LANline

10,– €
Mai 2021
27. April

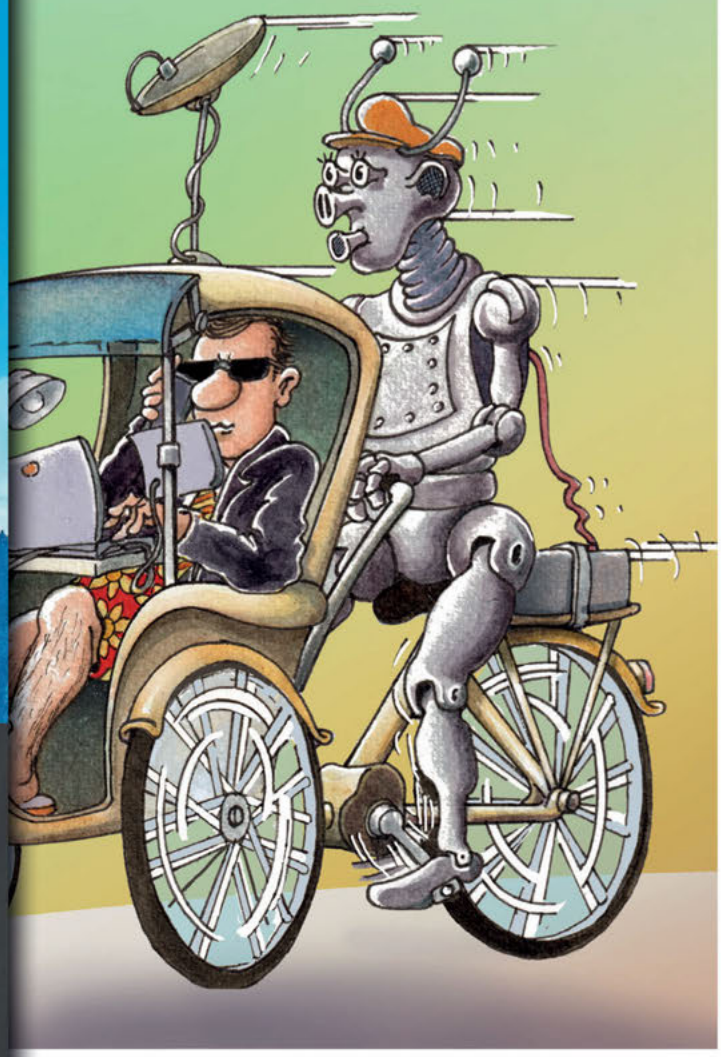
IT ▪ Network ▪ Datacenter

www.lanline.de

Future of Work

demie

en



eit

upe

iche

uxnet

Schwerpunkt Wireless-Technik

Mit Marktübersicht WLAN Access Points

Sicher, zuverlässig, flexibel

- gehostet, on-Premise oder in Ihrer privaten Cloud
- schnelle, einfache Installation und Handhabung
- Einbindung in bestehende Infrastruktur

Standortunabhängige Mitarbeiter

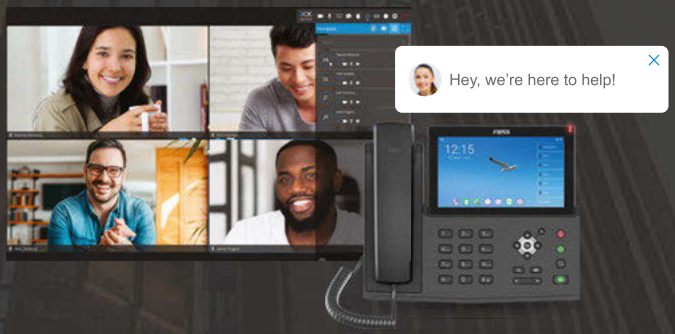
- Nutzung von Büro-Rufnummern via iOS & Android Apps
- Webclient mit integrierten Webkonferenzen
- unmittelbare remote Konfiguration neuer Benutzer

Simple Videokonferenz-Lösung

- browserbasiert - keine Downloads oder Plugins nötig
- Tools für Webinare & Kollaboration
- gratis Smartphone Apps für unterwegs

Kundenorientiertes Messaging

- Erweiterung der eigenen Website um Live Chat
- einfache Integration von Facebook Messenger
- Versand & Empfang von Business SMS



1 JAHR KOSTENLOS! WWW.3CX.DE

3CX

LANline

10,– €
Mai 2021
27. April

IT ▪ Network ▪ Datacenter www.lanline.de

Das digitale Büro/Future of Work

Arbeiten in und nach der Pandemie

Remote Work mit Privatgeräten

KI im Arbeitsalltag

Mit Marktübersicht Desktop as a Service

Start der neuen SASE-Testreihe
Cato Networks Security-Services

OT-Sicherheit unter der Lupe
Das gefährliche Erbe von Stuxnet

Schwerpunkt Wireless-Technik
Mit Marktübersicht WLAN Access Points

Für unsere Kunden nur das Beste!

Preisgekrönte IT-Infrastruktur

Vertrauen Sie auf das Beste. Rechenzentrumslösungen von Vertiv sind nicht nur effizient und zukunftsorientiert, sondern jetzt auch ausgezeichnet.

Wann dürfen wir für Sie da sein?

What's Your Edge?

Vertiv.com/WhatsYourEdge-DE

Vertiv freut sich über gleich drei wichtige Vertrauensbeweise unserer Kunden:

Die LANline Auszeichnung zum Anbieter des Jahres in den Kategorien

- **RZ-Stromversorgung**
- **RZ-Kühlung**
- **RZ-Monitoring**

Gemeinsam mit Ihnen sind wir auf dem richtigen Weg und freuen uns auf viele weitere Projekte!

VERTIV™

LANline ANBIETER DES JAHRES 2020 RZ-Stromversorgung Vertiv

LANline ANBIETER DES JAHRES 2020 RZ-Kühltechnik Vertiv

LANline ANBIETER DES JAHRES 2020 RZ-Monitoring Vertiv

33. Jahrgang, Ausgabe Mai 2021

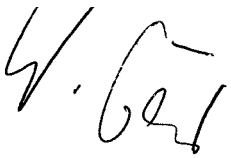
Zinnoberschwarz

Dr. Wilhelm Greiner, freier Mitarbeiter der LANline

„Was soll der ganze Zinnober?“ Diese schöne Redewendung – sie steht für: „Warum so viel Aufhebens um Nebensächliches?“ – kennt heute kaum noch jemand. Laut der weisen Eule Wikipedia stammt sie daher, dass einst Alchemisten, verrußt und hustend aus dem rauchumwölkten Labor hervorkriechend, feststellen mussten: Ihre Experimente mit Quecksilber und Schwefel hatten erneut kein Gold erbracht, sondern wieder nur Zinnoberrotes, wie man es vom Wasserfarbmalkasten der Schulzeit her kennt. Viel Zinnober gemacht wird heute um die „Zukunft der Arbeit“. Die Alchemisten unserer Tage wollen Gold nicht mehr per Knall und Rauch herstellen – dass Gold ein Element und folglich nicht im Reagenzglas fabrizierbar ist, hat sich herumgesprochen. Die Mittel moderner Alchemie sind vielmehr digital und heißen Big Data Analysis, künstliche Intelligenz und Robotik. Mit ihrer Hilfe strebt man einer gleißenden Zukunft entgegen, in der es von Quartal zu Quartal mehr Gold regnen möge in die Taschen des ewig gierigen Shareholders.

Einer, der dank Digitalisierung in Gold baden kann wie einst nur Dagobert Duck, ist Bill Gates. Anders als mancher Multimilliardärskollege nutzt Gates seinen Pool voller Geld nicht, um Raumschiff-Enterprise-Phantasien seiner Jugend auszuleben mit dem Ziel, auf dem Mars Cowboy und Indianer zu spielen. Er widmet sich lieber den wirklich drängenden Problemen der Menschheit: Mit der Bill & Melinda Gates Foundation arbeiten seine Frau und er daran, Gesundheit und Bildung der Weltbevölkerung zu verbessern, und 2015 scharte er im Projekt Breakthrough Energy Investoren um sich, um klimafreundliche Technik zu fördern. In seinem neuen Buch „Wie wir die Klimakatastrophe verhindern“ (es könnte das wichtigste Sachbuch des Jahrzehnts werden) diskutiert Gates die Frage, wie sich das bislang erfolgreiche Bemühen der Menschheit, das eigene Habitat möglichst zügig unbewohnbar zu machen, noch umkehren lässt. Er fordert nichts Geringeres als klimaneutrales Wirtschaften und unterscheidet hier zwischen Technik mit geringem und hohem „Öko-Aufpreis“ („Green Premium“): Sind klimaneutrale Lösungen nur etwas teurer als konventionelle, brauche man Aufklärung und staatliche Anreize; sind sie noch deutlich teurer, erfordere dies Investitionen in Innovation. Statt an immer schnellerer, effizienterer, gewinnträchtigerer Immernochmehrproduktion zu basteln, sollten wir Menschen das Forschen darauf konzentrieren, unser tägliches Treiben schnellstmöglich nachhaltig zu gestalten. Diese Wende wäre goldrichtig. Kommt sie nicht bald, sehe ich für unsere Zukunft – und damit auch die der Arbeit – rußschwarz.

Eine knall- und rauchfreie Lektüre wünscht



Inhalt

Markt

Produkte/Services

Schwerpunkt: Wireless-Technik

Technik

Schwerpunkt: Das digitale Büro/Future of Work

News

Rubriken

Cisco Live 2021 und Connect

Zukunft as a Service

Die Cisco-Hausmesse Live 2021 Ende März war Ciscos erste globale Veranstaltung, die ausschließlich online stattfand. Rund 100.000 Menschen verfolgten laut CEO Chuck Robbins dessen Keynote per – im wörtlichen Sinne – „Live-Stream“. Der Gastgeber hatte zahlreiche Neuheiten im Gepäck – vor allem, dass man ab Sommer das gesamte Portfolio als Service anbieten werde. Da geriet die nächste Generation von Optical-Routing-Technik schon fast zur Nebensache. Kurz vorher hatte die deutsche Regionalkonferenz Connect gezeigt, wie die Zukunft der Online-Hausmessen nach Social-Distancing-Zeiten aussehen könnte.

„Die Welt braucht uns, und die Welt braucht Sie alle“, so Chuck Robbins’ Message an die weltweit verstreuten IT-Fachleute draußen an den Empfangsgeräten. Zwar mag ein Hauch Silicon-Valley-typischer Unbescheidenheit diese Aussage umwehen, doch wer würde es wagen, dem Cisco-Chef im Daten- und „Immer mehr as a Service“-Zeitalter zu widersprechen? Schließlich war es das Internet (und damit Cisco-Router), Cloud-basierte Business-, Collaboration- und Videoconferencing-Services (darunter Cisco Webex) und IT-Security-Lösungen (von zahlreichen Anbietern, nicht zuletzt ebenfalls Cisco), die rund um den Globus einen Großteil des Geschäfts- und Privatlebens am Laufen hielten. Nicht umsonst ist der Internetverkehr laut Angaben des IT-Konzerns in manchen Ländern um bis zu 45 Prozent gestiegen (in Deutschland um 20 Prozent). Sein Unternehmen, so Robbins, habe in der Pandemie Remote Work ermöglicht, und nun sei man damit befasst, die Rückkehr ins Büro – genauer: in eine hybride Arbeitswelt aus Büro- und Remote-Arbeit – vorzubereiten, während man den Rollout der US-amerikanischen Impfkampagne unterstütze und absichere.

Selbst wenn eines Tages die letzte COVID-19-Vakzindosis verimpft ist, wird die Rolle der IT weiter an Gewicht gewinnen: Schließlich sollen – Stichwort „Internet of Things“ (IoT) und 5G – laut Cisco-Prognose bereits 2023 weltweit 29,3 Milliarden Geräte vernetzt sein. Es gehe deshalb nun darum, eine „inklusive Zukunft für alle“ – so Robbins mit Bezug auf den Slogan der letztjährigen Live – zu ermöglichen: „Eine inklusive Zukunft beginnt mit einer inklusiven Erholung (von der Krise, d.Red.)“, so der CEO. „Wir müssen eine inklusive Zusammenarbeit ermöglichen.“

„Inklusion“ ist derzeit ein Leitmotiv für Cisco, sieht man doch das Risiko, dass sich Beschäftigte im Lockdown-Heimbüro schnell „abgehängt“ fühlen. In der künftigen Arbeitswelt gelte es sicherzustellen, dass die Beschäftigten im Home-Office ebenso produktiv sein und sich ebenso eingebunden fühlen können wie die Belegschaft im Büro, so Robbins. Mit „Inklusion“ meint Cisco aber auch eine größere Nutzerbasis: Eine Milliarde Menschen will der Konzern weltweit bis 2025 ins digital gesteuerte Boot holen. Hier sei man bereits auf einem guten Weg.

Betonte die Bedeutung einer „inklusiven Zukunft“ mittels IT: Cisco-Chef Chuck Robbins.

Bild: Cisco

Cisco Plus

Der Weg ins inklusive Digitale ist ein Dreisprung: Wichtig sei es, so Robbins, IT-Umgebungen zu vernetzen, zu schützen und zu automatisieren. Da immer mehr Unternehmen ihre IT bevorzugt als Cloud-Service beziehen, also mieten, stellt Cisco nun – Trommelwirbel! – seine Produktpalette auf „as a Service“ um. Damit folgt der IT-Ausrüster dem Beispiel seiner Wettbewerber: HPE hatte schon im Sommer 2019 verkündet, sein Greenlake-Portfolio zu „Everything as a Service“ auszuweiten; Dell zog im Herbst 2020 mit „Project Apex“ nach.

Ab dem Sommer, so Todd Nightingale, verantwortlich für Ciscos Enterprise-Networking- und Cloud-Business, werde Cisco unter dem Namen „Cisco Plus“ das gesamte RZ-, Netzwerk- und Speichersortiment – Hardware wie auch Software – als Service anbieten. Cisco Plus soll, wie in solchen Fällen üblich, über ein intuitiv bedienbares Portal verfügbar sein und einen Marktplatz umfassen, über den man Services von Cisco wie auch von Partnern nach Bedarf buchen kann. Die Angebote werden

Todd Nightingale stellte das neue „As a Service“-Portfolio Cisco Plus vor. Bild: Cisco

Die Integration von ThousandEyes und AppDynamics ermöglicht „Full-Stack Observability“, so Ciscos Chefstrategin Liz Centoni. Bild: Cisco

laut Pressemitteilung zuerst in den USA, Kanada, UK, Deutschland, den Niederlanden und Australien verfügbar sein.

Den Anfang macht eine „As a Service“-Lösung für SASE (Secure Access Service Edge) – nicht weiter verwunderlich, ist doch SASE in Gartners Definition die Verschmelzung Cloud-basierter SD-WAN- und Security-Services (obschon mit lokal installierten Endgeräten). Die Grundlage dafür schuf Cisco, indem der Konzern die SASE-Komponenten – Cloud-Sicherheit inklusive ZTNA (Zero-Trust Network Access) sowie SD-WAN und Traffic-Monitoring – im Bundle anbietet. Zukünftig – ein genaues Datum nannte man nicht – sollen die SASE-Bausteine als ein einziges Abo erhältlich sein. Derzeit bewegt sich Cisco inkrementell auf ein einheitliches SASE-Angebot zu: Die Netzwerk-Management-Software Meraki integriere sich jetzt in Ciscos Cloud-basierte Security-Lösung Umbrella. Diese wiederum biete nun Remote-Browser-Isolation gegen Web-Gefahren sowie DLP (Data Loss Prevention) gegen Datenverlust und entferne Malware aus Cloud-Dateispeichern. Die Netzwerk-Bausteine – Meraki und die SD-WAN-Lösung Viptela – verstehen sich nun mit weiteren Public Clouds.

Den Kontext dazu erläuterte Jeetu Patel, der im Konzern Security und Collaboration verantwortet. Ciscos Security-Strategie umfasse drei Punkte: erstens den Schutz von Nutzern, Geräten, Netzwerken und Applikationen; zweitens kontextabhängige Zugriffsrichtlinien und drittens proaktive Erkennung und Reaktion auf Sicherheitsvorfälle (Detection and Response). Zu Punkt eins stellte Patel eine passwortlose Authentifizierung in Aussicht: Die Lösung Duo soll es Beschäftigten künftig erlauben, bei Cloud-Services die altbackene Authentisierung per Passwort durch Security-Tokens oder die Biometriefunktionen der Endgeräte wie Apple Face ID, Touch ID oder Windows Hello zu ersetzen. Duo soll ab Sommer als Public Preview verfügbar sein. In puncto Detection and Response wiederum aggregiert die Cloud-native SecureX-Plattform, vorgestellt letzten Juli, nun Informationen von Cisco-Seite und aus externen Quellen wie Google, ServiceNow oder Splunk. Zudem umfasst sie neue automatisierte Prozesse. Damit sollen sich Angriffe beispielsweise mittels Phishing deutlich schneller abwehren lassen: Ein Anwender könne eine E-Mail bei Verdacht auf Phishing an ein Alias weiterleiten, so Cisco, Secure X übernehme dann automa-

Cisco will sein umfangreiches Produktportfolio zu einer übersichtlichen Plattformsuite bündeln. Bild: Cisco

Cisco-Chef Uwe Peter (links) auf der Connect im Gespräch mit Cedrik Neike von Siemens und Claudia Nemat von der Telekom. Bild: Cisco

tisiert die Analyse und gebe in Minutenschnelle Bescheid, ob die E-Mail bösartig ist. Eine solche Automation vormals händischer Abläufe soll künftig Security-Workflows über alle Sicherheitsprodukte des Konzerns hinweg vereinfachen.

Schnellere Netze

Trotz manchen Knarzens: Das Internet hat sich in der Pandemie erstaunlich gut geschlagen. Doch Betrieb und Ausbau der globalen Internet-Infrastruktur sind, so Jonathan Davidson, Leiter von Ciscos Mass-Scale Infrastructure Group, große Herausforderungen für Netzwerkbetreiber: Für jeden investierten Dollar wende ein Provider fünf für Betriebskosten auf. Vor diesem Hintergrund will Cisco das Carrier-Dasein mit „Routed Optical Networking“ erleichtern. Gemeint ist: Kompakte Transceiver des jüngst akquirierten Optical-Networking-Spezialisten Acacia lassen sich direkt in die IP-Router stecken und sollen so helfen, IP- und optische Netze zusammenzuführen. Dadurch, so Davidson, könne ein Provider seine Legacy-Transport-Services auf das IP-Netz migrieren. Dies senkt die Gesamtkosten des Internetbetriebs laut Cisco-Angaben um bis zu 46 Prozent. Und mit „Converged SDN Transport“ könne man mehrere Netzwerke zu einer gemeinsamen, hoch skalierbaren Infrastruktur kombinieren. Davidson verkündete zudem die nächste Generation von Ciscos Silicon-One-Plattform: Ende 2019 vorgestellt, durchbrach die programmierbare Routing- und Switching-Architektur damals die 10-TBit/s-Marke, nun sollen bis zu 25,6 TBit/s möglich sein. Die neuen Router der 8000er-Familie zum Beispiel bieten laut Cisco-Angaben nun dank „Silicon One Q200“-Chips eine Kapazität von bis zu 14,4 TBit/s.

Das digitale Geschehen gilt es aber auch im Auge zu behalten. Chief Strategy Officer Liz Centoni stellte Neuerungen für mehr Durchblick im Applikations- und Netzwerkverkehr vor: Die Integration der Netzwerk-Überwachungssoftware ThousandEyes mit der APM-Lösung (Application-Performance-Management) AppDynamics führt Netzwerk- und Performance-Metriken in einem Dashboard zusammen. Dies, so Centoni, ermögliche „Full-Stack Observability“. Der unhandliche Begriff meint: Einblick in die Systemzustände entlang des gesamten Unterbaus und Datenpfads einer Applikation. Zusammen mit Secure X schaffe dies die Basis für die Entwicklung und den Betrieb sicherer Hybrid-Cloud-Applikationen inklusive Multi-Cloud-Management und -Compliance. Zu diesem Zweck ist die Thousand-Eyes-Software ab April ohne Zusatzkosten im Lieferumfang der Catalyst-9000-Switches enthalten.

Todd Nightingale gab im Rahmen der Keynote auch noch einen Ausblick auf Ciscos Portfoliostrategie. Man werde die Produktpalette zu einer übersichtlichen Plattformsuite bündeln, um den IT-Betrieb durch mehr Automation und Integration einfacher zu gestalten. Als Beispiel griff Nightingale auf den aktuellen Fall der Impfstofflogistik zurück: Die Kühlschränke für die Vakzinvorräte sind kameraüberwacht; meldet eine Kamera eine Bewegung, könne die Meraki-Software eine Warnung generieren und die Bilder automatisch zur Begutachtung in eine Webex-Konferenz überspielen. Man muss sich also wenigstens um den geordneten Ablauf des Impfprogramms in den USA keine Sorgen machen. Kleine Frage mit Blick auf die Situation hierzulande: Bietet eigentlich schon jemand „Vakzin-Rollout as a Service“?

Cisco Connect Germany

Zwei Wochen vor der Live fand die Online-Regionalkonferenz Connect Germany statt – eigentlich ein ungünstiger Zeitpunkt, konnte man doch im Vorfeld der globalen Hausmesse hier kaum News präsentieren. Lediglich eine Neuankündigung zauberte Cisco zur Connect aus dem Hut: Man werde im Juni ein neues RZ in Frankfurt eröffnen. Es soll Webex für die Kundschaft in Deutschland und der EU hosten – die Datenschutzbeauftragten freut’s. Spannend war die Connect vor allem, weil sie den Stand der Digitalisierung in Deutschland anschaulich umriss. Auch die Connect widmete sich vorrangig dem, was sich früher „Teilhabe“ nannte und Cisco mit „Inklusion“ meint: Neben Industrie 4.0 und Hybrid Work ging es um Chancengleichheit, Nachhaltigkeit und die Digitalisierung öffentlicher Einrichtungen wie Kliniken oder Schulen.

Vom Connect-„Hauptstadtstudio“ aus moderierte Ciscos Deutschlandchef Uwe Peter professionell eine Veranstaltung mit mehreren Streams angenehm knapp gehaltener Sessions. In seiner Keynote zog er nach einem Jahr COVID-19 Bilanz: Das hiesige Bruttosozialprodukt sei weitgehend stabil geblieben, die Klimabilanz

habe sich – mit freundlicher Unterstützung durch Lockdowns samt Home-Office-Boom – um über 40 Prozent verbessert. Nachholbedarf sah er aber beim Thema Chancengleichheit: Er verwies auf den Global Risks Report des World Economic Forums (WEF), in dessen Top-fünf-Risiken nun erstmals die digitale Spaltung auftaucht. Ihr müsse man entgegenwirken, so Peter.

Die Inszenierung der Connect – hier Uwe Peter im Gespräch mit Lena-Sophie Müller von der Initiative D21 – erinnerte mitunter an das Ambiente von Late-Night-Shows. Bild: Cisco

Mit Cedrik Neike, Siemens-Vorstand und CEO des Bereichs Digital Industries, sowie der aus Bonn zugeschalteten Claudia Nemat, Vorstand Technik und Innovation bei der Deutschen Telekom, diskutierte Peter den Stand der Dinge im Land der Dichter und über Digitalisierung Nachdenker. Um einen „digitalen Faden“ zwischen IT und OT zu spinnen, so Neike, gelte es, die IT mittels Low-Code- und No-Code-Plattformen zu vereinfachen. Claudia Nemat forderte eine „Human-centric Security by Design“, also nutzerorientierte, bereits ab Werk integrierte Sicherheitsfunktionen.

Neike berichtete von dem seit 2018 laufenden Projekt, den Berliner Stadtteil Siemensstadt – ein vor über 100 Jahren errichtetes Areal des Konzerns mit Werksneubauten und sachlich-schlichten Arbeitersiedlungen, damals Modellprojekt für das „Neue Bauen“ – zum Innovationscampus für das 4.0-Zeitalter umzugestalten. Das Ziel sei es, den Kiez auszulegen auf die Zukunft des Wohnens, Arbeitens und kontinuierlichen Lernens. Man werde über eine Million Quadratmeter komplett neu gestalten.

Das Themenspektrum der viertelstündigen Breakout-Sessions reichte vom hybriden Arbeiten über die Digitalisierung des Gesundheitssektors bis zur digital gestützten Bildung. Dem Home-Officer von Welt empfielt Cisco das KI-gestützte Desktop-Gerät Webex Desk Pro: Dank Greenroom-Funktion könne man damit eigene Präsentationsinhalte als Hintergrund einrichten, zudem gebe es Funktionen wie Whiteboard, Sprachbefehle oder das Ausblenden von Hintergrundlärm – für manch ein Online-Meeting der Rettungsanker.

Die Kommunen wiederum stehen laut Martin Schmiedel, Vorstand des IT-Dienstleisters kommune.digital, vor der „Mammutaufgabe digitale Bildung“ (so sein Vortragstitel), doch fehle es gerade kleinen und mittleren Gemeinden an Personal und Know-how. Gefragt sei Unterstützung von A bis Z: von der Bestandsaufnahme über die Vision (Was bedeutet Home-Schooling, Distanzunterricht, hybrides Lernen? Warum nicht mal für Fremdsprachenunterricht Muttersprachler remote aus dem Ausland zuschalten?) bis hin zu Anwenderschulung und Support.

Die Abschluss-Keynote drehte sich nochmals um das Kernthema Inklusion. Dazu war Lena-Sophie Müller, die Geschäftsführerin der Initiative D21, ins Studio geladen. Die Initiative will erreichen, dass alle Menschen hierzulande bestmöglich von der Digitalisierung profitieren. Dieses Ziel scheint noch einigermaßen weit entfernt. Müller argumentierte aber, beim Zugang zu Geräten stehe Deutschland gut da – bei den Digitalkompetenzen und der Offenheit für Neuerungen hingegen gebe es „noch Luft nach oben“. Beim Thema Bildung dürfe man nicht nur auf die Kinder schauen: In den Unternehmen seien Upskilling- und Reskilling-Aktivitäten nötig.

Für mehr Nachhaltigkeit, so Müller, biete Technologie eine große Chance, etwa durch emissionsärmere Stromerzeugungstechnik, zudem würden nun aufgrund der Pandemie Dienstreisen „ganz anders bewertet“ – sprich: eben durch Online-Meetings ersetzt. Während die IT-Branche sich gerne als weißer Ritter der Nachhaltigkeit inszeniert, legte Müller den Finger in die Wunde: Technologie bringe auch neue Herausforderungen, verbrauchen doch beispielsweise Quantencomputing oder Kryptowährungen enorm viel Energie.

Anti-Scheren-Fernsehen

Die Cisco Connect Germany war gut besucht, vor allem aber war sie gut gemacht. Denn sie orientierte sich nicht an jenen Webcasts und Zoom-Meetings, mit denen das Konferenzpublikum dieser Tage eh den Großteil seiner Zeit verbringt. Vielmehr schien sich Cisco das Unterhaltungsfernsehen als Vorbild genommen zu haben: Im Berliner „Hauptstadtstudio“ gab es neben Monologen vor Breitwand-Greenscreen-Kulisse auch eine Live-Band (ja, trotz Corona) für den kleinen Jingle zwischendurch sowie entspanntes Geplauder des Gastgebers mit seinen Gästen vor Kulissen, die stark an US-amerikanische Late-Night-Talkshows erinnerten. Denn wer sich in den USA fundiert informieren will, muss die TV-Nachrichten der Regionalsender meiden (die vorrangig aus Moderatorengeblubber, Lokal-Banalem, Werbung, Sport und Wetter bestehen) und auf die hellen Köpfe der Late-Night-Shows warten, allen voran Trevor Noah, Stephen Colbert und der geniale John Oliver. Dessen „Last Week Tonight“ ist praktisch schon Bildungsfernsehen – nur eben in unterhaltsam. Dass sich Cisco solche Vorbilder gesucht hat, ist ein Schritt in die richtige Richtung. Denn kurzweilige Online-Hausmessen erleichtern es, Reisen zu Konferenzen künftig „ganz anders zu bewerten“. Und das ist gut so, wie man in Berliner Hauptstadtstudios sagt. Zumindest, wenn man es mit der Nachhaltigkeit wirklich ernst meint. Zugleich ist der Besuch einer Online-Hausmesse – Bandbreite, Endgerät und Digitalkompetenz mal vorausgesetzt – selbst jenen möglich, die vor den Kosten und dem Zeitaufwand einer Dienstreise zurückschrecken würden. Die Umwelt gewinnt also durch eine „Hausmesse 4.0“ ebenso wie die Teilhabe. Auch an der Cisco Live hätten schließlich keine 100.000 Menschen offline teilnehmen können.

Dr. Wilhelm Greiner

Im Interview: Rainer Schmidt von Harting

Der Stand der Dinge bei Single Pair Ethernet

Single Pair Ethernet gilt als Hoffnungsträger für eine einfache und günstige Vernetzung, wenn eher Robustheit als Hochleistung gefragt ist. Rainer Schmidt, Busines Development Manager bei Harting und Normierungsfachmann mit langjähriger Erfahrung, erklärte im LANline-Gespräch den aktuellen Stand von Technik, Markt und Standardisierung bei Kabel und Stecker.

LANline: Herr Schmidt, wie ist der derzeitige Stand bei SPE in puncto Normierung?
Schmidt: Zunächst ist Single Pair Ethernet ein Ethernet-Protokoll oder genauer gesagt eine Familie von Protokollen, die nur ein Adernpaar zur Übertragung nutzt. Also vereinfacht: SPE ist Ethernet für ein neues Medium, nämlich einpaariges Kupferkabel. Als Beispiele nennen kann man etwa SPE 10 MBit/s über 1.000 m und spezifiziert bis 20 MHz nach IEEE 802.3cg, SPE 100 MBit/s über 15 m spezifiziert bis 66 MHz nach IEEE 802.3bw und SPE 1 GBit/s über 40 m spezifiziert bis 600 MHz nach IEEE 802.3bp. Diese und einige weitere SPE-Protokolle sind bei IEEE 802.3 publiziert. Weitere, etwa für Multidrop-Anwendungen nach IEEE 802.3da, sind in Vorbereitung.

LANline: Dieses System bildet die Basis für die technische Umsetzung.
Schmidt: Das ist richtig. Zur technischen Umsetzung gehört zuerst immer auch die Verkabelung. Da es so viele verschiedene SPE-Protokolle gibt, entsteht die Verkabelung dazu über zwei Ansätze. Zunächst gibt es den anwendungsspezifischen Ansatz. Dabei wird die jeweilige Spezifikation des SPE-Protokolls nach IEEE802.2.xx genutzt und mit den dort verankerten technischen Eckwerten, also etwa Bandbreite in MHz, IL in dB und Länge in Metern, eine passende Verkabelungsstruktur definiert. Dieser Ansatz findet sich in einem speziellen Technischen Report wieder, den die ISO/IEC JTC 1 SC 25/WG 3 im Auftrag der Industrie-Anwender entwickelt und publiziert. Der Report heißt ISO/IEC 11801 TR9906: „Technical Report: Balanced 1-pair cabling channels up to 600 MHz“. Die Standards für Industrieverkabelung nutzen den TR9906 als Basis und

Rainer Schmidt, Busines Development Manager bei Harting: „Während der Entwicklung neuer Steckverbinderkonzepte standen immer zwei Anforderungen ganz oben auf der Liste: Performance und Baugröße.“ Bild: Harting

erarbeiten Anhänge zu SPE oder zur einpaarigen Verkabelung mit ISO/IEC 11801-3 AMD-1 und IEC 61918 AMD-1. Diese Papiere will man in Kürze verabschieden und dann veröffentlichen.

