich der Normalzustand (die Baseline) individueller Umgebungen bestimmen lässt. Entsprechende Technologien sind aber bereits patentiert. Um alle Cloud-Aktivitäten bei diesen Lösungen erfassen zu können, fokussiert sich das Monitoring auf Prozesse, also auf die kleinstmögliche vom Betriebssystem unterstützte Einheit. Jede einzelne Applikation nutzt bestimmte Prozesse, verschiedene Applikationen mischen ihre Prozesse nicht. Folgende Faktoren machen Prozesse zu geeigneten Analyseeinheiten:

- Validierbar: Jeder Prozess ist mit einer bestimmten Binärdatei verbunden, die einen spezifischen SHA-256 Hash aufweist.
- Nachverfolgbar: Prozess-Monitoring erfasst die Startumstände von Prozessen und kann nachvollziehen, welche Anwender, Applikationen oder anderen Prozesse für den Aufruf verantwortlich sind.
- Vorhersagbar: Prozesse haben bestimmte Command Lines, Zwecke und Lebenszyklen.
- Unumgänglich: Prozesse sind verantwortlich für die gesamte Kommunikation. Nur Prozesse sprechen miteinander und mit externen Hosts im Internet.

Auf den Host-Systemen installierte Agenten erfassen alle Prozessinteraktionen in Echtzeit, auch wenn sie innerhalb einer Datei stattfinden. Auf einem einzelnen

Server laufen dabei in der Regel mehrere Applikationen und Container, die sich nicht identisch verhalten. Um eine präzise Baseline zu erzielen, unterscheidet das Prozess-Monitoring zwischen den Verhaltensweisen und differenziert zudem zwischen interaktivem (initiiert von Anwendern) und nicht-interaktivem Datenverkehr (initiiert von Applikationen).

Das Verhalten von App-zu-App-Datenverkehr lässt sich sehr gut vorhersagen und ändert sich auch nicht beim Auto-Scaling von Applikationen in der Cloud. Anwenderverhalten lässt sich hingegen schwerer voraussagen. Um solche und weitere Unterschiede in der Baseline zu berücksichtigen, gruppiert das Monitoring die Aktivitäten in verschiedene Kategorien. Zu diesen zählen:

- Kommunikation von Applikationen/Prozessen,
- Start von Applikationen,
- Maschinenkommunikation,
- Maschine-Server-Kommunikation,
- Änderungen von Privilegien, und
- Insider-Verhalten (menschliche Anwender).

Im Gegensatz zu anderen Host-basierten Intrusion-Detection-Systemen steht nicht die Analyse individueller Entitäten im Mittelpunkt: Das Prozess-Monitoring sammelt zwar Daten Tausender Maschinen, Prozesse, Anwender und Container, aggregiert diese aber auf Basis des Verhaltens in Gruppen. Die Analyse erfolgt nicht auf der Ebene der Host-Systeme, sondern auf Datacenter-Ebene.

Verhaltensbasiertes Prozess-Monitoring vergleicht das aktuelle Verhalten einer Entität mit dem bekannten Verhalten derselben Entität im Zeitverlauf und dem Verhalten der Peer-Gruppe aus vergleichbaren Entitäten. Alarmer generiert das Monitoring dementsprechend nicht pro Workload oder Applikation, sondern pro Analysegruppe. Das reduziert die Anzahl der Alarmer deutlich.

Vorteile für die Security

Die Konzentration auf das Verhalten von Applikationen und Prozessen eliminiert fragmentierte Detailinformationen, die ansonsten den Blick auf das Gesamtbild ver-

stellen. Stopp oder Neustart von VMs und Prozessen, ein A-B-Failover oder sogar der Start einer Applikation in einem neuen Cloud-Account ändern nichts am Verhalten. Aus mehreren Millionen Vorgängen im Cloud-Rechenzentrum entsteht eine kondensierte und stündlich aktualisierte „Karte der Normalität“. Der Abgleich mit dem bekannten Verhalten und dem Kontext der Peer-Analysegruppe identifiziert bekannte und unbekannte Bedrohungen sowie Anomalien, darunter Ab- oder Zuflüsse ungewöhnlicher Datenmengen in Amazon S3 Buckets, unerwartete Verbindungen von Applikationen oder auffälliges Anwenderverhalten.

Verhaltensbasierte Sicherheit

Mit Regeln können Sicherheitsverantwortliche solche verdächtigen, aber nicht grundsätzlich ausgeschlossenen Aktivitäten nur schwer im Vorfeld abfangen. Wenn Angreifer zum Beispiel legitime Anwender-Credentials für illegitime Zwecke einsetzen, ist das mit Regeln nicht immer zu erkennen. Verhaltensbasierte Sicherheit lernt hingegen, wie ein Anwender normalerweise agiert. Die Legitimität der Credentials ist hier nur ein Anhaltspunkt. Erfolgt der Zugriff zu einem ungewöhnlichen Zeitpunkt, nach längerer Inaktivität, auf neue Ressourcen oder von einer unbekannten Maschine aus, schlägt das Prozess-Monitoring aufgrund dieser Anomalien zuverlässig Alarm.

Unternehmen verabschieden sich nicht leichthin von etablierten Werkzeugen und langjährig bewährten Denkweisen. Aber im Bereich der IT-Sicherheit erscheint ein „Weiter so“ kaum mehr möglich: Hybrid Clouds, Multi-Clouds, Container und Serverless Computing haben die Infrastrukturen innerhalb kurzer Zeit grundlegend verändert – und das Tempo der Veränderung wächst. Hersteller können die bisherigen Ansätze nicht unbegrenzt auf dynamische Umgebungen übertragen. Deshalb spricht heutzutage einiges für einen Neustart der Sicherheit in der Cloud.

Bernd Mährlein/wg

Bernd Mährlein ist Area Director Central Europe bei Lacework.

Netzwerk-Management per Cloud

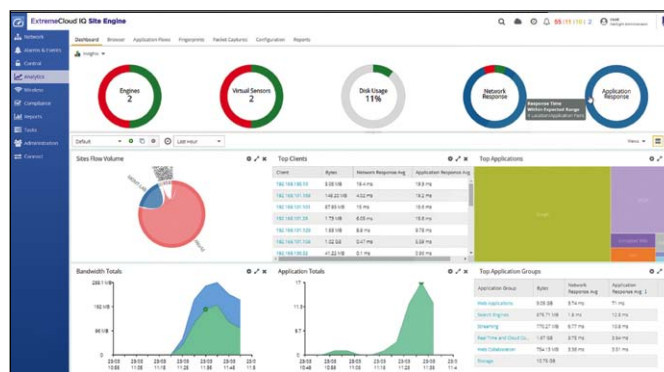
Vogelperspektive

Überlastung, Sicherheitsrisiken, zu wenig Zeit für wertschöpfende Tätigkeiten der Administratoren – es spricht nichts mehr dafür, dass Unternehmen ihre Netze klassisch verwalten. Cloud-basiertes Netzwerk-Management ist im Kommen. Weitgehend automatisierte, aus der Cloud heraus steuerbare Netzwerke sind für Digitalisierungsaspekte wie das IoT (Internet of Things), das Edge Computing oder die Multi-Cloud nahezu unabdingbar.

Unternehmen sind gefordert, Daten und Anwendungen nahtlos über den Cloud-Bestimmungsort ihrer Wahl zu verschieben. Seit dem Auftreten der Pandemie ist es zudem größtenteils Alltag geworden, in großer Zahl neue Remote-Work-Szenarien aufzusetzen, die auch zukünftig Bestand haben werden und für die ebenfalls ein klassisches Netzwerk-Management ausscheidet, da es schlicht zu aufwendig wäre. Fakt ist: Die Bereitstellung von IT-Ressourcen vor Ort kann kaum ein Unternehmen heutzutage noch stemmen. Mit einem Netzwerk-Management aus der Cloud können Unternehmen jedoch auf dedizierte IT-Ressourcen verzichten, weil die Lösung eine zentralisierte Netzwerksicht und -verwaltung für alle kabelgebundenen, Funk- und Remote-Netzwerkressourcen bietet. Mitgelieferte Management- und Überwachungsfunktionen ermöglichen Netzwerkautomatisierung, -einblicke und -sicherheit über das gesamte funkbasierte und kabelgebundene Netzwerk.

Da adäquate Lösungen auf modernen Web-Architekturen basieren, skalieren die Services dynamisch. Ein Kubernetes-Service hat sich dabei als praktikabel erweisen. Dieser beaufsichtigt die Nutzung und Überwachung von containerisierten Ser-

vice-Clustern, die sich je nach Netzwerkklast skalieren lassen. Mit diesem elastischen Design kann jedes regionale System Dutzende, Hunderte oder sogar Tausende von Nutzergruppen bedienen, die ihrerseits von der Transparenz profitieren.



Cloud-basiertes Netzwerk-Management sorgt für den Überblick über das Netzwerk vom Edge bis zum RZ.

Bild: Extreme Networks

Ein weiterer Punkt spricht für ein Cloud-basiertes Netzwerk-Management: das Plus an Sicherheit. So konstatierte eine IDC-Studie vor Kurzem, dass das „Dauerthema Sicherheit“ aus Sicht der Befragten gleichzeitig der größte Treiber für Netzwerkmodernisierung sei. Die Komplexität und die schiere Menge an Daten und Geräten sei mit manuellen Ansätzen nur noch schwer beherrschbar. Gleichzeitig stelle das manuelle Vorgehen wiederum ein Sicherheitsrisiko dar. Diese Risiken lassen sich durch die zentralisierte Verwaltung des Netzes

aus der Cloud naturgemäß deutlich mindern – aber nicht nur das: Um Informationssysteme, Datenschutz, Management und Konformität auf höchstem Niveau zu gewährleisten, sorgen seriöse Anbieter dafür, dass ihre Netzwerk-Management-Lösungen zertifiziert sind, beispielsweise nach ISO/IEC 27001. Selbstverständlich sein sollten darüber hinaus Maßnahmen und Kontrollen zum Schutz von Rechenzentren und der darin befindlichen Kundendaten, darunter Business-Continuity- und Disaster-Recovery-Prozesse, umfassende Kontrollen und Anlagenüberwachung. Dazu gehören auch technische Maßnahmen zum Schutz Cloud-basierter Anwendungen wie Firewalls, kontinuierliche Bedrohungsüberwachung, DDoS-Prävention, tägliche Backups, Penetrationstests und DevOps-Aktivitätsprüfungen.

Ein weiterer Risikofaktor bei tradiertem Netzwerk-Management ist die manuelle Konfiguration an lokalen Standorten. Diese ist nicht allein arbeitsintensiv, kostspielig und zeitaufwendig, sondern auch fehleranfällig. Qualifizierte, automatisierte Lösungen aus der Cloud machen lokale Konfiguration hingegen überflüssig. Mit Zero-Touch Provisioning können Administratoren Netzwerkgeräte an jedem beliebigen Ort auf der Welt bereitstellen. Wenn sie einen Access Point anschließen, erkennt dieser das Cloud-Konto und lädt dann automatisch die erforderliche Firmware und die spezifische Gerätekonfiguration herunter. Nach wenigen Minuten überträgt der Access

Point eine SSID, um Beschäftigten und Geräten den Funkzugriff zu gewähren. Sicherheit im Netzwerk-Management bedeutet auch Ausfallsicherheit. Einige Cloud-Anbieter streben eine extrem hohe Verfügbarkeit von 99,99999 Prozent an, verpflichten sich in ihren SLAs jedoch nur zu 99,9 Prozent. Durch umfassende Redundanzen und Backup-Maßnahmen können Anbieter heute jedoch eine kontinuierliche Verfügbarkeit der Netzwerkservices bei Ausfällen und Katastrophen sicherstellen, die über die 99,9 Prozent hinausgeht.

