business.technology.strategy

9. Dezember 2022
€ 12,00
12
22

funkschau

CYBERSECURITY
Kein Weg vorbei an ganzheitlichen Konzepten

BREITBAND
Die tragende Rolle des Glasfaserausbaus

DIGITAL WORKPLACE
Wann Cloud-Lösungen sinnvoll sind – und wann nicht

SOFTWAREENTWICKLUNG
Agile-Ansätze mit Low-Code optimieren

RUNDUM ABGESICHERT

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

STEFAN ADELMANN,
Chefredakteur funkschau
sadelmann@weka-fachmedien.de

CYBERSECURITY MUSS CHEFSACHE SEIN

Die Zeiten der klassischen Perimeter-basierten IT-Sicherheit sind vorbei, unvorsichtige Mitarbeitende stellen die größte Schwachstelle dar, hundertprozentige Sicherheit gibt es nicht – es sind Leitsätze wie diese, die Cybersecurity-Anbieter und -Spezialisten mit stoischer Disziplin seit Jahren wie Mantras wiederholen. Das ist auch notwendig. So lange, bis aus der Sicherheitstheorie in allen Unternehmen und ihren Abteilungen tatsächlich gelebte Praxis wird. Denn nach wie vor gilt es, zahlreiche (teils klaffende) Lücken im Sicherheitswall zu schließen – auch wenn das Bewusstsein für Cyberrisiken und für notwendige Maßnahmen glücklicherweise stetig steigt. Immerhin will die Hälfte der Befragten einer IDC-Studie weiter in Cyberbereitschaft und -verteidigung investieren – vor allem auch aufgrund der angespannten geopolitischen Lage. Doch Unternehmen stehen dabei vor gewaltigen Herausforderungen. Ob zunehmende Komplexität, fehlende Fachkräfte oder neue Anforderungen im Zuge von hybriden Arbeitsumgebungen: die Liste der potenziellen Hürden auf dem Weg zu mehr IT-Sicherheit ist lang.

Umso wichtiger ist es im Wettlauf gegen die Cyberkriminellen, dass das Thema Cybersecurity einerseits ganz oben an der Unternehmensspitze ankommt, und dass die verschiedenen Stakeholder andererseits gemeinsam daran arbeiten, die technische Komplexität zu reduzieren und Know-how auf breiter Fläche aufzubauen – bis aus der Theorie in jeder Branche Praxis wird. Wichtige IT-Sicherheits-Ansätze und -Impulse für diese Aufgabe finden Sie auch in dieser Ausgabe ab Seite 25.

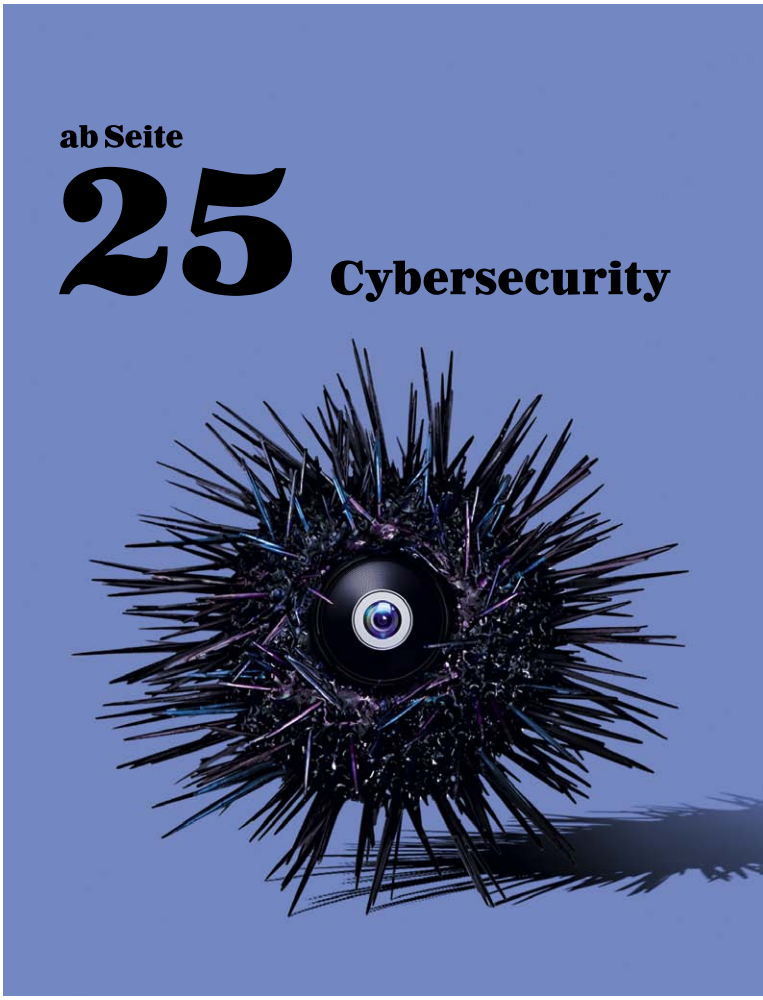
Zudem wünscht Ihnen das gesamte funkschau-Team zum Jahresende erholsame Tage und anschließend einen guten, gesunden Start in das neue Jahr 2023. Und ich möchte diese Ausgabe darüber hinaus gerne nutzen, um mich von Ihnen, liebe Leserinnen, liebe Leser, zu verabschieden. Nach sieben aufregenden, spannenden und aufschlussreichen Jahren als Chefredakteur werde ich die inhaltliche Verantwortung der Medienmarke funkschau ab Januar in die erfahrenen Hände von Dirk Waasen legen. Ich bedanke mich bei Ihnen für Ihr großes Interesse, Ihr Vertrauen und für zahlreiche Gespräche, die stets maßgeblich dazu beigetragen haben, unsere thematischen Schwerpunkte zu definieren.

Ihr

inhalt

funkschau 12/2022

Titelbild: Norbert Preiß, funkschau



NETZWERKE

DIGITAL WORKPLACE

CYBERSECURITY

ab Seite
12
Digital Workplace

DATACENTER

32
Stromversorgung

MARKT & TRENDS

STANDARDS

UWE RICHTER WIRD NEUER CEO BEI DIGITALL

➤ Uwe Richter (rechts im Bild) übernimmt zum 1. Dezember den Posten des CEO beim Technologie- und Beratungsunternehmen Digitall. Damit wird er Nachfolger von Ivaylo Slavov, der in das Advisory Board Digitalls einzieht. Dieser Schritt sei das Ergebnis eines strukturierten, mehrmonatigen Nachfolgeplanungsprozesses, mit dem die Führungsspitze von Digitall um Ivaylo Slavov sowie das Advisory Board die Weichen für eine weiterhin erfolgreiche Zukunft des Unternehmens stellen.

Uwe Richter war zuletzt knapp fünf Jahre lang als CEO bei der STP Informationstechnologie tätig, die Legal-tec-Softwareprodukte und -Dienstleistungen bereitstellt. In dieser Position hat er die Transformation hin zu einem SaaS-Unternehmen vorangetrieben. Zuvor hat Uwe Richter als CEO der Eurodata Unternehmensgruppe, die cloudbasierte Softwarelösungen und IT-Services entwickelt und betreibt, maßgeblich die strategische Neuausrichtung aufgesetzt. *(LS)*

Bild: Digitall

UWE RICHTER

wird ab dem 1. Dezember 2022 als CEO an der Spitze des Technologie- und Beratungsunternehmens Digitall stehen. Damit folgt er auf Ivaylo Slavov (links im Bild), der künftig im Advisory Board des Unternehmens tätig sein wird. „Ich freue mich sehr, meinen Erfahrungsschatz bei Digitall einbringen zu können, um den weiteren strategischen Ausbau der Gruppe mitzugestalten. Hierbei ist es mir besonders wichtig, dass wir unsere Kunden mit intelligenten Lösungsansätzen bestmöglich auf ihrem Weg der Digitalisierung unterstützen", sagt Richter.

KOMMERZIALISIERUNG DER CYBERKRIMINALITÄT

➤ Sophos hat den „Threat Report 2023" veröffentlicht, der unter anderem einen neuen Grad der Kommerzialisierung innerhalb der Cyberkriminalität beschreibt: Fast alle Szenarien sind käuflich. Ein boomender Cybercrime-as-a-Service-Markt stehe einer kriminellen Käuferschaft offen, die von technisch hoch versiert bis völlig unwissend reicht. Kriminelle Untergrundmarktplätze wie Genesis ermöglichen demnach seit Langem den Kauf von Malware und Malware-Implementierungsdiensten („Malware-as-a-Service") sowie den Verkauf gestohlener Zugangsdaten und anderer Daten in großen Mengen. In den letzten zehn Jahren hat sich mit der zunehmenden Beliebtheit von Ransomware eine „Ransomware-as-a-Service"-Wirtschaft herausgebildet. Cyberkriminelle haben sich laut dem Report ein Beispiel am Erfolg dieser Infrastruktur genommen und ziehen nach. Jetzt, im Jahr 2022, hat sich das „As-a-Service"-Modell daher massiv ausgeweitet, und fast jeder Aspekt der Cyberkriminalität – von der Erstinfektion bis hin zu Möglichkeiten, die Entdeckung zu vermeiden – sei käuflich zu erwerben. Zudem arbeiten auch cyberkriminelle Marktplätze laut Sophos immer mehr wie normale Unternehmen. Einige Marktplätze hätten eigene Seiten für Stellengesuche und die Rekrutierung von Mitarbeitenden eingerichtet, wo die Arbeitssuchenden ihre Fähigkeiten und Qualifikationen in Kurzform angeben. Die sich entwickelnde Ökonomie des Untergrunds hat laut Sophos zudem die Nachfrage nach gestohlenen Zugangsdaten erhöht. Mit der Ausweitung von Webdiensten könnten verschiedene Arten von Anmeldeinformationen, insbesondere Cookies, genutzt werden, um in Netzwerken tiefer Fuß zu fassen und sogar Multifaktorauthentifizierung zu umgehen. Der Diebstahl von Anmeldedaten sei auch eine der einfachsten Möglichkeiten für Kriminelle, Zugang zu Untergrundmärkten zu erhalten und ihre „Karriere" zu beginnen. *(DK)*