LANline: Wie sieht der zweite Ansatz aus?
Schmidt: Der generische Ansatz ist bekannt aus der strukturierten Verkabelung und geht einen Schritt weiter, indem er versucht, heutige und zukünftige Anforderungen von SPE an die Verkabelung zu clustern und daraus Verkabelungslösungen zu entwickeln. Schaut man sich die vielen unterschiedlichen SPE-Protokolle an, ist dies durchaus sinnvoll, um das ganze Thema zu vereinfachen und seine Implementierung in der Praxis zu beschleunigen.

LANline: Wie ist dabei der Stand?
Schmidt: Dieser Standardisierungsprozess läuft gerade und führt zu einem Anhang in ISO/IEC 11801-1 AMD 1 mit drei einpaarigen Übertragungskanälen und Verkabelungslösungen namens T1-A mit 20 MHz und 1.000 Metern, T1-B mit 600 MHz und 100 Metern sowie T1-C mit 1.250 MHz und ebenfalls 100 Metern.

LANline: Welche Rolle spielen die Richtlinien für die Komponenten?
Schmidt: Einpaarige Verkabelungen nutzen Verbinder und Kabel, die wiederum einer eigenen Normung unterliegen, aber natürlich aufeinander aufbauen. Die beteiligten Gremien der Verkabelungsstandards kommunizieren untereinander. Während die Verkabelungsnormen für den Systemintegrator und Installateur wichtig sind, haben die Komponentenstandards wesentliche Bedeutung für den Hersteller und liefern die technische Spezifikation für diese Bauteile. Für die Kabel sind dies IEC 61158-11 und -12 bis 600 MHz. Diese sind bereits publiziert. IEC 61158-13 und -14 bis 20 MHz sind in Vorbereitung.

LANline: Wie ist die Situation bei den Steckern?
Schmidt: Für Verbinder, also Stecker und Buchse, steht der bereits publizierte Standard IEC 63171-6 zur Verfügung. Das zu-

gehörige Steckgesicht hat sich auf Grund seiner Universalität und der Einsatzmöglichkeit in allen Installationsumgebungen vom Büro bis zur Industrie nach MICE1 bis MICE3 durchgesetzt und ist auch in den Verkabelungsstandards gefordert oder referenziert. Mit dem Papier IEC 63171-1 gibt es noch einen zweiten verabschiedeten Steckerstandard, der allerdings nur MICE1 abdeckt.

LANline: Kann man für alles, was der Markt derzeit benötigt, bereits Produkte kaufen?
Schmidt: Das kann man, wenn auch die Breite des Angebots speziell im Bereich PHY und Chipsets noch ausbaufähig ist. Auch Geräte mit SPE-Schnittstellen befinden sich vielfach noch in der Entwicklung. Kabel und Steckverbinder von einer Reihe von Herstellern sind verfügbar. In den Punkten Produktvielfalt und Verfügbarkeit sind Kabel und Verbinder unkritisch.

LANline: Gibt es Unterschiede zwischen den Branchen?
Schmidt: Getrieben wurde die Entwicklung von SPE wesentlich von der Autoindustrie und von der Industrieautomatisierung. Beide benötigen eine einheitliche Kommunikationsplattform, um einen höheren Grad an Automatisierung in ihre Anwendungen zu bringen. Bei der Autoindustrie ist dies zum Beispiel das autonome Fahren. Bei der Automatisierung ist es Industrie 4.0. Beide haben Ethernet als Basis für diese einheitliche Kommunikationsplattform identifizierten und die Entwicklung vorangetrieben. Daher sind diese beiden Branchen auch am weitesten in der Umsetzung. Interessanterweise waren es deutsche Firmen, die diese Initiative begründeten und zum Start von IEEE-Projekten führten. Bei der Autoindustrie war dies ein Konsortium um BMW und Bosch, das zu IEEE802.3bw und bp führte. Bei der Industrie war es Siemens.

LANline: Welche weiteren Kandidaten sehen Sie?
Schmidt: Zum Kreis gehören die Gebäudeautomatisierung und damit auch die technische Gebäudeausrüstung wie etwa die Beleuchtung. Allerdings ist dort die Ausgangssituation etwas anders als beim Auto oder in der Industrie. Während die erstgenannten bereits Ethernet-Plattformen genutzt haben und zur Andockung weiterer Funktionalität, etwa Sensorik, die Ethernet-Technologie dahin erweitern müssen, stellt sich die Gebäudeautomatisierung als ein mehr oder weniges geschlossenes System dar. Moderne Gebäudeautomatisierungslösungen haben den vollen Zugriff auf Sensornetzwerke. Kompatibilität zwischen unterschiedlichen Lösungen könnte an der einen oder anderen Stelle Vorteile bringen, aber es scheint so, als ob dieses Argument allein nicht ausreicht. Möglicherweise entsteht dort erst ein entsprechender Innovationsdruck, wenn es gilt, Konzepte wie Smart City umzusetzen.

LANline: Wie sieht das Bild in unserem Alltag aus, etwa bei der Unterhaltungselektronik?
Schmidt: Auch die Unterhaltungselektronik ist ein potenzieller Kandidat für die Nutzung von SPE. Allerdings erscheint mir dieser Markt derart fragmentiert, dass das wohl eher ein frommer Wunsch der Anwender bleibt. Solange dort anstatt in einzelnen Geräten nicht systemisch gedacht wird, wird sich auch nichts ändern. Dieser Industriezweig hat es ja bis heute noch nicht einmal geschafft, Geräte und Anwendungen, die zusammen genutzt werden, halbwegs vernünftig miteinander zu verknüpfen. Etwas überspitzt gesagt: Um ein Fernsehprogramm zu genießen, benötigt man heute meist noch mindestens drei Fernbedienungen. Eine für den Service, also Box, SAT oder Entsprechendes, eine für den Bildschirm, eine für die Audioanlage. Wer noch den PC oder Laptop mit Services wie iTunes einbinden möchte, der ist fast verloren. Seit 20 Jahren sprechen wir von Multimedia, aber es bleibt erschreckend viel ungenutztes Potenzial!

LANline: Zurück zum SPE-Equipment. Stellt das Konzept SPE besondere Anforderungen an die Hersteller?
Schmidt: SPE verlangt im Grunde lediglich, einmal abgesehen von PHYs und Chipsets, ein neues Medium, nämlich ein einpaarige Datenkabel in Verbindung mit einpaarigen Steckverbindern. Herausforderungen ergeben sich im Wesentlichen bei der Kombination von Bandbreite und Baugröße. Hersteller von Kabeln können jetzt ihr Datenkabel von vier Paaren auf ein Paar reduzieren. Im Aufbau der Seele und der entsprechenden Schirmung und des Kabelmantels greifen sie jedoch auf mehr oder weniger bewährte Konstruktionen zurück.
Daraus resultieren dann einpaarige Datenkabel, die im Schnitt zwischen 30 und 50 Prozent Platz und Gewicht einsparen können. Will man SPE aber über weite Entfernungen übertragen und auch Fernspeisung nutzen muss man entsprechende Adernquerschnitte von zum Beispiel AWG18 einsetzen. Die Physik begrenzt hier also das Streben nach Einsparung und Miniaturisierung.

LANline: Welchen Rahmenbedingungen unterliegen die Steckerhersteller?
Schmidt: Bei den Steckverbindern ist das im Grunde ganz ähnlich. Während der Entwicklung neuer Steckverbinderkonzepte standen immer zwei Anforderungen ganz oben auf der Liste: Performance und Baugröße. Das Thema Performance ist gut zu lösen, wenn man eine extrem hohe Symmetrie des Designs erzielen kann und gleichzeitig den Anschlussbereich, als Crimp oder IDC, klug wählt und möglichst kurz gestaltet. Das findet man im Harting T1 wieder, um unseren Beitrag zu nennen. Die Baugröße ist dagegen so eine Sache. Natürlich lässt sich Verbindungstechnik für SPE gut miniaturisieren. Das spart Bauraum etwa an Geräten oder Verteilern. Der Spielraum ist aber durch Kabeldimensionen und Handhabbarkeit begrenzt. Daher sind im IEC-63171-6-Standard unterschiedliche Bauformen mit immer gleich hoher Leistung kombiniert, sehr kleine Stecker für IP20 und Kabel bis AWG22, smarte Stecker für IP65/67 in M8-Bauformen und sehr robuste Stecker für AWG18 Kabel in M12.

LANline: Herr Schmidt, vielen Dank für das Gespräch. Dr. Jörg Schröper

Prysmian Group: Mehr Brandsicherheit für Kategorie-7-, 7_A- und -8.2-S/FTP-Kabel

Hochgeschirmte Draka-Kabel erfüllen CPR-Brandschutzklasse Dca s1 d1 a1

Die BU Multimedia Solutions (MMS) der Prysmian Group hat ihre hochgeschirmten Draka-Triple-S/FTP-Installations- und Anschlusskabel der Kategorien 7, 7_A und 8.2 mit mehr Feuerresistenz ausgestattet. Neben dem hohen Brandschutz der CPR-Klasse Dca bieten sie geringste Rauch- (s1) und Säureentwicklung (a1) sowie ein minimiertes Abtropfverhalten (d1). Die Kabel kombinieren eine besonders gute Schirmung mit höchster Brandsicherheit, so der Hersteller, und sollen somit wesentlich zu mehr Personenschutz in Gebäudebränden beitragen. Der Hintergrund: 44 Prozent der rund 4.000 Personen, die jährlich durch Brände ums Leben kommen, sind Folge von toxischen Gasen oder Rauch. Dies liegt vor allem daran, dass bei Bränden innerhalb von drei Minuten lebensgefährliche Bedingungen auftreten. Vor 50 Jahren betrug diese Zeitspanne noch mehr als 15 Minuten. Der Grund für diese dramatische Beschleunigung ist die vermehrte Verwendung von Kunststoffen innerhalb der Gebäude. Dem „World Fire Statistics"-Report (2006) zufolge entstehen rund 90 Prozent aller Brände in Gebäuden. Dort ist also die Gefahr besonders groß, dass Leib und Leben durch Feuer zu Schaden kommen – zumal die Zeit zur Flucht sehr knapp ist. Um die Brandsicherheit in Gebäuden so hoch wie möglich zu halten, ist die Beschaffenheit der dort verbauten Produkte und Stoffe hinsichtlich ihres Brandverhaltens ein entscheidender Faktor.

Die Prysmian Group hat ihre hochgeschirmten Draka-Triple-S/FTP-Installations- und Anschlusskabel mit mehr Feuerresistenz ausgestattet. Bild: Prysmian Group

Auch Kabel sind Produkte in Räumen, die verbrennen können. Sie sind gleichfalls als Rauchverursacher zu betrachten und das Sicherstellen einer hohen Brandschutzklasse spielt auch bei Kabeln eine wesentliche Rolle. „Wir arbeiten kontinuierlich an der Weiterentwicklung unserer Kupferkabel in Bezug auf Brandschutz, ohne dabei weitere wichtige Eigenschaften wie die Schirmung zu vernachlässigen", sagte dazu Zoran Borcic, Product Manager Copper Cables, BU Multimedia Solutions, Prysmian Group. Mit der Erweiterung des Portfolios um die hoch geschirmten Triple 1 Dca s1 d1 a1 S/FTP-Kabel in den Kategorien 7, 7_A und 8.2 vereine MMS die optimale Schirmung mit hohem Brandschutz, sehr geringer Rauchentwicklung und verzögerter Wärmefreisetzung. „Die neuen Kabel stellen vor allem die Sichtbarkeit des Fluchtwegs in brennenden Gebäuden sicher. Ein wichtiger Aspekt, wenn man bedenkt, dass die Feuerwehr erst nach rund acht Minuten eintrifft, den Flüchtenden aber nur drei Minuten Zeit bleibt, das brennende Gebäude zu verlassen. Selbstrettung ist ein wesentlicher Bestandteil heutiger Brandschutzkonzepte", so Borcic weiter.

Die Installations- und Anschlusskabel bieten laut Hersteller optimale Abschirmung in der Trennklasse „d". Sie erfüllen die in der EN 50174-2 geforderten Kriterien hinsichtlich der Abstände oder der Verwendung von Trennstegen bei Kabeltrassen. jos

Rechner für anspruchsvolle Workloads

Lenovo: Mehr Server-Leistung für Think-System-Serie

Die Lenovo Infrastructure Solutions Group (ISG) hat eine weitere Generation ihrer Lenovo-Think-System-Server vorgestellt, die sich durch ein besonders ausgewogenes Verhältnis von Leistung, Sicherheit und Effizienz auszeichnen sollen. Die Server basieren auf Intel-Xeon-Scalable-Prozessoren der dritten Generation und PCIe Gen4. Die Rechner eignen sich laut Lenovo für unterschiedliche Workloads, etwa für High Performance Computing (HPC), künstliche Intelligenz (KI), Modellierung und Simulation, Cloud Computing, virtuelle Desktop-Infrastruktur (VDI) und Advanced Analytics. Man biete „eine einzigartige Verbindung von Leistung, Sicherheit und Effizienz", hängt Kamran Amini, Vice President und General Manager of Infrastructure Solutions Platforms bei der Lenovo Infrastructure Solutions Group, die Messlatte hoch. Durch eine Kombination von Innovationen in den Bereichen Sicherheit, Wasserkühlung und As-a-Service-Angeboten ermögliche man Anwendern, eine breite Palette von Workloads sicher auszuführen und zu beschleunigen. Zum Portfolio zählen im Einzelnen nun die Systeme ThinkSystem SR650 V2, SR630 V2, ST650 V2 und SN550 V2 – die jeweils mehr Leistung, Zuverlässigkeit, Flexibilität und Sicherheit als ihre Vorgänger bieten sollen. jos

Die Lenovo-Server basieren auf Intel-Xeon-Scalable-Prozessoren der dritten Generation und PCIe Gen4. Bild: Lenovo

Studie bestätigt Nachholbedarf beim öffentlichen WLAN-Angebot in Deutschland

Cambium: Kostengünstige Drahtloslösungen für Städte und Gemeinden

Heute gilt es als nahezu selbstverständlich, dass öffentliche Orte wie Bibliotheken, Museen, Gesundheitszentren oder Parks ein öffentliches WLAN bieten. Um das Angebot an drahtloser Technik in Form von Hotspots zu erweitern, hat die EU die Förderinitiative WiFi-4EU ins Leben gerufen. Wie eine aktuelle Studie von Cambium Networks zeigt, wurden in Deutschland zwar die maximale Anzahl an WiFi4EU-Gutscheinen vergeben, bisher aber weniger als 30 Prozent der Projekte abgeschlossen. Die Installationszeit für die Gemeinden wurde daher vor Kurzem um sechs Monate, bis August 2021, verlängert. Mit seinen drahtlosen In- und Outdoorlösungen will Cambium Networks die Gemeinden dabei unterstützen, schnell und kostengünstig WLANs aufzubauen. Sie können über die WiFi-4EU-Initiative Gutscheine im Wert von 15.000 Euro für die Installation von WLANs beantragen.

Die Hotspots sollen an Orten entstehen, an denen noch kein kostenloses WLAN-Angebot verfügbar ist. Nach eigenen Angaben bietet Cambium Networks dazu mit seinem Produktportfolio, das sich über mehrere Fixed-Wireless-, Wi-Fi-Standards und -Frequenzen erstreckt, performante Lösungen für den In- und Outdoorbereich. Mit den Geräten lassen sich auch bei hoher Nutzerdichte eine hohe Bandbreite und eine stabile Leistung erreichen. Zu Beginn entstehen für den Kunden geringe Investitions- und Wartungskosten, spätere Kosten für Software-Updates und jährliche Lizenzen entfallen. Wie die Studie von Cambium Networks zeige, sei Deutschland im EU-Vergleich mit 856 WiFi4EU-Gutscheinen zusammen mit Italien, Spanien und Frankreich unter den Top 4 der Länder, die die Förderung erhalten haben. Allerdings wurden in Deutschland erst weniger als 30 Prozent der Projekte abgeschlossen.

„Unserer Erfahrung nach mangelt es bei den Projekten meist an Lösungen, die sich schnell und einfach integrieren lassen. Zusammen mit unseren WiFi-4EU-erfahrenen Partnern haben wir bereits erfolgreich Projekte in einigen Städten Deutschlands abgeschlossen“,

Tabatha von Kölichen, Regional Sales Director DACH, Israel und Benelux bei Cambium Networks. Bild: Cambium Networks

sagt Tabatha von Kölichen, Regional Sales Director DACH, Israel und Benelux bei Cambium Networks. „Uns ist es wichtig, auch ländlichen und abgelegenen Orten ein stabiles und leistungsfähiges WLAN-Netzwerk bereitzustellen, das sich einfach verwalten lässt. Mit unseren Richtfunklösungen sind wir in der Lage, Kabel zu ersetzen und schnell Drahtlosnetze aufzubauen.“ jos

R&M produziert PoP-Zellen für Glasfasernetze

Schlüsselfertiger Point of Presence bringt FTTH voran

Der Ausbau von Breitbandnetzen lässt sich weiter beschleunigen. Davon ist R&M überzeugt, bekannt als weltweit tätiger Schweizer Entwickler und Anbieter von Verkabelungssystemen für hochwertige Netzwerkinfrastrukturen mit Sitz in Wetzikon.

Ein neuer Beitrag dazu soll die von R&M Deutschland entwickelte schlüsselfertige Point-of-Presence-Zelle (PoP) für Glasfasernetze sein. Sie erspare wochenlange Bau- und Installationsarbeiten im Feld, so R&M. Der FTTH-Ausbau komme so deutlich schneller voran. R&M bestückt das PoP-Gebäude mit allem, was an Knotenpunkten von Glasfasernetzen benötigt wird. Netzbetreiber und Baufirmen können Größen und Equipment aus einem Set wählen, das R&M zur Verfügung stellt. Sie müssen sich nicht mehr um technische Details, Standards, örtliche und klimatische Bedingungen, Stücklisten oder Montage kümmern, so der Hersteller „Unser Prinzip lautet, ein PoP – ein Partner“, erläutert Gabriel Bogdan, Geschäftsführer R&M Deutschland und Österreich. Das R&M-Programm umfasst neben der fertigen Lieferung der Zellen alle Schritte von der Projektplanung bis zur Inbetriebnahme. R&M lässt die PoP-Stationen in Deutschland produzieren und bringt sie mit Tiefladern zur Baustelle. Vor Ort muss der Installateur nur die Kabel und Rohrverbände aus dem Erdboden in die Kabine ziehen und anschließen. Die PoP-Stationen bieten Platz für die Installation von 4.608 bis 32.256 Fasern oder Ports. Die Verteilergestelle und -module kommen aus dem R&Mfoxs- und Prime-ODF-Sortiment. Die Stationen bestehen aus Stahlbeton, sind neun bis 18 Quadratmeter groß und wiegen bis zu 30 Tonnen. Das Equipment umfasst neben den fiberoptischen Racks die Kabelführungen, Stromversorgung, IT-Systeme, Klimaanlage, Beleuchtung, Brandschutz und Sicherheitssysteme. FTTH-Projekte kommen damit deutlich schneller voran, so R&M. jos

Schlüsselfertige Point-of-Presence-Zellen liefert R&M Deutschland per Tieflader an den Einsatzort. Bild: R&M

Evolution und Zukunft der OT-Security

Das Erbe von Stuxnet

Über zehn Jahre nach Stuxnet ist die OT-Infrastruktur (Operational Technology) stärker vernetzt als je zuvor – und damit auch deutlich verwundbarer. IT-Bedrohungen dominieren zwar das Tagesgespräch, Cyberkriminelle erkennen jedoch in SCADA-Systemen (Supervisory Control and Data Acquisition) und industriellen Kontrollsystemen (ICS) besonders lohnende Ziele.

In einer Umfrage für den „Fortinet State of Operational Technology and Cybersecurity Report“ gaben bereits 74 Prozent aller OT-Unternehmen an, schon einmal von einem Malware-Angriff betroffen gewesen zu sein. Dies lässt sich auf verschiedene Faktoren zurückführen, darunter die Tatsache, dass Legacy-Systeme weit verbreitet sind. Manche Netzwerke sind 20 bis 30 Jahre alt und nur unregelmäßig aktualisiert. Dadurch weisen sie lang bekannte Schwachstellen auf. Darüber hinaus setzen potenzielle Angreifer vermehrt auf Verschleierung ihrer Tätigkeiten und nutzen fortschrittliche Anti-Analysetechniken, um unentdeckt zu bleiben.

Mit diesen Techniken erschweren sie es den IT-Teams, ihre Methode, ihren Ursprung und die Absicht der Attacke zu erkennen. In der Folge bleibt es eine Herausforderung, ähnliche zukünftige Angriffe zu verhindern. Die sich kontinuierlich weiterentwickelnden Angriffsmethoden auf OT-Systeme erfordern ohne Frage eine entsprechende Antwort. Es bedarf einer ganzheitlichen Analyse der eingesetzten Taktiken, um daraus Erkenntnisse für zukünftige Cybersecurity-Verteidigungsstrategien zu gewinnen und einzusetzen.

Weiterentwicklung von Stuxnet: EKANS 2019

Stuxnet machte 2010 Schlagzeilen, als öffentlich wurde, dass ein bösartiger PC-Wurm auf SCADA-Systeme abzielte – damals ein Novum. Der Code war viel größer und ausgeklügelter als seine Vorgängerversionen. Mit über 500 KByte konnte er sich leicht seinen Weg in Windows-Rechner sowie Netzwerke bahnen und sich mehrmals replizieren, bevor er das endgültige SCADA-Ziel auswählte.

Das Besondere an Stuxnet war seine Fähigkeit, speicherprogrammierbare Steuerungen (SPS) zu beeinträchtigen. Bei SPS-Devices handelt es sich um digitale Geräte in der Industrie, die besonders robust sind und darauf ausgelegt, Fertigungsprozesse zu steuern. In diesem Fall ermöglichten die SPSs die Automatisierung von elektromechanischen Prozessen, die in industriellen oder mechanischen Anlagen ablaufen. Die Präzision von Stuxnet war entscheidend für die OT-Sicherheit und die Entwicklung von Bedrohungsszenarien.

Auch im Jahr 2020 waren OT-Netzwerke häufig Ziele von Cyberkriminellen. Beispielsweise durch die Ransomware EKANS, die erstmals im Dezember 2019 in Erscheinung trat. Wie der Fortinet Threat Landscape Report von August 2020 feststellte, setzt EKANS stark auf Verschleierung und ist in der Programmiersprache GO geschrieben. Dies erfordert eine umfangreichere, manuelle Analyse. Die Malware ist daher schwer erkennbar.

Der Einsatz der Ransomware ist besonders besorgniserregend, wenn man die kostspieligen Auswirkungen auf anfällige OT-Systeme und die Zukunft der OT-Sicherheit bedenkt. Denn die Angreifer könnten diese Zielmethodik auf ganze OT-Umgebungen ausweiten. Und eine solche Form von Ransomware steht erst am Anfang ihrer Entwicklung. Im Juni 2020 wurde eine Variante bekannt, die nicht nur das übliche Verhalten einer Ransomware beherrschte – Daten zu verschlüsseln und ein Lösegeld zu fordern. Darüber hinaus konnte sie bereits die Firewall des Hosts deaktivieren.

Sicherheit für IT/OT-Konvergenz

EKANS ist bei Weitem nicht die einzige kürzlich identifizierte Ransomware, die auf OT-Netzwerke abzielt. Seit Stuxnet gab es viele weitere ausgeklügelte Angriffe, was möglicherweise auf die im Zuge der digitalen Transformation gestiegene Verwundbarkeit von OT-Netzwerken zurückzuführen ist, denn mittlerweile sind diese mit dem Internet verbunden. Durch die Konvergenz von IT- und OT-Netzwerken ist die Air Gap, die früher digitale und physische Anlagen isoliert hat, auf ein Minimum reduziert. Cyberkriminelle haben inzwischen außerdem die Möglichkeit, sich lateral von den IT- in die OT-Netzwerke zu bewegen, wodurch sie sich unbemerkt ausbreiten können.

ICS- und SCADA-Systeme sind damit zu attraktiven Zielen für Cyberkriminelle geworden, die in Terrorismus, Spionage oder Cyberkriegsführung verwickelt sind. Folglich wächst die Bedrohungslandschaft.

„Viele, wenn nicht sogar die meisten OT-Umgebungen sind wie Inseln, die seit Urzeiten isoliert waren“, erklärt Joe Robertson, Director of Information Security und EMEA CISO bei Fortinet. „Ihr Ökosystem entwickelte sich isoliert, weil die Air Gap zwischen dem OT-Netzwerk und dem Rest der IT-Umgebung sie geschützt hat. Infolgedessen sind viele OT-Systeme über Jahrzehnte gewachsen. Sie verwenden veraltete Technologien, haben wenig oder keine integrierte Security und sind deshalb verwundbar. Die Verbindung mit einem IT-Netzwerk öffnet OT-Umgebungen für die aggressive Welt der Cyberattacken und Malware, auf die sie nicht vorbereitet sind.“

Security-Teams müssen daher den OT-Systemen große Aufmerksamkeit schenken, nicht nur in Fabriken und Produktionsanlagen, sondern auch im Bereich kriti-

scher Infrastrukturen (KRITIS). Zu diesen gehören Kraftwerke, Wasseraufbereitungsanlagen, Ölplattformen und sogar Verkehrsleitsysteme. Sie sind anfällig für Angriffe, und sollte ein Hacker erfolgreich in ihre Netzwerke eindringen, wäre die schlimmstenfalls nationale Sicherheit gefährdet.

Die wichtigsten OT-Sicherheitsbedrohungen

In den ersten sechs Monaten des Jahres 2020 sind dem Forschungsteam von Fortiguard Labs unter anderem zwei bedeutende Entwicklungen im Bereich OT-Bedrohungen aufgefallen, die im Threat Landscape Report festgehalten sind.

Dies ist erstens die im Januar festgestellte Zunahme der Aktivitäten im Bereich von IPS-Sensoren in den USA, Deutschland und Brasilien. Der Anstieg betraf vor allem Modbus, TCP-Server und SPS-Systeme. Dieser Aktivitätsschub hatte das Potenzial, kritische Daten und Informationen offenzulegen. Letztendlich machten Modbus-bezogene Erkennungen die Mehrzahl der Bedrohungen aus, die in diesem Zeitraum auf OT-Systeme abzielten.

Auch wenn einige dieser Auslöser nicht bösartig waren, sollte man sie weiterhin beobachten. Ein Angriff, der das SCADA-Netzwerk infiltriert, könnte über den Zugriff auf den Modbus-Controller ernsthafte Verluste verursachen. Der zweite Punkt: Im Mai entdeckten Forscher das Spionage-Framework Ramsay, das für das Sammeln und Exfiltrieren sensibler Dateien in stark eingeschränkten oder isolierten Netzwerken entwickelt wurde – Merkmale, die einen kleinen Prozentsatz von OT-Umgebungen definieren. Obwohl es schwierig ist, festzustellen, wie lange die Ramsay-Malware schon aktiv ist, brachten einige Experten die Bedrohung mit der älteren APT-Einheit Darkhotel in Verbindung. Es bedarf zwar noch weiterer Forschung, es scheint jedoch, dass Hacker offensichtlich Nutzen im Angriffspotenzial von Ramsay sehen.

Raffiniertere Angriffe

Seit der Entdeckung von Stuxnet sind Cyberkriminelle noch raffinierter und engagierter in ihren Bemühungen geworden, OT-Netzwerke anzugreifen. Nach dem Ausbruch der COVID-19-Pandemie ließ sich ein weiterer Anstieg an OT-Angriffen beobachten. Um dem entgegenzuwirken, müssen Unternehmen eine proaktive Verteidigungsstrategie entwickeln, die ihre OT-Umgebungen abschottet, aktuelle Threat Intelligence nutzen und ihre Taktiken ständig analysieren und weiterentwickeln.

Eine Möglichkeit, den Angreifern einen Schritt voraus zu sein, ist die Nutzung des Mitre Att&ck-Frameworks. Fortiguard Labs empfiehlt Unternehmen zunächst, die Sicherheitskontrollen auf aktuelle Infiltrationstechniken zu testen, um sicherzustellen, dass sie vor diesen schützen oder diese zumindest erkennen. Aufgedeckte Lücken sollten sie festhalten und diese Daten verwenden, um zukünftige Verbesserung zu priorisieren.

Es ist darüber hinaus wichtig, dass die OT-Security-Lösungen in den Bedrohungsschutz der IT-Umgebungen von Unternehmen integriert sind. Diese Lösungen müssen nicht nur das Rechenzentrum, sondern auch die Cloud und den Netzwerkperimeter abdecken. Durch die Anwendung allgemeiner Best Practices für Cybersicherheit gewinnen Organisationen neben der automatisierten Erkennung von Analysen in Echtzeit an Transparenz und Kontrolle innerhalb der OT-Umgebung.

Durch den Einsatz solcher Strategien können Unternehmen einen aktiven Verteidigungsansatz gegenüber Cyberkriminellen verfolgen, die es auf OT-Umgebungen abgesehen haben. Dieser Ansatz konzentriert sich auf Transparenz, Kontrolle und Automatisierung.Darüber hinaus vermeidet man Latenzzeiten, schafft Skalierbarkeit und macht schnelle Analysen möglich, um die Sicherheit und Produktivität von OT-Systemen zu gewährleisten.

Rick Peters/jos

Rick Peters ist CISO Operational Technology bei Fortinet.

SASE-Testreihe, Teil 1: Cato Networks

Security-Services aus der Cloud

Cato Networks betreibt ein eigenes globales WAN und stellt dadurch aus der Cloud heraus leistungsfähige SASE-Funktionen (Secure Access Service Edge) bereit. Erfolgt die Standortanbindung über Cato-eigene SD-WAN-Geräte (Software-Defined WAN), lassen sich auch Funktionen wie Ende-zu-Ende-QoS (Quality of Service) nutzen. Für die Einbindung mobiler Mitarbeiter setzt Cato auf einen Software-Defined Perimeter (SDP).

Zum Auftakt der neuen LANline-Testreihe über SASE-Lösungen tritt Cato Networks an. Der Hersteller verfügt über einen eigenen weltweiten WAN-Backbone und kann damit Sicherheitsdienste überall auf der Welt aus der Cato-Cloud heraus performant bereitstellen. Zudem bietet Cato für die Anbindung von Unternehmensstandorten eigene SD-WAN-Geräte an, womit eine Ende-zu-Ende-Kontrolle des geschäftlichen WAN-Verkehrs mit zentral verwalteten Zugriffsregeln und einer garantierten Quality of Service möglich ist. Cato liefert damit eine SASE-Lösung aus einer Hand, die SD-WAN-Services und Cloud-basierte Sicherheitsfunktionen nahtlos integriert (siehe „Secure Edge löst Perimeter ab“, LANline 04/2021, Seite 16).