Durch Aufwärts- und Abwärtskompatibilität sind leistungsstarke Systeme in der Lage, diese hohen Verfügbarkeitsanforderungen zu erfüllen. Jede Codezeile in der Anwendung, die mit einer Datenbank interagiert, sollte deshalb potenzielle Änderungen des Datenbankschemas vorhersehen und somit eine reibungslose Verarbeitung ermöglichen. Die beteiligten Datenbanken müssen ebenfalls abwärtskompatibel sein, damit veraltete Anwendungen während des Upgrade-Prozesses weiterhin funktionieren. Dieses Zusammenspiel von Code, Verarbei-

trahiert es aussagekräftige Ereignisse, Ursachen und damit verbundene Probleme mit Konfigurationen, anderen Ereignissen oder Zustandsdaten, die nicht miteinander in Zusammenhang zu stehen scheinen. Durch KI abgeleitete Dateneinblicke helfen der IT, den Betriebszustand des Netzwerks auf einen Blick zu erkennen und zu überwachen.

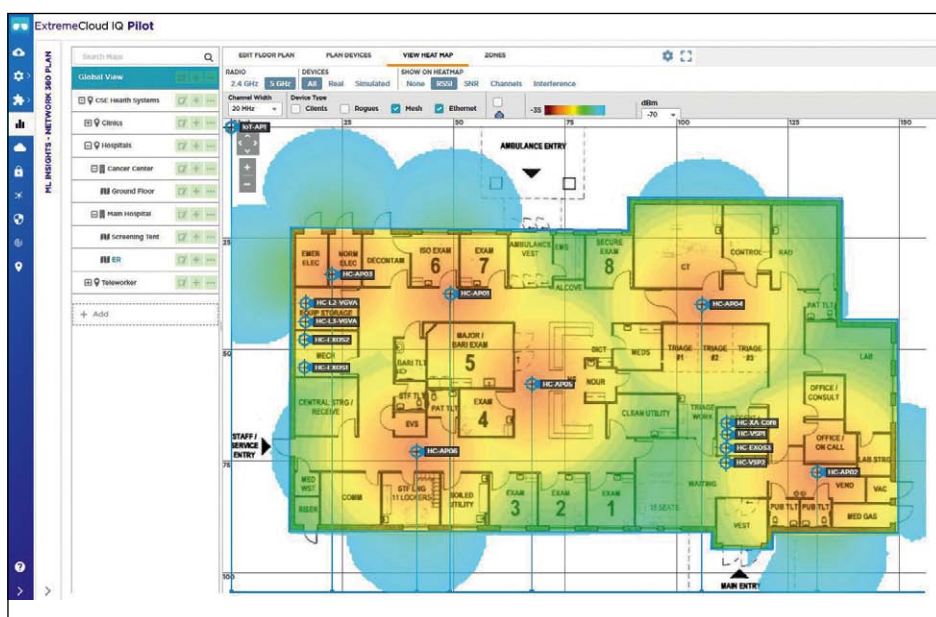
Wichtig indes für Unternehmen, die sich für eine solche Lösung entscheiden: Wie die Cloud-Nutzung an sich, so muss natürlich auch das Netzwerk-Management ein

naged Service Provider oder Unternehmen, die die Skalierbarkeit und Elastizität der Cloud mit zusätzlicher Kontrolle über das Hosting in ihrem eigenen Rechenzentrum oder innerhalb ihrer eigenen segmentierten RDC-Instanzen im Rechenzentrum eines Cloud-Providers wie AWS verbinden wollen. Selbstverständlich muss ein modernes Netzwerk-Management Cloud-agnostisch sein: Es muss dem Anwender überlassen bleiben, ob er die Lösung via Google Cloud, AWS oder Microsoft Azure einsetzt.

Betreibt ein Anwender sein Netzwerk-Management autonom, so ist er, was die Leistungsfähigkeit betrifft, auf die wenigen Werte angewiesen, die ihm seine Telemetriedaten darstellen können. Namhafte Anbieter von Cloud-Lösungen können ihm jedoch anonym operative und leistungsbezogene Kennzahlen zahlreicher anderer Unternehmen zu Vergleichszwecken zur Verfügung stellen. Dafür nehmen sie täglich mehrere PBytes an Telemetriedaten aus verschiedenen Kundennetzwerken auf. Im Hintergrund erfolgt dann eine Analyse der Integrität und der Verhaltensmuster von Daten. Data-Science- und Machine-Learning-Algorithmen werden auf die Datensätze angewandt, um genaue und aussagekräftige Einblicke in Systemdaten zu erhalten. Der Datenhorizont ist dabei bestenfalls unbegrenzt. Das heißt, dass der komplette umfangreiche Datensatz für die gesamte Service-Dauer zur Verfügung steht. Netzwerkinfrastruktur-, Client- und Anwendungsdaten sind somit in Echtzeit und als Verlauf verfügbar. Mit Zeitschieberegeln kann sich das Administrationsteam dann auf Zeitabschnitte konzentrieren, die von besonderem Interesse sind.

Mit einem leistungsfähigen, Cloud-basierten Netzwerk neuester Prägung können Unternehmen Netzwerkvorgänge End-to-End und vom Edge bis zum Datacenter automatisieren, neue Analysen erstellen, schneller skalieren sowie die Endanwendungserfahrung sichern und optimieren. Es ist Zeit für Cloud-basiertes Netzwerk-Management.

Olaf Hagemann/wg



Die Visualisierung der WLAN-Abdeckung an den Unternehmensstandorten erleichtert die Suche nach Störeinflüssen.

Bild: Extreme Networks

tung in Abhängigkeit von Bedingungen und Betriebsprozessen schafft eine Umgebung, die Updates ohne Ausfallzeiten ermöglicht.

KI im Netzwerk-Management

Künstlicher Intelligenz (KI) kommt im Cloud-basierten Netzwerk-Management eine tragende Rolle zu. Zeitgemäße Lösungen verfügen über eine KI-basierte Anomalie-Erkennung, die in die Überwachung von Zustandsmetriken eingebunden ist. Sie stellt fest, wann Netzwerkknoten oder Standorte Anomalien aufweisen, die sich auf die Clients auswirken, etwa durch hohe Verbindungsausfälle oder eine geringe Kapazität. Das Netzwerk-Management nutzt daher Algorithmen zur Erkennung von Ereignismustern: Auf dieser Basis ex-

Maß an Flexibilität mitbringen, das der Digitalisierung angemessen ist. Stimmige Cloud-Bereitstellungsoptionen für das Netzwerk-Management ermöglichen die Nutzung aus der Public Cloud, der Private Cloud und selbst aus einem lokalen Rechenzentrum. Denn auch die eigene Private-Cloud-Instanz muss dabei in der Lage sein, Millionen angebundener Access Points, Switches und Router zu verwalten. Oder das Unternehmen setzt auf ein regionales Private-Cloud-Rechenzentrum (Regional Datacenter, RDC), es kann dieselben Vorteile und Funktionen wie die Public Cloud bieten. Ein privates RDC lässt sich auch innerhalb der Infrastruktur eines Partners unterbringen. Privates Hosting schließlich ist eine ideale Lösung für Ma-

Olaf Hagemann ist Director Systems Engineering DACH bei Extreme Networks.

SD-WAN mit Out-of-Band-Management

WAN der Enterprise-Klasse

Mit SD-WAN-Technik (Software-Defined Wide Area Network) wollen Unternehmen ihre Netzwerkkosten senken und den Betrieb ihrer WAN-Infrastruktur vereinfachen. Doch mit der neuen Technik sind ihre Netzwerke auch anfälliger für Ausfälle und Angriffe. Ohne ein durchdachtes Out-of-Band-Management (OOB) stehen die Verantwortlichen auf verlorenem Posten.

Die Aufgabe eines herkömmlichen WANs besteht darin, Beschäftigte einer Zweigstelle mit den im RZ gehosteten Anwendungen zu verbinden. Um eine hohe Sicherheit und zuverlässige Netzwerkanbindung zu gewährleisten, kommen in der Regel dedizierte MPLS-Verbindungen (Multiprotocol Label Switching) zum Einsatz. Die Einrichtung und Wartung eines MPLS-basierten WANs ist allerdings teuer: An jedem Standort müssen Unternehmen eine aufwändige Infrastruktur aufbauen, bestehend aus Routern, Firewalls, Controllern, Switches etc. Gleichzeitig haben sich die Anforderungen an ein Unternehmens-WAN durch Cloud Computing, mobiles Arbeiten, Web-gestützte Applikationen und dem Internet of Things (IoT) stark geändert.

Immer mehr Unternehmen denken deshalb über den SD-WAN-Einsatz zur Standortvernetzung nach, um die notwendige Flexibilität zu erreichen, den Bedarf an immer mehr Bandbreite zu decken und die Netzwerkkosten überschaubar zu halten. Nach Prognosen der Analysten von IDC soll der Markt bis 2023 um jährlich mehr als 30 Prozent auf 5,25 Milliarden Dollar wachsen. Parallel dazu haben die Marktforscher in ihrer jüngsten Studie „Network Transformation in Deutschland 2021“ festgestellt, dass hiesige Firmen, angetrieben durch geschäftliche Anforderungen, das Thema Netzwerkmodernisierung voran-

treiben: Von softwaredefinierten Architekturansätzen versprechen sie sich dank Automatisierung ein einfacheres Management sowie mehr Transparenz und damit einen besseren Überblick über das Netzwerk und dessen Performance. Denn die Komplexität und schiere Menge an Daten und Geräten lässt sich mit manuellen Ansätzen nur noch schwer beherrschen.