137.000 IT-FACHKRÄFTE FEHLEN IN DEUTSCHLAND

➤ Der Mangel an IT-Fachkräften hat sich verschärft – trotz der schwierigen konjunkturellen Lage, weiterer Krisen und der Verwerfungen, die von dem russischen Angriffskrieg in der Ukraine ausgehen. Derzeit fehlen in Deutschlands Unternehmen 137.000 IT-ExpertInnen quer durch alle Branchen. Damit liegt die Zahl sogar über dem Vor-Corona-Jahr 2019 mit 124.000 unbesetzten Stellen. Das sind Ergebnisse der neuen Bitkom-Studie zum Arbeitsmarkt für IT-Fachkräfte. Bitkom-Präsident Achim Berg: „Der demographische Wandel führt dazu, dass signifikant weniger junge Menschen mit IT-Qualifikationen auf den Arbeitsmarkt kommen und zugleich scheiden mehr Ältere aus einschlägigen Berufen aus. Der Fachkräftemangel entwickelt sich zum Haupthindernis bei der Digitalen Transformation." Im Durchschnitt bleibt eine offene Stelle für IT-Fachkräfte inzwischen 7,1 Monate unbesetzt. Die Unternehmen verlassen sich dabei nicht nur auf Stellenausschreibungen und Initiativbewerbungen, sondern versuchen auf einer Vielzahl an Kanälen MitarbeiterInnen zu gewinnen. Gleichzeitig versuchen sie, die erste Bewerbung für Interessierte so einfach wie möglich zu gestalten: 39 Prozent setzen inzwischen auf Online-Bewerbungs-Tools, 16 Prozent ermöglichen eine Bewerbung mit einem Klick aus einem Business-Netzwerk heraus und 13 Prozent nutzen eine Bewerbungs-App. Bei praktisch allen Unternehmen kann man sich zudem per E-Mail bewerben, aber auch die klassische Bewerbungsmappe auf Papier wird meist akzeptiert. Jeweils rund drei Viertel nutzen zudem teilweise Videokonferenzen für Bewerbungsgespräche und bauen einen Bewerbungspool auf, um daraus künftig freiwerdende Stellen besetzen zu können. „Die Unternehmen bespielen beim Recruiting die komplette Klaviatur. Das hilft natürlich im Einzelfall, den gesamtgesellschaftlichen Fachkräftemangel löst es nicht", so Berg. *(DK)*

EINE ANWENDUNG STATT VIELE

DIE APP-FLUT BEWÄLTIGEN DURCH UCCAAS

➤ Kommunikation soll einfach, klar und zielführend sein. Was im beruflichen wie auch privaten Umfeld logisch erscheint, wird in Zeiten der Digitalisierung immer schwieriger. Die digitale Transformation schreitet stetig voran und bringt eine Vielzahl an möglichen Anwendungen mit sich, die Kommunikation und Zusammenarbeit über Distanzen eigentlich erleichtern sollen. Tatsächlich scheint die Flut von Apps aber eher das Gegenteil zu bewirken. Bereits 2019 zeigte eine Umfrage von RingCentral, dass die Zusammenarbeit von Teams aufgrund von zahlreichen, verschiedenen Collaboration-Apps eher erschwert wird. 69 Prozent der befragten Mitarbeiter:innen vergeudeten laut Umfrage pro Tag bis zu einer Stunde damit, zwischen 47 und 62 SaaS-Anwendungen zu nutzen. Und nicht nur die Zeit war ein Faktor, der negativ auffiel. Auch Wartung und Betreuung der Anwendungen kosteten Unternehmen mehrere Hunderttausend Euro pro Jahr.

Statt auf eine App pro Kommunikationskanal oder verschiedene Anwendungen je nach Ansprechpartner zu setzen, sollten Unternehmen sich auf einen einzigen Anbieter für die Kommunikation verlassen.

2019 vs. 2022

In den letzten drei Jahren hat sich die Situation noch nicht verbessert. Die Digitalisierung zeigte eine schnelle Entwicklung und mit ihr stieg auch die Anzahl der Anbieter und Lösungen. Remote-Arbeitsplätze und hybride Arbeitsplatzmodelle sind mehr und mehr auf dem Vormarsch. Kommunikation und Kollaboration geschehen oftmals über Distanzen und über viele verschiedene Kommunikationskanäle hinweg.

Statt Vereinfachung ist Überforderung und Überlastung die Folge zahlreicher verschiedener Anwendungen. Nicht mehr mit einem Klick kommunizieren, sondern zwischen verschiedenen Apps wechseln, sich immer wieder neu anmelden, Daten suchen und, und, und… Diese Unterbrechungen dauern im Schnitt 23 Minuten, ehe wieder wirklich produktives Arbeiten möglich ist.

Wie ist es Unternehmen und Mitarbeiter:innen in Zeiten von Remote Work und hybriden Arbeitsmodellen also möglich, die tatsächlichen Vorteile einer einheitlichen, flexiblen und einfachen Kommunikation und Kollaboration zu realisieren?

UCCaaS als Retter in der Not?

Helfen kann tatsächlich nur eines: Statt auf eine App pro Kommunikationskanal oder verschiedene Anwendungen je nach Ansprechpartner zu setzen, sollten Unternehmen sich auf einen einzigen Anbieter für die Kommunikation verlassen. Ziel ist es, eine Lösung zu finden, die alle Kommunikationskanäle anbietet, die Zusammenarbeit vereinfacht, die Integration verschiedener Anwendungen ermöglicht und Mitarbeiter:innen wie auch Kunden „glücklich“ macht. Dies können CIOs und IT-Teams mit einer Unified Communications und Collaboration as a Service (UCCaaS)-Plattform erreichen, bei der nur ein Vertrag zu verwalten ist, einmal Kosten anfallen und nur eine Lösung zu implementieren ist.

Die Cloud-Lösung bietet auch für Anwender:innen deutliche Vorteile. Sie melden sich mit Single Sign-on (SSO) – also einer einmaligen Anmeldung, die für alle Apps gilt – an, um auf alle Anwendungen und Kommunikationskanäle zuzugreifen. Ein Wechsel zwischen verschiedenen Apps unterschiedlicher Anbieter ist nicht mehr notwendig. Dem Ursprungsgedanken von Unified Communications folgend ist die gesamte professionelle Kommunikation auf einer einzigen Oberfläche zusammengefasst.

Das bedeutet nicht, dass Mitarbeitende auf viele der täglich genutzten Anwendungen wie Google, Workspace, Salesforce oder DocuSign verzichten müssen. Anbieter wie RingCentral setzen bei ihren UCaaS-Lösungen auf die Integration gängiger Apps. Dabei wird das Nutzererlebnis vereinfacht und der Wechsel zwischen verschiedenen Anwendungen minimiert. Dies gelingt zum Beispiel durch den Erhalt von Benachrichtigungen in der RingCentral App, sobald eine Google Doc-Datei aktualisiert wird.

Moderne UCaaS-Lösungen bieten darüber hinaus weitere Features, die den Arbeitsalltag erleichtern und die Produktivität über die 23 gewonnenen Minuten hinaus steigern. Durch den Einsatz von KI können beispielsweise Meeting-Zusammenfassungen und Übersetzungen mit einem Klick erstellt werden, Arbeitsabläufe werden automatisiert und der Kontakt zum Kunden vereinfacht.

Statt Produktivität und Motivation in einer Flut von Apps untergehen zu lassen, sollten sich Unternehmen darauf besinnen, eine Lösung zu suchen, die Kommunikation und Kollaboration wirklich vereinheitlicht und damit langfristig Motivation, Produktivität und Erfolg sichert.

www.ringcentral.com/de/de

RingCentral

„DIE ZUKUNFT IST DIGITAL“

Bild: 1&1 Versatel

„Glasfaser ist die einzige Übertragungstechnologie, die den zunehmenden Bedarf durch Internet of Things (IoT), Cloud-Dienste oder eine hohe Anzahl von mobilen Endgeräten langfristig abdecken kann.“

SÖREN TREBST

verfügt über langjährige Erfahrungen in der Telekommunikationsbranche. Seit April 2020 ist er CEO von 1&1 Versatel, einem Düsseldorfer Telekommunikationsanbieter mit Fokus auf Geschäftskunden. Seit Mitte 2014 ist der Provider ein Tochterunternehmen von United Internet.