Catos SASE-Lösung kommt unter anderem bei Unternehmen zum Einsatz, die ihre bisher für die Standortkopplung genutzten MPLS-Netze durch ein modernes und flexibel konfigurierbares SD-WAN ablösen wollen. Auch für die infolge der Corona-Pandemie stark gestiegene Nachfrage nach einer sicheren und leistungsfähigen Anbindung von Heimarbeitsplätzen an das Unternehmensnetz bietet Catos Cloud-basierte Plattform eine geeignete Lösung. Alle SD-WAN-Geräte und SDP-Endpunkte verbinden sich immer mit dem nächstgelegenen Cato-POP (Point of Presence), um eine möglichst hohe Performance zu gewährleisten.

Auch bei Cloud-Providern wie Amazon Web Services (AWS) oder Microsoft Azure laufende Workloads lassen sich in die SASE-Cloud integrieren. Diese Architektur stellt sicher, dass der gesamte Datenverkehr eines Unternehmens immer über die zentralen Security-Engines der Cato-Cloud läuft. Für Unternehmen bietet die SASE-Lösung zudem den Vorteil, dass der Hersteller die Plattform bei steigenden Kapazitäts- oder Performance-Anforderungen automatisch erweitert: Cato sorgt dafür, dass die in der Cloud laufenden zentralen Security-Systeme immer den gesamten Datenverkehr eines Anwenders mit hoher Performance verarbeiten können.

Mit Catos SD-WAN-Geräten lässt sich der volle Funktionsumfang der Cloud-basierten SASE-Lösung nutzen.

Catos Sicherheitslösung arbeitet nach dem Zero-Trust-Prinzip und lässt nur Datenverkehr passieren, den der Administrator explizit erlaubt hat. Erst nachdem dieser die erforderlichen Regelwerke konfiguriert hat, dürfen Benutzer, Geräte und Anwendungen miteinander kommunizieren. Die Verwaltung der Firewall-Regeln erfolgt über eine zentrale Management-Konsole in der Cloud. Auf den lokalen SD-WAN-Geräten lassen sich zusätzliche Regeln für die Kommunikation innerhalb des jeweiligen Standorts konfigurieren.

Zero-Trust und Single Pass

Zu den von Cato bereitgestellten Sicherheitsfunktionen zählt ein Secure Web Gateway, das den Internet-Traffic überwacht und Zugriffe auf alle als gefährlich oder als nicht zulässig klassifizierten Seiten blockiert. Eine Anti-Malware-Lösung führt eine Deep Packet Inspection durch, um potenziell gefährliche Dateien zu erkennen und zu blockieren. Ein IPS (Intrusion Protection System) untersucht den gesamten Datenverkehr auf mehreren Ebenen und lässt sich im Monitormodus oder mit aktiviertem Blocking betreiben. Security-Spezialisten von Cato betreiben das IPS. Die Anwender sind so automatisch vor aktuellen Bedrohungen geschützt, sobald Cato sie erkannt hat. Um alle Sicherheitsüberprüfungen möglichst effizient durchführen zu können, verwendet die modular aufgebaute Cato-Software eine Single-Pass-Architektur: Cato entschlüsselt verschlüsselte Datenpakete, die verschiedenen Security-Engines verarbeiten sie, danach werden sie wieder verschlüsselt.

Anwender können ihre eigenen Netze entweder selber überwachen und verwalten oder den Managed Service eines Cato-Dienstleisters nutzen. Mit MDR (Managed Detection and Response) bietet Cato einen Premium-Service an, bei dem das hauseigene SOC-Team (Security Operations Center) den Datenverkehr eines Unternehmens permanent überwacht und auf mögliche Bedrohungen untersucht. Die SASE-Lösung erstellt fortlaufend umfangreiche Netzwerk- und Security-Event-Protokolle,

die sich für weitergehende Auswertungen an SIEM-Anwendungen übergeben lassen. In der Cato-Konsole kann der Administrator aktuelle und historische Analysen und Berichte erstellen. Cato speichert dazu die Event-Daten für die letzten zwölf Monate in der Cloud.

SD-WAN-Box anschließen und loslegen

Für den LANline-Test stellte Cato das Modell Socket X1500 mit zwei WAN-, zwei LAN- und zwei USB-Ports zur Verfügung. Mit dem X1700 ist auch ein System für größere Unternehmen erhältlich. Cato unterstützt die Bündelung mehrerer SD-WAN-Verbindungen und hochverfügbare Konfigurationen mit zwei Geräten. Die SD-WAN-Geräte lassen sich denkbar einfach in Betrieb nehmen. Vor dem ersten Einschalten gilt es lediglich, sie in der Cato-Cloud zum Kundenkonto hinzuzufügen und mit den Konfigurationsdaten des Standortnetzes zu erfassen. Im LANline-Testnetz erfolgt der Internet-Zugang (50/10 MBit/s) über einen Linksys-Router mit DSL-Modem. Für die Inbetriebnahme der SD-WAN-Box verbanden wir den LAN-Port des Linksys-Geräts mit dem WAN-Port des Cato-Systems und hängten den LAN-Switch vom Linksys auf einen LAN-Port des SD-WAN-Geräts um. Die Cato-Box übernahm anschließend automatisch die Default-Gateway-IP-Adresse vom Linksys-Router, wodurch der gesamte Datenverkehr in die Außenwelt nun über das Cato-Device geroutet wurde. Zudem lud sich das Gerät die aktuelle Firmware aus der Cato-Cloud herunter und aktualisierte sich selbständig.

Die Einbindung von VM-Workloads, die bei AWS oder Azure in der Cloud laufen, erfolgt über virtuelle vSocket-Systeme, die beim Provider installiert sind. Damit verhält sich eine Cloud-Region wie ein Kundenstandort und unterstützt dieselben Funktionen. Der Datenverkehr eines Unternehmens läuft bei diesem Szenario nicht mehr über eine direkte WAN-Verbindung zu AWS oder Azure, sondern über den Cato-Backbone. Um andere Hyperscaler wie zum Beispiel Google an die Cato-Cloud anzubinden, unterstützt der Hersteller auch Standard-IPSec-VPN-Tunnel. Unternehmen können ihre Standorte auch per IPSec-VPN mit der Cato-Cloud verbinden.

SDP für Client-Zugriffe

Die Einbindung von Heimarbeitsplätzen und mobilen Mitarbeitern ist auf mehreren Wegen möglich. Der größte Funktionsumfang steht mit Catos VPN-Client zur Verfügung, der für Windows, Linux, macOS, iOS und Android erhältlich ist. Der Anbieter unterstützt auch einen agentenlosen Software-Defined Perimeter. Benutzer greifen dabei per Web-Browser auf Catos Anwendungsportal zu und erhalten beim Login die für sie definierten Berechtigungen. Die Benutzerverwaltung lässt sich mit LDAP- und Active-Directory-Verzeichnisdiensten integrieren. Die Lösung unterstützt auch ein Single Sign-on mit Lösungen wie Azure AD, Office 365, Google oder Okta.

Um die Remote-Zugriffe zu testen, konfigurierten wir in der Cato-Konsole im VPN-Menü einen IP-Bereich für die VPN-Benutzer. Zudem legten wir einen Notebook- und einen iPhone-Benutzer an und gaben für jeden Account eine eigene E-Mail-Adresse an. Dann öffneten wir auf dem Testnotebook Catos Aktivierungs-E-Mail. Über den darin enthaltenen Download-Link installierten wir den VPN-Client. Bei der ersten Anmeldung am VPN muss der Benutzer sein Passwort und den Namen des Cato-Firmenkontos eingeben. Der VPN-Client lud anschließend automatisch seine Konfiguration aus der Cloud herunter und stellte die Verbindung zum LANline-Testnetz über den Cato-Backbone her. Bereits nach wenigen Sekunden zeigte die Management-Konsole den Notebook-VPN-Benutzer als neue Verbindung. Nachdem wir für den Notebook-Benutzer in der Cato-Konsole eine Firewall-Regel eingerichtet hatten, die den RDP-Zugriff auf den Testnetzstandort erlaubt, konnten wir uns über die VPN-Verbindung an den Test-Servern anmelden.

Im nächsten Schritt richteten wir auf dem iPhone den VPN-Client ein. Das Vorgehen war weitgehend dasselbe wie mit dem Notebook, auch das iPhone verband sich auf Anhieb mit der Cato-Cloud.

Zum Abschluss konfigurierten wir in der Cato-Management-Konsole eine neue Applikation, um Fernzugriffe auf Ressourcen im LANline-Testnetz per Web-Browser zu ermöglichen. Dafür installierten wir im Testnetz auf einem Windows-IIS-Web-Server die Web-Anwendung Myrtille, die eine einfache Konsole für den Aufbau von RDP- und SSH-Verbindungen bereitstellt. Nachdem wir Myrtille in Catos Applikationsportal hinzugefügt und die erforderlichen Firewall-Regeln konfiguriert hatten, konnten wir uns von beliebigen Rechnern aus über das Internet am Portal anmelden, auf die Myrtille-Web-Anwendung zugreifen und RDP-Verbindungen zu den Servern im LANline-Testnetz aufbauen.

Gelungenes Gesamtpaket

Catos SASE-Lösung überzeugte im LANline-Test durch eine schnelle Inbetriebnahme der SD-WAN-Geräte an den Standorten. Die per SASE-Cloud bereitgestellten Sicherheitsfunktionen sind für alle Benutzer, Geräte und Anwendungen unabhängig vom jeweiligen Standort verfügbar. Die VPN-Konfiguration der Clients bereitete im Test keine Probleme. Auch im Applikationsportal ließ sich mit wenig Aufwand ein Browser-Zugriff auf Web-basierte Anwendungen einrichten. Die Preise für die SASE-Lösung hängen stark vom Projektumfang ab und sind deshalb nur auf Anfrage erhältlich. Die Lizenzierung richtet sich nach der benötigten WAN-Bandbreite.

Christoph Lange/wg

Tested by LANline IT = Network = Datacenter

Cato Networks

https://www.catonetworks.com

- Schnelle Inbetriebnahme und einfache Konfiguration
- Flexible Anbindung mobiler Mitarbeiter über VPN-Client oder agentenlos per Web-Browserzugriff auf das Applikationsportal
- Umfangreiche Sicherheitsfunktionen mit effizienter Single-Pass-Engine
- Weltweiter WAN-Backbone mit eigenen POPs an allen wichtigen Standorten

Nachhaltigkeit und „IT Made in Germany“

Die Zukunft der Rechenzentren

Die Digitalisierung hat derzeit durch COVID-19 und den Wechsel der Beschäftigten ins Home-Office einen enormen Schub erfahren. Die Datenmengen wachsen nahezu ins Unermessliche, was unter anderem aus dem vermehrten Konsum von Streaming-Services, der Remote-Arbeit und der steigenden Zahl an Videokonferenzen resultiert. Die Bedeutung der RZs nimmt gleichermaßen zu.

Rechenzentren sind das Rückgrat der Digitalisierung und verantwortlich für die Datenverarbeitung. Doch auch Rechenzentren wandeln sich: Die Betreiber stehen vor wachsenden Anforderungen und aktuellen Entwicklungen, um für die Zukunft gerüstet zu sein. Es gilt zu klären, welche Trends sich abzeichnen. Welche Faktoren beim Rechenzentrum der Zukunft eine zentrale Rolle spielen, ist für Planer, Betreiber und Nutzer interessant.

Nachhaltigkeit wird zum Wettbewerbsvorteil

Nachhaltigkeit und Green IT sind längst kein bloßer Trend mehr, sondern entscheidend für die positive Außenwahrnehmung von Unternehmen und deren Fortbestehen auf dem Markt. Wirtschaftlichkeit und Nachhaltigkeit schließen sich in der IT nicht mehr aus – im Gegenteil. Betrachtet man jedoch den aktuellen Energieverbrauch von Rechenzentren, gibt es hier noch einiges zu tun, denn RZs sind massive Energiefresser. Allein in Frankfurt am Main waren Rechenzentren mit 1,3 Terawattstunden für etwa ein Fünftel des Gesamtstromverbrauchs verantwortlich. Sie sind somit der größte gewerbliche Stromabnehmer der Stadt – noch vor dem Frankfurter Flughafen. Eine Studie der Europäischen Kommission zeigt, dass der Energieverbrauch von Rechenzentren in der EU voraussichtlich von 2,7 Prozent des Strombedarfs im Jahr 2018 auf 3,2 Prozent bis 2030 ansteigen wird. Es ist also Zeit, dass Rechenzentren nicht nur in Frankfurt am Main grüner werden und auf den steigenden Energieverbrauch reagieren.

Generell gibt es verschiedene Optionen, um den Energieverbrauch von Rechenzentren möglichst gering zu halten. Dazu zählen eine energiesparende Planung, ein optimierter Betrieb sowie der Einsatz passender Komponenten, die auch im Teillastbereich hocheffizient arbeiten. Größtes Potenzial für einen energieeffizienteren und nachhaltigeren Betrieb von Rechenzentren bilden innovative Techniken rund um neue Kühlkonzepte und die Abwärmenutzung. Die Abwärme von Rechenzentren bietet ein enormes Potenzial und lässt sich nachhaltig nutzen, zum Beispiel für das Heizen von Wohnungen oder Bürogebäuden. Eine weitere Möglichkeit ist die Einspeisung der Energie in das Fernwärmenetz. Rechenzentren und Rechenzentrumsbetreiber sind allerdings auf Unterstützung angewiesen. Voraussetzung für die Implementierung innovativer Technik ist, dass Städte, Regierung und Unternehmen die nötigen Budgets für die Forschung auf diesem Gebiet bereitstellen, um die Zukunft grüner zu gestalten.

Entscheidende Messgröße für die Energieeffizienz von Rechenzentren ist bekanntlich der PUE-Wert (Power Usage Effectiveness). Dieser Wert beschreibt die Energieeffizienz eines Rechenzentrums. Er stellt das Verhältnis zwischen Gesamtenergieverbrauch des Rechenzentrums und dem Energieverbrauch der gesamten IT dar. Je niedriger der PUE-Wert eines Rechenzentrums, desto umweltfreundlicher und energieeffizienter arbeitet es. Will der Betreiber diesen Wert senken, muss er meist seine vorhandene Infrastruktur mit neuer Technik modernisieren. Der PUE-Wert der existierenden Rechenzentren in Deutschland liegt aktuell im Durchschnitt bei 1,9.

Zudem stellt sich die Frage: Wie wird der Strom für den Betrieb eines Rechenzentrums erzeugt? Voraussetzung für einen nachhaltigen Rechenzentrumsbetrieb ist die maximale Nutzung regenerativer Energiequellen wie Wasser oder Wind. Einige europäische Standorte wie die Nordsee oder Skandinavien bieten dabei durch ihre Lage und die klimatischen Bedingungen einige Vorteile. Betreibt ein Anbieter sein Rechenzentrum beispielsweise in Skandinavien, lassen sich aufgrund der geringeren Außentemperatur Energie und somit Kosten für die Kühlung einsparen. Sollen Unternehmen also ihr Rechenzentrum außerhalb Deutschlands in kühleren Regionen betreiben?

IT Made in Germany

Die Geschäftswelt arbeitet immer stärker global und rückt zusammen, doch die Corona-Pandemie hat dieser Entwicklung einen Strich durch die Rechnung gemacht und sie erst einmal verlangsamt. Der Trend hin zu einem Rechenzentrumsstandort im kalten Skandinavien oder Island kehrt sich derzeit um. Durch ständig wechselnde Reisebeschränkungen und strengere Grenzkontrollen wird es immer schlechter planbar, in Länder außerhalb Deutschlands oder der EU zu reisen. Dies stellt Unternehmen vor die Herausforderung, dass bei Wartungsarbeiten oder Störungen im Rechenzentrum ein schnelles, manuelles Handeln nicht mehr ganz einfach möglich ist. Besser sieht es für Unternehmen aus, die ihr Rechenzentrum vor Ort haben. Der Trend geht also zurück zum eher heimischen Rechenzentrumsbetrieb und „IT Made in Germany“.

Sollte jedoch in Zukunft jedes Rechenzentrum, das deutsche Unternehmen nutzen, in Deutschland betrieben werden, würden die Kapazitäten an ihre Grenzen stoßen. Der Flächenverbrauch von Rechenzentren wächst vor allem in Ballungszentren wie Frankfurt am Main immer weiter. Dies hat nicht nur enorme negative Auswirkungen auf die Stromversorgung – irgendwann fehlt es schlussendlich schlicht auch an nötigen Flächen. Die Frage lautet folglich: Wohin also mit den Rechenzentren?

Der Trend geht immer stärker hin zu Regionalität, also dezentrale Rechenzentren abseits der großen Ballungsräume. Unternehmen wünschen sich verstärkt ein Rechenzentrum mit besonders geringer Distanz zum Unternehmensstandort. Durch kürzere Wege sparen sie Zeit und Geld – und fördern auch einen nachhaltigen Rechenzentrumsbetrieb. Kommt es in Großstädten vermehrt zu Platzmangel, bieten sich Colocation-Rechenzentren an. Diese werden in Zukunft eine zentrale Rolle spielen, da sie mehr Flexibilität ermöglichen und die Rechenzentrumsfläche meist vielen Kunden gleichzeitig bereitsteht. Colocation-Rechenzentren bieten Unternehmen die Möglichkeit, individuell benötigte Rechenzentrumsfläche, Racks oder Cages anzumieten – die Fläche ist sogar im laufenden Betrieb skalierbar – ein großer Vorteil, besonders mit Blick auf die Zukunft, in der der Bedarf an Rechenzentrumskapazitäten weiter steigen wird. Bereits jetzt melden Colocation-Rechenzentren Auslastungsrekorde.

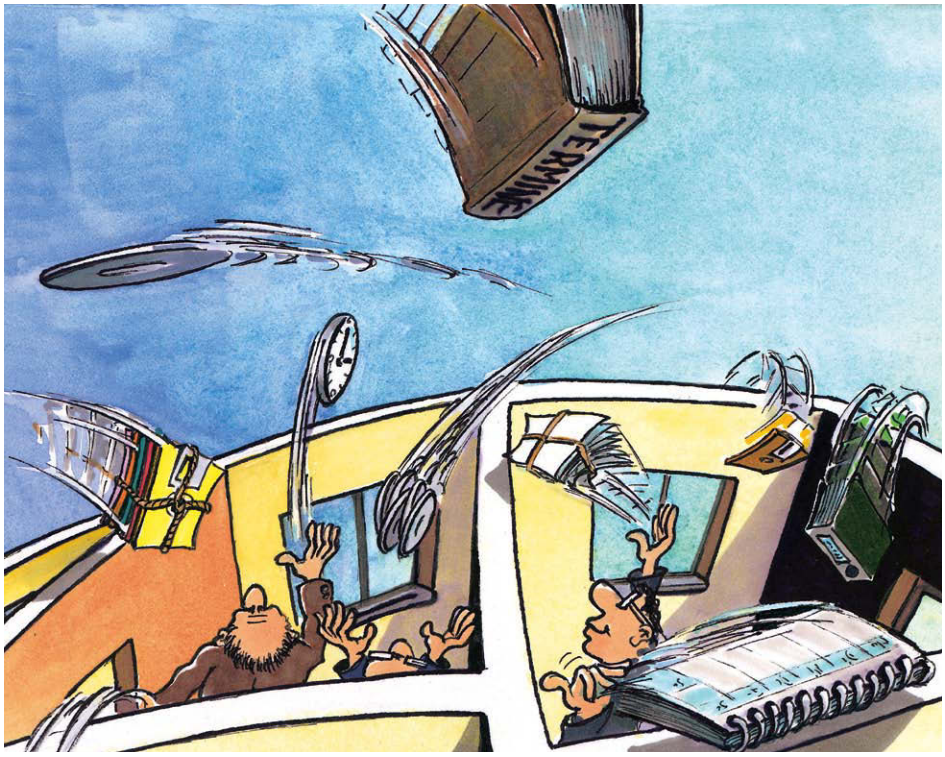
Doch Unternehmen müssen sich nicht zwingend für eine Rechenzentrumsvariante entscheiden – stattdessen sind verschiedene Services und Rechenzentrumsanbieter kombinierbar, um bestmöglich von den jeweiligen Modellen zu profitieren und durch eine Kombination die am besten für das Unternehmen geeignete Lösung zu finden. Der Trend geht also hin zu einem hybriden Rechenzentrumsbetrieb mit eigenem Rechenzentrum, Colocation-Anteil sowie Cloud-Anteil. Während große Konzerne ihre IT-Infrastruktur komplett in die Cloud verlagern, ist ein solches Mammutprojekt für die meisten mittelständischen Unternehmen aufgrund fehlender Ressourcen kaum möglich – und nicht unbedingt wirtschaftlich sinnvoll. Aus diesem Grund migrieren sie oft nur Teilbereiche der IT in die Cloud – der „Rest“ ist in einem Colocation-Rechenzentrum oder dem unternehmenseigenen Rechenzentrum untergebracht. Die Kombinationsmöglichkeiten sind vielfältig.

Die Entwicklung hin zu hybriden Rechenzentrumsstrukturen erlaubt es Unternehmen, sensible Daten im Griff zu behalten und gleichzeitig die steigenden Anforderungen der Kunden an Kapazitäten und Rechenleistung zu erfüllen. In Zukunft liegt der Fokus verstärkt auf der nahtlosen Kommunikation zwischen On-Premise, Cloud und Edge. Wolfgang Kaufmann/jos

Wolfgang Kaufmann ist Geschäftsführer bei Datacenter One.

5G versus Wi-Fi 6

Die Wireless-Standards im Vergleich



Wenn es um die Vernetzung der Zukunft geht, steht so gut wie immer 5G im Fokus. Es scheint, als würde WLAN als Funktechnik schon bald nur noch eine untergeordnete Rolle spielen. Doch der Eindruck täuscht: Mit Wi-Fi 6 gibt es auch hier einen neuen Standard, der zahlreiche Verbesserungen mit sich bringt. Technikunternehmen wie Cisco setzen beispielsweise sowohl auf 5G als auch auf Wi-Fi 6, denn beide ermöglichen neue Anwendungen, erhöhen die Netzwerkkapazität und bieten höhere Datenraten. Interessierte sollten wissen, worin sich die Techniken unterscheiden und welche sich für bestimmte Anwendungsfälle am besten eignet.

Wi-Fi 6 ist auch bekannt als 802.11ax. Die neue WLAN-Generation nutzt Bänder im etablierten Frequenzbereich bei 2,4 und 5 GHz, bringt aber Verbesserungen beim Durchsatz, bei der Unterstützung mehrerer Geräte sowie bei der Bandbreiteneffizienz mit.

Im Optimalzustand erreicht Wi-Fi 6 Datenübertragungsraten bis zu 10 GBit/s, Wi-Fi 5 erreicht zum Vergleich maximal 1,5 bis 2 GBit/s. In der Praxis sind bis zu 30 Prozent höhere Datenübertragungsraten realistisch. Der größte Vorteil ist aber, dass die Bedienung von deutlich mehr mobilen End- und IoT-Geräten gleichzeitig mit geringerer Verzögerung erfolgen kann. Gebäudekomplexe, Firmengelände und Produktionshallen lassen sich damit völlig drahtlos vernetzen.

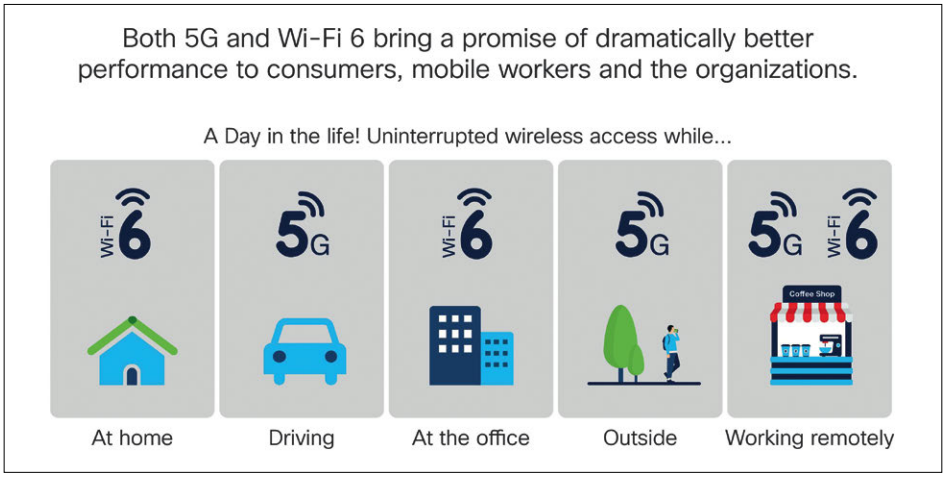
Auch wo überlastete WLANs gang und gäbe sind – an öffentlichen Plätzen, an Flughäfen und auf Messen – kann Wi-Fi 6 Abhilfe schaffen. Durch einen starken Anstieg von datenhungrigen Anwendungen wie Videokonferenzen wird dies umso wichtiger. Wi-Fi 6 eignet sich daher optimal für die Vernetzung von Innenräumen und klar abgegrenzten Gebieten.

5G vernetzt den Außenbereich

5G wird hingegen den Ausbau offener, komplexer Systeme durch die Vernetzung mobiler Geräte und Prozesse vorantreiben – von autonomen Fahrzeugen über verteilte Produktionsstandorte bis hin zu Smart Cities. In Deutschland läuft der 5G-Ausbau entsprechend auf Hochtouren. So macht die Deutsche Telekom heute für zwei Drittel der Bevölkerung 5G potenziell verfügbar, bis Ende 2021 sollen es sogar 80 Prozent sein. Laut Cisco Annual Internet Report werden 2023 18 Prozent aller mobilen Verbindungen in Deutschland

über 5G abgedeckt sein. Die durchschnittliche 5G-Geschwindigkeit liegt dann bei zirka 700 MBit/s. Im Vergleich: 4G kommt auf ein Tempo von 30 MBit/s.

Noch wichtiger als neue Geschwindigkeitsrekorde ist, dass 5G Informationen ultraschnell und besonders zuverlässig übermittelt. Im vernetzten Verkehr und in Fabrikanlagen macht die geringe Latenzzeit den entscheidenden Unterschied: Liegt die Antwortzeit im 4G-Netz noch bei etwa 30 Millisekunden, beläuft sie sich bei 5G nur noch bei rund einer Millisekunde. Dies bedeutet, dass sich Daten nahezu in Echtzeit übertragen lassen.



Veranschaulichung der Einsatzmöglichkeiten von Wi-Fi 6 und 5G. Bild: Cisco

Was wird die Zukunft bestimmen?

Vereinfacht zusammengefasst ist Wi-Fi 6 also der neue Funkstandard für den Innenbereich, 5G für den Außenbereich. 5G wird das WLAN schon allein deshalb nicht ersetzen, weil die Kosten deutlich höher sind.

Die Infrastruktur von 5G wird von den Netzbetreibern bereitgestellt. Für die Nutzung der Frequenzen entstehen hohe Lizenzkosten, die sie an die Anwendenden weitergeben müssen. Die Frequenzbänder von Wi-Fi 6 sind hingegen wie bei den vorherigen WLAN-Standards lizenzfrei, also kostenlos nutzbar. Unternehmen, Organisationen und Privatpersonen müssen lediglich die Infrastruktur wie Router, Stationen und Repeater bereitstellen.

Wi-Fi 6 und 5G ergänzen sich also, um flächendeckende drahtlose Konnektivität der nächsten Generation zu gewährleisten.

Im zukünftigen Alltag werden Personen ununterbrochen verbunden sein. Durch ein Zusammenspiel der beiden Standards wird man in den verschiedenen Bereichen der Arbeits- und Lebenswelt zwischen 5G und Wi-Fi hin- und herwechseln. Beide sind erforderlich, um das volle Potenzial neuer Entwicklungen wie IoT, Industrie 4.0 und Smart Cities zu nutzen. Die Vernetzung von Maschinen, Fahrzeugen und Geräten, vor allem im industriellen Umfeld, wird das auf ein komplett neues Niveau heben und einen signifikaten Digitalisierungsschub in Deutschland bewirken.

Cisco hat sich aus diesem Grund beiden Techniken verschrieben. Neben dem Angebot für Wi-Fi 6 (Router, Switches und Cloud-Services wie Meraki) stellt das Unternehmen auch sämtliche Techniken für den Mobilfunkstandard bereit – mit Ausnahme von Funkmasten. Dirk Wettig/am

Dirk Wettig ist Client Director Deutsche Telekom Account bei Cisco Deutschland.

News

Commscope erweitert das Ruckus-Wi-Fi-6-Portfolio

Wi-Fi 6 Access Points für IoT-Konnektivität und mehr

Commscope, Anbieter von Infrastrukturlösungen für Kommunikationsnetzwerke, hat Ergänzungen seines Wi-Fi-6-Access-Point-Portfolios angekündigt. Dies betrifft das Access-Point-Modell Ruckus H550 für den Innenbereich und den Ruckus T350 für den Außenbereich. Außerdem gibt es neue Funktionen für Unternehmen und Service-Provider im Ruckus SmartzoneOS.

Eine moderne Geräteumgebung umfasst bekanntlich oft zahllose WLAN-fähige Endbenutzer-Computer und eine schwindelerregende Anzahl von IoT-Endpunkten, die über verschiedene Funktechniken wie WLAN, Bluetooth Low Energy (BLE) und Zigbee kommunizieren.

Der H550 und der T350 beherrschen laut Hersteller alle drei Protokolle und ermöglichen es Unternehmen damit, eine einzige, konvergierte Netzwerkinfrastruktur zu implementieren, die sowohl die Bedürfnisse der Endbenutzer als auch die betrieblichen Anforderungen unterstützt. Dazu gehören auch das Gebäude- und Energie-Management, Asset-Tracking, physische Sicherheit und Telemetrie.

Unternehmen können diese APs mit jeder Ruckus-Management-Option verwalten, so Commscope, einschließlich SmartzoneOS-basierender Netzwerk-Controller, der hauseigenen Cloud und Ruckus Unleashed. Die Access Points dienen bei Bedarf auch als Datenquelle für die von Ruckus Analytics bereitgestellten Netzwerkanalysefunktionen mit künstlicher Intelligenz (KI) und maschinellem Lernen (ML). SmartZoneOS ist eine Familie von physischen und virtuellen Netzwerk-Controllern, die von Service-Providern und Unternehmen für die Verwaltung von kabelgebundenen und drahtlosen Netzwerken im Einsatz sind, so die Commscope-Erläuterung. jos

Wireless WAN: Reichweite am Netzwerkrand

Gründe für eine kabellose Zukunft

Die Corona-Pandemie hat eine Netzwerktransformation beschleunigt, die sich schon länger abzeichnete: Den Übergang von kabelgebundenen Netzwerken zu Wireless WANs. Ähnliche Anforderungen haben den Wechsel von Wired-Ethernet-LANs zu WLAN vorangetrieben. Mit der Verbesserung von Zuverlässigkeit, Sicherheit, Entfernung und Bandbreite übertrumpften die Flexibilität und Wirtschaftlichkeit von WLAN die des kabelgebundenen LANs. LTE und der Mobilfunkstandard 5G haben einen ähnlichen Effekt auf Wired WANs – insbesondere dann, wenn sie mit den Funktionen von softwaredefinierten WANs (SD-WANs) integriert sind.