Intelligentes Routing

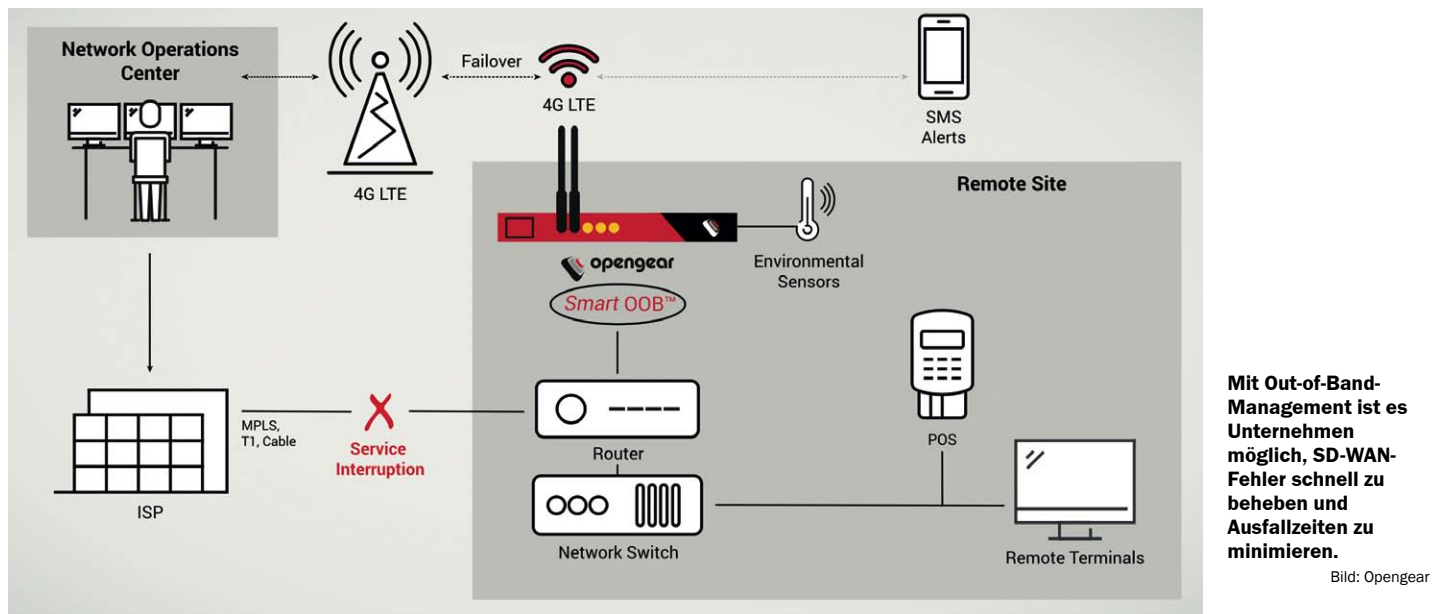
Bei aller Euphorie für das SD-WAN dürfen Unternehmen nicht übersehen, dass die „neue“ Architektur auch einige Herausforderungen mit sich bringt und ein Sicherheitsrisiko darstellen kann. Grundsätzlich ist es mit einem softwaredefinierten WAN möglich, verschiedenste Verbindungswege zentral zu verwalten und zu orchestrieren, indem man den Datenverkehr wie die Applikationen priorisiert. Der Ansatz entkoppelt die Netzwerkkontrolle von der zugrunde liegenden physischen Infrastruktur (Underlay) und macht sie direkt programmierbar. Über ein Web-Portal können Unternehmen Änderungen – beispielsweise bei der Bandbreite – für dedizierte Anwendungen vornehmen und diese flexibel und in Echtzeit erhöhen oder senken. Zudem können sie Regeln für die Priorisierung festlegen. In der Konsequenz wählt eine SD-WAN-Lösung automatisch den jeweils am besten geeigneten Pfad für die Übertragung aus – von LTE

über Breitband bis hin zu MPLS. Dank dieses intelligenten Routings laufen sicherheitskritische Daten mit hoher Priorität über das private MPLS, weniger sensible, aber bandbreitenintensive Daten hingegen über günstigere Internetverbindungen. Das heißt, ein SD-WAN nutzt Leitungskapazitäten optimal aus, erhöht so die Service-Qualität und senkt gleichzeitig die Kosten.

Demgegenüber stehen zahlreiche Risiken, die mit der neuen Technik einhergehen. In traditionellen Zweigstellen und Netzwerken laufen Router oft monatelang, ohne dass Eingriffe wie Konfigurationsänderungen oder Firmware-Updates erforderlich sind. Intelligente SD-WAN-Router sind dagegen stärker von ihrer Software abhängig und benötigen häufiger Anpassungen und Firmware-Aktualisierungen, etwa wenn der Hersteller neue Features einführt oder Bugs behebt, oder wenn das Anwenderunternehmen die Routing-Richtlinien ändert. Jedes Update stellt jedoch ein Risiko dar und kann dazu führen, dass der Router ausfällt oder nicht wieder richtig startet und in der Folge das Netzwerk lahmlegt. Zudem sind die grundlegenden Sicherheitsfunktionen eines SD-WANs für Unternehmen unzureichend – sie müssen die neue Technik in ihre bestehende Security-Infrastruktur integrieren. Allerdings haben Monitoring- und Netzwerk-Management-Tools oft Schwierigkeiten im Zusammenspiel mit dem SD-WAN und scheitern beispielsweise daran, nicht autorisierte IoT-Geräte im Netzwerk aufzuspüren. Da in einem SD-WAN häufig alle Geräte miteinander verbunden sind (Full Mesh), reicht bereits ein einziges kompromittiertes Gerät aus, damit Angreifer einen Überblick über alle Datenflüsse erhalten.

Grenzen des In-Band-Managements

Das vielleicht größte Problem stellt das In-Band-Management dar. So vereinfacht beim SD-WAN das Cloud-basierte Provisioning zwar die Bereitstellung und Konfiguration der Netzwerkausrüstung spürbar: Neue Router und Switches laden nach dem Anschluss an das Netzwerk ihre Konfiguration aus der Cloud oder von einem Server und richten sich selbstständig ein. Damit sind neue Standorte schnell angebun-



den oder neue Geräte rasch in Betrieb genommen, ohne einen Techniker vor Ort zu erfordern. Trotzdem handelt es sich beim Cloud-Provisioning letztlich immer noch um ein In-Band-Management, bei dem alle Zugriffe auf das Netzwerk vom selben Router abhängen. Beim Ausfall der Internetverbindung kann dieser aber keine neue Konfiguration herunterladen und ist auch für die IT-Abteilung nicht mehr erreichbar. Kleine Fehler wie falsche Konfigurationen verteilen sich zudem schnell im Netzwerk und können zu größeren Ausfällen führen. Ohne ein Out-of-Band-Management führen Netzwerkvorfälle deshalb schnell zu ernsthaften Unterbrechungen.

OOB ist grundsätzlich unabhängig von der Funktion und Konnektivität des lokalen Netzwerks und erlaubt den Administratoren, kritische IT-Komponenten wie Switches und Router sowie Sicherheits-Appliances wie Firewalls und Verschlüsselungs-Tools aus der Ferne und unterbrechungsfrei zu verwalten. Treten Probleme mit der Netzwerkanbindung auf, bietet OOB über Mobilfunk oder andere Optionen eine Failover-Lösung, um den ununterbrochenen Geschäftsbetrieb zu gewährleisten. Der Zugriff auf die Protokolldateien der betroffenen Geräte hilft zudem, die Hauptursachen eines Ausfalls zu identifizieren und zeitnah Wiederherstellungsmaßnahmen einzuleiten. In den allermeisten Fällen erübrigt sich dadurch der Vor-Ort-Be-

such eines Service-Technikers. Sollte er doch notwendig sein, weiß der Techniker im Voraus, welche Ersatzteile notwendig sind, um die Störung zu beheben.

Fehlerdiagnose

Der Einsatz einer OOB-Plattform bringt darüber hinaus Vorteile in Sachen Sicherheit: Einerseits lassen sich die Konsolen-Server leicht in bestehende Multi-Faktor-Authentifizierungslösungen integrieren und sind somit in den gesamten Sicherheits-Appliance-Layer eingebunden. Andererseits liefert OOB-Technik ein Protokollsystem für alle Konfigurationsänderungen und Patches – dazu zählen auch Änderungen, die man über alternative Zugriffspfade gesendet und im Security Operations Center (SOC) zum Beispiel in einer SIEM-Lösung (Security-Information- und Event-Management) gespeichert hat. Somit können die IT-Verantwortlichen überprüfen, ob das Netzwerkteam eine kritische Infrastruktur gepatcht und somit potenzielle Sicherheitslücken geschlossen hat.

Ein großer Pluspunkt ist auch das proaktive Erkennen von Fehlern in SD-WANs: Der OOB-Konsolen-Server stellt eine verschlüsselte direkte Verbindung zu wichtigen Geräten wie Routern und Firewalls her. Der schnelle und sichere Zugriff auf die Protokolldateien der betroffenen Geräte hilft nicht nur, die Hauptursachen eines Ausfalls zu identifizieren und Recovery-Maßnah-

men schnell einzuleiten: Out-of-Band-Konsolen-Server lassen sich auch so konfigurieren, dass sie kritische Geräte ordnungsgemäß herunterfahren, wenn die Temperatur im Rack zu hoch ist, die unterbrechungsfreie Stromversorgung einen Stromausfall erkennt oder die Batterieleistung unter einen Schwellenwert sinkt. Zusammen bewahrt dies Unternehmen vor schweren finanziellen Verlusten und einem Reputationsschaden nach einem Netzwerkausfall.

Erst mit OOB ist das SD-WAN sicher

Softwaredefinierte WANs helfen Unternehmen, ihre Niederlassungen günstig an das zentrale Rechenzentrum anzubinden, einen zuverlässigen Zugriff auf Cloud-Dienste herzustellen und ihren Datenverkehr geschickt über verschiedene Netzwerktechniken zu verteilen. Trotz all dieser Vorteile dürfen Unternehmen jedoch nicht vergessen, dass das SD-WAN auch einige Schwachstellen hat, die sich als großes Sicherheitsrisiko erweisen können. Mit einem smarten Out-of-Band-Management minimieren die Verantwortlichen alle Fehlerquellen, können das Netzwerk im Notfall aus der Ferne wieder in Gang bringen und profitieren dabei von der Flexibilität und den Kostenvorteilen eines SD-WANs.

Dirk Schuma/wg

Dirk Schuma ist Sales Manager Europe bei Opengear.

Multi-Cloud-Architekturen

Resilienz und Innovation

Viele Unternehmen nutzen zwei oder sogar mehr Cloud-Infrastrukturanbieter parallel, beispielsweise die bekannten Hyperscaler. Das stärkt die Resilienz der Geschäftsprozesse und im Idealfall auch die Innovationsfähigkeit – vorausgesetzt, die Unternehmen achten dabei auf den sicheren Cloud-Betrieb.

Die letzten zwölf bis 18 Monate haben dem Cloud Computing in der deutschen Wirtschaft einen deutlichen Schub gegeben. Laut dem aktuellen Cloud Monitor 2021 von Bitkom Research setzen aktuell acht von zehn Unternehmen die Cloud ein. Parallel dazu verbreitet sich die Multi-Cloud. Bereits in der Vorjahresstudie gab ein Drittel der befragten Unternehmen an, ein Multi-Cloud-Konzept zu nutzen. Multi-Cloud-Computing bedeutet: Ein Unternehmen nutzt mindestens zwei Public Clouds, meist die Lösungen der großen Hyperscaler. Damit überträgt es einen großen Teil des Betriebsaufwands an Spezialisten und entlastet das IT-Budget. Zudem bieten die Hyperscaler den einfachen Zugriff auf innovative Techniken wie Industrial IoT, Data Analytics, Machine Learning, Sprachverarbeitung sowie andere KI-Verfahren. Diese sind vor allem für mittelständische Unternehmen nur per Cloud erreichbar. Häufig führt der Einsatz dieser Techniken zu einem Multi-Cloud-Szenario.