Deutschland wird zum Breitbandland, so der erklärte Wunsch der Politik. Demnach sollen bis 2030 alle Haushalte und Unternehmen über einen Glasfaseranschluss verfügen können. Damit das aber nicht nur als theoretisches Ziel auf dem Papier steht, sondern tatsächlich bei Privat- wie Business-Unternehmen ankommen kann, bedarf es weiterer Schritte. Ein Interview mit Sören Trebst von 1&1 Versatel.

Interview: Diana Künstler

➤ ***funkschau:*** *Wo liegen für 1&1 Versatel die Herausforderungen bei der Umsetzung der ambitionierten Breitbandziele?*

Sören Trebst: Als Telekommunikationsunternehmen tragen wir eine besondere Verantwortung, die Digitalisierung unseres Landes voranzutreiben. Wir setzen uns daher bereits seit vielen Jahren mit Nachdruck und auf eigenwirtschaftlicher Basis für die Gigabit-Erschließung von Unternehmen, öffentlichen Einrichtungen und Kommunen ein. Ein flächendeckendes Glasfasernetz ist jedoch nur mit vereinten Kräften möglich. Das gilt auch für den Aufbau des neuen 5G-Mobilfunknetzes unserer Schwestergesellschaft 1&1, bei dem wir als Infrastrukturdienstleister zentrale Aufgaben übernehmen. Um den aktuellen Glasfaser-Flickenteppich in unserem Land in ein flächendeckendes Gigabit-Netz zu verwandeln, braucht es aber auch politische Rahmenbedingungen und gezielte Partnerschaften.

funkschau: *Inwiefern kann die Politik hier noch mehr unterstützen?*

Trebst: Es ist ein enger Schulterschluss von Politik und Netzbetreibern gefragt. Mit dem Glasfaserpakt in Hessen wurde im Mai 2022 ein wichtiger Grundstein gelegt – insbesondere der von der Landesregierung unterstützte Bürokratieabbau und die Beschleunigung der Genehmigungsverfahren werden der Umsetzung der Ausbauziele auch in Zukunft zugutekommen. Darüber hinaus liegt uns ein Punkt sehr am Herzen: Gigabitnetzausbau und Gigabitnetzauslastung gehören zusammen. Daher müssen auch Kooperationen, Open-Access-Plattformen und andere Formen der Zusammenarbeit gestärkt und gefördert werden – auch, um bereits vorhandene Netze optimal auszulasten und möglichst vielen Nutzerinnen und Nutzern Zugang zu leistungsfähigem Internet zu ermöglichen.

funkschau: *Zahlreiche Akteure – sei es aus Politik oder der TK-Branche – treiben den Glasfaserausbau voran. Wie wichtig ist es vor diesem Hintergrund, gezielte Partnerschaften einzugehen?*

Trebst: Ich bin fest davon überzeugt, dass wir gemeinsam schneller vorankommen. Bei der Etablierung einer deutschen Glasfaserinfrastruktur bedeuten Partnerschaften und gebündelte Verantwortlichkeiten eine deutliche Beschleunigung von Ausbauvorhaben. Gezielte Kooperationen sind ein zentraler Hebel, damit Deutschland zum Breit-

bandland wird. Mit vitronet haben wir im Juni 2022 zum Beispiel einen sehr erfahrenen Partner in der Abwicklung von Erschließungsprojekten gewonnen. Neben dieser Partnerschaft sind Synergien im Tiefbau oder auch beim Vertrieb essenziell. Nur wenn wir vernetzt denken und Hand in Hand zusammenarbeiten, werden wir erfolgreich sein.

funkschau: *Es gibt Marktbegleiter, die in der verstärkten Akzeptanz alternativer Aufrüstungsmethoden – Stichwort Vectoring – die Chance sehen, den Netzausbau zu beschleunigen. Wie sehen Sie das?*

Trebst: Schon in naher Zukunft wird ein Großteil der deutschen Haushalte und Unternehmen Bandbreitenbedarfe haben, die mit herkömmlichen Kupferleitungen nicht mehr gedeckt werden können. Die Zukunft ist digital und Glasfaser ist die einzige Übertragungstechnologie, die den zunehmenden Bedarf durch das Internet of Things (IoT), Cloud-Dienste oder eine hohe Anzahl von mobilen Endgerätenden langfristig abdecken kann. Gesellschaft und Wirtschaft benötigen daher flächendeckend leistungsfähige Glasfasernetze bis ins Gebäude. Aus diesem Grund liegt unser Fokus bei 1&1 Versatel auf dem Glasfaserausbau. Aber natürlich umfasst unser Lösungsspektrum auch andere Übertragungstechnologien, die wir begleitend und in der Übergangszeit berücksichtigen. So können im Rahmen von Redundanzkonzepten auch VDSL-Vectoring und damit Kupferleitungen zum Einsatz kommen. Unser Hauptziel ist und bleibt es jedoch, unseren Kundinnen und Kunden die schnellste, stabilste und zukunftsfähigste Anbindung zur Verfügung zu stellen. Und das ist ganz klar Glasfaser.

funkschau: *Welche Leistungen kann 1&1 Versatel auf Basis des Glasfasernetzes speziell für Businesskunden bereitstellen?*

Trebst: Glasfaseranschlüsse ermöglichen Internet-Geschwindigkeiten von bis zu 100 GBit/s und lassen damit andere Übertragungstechnologien im direkten Geschwindigkeitsvergleich weit hinter sich. Kupferleitungen (also DSL und Vectoring) schaffen höchstens 250 MBit/s und bei den Koaxialnetzen der TV-Kabelanbieter ist im Download bei maximal 1 GBit/s Schluss, im Upload sogar schon bei 50 MBit/s. Damit ist Glasfaser die einzige Übertragungstechnologie, die den steigenden Bandbreitenbedarf auch langfristig abdecken kann. Manche Anwendungen, wie das Internet of Things (IoT) oder KI-basierte Services, werden durch die hohen Bandbreiten von Glasfaseranschlüssen überhaupt erst möglich. Und auch da, wo es heute noch keinen akuten Bedarf an höheren Bandbreiten gibt, kann es in Zukunft Geräte oder Dienste geben, die auf eine Übertragungstechnologie in Gigabit-Geschwindigkeit angewiesen sind, zum Beispiel sichere Zahlungssysteme, digitalisierte Lieferdienste oder Virtual-Reality-Anwendungen.

Immer wichtiger wird außerdem die symmetrische Anbindung – also die gleiche Geschwindigkeit im Up- und Download. Während beim einfachen Internetsurfen DSL- oder TV-Kabelanschlüsse mit wesentlich geringerer Upstreamleistung ausreichen, benötigen relevante Geschäftsanwendungen wie Cloud-Applikationen oder Videokonferenzen symmetrische Bandbreiten, die nur echte Glasfaseranschlüsse bieten. Allerdings verpufft der Geschwindigkeitsvorteil wieder, wenn auf der letzten Meile Kupfer zum Einsatz kommt. Daher sind alle von uns reali-

sierten Glasfaseranschlüsse FTTH – gehen also direkt bis ins Gebäude. Diese FTTH-Glasfaseranschlüsse für Geschäftskunden sind die Kernleistung unseres Geschäfts.

Darüber hinaus sind wir Lösungsanbieter für alle Anforderungen der modernen Telekommunikation unserer Gigabit-Gesellschaft. Wir bieten individuelle Lösungen im Bereich Vernetzung und IT-Services an. Mit intelligenten Standortvernetzungen binden wir Mitarbeitende, Firmenstandorte und Rechenzentren effizient in Firmennetzwerke ein. Unsere starken IT-Security-Lösungen schützen Unternehmen vor Cyberangriffen, Viren und Fremdzugriffen auf ihre Netzwerke – ein Thema, dem eine immer größer werdende Bedeutung zukommt.

funkschau: *Während Unternehmen relativ schnell digital nachrüsten können, haben die letzten zwei Jahre die Erkenntnis gebracht, dass sich deutsche Schulen und Behörden schwerer tun. Wo sehen Sie die Gründe hierfür? Und wie lässt sich gegebenenfalls gegensteuern?*

Trebst: Schulen und Behörden im ganzen Land stehen vor der Herausforderung, ihre Angebote und Verwaltungen zu digitalisieren, denn aktuell erfüllen sie oft die hierfür notwenigen technischen Voraussetzungen nicht. Damit der Sprung ins digitale Zeitalter gelingt, ist schnelles Handeln aller verantwortlichen Akteure gefragt. Es wird eine leistungsfähige Telekommunikationsinfrastruktur gebraucht, wo möglich auf Basis von Glasfaser. Spätestens seit Beginn der Corona-Pandemie haben digitale Lehr- und Lernmethoden an Schulen in ganz Deutschland Einzug gehalten. Dennoch reichen die zur Verfügung stehenden Bandbreiten häufig nicht aus.