Die SD-WAN-Technik schafft mit ihren Funktionen für Unternehmensnetzwerke neue Möglichkeiten. Dazu gehört unter anderem die Konsolidierung mehrerer Netzwerkfunktionen, die zur Senkung von Hardware- und Betriebskosten beitragen. Auch die Unterstützung multipler WAN-Links ist als signifikanter Faktor zu nennen, da sich so die Zuverlässigkeit verbessert und die Bandbreitenaggregation sowie die Trennung des Datenverkehrs möglich sind. Die Anwendungserkennung und das richtlinienbasierte Routing eröffnen zudem neue Wege zur Netzwerkoptimierung. Hinzu kommt, dass das zentrale, Cloud-basierte Management die Bereitstellung und Verwaltung von Netzwerkgeräten vereinfacht. Solange die daraus resultierenden Netzwerke jedoch immer noch kabelgebunden sind, lassen sich die Vorteile der Technik nicht vollumfänglich nutzen. Um mehr Vielfalt, Flexibilität und Reichweite in die Unternehmensnetzwerke zu bringen, bedarf es Wireless WANs. Grundlage dafür ist ein zuverlässiges WAN, das sich durch die Unterstützung verschiedener Netzwerkverbindungsarten erreichen lässt. Um über Mobilfunkverbindungen zu verfügen, eignet sich die Ergänzung von Wireless-Edge-Lösungen. Damit lassen sich die Reichweite der Unternehmensnetzwerkfunktionalität vergrößern und die gewünschten Personen, Orte oder Geräte einfach anbinden. Auf Basis der intelligenten SD-WAN-Lösungen kann man einen dynamischen Wechsel zwischen Verbindungen, das Trennen und Priorisieren bestimmter Applikationen oder die schnelle Eröffnung eines neuen Geschäftsstandorts problemlos realisieren. Hierbei spielt auch 5G hinsichtlich geringer Latenzzeiten und hoher Bandbreite eine tragende Rolle.

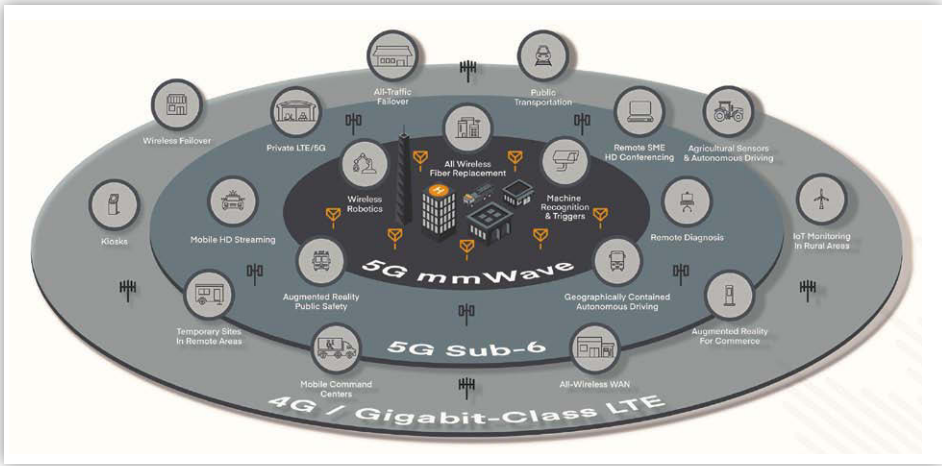


Bild 1. Veranschaulichung der 5G-Business-Landschaft der Zukunft. Bild: Cradlepoint

Mit bezahlbaren Flatrate-Tarifen und größerer Bandbreite durch Gigabit-Class-LTE ist Mobilfunk eine attraktive Alternative oder Ergänzung zu den konventionellen Anbindungen. Die aufkommenden 5G-Dienste bieten in vielerlei Hinsicht gesteigerte Leistungen. 5G ist darauf ausgelegt, niedrige Latenzzeiten zu liefern.

Die kürzeren Reaktionszeiten ermöglichen die uneingeschränkte Nutzung unternehmenskritischer Anwendungen und helfen dabei, Prozesse flexibler zu gestalten. Verbesserte Antennen- und Übertragungstechniken erhöhen die Anzahl der Geräte und Verbindungen, die jede 5G-Station verarbeiten kann. Auf diese Weise lässt sich die drahtlose Unterstützung von IoT-Netzwerken und anderen Anwendungen mit hoher Leistungsdichte realisieren. Da Gigabit-Class-LTE weithin verfügbar ist und die meisten großen Carrier die Einführung von 5G-Services fokussieren, lassen sich nahezu überall und jederzeit hochverfügbare Netzwerke in Betrieb nehmen.

Wireless WANs lösen zahlreiche Probleme für Unternehmensnetzwerke, eröffnen neue Möglichkeiten und legen den Grundstein für weitere Transformationen. Die folgenden fünf Punkte sollen diese im Unternehmenskontext verdeutlichen:

1. Verbesserung des Netzwerk-Failovers: Da Netzwerke die Grundlage für die digitale Transformation von Unternehmen bilden, ist Non-Stop-Verfügbarkeit entscheidend. Dafür eignet sich der Auf-

bau eines mehrschichtigen Systems mit verschiedenen Verbindungsarten – Wired und Wireless. Wired-to-Wireless-Failover wechselt unterbrechungsfrei von einem Verbindungstypen zu einem anderen. Bei LTE-Verbindungen mit geringerer Bandbreite identifizieren und priorisieren SD-WAN-Richtlinien den kritischen Datenverkehr. Mittels Gigabit-Class-LTE- und 5G-Verbindungen ist ein Failover des gesamten Datenverkehrs realisierbar. Insgesamt ist die Bereitstellung drahtloser Failover-Funktionen deutlich schneller und einfacher als die Installation neuer Kabel. Fallen kabelgebundene Verbindungen aus, geht die Netzwerkverwaltungsfunktion zusammen mit dem Remote-Datenverkehr verloren. Da die meisten Störungen des Festnetzes auf der letzten Meile auftreten, fallen die sekundären Festnetzanschlüsse oft ebenfalls aus, sodass die entfernte Einheit nicht erreichbar ist. Wireless-Verbindungen bieten eine effiziente Out-of-Band-Management-Option, die eine direkte Verbindung mit dem Konsolen-Port eines oder mehrerer entfernter Geräte herstellt.

2. Vergrößerung der Netzwerkbandbreite: Ein großer Vorteil von SD-WAN ist die gleichzeitige Aggregation mehrerer Verbindungen, um größere Bandbreite zu erzeugen. Dabei ist die Erweiterung des Kabelnetzwerks um eine Wireless-Verbindung oder die Verwendung mehrerer drahtloser Verbindungen eine leistungsstarke Alternative zur Bandbreitenerhöhung. Mit LTE, das Geschwindigkeiten von bis zu 50 MBit/s erreicht, Gigabit-LTE mit bis zu 350 MBit/s und 5G mit über 1 GBit/s erreichen oder übertreffen die drahtlosen Verbindungsmöglichkeiten schnell die Kapazität herkömmlicher Verbindungen.

3. Wireless zur primären Verbindung machen: Wireless WANs bringen eine größere operative Flexibilität für diverse Unternehmensstandorte. Mit ihnen zeigt sich die Eröffnung oder Verlegung von Filialen und Büros enorm erleichtert. Darüber hinaus ergibt die Technik auch für Geschäftsszenarien Sinn, bei denen drahtlose Netzwerke die einzige Option sind – beispielsweise bei Baustellen oder Pop-up-Stores. Eine weitere Anwendung, bei der sich Wireless als primäre Netzwerkverbindung von Vorteil erweist, ist der Aufbau eines hochredundanten Netzwerks mit reduzierten Betriebskosten. So können Unternehmen eine optimale Standortvernetzung mit maximaler Netzwerkverfügbarkeit sicherstellen – und das mit einem zentralen Management in der Cloud.

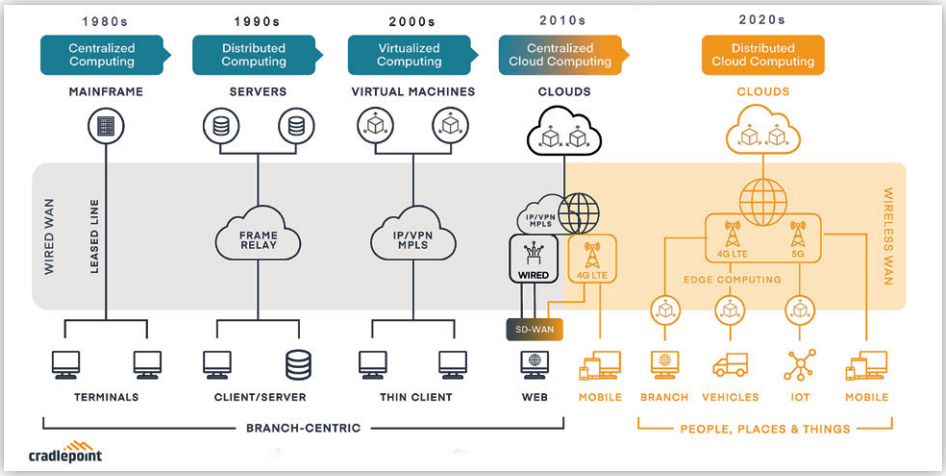


Bild 2. Die Evolution des Wireless WANs. Bild: Cradlepoint

4. Erweiterte IoT-Anwendungen und -Funktionen: Viele denken bei IoT (Internet of Things) an gelegentlich anfallende Daten, die das bestehende Netzwerk nur wenig beeinflussen. Gerade wenn es um Smart Buildings, Smart Cities oder vollautomatisierte Fertigung geht, fallen große Datenmengen an. Stehen diese IoT-Szenarien zwar vielleicht mehr im Rampenlicht, sind bandbreitenintensive Dinge wie Videoüberwachung, Selbstbedienungskioske im Einzelhandel und alle Arten von medizinischem, Fertigungs- und industriellem Betrieb die führenden Anwendungsfälle. Bei solchen groß angelegten IoT-Initiativen sind vor allem die niedrige Latenzzeit und die höhere Bandbreite von drahtlosen Verbindungen entscheidend.

Manchmal sind IoT-Geräte mit integrierten Wireless-Funktionen ausgestattet und können sich direkt mit einem Mobilfunknetz oder WLAN verbinden. Wenn jedoch die Anzahl der Geräte wächst, ist es zu kosten- und zeitintensiv, SIM-Karten und drahtlose Netzwerkabonnements oder Access Points zu verwalten.

Hier setzen Organisationen auf eigene private LTE- oder 5G-Netzwerke, auch als Wide Area LAN bezeichnet. Damit lässt sich kostenkontrolliert der gesamte IoT-Verkehr bündeln und einfacher sowie sicherer administrieren.

5. Steigerung der Business Mobility: Die mobile Unterstützung von Geschäftsprozessen, vor allem in Fahrzeugen, gilt als wachsender Markt für die Datenkonnektivität, da Unternehmen versuchen, auf papierlose Büros umzusteigen und die Datenerfassung zu verbessern. Vieles davon ist bereits mit der LTE-Technik realisiert und bekommt durch 5G noch mehr neue Möglichkeiten. Beispiele hierfür sind Daten- und Video-Uploads in Echtzeit, automatisierte Arbeits- und Routenanpassungen und Konnektivität für das gesamte Fahrzeug. Unternehmensnetzwerke lassen sich nicht mehr durch feste Standorte definieren. Stattdessen bestehen sie aus Menschen, Fahrzeugen, Pop-up-Standorten, Kiosken, Cloud-Diensten und einem ständig wachsenden Universum von IoT-Geräten. Die Expansion des Netzwerk-Edges ermöglicht eine Vielzahl neuer Standorte, Dienste und Initiativen zur digitalen Transformation. Der kombinierte Effekt ist eine größere organisatorische Agilität, die auf der großen Reichweite und den wachsenden Fähigkeiten von Wireless WANs aufbaut. Diese unsichtbaren, aber leistungsstarken Netzwerke, die auf 4G-LTE- und 5G-Technik basieren, bieten schnelle, sichere und flexible Konnektivität, wo und wann immer sie nötig ist. Jan Willeke/am

Jan Willeke ist Area Director Central Europe bei Cradlepoint.

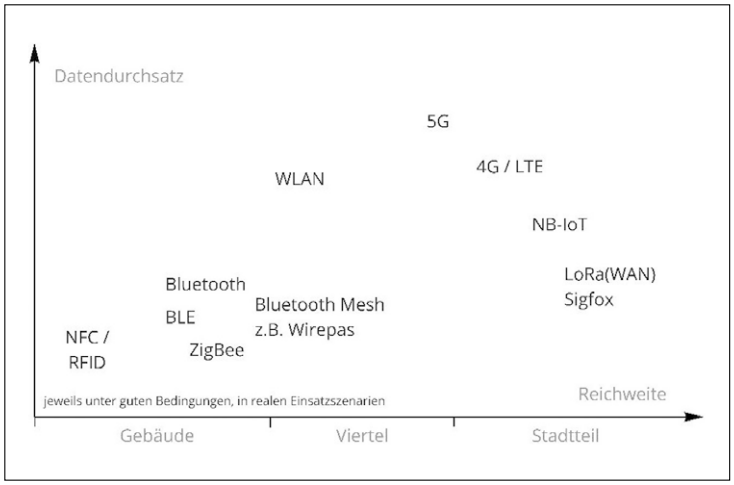
Grundpfeiler von IoT-Strategien

Funktechnik für das IoT

Das Internet der Dinge (IoT) ist oft zur zentralen Aufzeichnung von Messwerten weit verteilter Sensoren in Gebrauch. Dabei ist die Frage nach einer adäquaten Funktechnik immer entscheidender. Die Auswahl der geeigneten IoT-Funktechnik ist komplex. Eine große Rolle spielen bei den zur Verfügung stehenden Angeboten LPWAN-Techniken (Low Power Wide Area Network) wie LoRaWAN – eine LPWAN- oder Niedrigenergie-Weitverkehrnetzwerk-Spezifikation für drahtlose batteriebetriebene Systeme in einem regionalen, nationalen oder auch globalen Netzwerk – und NB-IoT. Lange galten diese Techniken als Lückenfüller, bis beispielsweise 5G kommt. Inzwischen etablieren viele Projekte diese Techniken als Basis für langfristige IoT-Strategien.

Zunächst kommt die Frage auf, was Funktechnik im Zusammenhang mit dem Internet der Dinge interessant macht: Die nicht an ein Kabel gebundene Lösung lohnt sich dann, wenn es darum geht, über eine Stadt verteilte Pegelmesssonden zu verbinden und auszulesen. Oder in Bereichen, in denen sich verkabelte Systeme nicht lohnen, etwa auf einem großen Betriebsgelände, das man nachträglich mit einer Überwachung der Eingangs- und Ausgangslogistik ausgestattet hat. Bis vor Kurzem waren viele Systeme auf dem Markt teuer im Betrieb, da pro Gerät Gebühren an den Netzbetreiber anfielen, oder der Ausbau war kostspielig und aufwendig, da das selbst auszubauende Netz (WLAN) keine große Reichweite besaß.

Nur für kleinere Bereiche, also etwa innerhalb eines Gebäudes, schienen andere Funktechniken wie ZigBee aufgrund ihrer geringen Reichweiten geeignet. Sigfox oder ZigBee sind auf spezielle Anwendungen ausgerichtet und nicht für eine breite, zukunftsoffene IoT-Strategie interessant. Viele dieser existierenden Techniken lohnten sich kaum, weil sie nicht sparsam genug waren, um viele Jahre ohne Batteriewechsel laufen zu können. Ein weiterer Grund ist die Abhängigkeit von der Netzverfügbarkeit des Netzbetreibers, was den Einsatz bei sogenannten Deep-Indoor-Anwendungen (zum Beispiel ein Gaszähler im Keller) erheblich erschwerte. Techniken im LPWAN-Bereich wie LoRaWAN hingegen versprechen hohe Reichweiten, Batterielaufzeiten von mehreren Jahren und die Fähigkeit, ein eigenes lizenzfreies Netz zu betreiben. Ähnliches ist auch von Bluetooth-Mesh zu erwarten. Hier umfassen die Vorteile günstige Sensoren und eine sich selbst erweiternde Netzabdeckung bei eng ausgebauten Sensornetzwerken. Auch wenn sich beide Techniken diese Vorteile mit geringerem Datendurchsatz erkaufen, bleiben sie dennoch interessant, denn die Erfahrung zeigt, dass die meisten Anwendungen nicht dauerhaft viele Datenpakete pro Sekunde benötigen.



Einordnung von Funktechniken unter Berücksichtigung der Parameter Reichweite und Datendurchsatz. Bild: ECBM

Auswahl der passenden Funktechnik

Um die passende Funktechnik für eine langfristig erfolgreiche IoT-Strategie zu finden, bedarf es der Untersuchung einiger Kriterien.

Zunächst sollte die genaue Betrachtung der Marktreife der zur Wahl stehenden Technik erfolgen. Auch wenn eine Funktechnik hervorragende technische Eigenschaften mit sich bringt, ist sie nutzlos ohne ein Ökosystem hochwertiger Endgeräte und Software. Außerdem sollte man auf erprobte und zuverlässige Geräte setzen. Geräte, bei denen der Hersteller Entwicklungsfehler noch nicht behoben hat, sind bei der Installation und im Support womöglich kostspielig. Außerdem sollten Unternehmen nur auf Hersteller setzen, die einen kompetenten Support mitbringen, was im Fall von defekten Geräten oder Firmware-Fehlern vorteilhaft ist.

Neben der Marktreife sollte auch die Verfügbarkeit des Netzes Beachtung finden. 5G oder NB-IoT sind Netze im Aufbau und kommen daher für manche IoT-Anwendungen nicht in Frage, denn wo kein Netz existiert, ist die IoT-Umsetzung nicht möglich. Anzumerken ist außerdem, dass bei NB-IoT-Endgeräten oft der Rückfall auf andere, weniger energiesparende Mobil-

funknetze möglich ist. Spannend ist nach wie vor LoRaWAN. Das Netz lässt sich dank Lizenzfreiheit gut selbst aufbauen. Auch Bluetooth-Mesh, zum Beispiel Wirepas, ist eine mögliche Lösung. Hier erweitert sich ein Netz mit wenigen Gateways durch die Installation weiterer Sensoren selbst.

Auch auf den Gesamtkosten der Funktechnik sollte ein hohes Augenmerk liegen – also die Kosten aller Komponenten eines Gesamtsystems über ihre Lebensdauer hinweg. Darunter fallen die Anschaffungs- und Installationskosten für Hard- und Software, die Netznutzungskosten, etwa im Mobilfunknetz, die bei Aufbau eines eigenen Netzes meist günstiger ausfallen, die Lizenzkosten (Software) und die Wartungskosten. Setzt man bei Lizenzen, zum Beispiel für die IoT-Plattform, auf Open-Source-Lösungen, lassen sich durch gute IT-Architektur und Betrieb Kosten einsparen. Auch qualitative Hardware und ein vorausschauendes Management des Systems sorgen für geringere Kosten. Selbst der Batteriewechsel von Endgeräten lässt sich durch geschickte Netzplanung auf viele Jahre verlängern.

Auch die Zukunftssicherheit ist ein Kriterium. Schon die Sensorauswahl sollte mit Weitblick erfolgen. Setzt man auf Mobilfunknetze, könnten diese mit der nächsten Mobilfunkgeneration unbrauchbar werden, wenn Netzbetreibende ältere Netze zugunsten der nächsten abschalten. Auf der sicheren Seite ist man, wenn die gewählte Technik eine hohe Verbreitung bei anderen Organisationen mit ähnlichen Zielen findet, etwa bei Stadtwerken oder Chemieparks. Dies führt in der Regel auch zur Verfügbarkeit von Hardware, Software und Fachleuten, die langfristig unterstützen können.

Schließlich sollte man die Technik auf ihre Eignung für die entsprechenden Anwendungsfälle prüfen. So funktionieren Mesh-Techniken zum Beispiel nur dann gut, wenn sich viele Sensoren in überschaubarer Entfernung befinden, etwa in einer Lagerhalle. Für weit verteilte Anwendungen, wie das in einer Stadt der Fall ist, eignen sich eher LPWAN-Techniken. Sie sind besonders sinnvoll, wenn ein regional begrenzter Bereich abgedeckt sein soll, beispielsweise eine Städteregion, eine einzelne Stadt oder ein Industriepark.

Die ersten Jahre mit neuen Techniken sind immer die schwierigsten. Das Beispiel LoRaWAN unterstreicht dies: Gerade zu Beginn waren die Hersteller noch unerfahren und die Qualität mancher Produkte (Hardware, Firmware und Dokumentation) eher mangelhaft. Auch die Konfiguration der Sensoren stellte sich oft als fehleranfällig und die Dokumentation als nicht aktuell und zeitintensiv heraus. Außerdem fehlte es an entsprechender Standardisierung etwa bei Decodern, also den Übersetzern der sparsam übertragenen Daten in die Messparameter, die die Hersteller zum Teil nicht mitgeliefert haben.

Auch bei den IoT-Plattformen selbst boten sich wenige Optionen: So gab es All-in-One-Plattformen, die oft unflexibel und nur für bestimmte Anwendungsfälle ausgelegt waren. Oft waren sie proprietär in starker Abhängigkeit vom Hersteller beziehungsweise zu stark an das Geschäftsmodell des Anbieters gekoppelt. Neben diesen Plattformen erfolgte auch die Entwicklung von Open-Source-Plattformen, die tendenziell zukunftssicherer sind, eine freie Auswahl von Dienstleistern für Betrieb und Weiterentwicklung bieten und sich auch nach eigenen Prioritäten weiterentwickeln lassen.

Neben diesen Herausforderungen sind viele IT-Abteilungen selbst nicht ausreichend auf den Betrieb eines IoT-Funknetzwerks vorbereitet. So unterscheiden sich die Herausforderungen bei IoT-Funknetzwerken mit vielen verteilten, oft statischen Sensoren im Betrieb deutlich beispielsweise von einem internen WLAN. Auch die Netzüberwachung ist nicht simpel - ist sie doch hersteller- und anwendungsabhängig und muss mit höheren Latenzzeiten und irregulär sendenden Sensoren umgehen können. Außerdem muss der technische Support effiziente Prozesse etablieren und Vorfälle gerade zu Beginn detailliert auf systemische Probleme untersuchen, um diese früh beheben zu können. Sonst können erhöhte Supportaufwände die Vorteile von IoT-Projekten mit der Zeit stark reduzieren. Bei der Netzplanung gilt es, sich an den geplanten Anwendungen zu orientieren und gleichzeitig offen für zukünftige Anwendungen zu bleiben. Außerdem ist zu berücksichtigen, dass sie ungewohnt große Flächen betrifft. Hilfreich sind hier Planungsmodelle und die Erfahrung aus der Netzplanung im Mobilfunk.

LoRaWAN – ein Kurzplädoyer

LoRaWAN ist inzwischen den Kinderschuhen entwachsen und insbesondere bei vielen Mittelständlern erfolgreich und gewinnbringend im Einsatz. Es existiert mittlerweile ein großes Angebot fertiger Endgeräte von guter Qualität. Viele Anwendungsfälle sind bereits durch Early Adopters erprobt und die Produkte verbessert. Auch individuelle Lösungen für bestehende Geräte sind heute möglich, zum Beispiel mit RS485- oder Modbus-Adaptern. Multifunktionale Geräte wie etwa komplette Wetterstationen ermöglichen es darüber hinaus, mit geringem Aufwand bestehende Gerätekategorien ohne eigenen Netzwerkanschluss flexibel einzusetzen.

Fazit

Zu Beginn galten LPWAN und Bluetooth für das IoT als temporäre Brückentechniken. Die Erfahrung des Beratungsunternehmens ECBM zeigt jedoch, dass sich LoRaWAN und Bluetooth-Mesh durchgesetzt haben und dass sie auch langfristig erfolgreich bleiben. LoRaWAN kann überall dort zum Einsatz kommen, wo sich regional ein Netz aufbauen lässt, zum Beispiel durch Stadtwerke und Gemeinden. Mesh-Netzwerke sind dort geeignet, wo lokal eine hohe Sensordichte erreicht ist, wie zum Beispiel auf dem Firmengelände. Hingegen werden Mobilfunknetze wie 5G auch in absehbarer Zukunft nicht immer die lokal notwendige Abdeckung erreichen und höhere laufende Kosten in größeren Installationen verursachen. Eine gut geplante IoT-Architektur ist für viele Techniken offen. Der große Vorteil dabei ist, dass dann, wenn die nächste, bessere Technik kommt, sich diese einfach an die flexible IoT-Plattform anschließen lässt.

Elisabeth Schloten/am

Elisabeth Schloten ist Gründerin und Geschäftsführerin von ECBM.

Wi-Fi 6: Höhere Datenraten und mehr Stabilität

Pluspunkte für das neue WLAN

Die Einführung von Wi-Fi 6 war ein wichtiger Schritt hin zur Realisierung einer umfassend vernetzten, technisch intelligenten Welt. Die Wege, um ein Maximum an digitaler Höchstleistung zu erreichen, sind dabei jedoch sehr individuell. Um alle Potenziale bestmöglich auszuschöpfen, ist es nötig, jeden Unternehmensbedarf und jedes Projekt spezifisch zu analysieren.

Wi-Fi 6 wird den Aufstieg des Internet of Things weiter begünstigen und den Weg für zusätzliche Mobilität, Skalierbarkeit, Sicherheit sowie Agilität auf einem völlig neuen Niveau ermöglichen. Darüber herrscht Einigkeit unter den Fachleuten. Für den Erfolg ist es jedoch notwendig, die dadurch nutzbare neue technische Infrastruktur innerhalb eines optimierten Netzwerks – entsprechend der spezifischen Bedürfnisse des jeweiligen Unternehmens – optimal zu gestalten sowie passgenau zu integrieren.

Als neuer Standard für drahtlose Netzwerkübertragungen hat 802.11ax (oder Wi-Fi 6) das zentrale Kapazitätsproblem innerhalb von Netzwerken gelöst. Jedes angeschlossene Gerät und jeder Dienst bekommt künftig genau die benötigte Bandbreite zur Verfügung gestellt. Auf diese Weise wird etwa eine intelligente Glühbirne, die relativ wenig Bandbreite benötigt, die Anforderungen eines nahegelegenen Laptops nicht mehr beeinträchtigen. Zukunftsweisende Techniken wie Augmented Reality, 4K, Machine Learning oder künstliche Intelligenz erfordern mehr Bandbreite, ein höheres Maß an paralleler Datenübertragung sowie eine geringere Latenz, was für herkömmliche drahtlose Netzwerke eine Herausforderung darstellt, was Wi-Fi 6 jedoch bewältigen kann. Die steigende Unterstützung von Multi-User-Systemen wird auch die Überlastung und damit die Gefahr der Erzeugung eines Flaschenhals-Effekts in stark genutzten Umgebungen verringern und es Unternehmen ermöglichen, drahtlose Netzwerke ohne Versorgungslücken aufzubauen. Im Wesentlichen unterstützt Wi-Fi 6 so alle anderen digitalen Trends, die derzeit moderne Business-Aktivitäten optimieren und beschleunigen. Die Kunst, aus Wi-Fi 6 Nutzen zu ziehen, besteht allerdings nicht nur in der reinen Einführung, sondern einer Integration in das gesamte Netzwerk.

Privathaushalte und Unternehmen

Da der zentrale Vorteil von Wi-Fi 6 in einer optimierten Effizienz und Kapazität drahtloser Netzwerke liegt, wird die kommerzielle vor der privaten Nutzung erfolgen und für Einsatzszenarien wie etwa Verkehrsknotenpunkte, öffentliche Veranstaltungsorte, Universitäten und Schulen von hohem Interesse sein. Anwendungsfälle bei Hochhäusern, innerhalb der intelligenten Fertigung und im Bereich der Gesundheitsversorgung werden zeitnah folgen.

Im Bereich privater Dienstleistungen wird besonders das Gastgewerbe interessant sein. Für Unternehmen, die in diesem Bereich tätig sind, eröffnet Wi-Fi 6 vor allem die Option, langfristig auch nachhaltiger zu arbeiten. Zudem lassen sich Betriebskosten reduzieren und weitere Einsparpotenziale nutzen. Geschwindigkeit und Effizienz innerhalb der Netzwerktechnik sind in dieser Branche mit erfolgsentscheidend, da durch Besucher und interne digitale Abläufe fortwährend Daten zur weiteren Verarbeitung ankommen oder Anfragen entstehen.

Unternehmen müssen in der Lage zu sein, diese Daten zu filtern und darauf so schnell und präzise wie möglich zu antworten sowie entsprechend reagieren zu können. Die Vernetzung der Geräte von Mitarbeitern, die im Rahmen ihrer Tätigkeit häufig unterwegs sind oder sich an abgelegenen Standorten befinden, ist dabei entscheidend. Wi-Fi 6 verbessert diese Situation maßgeblich.

In Geschäftsbereichen, in denen die Personalisierung im Mittelpunkt steht oder persönliche Profile und Datenbanken kontinuierlich erstellt und fortwährend aktualisiert werden, müssen Unternehmen sicherstellen, dass ihre Systeme nicht nur die reine Datenmenge, sondern auch deren Skalierungen ordnungsgemäß verarbeiten können. Deren digitale Infrastruktur soll nicht nur schneller werden, sondern auch leistungsfähig bleiben, wenn die Datenflut zunimmt. Gleichzeitig muss für Qualität, Ausfallsicherheit, Online-Security und eine zuverlässige Vernetzung gesorgt sein.

Das Thema Sicherheit ist ein weiteres Merkmal, das im Fokus stehen sollte. Die Reduzierung von Risiken durch Big Data gestaltet sich bei öffentlichen Verwaltungen und Institutionen – beispielsweise Schulen und Universitäten – besonders schwierig.

Die Abläufe sind mindestens so umfangreich wie im Gastgewerbe, sodass auch dort ein überaus hohes Maß an Qualität, Geschwindigkeit, Organisation und Effizienz innerhalb der digitalen Landschaft erforderlich ist. Um dies zu gewährleisten, muss auch hier der Grad der Sicherheit maximal sein. Wi-Fi 6 bietet die Möglichkeit, geschäftliche Potenziale optimaler auszuschöpfen und dabei gleichzeitig einen besseren Schutz kritischer Daten zu gewährleisten. Patrick Hirscher/jos

Patrick Hirscher ist EMEA Wireless Market Development Manager bei Zyxel.

Marktübersicht WLAN Access Points

Hersteller/Anbieter	Web
Alcatel-Lucent Enterprise	www.al-enterprise.com
Aruba (HPE)	www.arubanetworks.com
Avaya	www.avaya.com
AVM	www.avm.de
Belden	www.belden.com
Bintec Elmeg	www.bintec-elmeg.com
Cambium Networks	www.cambiumnetworks.com
Cisco	www.cisco.com
Commscope	www.commscope.com
Devolo	www.devolo.de
D-Link	www.dlink.com
DrayTek	www.draytek.de
Edimax	www.edimax.com
EnGenius	www.engeniustech.com
Extreme Networks	www.extremenetworks.com
Fortinet	www.fortinet.com
Huawei	www.huawei.com

Hersteller/Anbieter	Web
Juniper	www.juniper.net
Lancom	www.lancom-systems.de
LevelOne	www.level1.com
Linksys	www.linksys.com
Moxa	www.moxa.com
Netgear	www.netgear.de
N-Tron	www.redlion.net
ORing Networking	www.oringnet.com
Phoenix Contact	www.phoenixcontact.com
Primation	www.primation.de
Riverbed Xirrus	www.riverbed.com
Sophos	www.sophos.com
TP-Link	www.tp-link.com
Ubiquiti	www.ui.com
WatchGuard	www.watchguard.com
Zyxel	www.zyxel.com

Alle Marktübersichten sind unter www.lanline.de/marktuebersicht abrufbar.