Ein realitätsnahes Beispiel aus der produzierenden Industrie: Ein größerer Mittelständler mit mehreren Standorten in Europa will sämtliche Fertigungsanlagen per Industrial IoT vernetzen. Dafür stattet er die Anlagen mit Sensoren aus und nutzt die ermittelten Daten für eine Anomalie-Erkennung. Dies erfordert auf Seiten der Cloud mindestens drei Komponenten: erstens eine IoT-Plattform für den Anschluss der Maschinen an allen Standorten; zweitens eine Analytics-Anwendung, um die Daten aufzubereiten und in Dashboards zu visualisieren;

drittens eine KI-Lösung, die lernfähige Algorithmen anbietet, um Anomalien frühzeitig zu erkennen. Generell bieten alle großen Cloud-Provider die dafür notwendige Infrastruktur. Doch bei Themen wie IoT oder KI setzt jeder Anbieter unterschiedliche Schwerpunkte. Letztlich müssen die Unternehmen sich die technischen Rahmenbedingungen anschauen und die Clouds in Pilotprojekten vergleichen. Die Konsequenz kann sein, Leistungen von drei Providern zu beziehen. Denn letztlich ist es unerheblich, ob die geeignete Lösung aus einer Hand oder drei Händen kommt.

Gretchenfrage: Was ist mit der Datensicherheit?

Mit einer Multi-Cloud entstehen neue Sicherheitsfragen. Zwar liefern alle Anbieter Tools, um Daten zu schützen, doch diese erfordern spezifisches Know-how. Hier entsteht in vielen Unternehmen die Gefahr der Überforderung. Es ist bereits schwierig, mit der Weiterentwicklung nur eines einzelnen Providers Schritt zu halten. Mit jedem weiteren Anbieter steigen Komplexität und Risiko. Die Administrationsteams müssen jeden neuen sicherheitsrelevanten Service optimal auf Security und Verfügbarkeit trimmen.

Sicher betrieben stärken Multi-Cloud-Szenarien die Business Resilience. Zwar bieten alle Hyperscaler und die Mehrheit der kleineren Provider georedundante Rechenzentren als Service an. Katastrophenszenarien wie Großbrände, großflächige Stromausfälle, Überflutungen und Terroran-

schläge sollten also kein Problem sein – eigentlich. Doch Murphy's Law kann kräftig zuschlagen: Es gab in der jüngsten Vergangenheit vollständig niedergebrannte Rechenzentren und kurze Störungen mit weltweiten Folgen. Solche Probleme setzen die gesamte Infrastruktur eines Unternehmens über Stunden oder Tage außer Gefecht. Hier bietet sich die Multi-Cloud als Fallback-Lösung an.

Doch es gibt noch weitere Aspekte, die für eine Multi-Cloud sprechen. Ein typisches Kriterium ist die maximale Netzwerklatenz. Hier machen ein paar hundert Kilometer weiter vom oder näher am Produktionsstandort durchaus einen Unterschied. Die Verteilung der Cloud-Region kann für Anwendungen im Industrial IoT ein K.o.-Kriterium sein, und es ist wirtschaftlich sinnvoll, den besten Provider zu buchen. In vielen dieser Szenarien kommt außerdem noch eine vierte Komponente hinzu: Edge Computing mit Rechenkapazität vor Ort, am „Rand“ des Netzwerks. IoT-Anwendungen analysieren und speichern häufig die Daten zehntausender Sensoren. Dabei entsteht ein enormer Datenstrom, den man nicht ungefiltert in die Cloud senden kann. Es ist hilfreich, wenn der Cloud-Provider passende Infrastruktur und Software für die Edge anbietet – das senkt den Entwicklungsaufwand für die Lösung.

Ein weiterer Aspekt schließlich sind die Kosten. Auch hier müssen die Unternehmen abwägen: Auf der einen Seite bedeutet der Einsatz mehrerer Provider, dass die Kostenverhandlungen einfacher sind – das Unternehmen kann jederzeit wechseln. Verteilen sich die Umsätze über mehrere Provider, erreicht es womöglich bei keinem den Bereich, in dem individuelle Preisabsprachen möglich sind.

Zielkonflikt

Auch aus strategischer Sicht gibt es beim Cloud Computing einen Zielkonflikt: Einerseits soll die Cloud die Bereitstellung vereinfachen, andererseits müssen die IT-Services aber leicht von Anbieter A zu Anbieter B umziehen können. Ein möglicher Ausweg ist der Verzicht auf die (Micro-) Services der Hyperscaler. Diese proprietären Dienste bewirken einen Anbieter-Lock-

Marktübersicht SD-WAN-Lösungen

Anbieter	Web
Aryaka	aryaka.com
Barracuda	barracuda.com
Cato Networks	catonetworks.com
Cisco	cisco.com
Citrix	citrix.com
Ecessa	ecessa.com
Ericsson (Cradlepoint)	cradlepoint.com
Fatpipe Networks	fatpipeinc.com
Fortinet	fortinet.com
HPE (Aruba)	arubanetworks.com
HPE (Silver Peak)	silver-peak.com
Huawei	huawei.com
Infiot	infiot.com
Infovista	infovista.com
Juniper	juniper.net
NetFoundry	netfoundry.io
Nokia (Nuage Networks)	nuagenetworks.net
Open Systems	open-systems.com
Oracle	oracle.com
Palo Alto Networks	paloaltonetworks.com
PDI (Cybera)	pdisoftware.com
Peplink	peplink.com
Riverbed	riverbed.com
Teldat	teldat.com
Versa	versa-networks.com
VMware	vmware.com

Die wichtigsten SD-WAN-Anbieter. Quellen: Gartner's Magic Quadrant for WAN Edge Infrastructure, LANline-Recherche. Der SD-WAN-Markt soll laut Research and Markets von 1,4 Milliarden Dollar 2020 bis 2030 auf stolze 43 Milliarden Dollar anwachsen.

in und erschweren den Umstieg auf andere Provider. Die Alternative sind Container. Sie benötigen einen höheren Administrationsaufwand, lassen sich aber leichter zu einem anderen Provider verschieben. Rückt ein Unternehmen strategisch die Unabhängigkeit von einem einzelnen Provider in den Vordergrund, empfiehlt sich ein Cloud Broker als Abstraktionsschicht zwischen

Nutzer und Cloud. Vorteile sind Interoperabilität und Portabilität, doch es gibt auch einen Nachteil: Die Unternehmen erhalten nur einen Teil der Möglichkeiten und neue Technologien tauchen bei den Brokern nur mit Verzögerung auf.

Für einen echten Multi-Cloud-Ansatz ohne Broker müssen Unternehmen einige organisatorische und technologische Voraussetzungen erfüllen. Anders können sie die Vorteile nicht erzielen. Dafür müssen im Management und in den IT-Teams die folgenden sechs Themen auf die Agenda:

Strategie: Unternehmen benötigen eine anbieteragnostische Cloud-Strategie. Sie sollte alle notwendigen Maßnahmen treffen, damit ein Unternehmen den Anbieterwechsel rasch und ohne Schwierigkeiten bewältigen kann.

Governance: Die Multi-Cloud bringt zusätzliche Steuerungsaufgaben. So sollte das Management jedem Anbieter Richtlinien zuordnen, beispielsweise zur Kostenkontrolle, zu den Sicherheitsanforderungen und der Bereitstellung sowie der Service-Levels.

Identity- und Access-Management (IAM): Jeder Cloud-Provider bietet eigene IAM-Routinen, was die Komplexität erhöht. Sinnvoll ist ein übergreifendes IAM: Es sorgt dafür, dass es unternehmensweit einheitliche Zugriffsrechte auf alle IT-Ressourcen gibt, inklusive der Cloud.

Security-Information- und Event-Management (SIEM): Die IT-Teams müssen die

gesamte Infrastruktur inklusive der Clouds überwachen. Empfehlenswert ist eine moderne SIEM-Lösung, die eine ganzheitliche Sicht auf die IT-Sicherheit erlaubt. Sinnvoll sind auch regelmäßige Security Audits, um Lücken im Sicherheitskonzept aufzudecken.

Automatisierung: Auch für die Automatisierung des Betriebs bietet jeder Hersteller eigene Tools. Und ähnlich wie bei Identitäten ist es deutlich sinnvoller, ein übergreifendes Automatisierungswerkzeug zu benutzen, sodass der Aufwand im Rahmen bleibt.

Landing Zones: Die Anforderungen an die Infrastruktur bilden die Grundlage für die Definition von Landing Zones. Damit können Unternehmen sicher konfigurierte Cloud-Umgebungen ausrollen, die funktionsgleich und an den jeweiligen Provider angepasst sind.

Die Multi-Cloud ist nicht zum Nulltarif zu haben. Sie bietet Kostenvorteile und senkt die Komplexität der IT-Infrastruktur, stellt aber höhere Anforderungen an die IT-Governance und das Know-how der IT-Fachkräfte. Doch im Ergebnis steht für IoT- oder KI-Technik eine größere Palette an Lösungen bereit. Damit fördert die Multi-Cloud nicht nur die Resilienz eines Unternehmens, sondern auch seine Innovationsfähigkeit.

Helmut Weiss/wg

Helmut Weiss ist Enterprise Cloud Architect bei Skaylink.

News

Fortinet ergänzt Sicherheitsportfolio

Security-Services für Endpunkte, Netzwerke und die Cloud

Fortinet erweitert seine FortiCare und FortiGuard Security Services: Mit den neuen FortiTrust Security Services bietet man eine benutzerbasierte Lizenzierung über alle Netzwerke, Endpunkte und die Cloud hinweg, die traditionell in Silos untergebracht waren. Die Einführung umfasse zunächst Zero Trust Network Access (ZTNA)

mittels FortiTrust Access und die Identitätsüberprüfung per FortiTrust Identity. FortiTrust Access bietet ZTNA-Dienste mit Agenten und Cloud-basierter Orchestrierung. Alle Benutzer und Geräte, die auf ein Netzwerk und Anwendungen zugreifen wollen, werden laut Anbieter eindeutig identifiziert und klassifiziert, unabhängig

davon, ob sich die Benutzer und ihre Geräte im Netzwerk oder außerhalb befinden oder die Anwendungen lokal oder in einer Cloud-Umgebung laufen. FortiTrust Identity wiederum liefere als wichtige ergänzende Abicherungsmaßnahme eine Cloud-basierte Multi-Faktor-Authentifizierung (MFA) zur Identitätsüberprüfung.

Alle Sicherheitsdienste sind laut Fortinet-Angaben auch über Partner erhältlich und bieten Channel-Partnern so die Möglichkeit, ihr Geschäft und ihr Angebot auszubauen. Weitere Service-Optionen für SASE (Secure Access Service Edge) und CASB (Cloud Access Security Broker) seien in Planung.

wg

Do it yourself vs. Managed Service

SASE verwalten per Co-Management

Im Netzwerkbereich geht der Trend klar in Richtung SASE (Secure Access Service Edge): Anbieter schnüren Pakete aus SD-WAN-Services (Software-Defined WAN) und Security-Funktionen auf Cloud-Basis. Eine SASE-Blaupause, die auf jedes Unternehmen passt, gibt es allerdings nicht. Zu unterschiedlich sind die Herausforderungen, denen sich Unternehmen in ihren jeweiligen Branchen wie auch intern gegenübersehen. Bereits bei der Implementierung müssen SASE-Anbieter daher Flexibilität bieten, um den Anforderungen von größtmöglicher Verwaltungshoheit bis hin zu kleinstmöglichem Wartungsaufwand gerecht zu werden.