1&1 Versatel hat im Bildungsbereich bereits zahlreiche Digitalisierungsprojekte realisiert. So haben wir zwischen 2017 und 2020 über 600 Schulen in ganz Schleswig-Holstein ans Glasfasernetz gebracht. Ein besonders gelungenes Beispiel ist zudem die Rundumlösung für den Dansk Skoleforening for Sydslesvig e.V., der in Schleswig-Holstein zahlreiche Schulen und Kindergärten betreibt: Die Kindergärten werden mit Bandbreiten von je 100 MBit/s und die Schulen mit je 1 GBit/s ans Internet angebunden. Über eine SD-WAN-Standortvernetzung können Lehrkräfte zudem ortsunabhängig auf alle zentralen Dienste und Anwendungen im Vereins-Rechenzentrum wie etwa Telefonie-Server oder Drucker zugreifen. Eine ebenfalls integrierte Sicherheitslösung steuert und überwacht den gesamten Internetverkehr des Vereins, von der Abwehr von Cyber-Attacken bis hin zur Sperrung bestimmter Websites unter Jugendschutzgesichtspunkten. Bis Ende 2024 werden wir außerdem mehr als 550 Berliner Schulen mit Glasfaser ausstatten. In Schleswig-Holstein und Berlin funktionieren die Digitalisierungsprojekte so gut, weil die Bundesländer sich der Verantwortlichkeit der Digitalisierung angenommen und die Glasfaserversorgung der Schulen damit zur Landesaufgabe gemacht haben. Die beiden Länder stellen allen Schulen ein einheitliches Budget für Glasfaseranschlüsse zur Verfügung.

„Spätestens seit Beginn der Corona-Pandemie haben digitale Lehr- und Lernmethoden an Schulen in ganz Deutschland Einzug gehalten. Dennoch reichen die zur Verfügung stehenden Bandbreiten häufig nicht aus. [...] Es bedarf zentraler Projekte, in denen Bildungseinrichtungen Hand in Hand mit Kommunen und Telekommunikationsanbietern Lösungen entwickeln und konsequent umsetzen.“

Damit Deutschland auch in Zukunft in der oberen Bildungsliga mitspielen kann, müssen alle verantwortlichen Akteurinnen und Akteure in Bund und Ländern jetzt reagieren, die Digitalisierung forcieren und die Schulen nicht sich selbst überlassen. Es bedarf zentraler Projekte in denen Bildungseinrichtungen Hand in Hand mit Kommunen und Telekommunikationsanbietern Lösungen entwickeln und konsequent umsetzen.

funkschau: *Inwiefern liefert ein leistungsfähiges Glasfasernetz die Voraussetzung für einen flächendeckenden 5G-Netzausbau?*

Trebst: Autonomes Fahren, Industrie 4.0 und Smart Cities: All das wird mit dem neuen Mobilfunkstandard 5G in Zukunft möglich sein. Doch auch Privatkundinnen und -kunden profitieren vom 5G-Netz. Durch die hohen Kapazitäten können sie bei Festival- oder Stadionbesuchen ihre Eindrücke ohne Probleme und gleichzeitig auf Social Media hochladen, parallel Videos streamen und in Gigabit-Geschwindigkeit surfen. Mit Spitzendatenraten von bis zu 20 GBit/s überträgt die neue Technik große Datenmengen quasi in Echtzeit.

Der erfolgreiche Glasfaserausbau bildet die Basis für die fünfte Mobilfunkgeneration, die technisch einige Herausforderungen mit sich bringt. So beträgt die Reichweite der Highspeed-Sendemasten nur wenige Hundert Meter. Für eine Flächenabdeckung ist daher eine hohe Anzahl an Sendeanlagen notwendig, die wiederum über Rechenzentren als übergeordnete Netzknoten miteinander verbunden werden müssen. Für den schnellen Datentransport ist die Anbindung der Mobilfunkanlagen an die Netzknoten entscheidend. Die technisch einzig sinnvolle Option, um die Potenziale von 5G langfristig voll auszuschöpfen, ist Glasfaser.

funkschau: *Welche Aufgaben übernimmt 1&1 Versatel beim Aufbau des 5G-Netzes hierzulande und in Europa?*

Trebst: Das neue Mobilfunknetz unserer Schwestergesellschaft 1&1 wird das europaweit erste vollständig virtualisierte 5G-Netz auf Basis der neuen Open-Ran-Technologie sein. Als Infrastrukturdienstleister der United Internet Gruppe übernehmen wir dabei zwei zentrale Aufgaben: Zum einen stellt 1&1 Versatel den Backbone zur Verfügung und übernimmt den Aufbau und Betrieb des deutschen Transportnetzes. Zum anderen stellen wir die Rechenzentrumsinfrastruktur für das 1&1-Mobilfunknetz bereit. An das Kernnetz werden dezentrale Rechenzentren in ganz Deutschland angeschlossen, die wiederum per Glasfaser mit Tausenden 1&1-Antennenstandorten verbunden werden. Diese Architektur ermöglicht extrem kurze Übertragungswege, die für Echtzeitanwendungen unabdingbar sind. Denn nur Glasfaserkabel ermöglichen die Übertragungen zwischen Mobilfunkantennen und Rechenzenten mit der geforderten hohen Datenrate. Sie sind zudem deutlich weniger störanfällig und bieten so die nötige Stabilität, um auch kritische Industrieprozesse zuverlässig abzubilden.

easybell

PARTNERPROGRAMM

Jetzt easybell-Partner werden und profitieren!

Professionelle Telekommunikation für Ihre Kunden

Bis zu 20 Prozent Lifetime-Provision für Sie

easybell

SIP Trunks | Cloud Telefonanlage | VDSL für Geschäftskunden | Microsoft-Teams-Anbindung

ohne Mindestvertragslaufzeit

www.easybell.de/partner

CLOUD – ODER NICHT?

Die Anforderungen an die Business-Kommunikation haben sich verändert: Unternehmen müssen ihre ITK-Systeme auf die neue Arbeitswelt ausrichten und dabei vor allem eine hohe Flexibilität mit Blick auf den Nutzungskontext sicherstellen. Oft scheint die Cloud die naheliegende Antwort zu sein. Aber welche Vor- oder Nachteile hat Business-Kommunikation aus der Cloud konkret und welche Bereitstellungsform eignet sich für wen?

Bild: nexusby-123rf

Autor: Jörn Lembke

Redaktion: Sabine Narloch

➤ Mobiles Arbeiten, geräteunabhängiger Zugriff, eine hohe Skalierbarkeit: Immer mehr Unternehmen machen von den Vorzügen Gebrauch, die IT-Lösungen aus der Cloud bieten. Auch wenn sich hierzulande die Vorbehalte insbesondere in kleinen und mittleren Unternehmen lange gehalten haben, so kommen immer mehr Entscheider zu der Erkenntnis, dass es angesichts der Anforderungen einer stark veränderten Arbeitswelt inzwischen weniger um ein „ob“ als vielmehr um das „wann“ und „wie“ geht.

Diverse Lockdowns und die damit eingehergehende Homeoffice-Pflicht waren vielerorts ein Boost für Digitalisierungsprojekte auf Cloud-Basis, wie bereits der „Cloud-Monitor 2021“ von Bitkom Research und KPMG zutage förderte. Demnach nutzen etwa vier von fünf deutschen Unternehmen inzwischen Technologien aus der Cloud. Nicht zuletzt Systeme für die Business-Kommunikation werden dabei immer häufiger aus der Wolke bezogen. Doch ist die Cloud tatsächlich alternativlos geworden oder hat auch On-Premises nach wie vor eine Berechtigung? Welche Vor- und Nachteile bieten sich konkret für kleine und mittlere Unternehmen und für welche Zielgruppe ist welche Cloud-PBX-Variante die richtige?

Neue Anforderungen: Die Arbeitswelt wird hybrid

Dass sich die Anforderungen vieler Unternehmen und Organisationen infolge der Pandemie rasant verändert haben, ist kein Geheimnis. Immer mehr hybride Arbeitsplätze werden eingerichtet, um die Zusammenarbeit sowie die Kommunikation in dezentralen Teams zu unterstützen. Das erfordert eine hohe Flexibilität mit Blick auf die eingesetzten Arbeitswerkzeuge. Anwender erwarten heute zudem eine hohe Skalierbarkeit entsprechender Dienste, um schnell auf sich wandelnde Rahmenbedingungen reagieren zu können. In dieser Hinsicht schneiden Cloud-Systeme gut ab. Entsprechende Kommunikationslösungen bieten hierbei insbesondere Aspekte wie:

- Orts- und Geräteunabhängigkeit
- Unterstützung für mobiles Arbeiten
- Zentrale Back-ups
- Flexibilität und Skalierbarkeit
- Hohe Ausfallsicherheit
- Einfache Inbetriebnahme bei geringen Initialkosten
- Nutzungsbasierte Kosten (Pay-per-Use)
- Kurze Innovationszyklen dank schneller Rollouts

Aus dieser Vorteilsargumentation zu schließen, dass die Cloud in jeder Ausgangssituation die beste Wahl für den Anwender ist, wäre jedoch zu kurz gegriffen. Nach wie vor gibt es Szenarien, in denen Unternehmen und Organisationen vor einer vollständigen Migration ihrer Business-Kommunikation in die Cloud zurückschrecken.

On-Premises: In welchen Fällen weiterhin eine Alternative?

So fürchten manche Entscheider im Falle einer Cloud-Migration den Kontrollverlust – einerseits hinsichtlich der Datenübertragung und -speicherung mittels Dritter, andererseits über das System als solches, inklusive der Wartung, der Entwicklung von Backup-Szenarien und dem Ausführen von Updates. Auch was die Konfigurationsmöglichkeiten und den Funktionsumfang einer Lösung betrifft, können On-Premises-Systeme Vorteile bieten. In manchen Fällen liefern diese mitunter eine individuellere Anbindung der Kommunikationslösung an angrenzende Geschäftsprozesse. Ebenso ist zu beachten, dass es nach wie vor Regionen gibt – vorwiegend im ländlichen Raum – in denen eine vollständige Migration der Business-Kommunikation in die Cloud als riskant einzustufen ist. Denn komplett auf Cloud umzustellen, setzt eine ausreichende Netzabdeckung voraus.