News

Lancom: Cloud-Update im SD-WAN- und SD-Branch-Bereich

Verwaltung von Weitverkehrsnetzen mit LMC

Mit einem Update für die Lancom Management Cloud (LMC) will der deutsche Netzwerkinfrastruktur-Ausstatter Lancom Systems neue Impulse für SD-WAN und SD-Branch setzen. Als zentrale Management-Instanz stellt die LMC SD-WAN-Funktionen zur Verfügung, die die Skalierbarkeit und Effizienz der Weitverkehrsnetze mittelständischer und großer Firmen erhöhen sollen. Im Bereich SD-Branch halte das Update einen neuen WLAN-Hotspot-Dienst bereit.

Zentraler Nutzen des Cloud-Updates ist laut Lancom die Verwaltung mehrerer WAN-Verbindungen an einzelnen Standorten. Damit seien SD-WAN-Funktionen wie automatisches Load Balancing sowie anwendungs- oder qualitätsbasiertes Routing mit dynamischer Pfadwahl möglich.

Die von Lancom entwickelte SD-WAN-Technik High Scalability VPN (HSVPN) bringe ein Mehr an Skalierbarkeit und Effizienz in VPN- und SD-WAN-Architekturen mit vielen Gegenstellen und Anwendungen. War bislang im Rahmen der Virtualisierung für jeden Dienst ein eigener VPN-Tunnel nötig, sollen sich diese über HSVPN innerhalb eines einzigen Tunnels sicher trennen lassen.

Mit Dynamic Path Selection steht eine weitere SD-WAN-Optimierungsfunktion zur Verfügung, die Anwendungen dynamisch über die jeweils aktuell beste Verbindung routen soll. Bis zu vier parallel nutzbare WAN-Leitungen unterstützt das System. Diese lassen sich auch über 4G/LTE oder 5G realisieren, so der Netzwerkausstatter. Das Feature überwache kontinuierlich die WAN-Verbindungen in Bezug auf Last, Paketverlust, Latenz oder Jitter und entscheide in Abhängigkeit der Verbindungsqualität dynamisch über die bestmögliche Leitung für bestimmte Anwendungen. In den Standorteinstellungen könne man außerdem den Gateways eine feste, selbstgewählte Sub-Domain (mycompany.dyndns-lmc.de) zuweisen. So sollen auch Gateways mit dynamischen WAN-IP-Adressen jederzeit über diesen Domain-Namen erreichbar bleiben.

Parallel zur Erweiterung der klassischen SD-WAN-Funktionen hat Lancom die LMC laut eigenen Angaben zur intuitiven WLAN-Hotspot-Plattform für SD-Branch-Installationen ausgebaut. Der Dienst sei mit wenigen Klicks eingerichtet und über vorhandene WLAN-Access-Points sicher getrennt ausgerollt. Man kann ihn außerdem mit einem individuellen Hotspot-Begrüßungsbildschirm mit eigenem Logo und CI sowie Impressum und Nutzungsrichtlinien für die Hotspot-Benutzenden versehen, so der Hersteller weiter. Zusätzliche Hardware in Form eines Hotspot-Gateways sei nicht erforderlich. Die Lancom Management Cloud ist vollständig in Deutschland entwickelt und gehostet. Sie erfülle die Datenschutzanforderungen der DSGVO und unterstütze Unternehmen, Verwaltung wie auch Organisationen dabei, Compliance-Risiken bei Cloud-gemanagten Netzwerken zu minimieren. Anwender mit erhöhtem Sicherheitsbedarf sollen die LMC alternativ als Private Cloud „on-premise“ im eigenen Rechenzentrum betreiben können.

Die SD-WAN-Funktionen lassen sich automatisch in der Cloud abbilden. Die Router und SD-WAN-Gateways unterstützen die Funktionen ab Firmware LCOS 10.42, so die Lancom-Angaben. Die SD-Branch-Funktion „Cloud-managed Hotspot“ funktioniere mit allen Access Points von Lancom ab Firmware LCOS 10.42 oder LCOS LX 5.30. am

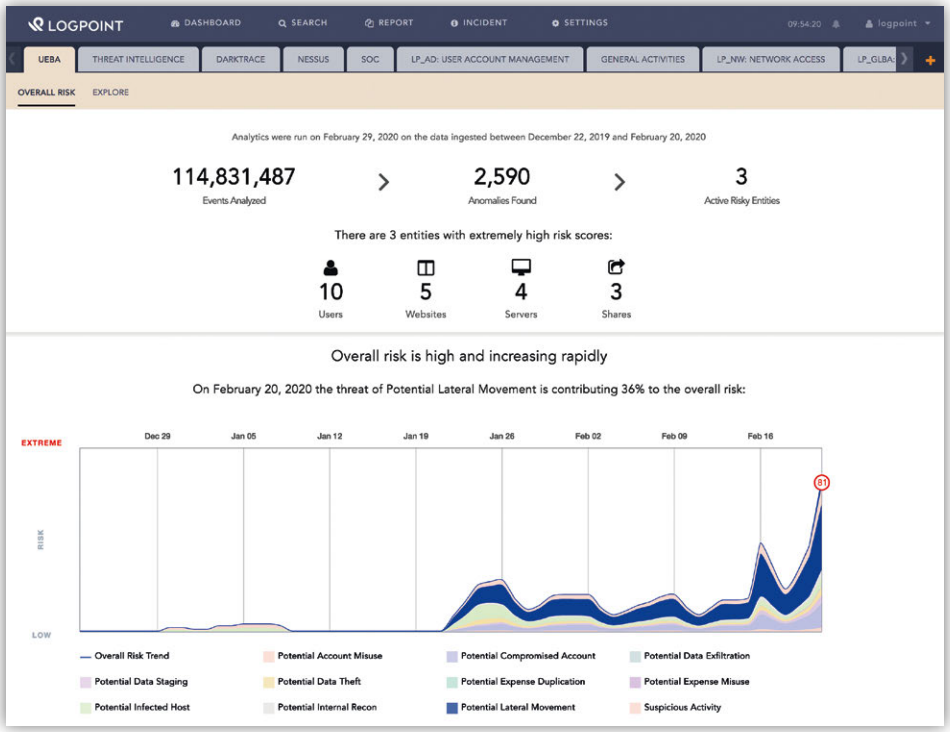
UEBA und das Mitre Att&ck Framework

Kenne deinen Feind

Sicherheitsexperten sollten nicht davon ausgehen, alle Vorfälle verhindern zu können, sondern für den Fall Vorsorge treffen, dass Kompromittierungen auftreten. Sie sollten das Prinzip „Defense in Depth“ (Verteidigung in der Tiefe) und überlappende Kontrollmechanismen nutzen, um „Single Points of Failure“ zu minimieren.

Es ist ratsam, einen risikobasierten Ansatz für die Sicherheit zu wählen. Es gilt zu verstehen, wo sich die unternehmenskritischsten Werte befinden und wo das größte Risiko liegt, um die Ressourcen klassifizieren und schützen zu können. Dazu sollten IT-Sicherheitsverantwortliche Präventions- und – wo dies unmöglich ist – Erkennungstechnologien einsetzen. Eine dieser Erkennungstechnologien ist das SIEM-System (Security-Information- und Event-Management). Sicherheitsanalysten ziehen außerdem Bedrohungsinformationen wie Listen bekannter IoCs (Indicators of Compromise) hinzu, ebenso Tools wie Antivirus, IDS, Spam-Filter etc.

Doch die bisherige Strategie hat ihre Schwachstellen. Erstens gibt es immer mehr IoCs, was zu immer längeren Listen führt und die Übersichtlichkeit beeinträchtigt. Zweitens ändern Angreifer immer wieder bestimmte Attribute eines Angriffs, etwa die Quell-IP-Adresse netzwerkbasierter Angriffe oder auch nur ein einzelnes Bit innerhalb des Malware-Codes, sodass der Hash-Wert nicht mehr mit den bekannten IoCs übereinstimmt. Gegen Zero-Day Exploits oder unbekannten Bedrohungen nutzt das etablierte Vorgehen ebenfalls nicht. Eine Erkennungsstrategie muss vielmehr bekannte wie auch unbekannte Bedrohungen in Betracht ziehen.



UEBA-Software weist jedem Nutzer und jeder Entität in der Organisation ein Risikowert zu, je nach Zahl und Schweregrad anomaler Ereignisse. Bild: LogPoint

Die Verhaltensanalyse ist eine Methode zur Erkennung von Bedrohungen. Ihr Schwerpunkt liegt auf dem Verständnis des Verhaltens von Benutzern und Entitäten (Servern, Dateifreigaben etc.) in der eigenen Umgebung sowie des Verhaltens der Gegner einschließlich deren Motivationen und Methoden. Mit diesem Verständnis können Sicherheitsanalysten nicht nur potenziell bösartige Aktivitäten aufdecken, sondern sogar subtile Änderungen im bekannten Verhalten der Benutzer und Entitäten in der eigenen Umgebung feststellen. Beobachten Security-Analysten das Verhalten eines Angreifers oder einer Malware, unterscheidet sich dieser Ansatz von der reinen IoC-Erkennung dadurch, dass sie hier eine makroskopische Perspektive einnehmen. Die mikroskopische Sichtweise hingegen richtet das Augenmerk nur auf die Signaturerkennung. Der makroskopische Ansatz entschärft eine der größten Herausforderungen traditioneller Signaturerkennung, nämlich die Einschätzung der stetig wachsenden und veränderlichen Bedrohungslage: IT-Sicherheitsverantwortliche können sich bei der Verhaltensanalyse auf eine begrenzte Anzahl bekannter Verhaltensweisen der Angreifer konzentrieren. Ein weiterer entscheidender Vorteil im Vergleich zu bisherigen signaturbasierten Erkennungsmethoden ist, dass das Security-Team Alarme erhält, sobald die Software unbekannte Bedrohungen entdeckt.

Angreiferverhalten analysieren

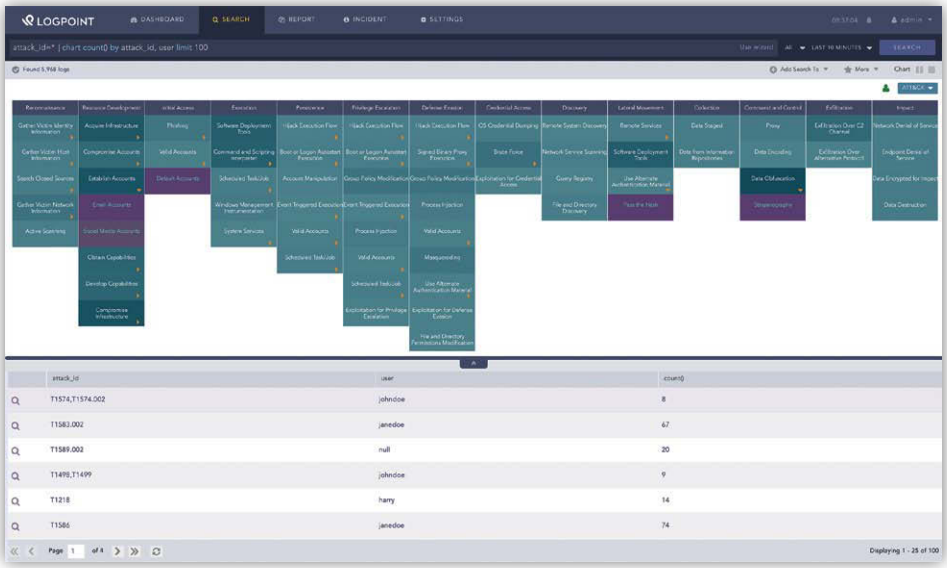
Die Betrachtung der Umgebung anhand von Verhaltensweisen ist anspruchsvoller als die einfache Suche nach Signaturen. David Bianco, damals Incident Handler bei FireEye, schlug 2014 eine sogenannte „Pyramid of Pain“ (Schmerzpyramide) vor. Sie stellt die relativen Stärken und Schwächen der Verwendung verschiedener IoCs in zwei Dimensionen dar: eine Rangfolge von IoC-Typen in Bezug darauf, wie einfach sie zu implementieren waren, und

die relative Verbreitung jedes IoC-Typs. Am unteren Ende der Pyramide befinden sich Hash-Werte, die reichlich vorhanden und leicht zu sichten sind, an der Spitze TTPs (Taktiken, Techniken und Prozeduren, also Verhaltensweisen), die ein Security-Team am schwierigsten erkennen und verfolgen kann. Zwei Möglichkeiten bieten sich an, um Verhaltensanalysen in das Sicherheitsprogramm zu implementieren: die Nutzung des Mitre Att&ck-Frameworks und von UEBA (User and Entity Behavior Analytics).

Das Mitre Att&ck Framework ist eine von der Community bereitgestellte Wissensdatenbank zu Taktiken und Techniken von Angreifern. Die Mitre Corporation pflegt diesen Informationsbestand, der auf realen Beobachtungen basiert. Mit dem Framework steth IT-Sicherheitsfachleuten eine Fülle von Wissen über Angreifer zur Verfügung, das Tausende Sicherheitsforscher auf der ganzen Welt sammeln. Dieses Wissen hilft, sich auf Cybersicherheitsbedrohungen vorzubereiten und darauf zu reagieren. Die Integration der Wissensdatenbank in Erkennungstechnik bringt Licht ins Dunkel der Hacker-Aktivitäten.

Während das Framework Einblicke gibt, um das Verhalten der Angreifer zu verstehen, bietet UEBA den Ausblick: Hier geht es darum, die Umgebung gut zu verstehen, um subtile künstliche Veränderungen zu erkennen. UEBA nutzt unüberwachtes maschinelles Lernen (Unsupervised ML), um die traditionellen regel- und signaturbasierten Erkennungsfunktionen des SIEM-Systems zu ergänzen. UEBA-Software modelliert dazu das Verhalten jedes Benutzers und jeder Entität in der Umgebung zu verschiedenen Tageszeiten, Wochentagen und Wochen des Monats. Sie verwendet diese Referenzwerte dann als Grundlage für die Erkennung von Anomalien und wendet heuristische Algorithmen darauf an. So lässt sich die Wahrscheinlichkeit bestimmen, dass die beobachteten Verhaltensunterschiede auf eine Bedrohung hindeuten.

Mittels des unüberwachten maschinellen Lernens kann die Software Benutzer und Entitäten gruppieren, die ähnliches Verhalten aufweisen. Diese Gruppierungen sind wichtig für höhere Erkennungsgenauigkeit, da sie nicht nur das Verhalten einer einzelnen Entität mit ihrer eigenen Baseline (Referenzwert) vergleichen, sondern auch mit der Baseline ihrer Gruppe. Dieser Vergleich senkt das Risiko von Fehlalarmen in Situationen, in denen ein Benutzer etwas Neues tut, das aber sonst unter den Mitgliedern seiner Gruppe oder Abteilung sehr häufig vorkommt.



So stellt sich die Nutzung des Mitre Att&ck Frameworks für den Anwender einer SIEM-Software dar.
Bild: LogPoint

Von Rohdaten zur Information

Im Kern basiert UEBA auf Techniken der Datenwissenschaften (Data Science), um mittels statistischer Ansätze Anomalien zu erkennen. Die Herausforderung besteht darin, diesen Anomalien einen Sinn zu geben und sie mit Kontext und Fachwissen anzureichern, damit ein Sicherheitsanalyst darauf reagieren kann: Statt die Analysten einfach nur auf ein anomales Ereignis ohne jeglichen Kontext hinzuweisen, muss die Software verwertbare Informationen in klaren und eindeutigen Begriffen liefern.

UEBA bietet zwei Vorteile: Erstens erkennt es anomale Verhaltensweisen und trifft mit hoher Sicherheit eine Entscheidung darüber, ob sie verdächtig oder legitim sind. Diese Analyse basiert auf dem Verständnis des Kontextes und ist mit nicht-verhaltensbasierten Methoden nur schwer oder gar nicht zu automatisieren. Der zweite Vorteil besteht darin, dass die Software jedem Benutzer und jeder Entität in der Organisation eine Risikobewertung zuweist, die der Anzahl und dem Schweregrad der anomalen Ereignisse entspricht. Diese Risikowerte stellen eine zusätzliche Dimension der regelbasierten Analyse im SIEM dar: Statt jedes Mal einen Alarm auszulösen, wenn ein Nutzer auf eine File-Sharing-Website zugreift, warnt ein vorkonfigurierter intelligenterer Alarm nur dann, wenn dieser Benutzer einen hohen Risikowert aufweist. Dies steigert letztendlich die Zuverlässigkeit der Warnungen und senkt die Zahl falsch-positiver und falsch-negativer Ergebnisse.

Für „Defense in Depth“ ist es sinnvoll, sich überschneidende Kontrollmechanismen zu nutzen, durchaus also auch traditionelle Methoden der Signaturerkennung wie IDS, Blacklists und Virenschutz. Eine Verhaltensanalyse ergänzt traditionelle Ansätze und füllt viele Lücken, die diese Ansätze schaffen. Unternehmen verfügen dabei über zwei Möglichkeiten, verhaltensbasierte Techniken zu implementieren: Erstens gibt es mit der Ausrichtung an Mitre Att&ck einen einfachen Weg, das Angreiferverhalten besser zu verstehen und zu erkennen. Zweitens hilft UEBA mit einer ergänzenden Verhaltensanalyse zu verstehen, wann etwas Ungewöhnliches ein Hinweis auf eine Kompromittierung sein könnte.

Jake McCabe/wg

Jake McCabe ist CISSP und Presales Director bei LogPoint.

Grundlagen des Netzwerk-Managements

Netze am Laufen halten

Die Ansprüche an eine hochperformante Netzwerkinfrastruktur sind in jüngster Zeit rapide angestiegen. Eine hohe Verfügbarkeit und Performance aller Komponenten sind noch kritischer geworden, als sie es schon waren. Durch die Digitalisierung der Prozesse, unzählige Videokonferenzen etc. sind Unternehmen auf die allzeit funktionierende Online-Verbindung angewiesen. Dies erfordert ein entsprechendes Netzwerk-Management.

Um den Anforderungen gerecht zu werden, schafften die Unternehmen über die Jahre immer wieder einzelne Softwarepakete an oder programmierten diese selbst – oft auf der Basis von Freeware-Tools. Dadurch können Kompatibilitäts- und Sicherheitsprobleme entstehen, die sich negativ auf Produktivität, Kosteneffizienz und Sicherheit auswirken. Als Beispiel kann die oft getrennte Erhebung von Stammdaten (Asset-Management, Lokationen, Kunden etc.) und Bewegungsdaten (Performance-Messungen, Traffic-Daten etc.) dienen. Um die Daten konsistent in zwei oder mehr Systemen zu halten, ist ein erheblicher Aufwand zu leisten, der häufig mit Unsicherheit über die Aktualität einhergeht. Dem sollten Unternehmen durch den Einsatz eines integrierten, homogenen Netzwerk-Management-Systems entgegenwirken.

Viele Unternehmen sind heute global aufgestellt und verfügen über mehrere Standorte in unterschiedlichen Ländern. Die Verwaltung von Datenströmen und Netzwerkressourcen gestaltet sich in diesem Fall oft schwierig. Einfacher wird es mit einer verteilten Management-Server-Struktur, bestehend aus einer zentralen Einheit (Center) und einem oder mehreren Satellitengruppen. Das Center-System speichert alle Monitoring- und Performance-Daten, die für den stabilen Betrieb notwendig sind. Die Satelliten sammeln und empfangen in einer solchen Konstellation alle relevanten Netzwerkdaten (SNMP-Traps, Syslogs, Performance-Messungen etc.) und geben sie an das Center weiter. Der Vorteil dabei ist die horizontale Skalierbarkeit: Wächst das Netz, kann das IT-Team einfach weitere Satelliten hinzufügen.

Zudem lassen sich auf diese Weise Latenzen minimieren und die Zugriffe auf Netzwerkgeräte, auch in abgeschotteten Netzbereichen (DMZ), auf lokale Satelliten begrenzen. Die Satelliten fungieren als Datenpuffer und können die Netzwerkdaten im Fall einer Verbindungsstörung zum Center zwischenspeichern und später gesammelt weiterleiten. Die vielfältigen Informationen werden in der zentralen Einheit kombiniert und analysiert. Einsicht erhalten berechtigte Gruppen wie zum Beispiel Technik, Management oder Finanzabteilung über eine zentrale, für die jeweiligen Bedürfnisse konfigurierbare GUI. Dazu gehören unter anderem Kunden-, Geräte- und Performance-Daten.

Für Netzwerk-Administratoren kommt es auf einige Funktionen besonders an, wenn es um die Aufrechterhaltung des Netzwerkverkehrs geht. Unter anderem sind folgende Funktionalitäten von zentraler Bedeutung:

Fault-Management: Die präzise Fehlererkennung ist entscheidend für die Zuverlässigkeit des Netzwerks. Nur wenn die Administration alle Fehler schnell und zuverlässig erkennt, kann sie den stabilen Betrieb eines komplexen Netzwerks dauerhaft sicherstellen. Dazu ist es unabdingbar, Alarme schnellstmöglich zu bearbeiten und zu korrelieren, um die Fehlerquelle analysieren zu können. Diagnosetests sowie umfangreiches Logging und Reporting gehören heute zum Standardumfang moderner Netzwerk-Management-Lösungen.

Configuration-Management: Insbesondere in großen IT-Infrastrukturen kommt es darauf an, Changes automatisiert und schnellstmöglich durchzuführen. Da die IT-Administration hier eine Vielzahl von Geräten konfigurieren muss, ist es wichtig, den Rollout zeit- und kosteneffizient zu gestalten. Professionelle Provisioning-Module schaffen es, Konfigurationsänderungen global auf tausenden Switches innerhalb weniger Minuten durchzuführen. Die Inbetriebnahme neuer Netzwerkgeräte kann mittels Netzwerkautomatisierung (Zero-Touch) schnell erfolgen. Verfügt die Netzwerk-Management-Lösung über einen Compliance-Check für die Konfigurationen, kann die IT-Administration Inkonsistenzen automatisch erkennen und per Provisioning schnell korrigieren.

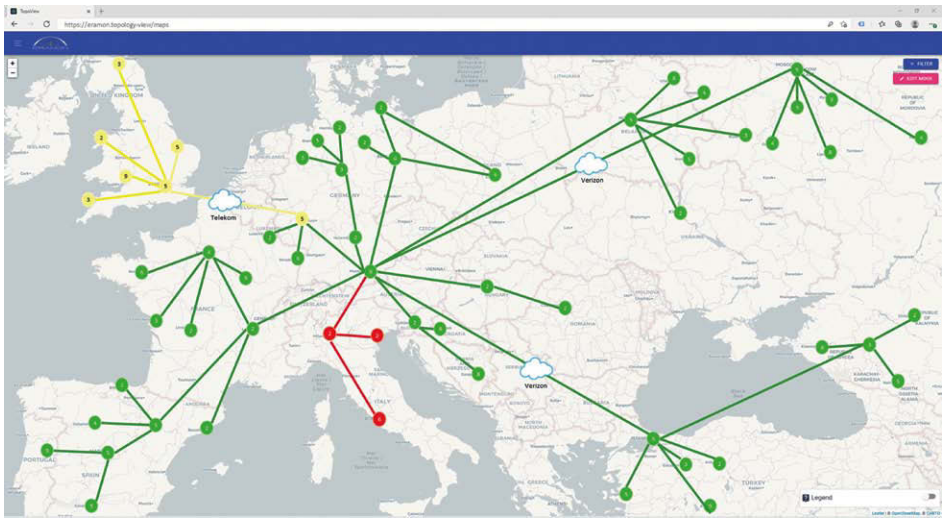
Asset-Management: Die Geräteverwaltung ist ein entscheidender Faktor für die Zuverlässigkeit des Netzwerks. Um Geräte auf einem aktuellen Stand bezüglich Updates und Patches zu halten, ist es unabdingbar, alle Informationen zu kennen, die zur Aktualisierung der Geräte notwendig sind. Dazu gehören detaillierte Informationen wie etwa Hersteller, Modell, Ausstattung, Softwarestand, Seriennummern sowie Angaben über Standorte und die Netzwerktypologie. Die Dokumentation sollte automatisch per SNMP-Abfragen erfolgen und tagesaktuell oder auf Abruf zur Verfügung stehen.

Performance-Management: Ein wichtiger Teil unserer digitalen Welt besteht aus Echtzeitanwendungen wie Voice- oder Videodiensten. Eine Echtzeitüberwachung des Netzwerks ist daher die Voraussetzung für eine schnelle Reaktion auf Störungen. Um die aktuelle Auslastung des Netzwerks zu erfassen und bei Problemen schnell eingreifen zu können, bedarf es eines ausge-

feilten Performance-Managements. Dieses sammelt unter anderem anhand von SNMP oder RESTful APIs Daten wie MOS, Latenz, Jitter, Paketverluste oder QoS von Switches, Routern sowie Servern und analysiert diese. Das macht schnell ersichtlich, an welchen Stellen Engpässe im Netzwerk entstehen.

Jitter zum Beispiel, also zeitliche Schwankungen zwischen dem Empfang von Datenpaketen, liegt oft im einstelligen Millisekundenbereich, aber auch Werte bis zu 30 ms sind durchaus noch normal. Das Polling-Intervall sollte hier genau definierbar sein und die Administration sollte entscheiden können, in welchen Zeiträumen sie die Daten sammeln und wie lange sie diese in welchen Aggregationsstufen speichern will. In der Regel fragen Management-Systeme Messdaten im Abstand von fünf bis zehn Minuten ab. Im Fehlerfall ist dieses Intervall aber eher zu lang. Dann sollte man es durch ein temporäres Turbopolling (zum Beispiel Messungen im Zehn-Sekunden-Takt) ersetzen oder ergänzen. Kommt es zu einem Ausfall, kann ein SLA-Modul die Verfügbarkeit der Ressourcen und die Einhaltung der Verträge protokollieren. Dabei sollten sich Geschäftszeiten und Wartungsfenster berücksichtigen lassen, gegebenenfalls auch in unterschiedlichen Zeitzonen.

SIEM-Integration: Ein Netzwerk-Management-System übernimmt dabei auch elementare Aufgaben einer SIEM-Lösung (Security-Information- und Event-Management) oder speist diese per RESTful APIs. Der Vorteil einer separaten Netzwerk-Management-Lösung liegt in der bereits korrelierten Analyse von Event-Informationen, etwa zu Ausfällen, Zugriffen oder Datenflüssen. So sind Informationen über den Ausgangspunkt eines Angriffs bereits mit Lokationsdaten, Gerätedetails und Traffic-Daten (etwa Zugriffe aus einem nicht erlaubten Netzbereich) verknüpft und sichtbar. Diese Daten müsste die IT-Administraton ansonsten aus unterschiedlichen Quellen zusammentragen.



Integrierte Netzwerk-Management-Lösungen sorgen für den Überblick über das Netzwerk, im Bild mittels einer Topologieansicht. Bild: Eramon

Topologieansicht: Sind alle Geräte in die Netzwerk-Management-Lösung eingepflegt, hilft eine Topologiedarstellung, den Überblick über alle Standorte und deren Status zu behalten. Der Entstehungsort von Störungen wie Jitter oder niedrigen MOS-Werten lässt sich somit ermitteln, um die passenden Gegenmaßnahmen ergreifen zu können.

Support: Der Kundensupport ist bei der Netzwerkverwaltung von entscheidender Bedeutung. Denn im Notfall müssen schnell Lösungen für Probleme zu finden sein – und zwar bevor sie den Betrieb beeinträchtigen oder im schlimmsten Fall komplett zum Erliegen bringen. Daher sollten Entscheider bei der Suche nach einer geeigneten Lösung nicht nur auf die enthaltenen Module, sondern auch auf die Reaktionsschnelligkeit des Anbieters achten. Erfahrene und etablierte Anbieter weisen eine Reaktionszeit von einem Tag nach Ankunft einer Anfrage auf und bieten wenig später bereits die passende Problemlösung. Denn die digitalen Infrastrukturen von Unternehmen sind die Pulsadern der globalen Wirtschaft und sind unbedingt vor einem Infarkt zu bewahren.

Florian Schönknecht/wg

Florian Schönknecht ist Head of Operations bei Eramon.

News

Orca will mit SideScanning-Technik punkten

Agentenlose, Cloud-native Sicherheitsplattform

Die Integration von Security-Agents bremst agile Umgebungen aus, mahnt Orca Security. Deshalb hat das israelische Startup-Unternehmen einen agentenlosen Ansatz für die Cloud-Sicherheit entwickelt, den es „SideScanning“ nennt. Im Gegensatz zu Agenten, die in der VM oder im Container implementiert sind, sammle das SideScanning Daten ausschließlich extern, nämlich per Nur-Lese-Zugriff auf den Laufzeit-Blockspeicher der Workloads. Diese Daten kombiniere die Software dann über APIs mit Metadaten der Cloud-Konfiguration, um den vollständigen Überblick über den Bestand und dessen Kontext zu erhalten. Damit sei dann eine ganzheitliche Sicherheitsbewertung der Cloud-Umgebung möglich, so Orca. Die Software unterstütze dabei AWS ebenso wie Microsoft Azure und die Google Cloud. wg

Qualitätssicherung durch mehrstufige Tests

Integrations- und Härtetests im RZ

Ganzheitliches Sicherheits-Management bedeutet, Sicherheit konzeptionell vom Anfang bis zum Ende zu denken. Integrations- und Härtetests für Server-Räume, Rechenzentren und Datacenter sind eine erprobte Methode, die Zuverlässigkeit einer Sicherheitskonzeption testweise vorwegzunehmen und beurteilen zu können. Somit ergibt sich die Chance, Fehlerquellen und Risiken im Vorfeld der Inbetriebnahme und somit vor Aufnahme des produktiven IT-Betriebs zu eliminieren.

Außerhalb der Rechenzentrumswelt, beim Neubau eines Büro- oder Verwaltungsgebäudes, werden technische Anlagen nach der Montage im Vorfeld der Abnahme getestet. Diese Art von Tests erfolgt in der Regel gewerke- und fachspezifisch durch unterschiedliche Beteiligte und zu verschiedenen Zeitpunkten, denn jedes Gewerk hat einen anderen Fertigstellungszeitpunkt. Häufig erfolgt die Arbeit nach diesem Schema auch bei anspruchsvolleren Bauvorhaben.

Die HOAI (Honorarordnung für Architekten und Ingenieure) sieht es vor, jedes Gewerk für sich zu betrachten und Schnittstellen zwischen den Gewerken nicht zu testen. Bei einem bestandenen Test der technischen Anlagen besteht oft die Annahme, dass alles zusammen funktioniert. Doch das ist ein Trugschluss, denn am Bau arbeiten Menschen, und denen unterlaufen Fehler.