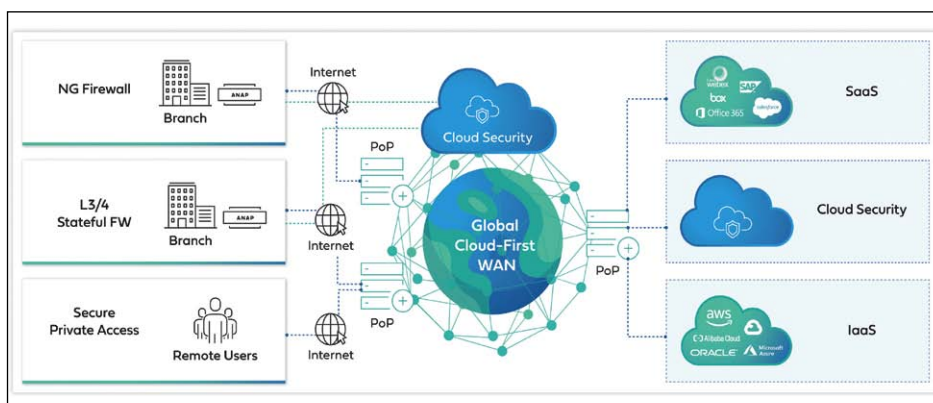
Von Erpressung bis Industriespionage: Die Unternehmensnetze von heute sind einer stetig steigenden Bedrohungslage ausgesetzt. Dieser Status quo bringt neue Ansätze und Trends hervor – einer davon ist Secure Access Service Edge (SASE). Mit dem Ziel, eine Infrastruktur zu schaffen, welche die Sicherheits- und die Performance-Anforderungen eines digitalen Geschäftsbetriebs gleichermaßen erfüllen kann, setzt SASE auf die Bündelung von Security- und Netzwerkfunktionen. Zurecht könnte man an dieser Stelle entgegenhalten, dass es für die Erfordernisse moder-

ner Unternehmensnetze doch schon eine lang bewährte Lösung gibt: MPLS (Multi-protocol Label Switching). Doch trotz schneller Übertragung und hoher Sicherheit beim Datentransfer kann dieses nicht länger allen Unternehmensanforderungen gerecht werden. Denn die Datenströme in modernen Unternehmen haben sich stark gewandelt: Das Volumen steigt stetig an, hinzu kommen vielfältigste Datentypen und eine zunehmende Anzahl an Access Points. Größere Angriffsflächen und ein erheblicher Mehraufwand bei der Installation und Wartung sind die Folge.

Genau an diesem Punkt setzt das SASE-Konzept an, das Gartner 2019 in dem Artikel „The Future of Network Security Is in the Cloud“ entwickelte. Es bezeichnet zwar keine neuen, innovativen Security- oder Netzwerkfunktionen, beschreibt jedoch eine Netzwerkarchitektur, die SD-WAN-Funktionen mit Cloud-nativen Sicherheitsfunktionen konsolidiert, um den Nutzen bereits vorhandener Funktionen zu steigern und deren Management und Instandhaltung zu vereinfachen. Dazu implementieren Hersteller SASE hauptsächlich als „Heavy Cloud“-Ansatz, was bedeutet, dass der Großteil der Netzwerk- und Sicherheitsressourcen in der Cloud zur Verfügung steht. Im Gegensatz zum „Heavy Branch“-Modell, bei dem der Schwerpunkt auf der Bereitstellung vor Ort liegt, ist also nur noch ein Minimum an Komponenten vor Ort (on-premises) vorhanden.

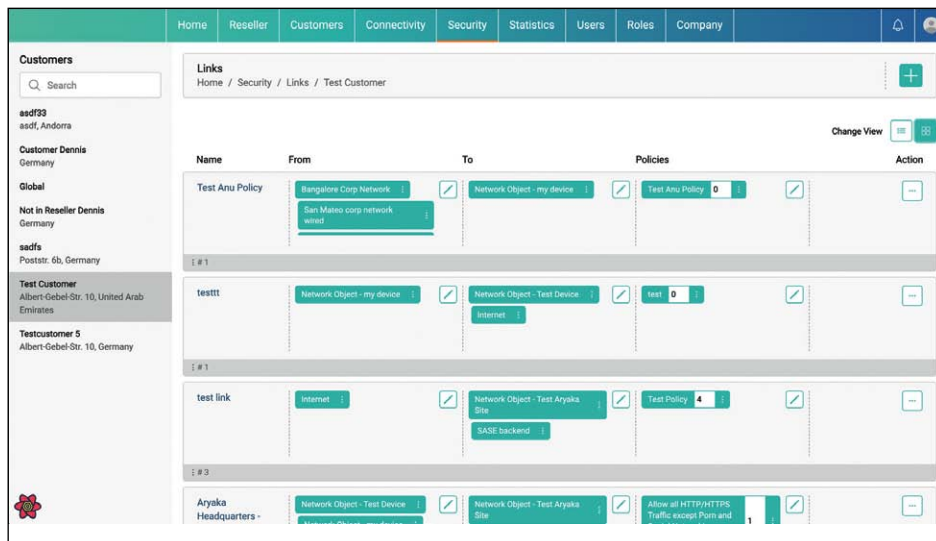
Eine moderne SASE-Architektur ermöglicht Unternehmen eine effiziente Verbindung verschiedener Standorte, indem der Netzzugang über global verteilte Zutrittspunkte (Points of Presence, POPs) erfolgt. Dies macht ein Zurückgreifen auf Service-Provider und Peering obsolet. Das Tor zur SASE-Welt stellt das Teilnehmernetzgerät (Customer Premise Equipment, CPE) dar. Es liefert die erforderlichen WAN-Services und kann gleichzeitig weitere benötigte Anwendungen – beispielsweise eine Next-Generation Firewall – vor Ort hosten.

Bei der Implementierung und Wartung einer solchen Lösung bestehen zwei Möglichkeiten: Unternehmen können das Netz in Eigenregie aufsetzen und verwalten oder den gesamten Prozess als Managed Service an einen Drittanbieter auslagern. Welche der beiden Varianten zu bevorzugen ist, hängt von den Gegebenheiten im Unternehmen ab. Welche Anforderungen stellen beispielsweise Branchenvorgaben und Regularien an das Unternehmen? Welche Kompetenzen sind intern vorhanden? Und verfügen die hauseigenen Experten über die benötigten Kapazitäten, sich um das SASE-Netz zu kümmern? Nicht selten gilt es, dabei den Aufwand und die Verwaltungshoheit gegeneinander abzuwägen. Zweifelsohne benötigt ein reibungsloser Geschäftsbetrieb eine zuverlässige Sicher-



Aufbau einer SASE-Infrastruktur im schematischen Überblick.

Bild: Aryaka



Per Co-Management lassen sich Verwaltungsaufgaben – im Bild das Management der Security-Policies – zwischen Anwenderunternehmen und SASE-Provider aufteilen.

Bild: Aryaka

heitsstrategie. Gleichzeitig gestaltet sich jedoch der Versuch, bei der Konfiguration, Nutzung und Aktualisierung aller Bestandteile einer fortschrittlichen Security-Lösung den Überblick zu behalten, als Mammutaufgabe – nicht zuletzt angesichts der konstanten Weiterentwicklungen in der IT sowie der zunehmenden Sicherheitsbedrohungen, die IT-Teams an ihre Grenzen bringen. Immer mehr Unternehmen entscheiden sich bereits im Netzwerkbereich – zum Beispiel im Kontext der SD-WAN-Technik – für eine Auslagerung als Managed Service, die sich durchaus positiv auf die Geschäftsgilität und den manuellen Verwaltungsaufwand auswirkt. Nun kommt analog dazu die Auslagerung des Security-Bereichs in Mode – angesichts der dadurch ermöglichten Entlastung der IT-Abteilungen mehr als naheliegend. Doch bei Security handelt es um einen hochsensiblen Bereich, den Unternehmen häufig nur ungern in fremde Hände geben. Gerade in hochregulierten Branchen gilt es, teils sehr spezifische Anforderungen zu erfüllen. So erfordern beispielsweise die strengen Regulierungen in der Finanzbranche die Einhaltung außergewöhnlich hoher Security-Standards. Ähnliches gilt für die Fertigungsbranche, in der Systeme gerade im Kontext der smarten Fabrik wertvollste Prozess- und Produktdaten übertragen und verarbeiten. Dass Unternehmen wie diese ihre Sicherheitsarchitektur umfassend

kontrollieren und auch lückenlos die Hoheit über sensible Daten behalten wollen, ist nicht überraschend. So bevorzugen zumindest manche von ihnen zunächst, ihre SASE-Lösung à la „do it yourself“ einzuführen und zu managen: In der neuesten Ausgabe von Aryakas jährlichem „State of the WAN“-Reports zeigt sich, dass zwar für 71 Prozent der befragten Unternehmen eine SASE-Implementierung als Managed Service eine Option wäre, knapp ein Fünftel (18 Prozent) jedoch die Einführung und Nutzung in Eigenregie präferiert.

Kein Entweder-oder

Für SASE-Hersteller lautet die Devise also Flexibilität, um den vielfältigen Anforderungen der Unternehmen gerecht zu werden. Konkret kann dies beispielsweise in Form der sogenannten „Co-Managed Services“ erfolgen: Während der Anbieter Netzwerk- und Sicherheits-Stack als Managed Services zur Verfügung stellt, behält der Kunde die Freiheit, über ein eigenes Co-Management-Portal individuelle Anpassungen vorzunehmen und weiterhin sämtliche Netzwerk- und Sicherheitsparameter selbst zu bestimmen. Geführte Workflows bilden dabei eine Art Leitplankensystem, um Konfigurationsfehler zu vermeiden und damit einen gewissen Qualitätsstandard zu sichern. Auf diese Weise ist jede Abstufung eines Managed Services flexibel umsetzbar – auch ein vollständiger

Managed Service durch den SASE-Anbieter ist möglich. In diesem Fall wartet der Hersteller nicht nur mit der Bereitstellung von Konfigurationen auf, sondern stellt dem Unternehmen zudem seine IT-Sicherheitsexperten quasi als erweiterte IT-Abteilung zur Verfügung.

Gerade im Bereich der Sicherheit ist der flexible Ansatz des Co-Managements aufgrund der im Vergleich zu Netzwerkkonfigurationen je nach Unternehmen sehr individuellen Ansprüche von besonderer Bedeutung. Die dynamischen Gegebenheiten erfordern dort stetige Überprüfungen und Anpassungen, um der jeweiligen Bedrohungslage angemessen begegnen zu können. Entsprechend komplex gestaltet sich auch die Erstimplementierung der Sicherheitskomponenten, weshalb es – gänzlich unabhängig vom zukünftig geplanten Umfang der Nutzung des Managed Services – ratsam ist, diese durch den SASE-Anbieter vornehmen zu lassen.