Außerdem ist wichtig zu beachten: Cloud-Technologien können auf ganz unterschiedlichen Wegen bereitgestellt werden. So schließt sich an die Frage „Cloud, ja oder nein?“ unweigerlich die Herausforderung an, die richtige Variante der Bereitstellung zu wählen. Je nach Ausgangssituation (zum Beispiel Branche oder Unternehmensgröße) bieten sich individuelle Vor- und Nachteile. Im B2B-Bereich lassen sich vor allem drei Varianten voneinander differenzieren.

Public Cloud mit Multi-Tenant-Struktur

Eine häufige Variante ist die Multi-Tenant-Struktur. Bei dieser Public-Cloud-Architektur betreibt der Anbieter selbst das Cloud-Angebot, wobei er verschiedene Kunden auf einer Plattform bedient. Entsprechende Systeme sind meist mehrmandantenfähig, die Abrechnung erfolgt monatlich nach dem Pay-per-Use-Prinzip.

Die wesentlichen Vorteile dieser Bereitstellungsform liegen in der hohen Flexibilität und Skalierbarkeit. Verglichen mit anderen Modellen profitieren Nutzer unter anderem von geringen Kosten, beispielsweise bei der Anpassung der Nutzer oder auch beim dahinterliegenden Bezahlmodell.

Regelmäßige Updates entfallen auf Seiten der Nutzer, da Leistungen wie der Rollout neuer Features, Bugfixing oder das Schließen von Sicherheitslücken vom Anbieter für die gesamte Plattform programmiert und für alle Mandanten zur Verfügung gestellt werden. Der hohe Standardisierungsgrad einer Multi-Tenant-Struktur kann an anderer Stelle aber auch nachteilig sein, etwa wenn individuelle Anforderungen umgesetzt werden sollen.

Public Cloud mit Single-Instance-Struktur

Auch bei der Single-Instance-Struktur ist der Anbieter selbst der Plattformbetreiber. Im Gegensatz zum Multi-Tenant-Modell bekommt hier jedoch jeder Endkunde seine eigene Instanz in der Public-Cloud-Umgebung. Diese wird den jeweiligen Bedürfnissen des Kunden entsprechend aufgebaut, wobei physische Ressourcen logisch voneinander getrennt werden. Die Vorteile mit Blick auf die Flexibilität bei der individuellen Anpassungsfähigkeit schlagen sich beim Single-Instance-Modell jedoch in höheren Kosten nieder; so ist der administrative Aufwand für den Betreiber in der Regel höher. Auch können Software-Updates meist nicht zentral ausgeführt werden, weil in der Regel die Zustimmung des einzelnen Endkunden notwendig ist.

PBX in der Private Cloud

Für den Betrieb einer PBX in der Private Cloud erwirbt der Kunde diese als Softwarepaket. Die Installation erfolgt auf einem eigenen oder gemieteten Server, wodurch der Kunde nicht nur Eigentümer, sondern auch Betreiber der Cloud-Plattform ist. Dies zieht naturgemäß gewisse Verantwortlichkeiten bei der Pflege- und Wartung nach sich.

Der Vorteil dieser Variante liegt im hohen Individualisierungsgrad aus Sicht des Anwenders. Auch beim Hosting-Anbieter kann der Kunde frei wählen. Ein Modell, das sich vor allem für größere Unternehmen anbietet, die beispielsweise schon Cloud-Ressourcen in einem Rechenzentrum gebucht haben und die PBX als zusätzliches Element integrieren möchten.

Kein One-size-fits-all-Prinzip

Hybride Arbeitswelten sind auf dem Vormarsch: Telefonanlagen aus der Cloud können die damit verbundenen Anforderungen gut erfüllen – vorausgesetzt Unternehmen finden hierfür die nötige Netzabdeckung an ihrem Standort vor. Doch ist Cloud nicht gleich Cloud. Branche, Unternehmensgröße, Geschäftsmodell: Viele Faktoren müssen berücksichtigt werden, wenn Unternehmen die Frage nach der richtigen Bereitstellungsform ihrer Kommunikationslösung beantworten möchten. Ebenso muss prinzipiell die Bereitschaft vorhanden sein, die Kontrollmöglichkeiten mit Blick auf Datenverkehr und Konfigurationsmöglichkeiten aus der Hand zu geben.

Es zeigt sich, dass die Kostenvorteile einer höheren Standardisierung (Multi-Tenant-Struktur in der Public Cloud) eher für KMU mit bis zu fünfzig Mitarbeitenden interessant sind. Auch Unternehmen mit Saisonbetrieb können von diesen flexiblen Produkten profitieren. Der Aufbau individuellerer Strukturen, wie sie sich bei Single-Instance-Modellen in der Public Cloud finden, eignet sich hingegen eher für größere Unternehmen mit bis zu 100 Mitarbeitenden.

Für noch größere Unternehmen sind wiederum die Vorteile von Private-Cloud-Infrastrukturen interessant. Aufwand und Kosten für die Individualisierung skalieren auf diesem Niveau meist bereits ausreichend. Zudem ist oft das erforderliche Wissen im Unternehmen vorhanden, um Pflege und Wartung selbst zu bewerkstelligen.

Jörn Lembke ist Head of Product Management bei Auerswald

DIE ROLLE VON GIT

Bild: binaryproject-123rf

Git zählt heutzutage zu den am weitest verbreiteten Versionskontrollsystemen. In der Unternehmenswelt trifft das System vielerorts auf Mainframes. In diesem Fall kann Git zu einer sinnvollen Ergänzung bei der Mainframe-Entwicklung werden.

Autor: Tony Anter ***Redaktion: Sabine Narloch***

➤ Die Technologie schreitet voran, und Unternehmen suchen nach der nächsten Stufe von DevOps für den Mainframe. Viele sehen Git (kurz für Global Information Tracker) als die nächste Phase an, da es alle Quellen auf einer Plattform konsolidieren kann. Git hat sich bereits als Werkzeug für EntwicklerInnen in verteilten Umgebungen zur Erstellung und Änderung von Code bewährt. Dabei handelt es sich um ein Versionskontrollsystem, das ursprünglich vor über 20 Jahren von Linus Torvalds geschaffen wurde; Torvalds, der als der Entwickler von Linux gilt, erkannte die Bedeutung der Versionskontrolle von Quellcode.

Git ist nun nicht nur ein Versionskontrollsystem, sondern auch ein Quellcode-Verwaltungssystem (SCM), eine Repository-Technologie, die die gemeinsame Speicherung von Quellcode-Artefakten ermöglicht, um Änderungen am Anwendungscode zu speichern und zu verfolgen. Diese Prozesse sind für die Förderung der Zusammenarbeit zwischen ProgrammiererInnen bei der gemeinsamen und parallelen Entwicklung von Quellcode unerlässlich. Viele IT-Mitarbeitende sind mit Git möglicherweise erst durch ihre Kenntnis von sekundären Anbietern wie GitHub vertraut, einem Repository für Code, während Git selbst eine zentrale Rolle im Softwarebereitstellungszyklus spielt.

Zu den allgemeinen Vorteilen von Git gehören Geschwindigkeit, Datenintegrität und Unterstützung für verteilte, nicht lineare Workflows. Die Verwendung von Git bedeutet, dass sich alle Quellen an einem Ort befinden, was die Erstellung und Sicherung von Back-ups vereinfacht. Außerdem fungiert es als Aufzeichnungssystem für den Quellcode, der wiederum das wertvolle geistige Eigentum eines Unternehmens enthält. Git ermöglicht die Überprüfung und bei Bedarf die Rückkehr zu früheren Iterationen des Codes – kann aber auch mehr als nur Quellcode enthalten. So kann es Dokumentation, Testszenarien und andere Formen von Metadaten beinhalten, die sich auf eine Anwendung beziehen. Es ist ein Open-Source-Tool, das von IngenieurInnen für IngenieurInnen entwickelt wurde, um ihnen eine nahtlose Zusammenarbeit zu ermöglichen. Es gibt zwar auch andere Tools im Technologiebereich, aber es dürfte schwer sein, ein Unternehmen zu finden, das nicht irgendeine Variante von Git als primäre Versionskontrolllösung einsetzt.

Außerdem sind gerade die jüngeren Mitarbeitenden, die in die Branche eintreten, bereits mit Git vertraut, da es Bestandteil des Lehrplans in der Ingenieursausbildung weltweit ist. Das bedeutet eine einfachere Einarbeitung mit geringeren zusätzlichen Schulungskosten. Der größte Vorteil aller von Git gebotenen Funktionen dürfte sein, dass Teams schnellere Versionszyklen produzieren können, was einen agilen Arbeitsablauf erleichtert.

Weitere Eigenschaften von Git sind:

- Git wurde mit Blick auf die Erfahrung der EntwicklerInnen entwickelt. Unabhängig davon, ob man natives Git oder einen der Remotes wie GitLab, GitHub oder Bitbucket verwendet, erleichtert Git die tägliche Entwicklung mit integrierten Funktionen zum Vergleichen, Zusammenführen und Genehmigen von Änderungen.
- Git unterstützt mehrere Sprachen und Methoden für die Arbeit an Mainframe-Anwendungen, zum Beispiel Java, C, Node, Python,

Cobol, JCL, Rexx, PL1, Assembler und andere Quellcode-Sprachen.