Ein Übergabeverteiler könnte zum Beispiel Schnittstellen aus der Brandmeldeanlage, der Lüftungsanlage sowie weiterer Gewerke beherbergen. Ein einziger Denkfehler, sprich Dreher in dieser Schnittstelle (Öffner versus Schließer), führt zu einer Fehlfunktion. Wie können RZ-Betreiber solche Fehler verhindern – insbesondere bei anspruchsvollen Bauvorhaben, die eine große Zahl hochvernetzter technischer Anlagen beherbergen? Die Gesamtheit aller technischen Anlagen der TGA-Gewerke (Technische Gebäudeausstattung) stellt die versorgende und überwachende Infrastruktur des Rechenzentrums dar und ist meist sehr komplex. Sicherheit bringt nur die Durchführung eines mehrstufigen Testverfahrens mit abschließenden Integrations-, Resilienz- und Härtetests.

Stufen des Verfahrens

Zum Verständnis dieser Begriffe sind nachfolgend die einzelnen Stufen des Verfahrens aufgelistet. Für den international operierenden RZ-Manager gibt es entsprechende englische Bezeichnungen zu dem mehrstufigen Testverfahren (FAT, SAT, ISAT).

Stufe 1 - Werkstest (FAT: Factory Acceptance Test): Beim Werkstest testet der Hersteller jede technische Anlage auf dafür vorbereiteten Testständen und nach einem eigens entwickelten und auferlegten Protokoll. Der Hersteller führt den Werkstest in der Regel eigenverantwortlich durch. Lange und erfolgreich agierende Hersteller besitzen keine Scheu, den Auftraggeber oder einen Bevollmächtigten dazu einzuladen. Sie stellen die Protokolle auch vorab zur Verfügung und erlauben dem Auftraggeber, diese individuell, im Rahmen des Möglichen, anzupassen.

Dies ermöglicht kundenspezifische Tests bei den Fachleuten im Werk.

Tipps zum Testverfahren

- Verantwortliche sollten genügend Zeit für das gesamte Testverfahren einplanen – zusätzlich zur Vor- und Nachbereitung. Allein die Stufe 3 kann, je nach Umfang, mehr als eine Woche dauern.
- Das Testen sollte vom Kleinen zum Großen erfolgen. Den Anfang machen überschaubarere Redundanztests, bevor die komplexen Black-Building-Tests an der Reihe sind. Sonst kommt man mit dem Notieren der Feststellungen kaum nach.
- Die Tests finden in der schwierigsten Projektphase, nämlich während und nach der Fertigstellung statt. Es herrscht Zeitdruck, der schnell zu Fehlern führen kann. Fehler und damit verbundene Havarien können den Projektplan um mehrere Monate verzögern. Daher sollte ein Puffer in dieser Phase eingeplant sein, um später den Druck zu mindern.
- Verantwortliche sollten schon in der Planungsphase mit der Planung der Integrationstests beginnen, denn die Auftragnehmer müssen den Aufwand (personell und materiell) kalkulieren.
- Es sollte eine Personalplanung für die Tests erfolgen, sowohl in quantitativer als auch in qualitativer Hinsicht. Es sind mindestens zwei Personen für die Auslösung der technischen Reaktionen und die Beobachtung nötig. Letztere muss vielleicht an mehreren Stellen gleichzeitig erfolgen, um verlässliche Ergebnisse zu erzielen.
- Es sind verlässliche Kommunikationsmittel zwischen den Testbeteiligten nötig. Funklöcher beispielsweise führen zu fehlerhaften Testergebnissen, was zum Beispiel im Havariefall zu gefährlichen Situationen führen kann.

Stufe 2 - Inbetriebnahme und Eins-zu-Eins-Funktionstest (SAT: Site Acceptance Test): Zur Inbetriebnahme testet der Errichter seine technischen Anlagen ebenfalls in Eigenregie komplett durch. Das bedeutet am Beispiel einer Brandmeldeanlage, dass ein Testspray jeden Melder auslöst. Die Auslösung ist eins zu eins protokolliert und für die Dokumentation gespeichert. Andere Gewerke, wie zum Beispiel Netzersatzanlagen, bestehen aus Großkomponenten, die man am Montageort zusammenbaut und danach im Verbund einschaltet.

Auch bei diesen Anlagen erfolgt die Prüfung und Protokollierung aller Funktionen. Die Protokolle der Funktionstests muss der Errichter im Rahmen der Qualitätssicherung mindestens stichprobenartig kontrollieren. Die Stufen 1 und 2 entsprechen der üblichen Vorgehensweise bei Bauprojekten. Erst mit Stufe 3 ist die höchste Qualitätssicherung erreicht.

Stufe 3 - Integrations- und Härtetest (ISAT: Integrated SAT): Bei Integrationstests erfolgt der Test aller technischen Anlagen sämtlicher Gewerke im funktionalen Zusammenhang. Prozesse und Szenarien stellen realistische Störungsursachen nach. Die Protokolle dieser Tests sind individuell vorbereitet, die Szenarien detailliert beschrieben und das erwartete Verhalten aller beteiligten technischen Anlagen aufgelistet. Im Testverlauf erfolgt das Abhaken von Checklisten, der Abgleich der Werte und das Eintragen der Messwerte. Jede Abweichung vom erwarteten Anlagenverhalten muss akribisch dokumentiert sein, um zu gewährleisten, dass die Tests reproduzierbar sind.

Die Voraussetzung für den Integrationstest ist, dass das RZ fertiggestellt ist. Das klingt zunächst banal, ist aber vor dem Hintergrund ehrgeiziger Projektpläne sehr umfangreich. Dies heißt im Detail:

– Alle beteiligten Anlagen müssen in Betrieb und nach Stufe 2 erfolgreich getestet sein.
– Etwaige Fehler sind beseitigt. Dies muss durch eine Vorbegehung überprüft sein. Nicht selten müssen die Beteiligten auf die Fertigstellung einer sicherheitstechnischen Anlage oder eines übergeordneten Management-Systems warten.
– Die Dokumentation ist – wenigstens als Vorabzug oder Arbeitsversion – vorhanden.

Integrations- und Härtetests unter voller Lastbedingung

Im Test sind die Anlagen den vollen, teilweise sogar extremen Lastbedingungen ausgesetzt. Dazu sollten spezielle Lastbänke (Bauteile in der Elektrotechnik) zum Einsatz kommen, die ein RZ-spezifisches Lastverhalten am besten simulieren. Üblicherweise sind deren Heizwiderstände in mehreren Stufen schaltbar.

Große Lastbänke lassen sich auf Rollen transportieren und gleichmäßig im RZ verteilen. Mit den Lastbänken erfolgt der Test der kompletten Stromversorgung von Normalnetzeinspeisung über Trafos und Schaltanlagen sowie der gesicherten Stromversorgung über Netzersatz- und USV-Anlagen. Unter diesen realen Lastbedingungen lassen sich dann Einzelkomponenten oder ganze Versorgungspfade abschalten, sodass die Redundanzen greifen müssen.

Gleichzeitig lässt sich die Kühlung des Rechenzentrums über die entstehende Abwärme prüfen. Zu den Testkandidaten gehören die Sicherheitstechnik (Einbruch-, Brandmelde-, Zutrittskontroll-, Wassermelde- und Videoüberwachungsanlagen) sowie Lüftungs- und Löschanlagen. Hier werden Schnittstellen interoperabel über Systemgrenzen hinaus getestet, um die vollständige Durchgängigkeit nachzuweisen.

Eigene Messungen im Testverfahren

Viele Vorgänge im elektrotechnischen System, wie die Lastgänge im Testverlauf, der Nachweis der eingebrachten elektrischen Leistung oder das unterbrechungsfreie Umschalten der Stromversorgung, sind messtechnisch nachweisbar.

Diesen Job können zwar integrierte Messsysteme in den Anlagen erledigen, doch ein blindes Vertrauen ist nicht ratsam. Falsch eingestellte Wandlereingänge und Phasendreher können die Messwerte verfälschen. Daher führen die Sicherheitsfachleute der VZM (Von Zur Mühlen'sche) im Rahmen der Tests eigene Messungen mit eigenem Messequipment durch. Dies umfasst Netzanalysegeräte, Speicheroszilloskope sowie zahlreichen Zangenamperemeter und Universalmessgeräte.

Während der Integrationstests darf man keine anderen Arbeiten durchführen, die das Ergebnis beeinflussen könnten. Bei der Feststellung von Fehlern muss eine Klassifizierung dieser erfolgen – mindestens als kritisch oder unkritisch. Dabei fällt auch die Entscheidung, ob man den gesamten Test wiederholen oder nur nacharbeiten muss. Da alle Beteiligten vor Ort sind, kann in einem gewissen Rahmen eine sofortige Fehlersuche und Reparatur sinnvoll sein.

In jedem Falle sind die Verantwortlichen gut beraten, wenn sie bei der Planung des Testablaufes zeitliche Puffer einplanen.

Qualitätssicherung durch regelmäßige Integrationstests

Zur Sicherstellung der Leistungsfähigkeit sollte die Durchführung von Integrationstests regelmäßig erfolgen. Da die Umsetzung bei ohnehin sehr vollen Terminplänen für Wartung und Instandhaltung für die Rechenzetrumsbetreiber schwierig ist, ist die Konzentration auf die wichtigsten Szenarien empfehlenswert. Dazu zählt beispielsweise der jährliche Black-Building-Test für den stets drohenden Ausfall beim Energieversorger.

Darüber hinaus muss eine Wiederholung des Integrationstests beim Austausch von technischen Anlagen erfolgen – und zwar überall dort, wo diese Anlagen beteiligt sind.

Aus der Erfahrung dutzendfach durchgeführter Härtetests berichten die Berater der Von Zur Mühlen'schen über vertauschte Adern an einer Schnittstelle bis hin zu lediglich handfest angezogenen Verbindungsschrauben einer Stromschiene.

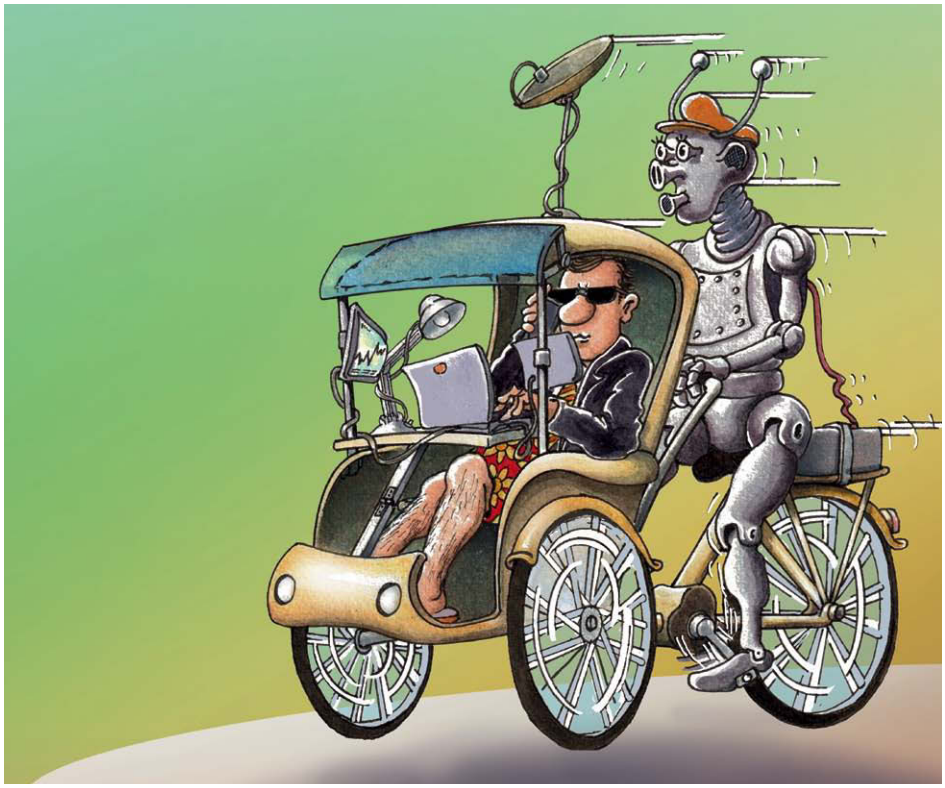
Sie betonen, dass dies ein ernst zu nehmendes Problem ist, denn rund 70 Prozent aller Fehlerentdeckungen hätten direkt und unmittelbar zu einem Ausfall des Betriebs im Rechenzenturm geführt.

Jörg Schulz/am

Jörg Schulz ist Sicherheitsberater bei Von Zur Mühlen'sche.

Arbeiten in und nach Pandemiezeiten

Vom Höhlenmenschen zur KI



Zukunftsforscher malten uns einst eine „Future of Work“, in der Roboter und künstliche Intelligenz (KI) uns alles Öde und Schweißtreibende abnehmen, auf dass wir uns wohlgemut dem Guten, Wahren, Schönen widmen können. Schließt man vom letzten Jahr auf folgende, wird die Zukunft der Arbeit eher darin bestehen, dass wir uns im Home-Office verschanzen, von Zoom-Konferenz zu Zoom-Konferenz hecheln und ansonsten versuchen, Reste von Haltung zu wahren. Zwar lockt dank Impfstoff ein Licht am Ende des Hausflurs, doch das Tempo deutschen Impfbemühens erinnert stark an das der BER-Baustelle. Nach einem Jahr Pandemie lohnt der Blick darauf, wie die Krise unsere Arbeitswelt verändert.

Der Mensch war schon immer Höhlenbewohner. Nun hat ein Virus ihn über den Umweg von Jagen und Sammeln, Ackerbau und Viehzucht, Manufaktur und Fabrik, Globalisierung und Digitalisierung wieder in die Höhle zurückgedrängt. Die Höhle von heute bietet gegenüber ihrem Steinzeitvorbild zwei wesentliche Vorteile: Erstens ist der moderne Höhlenbewohner nicht mehr von seiner gesamten Sippschaft umgeben, sondern höchstens noch von seiner Kernfamilie – aus Sicht des Verfassers dieser Zeilen ein nicht zu unterschätzender Fortschritt. Zweitens ist die moderne Höhle deutlich breitbandiger ans Internet angebunden als jene aus steiniger Vorzeit. Dies steigert die Vielfalt des Unterhaltungsprogramms und erleichtert auch das Arbeiten ungemein. Musste einst Fred Feuerstein bei dämmrigem Feuerschein sein Werkzeug mühsam selber schnitzen, so bestellt sein aktuelles Pendant derlei Gerätschaft einfach per Internet, ordert einen 3D-Drucker für den Eigenbau oder gründet ein Startup-Unternehmen, um dann mittels Cloud-basierter Collaboration-Tools die Produktion an andere zu delegieren, bevorzugt in einem Niedriglohnland.

Wir sehen also: Auch im Lockdown lässt sich’s leben und arbeiten – zumindest wenn man dank digitaler Technik seiner Tätigkeit überall nachgehen kann. Alle anderen sind gekniffen: Werktätige am Fließband ebenso wie in der Kranken- und Altenpflege, in kommunalen Services oder – sei es auf Befehl eines präsenzfixierten Chefs oder aus Angst vor grottenlangweiligem Einsiedlerdasein – im durchseuchungsfreundlichen Großraumbüro. Der Fokus der IT-Branche richtet sich dabei vorrangig auf die Beschäftigten in der Höhle 4.0, gilt doch mobiles, ortsungebundenes Werkeln mittels allerlei digitaler, Cloud- oder gar KI-gestützter Assistenz als zukunftsweisend.

Das mobile digitale Arbeiten – obschon aus gegebenem Anlass nicht ganz so mobil, wie

Arbeitsvisionäre es einst visionierten – machte letzthin bekanntlich einen Riesensprung nach vorn. Wie aber reagierte das frischgebackene – genauer: frischwiederaufgetaute – Höhlenvolk? Aufschluss darüber gibt eine Fülle von Umfragen, darunter zum Beispiel der „2021 State of Work Report für Deutschland" des Arbeits-Management-Anbieters Workfront. Dieser Bericht nutzt Daten aus zwei Erhebungen, durchgeführt von CGK (Center for Generational Kinetics) im Februar/März 2020 und November/Dezember 2020. CGK befragte hierzulande jeweils 1.000 Werktätige aus Unternehmen mit mindestens 500 Beschäftigten, die – eine angenehm präzise Einschränkung und wichtig für die Einordnung der Ergebnisse – am Computer und mit anderen zusammenarbeiten.

Das digitale Höhlendasein scheint manchen gut zu bekommen. So fühlen sich die deutschen Befragten laut dem Report seit der Pandemie zumindest ein kleines bisschen souveräner, beispielsweise beim Zeit-Management (67 Prozent, fünf mehr als in einer Umfrage kurz vor der Pandemie) oder in der Team-Zusammenarbeit (82 Prozent, plus drei gegenüber dem Präcoronarium). Doch wo Licht ist – der humanistisch gebildete Leser denkt an Platons Höhlengleichnis und nickt wissend –, da ist auch Schatten. So berichteten fast ein Viertel (23 Prozent) der deutschen Befragten von technischen Problemen bei der Arbeit, etwa durch neue Geräte oder Software. 25 Prozent beklagten fehlenden Austausch mit Kollegen. Nachholbedarf besteht offenbar insbesondere bei der Zusammenarbeit über Ländergrenzen und Zeitzonen hinweg: Nur gut die Hälfte (55 Prozent) der Deutschen bezeichneten sich hier als selbstsicher; bei US-amerikanischen und britischen Befragten waren es 77 beziehungsweise 76 Prozent. Dieser Rückstand dürfte nicht zuletzt daran liegen, dass die Amtssprache internationaler Unternehmen Englisch ist. Spräche man in Online-Meetings Deutsch, wäre das Verhältnis wohl eher umgekehrt. Hier besteht Hoffnung, dass KI-gestützte Übersetzung und Untertitelung eines Tages auch uns zu souveränen Videoconférenciers machen wird.

Allerdings erachtet nicht einmal jeder zweite deutsche Arbeitnehmer Technologie als sehr wichtig für die Team-Zusammenarbeit (41 Prozent) oder die eigene Bestleistung (42 Prozent). Am wichtigsten war den Dichtern und Denkern, dass die Technik genau auf ihr Arbeitsumfeld abgestimmt ist (80 Prozent); auf „State of the Art"-Technologie legten hingegen nur 64 Prozent Wert. Zugleich fühlten sich jedoch 47 Prozent durch veraltete oder irrelevante Technik weniger produktiv, 33 Prozent gestresster.

In den USA und UK nannten jeweils fast die Hälfte der Arbeitnehmer mangelnde technische Ausstattung als Kündigungsgrund, bei uns hingegen nur 27 Prozent. Hier führte die Krise offenbar zu neuer Bescheidenheit. Präcoronar lag der Wert noch bei 38 Prozent. Auffällig ist der Unterschied zwischen den Generationen: 29 Prozent der Millenials haben laut eigenen Angaben schon eine Stelle abgelehnt, weil veraltete Technik sie abschreckte, bei den Älteren waren es nur 16 Prozent.

Remote Work scheint zu bewirken, dass Beschäftigte sich weniger an ihren Job gebunden fühlen. Der Wert lag bei nur 70 Prozent, neun weniger als im Vorjahr. Denn verteiltes Arbeiten erfordert motivierte Beschäftigte, aber das mit der Motivation ist eben nicht so einfach. Die drei Haupthindernisse für motiviertes Arbeiten in Pandemiezeiten sind laut der Umfrage das Gefühl, nicht genügend geschätzt zu werden (64 Prozent), das Gefühl, die eigene Arbeit sei nicht wichtig (58 Prozent, ein Plus von stolzen 17 Prozent gegenüber 2019) sowie mangelhafte Kommunikation mit Kollegen und Vorgesetzten (64 Prozent). Workfront rät den Unternehmen deshalb, man müsse im Remote-Work-Zeitalter Wege finden, um die Wertschätzung der verteilten Belegschaft zu reflektieren.

Remote Work nach der Pandemie

Ein großer Teil der deutschen Beschäftigten wünscht sich, die Option flexiblen Arbeitens möge auch im Postcoronarium erhalten bleiben: Laut einer Citrix-Umfrage – der Remote-Work-Spezialist ließ OnePoll 3.750 Bürobeschäftigte in Deutschland, Frankreich, den Niederlanden, der Schweiz und UK befragen, darunter 1.000 hierzulande – bevorzugt knapp die Hälfte der deutschen Befragten (48 Prozent) nach der Pandemie ein hybrides Modell, hätte also gern die Wahl zwischen Büro und mobilem Arbeiten. Nur 15 Prozent wollen tagtäglich ins Büro zurück. 50 Prozent der Deutschen stimmten der Aussage zu, Unternehmen, die kein flexibles Arbeiten anbieten, seien für die Beschäftigten unattraktiv. 46 Prozent gaben sogar an, sie würden eine neue Stelle nur antreten, wenn das Unternehmen Home-Office oder flexible Optionen bietet. Jeder zweite (51 Prozent) wünschte sich ein gesetzlich verankertes Recht auf Home-Office und Remote-Arbeit.

Oliver Ebel von Citrix rät den Unternehmen, „ihre Werte in einer Welt nach der Pandemie zu definieren". Bild: Citrix

Die gute Nachricht für Arbeitgeber: Bei der Citrix-Umfrage erklärten mehr als drei Viertel (77 Prozent) der deutschen Befragten, zu Hause mindestens ebenso lange zu arbeiten wie im Büro, 34 Prozent sogar länger. Wie im Büro, so stellt sich allerdings auch in der häuslichen Höhle die Frage, ob Arbeitsdauer gleichzusetzen ist mit Produktivität. Bedenklich: 40 Prozent der Befragten gaben zu Protokoll, ihre psychische Gesundheit habe sich in den letzten zwölf Monaten verschlechtert. Vor diesem Hintergrund halten fast neun von zehn Beschäftigten (88 Prozent) eine Unternehmenskultur für wichtig, die das psychische und/oder physische Wohlbefinden fördert. Citrix' DACH-Chef Oliver Ebel riet Unternehmenslenkerinnen und -lenkern anlässlich der Umfrage: „2021 sollten sie den Blick von der rein operativen Seite des Geschäfts lösen und mehr Zeit und Ressourcen darauf verwenden, ihre Werte in einer Welt nach der Pandemie zu definieren –

„Kein einziges Unternehmen kann sich mehr davor wegdrehen, das Konzept der Arbeitswelt neu zu überdenken," sagt Cisco-Managerin Katharina Jessa. Bild: Cisco

mit einer hybrid arbeitenden Belegschaft, die von ihrem Arbeitgeber unterstützt und eingebunden werden möchte."

Zwar sei der deutsche Mittelstand in puncto Digitalisierung längst nicht so ein Nachzügler wie häufig dargestellt, so Katharina Jessa, die bei Cisco Deutschland den KMU-Vertrieb leitet, gegenüber LANline, doch bei der Förderung neuer Arbeitsweisen sieht auch sie noch Luft nach oben: „Kein Unternehmen kann sich mehr davor wegdrehen, das Konzept der Arbeitswelt neu zu überdenken," so Jessa. Die Unternehmen müssten sich fragen: „Was passiert mit der gesamten kulturellen Herangehensweise? Wie arbeitet man als Team zusammen? Wie gestaltet man die Mitarbeiterführung, die Mitarbeiterentwicklung? Wie motiviert man die Menschen, den persönlichen Kontakt zu halten, wenn sie nicht die Kaffeeküche haben?" Jessa sieht hier drei Baustellen. Erstens gelte es, die Sicherheitsfragen zu klären: „Was braucht man zur IT-Absicherung? Wer darf im Home-Office drucken, wer nicht? Wie stellt man sicher, dass die Daten des Unternehmens und der Endkunden geschützt sind?" Zur Remote-Work-Sicherheit sagt Peter Machat, DACH-Chef bei Ivanti: „Bis 2025 werden Zero-Trust-Zugänge und -Architekturen die Norm sein." Denn ein Unternehmen müsse heute davon ausgehen, dass sich Angreifer bereits im Netzwerk befinden. Sicherheit lasse sich deshalb nur gemäß dem Zero-Trust-Motto „Vertraue nie, verifiziere immer" gewährleisten. Ergänzend, so Machat, sollten Unternehmen Datenzugriffe nur jenen Apps erlauben, denen sie vertrauen und die sie verwalten können – und selbst hier sollte man DLP-Richtlinien (Data Loss Prevention) einrichten.

Zur IT-Security gesellen sich laut Katharina Jessa weitere Sicherheitsaspekte, etwa Regelungen für Arbeitsunfälle im Home-Office. Ist eine rundum sichere Basis geschaffen, gehe es zweitens um eine Hybrid-Work-Strategie: „Um nicht in eine Art Zweiklassengesellschaft abzurutschen, brauchen Unternehmen ein klares Konzept zum Thema hybrides Arbeiten", so Jessa. „Denn der Arbeitsplatz ist zukünftig da, wo man sich befindet, und nicht da, wo man hingeht." Das Unternehmen müsse auch im Home-Office das geeignete Arbeitsumfeld schaffen, damit die Beschäftigten sich auf ihre Arbeit konzentrieren können.

Der dritte Kernpunkt ist für die Cisco-Managerin die Unternehmenskultur. Denn, so Jessa, weder Gesellschaft noch Unternehmen förderten es, beispielsweise zu sagen: „Meine Kinder sind zu Hause, ich kann heute Vormittag nicht arbeiten." Ihre Forderung: „Das Management muss es unterstützen, dass Offenheit gelebt werden darf, dass Verletzlichkeiten gezeigt werden können, dass man sich aufeinander verlassen kann." Hier sei es wichtig, Unterschiede zu akzeptieren: „Nicht jeder ist digital affin, nicht jeder fühlt sich wohl, per Video zu sprechen." Eine Hybrid-Work-Kultur beginnt laut Chris Dercks, DACH-Chef bei F5, schon beim Onboarding: „Die größten Hindernisse beim Digital Onboarding sind das gegenseitige Kennenlernen, die Integration in das Team und die Sicherstellung der Teamdynamik", sagt Dercks. „Dies erfordert deutlich mehr und früheres Nachfragen, erfahrene Mentoren, digitale Einarbeitungspläne, individuelle Lösungen für die Mitarbeitenden sowie Teaming-Events zur Identifikation mit dem Unternehmen." Gefragt sei hier mehr Proaktivität seitens des Managements wie auch der Beschäftigten. Zum Wir-Gefühl verteilter Teams merkt Christian Koch, Digital-Workplace-Experte bei Campana & Schott, an: „Mit den richtigen Voraussetzungen des digitalen Arbeitsplatzes lassen sich Firmen-Events, Expertengespräche oder Kaffeepausen erfolgreich virtualisieren – und fördern so die Interaktion sowie das Zugehörigkeitsgefühl." Hier sei das Führungsteam gefordert, diese Kultur vorzuleben und zu fördern. Wie das in der Praxis aussehen kann, erläuterte Cisco-Managerin Jessa an einem Beispiel: Als die „Black Lives Matter"-Bewegung letztes Jahr in den USA ein brisantes Thema war, sei die Cisco-Führung mit der Belegschaft im Gespräch geblieben, bis alle Fragen dazu beantwortet waren. Eine solche Diskussionskultur dürfte künftig an Bedeutung gewinnen – selbst und gerade wenn die Beschäftigten großflächig verstreut sind.

Ivantis DACH-Chef Pater Machat prophezeit: „Bis 2025 werden Zero-Trust-Zugänge und -Architekturen die Norm sein." Bild: Ivanti

Der lange Weg aus der Höhle

Manch ein pandemiemüder Höhlenbewohner kann es kaum erwarten, den endlosen Schattenspielen auf seinem Display zu entkommen und hinaus ins Sonnenlicht zu treten. Der Weg vom verschanzten zum flexiblen Arbeiten, wie es „Future of Work"-Propheten propagieren, kann steinig sein. Er erfordert nicht nur digitale Tools, KI-Assistenten und Cloud-Services, sondern auch eine Wende in der Unternehmenskultur: weg vom Sippenältesten, der am Lagerfeuer seine Horde um sich schart, hin zum Online-Miteinander, das auf Vertrauen, Offenheit und standortübergreifender Kollegialität beruht. So wie unser innerer Höhlenmensch gestrickt ist, liegt vor uns wohl eine Aufgabe, die den BER-Bau und die Impfkampagne als Fingerübungen erscheinen lässt. Dr. Wilhelm Greiner

LogMeIn erweitert GoToConnect

Digitale Helferlein für flexibles und verteiles Arbeiten

LogMeIn hat sein UCC-Tool (Unified Communications and Collaboration) GoToConnect erweitert. Zu den Neuerungen zählen eine überarbeitete Mobilnutzung, CCsaS-Updates (Cloud Contact Center as a Service), neue Integrationen mit Microsoft Teams sowie Angebotspakete, die LogMeIn-Tools wie LastPass, GoToWebinar und GoToAssist enthalten. Viele GoToConnect-Angebote sind nun direkt online verfügbar.

Das neue GoToConnect, so LogMeIn, sei einfach zu nutzen und biete sich somit für Unternehmen an, die für ihre Belegschaft ein Gleichgewicht zwischen langfristiger Remote-Arbeit und Rückkehr ins Büro anstreben. So ermögliche die Software Remote-Anwendern, berufliche Anrufe auf ihrem Mobilgerät zu empfangen und zu tätigen, ohne ihre Privatnummer zu verwenden. Die aktualisierte Telefonie-App biete verbesserte Funktionen wie Find Me und Follow Me oder auch Voicemail-Transkriptionen.

Mit der aktuellen Version von GoToConnect Support Center erhalte ein Unternehmen konfigurierbare Berechtigungen und benutzerdefinierte Pausenbegründungen. In Kürze folgen sollen anpassbare Dashboards, Auto-Queue Call-Back, intelligentes Call Routing sowie das neue Produkt Revenue Center für Vertriebsorganisationen.

GoToAdmin wiederum biete ein zentrales Portal, um Benutzer, Lizenzen und Einstellungen für mehrere Produkte gleichzeitig zu verwalten. Die Software sei selbst für Neulinge einfach zu bedienen. Der GoToConnect Teams Connector schließlich dient dem Zweck, den der Name verspricht: Er verbindet GoToConnect mit Microsoft Teams. So könne man Microsofts Collaboration-Software weiter verwenden, während GoTo-Connect den Telefonie-Service Backend-seitig mit direkten Routing-Funktionen und Features wie Click to Call und Benutzerpräsenz versorge.

GoToConnect gibt es in drei Paketen: GoToConnect Basic bietet – man ahnt es – Basisfunktionen wie Cloud-Telefonie-, Meeting- und Messaging-Features. GoToConnect Standard Plus umfasse darüber hinaus eine Passwortverwaltung und virtuelle Veranstaltungen. Am oberen Ende der Skala findet man GoToConnect Premium Plus, das es erlauben soll, die gesamte „Work from Anywhere“-Belegschaft zu unterstützen. Enthalten ist hier das Tool GoToRoom, um Besprechungszimmer in videofähige Meeting-Räume zu verwandeln, GoToWebinar für Online-Veranstaltungen, GoToAssist für Remote Support und LastPass Enterprise für den Schutz der Fernzugriffe. wg

Remote Work mit Privatgeräten

Bring dein eigenes

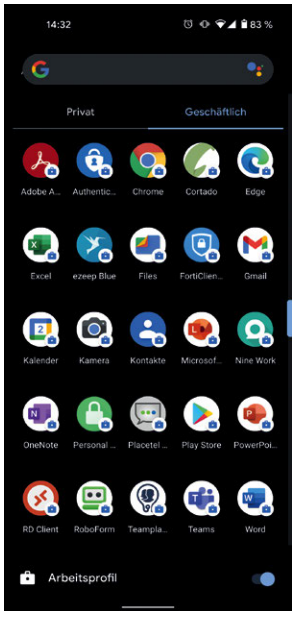
In Australien ist es durchaus üblich, seinen eigenen Wein ins Restaurant mitzunehmen (Bring Your Own, BYO). Deshalb kann vermutlich jeder Australier mit dem Begriff „Bring Your Own Device“ (BYOD) etwas anfangen. Hierzulande hingegen ist der Begriff nach wie vor ziemlich unbekannt. Doch es lohnt die Diskussion, ob und wie Unternehmen und deren Belegschaft Privatgeräte im Berufsalltag nutzen können und vielleicht sogar sollten. Dabei stellt sich im übertragenen Sinne die Frage, wer zum Schluss die „Entkorkungsgebühr“ zahlt, die in Australien bei BYO anfällt.