Schlussendlich lässt sich die Frage, welcher Implementierungsweg – Managed Service, DIY oder eine Kombination aus beiden – zielführender ist, nicht pauschal beantworten. Vielmehr gilt es, bereits vor Beginn der Implementierung genau abzuwägen, welche Ziele das Unternehmen erreichen möchte und welche Voraussetzungen gegeben sind: Gibt es im Unternehmen Spezialisten, die über die für Betrieb und Wartung eines SASE notwendige Expertise verfügen? Wie viel Abstimmungsaufwand ist bereits heute zwischen unterschiedlichen Herstellern erforderlich, um Probleme zu beheben? Verfügt das Unternehmen über hohe Transparenz bezüglich seiner bisherigen Infrastruktur? Und würde ein gemanagter Dienst Risiken tatsächlich reduzieren oder diese vielleicht sogar erhöhen? Indem Unternehmen Fragen wie diese im Vorfeld klären, können sie die optimale Implementierungsmethodik ermitteln – idealerweise gemeinsam mit dem SASE-Anbieter. Dadurch sorgen sie dafür, dass die Einführung der Netzwerkinfrastruktur genauso passgenau erfolgt wie die spätere Nutzung. Hugo Vliegen/wg

Hugo Vliegen ist Vice President Product Management bei Aryaka.

Netzwerkzubehör/RZ-Ausstattung



FICONET systems GmbH
Neue Wildenauer Str. 7
08237 Steinberg

Tel.: 037462/6360-0, Fax: 037462/6360-699
E-Mail: sales@ficonet.de
Homepage: www.ficonet-shop.de

Der LWL-Spezialist

Hersteller & Distributor eines kompletten LWL Sortiments: Spleißgeräte, OTDR, Video Inspection Probes und sonstige LWL Messtechnik, LWL Universal-, Außen-, Mikro-, FTTH Drogkabel, FTTH Komponenten, 19" Spleißboxen und LWL Wandverteiler, LWL Muffen, LWL Reinigungsgeräte und Zubehör, Kabelgleitmittel, LWL Stecker & Kupplungen, PLC Splitter, FWD Komponenten, Realisierung von Sonderfertigungen durch eigene LWL Konfektion, Werkzeuge für LWL-, Koax- und strukturierte Verkabelung, optische Transceiver (SFP, SFP+, QSFP+, QSFP28, etc.), AOC & DAC Kabel, Industrial Ethernet Switches & Medienkonverter, Netzwerk- & Serverschränke, strukturierte Verkabelungssysteme **Vermietung, Distribution und Service bei Spleiß- und Messtechnik, breites Lagersortiment + Top Service + höchste Verfügbarkeit**



Avanis GmbH
Thomas Passlack, Geschäftsführer
Meisenstraße 79a, **33607 Bielefeld**

Tel.: 0521/26012-0, Fax: 0521/26012-12
E-Mail: info@avanis.de
Homepage: www.avanis.de

Spezialdistributor im Netzwerkbereich mit breitem Markensortiment: Medienkonverter, Switches, Industrial Ethernet, VDSL/Breitband, Transceiver, WLAN, Ortung, Software, IP-Kameras, IT-Security, Kabel, Zubehör, Schulungen und Seminare. Avanis bietet: Hohe Qualitätsstandards, benutzerfreundliche Produkte und kundenorientierte Beratung.



NEFTEC
Herr Fred Tegtmeyer
Zeisigweg 31
50829 Köln

T: +49 221 88 88 8-765 • F: -764
E: info@neftec.de • www.neftec.de

Service: Qualitativ hochwertige passive Kupfer- und LWL Komponenten für FTTH-, LAN- und Telekommunikations-Anwendungen. Individuelle kundenspezifische Sonderkonstruktionen wie auch Standard Komponenten: Adapter-Patchkabel, Spleißboxen, Faser-/Kabelpigtails APC, MTP usw runden unser Lagersortiment ab.



ServiceNet EDV-Vertriebsgesellschaft GmbH
Provinzialstraße 40
53859 Niederkassel

Tel. 0228/7228-0, Fax: 0228/7228-199

E-Mail: info@lichtleiterkabel.com

Homepage: www.lichtleiterkabel.com

Ihr Spezialist für LWL-Kabel und Sonderkonfektionen. Anschlussfertige LWL-Kabel in jeder benötigten Ausführung, mit allen Steckern (LC, SC, ST, FC, DIN, E2000®, MTP®/MPO, etc.) in jeder gewünschten Länge. Datenkabel in Standardlängen (Kupfer bis 100 m/Glasfaser bis 500 m) sofort ab Lager lieferbar.



IT-BUDGET GmbH
Mike Spormann,
Senior Account Manager
Nassaustraße 12,
65719 Hofheim

Tel. 06122/92789-0, Fax: 06122/92789-20

E-Mail: m.spormann@it-budget.de

Homepage: www.it-budget.de

Distributor und Hersteller für Serverschränke, 19"-Verteiler, Datenkabel (LWL, Kupfer), Stromverteilung/19"-Speziallösungen für Industrie (Schutzgrad), Büro (SILENCE RACK)/Montageservice für Schrankaufbau und Bestückung, RZ-Montagen/Individuelle Lösungen nach Kundenwunsch: Schränke & Gehäuse, Datenkabel, Steckdosenleisten

Shop-Rabatt mit Kupon LAN2021



Dätwyler IT Infra GmbH
Auf der Roos 4-12,
65795 Hattersheim

Tel. +49 (0)6190 8880-0, Fax: +49 (0)6190 8880-80

E-Mail: info.itinfra.de@datwyler.com

Homepage: www.ITinfra.datwyler.com

Dätwyler ist Entwickler, Hersteller und – gemeinsam mit kompetenten Partnern – Komplettanbieter von hochwertigen **IT-Infrastrukturlösungen für Rechenzentren, Glasfasernetze (FTTx) und intelligente Gebäude**, inklusive Software und Services.



CobiNet Fernmelde- und Datennetzkomponenten GmbH

Uwe Tanner

Robert-Bosch-Str. 33, **68542 Heddeshheim**

Tel.: 06203/4900-0, E-Mail: info@cobinet.de

Homepage: www.cobinet.de

Entwickler, Hersteller und Komplettanbieter von Fernmelde-, Datennetz-, LWL-Komponenten u. -systemen wie LSA-/LSA-HD®-Leisten, Verteiler, Patchfelder/-kabel, Datenschränke/-dosen/-kabel, Spleißbox, LWL-/Consolidation-Point-Kabel, vorkonfekt. Kabel, strukt. Verkabelung, Planungsunterlagen/Planung, Seminare.

Rosenberger

Rosenberger-OSI GmbH & Co. OHG

Optical Solutions & Infrastructure

Endorferstraße 6, **86167 Augsburg**

Tel. 0821/24924-0, Fax: 0821/24924-929

E-Mail: info-osi@rosenberger.com

Homepage: www.rosenberger.com/osi

Seit 1991 gilt Rosenberger OSI europaweit als Experte für faseroptische Verkabelungs- und Servicelösungen für Datacom, Telecom und Industrie. Neben der Entwicklung und Herstellung des breiten Portfolios an LWL- und Kupferverkabelungssystemen, bietet Rosenberger OSI eine Vielzahl an Services wie Planung, Installation und Instandhaltung von Verkabelungsinfrastrukturen an.



LWL-Sachsenkabel GmbH
Hauptstraße 110
09390 Gornsdorf

Tel.: +49 (0)3721 39 88-0

E-Mail: info@sachsenkabel.de

Homepage: www.sachsenkabel.de

Die LWL-Sachsenkabel GmbH steht für mehr als 25 Jahre Kompetenz in Glasfaser. Basierend auf langjähriger Erfahrung und höchsten Qualitätsansprüchen entwickelt und fertigt Sachsenkabel leistungsfähige sowie wirtschaftliche Verkabelungssysteme für Rechenzentren. Unser Team von Experten unterstützt Sie bei allen Herausforderungen, von der Planung über die Implementierung bis zum Betrieb Ihres Rechenzentrums. So entstehen maßgeschneiderte Kundenlösungen die Ihnen zwei entscheidende Faktoren garantieren: absolute Betriebs- und Zukunftssicherheit.



„Sie brauchen Bandbreite – wir liefern. Als erfahrener Spezialist für LAN, Telekommunikation und FttX bieten wir Ihnen neben Glasfaser- und Kupferkabeln, Spleißboxen, Patchkabeln, Spleißzubehör und Gehäusetechnik auch Sonderlösungen für alle Bereiche. **Wir beraten Sie gern, individuell und unabhängig.**“

Rheinland Daten- und Netzwerktechnik GmbH & Co. KG

Ramona u. Torsten Bohlmann

Bendenweg 79, D-53902 Bad Münstereifel

Tel.: 02253-93245-82, Fax: 02253-93245-84

Mobil: 0157-77808957

E-Mail: info@rdun.de

Web: www.rdun.de



proemtor ist Ihr Partner für Zubehörlösungen im DataCenter.

Wir sind Spezialist in den Bereichen aktive und passive Steckdosenleisten (PDU's) und Netzwerkschränke mit eigenen Produkten.

proemtor bietet innovative Technik für individuelle Lösungen.

Mehr Info's finden Sie auf **www.proemtor.de** und fragen Sie uns am **Telefon 02645/2070** oder **02389/7799042**

Serverschränke



serverschrank.de
netzwerkschrank.de
Nassaustraße 12, **65719 Hofheim**
Tel. 06122/92789-0, Fax: 06122/92789-20
E-Mail: info@serverschrank.de
Homepage: www.serverschrank.de

Das Beschaffungsportal serverschrank.de / netzwerkschrank.de bietet die größtmögliche Übersicht über die Produkte und Anbieter von 19"-Technik – aber auch 10" und 21"-Technik – in Deutschland, kombiniert mit einem möglichst einfachen Beschaffungsablauf. Vorteile für Nutzer: + größte Übersicht und Auswahl zu Netzwerk-, Serverschränken, Datacentern, Containments + einfache Konfiguration des oder der benötigten Racks + herstellerunabhängige Beratung und Angebotserstellung durch ausgebildete Techniker + zusätzlich direkte Kontaktmöglichkeit zu Herstellern und Importeuren + herstellerübergreifende Montage-Dienste als Vormontage (Off-Site) oder am Verwendungsort (On-Site) + klare, leicht kalkulierbare, einheitliche Versandkonditionen + flexible Zahlungsmodelle
Shop-Rabatt mit Kupon LAN2021

Verkabelungsspezialisten



ACOME GmbH

Herr Alfred Jansen, Vertriebsleiter

Eutelis-Platz 1, **40878 Ratingen**

Tel.: 02102/30975-11, Fax: 02102/30975-50

E-Mail: Vertrieb@acome.de

Homepage: www.acome.de

Service: Sichere und wirtschaftliche Verkabelungssysteme, Glasfaser- und Kupferkabel für Daten- und Telekommunikation



bda connectivity GmbH

Herborner Str. 61a

35614 Asslar

Tel. 06441-384520, Fax: 06441-3845299

E-Mail: info@bda-c.com

Homepage: www.bda-connectivity.com

Seit mehr als 60 Jahren fertigen wir Spezialkabel, die auf das jeweilige Anwendungsgebiet optimiert sind, z.B. RG-Kabel, BK-Kabel, 50-Ohm-Kabel, Sat-Kabel, Videokabel, Lautsprecherleitungen, Diodenleitungen und Mikrofonkabel. Unsere besondere Stärke sind Kabel nach individuellem Kundenwunsch.