- Es bietet Unterstützung für Verzweigungen, um parallele Entwicklung für Teams und Einzelpersonen zu ermöglichen, sodass Benutzende eine isolierte Umgebung für Entwicklung oder F&E erstellen und diesen Code dann wieder in den Hauptzweig oder Stamm einbringen können.
- Mit Git können Unternehmen ihre SDLC-Prozesse (Software Delivery Lifecycle) unternehmensweit und plattformunabhängig konsolidieren. Der Mainframe ist dann keine isolierte Plattform mehr, wenn er das gleiche Tool und den gleichen Prozess wie der Rest des Unternehmens verwendet.
- Git-Plattformen sind offen und lassen sich in fast jedes System integrieren. Aufgrund der weiten Verbreitung unterstützt fast jedes DevOps-Tool oder jede Umgebung bereits Git, und Git-Systeme unterstützen die meisten Plattformen und Tools.

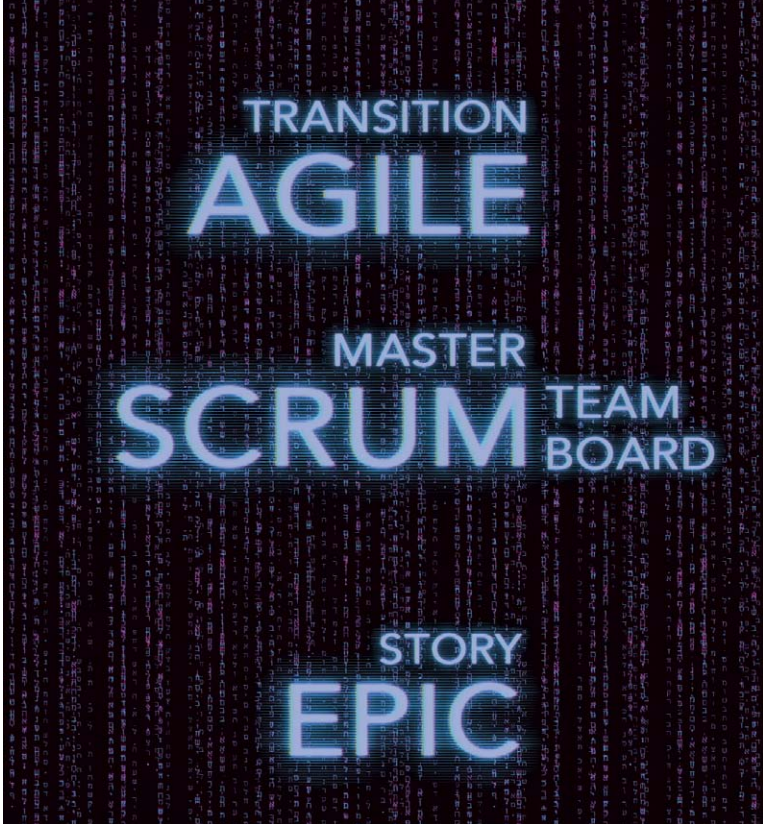
Git für Mainframe-Code?

Der Umgang von Git mit Mainframe-Quellcode unterscheidet sich letztlich nicht von dem mit verteilten Assets. Aus Sicht von Git ist der Mainframe wie jede andere Code-Basis und kann auf die gleiche Weise bearbeitet werden wie Java, Node.js, C# oder jede andere Codebasis. Git ist zudem ein Weg, um die grundlegenden Funktionen des Überprüfens, Bearbeitens und Wiedereincheckens von Code durchzuführen. Da Git jedoch nur ein Drittel des DevOps-Prozesses abdeckt, benötigt ein Unternehmen Tools für die verbleibenden zwei Drittel, also Build-Management und Deployment-Management.

Die Vielseitigkeit und die Marktakzeptanz von Git zeigen seinen Wert als leistungsfähiges Entwicklungstool und sind eine natürliche Ergänzung für die Mainframe-Entwicklung. Mit Git können Teams entscheiden, was ihren Anforderungen am besten entspricht. Es gibt jedoch Fälle, in denen es nicht sinnvoll ist, auf Git zu setzen: Ein Beispiel ist, wenn sich ein Team um eine Batch-Anwendung kümmert, die sich im Wartungsmodus befindet. Wenn ein solches Team über zweieinhalb Millionen Batch-Artefakte verfügt – alle Komponenten, aus denen die tägliche, wöchentliche, monatliche, vierteljährliche und jährliche Verarbeitung von Daten besteht –, werden die Mitarbeitenden dieses Teams nicht ein Git-Repository für jede Komponente auschecken wollen, um eine einzeilige JCL-Änderung an diesem Teil der Organisation vorzunehmen. So etwas könnte zum Beispiel in einem Unternehmen vorkommen, das seine Anwendung nur alle paar Jahre für eine Aktualisierung der Umsatzsteuer ändert.

Trotz der Vielzahl von Veränderungen und technologischen Innovationen in der Unternehmenswelt gibt es zwei Konstanten: die Präsenz des Mainframes als Grundlage der Datenverwaltung und die Präsenz von Git als Repository für die Versionskontrolle. Unternehmen müssen sicherstellen, dass der Code an einem Ort verwaltet wird, der die parallele Entwicklung fördert und sofort verständlich ist, und gleichzeitig eine nahtlose und genaue Erstellung, Prüfung und Bereitstellung von Code für Handel und Industrie ermöglicht.

Tony Anter ist DevOps-Evangelist für BMC



LOW-CODE UND DER AGILE-ANSATZ WEITERGEDACHT

Agile 2 ist der Versuch, einige Aspekte des Agile-Ansatzes zu ergänzen, um damit eine erfolgreiche Softwareentwicklung zu fördern. Allerdings sind einige der Empfehlungen von Agile 2 bei der Verwendung traditioneller High-Code-Entwicklungsmethoden nicht unbedingt leicht umzusetzen – anders sieht die Sache mit Low-Code aus.

Autor: Dirk Pohla Redaktion: Sabine Narloch

➤ Softwareentwicklung ist normalerweise sehr komplex. Daher gibt es nicht immer den einen „richtigen“ Weg. Jedes Projekt hat seine eigenen Variablen, Herausforderungen und Eigenheiten. Und jeder Entwickler hat eine bevorzugte Arbeitsweise – feste Regeln aufzustellen, ist daher schwierig. Das bedeutet jedoch nicht, dass sich Unternehmen ohne Richtlinien oder eine Methodik in ihre Entwicklungsprojekte stürzen sollten.

Jedes Entwicklungsprojekt ist einzigartig, daher ist keine einzelne Methode die beste für jedes Szenario. Methoden wie Scrum, Agile, Lean Software Development oder Kanban wurden mit dem Ziel entwickelt, um die Softwareentwicklung zu systematisieren oder zu steuern. Oft sind die neueren Methoden Reaktionen auf ältere Verfahren, die eine Über- oder Unterbetonung von Struktur, Planung und Management korrigieren – dazu gehört etwa die Wasserfall-Methode. Und obwohl die Grundlage vieler Methoden ein iterativer Ansatz ist, sind sie selbst manchmal zu starr geworden, um die notwendige Entwicklung zu durchlaufen, zu reifen und sich zu verbessern. „Agile” selbst entstand als Gegenmittel zu den „dokumentationsgesteuerten, schwerfälligen Softwareentwicklungsprozessen“. Aber auch diese Methode hat ihre Kritiker, die den Mangel an Vorhersehbarkeit und Dokumentation als potenzielle Probleme anführen, während andere die Fallstricke darin sehen, dass sie ihr Versprechen eines nachhaltigen Tempos nicht erfüllt hat.

Hier kommt Agile 2 ins Spiel. Wie der Name schon sagt, ist es keine völlige Abkehr von „Agile”, sondern ein Versuch, die besseren Aspekte durch Ansätze zu ergänzen, die eine erfolgreiche Softwareentwicklung fördern.

Kräfte bündeln

Einige der Empfehlungen von Agile 2 sind bei der Verwendung traditioneller High-Code-Entwicklungsmethoden aber nicht unbedingt leicht umzusetzen: Der „zweigleisige“ Ansatz für das Produktdesign beispielsweise, bei dem Produktdesign und technisches Design parallel arbeiten, aber keiner den Fortschritt des anderen behindert. Obwohl dies bei der Erstellung von Software durch das Schreiben von langem Code möglich ist, kann der Weg langwierig sein; von der Feature-Definition bis zur Feature-Implementierung können Wochen oder auch Monate vergehen. Zwischen dem Zeitpunkt, an dem ein Entwicklungsteam die Anforderungen des Unternehmens erhält, und dem Punkt, an dem die Produktdesigner diese Anforderungen in eine testfähige Version umsetzen können, liegt oft eine beträchtliche Zeitspanne. Die lange Entwicklungszeit verhindert also, dass ein zweigleisiger Prozess, der idealerweise aus einem schnellen Zyklus von Feature-Konzeption und -Implementierung mit geringen Verzögerungen bestehen sollte, optimal genutzt werden kann.