Insbesondere während des ersten Lockdowns – und nochmals verstärkt durch die Einführung der Home-Office-Pflicht – gab es viele Ansätze, Remote Work spontan umzusetzen. Einige packten ihren Arbeitsplatzrechner einfach ein, manchen Firmen gelang es noch, Bestände von neuen Laptops zu sichern, und andere hofften einfach auf eine gute technische Ausstattung ihrer Beschäftigten. Kombiniert mit Lösungen wie VPN, virtuellen Desktops und Device-Management konnten Unternehmen die Produktivität nicht nur erhalten, sondern teilweise sogar deutlich erhöhen.

Die Diskussion, ob Unternehmen Privatgeräte zulassen sollten, ist mitunter hochemotional aufgeladen. Die einen warnen vor Datenschutzproblemen, die anderen unterstellen die Ausnutzung von Beschäftigten. Beides mag ein Problem darstellen, ist aber eher ein Argument für die Einführung einer durchdachten BYOD-Strategie als dagegen. Denn eines ist klar: Ohne weitere Maßnahmen einfach die geschäftliche E-Mail auf einem privaten Gerät zu empfangen, ist in jeder Hinsicht problematisch – und diese ungeschützte Nutzung der Privatgeräte in einer Schatten-IT ist durchaus verbreitet.

Der Stand der Technik bietet ausreichend Möglichkeiten des Datenschutzes, und bei einer korrekten Ausgestaltung eines BYOD-Vertrages kann ein Unternehmen die geschäftliche Nutzung privater Geräte angemessen erstatten. Wählt man dann für Smartphones noch das richtige Mobile-Device-Management, sodass Mitarbeiter transparent erkennen können, welche Einflussmöglichkeiten die IT auf das private Gerät hat, dann kann BYOD ein Vorteil sowohl für das Unternehmen als auch für die Beschäftigten sein.

Es gibt viele Gründe für BYOD, zum Beispiel wenn es viele häufig wechselnde Beschäftigte gibt, typischerweise bei Lieferdiensten, oder wenn Unternehmen ihrer Belegschaft mehr Freiheiten bei der Auswahl des Endgeräts bieten wollen. Teilweise reichen für die betrieblichen Anforderungen einfachere Geräte, die Beschäftigten würden aber höherwertige Geräte bevorzugen. In Unternehmen, die auf eine gute Work-Life-Balance setzen, kann es für die Belegschaft einfacher und angenehmer sein, mit einem Privatgerät zu arbeiten als mit zwei getrennten.



Mit MDM-Lösungen kann die IT-Abteilung die mobilen Endgeräte in einen privaten und einen geschäftlichen Bereich unterteilen und letzteren zentral verwalten.
Bild: Cortado

Work-Life Balance und rechtlicher Rahmen

Der Erfolg von Remote Work und Home-Offices fußt auch auf respektvoller Kommunikation. Wenn Vorgesetzte zu Unzeiten Beschäftigte kontaktieren, um Dinge anzusprechen, die auch bis zum nächsten Tag warten könnten, dann mindert dies die Akzeptanz neuer Arbeitskonzepte erheblich. Die Nutzung der „Später senden“-Funktion von Outlook kann hier helfen, die unterschiedlichen Arbeitszeiten im Home-Office auszugleichen. Auch die technischen Anforderungen sollten Unternehmen aufeinander abstimmen: Seltene Linux-Versionen auf dem Desktop sind ähnlich hinderlich wie Mobilgeräte mit exotischen Betriebssystemen.

Ein weiterer Stolperstein ist der gesetzliche Rahmen. Für den Fall, dass Beschäftigte, und sei es auch nur aus Versehen, das geschäftliche E-Mail-Konto zu privaten Zwecken nutzen, sollten sie unbedingt dem §88 TKG zugestimmt haben. Andernfalls wäre es unrechtmäßig, Spam-Filter und Ähnliches einzusetzen. Der Arbeitgeber sollte die Belegschaft über alle Aspekte in Hinblick auf den Datenschutz aufklären und klar darlegen, welche Eingriffe er auf dem Gerät des Angestellten vornehmen kann. So muss er klarstellen, dass es nicht ausreicht, das Gerät mit der PIN 1234 zu schützen. Auch Dinge, die eigentlich im Sinne der Beschäftigten liegen, sollte das Unternehmen klar benennen. So kann die IT-Abteilung beispielsweise bei Verdacht auf Verlust des Geräts den Bildschirm sperren oder den geschäftlichen Bereich ohne Nachfrage löschen. Zudem sollte das Unternehmen mit der Belegschaft vereinbaren, dass es den ge-

Remote-Work-Lösungen wie Igels UD Pocket bieten eine sichere portable Arbeitsumgebung, die sich auf privaten Desktops und Laptops vom USB-Stick aus starten lässt. Bild: Igel

schäftlichen Bereich auch beim Ende des Arbeitsverhältnisses löschen darf.

Bei aller Technik: Keine Lösung kann alles abfangen. Ist es zum Beispiel für die Geschäftsprozesse hilfreich, die Kamera einzusetzen, etwa im Rahmen einer Schadensbegutachtung, dann kann das System vermutlich diese Fotos nicht von privaten Fotos unterscheiden. Gleiches gilt für PDF-Dokumente. Doch das ist kein BYOD-typisches Problem, denn auch mit geschäftlichen Geräten kann ein Mitarbeiter private Fotos aufnehmen. Aber ein BYOD-Vertrag kann hier ein guter Anlass sein, um zu vereinbaren, dass Beschäftigte private Inhalte nicht in das Unternehmensnetzwerk einbringen und umgekehrt auch Unternehmensdaten nicht privat verwenden.

Abgesehen vom Datenschutz gilt für alle Remote-Work-Bereiche, dass sich Arbeitgeber wie Arbeitnehmer an die geltenden Arbeitszeitregelungen halten. Durch die Möglichkeit, auch noch spät schnell die eine oder andere E-Mail zu beantworten, ist das mitunter eine echte Herausforderung. Und letztendlich müssen sich beide Seiten einigen, wie mit einem Geräteverlust umzugehen ist, denn dann ist der Beschäftigte eventuell nicht mehr arbeitsfähig. Soll er für den Ersatz aufkommen, gibt es eine Versicherung oder stellt das Unternehmen Ersatzgeräte?

Smartphones und Tablets

Android wie auch iOS bieten die Basis für die vollständige Umsetzung einer BYOD-Strategie – ein MDM (Mobile-Device-Management), das den aktuellen Stand unterstützt, vorausgesetzt. Zudem sollten sich Unternehmen den Prozess der Einbindung privater Geräte einmal aus Mitarbeitersicht anschauen. Denn viele Implementierungen sind eher abschreckend als anwenderfreundlich. Klar aber ist: Ohne MDM ist es unmöglich, den Anforderungen des Datenschutzes und der Privatsphäre gerecht zu werden. Im Prinzip wird dazu bei Android und iOS ein geschützter Geschäftsbereich (Business-Container) angelegt. Nur diesen Business-Container verwaltet das Unternehmen. Isolierte PIM-Systeme, die wegen ihrer anderen Bedienung als die nativen Programme oft auf Ablehnung stoßen, sind somit überflüssig.

Wie aber lässt sich ein solcher Business-Container auf einem Desktop- oder Laptop-Rechner abbilden? Schließlich existieren hier die von iOS und Android bekannten Mechanismen nicht. Ganz einfach: Der Remote Desktop ist die Antwort für Remote Work. Für BYOD hat ein Remote Desktop – unabhängig davon, ob das Unternehmen ihn in der Cloud (etwa per Windows Virtual Desktop) oder lokal (beispielsweise Windows Server mit Remote Desktop Session Host) – betreibt, den Vorteil, dass die Anforderungen an die Endpunkt-Hardware minimal sind. Zudem lässt sich der Remote Desktop per Konfiguration hermetisch vom Rest des Privatrechners abgrenzen. So kann man den Zugriff auf Drucker, Zwischenablage, Verzeichnisse, Kamera und Mikrofon unterbinden. Wem das noch nicht ausreicht, der kann mit USB-Stick-basierten Lösungen wie etwa dem Igel UD Pocket sogar erreichen, dass der Rechner für den Remote Desktop mit einem eigenen Betriebssystem startet. So ist die Abschirmung perfekt, und über Cloud Printing kann der Nutzer von einem solchen Rechner aus dennoch sicher drucken. Durch Remote Desktops besteht für die Beschäftigten zudem vollständige Freiheit bei der Wahl des Endgeräts, ohne dass das Betriebssystem oder dessen Version einen Einfluss auf die Umsetzung der Geschäftsprozesse hätte.

Bring Your Own Device passt vielleicht nicht für jedes Unternehmen, aber es gibt viele Anwendungsbereiche, in denen BYOD die Erwartungen von Mitarbeitern und Arbeitgebern gut erfüllen kann. Dank der aktuellen MDM-Systeme und der schon lange etablierten Remote-Desktop-Lösungen steht BYOD technisch wie auch rechtlich nichts mehr im Weg.

Carsten Mickeleit/wg

Mythen der BYOD-Gefahren bei Smartphones

Die folgenden Punkte gelten vielen als Risiko von BYOD-Szenarien. Aber trifft das zu?

1. Sicherheitsrisiko Mitarbeiter, insbesondere Geräteverlust: Nein, denn Mitarbeiter passen wesentlich sorgfältiger auf private Geräte auf, und geschäftliche Daten kann das IT-Team per MDM aus der Ferne löschen.
2. Sicherheitslücke mobiles Betriebssystem: Nein, denn mobile Betriebssysteme sind bei zeitnaher Aktualisierung deutlich sicherer als Desktop-Betriebssysteme.
3. Schadsoftware: Nein, denn mobile Betriebssysteme sind in der Regel deutlich weniger anfällig, und die OS-Anbieter kuratieren die Apps in ihren App Stores. Das vereinfacht es, Schadsoftware auszuschließen.
4. Unsichere Apps: Nein, denn die IT-Abteilung kann unsichere Apps auf die Blocklist setzen und ihre Installation auf diese Weise ausschließen.
5. Jailbreak, Rooten und Custom ROM: Nein, denn solche Geräte lassen sich per MDM ebenfalls ausschließen.
6. Netzwerkverbindungen: Ja, allerdings sind die Gefahren bei privaten und geschäftlichen Geräten identisch. Zusätzlich kann die IT ein Always-on-VPN per MDM einrichten.
7. Datenschutz bei Mischnutzung: Ja, ganz klar. Deshalb sollte man BYOD auch nie ohne MDM einführen.
8. Privatsphäre in Gefahr: Nein, bei Android kann man schon längst, bei Apple seit iOS 13 den Zugriff auf private Daten ausschließen.
9. Steuerrechtliche Probleme durch Aufwandserstattungen: Nein, die Erstattung von Aufwendungen durch den Arbeitgeber muss lediglich dem Maß der betrieblichen Nutzung entsprechen.
10. Urheber-Lizenzrecht: Nein, denn per MDM können Unternehmen sicherstellen, dass die Beschäftigten nur lizenzierte Software nutzen.

Carsten Mickeleit ist CEO der Cortado Holding.

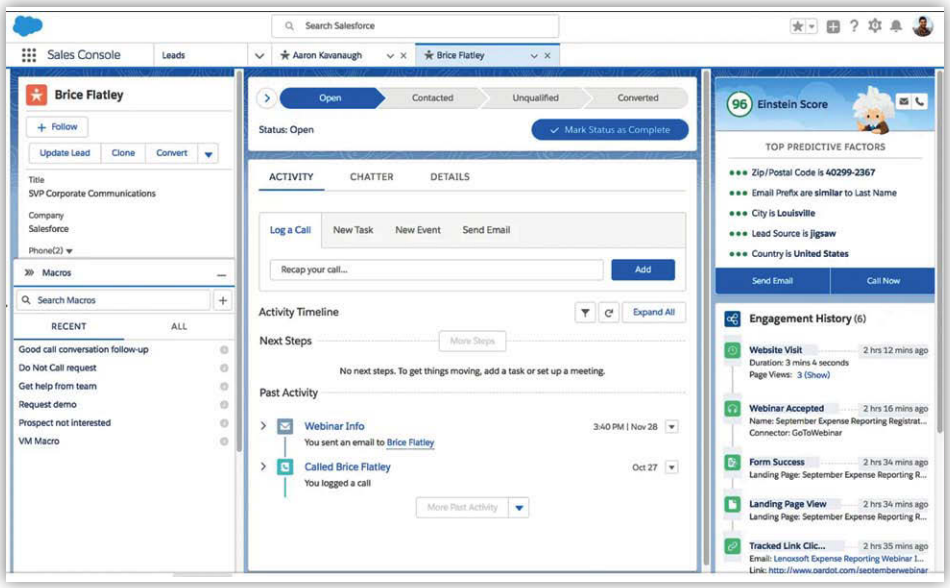
Künftige Rolle der KI im Alltag

Intelligenter arbeiten

Die Coronavirus-Pandemie wirkt als Beschleuniger für die digitale Transformation und hat auch die Akzeptanz künstlicher Intelligenz (KI) zur Ergänzung, Unterstützung und Entlastung von Teams verschiedener Abteilungen erhöht. KI-Vorhersagen werden die Arbeitswelt auf vielfältige Weise weiter verändern.

KI-gestützte Lösungen helfen Unternehmen unter anderem dabei, passgenauer zu verkaufen, den Support zu skalieren, mit Kunden besser zu interagieren und das Kundenerlebnis zu personalisieren. Basierend auf vorhandenen Daten und Annahmen lernen KI-gestützte Bots („Softwaremaschinen“) immer besser, vorausschauende Einschätzungen und Empfehlungen zu geben. Allein bei Salesforce liefert KI-Technik heute schon mehr als 93 Milliarden Vorhersagen pro Tag. Diese Zahl zeigt, wie groß die Akzeptanz von KI bereits ist. Hier profitieren Unternehmen besonders, die KI einsetzen, um ihre Kunden besser zu verstehen und einzubinden. Dabei arbeitet KI-Technik quasi unsichtbar hinter den Kulissen und versetzt Unternehmen in die Lage, das Verhalten und die Vorlieben ihrer Kunden in großem Umfang vorherzusagen und ihre Erwartungen zu erfüllen.

Damit verändert sich auch die Arbeitswelt, wie wir sie kennen, grundlegend. KI-unterstützte Analysen und Empfehlungen helfen Unternehmen dabei, Prozesse effizienter zu gestalten. Der Belegschaft ermöglichen sie die Automatisierung von Routineaufgaben. So können sie sich auf strategischere Arbeiten konzentrieren, für die ihre menschlichen Stärken unersetzlich sind. Durch leistungsfähige und anwenderfreundliche KI-Tools müssen die Mitarbeiter keine Programmierer und Datenwissenschaftler mehr sein, um Vorhersagen zu erzeugen und zu nutzen. Denn um mit ihnen zu arbeiten, braucht es nur Klicks, nicht Code.



Ki-gestützte Assistenzfunktionen (im Bild rechts oben) können im Vertrieb und anderen Abteilungen die Orientierung und Priorisierung verbessern. Bild: Salesforce

Praxisbeispiele

Personalisierte Konversationen: Als die Coronavirus-Pandemie ausbrach, mussten viele Unternehmen schnell auf das sich in Richtung online verändernde Kaufverhalten reagieren. Dabei war entschied allem die Fähigkeit einer individualisierten Kundenansprache über den Erfolg. Mit KI-unterstützter Personalisierung konnten sie beispielsweise über gezielte Kampagnen passgenauer kommunizieren, den Traffic auf ihren Online-Plattformen erhöhen und deutlich schneller auf Trends reagieren. So konnten sie Kundenerwartungen erfüllen und Umsätze nicht nur schützen, sondern teils sogar steigern.

Nachfragespitzen bewältigen: Durch Lokalschließungen und Social Distancing sahen sich Branchen wie Essensliefer- oder Paketdienste mit einem enormen Anstieg der Nachfrage konfrontiert. In diesem Fall hat KI geholfen, das wachsende Volumen an Kontakten zu bewältigen. Kunden konnten KI-gestützt – zunehmend auch über Service-Bots – ihre Bestellungen oder Pakete nachverfolgen, Probleme mit Verspätungen oder Schäden melden und zeitnah eine Gutschrift oder Erstattung erhalten. Dies hat bei vielen Unternehmen für zufriedene Kunden und einer besseren Service-Bewertung gesorgt.

Mensch-Maschine-Vertriebsteams: Die Wertschätzung kompetenter Vertriebsmitarbeiter als informierte und einfühlsame Berater ist während der Pandemie zwar gestiegen; zugleich haben sie immer weniger Zeit, hilfreiche Erkenntnisse zu sammeln. Immer mehr Teams gehen deshalb dazu über, wiederkehrende Routineaufgaben zu automatisieren. So gewinnen die Beschäftigten mehr Zeit für Aufbau und Pflege von Kundenbeziehungen und andere wertschöpfende Vertriebstätigkeiten. KI hilft Vertriebsteams in diesem Zusammenhang beispielsweise, Anfragen leichter zu priorisieren sowie und zu erkennen, welche Folgeschritte im Dialog zielführend sind. Außerdem ist KI ein willkommener Assistent, um Verwaltungsaufgaben wie die Da-

tenerfassung oder Gesprächsnotizen zu beschleunigen.

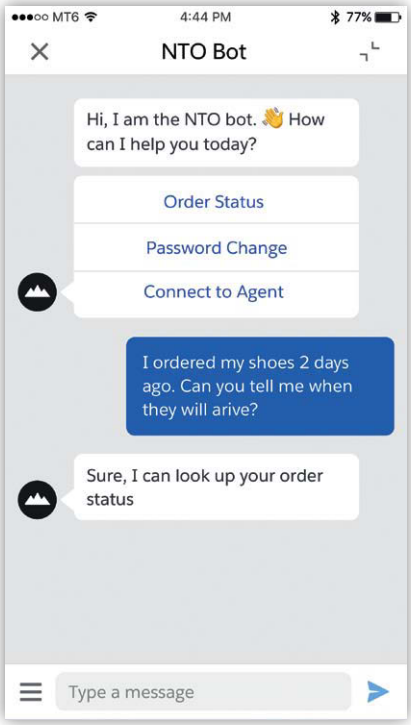
Genauere Cashflow-Prognosen: In Branchen wie dem Bankensektor verzögern sich Zahlungseingänge immer häufiger. Dies erschwert es auch, kurz- und langfristige Cashflows vorherzusagen. Hier tragen KI-unterstützte Einblicke und Prognosen dazu bei, den Betrieb aufrechterhalten zu können. Gleichzeitig helfen sie auch, ein besseres Bild der zugrunde liegenden Herausforderungen der Kunden zu erhalten und schneller darauf einzugehen.

Diese Beispiele zeigen, wie Unternehmen KI nutzen, um beispielsweise Anomalien und Korrelationen in Daten zu erkennen, die zuvor verborgen waren, um Prognosen zu erstellen, Empfehlungen zu geben und individuelle Ansprache auch in der Masse zu ermöglichen oder einfach, um wiederkehrende Abläufe zu automatisieren. Einerseits hilft Automatisierung durch Techniken wie Chatbots, administrative Vorgänge oder Routineanfragen effizient und skalierbar zu bewerkstelligen. Andererseits ermöglichen KI-unterstützte Einblicke und Empfehlungen den nun von Routinetätigkeiten befreiten Mitarbeitern, sich auf die Betreuung der wichtigsten Kunden zu fokussieren und sich Themen zu widmen, die menschliche Kompetenzen wie emotionale Intelligenz und Empathie erfordern.

KI verhilft Unternehmen damit zu mehr Kundenzentriertheit und Agilität. Sie können ihre Kundenbasis ebenso wie jeden einzelnen Kunden anhand der neuen Einblicke besser verstehen. Zugleich können sie Strategie und Prozesse kontinuierlich optimieren, um sich im Wettbewerb zu differenzieren. Denn datengetriebene Unternehmen, die schneller und proaktiv erkennen, wie sich der Markt und Erwartungen verändern, können die Weichen leichter auf Wachstumskurs stellen.

Vertrauen in KI aufbauen

In dem Maße, wie Technologie immer „intelligenter“ wird, wächst auch die Notwendigkeit, die Entwicklung und Nutzung von KI vertrauenswürdig zu gestalten. Eine neue Generation von Mitarbeitern, die in einer KI-Welt zu arbeiten beginnt, wird



Chatbots nehmen den Service-Teams die Bearbeitung von Routineanfragen ab. Bild: Salesforce

mit automatisierten KI-Aktionen wie mit jedem anderen Werkzeug interagieren. Wir treten in eine Ära ein, in der teils noch bestehende Vorbehalte gegenüber KI einem immer größeren Miteinander weichen. Eines Tages werden wir die KI in unserer Arbeitswelt so wenig hinterfragen wie die Nutzung von Elektrizität.

Dabei ist es wichtig, transparent zu machen, wie genau ein Algorithmus arbeitet, und die ethische Nutzung sicherzustellen. Denn auch das gehört zu den wachsenden Herausforderungen: die steigende Erwartung wertebasierter Unternehmensführung. Dies schließt ökologische Nachhaltigkeit ebenso ein wie ethische Geschäftspraktiken im Umgang mit Daten und deren KI-gestützter Nutzung.

Dafür existiert zum Beispiel die Methode der „Explainable AI“ (erklärbare KI): Sie hilft zu verstehen, wie und warum ein KI-System Vorhersagen trifft oder Empfehlungen gibt. Je nach Benutzer oder Anwendungsfall existieren unterschiedliche Ebenen der Erklärbarkeit oder Interpretierbarkeit. Manchmal genügt es, die wichtigsten Prädiktoren (Vorhersagevariablen) eines Modells aufzuzeigen, die Proxy-Variablen (Variablen zur Messung nicht direkt zugänglicher Eigenschaften) und die Korrelationen, die eine Empfehlung beeinflussen. Ein Beispiel ist das sogenannte Commonsense Reasoning (menschenähnliche Einschätzung von Alltagssituationen) bei der Verarbeitung natürlicher Sprache. Dabei kommt ein Erklärmodell zum Einsatz, um Commonsense Reasoning in ein Deep-Learning-Modell zu integrieren. Damit können auch Businessnutzer Entscheidungen nachvollziehen. Auf diese Weise trägt Explainable AI nicht nur zum Vertrauen der Anwender, sondern auch zu einer besseren Leistungsfähigkeit der Technik an sich bei.

In einer Zeit, in der viele Unternehmen mit weniger mehr erreichen müssen, kann die Investition in KI-Tools die Widerstandsfähigkeit erhöhen. Unternehmen sollten deshalb ihre Mitarbeiter dazu ermutigen, KI-Techniken kennenzulernen, und entsprechende Trainings anbieten. Durch Vertrauen, Akzeptanz und das Wissen über die Anwendung von KI-Lösungen gelingt ein wesentlicher Veränderungsprozess: Es entsteht eine neue Arbeitskultur der stetigen Weiterentwicklung in enger Abstimmung mit den Unternehmenszielen.

Fazit

Indem KI uns in die Lage versetzt, bessere Entscheidungen zu treffen, hat sie das Potenzial, jeden Menschen und jedes Unternehmen schneller, besser informiert, effizienter und damit produktiver zu machen. Mitarbeiterinnen und Mitarbeiter treffen fundiertere Entscheidungen und verändern die Kundeninteraktion mit ihrer Kundschaft grundlegend. Sie schaffen so tiefere, persönliche Verbindungen und haben mehr Zeit für echte Innovationen. Somit ist KI keine Konkurrenz für menschliches Handeln. Im Gegenteil: KI liefert die Grundlage für Erkenntnisse, um neue Produkte, Dienstleistungen und Arbeitsplätze zu schaffen. Das Potenzial dieser intelligenten Unterstützung ist enorm. KI wird unser Leben, unsere Art zu arbeiten und unsere Wirtschaft durchaus positiv verändern.

Frank Engelhardt/wg

Frank Engelhardt ist Vice President Enterprise Strategy bei Salesforce.

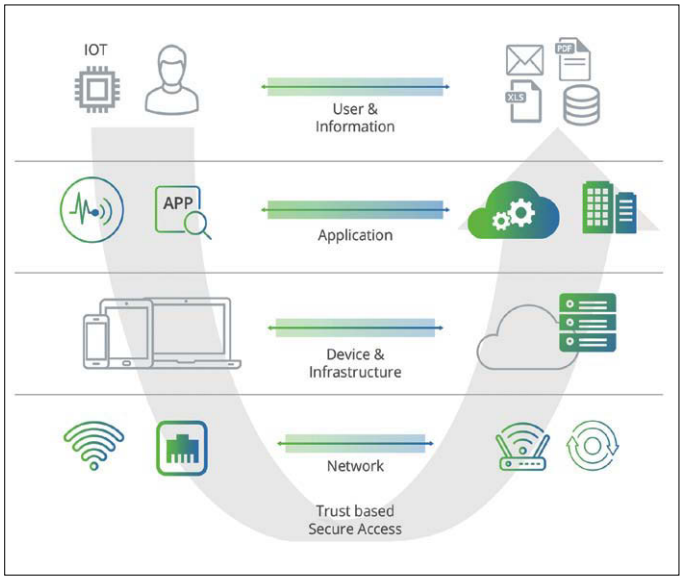
Zero-Trust-Netzwerke

Sicherheit für das Cloud-Zeitalter

Die Idee eines Zero-Trust-Netzwerks entstand während der 2000er-Jahre im US-Verteidigungsministerium. Später entwickelte die IT-Security-Community das Konzept mit Beteiligung der Cloud-Security-Alliance (CSA) zum aktuellen ZTNA/SDP-Framework (Zero-Trust Network Access, Software-Defined Perimeter) weiter. Denn vor allem eine sich immer schneller ändernde IT-Bedrohungslage erforderte eine Alternative zur klassischen Firewalling-Strategie.

Zunehmende Vernetzung und die wachsende Akzeptanz von Cloud- und IoT-Technologien bringen die klassische Idee eines festen Domänenübergangs mehr und mehr an ihre Grenzen. Remote-Arbeit, Multi-Cloud-Anwendungen und Edge Computing benötigen ein flexibleres Sicherheitskonzept, das eine granulare Sicherheitsabstufung auf Nutzerbasis bietet und sich gleichzeitig schnell skalieren und an den aktuellen Bedarf anpassen lässt. Genau hier setzen Zero-Trust-Modelle mit einem softwaredefinierten Perimeter an. Der Begriff Zero-Trust bezieht sich dabei auf einen entscheidenden Paradigmenwechsel: Früher stattete man Clients, die sich aufgrund ihrer IP-Zuordnung im vermeintlich sicheren lokalen Netzwerk bewegten, mit zusätzlichen Privilegien wie File-Server-Zugriff und Druckberechtigung aus; im Zero-Trust-Netzwerk hingegen gilt immer das Prinzip „traue niemandem“ – unabhängig davon, ob sich die Quell-IP-Adresse eines Nutzers im eigenen LAN, WAN oder Internet befindet.

Um ein Zero-Trust-Modell durchzusetzen, kommt anstelle eines durch Firewall und DMZ abgesicherten statischen Netzwerkübergangs ein flexibler Netzwerkperimeter zum Einsatz. Der softwaredefinierte Perimeter baut dafür – ähnlich wie ein VPN – ein privates Overlay-Netzwerk auf, das Benutzer und IT-Geräte sicher über das Internet mit Servern und Anwendungen in einem RZ oder in der Public Cloud verbindet. Jeder Host verfügt dabei über einen eigenen privaten IP-Adressraum, sodass er im Internet sozusagen unsichtbar ist. Dieser Ansatz reduziert die IT-Angriffsfläche einer Infrastruktur deutlich und minimiert so das Gefahrenpotenzial häufig auftretender Bedrohungen wie Denial-of-Service-Angriffe, Man-in-the-Middle-Attacke und Malware-Befall.



Die Sicherheitsebenen in einem Zero-Trust-Netzwerk. Bild: Sysob

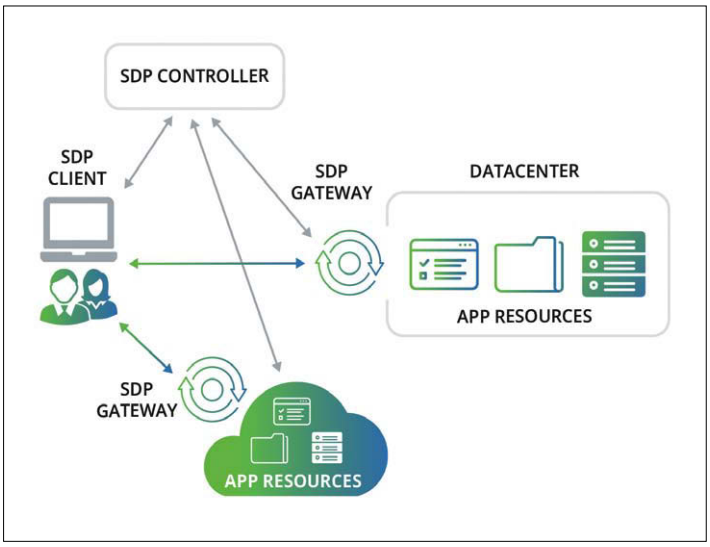
Um möglichst wenig Angriffsfläche zu bieten, setzt das SDP-Konzept auf zusätzliche Sicherheitsmechanismen: die Kombination von Netzwerk-Virtualisierung, Segmentierung und Ende-zu-Ende-Verschlüsselung. Da ein Software-Defined Perimeter weitestgehend unabhängig von der zugrunde liegenden IP-basierten Infrastruktur agiert, bietet das Konzept eine effektive Architektur für die Einführung einer Zero-Trust-Strategie. Die im SDP implementierten Sicherheitsmechanismen greifen noch vor der Transport- und Session-Schicht in die TCP/IP-Netzwerkschicht ein. Dies ist ein wichtiger Aspekt, da die Transportschicht die Host-zu-Host-Kommunikationsdienste für Anwendungen bereitstellt und der Session-Layer für das Session-Handling von Verbindungen zwischen Endbenutzer-Anwendungsprozessen verantwortlich ist.