Dätwyler IT Infra GmbH
Auf der Roos 4-12,
65795 Hattersheim

Tel. +49 (0)6190 8880-0, Fax: +49 (0)6190 8880-80

E-Mail: info.itinfra.de@datwyler.com

Homepage: www.ITinfra.datwyler.com

Dätwyler ist Entwickler, Hersteller und – gemeinsam mit kompetenten Partnern – Komplettanbieter von hochwertigen **IT-Infrastrukturlösungen für Rechenzentren, Glasfasernetze (FTTx) und intelligente Gebäude**, inklusive Software und Services.



CobiNet Fernmelde- und Datennetzkomponenten GmbH

Uwe Tanner

Robert-Bosch-Str. 33, **68542 Heddeshheim**

Tel.: 06203/4900-0, E-Mail: info@cobinet.de

Homepage: www.cobinet.de

Entwickler, Hersteller und Komplettanbieter von Fernmelde-, Datennetz-, LWL-Komponenten u. -systemen wie LSA-/LSA-HD®-Leisten, Verteiler, Patchfelder/-kabel, Datenschränke/-dosen/-kabel, Spleißbox, LWL-/Consolidation-Point-Kabel, vorkonfekt. Kabel, strukt. Verkabelung, Planungsunterlagen/Planung, Seminare.



Sommer Cable GmbH
Humboldtstraße 32–36,
75334 Straubenhardt

Tel. 07082/49133-0, Fax 07082/49133-11
E-Mail: info@sommercable.com
Homepage: www.sommercable.com
Intelligente Verkabelungs- & Installationslösungen.
Modulare, kundenspezifische **Verteilssysteme** (Rack-, Tisch-, Boden- & Wandintegration) für **Audio-/Video-/Netzwerk- & Medientechnik**. CPR-Meterware, Hybridleitungen, zertifizierte Steckverbinder, Trunk- und Anschlusskabel, Elektronik-Komponenten uvm.

MALINOWSKI GEBÄUDETECHNIK

Wir sind der Elektrohandwerksbetrieb mit Ausrichtung auf die IT-Branche, wir kümmern uns ausschließlich um das passive Netz, keine Switches, APs etc.
Wir installieren Netze in Kupfer- und Glasfaser, Strom und Licht kommt auch noch dazu, alles aus einer Hand.
Wir suchen die Zusammenarbeit mit IT-Firmen zwecks Kooperation und Durchführung gemeinsamer Projekte.

Malinowski Gebäudetechnik GmbH
Richard-Byrd-Strasse 43 50829 Köln
Tel. 0221/592281 Fax 0221/592274
www.malinowski.de info@malinowski.de



tso GmbH
Hermann-Köhler-Str. 13,
58553 Halver, Tel.: 02353/66987-0,
Fax: 02353/66987-29

E-Mail: info@tso-gmbh.de · Homepage: www.tso-gmbh.de
Wir sind die Experten für Spleiß- und Messgeräte-technik. Als autorisierter Vertriebspartner von Sumitomo, VIAVI Solutions, Fluke Networks, ITW und Miller Tools bieten wir neben dem Verkauf der Gerätetechnik auch Reparatur- und Kalibrierdienstleistungen, sowie LWL-Schulungen online oder vor Ort an der tso Akademie in Frechen an.

Netzwerkanalyse



Softing IT Networks
Richard-Reitzner-Allee 6,
85540 Haar, E-Mail:
info.itnetworks@softing.com

Wir sind Hersteller von Test- und Messgeräten zur Leistungsqualifizierung, Zertifizierung und Dokumentation komplexer IT-Verkabelungssysteme.

Wir optimieren mit unseren Messlösungen für Kupfer- und Glasfasernetze Ihre täglichen Arbeitsabläufe. Die handlichen und einfach zu bedienenden Geräte sind äußerst robust und liefern hochgenaue Messergebnisse.

Wir bieten kompetenten Support und zukunftsichere Lösungen für jedes Budget.

Weitere Informationen hier: itnetworks.softing.com oder rufen Sie uns an: **089/45 656 660**. Wir freuen uns auf Sie!

VIAVI Solutions Deutschland GmbH

Monica Iordache, Marketing EMEA
Arbachtalstr. 5, **72800 Eningen u.A.**
Tel. 07121/86-1297

E-Mail: Monica.Iordache@viavisolutions.com
Homepage: www.viavisolutions.de

VIAVI ist ein führender Anbieter von Netzwerktest-equipment, Monitoring und Assurance für LWL-, Kupfer- und Mobilfunk-Netze. VIAVI-Lösungen liefern Transparenz über physische, virtuelle und hybride Infrastrukturen. Hierzu bietet VIAVI Messgeräte, Systeme, Software und Dienstleistungen für den Lebenszyklus eines Netzwerkes.

Netzwerkdienstleister



Frings Building Solutions GmbH, Herr André Rütters,
Vertriebsleitung

Kleinhülsen 42, **40721 Hilden**
Tel. +49 (2103) 58 77 -180, Fax: +49 (2103) 58 77 -320
E-Mail: andre.ruetters@frings-building.de
Homepage: www.frings-building.de
Service: Netzwerk- & Systemlösungen, bundesweit. Projektierung, Installation, 24h-Service, LAN/WAN; Inastallation, Betrieb & Wartung aktiver & passiver Netzwerke, Kupfer- & LWL-Verkabelungssysteme. Zertifiziert u.a. Dätwyler, Leoni, Corning, R&M, Axis, Cisco, HP. Bundesweite Standorte: Leipzig, Hannover, Hamburg, München, Düsseldorf und Frankfurt am Main



TP Networks Dienstleistungs GmbH
Herr Endres, Abteilungsleiter
IT-Dienstleistungen

Klausenburger Str. 9, **81677 München**
Tel.: 089/357151-0, Fax: 089/357151250
E-Mail: info@tpnetworks.de
Homepage: www.tpnetworks.de,
www.sicher-daten-entsorgen.de
Service: Projektierung, Installation und Wartung von aktiven und passiven Netzwerken, WLAN-Ausleuchtung und Messung, IT/RZ-Umzüge und Geräte Logistik, Dokumentation FNT Command, Datenträgervernichtung



dtm Datentechnik Moll GmbH

Herr Jan Moll
Benzstr. 1, 88074 Meckenbeuren
Tel.: 07542/9403-0
Email: info@dtm-group.de
Homepage: www.dtm-group.de
Service: Von der Beratung zum maßgeschneiderten IT-Konzept, wir sind Ihr Komplettanbieter für hochwertige und individuelle IT-Infrastrukturen in Ihrem Unternehmen. Planung, Ausführung und Dokumentation von Rechenzentren, Office-Verkabelungen & Industrievernetzungen.



DATENTECHNIK GMBH



Seit über **30 Jahren** strukturierte Netzwerkverkabelung von **Dipl.-Ing. Edwin Myk** mit Familie, Team und Ihnen.
Gemeinsam Zukunft mit dem Partner fürs **Handwerk** und den

Mittelstand – Ready for Take-off? Contact us!
TEL 030/232566110 MAIL mail@mykdatentechnik.de

USV-Anlagen



Riello UPS GmbH
Wilhelm-Bergner-Straße 9b
21509 Glinde

Tel.: 040/527211-0, Fax: 040/527211-200
E-Mail: vertrieb@riello-ups.de
Homepage: www.riello-ups.de
Die Riello UPS GmbH bietet USV-Anlagen mit Leistungen von 400 VA bis 6,4 MVA, individuelle Beratung sowie einen kompetenten Werkskundendienst.



Notstromtechnik-Clasen GmbH
Kurt-Fischer-Straße 39, **22926 Ahrensburg**
Tel.: 04102 2102-0, Fax: 04102 2102-20
E-Mail: info@ntc-gmbh.com
Homepage: www.ntc-gmbh.com



NTC ist Ihr Partner für hochverfügbare, unterbrechungs-freie und energieeffiziente Notstromversorgung. Wir bieten Ihnen alle Leistungen von A bis Z aus einer Hand. Professionell und herstellerunabhängig. Von der Analyse über Konzeption, Vertrieb und Montage bis hin zur Wartung. NTC – Sicherer ist das!



U.T.E. Electronic GmbH & Co. KG
www.ute.de

Friedrich-Ebert-Str. 86, **58454 Witten**
Tel. 02302/282830, E-Mail: info@ute.de
Seit über 25 Jahren **der** Spezialist in NRW für Unterbrechungs-freie Stromversorgung (USV) in allen Leistungsbereichen.

- Vertrieb von Neuanlagen, auch in kundenspezifischen Ausführungen
- Breites Serviceangebot mit eigener Werkstatt.
- Wartungsverträge mit unterschiedlichsten Leistungsumfängen und Reaktionszeiten.
- Montage, Reparatur, Wartung und Batteriewechsel an ein- und dreiphasige USV Anlagen verschiedenster Hersteller.

Besuchen Sie unser Democenter in Witten (Ruhrgebiet) und klären Sie alle Fragen rund um das Thema USV mit unseren Spezialisten. Zahlreiche Anlagen stehen vor-fürbereit zur Ansicht und Erklärung zur Verfügung.



Wöhrle Stromversorgungssysteme GmbH
Lerchenstraße 34,
71144 Steinenbronn

Stromversorgungssysteme
Tel. 07157/7374-0, Fax: 07157/7374-44
E-Mail: verkauf@woehrl-svs.de
Homepage: www.woehrl-svs.de
Wöhrle bietet ein- und dreiphasige USV-Anlagen im Leistungsbereich von 1 kVA bis zu mehreren MVA, eine individuelle Beratung sowie umfangreiche Service- und Supportleistungen für höchste Zuverlässigkeit und Verfügbarkeit. Zusätzlich können Sonderlösungen realisiert werden.



ABB Automation Products GmbH
Am Fuchsgraben 2–3
77880 Sasbach

Tel. 07841/609680, Fax: 07841/609681
E-Mail: ups-deabb@de.abb.com
Homepage: www.abb.de/ups
Energieeffiziente 1- bis 3-phasige USV-Anlagen (1 kVA – 5 MVA). Dezentrale Parallele Architektur (DPA TM) für höchste modulare Verfügbarkeit.

Rechenzentrum



Hochsicherheits-Rechenzentrum im ex. Atomschutzbunker für kritische Infrastrukturen mit Premium Internet

www.colocationIX.de/Lanline | sales@colocationix.de
ColocationIX bietet Ihr eigenes Rack ab € 695 netto / Monat

Leistungen: Rechenzentrum, Colocation Racks, Server Housing, Private Cloud Services, Managed Services, Infrastruktur Services, CDN, Cybersecurity, Standortvernetzung, 1G/10G/100G IP-Transit für Ihr Autonomes System (AS), 100Gbit/s Internet Exchange, China Direkt Verbindung 160ms

Features: 2m Stahlbeton, permanente Sauerstoffreduktion, 500x 42HE Racks in 10 Sicherheitszonen, Sicherheitsdesign DIN EN 50600 Klasse 4, CO₂-neutral, Energieeffizienzklasse A+++, Erbenbenfrei

Zertifizierungen: ISO 27001, ISO 27018, ISO 27018, EcoStep ISO 9001, ISO 14001, ISO 45001, ISO 50001

Erleben Sie, welche Vorteile die Auslagerung zu ColocationIX für Ihr Unternehmen hat.