Die Entwicklung von Low-Code-Anwendungen ist gut für die in Agile 2 dargelegten Grundsätze geeignet. Low-Code-Plattformen für Unternehmen verfügen über Funktionen, die viele Probleme von Agile 2 lösen:

Planung: Die Prozessmodellierung in Low-Code erleichtert die Planung, indem sie eine grafische Darstellung für die Erstellung des Prozessablaufs bereitstellt. IT- und Business-Stakeholder können sich darauf einigen, welche Aktivitäten ausgeführt werden müssen, welche Aufgaben den Automatisierungstechnologien zugewiesen werden sollen und wo menschliches Eingreifen erforderlich ist. Die Prozesslandkarte lässt sich bei der Durchführung des technischen Entwurfs und des Produktdesigns jederzeit anpassen, abgestimmt auf die Bedürfnisse des Unternehmens. Auf diese Weise ist die Pla-

Bild: mbruska-123rf

wie sich diese auswirken, wenn sie gemeinsam eingesetzt werden.

Daten: Low-Code-Plattformen machen mitunter die Erstellung komplexer Datenbankansichten oder die Migration von Daten überflüssig. Low-Code-Konnektoren ermöglichen den Zugriff auf die Daten dort, wo sie vorhanden sind. Sie bieten gleichzeitig die Möglichkeit, die Daten zu erweitern und umzuwandeln; das kann es einfacher machen, auf die Erkenntnisse, die die Daten liefern, zu reagieren. Low-Code-Plattformen können nicht nur eine einheitliche Sicht auf die Daten eines Unternehmens bieten, sondern auch integrierte Datenvalidierungen zur Maximierung der Datenzuverlässigkeit umfassen. Das Versprechen von „Low-Code-Daten", einheitliche, validierte Daten zu liefern, bietet die Art von strategischem Wert, der Daten zu einem echten Stakeholder im Softwareentwicklungsprozess macht.

Bereinigen von starren Elementen aus Agile

Das Ziel von Agile 2 ist es, einen Teil der De-facto-Starrheit von Agile zu beseitigen. Es hebt die Ideen einer flexiblen Zusammenarbeit, einer besseren Abstimmung von technischem Design und Produktdesign und einer Weiterentwicklung der Teamdynamik hervor und erweitert diese um die Fähigkeiten und das Wissen aller Teammitglieder und Interessengruppen. Das Ergebnis können bessere Geschäftsergebnisse sein. Agile 2 erkennt auch den Wert und die Bedeutung von Daten im Zusammenhang mit der Softwareentwicklung und betont die Notwendigkeit, die verfügbaren Daten eines Unternehmens so nutzbar wie möglich zu machen. Mit Low-Code sind Unternehmen in der Lage, diese Themen besser anzugehen und ihre bestehenden Agile-Praktiken zu optimieren.

Das Ziel von Agile 2 ist es, einen Teil der De-facto-Starrheit von Agile zu beseitigen. Es hebt die Ideen einer flexiblen Zusammenarbeit, einer besseren Abstimmung von technischem Design und Produktdesign und einer Weiterentwicklung der Teamdynamik hervor und erweitert diese um die Fähigkeiten und das Wissen aller Teammitglieder und Interessengruppen.

nung gut sichtbar, und man kann leicht umschwenken. Low-Code-Plattformen bieten mitunter die Möglichkeit, die Dokumentation an einem zentralen Ort zu organisieren. Künftige Teams, die an der Software arbeiten, können diese dann nutzen. Durch die Verknüpfung wichtiger Informationen mit dem Projekt selbst wird sichergestellt, dass Informationen nicht verloren gehen. Zudem lassen sich so beispielsweise neue Entwickler schneller einarbeiten.

Zusammenarbeit: Low-Code hilft, die Kluft zwischen Entwicklern und Fachbereichsanwendern zu überbrücken, indem es die Zusammenarbeit einfach und visuell gestaltet. Gleichzeitig fördert Low-Code klare, häufige Beiträge, die helfen, Annahmen auf dem Weg zur richtigen Lösung zu testen. Prototypen und laufende Builds geben Produktdesignern und Testnutzern konkrete Beispiele an die Hand, auf die sie reagieren können. Sie beschleunigen den Produktdesignprozess, indem sie sicherstellen, dass das Entwicklungsteam ein klares Verständnis der Anforderungen hat.

Teamstruktur: Low-Code bietet eine niedrigere Einstiegsschwelle als High-Code-Umgebungen. Dadurch kann eine Vielzahl unterschiedlicher Teams an Entwicklungsprojekten arbeiten. Das erweitert das im ursprünglichen agilen Manifest gegebene Versprechen einer funktionsübergreifenden Zusammenarbeit. Von erfahrenen Entwicklern, die mehrere Code-Sprachen beherrschen und ihr Fachwissen mit Low-Code erweitert haben, bis hin zu „Citizen Developer" und anderen Mitarbeitern, die eine Vielzahl von fachlichen Hintergründen und Fähigkeiten mitbringen, bietet Low-Code einen umfassenderen Ansatz für die Entwicklung. Low-Code-Plattformen können außerdem hilfreich sein, wenn mehrere Entwickler Änderungen an einer Anwendung vornehmen und sich darüber im Klaren sein müssen,

Beim agilen Ansatz mit Scrum-Teams und Programmiersprache, dauert es in der Regel Wochen, manchmal Monate, um von der Feature-Definition zur Feature-Implementierung zu gelangen. Mit Low-Code-Tools sind Teams in der Lage, innerhalb von Tagen vom Prototyp zu einer funktionierenden und dann in einem ähnlichen Zeitrahmen zu einer vollständigen produktionsreifen Version zu kommen.

Dirk Pohla ist Area Vice President bei Appian Deutschland

AGILE 2

➤ **Unter dem Schlagwort „Agile 2" haben sich einige Agile-Experten mit den ursprünglichen Werten und Attributen von „Agile" auseinandergesetzt und sie weitergedacht. Hier wie dort handelt es sich um eine Reihe von Ideen hinsichtlich Attributspaaren wie: Durchdachtheit und Vorgabe, Ergebnisse und Output, Einzelpersonen und Teams, geschäftliches und technisches Verständnis, individuelle Befähigung und gute Führung.** *(SN)*

LOW CODE, HOHE AKZEPTANZ

Fachabteilungen kennen ihre genutzte Software und deren Schwächen am besten. Da macht es Sinn, dass Teammitglieder aus den entsprechenden Abteilungen die Entwicklung neuer Funktionen selbst in die Hand nehmen. Dank Low-Code, No-Code und Citizen Development wird das in Unternehmen immer mehr praktiziert.

Autor: Andreas Grydeland Sulejewski Redaktion: Sabine Narloch

➤ Die Mitglieder eines Marketingteams, das in den letzten fünf Jahren dieselbe Software verwendet hat, kennt ihre Möglichkeiten – aber auch ihre Grenzen sowie die daraus resultierenden Herausforderungen. Doch die Softwareentwicklung liegt oder lag bislang bei der IT-Abteilung. Mit Low-Code-Technologie können nun jedoch Geschäftseinheiten im gesamten Unternehmen ihre abteilungsinternen technischen Herausforderungen selbst bewältigen. So können Anwender mithilfe von Low-Code-Plattformen einen Teil der Kontrolle über technische Prozesse übernehmen, wie zum Beispiel die Integration von Daten zwischen Anwendungen und die Automatisierung von benutzerdefinierten Datenflüssen in ihrem gesamten technischen Umfeld.

Mehr als nur Spielerei

Low-Code- und No-Code-Entwicklungsumgebungen sowie visuelle Programmiertools gibt es seit den 1980er Jahren. Lange Zeit wurden sie jedoch von IT-Fachleuten eher als Hilfsmittel angesehen, die lediglich für sehr einfache Aufgaben geeignet sind. In der Vergangenheit schnitten No-Code/Low-Code-Tools mitunter schlecht ab, weil diese Tools nicht für Design-Konzepte genutzt wurden. Die Funktionalität beschränkte sich auf Prozesse, die per Drag-and-Drop visualisiert werden konnten. Dies ist heute nicht mehr der Fall und eine Reihe von Faktoren – einschließlich der Möglichkeit, Low-Code-Tools in bestehende Tools etablierter Hersteller zu integrieren – machen dieses Prinzip für Unternehmen durchaus attraktiv.

Low-Code ist heutzutage somit mehr als nur eine Spielerei. Nach dem Prinzip des modularen Baukastens können die zu erstellenden Softwareanwendungen beliebig komplex werden. Die Kunst besteht darin, mit Fantasie und Planung für jedes Projekt die wiederkehrenden Bausteine zusammenzustellen, um Papierprozesse oder veraltete Arbeitsweisen zu digitalisieren und den Mitarbeitern den Arbeitsalltag zu erleichtern.

Um die App-Entwicklung für digitale Lösungen zu beschleunigen, setzen Unternehmen zunehmend auf Low-Code- und No-Code-Tools. Das kann von Fall zu Fall manuelle Programmierung, die durch hochqualifizierte Softwareentwickler vorgenommen werden müsste, ersetzen. Damit einhergeht, dass Unternehmen Software und Funktionen in neuem Tempo entwickeln und bereitstellen können. Die Zeiten, in denen man Monate oder länger auf die nächste Softwareversion aus der IT-Abteilung warten musste, dürften damit vorbei sein.