Viele Unternehmen setzen heute noch auf rein IP-basierte Kontrollfunktionen, um auf den Schichten 1 bis 4 des OSI-Stacks ein Trust-Modell zu etablieren. Dieser Ansatz stellt aber ein grundsätzliches Problem dar, denn IP-Adressen fehlt jede Information über einen Nutzer oder über die Integrität eines IT-Geräts. IP-Adressen liefern lediglich Verbindungsdaten, geben aber keinen Hinweis auf die Vertrauenswürdigkeit eines Endpunkts oder eines Benutzers. Ein Beispiel dafür ist das bidirektional arbeitende Protokoll TCP. Es arbeitet auf Schicht 4 des OSI-Netzwerk-Stacks und ermöglicht es internen vertrauenswürdigen Hosts, mit externen nicht vertrauenswürdigen Hosts zu kommunizieren. Dabei können auch potenziell gefährliche oder veränderte Datenpakete in ein internes Netz gelangen. Jede Änderung an einer einzelnen IP-Adresse kann zudem einen hohen Konfigurationsaufwand mit sich

bringen, wodurch sich leicht Fehler in Netzwerk-Sicherheitsgruppen und Access-Listen einschleichen können. Schlecht konfigurierte interne Hosts bieten Hackern einen leichten Einstiegspunkt, indem sie Standardantworten auf veraltete Protokolle wie ICMP versenden. Die allgemeine Transparenz von IP-Netzwerkverbindungen ist eines der Hauptprobleme der IP-basierten Netzwerksicherheit und stellt eine Hürde für die Implementierung von erweiterten IT-Sicherheitslösungen dar.

Individuelle Anwendungen mit zusätzlichen Sicherheitsmechanismen auszustatten ist eine komplexe, zeit- und kostenintensive Herausforderung. Die Nachrüstung von Sicherheitsfunktionen in Anwendungs- und Containerplattformen erfordert die Integration von Access Control, Identitäts-Management, Token- und Firewall-Management sowie eine übergreifende Orchestrierung. Dieser Aufwand erweist sich für die meisten IT-Organisationen jedoch als kaum zu meistern. Deshalb erfolgt die Implementierung zusätzlicher Security-Kontrollmechanismen heute meist durch das zentralisierte Erfassen von Verlaufsdaten auf Protokollebene. Diese Informationen erreichen dann ein zentrales SIEM- oder SOAR-System (Security-Information- und Event-Management; Security Orchestration, Automation, and Response) zur Analyse.

Einen „Single Point of Trust“ für Netzwerkverbindungen zu etablieren ist in der Praxis jedoch sehr komplex, da eine Integration von Identitäts-Management-Funktionen innerhalb einer heterogenen Netzwerkstruktur ressourcenintensiv ist. Eine Alternative dazu bieten aufeinander abgestimmte NAC-Lösungen (Network Access Control). Sie ermöglichen den Aufbau eines Zero-Trust-Netzwerks, das bereits alle modernen Geschäftsanforderungen erfüllt und sich leicht an Bedarfsänderungen anpassen lässt. Ein solches System muss grundlegende Elemente vereinen, darunter eine zentrale Richtlinienverwaltung und -autorisierung sowie mikrosegmentierte Anwendungs- und Ressourcenzugriffskontrolle für Datacenter- und Cloud-Anwendungen. Statt auf IP-Adressen basiert eine solche Secure-Access-Lösung ausschließlich auf Mikrosegmentierung und verteilte Richtliniendurchsetzung innerhalb des softwaredefinierten Perimeters.



Ein dynamisches, verbindungsbasiertes SDP-Modell reduziert das Risiko einer Malware-Infiltration. Bild: Sysob

Manche spezialisierte Lösungsanbieter erweitern dieses Modell nochmals und teilen es in verschiedene Sicherheitsebenen wie Benutzer, Anwendungen, Geräte und Infrastruktur sowie Netzwerk. Diese sind typischerweise mit unterschiedlichen Verwaltungsdomänen innerhalb der IT-Organisation verbunden. Das Ziel der obersten Ebene ist es, dem Benutzer (oder IoT-Gerät) einen sicheren Zugriff zum Erstellen, Speichern und Abrufen von Informationen bereitzustellen. Der Zugriff erfolgt auf Basis einer Vertrauensbeziehung über und zwischen den einzelnen Ebenen. Einige Einsatzfälle beruhen auf implizitem Vertrauen, während andere explizite Vertrauensbeziehungen erfordern. Beispielsweise könnte eine IT-Umgebung einem Benutzer, der sich an einem alten, mit dem Unternehmens-LAN verbundenen Computer anmeldet, implizit vertrauen, sodass er auf die meisten lokalen Unternehmensanwendungen zugreifen kann (Dateifreigaben, E-Mail-Server, Intranet-Server etc.). In modernen Umgebungen muss sich ein Benutzer möglicherweise auch mit einer Mobilgeräte-App authentifizieren, die von einer Endpoint-Management-Lösung installiert wurde und ein gesichertes Geräteprofil für WLAN-Verbindungen erzwingt, um auf die Unternehmensanwendung hinter der Firewall zuzugreifen. Benutzerrollen mit individuellem Profilteil bestimmen dann, auf welche Informationen und Anwendungen der Benutzer zugreifen darf.

Solche dynamischen, verbindungsbasierten Modelle beruhen ausschließlich auf Benutzer-, Geräte- oder Anwendungssicherheit und stellen eine natürliche Erweiterung von anwendungsspezifischen oder NAC-basierten Verbindungen dar. Dadurch lässt sich ein Unternehmensnetz effektiv absichern und das Potenzial von Malware-Infiltration verringern. Zudem sorgt die Integration und Erweiterung des SDP-Clients mit Richtlinien für echte Zero-Trust-Sicherheit mit zusätzlichen, dynamisch granularen Verbindungsoptionen. Und die Ermöglichung von Anwendungstransparenz über den Datenpfad des SDP-Gateways hinaus bietet einen Mehrwert für Unternehmensnetze: So ist jederzeit sichergestellt, dass Anwendungen betriebsbereit sind und Mitarbeiter rund um die Uhr und unabhängig von ihrem Standort sicheren Zugriff haben.

Idealerweise bietet eine SDP-Lösung die nötigen Funktionen, um einen SDP ebenso wie gemischte Secure-Access-Modelle zu ermöglichen, wenn Unternehmen zu hybrider IT migrieren oder diese vollständig nutzen. Wollen Unternehmen ihre Sicherheit und Compliance verbessern, die Flexibilität ihrer Mitarbeiter erhöhen und ihre Reaktionsfähigkeit steigern, sollten sie genau prüfen, in welchem Umfang ein SDP ihre Geschäftsanforderungen erfüllen kann. Markus Senbert/wg

Markus Senbert ist Channel Account Manager bei Sysob IT-Distribution.

Enterprise Social Networking

Zusammenarbeit jenseits des PCs

Die Arbeitswelt befindet sich im Wandel. Vielen ist jedoch nicht bewusst, wie vielschichtig dieser Wandel ist. Zahlreiche Unternehmen plädieren für neue Arbeitsmodelle und flexibleres Arbeiten, aber setzen dies selbst noch nicht um. Sie verteilen Dokumente immer noch händisch, Schichtpläne hängen am schwarzen Brett aus und Digitalisierung existiert nur auf Strategiepapieren. Die Zukunft der Arbeitswelt („New Work“) erfordert ein Umdenken: einen Wandel der gesamten Unternehmensstruktur.

Großkonzerne mit Home-Office-Regelungen und Gleitzeitmodellen mögen der Meinung sein, New Work habe schon Einzug in das Unternehmen gehalten. Doch mit zeitlicher und örtlicher Flexibilisierung ist es nicht getan. Sie bilden lediglich die Grundsteine für selbstbestimmtes Arbeiten. Unternehmen stehen vor tiefgehenden Veränderungen und Herausforderungen. Eine dieser Herausforderungen besteht darin, das Unternehmen zu einer Gemeinschaft zu formen: New Work verlangt die Teilhabe jedes Einzelnen an der Gemeinschaft. Gerade Unternehmen mit einer vielfältigen Belegschaft müssen sich mit dieser Entwicklung befassen. Daher stellt sich die Frage, wie New Work auch für Beschäftigte funktionieren kann, die nicht am PC arbeiten. Grundlage dafür sind eine funktionierende interne Kommunikation und Vernetzung sowie vor allem die effiziente Zusammenarbeit der gesamten Belegschaft.

Kommunikation in Unternehmen entwickelt sich weg von der klassischen Top-Down-Kommunikation hin zu einem ausgewogenen Austausch aller Beschäftigten. In Anbetracht zunehmender Komplexität haben Firmen erkannt, dass die stärkere Einbindung der Beschäftigten in die Belange des Unternehmens ein Wettbewerbsvorteil sein kann. So soll eine offene Mitarbeiterkommunikation dabei helfen, Betriebsprozesse zu beschleunigen, Projekte schneller umzusetzen und damit die Produktivität zu erhöhen. Das Einbeziehen der Beschäftigten alleine genügt nicht mehr, denn Kommunikation muss mobil und flexibel sein. Sie muss sich ständig neuen Gegebenheiten anpassen. Die Kommunikation der Beschäftigten über geografische Grenzen und Zeitzonen hinweg wird zur Notwendigkeit. Eine weiterreichende Digitalisierung der Kommunikation ist daher unumgänglich. Und dennoch scheint gerade eine digitalisierte Kommunikation vielen Unternehmen Schwierigkeiten zu bereiten und verhindert damit die abteilungsübergreifende Zusammenarbeit. Dabei gibt es mittlerweile ein großes Angebot an Applikationen, die digitale Kollaboration für alle im Unternehmen ermöglichen.

Auf Mobilität ausgerichtete Lösungen für das Enterprise Social Networking erleichtern die unternehmensweite Zusammenarbeit. Bild: Flip

Das Social Intranet und die Mitarbeiter-App sind die wohl bekanntesten Applikationen für die mobile Kommunikation und Kollaboration. Das klassische Intranet hat man dabei um eine Social-Networking-Komponente ergänzt. Das Kernelement einer Mitarbeiter-App ist der Newsfeed. Ähnlich wie in den bekannten sozialen Netzwerken zirkulieren hier unternehmensinterne Neuigkeiten, Veröffentlichungen, Umfragen und wichtige Termine. Durch eine integrierte Chat-Funktion können sich einzelne Beschäftigte, aber auch größere Teams austauschen. Dabei findet der Austausch unmittelbar statt und nicht asynchron wie im Fall der E-Mail. Zudem können die Beteiligten Dateien in sämtlichen Formaten schnell verschicken, was die Effizienz der Zusammenarbeit enorm verbessert.

Zudem sind Lösungen denkbar, die das Projekt-Management vereinfachen und ein übersichtliches Aufgaben-Management ermöglichen. Aufgaben für unterschiedliche Projekte lassen sich einfach priorisieren und einzelnen Beschäftigten oder Teams zuordnen. Insbesondere für das Management komplexer Projekte und deren Workflow sind Projekt-Management-Tools eine nützliche Lösung. Viele Mitarbeiter-Apps verfügen bereits über eigene Module für das Projekt-Management und haben in puncto Kollaboration stark aufgeholt. Ein solches Tool vereinfacht zudem die Kooperation zwischen der Desktop- und der Non-Desktop-Belegschaft. Auf diese Weise lassen sich abteilungsübergreifende Projekte effizienter koordinieren. Fraglich bleibt, inwieweit sich digitale Lösungen für Non-Desktop-Beschäftigte lohnen.

Eines verbindet alle Tools und Funktionen: Sie sind darauf ausgerichtet, Menschen zu helfen und ihnen den Arbeitsalltag zu erleichtern, beispielsweise Beschäftigten in der Produktion mit jahrelanger Erfahrung an einer bestimmten Maschine. Sie haben sich ein fundiertes Wissen in einem Bereich angeeignet und den Arbeitsablauf perfektioniert. Sie haben somit Wissen, das niemand anderem zur Verfügung steht. Gibt man diesen Beschäftigten die Chance, ihr Wissen mit anderen zu teilen, profitiert das gesamte Unternehmen. Mit Lösungen für die interne Kommunikation lassen sich zum Beispiel Fachleute der einzelnen Abteilungen schnell und einfach ausfindig machen. Wissen wird damit für alle Beschäftigten transparent. Gleichzeitig regt dies abteilungs-, standort- und vielleicht sogar länderübergreifende Diskussionen an, aus denen sich interessante Ideen ergeben können. Denn Vernetzung – gepaart mit einem Raum zur öffentlichen Diskussion – führt zu Denkanstößen und kreativen Ideen. Durch eine Plattform für die mobile Zusammenarbeit lassen sich so unterschiedliche Sichtweisen von Fachleuten aus diversen Bereichen zum bestmöglichen Ergebnis zusammenfügen. Voraussetzung ist jedoch ein gleichberechtigter Zugang zur unternehmensinternen Plattform oder App.

Hier stehen Unternehmen vor der nächsten Herausforderung: Non-Desktop-Beschäftigte haben andere Ansprüche an digitale Lösungen als ihre Desktop-Kolleginnen und -Kollegen. Sie sind die tägliche Nutzung komplexer digitaler Systeme meist nicht gewohnt. Daher müssen sich Betriebe im Klaren sein, dass eine funktionierende mobile Zusammenarbeit im gesamten Unternehmen bedeutet, die Anwendungen allen zugänglich zu machen. Folglich sollten sie auf eine einfache und intuitive Anwendung setzen. So können sich auch weniger technikaffine Beschäftigte leicht informieren und vernetzen. Zusätzlich sollten die Anwendungen nicht an einen festen Desktop-Arbeitsplatz gebunden, sondern auch mobil abrufbar sein. So sind der Nutzerschaft keine Grenzen gesetzt. Beschäftigte fühlen sich damit besser in das Unternehmen integriert, wertgeschätzt und verstanden. Dies stellt eine Nähe zum Arbeitgeber her, was die Motivation erhöht. Die Teilhabe an einer Gemeinschaft ist somit kein Privileg der Desktop-Beschäftigten. Denn die Zukunft der Arbeit wird davon geprägt sein, ein „Wir-Gefühl“ zu erzeugen, das auch alle Non-Desktop-Beschäftigten inspiriert, Verantwortung zu übernehmen und so selbstbestimmt wie möglich zu arbeiten.

Dieses „Wir-Gefühl“ steht ganz im Zeichen langfristiger Mitarbeiterbindung. Der Fachkräftemangel zwingt Unternehmen dazu, fähige Beschäftigte so lange wie möglich im Unternehmen zu halten. Diese wollen inkludiert, verstanden und motiviert sein. Durch Enterprise Social Networks fühlen sich alle im Betrieb stets informiert und am Unternehmensgeschehen beteiligt. Dies verbessert neben der Bottom-up-Kommunikation auch die Zusammenarbeit mit der Führungsebene: Führungskräfte können sich durch Feedbackmechanismen einen Überblick über die aktuelle Gemütslage im Unternehmen verschaffen. So können sie gezielt auf mögliche Frustrationen und Ängste reagieren.

Blickt man ferner in die Zukunft, so werden verschiedene Entwicklungen die mobile Zusammenarbeit in Unternehmen maßgeblich beeinflussen. Innovative Technologien schaffen ein komplett neues Arbeitsumfeld in allen Arbeitsbereichen. Beispielsweise finden Cloud-basierte Prozesse Einzug in die Produktionshalle und revolutionieren das Prozess-Management. Künstliche Intelligenz erleichtert die Arbeit in Kliniken und Pflegeheimen. Der klassische „Nine to five“-Arbeitstag im Büro gehört der Vergangenheit an. Das bestmögliche Ergebnis stammt nicht mehr von der Führungskraft, sondern entsteht in einem Gremium von Fachleuten aus allen Bereichen. Grundlage für diese Entwicklungen ist ein multidirektionaler Kommunikationskanal, der es allen Beteiligten ermöglicht, sich zu vernetzen, zu informieren und Gehör zu verschaffen. Letztlich ist Zusammenarbeit der Schlüssel zu einer wettbewerbsfähigen Organisation, die agil, flexibel und effizient auf Bekanntes und Unvorhersehbares gleichermaßen reagieren kann. Benedikt Ilg/wg

Benedikt Ilg ist CEO und Mitgründer von Flip.

Marktübersicht Desktop as a Service

Hersteller/Anbieter	Web
Affinis & PTS	affinis.de
Also	also.com
Amazon Web Services	aws.amazon.com
Apps4rent	apps4rent.com
Bechtle	bechtle.com
Blue Consult	blue-consult.de
Cameyo	cameyo.com
Cancom Pironet	cancom-pironet.de
Citrix	citrix.com
Cloudshift	cloudshift.de
FastDesk	ukfast.co.uk
German Edge Cloud	gec.io
Google	cloud.google.com
Hornung Consulting	it-business-suite.com
Hosting Base	hosting-base.com
HPE	hpe.com
IBM	ibm.com

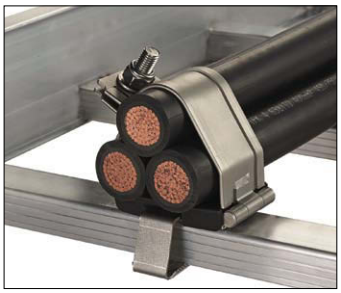
Hersteller/Anbieter	Web
INS	ins-online.net
Kivito	deskmate.cloud
Leostream	leostream.com
Login Consultants	loginconsultants.de
Medialine	medialine.com
Microsoft	azure.microsoft.com
NetPlans	netplans.de
Netzbest	desktop-as-a-service.de
NTT	ntt.com
Nutanix	nutanix.com
Q.beyond	qbeyond.de
SoftwareOne	softwareone.com
Squild	squild.de
Telekom	open-telecom-cloud.com
V2 Cloud	v2cloud.com
VMware	vmware.com
Workspot	workspot.com

Kurzschlussfest nach neuer Norm mit konfigurierbaren Kabelschellen

Kabelschellen von Panduit für mehr Sicherheit und Ausfallschutz

Strom führende Kabel lassen sich in Anlagen, Produktion, Gebäuden oder Rechenzentren auf unterschiedliche Arten verlegen und sichern. Als strukturmechanische Lösung sollen die neuen Kabelschellen von Panduit bei Kurzschlüssen schützen und so die Anlagensicherheit maßgeblich erhöhen. Bei der Entwicklung der Panduit Kabelschellen spielt die IEC-Norm 61914:2015 eine besondere Rolle. Der Standard mit dem Zusatz „2015“ bildet die aktuelle, umfassendste und weltweit anerkannte Anforderung zum Testen von Kabelschellen. Panduit erfülle als erster diese hohen Vorgaben, wie der Hersteller angibt, sodass die Kabelschellen im Kurzschlussfall auch enormen mechanischen Kräften sicher standhalten. Im Detail: Die größte Belastung bei Kurzschlüssen tritt bis zu 0,006 Sekunden vor dem Auslösen von Leistungsschaltern und anderen Schutzvorrichtungen auf. Die neuen Kabelschellen fixieren Kabelbündel und sorgen dafür, dass Kabel bei einem Kurzschluss weiterhin sicher befestigt und an Ort und Stelle bleiben. Dies schütze das Arbeitsumfeld inklusive der Ausrüstung und der Mitarbeiter und verhindere Ausfallzeiten. Die neuen Kabelschellen von Panduit variieren in Größe, Design und Materialien und eignen sich für unterschiedliche Applikationen in prozesstechnischen Anlagen, in der Informationstechnik oder der industriellen Fertigung, so der Hersteller weiter.

An Werkstoffen stehen zur Auswahl: Aluminium, Kunststoff sowie der sehr korrosionsbeständige, dual zertifizierte Edelstahl 316/316L. Die Edelstahl-Kabelschellen haben gefalzte Kanten, damit sie die Kabel schützen. Für die Nutzung der Edelstahl-Kabelbinder gibt es eine Kunststoffschnalle sowie außerdem verschiedene Befestigungshalter. Als Beispiel erhält man die Edelstahl-Kabelbinder-Varianten für Kabeldurchmesser von zwölf bis 86 mm in Breiten von 12,7 bis 19,1 mm für Kurzschlussströme von 45 bis 188 kA. Um die kosteneffizienteste Lösung für die jeweilige Anwendung zu konfigurieren, unterstützt ein hauseigenes Simulationsprogramm per App oder Internetanwendung. Zudem gibt es professionelle Werkzeuge für die fachgerechte und schnelle Installation. jos



Die Kabelschellen von Panduit sollen für mehr Sicherheit und Ausfallschutz sorgen. Bild: Panduit

Deutschland beim Wissen zu Online-Privatsphäre und -Datenschutz vorn

Bisweilen widersprüchlich: Online-Sicherheit in Theorie und Praxis

In einem international durchgeführten Test fragte NordVPN nach Fähigkeiten, Kenntnissen und Gewohnheiten, die die Menschen online an den Tag legen. Das Ergebnis zeigt, dass die Befragten aus Deutschland auf diesem Gebiet offenbar die Nase vorn haben, was die Kenntnisse im Bereich Online-Datenschutz betrifft. Sie erreichten 71,2 von 100 Punkten. Dies sind sechs Punkte mehr als der Rest der Befragten in 192 Ländern. Leider werde das Wissen nicht im ausreichenden Maße angewendet, um die eigene Privatsphäre online tatsächlich zu schützen, so NordVPN weiter. Teilnehmer aus Deutschland haben in den meisten getesteten Bereichen herausragende Ergebnisse erzielt. Bei den Grundlagen des Online-Datenschutzwissens erzielten die Deutschen 78,0 von 100 Punkten. Anscheinend wissen die Menschen in Deutschland sehr gut, dass ein sicheres Passwort eher so aussieht kgZ{J.P0WO#r als so QwertY1234. 6,5 Prozent von ihnen gaben dennoch an, dass sie immer noch schwache Passwörter wählen. Des Weiteren sind 82,4 Prozent darüber im Bilde, dass dasselbe Passwort nicht für mehrere Konten verwendet werden sollte. Außerdem wissen sie, wie sich Malware verbreitet und welche Informationen Internetdienstanbieter aufzeichnen. Auch die Testfrage, wie sie sich in Situationen verhalten würden, die mit digitalen Risiken verbunden sind, haben die Befragten in Deutschland mit einer beeindruckenden Leistung von 90,2 von 100 Punkten gemeistert. Allerdings fielen die Deutschen bei den digitalen Gewohnheiten zurück und erreichten nur knapp mehr als die Hälfte der möglichen Punkte (53,2 von 100). Am meisten haperte es am Umgang mit den Datenschutzbestimmungen: Ganze 36,4 Prozent akzeptieren diese, ohne sie zu lesen. Lediglich 50,6 Prozent der Teilnehmer konnten Tools nennen, die Online-Privatsphäre gewährleisten können. Obwohl die Mehrheit der Deutschen weiß, wie sie sich online verhalten sollte, werde das Wissen leider nicht im digitalen Alltag ausreichend praktiziert, so Daniel Markuson, Experte für digitalen Datenschutz bei NordVPN. Im Bereich „Digitale Gewohnheiten” schnitten die Deutschen am schlechtesten ab und folgten hier dem globalen Trend. „Es sind die kleinen Dinge, die unsere digitale Hygiene ausmachen: die Verwaltung von App-Einstellungen oder Standortinformationen, die wir in den sozialen Medien teilen“, erklärte Markuson. Dies seien die Schwachstellen, die sich schnell beheben lassen, um die Online-Privatsphäre täglich besser zu schützen. Leider glaubten immer noch viele Menschen, dass das Löschen des Browser-Verlaufs zu mehr Datenschutz im Internet beitrage. Mehr Privatsphäre könnten hingegen das richtige Verhalten und umfassende Cybersicherheits-Tools wie VPNs und Antiviren-Software gewährleisten. jos

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-, Mikrokabel, FTTH Dropkabel, FTTH Komponenten, 19“ Spleißboxen und LWL Wandverteiler, LWL Muffen, LWL Reinigungsgeräte und Zubehör, Kabelgleitmittel, LWL Stecker & Kupplungen, PLC Splitter, FWDM 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 Switche & 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 Tegtmeier
Zeisigweg 31
50829 Köln
Tel.: 0221/938878-0, Fax: 0221/938878-28
E-Mail: info@neftec.de
Homepage: www.neftec.de
Service: Qualitativ hochwertige passive Kupfer- und LWL Komponenten für FTTx- , 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 Heddesheim**
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-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

proemptor ist Ihr Partner für Zubehörlösungen im DataCenter.
Wir sind Spezialist in den Bereichen aktive und passive Steckdosenleisten (PDU‘s) und Netzwerkschränke mit eigenen Produkten.
proemptor bietet innovative Technik für individuelle Lösungen.
Mehr Info‘s finden Sie auf **www.proemptor.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
eMail: 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 Heddesheim**
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 **Verteilsysteme** (Rack-, Tisch-, Boden- & Wandintegration) für **Audio-/Video-/Netzwerk- & Medientechnik.** Zusätzlich Meterware-Kabel, Hybridleitungen, passende Steckverbinder, Konfektionskabel, aktive Komponenten und Zubehör.

MALINOWSKI
GEBÄUDETECHNIK

Wir sind der Elektrohandwerksbetrieb mit Ausrichtung auf die IT-Branche, wir kümmern uns ausschließlich um das passive Netz, keine Switche, 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 Messgerätetechnik. 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 zukunftssichere 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 Netzwerktestequipment, 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 Gerätelogistik, Dokumentation FNT Command, Datenträgervernichtung

dtm. group
IT MANUFAKTUR

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.

MYK
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, unterbrechungsfreie 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 Unterbrechungsfreie Stromversorgung (USV) in allen Leistungsbereichen.
- Vertrieb von Neuanlagen, auch in kundenspezifischen Ausführungen
- Breites Serviceangebot mit eigener Werkstatt.
- Wartungsverträge mit unterschiedlichsten Leistungsumfängen und Reaktionszeiten.
- Montage, Reparaturen, 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 vorführbereit zur Ansicht und Erklärung zur Verfügung.

Wöhrle Stromversorgungssysteme GmbH
Lerchenstraße 34,
71144 Steinenbronn
Tel. 07157/7374-0, Fax: 07157/7374-44
E-Mail: verkauf@woehrle-svs.de
Homepage: www.woehrle-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, CO_2-neutral, Energieeffizienzklasse A+++, Erbebenfrei

Zertifizierungen: ISO 27001, 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 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

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, unterbrechungsfreie 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

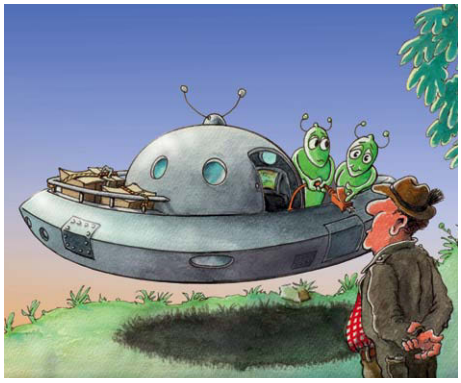
Ein Partner von **SUNBIRD Software** - DCIM Lösungen für ihr RZ
Monitoring von Energie und Sensorik, iPDU und Umgebungsverwaltung.
Berichterstellung für Assets, Strom und Kühlung, Kapazitätsplanung, Kabelmanagement sowie Einbindung bestehender Tools wie z.B. ServiceNow...

Nähere Infos:
Tel: 089 84061799
mail: info@procom-data.de
Homepage: www.procom-data.de

Inserentenverzeichnis

Anzeigenschluss für die Ausgabe 06/2021 ist der 05. 05. 2021

Die Ausgabe 6/2021 erscheint am 26. Mai 2021



Schwerpunkt

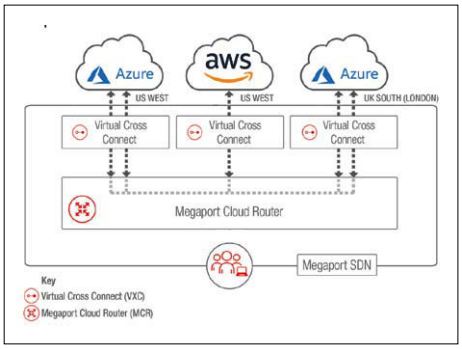
Verkabelung

Die Kabelentwicklung schreitet sowohl im High-Speed-Segment wie bei der einfachen Anschlusstechnik weiter. Die Beiträge greifen daher sowohl den LWL-Bereich wie das Thema SPE auf. Außerdem: Welchen Beitrag kann die Verkabelung zu einem modernen Brandschutzkonzept leisten? Mit Marktübersicht Kategorie-7/7_A/8.1/8.2-Kabel.

Schwerpunkt

Stromversorgung und Klimatisierung im RZ

Auch ein eigenes RZ muss heute in ein übergreifendes Computing-Szenario mit Hybrid-Cloud-, Colocation- oder As-a-Service-Ansätzen einbezogen sein. Was wo am besten passt, müssen Unternehmen meist individuell entscheiden. Mit Marktübersicht USV-Anbieter.



Technik

Cloud vs. Edge Computing

Mittlerweile ist es einfacher denn je, Cloud-Strukturen aufzubauen. Der Vorsprung Cloud-nativer Unternehmen schwindet allerdings, je mehr es von ihnen gibt. In Konkurrenz zu den bisherigen Strukturen steht nun auch das Edge Computing – alternativer Ansatz oder ergänzendes Konzept?

Vorschau auf kommende LANline-Schwerpunkte

Ausgabe 07/2021
erscheint am 24.06.2021

Datacenter-Networking
Mit Marktübersicht Videoüberwachung

KI im IT-Betrieb
Mit Marktübersicht Machine Learning as a Service

Redaktionsschluss 28.04.2021

Ausgabe 08/2021
erscheint am 27.07.2021

Datacenter und Verkabelung
Mit Marktübersicht Steckverbinder Kategorie $7/7_A$/8.1/8.2

Mit Marktübersicht RZ-Bau, General-Unter/Übernehmer

Redaktionsschluss 28.05.2021

Ausgabe 09/2021
erscheint am 26.08.2021

Hybrid-Cloud-Vernetzung
Mit Marktübersicht SD-WAN-Lösungen

Backup und Archivierung
Mit Marktübersicht Backup-Lösungen

Redaktionsschluss 23.06.2021

LANline
IT ▪ Network ▪ Datacenter

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 Schröper (jos)
Redaktion: Anna Molder (am)
Autoren dieser Ausgabe: Frank Engelhardt, Dr. Wilhelm Greiner (wg), Patrick Hirscher, Benedikt Ilg, Wolfgang Kaufmann, Christoph Lange, Jake McCabe, Carsten Mickeleit, Rick Peters, Elisabeth Schloten, Florian Schönknecht, Jörg Schulz, Markus Senbert, Dirk Wettig, Jan Willeke
Layout: JournalMedia GmbH, 85540 München-Haar
Titelbild: Wolfgang Traub

MEDIABERATUNG

Verlagsrepräsentantin: Cornelia Truchseß-Jacobi,
Tel. +49 170 3372234 oder +49 89 71940003,
E-Mail: truchsess-jacobi@ctj-media.de,
cornelia.truchsess@lanline.de
Verantwortl. 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 Gründen oder höherer Gewalt entsteht kein Anspruch auf Ersatz.

ALLE AUSGABEN JETZT AUCH ALS **E-PAPER** LESEN!


NCP
SECURE COMMUNICATIONS
Auffallend flexibel
Richten Sie Ihr Unternehmen jetzt produktiv und sicher für die Zukunft aus!
Ermöglichen Sie Homeoffice und mobiles Arbeiten – mit skalierbaren VPN-Lösungen und Lizenzmodellen für jeden Bedarf.
Wie flexibel sind Sie?
www.ncp-e.com
NCP
my access
SecurITy
made in Germany