Mehr Infos finden sie auf www.colocationix.de/Lanline oder fragen Sie uns am Telefon unter 0421 33388-0

Telefonielösungen

FRINGS

Frings Informatic Solutions GmbH, Herr Christian Gaul,
Vertriebsleitung

Kleinhülsen 42, **40721 Hilden**

Tel. +49 (2103) 58 77 -274, Fax: +49 (2103) 58 77 -310

E-Mail: christian.gaul@frings-informatic.de

Homepage: www.frings-informatic.de

Systemhausgruppe, MS Office 365, Cloud- und Backup-Services, IP-Telefonie aus dem eigenem Rechenzentrum. ITIL-HelpDesk-24h-Service, Field-Services bundesweit. Zertifiziert u.a. Swyx, Cisco, Microsoft, Unify, Citrix, AudioCodes, Baramundi und HP. Bundesweite Standorte: Hamburg, Hannover, Düsseldorf, Frankfurt a.M. und München

IT-/RZ-Stromversorgung



NTC
NOTSTROM
TECHNIK CLASEN

Notstromtechnik-Clasen GmbH

Kurt-Fischer-Straße 39, **22926 Ahrensburg**

Tel.: 04102 2102-0, Fax: 04102 2102-20

E-Mail: info@ntc-gmbh.com

Homepage: www.ntc-gmbh.com

NTC ist Ihr Partner für hochverfügbare, unterbrechungs-freie und energieeffiziente Notstromversorgung. Wir bieten Ihnen alle Leistungen von A bis Z aus einer Hand. Professionell und herstellerunabhängig. Von der Analyse über Konzeption, Vertrieb und Montage bis hin zur Wartung. NTC – Sicherer ist das!

DCIM

PROCOM

www.procom-data.de

Ein Partner von **SUNBIRD Software** - DCIM Lösungen für ihr RZ

Monitoring von Energie und Sensorik, iPDU und Umgebungsverwaltung.

Berichterstellung für Assets, Strom und Kühlung, Kapazitätsplanung, Kabelmanagement sowie Einbindung bestehender Tools wie z.B. ServiceNow...

Nähere Infos:

Tel: 089 84061799

mail: info@procom-data.de

Homepage: www.procom-data.de

Auch Ihre Anzeige könnte hier stehen!

Werben Sie kostengünstig und effektiv mit Ihrer Anzeige im IT Service Guide.

Ihre nächste Möglichkeit:

Ausgabe 11/2021

Anzeigenschluss:

08. Oktober 2021

Ihr Kontakt:

truchsess-jacobi@ctj-media.de

Inserentenverzeichnis

AIRSYS Refrigeration Engineering Technology (Beijing) Co. Ltd.	15
Bachmann GmbH	29
Klaus Faber AG	13
Kentix GmbH	3
KIOXIA Europe GmbH	21
MailStore Software GmbH	52
MicroNova AG	9
Paessler AG	7
Stulz GmbH.....	27
tde trans data elektronik GmbH	31
WEKA FACHMEDIEN GmbH	2, 11, 17, 51

Anzeigenschluss für die **Ausgabe 10/2021**
ist der 10. 09. 2021



aktuell.
modern.
mobil.



lanline.de

Die Ausgabe **10/2021** erscheint am 29. Sept. 2021



Schwerpunkt Security

Cyberkriminalität hat der deutschen Wirtschaft 2020/21 einen Schaden von über 220 Milliarden Euro beschert. Security bleibt damit das drängendste Problem, das es in Sachen Digitalisierung zu bewältigen gilt. Die Abwehr von Ransomware steht im Rampenlicht, doch die Herausforderung, das digitalisierte Wirtschaften abzusichern, ist deutlich breiter gefächert. Die Branche setzt auf Zero Trust und KI-Unterstützung.

Schwerpunkt Gebäudevernetzung

Sensoren und Aktoren lassen sich auf unterschiedliche Weise miteinander verbinden. Leitungsgebundene Verbindungen sind einfach und energieeffizient, können aber bei der Nachrüstung in bestehenden Gebäuden teuer sein. Viele Systementwickler interessieren sich daher für drahtlose Systeme.



Produkte/Services

Messtechnik und Energiespeicher

Betreiber müssen die Energieeffizienz ihrer Rechenzentren erhöhen. Die Bundesregierung hat in ihrem neuen Klimaschutzgesetz die Vorgaben verschärft. Bis 2030 soll die Industrie 43 Millionen Tonnen CO₂ einsparen. Auf die Rechenzentren entfällt dabei ein Anteil von etwa acht Millionen Tonnen CO₂. Die Konsequenzen reichen von der Planung bis zum RZ-Betrieb.



Vorschau auf kommende LANline-Schwerpunkte

Ausgabe **11/2021**
erscheint am 27.10. 2021

Verkabelung in IT & Industrie
Mit Marktübersicht
Kategorie-6_A-Kabel

Physische RZ-Sicherheit
Mit Marktübersicht Alarm- und Brandmelde-Systeme

Redaktionsschluss 01.09. 2021

Ausgabe **12/2021**
erscheint am 24.11. 2021

Das energieeffiziente RZ
Mit Marktübersicht
Intelligente PDUs

Digital Workspace
Mit Marktübersicht
Workspace-Management

Redaktionsschluss 28.09. 2021

Ausgabe **13/2021**
erscheint am 22.12. 2021

Server, Storage, Container
Mit Marktübersicht
HCI-Systeme

Endpoint-Management
Marktübersicht
UEM-Lösungen

Redaktionsschluss 26.10. 2021

Impressum

REDAKTION

Anschrift: Redaktion LANline, WEKA FACHMEDIEN GmbH,
Richard-Reitzner-Allee 2, 85540 Haar,
Tel. + 49 89 25556-1000, Fax + 49 89 25556-1199

Chefredakteur: Dr. Jörg Schröder (jos)

Redaktion: Anna Molder (am)

Autoren dieser Ausgabe: Achim Freyer, Dr. Wilhelm Greiner (wg), Olaf Hagemann, Christian Koch, Oliver Kolb, Christoph Lange, Roland Latzel, Bernd Mährlein, Robert Meiners, Udo Schneider, Dirk Schuma, Sergei Serdyuk, Marcel Teupe, Hugo Vliegen, Helmut Weiss

Layout: Norbert Preiß

Titelbild: Wolfgang Traub

Gekennzeichnete Artikel stellen die Meinung des Autors, nicht unbedingt die der Redaktion dar. Für unverlangt eingesandte Manuskripte keine Gewähr. Alle in der LANline erscheinenden Beiträge sind urheberrechtlich geschützt. Alle Rechte, auch Übersetzungen, vorbehalten. Reproduktionen, gleich welcher Art, nur mit schriftlicher Genehmigung des Verlages.

Aus der Veröffentlichung kann nicht geschlossen werden, dass die beschriebenen Lösungen oder verwendeten Bezeichnungen frei von gewerblichem Schutzrecht sind.

Erfüllungsort und Gerichtsstand ist München.

MEDIABERATUNG

Verlagsrepräsentant: Cornelia Truchsess-Jacobi,

Tel. + 49 170 3372234 oder +49 89 71940003,

E-Mail: truchsess-jacobi@ctj-media.de,

cornelia.truchsess@lanline.de

Verantw. für den Anzeigenteil: Eric Weis,

Tel. + 49 89 25556-1390

Zurzeit gilt Anzeigenpreisliste Nr. 33 / 2021

VERLAG

Anschrift: WEKA Fachmedien GmbH

Richard-Reitzner-Allee 2, 85540 Haar,

Tel. + 49 89 25556-1000, Fax + 49 89 25556-1199

HRB 119806, Amtsgericht München

Geschäftsführung: Kurt Skupin, Matthäus Hose

Verlagsleitung: Matthäus Hose

Vertriebsleitung: Marc Schneider,

Tel. + 49 89 25556-1509

Herstellungsleitung: Marion Stephan

Druck: Vogel Druck und Medienservice GmbH, Höchberg

Erscheinungsweise: monatlich

ISSN: 0942-4172

HIER KÖNNEN SIE BESTELLEN

Fragen zu Ihrem Heftbezug

Bestell- und Abonnement-Service:

WEKA Fachmedien GmbH,

c/o ZENIT Pressevertrieb GmbH,

Postfach 810640, 70523 Stuttgart

Tel. + 49 711 7252210, Fax + 49 711 7252333

E-Mail: abo@weka-fachmedien.de

Shop: www.weka-fachmedien.de

Erscheinungsweise: 12 Ausgaben

Jahresabonnement Print Inland 107,60 €

davon 78,20 € Heft, 29,40 € Versand

Jahresabonnement Print Ausland 117,80 €

davon 78,20 € Heft, 39,60 € Versand

Einzelheft 10,00 € (zzgl. 3,- € Versand)

jeweils inkl. der aktuellen MwSt.

Jahresbezug digitales E-Paper (Inland/Ausland) 29,99 €

Einzelausgabe digitales E-Paper (Inland/Ausland) 2,99 €

inkl. der aktuellen MwSt. ohne Versandkosten.

Bankverbindung: Postbank München, BLZ 70010080,

Kontonummer 9339809

Bezugszeit: Das Abonnement kann jederzeit, spätestens jedoch

sechs Wochen zum Ende des Bezugsjahres

gekündigt werden. Ansonsten verlängert sich das Abonnement um

weitere zwölf Monate. Bei Nichterscheinen aus technischen Grün-

den oder höherer Gewalt entsteht kein Anspruch auf Ersatz.

LANline TECH·days



**KOSTENFREIE
TEILNAHME**

Mit den TECH Days stellt die LANline ein digitales Event-Konzept bereit, dass sich an Expertinnen und Experten aus den Bereichen Datacenter und Verkabelung richtet. Hier kommen Fachleute nicht nur in hochinformativen Vorträgen und Workshops zusammen, sondern treffen sich auch zum Austausch und Networking – inklusive aller Optionen, die ein modernes virtuelles Meeting heute bietet. Die Themen reichen von der **Energieeffizienz im Datacenter** mit **Kühl-** und **Stromversorgungsthemen** bis zur **Datenverkabelung mit LWL** oder dem neuen **SPE**.

LANline Tech Days
**RZ-STROM-
VERSORGUNG**
09.09.2021

LANline Tech Days
**EINSATZ VON SINGLE
PAIR ETHERNET (SPE)**
07.10.2021

lanlinetechdays.de

Rechtssichere E-Mail-Archivierung made in Germany

Einfach. Zuverlässig. Weltweit erprobt.

MailStore Server

bietet GoBD-konforme E-Mail-Archivierung für kleine und mittelständische Unternehmen und hilft bei der Einhaltung der EU-DSGVO.



Warum E-Mail-Archivierung?

- Langfristige, manipulationssichere Aufbewahrung geschäftskritischer Kommunikation
- Ständige Verfügbarkeit und Wieder auffindbarkeit von E-Mails für alle Anwender
- Ideale Ergänzung zu einer Backup-Lösung

Ihre Vorteile

- Schutz vor Datenverlusten
- Schnelle Suche über E-Mails und Dateianhänge
- Verschlüsselte Speicherung und Compliance-Funktionen
- Nahtlose Integration in Microsoft Outlook
- Unabhängigkeit von PST-Dateien
- Regelmäßig unabhängig zertifiziert



**Kostenlose
30-Tage-
Testversion**

Mehr Informationen auf www.mailstore.com/de
oder direkt unter 02162-502990.