Wie No-Code-/Low-Code ist auch die Rolle des „Citizen Developer“ – also eines nicht IT-ausgebildeten Mitarbeiters mit der Fähigkeit, Apps zu erstellen – ein Konzept, das lange Zeit eher skeptische Reaktionen hervorgerufen hat. Die demokratisierte Nutzung von Technologie führt zwar zur Dezentralisierung der IT-Abteilungen, bietet aber die Möglichkeit, dass Mitarbeiter, die keine Techniker sind, ihre eigenen technischen Herausforderungen mithilfe von Low-Code-Automatisierungs- und Integrationsplattformen lösen können. Dabei kommen mitunter sogenannte „Fusion-Teams“ zum Einsatz; sie vereinen das technologische und betriebswirtschaftliche Fachwissen und treiben gemeinsam die Entwicklung von Apps, No-Code-Tools und agilen Prozessen voran. Durch sie werden Citizen Developer befähigt, ihren Beitrag zur Digitalisierung des Unternehmens zu leisten. Darüber hinaus ermöglichen Online-Schulungen den Anwendern, in ihrem eigenen Tempo zu lernen, und ihre modularen Application Building Blocks können bei Bedarf in den formalen IT-Entwicklungsprozess einfließen.

Kritikern zum Trotz ist man der Ansicht, dass Citizen Developer – als Teil eines demokratischen und kollaborativen Ansatzes zur Deckung des Bedarfs an digitalen Lösungen – formalisiert werden sollte. Laut Gartner soll die Zahl der Citizen Developer die der professionellen Entwickler bis 2023 um den Faktor vier zu eins übersteigen. Das kann für überlastete IT-Organisationen zum Vorteil werden, denn so lassen sich ihre knappen Ressourcen auf strategischere Projekte umleiten.

Doch noch sind Citizen Developer in vielen modernen Unternehmen oftmals eine ungenutzte Ressource. Das internationale Marktforschungsunternehmen Forrester hatte zwar für das Jahr 2021 prognostiziert, dass 75 Prozent aller Entwicklungsunternehmen Low-Code-Plattformen einsetzen werden. Laut der aktuellen Studie „No-Code/Low-Code 2022“ mehrerer Fachzeitschriften liegt die Zahl jedoch niedriger; demnach nutzen 60 Prozent der befragten Unternehmen ein bis zwei No-Code- oder Low-Code-Plattformen, um ihre Digitalisierungsstrategie umzusetzen.

Doch dort, wo Mitarbeiter durch Citizen Development bereits zur App-Entwicklung befähigt sind, besteht die Chance, Lösungen zu kreieren, die von den Anwendern akzeptiert werden und exakt auf die Geschäftsprozesse zugeschnitten sind.

Andreas Grydeland Sulejewski ist Chief Executive Officer von Neptune Software

INEFFIZIENT – TROTZ MODERNER TOOLS ?

Bild: liudmilachernetska - 123rf

Mit dem Einzug hybrider Arbeitsmodelle wurde vielerorts die Anzahl der technischen Tools erhöht. Doch allein die Quantität oder die Neuheit von Tools gewährleistet noch keine höhere Produktivität. Entscheidend ist die Art und Weise, wie Teams damit arbeiten.

Autor: Steve Wood Redaktion: Sabine Narloch

➤ Ob im Homeoffice, im Büro oder im Café: Im Arbeitsalltag sind regelmäßig Dutzende Tools im Einsatz. Ob Task-Management, Dokumentenkollaboration, Finanzsoftware, Kalender-Apps oder Messaging-Plattformen – wir arbeiten ständig mit Informationen und tauschen sie aus, um unseren Arbeitsalltag zu bewältigen. Es ist daher nicht verwunderlich, dass die Zahl der verwendeten Anwendungen exponentiell gestiegen ist: Einem Bericht des Softwareentwicklers Productiv zufolge nutzen die meisten Abteilungen zwischen 40 und 60 verschiedene Anwendungen.

Unternehmen sehen sich daher mit einem sich ständig weiterentwickelnden Netz von Prozessen und Anwendungen konfrontiert. Gleichzeitig verändern sich die Tools, Technologien und Sprachen für die Iteration und Bereitstellung von Software schneller denn je. IT- und DevOps-Teams sind dabei das Herzstück der Softwarebereitstellung und -innovation. Sie sorgen für einen reibungslosen Arbeitsablauf. Doch ihre Aufgaben werden komplizierter. Deshalb ist es an der Zeit, dass Führungskräfte einen Schritt zurücktreten und ihre Herangehensweise zur Optimierung und Modernisierung ihres Tech-Stacks überdenken. Denn mehr Software und technische Lösungen spornen ein Team nicht automatisch zu besserer Arbeit an. Stattdessen sollten Führungskräfte sich verstärkt auf Produktivität, effiziente Zusammenarbeit und erfolgreiche Ideenfindung konzentrieren. Ein Weg dorthin kann sein, die Produktivität und den Output anhand der Faktoren „Time to Audience“ oder „Speed plus Quality“ zu messen. Durch das Prüfen von Fragen wie etwa „Wie lange dauert es, die Aufgabe zu spezifizieren?“, „Wie lange dauert es, die Aufgabe zu bearbeiten und zu iterieren?“ oder „Wie lange dauert es, das Ergebnis bereitzustellen und zu messen?“ kann man Erkenntnisse gewinnen, die dazu beitragen, die Entwicklungspraktiken eines Teams zu beschleunigen oder zu verändern – und das, ohne eine neue Technologie einzuführen.

Alt ist nicht zwangsläufig schlecht

Das neueste Must-Have-Tool mag verführerisch wirken. Wenn es aber um ein optimiertes Tech-Stack geht, wird oftmals ein Aspekt übersehen: dass es darum geht, wie effizient Tech-Teams damit arbeiten können – unabhängig davon, wie alt oder neu es ist. Denn ältere Tools wie Java und SQL können für sich genommen immer noch leistungsstark sein. Wenn die Arbeit mit einem älteren Tech-Stack bedeutet, dass Änderungen nicht schnell genug umgesetzt werden können, ist das nicht immer ein Problem des Tech-Stacks, sondern kann eher ein Innovations- und DevOps-Problem sein.

Ein Beispiel ist die Entwicklung einer Mobile App. Das Kompilieren dauert etwa drei bis vier Minuten. Angenommen, dieser Zeitraum soll auf eine Minute verkürzt werden: Dieser Unterschied von lediglich ein paar Minuten mag auf den ersten Blick nicht gravierend klingen. Anders sieht es aus, wenn die App jeden Tag mehr als 50 Mal kompiliert werden muss. Lassen sich bei jedem Zyklus einige Minuten sparen, indem die Arbeitsabläufe in den Teams effizienter gestaltet werden, kann das signifikante Auswirkungen auf den ROI des Unternehmens haben.

Grundsätzlich lässt sich eine Erhöhung des ROI beispielsweise durch schnellere Freigaben, kürzere Zeiten für das Incident Management oder die Verbesserung der Change Failure Rate herbeiführen. Auch hier ist nicht so entscheidend, wie neu die verwendeten Tools sind, sondern, ob sie effizient genutzt werden.

Eine Rolle spielen hier Low-Code- und Automatisierungstools. So erhalten die Menschen mit dem Einsatz von Low-Code-Tools mehr Gestaltungsmacht – egal ob sie technisch versiert sind oder nicht. Mit Low-Code- und Automatisierungstools können sich IT-, DevOps- und Engineering-Teams zudem auf die Lösung komplexerer Probleme konzentrieren und Produkte schneller und effizienter iterieren, testen und ausrollen. Gartner geht davon aus, dass bis 2024 80 Prozent der Technologieprodukte von Personen entwickelt werden, die keine Tech-Experten sind.

Angesichts hybrider Arbeitsweisen gilt es einerseits einen reibungslosen Geschäftsbetrieb aufrechtzuerhalten, andererseits neue Technologien zu testen und zu implementieren, die das Unternehmen voranbringen sollen. IT-, DevOps- und Engineering-Führungskräfte sollten daher ihr größtes Kapital in den Vordergrund stellen – ihre MitarbeiterInnen. Das wird möglich, indem sie sich auf bessere Prozesse für Innovationen, neue Wege zur Erfolgsmessung sowie Tools konzentrieren, die durch Automatisierung Komplexität reduzieren.

Steve Wood ist Senior Vice President Product & Platform bei Slack

DRUCK ÜBER DIE CLOUD

Lokale IT-Systeme lassen sich in die Cloud verlegen – auch die Druckinfrastruktur. Das kann in mehrerer Hinsicht Auswirkungen haben.

Autor: Daniel Taylor
Redaktion: Sabine Narloch

➤ Auch in Zeiten von E-Mails, Apps und eBook-Readern wird im geschäftlichen Alltag noch einiges auf Papier ausgedruckt: beispielsweise Verträge, Akten und offizielle Schreiben. Doch das Aufkommen neuer Arbeitsmodelle wie Remote Work und aktuelle Technologien verändern Anforderungen und Möglichkeiten in Sachen Druckmanagement. Konkret heißt das, dass die klassischen lokalen Printserver mehr und mehr auf dem Prüfstand stehen. An ihre Stelle treten mittlerweile vielerorts Cloud-basierte Drucklösungen.

Doch Cloud-basierte Lösungen bringen zahlreiche Neuerungen auch für IT-Teams mit sich. In einer herkömmlichen Druckinfrastruktur ist es die Aufgabe der IT-Abteilung beispielsweise, sämtlichen Endgeräten (Clients) eines Firmenstandortes den Zugang zur Druckflotte zu ermöglichen. Dazu müssen die Administratoren zunächst dafür sorgen, dass auf allen Clients die jeweils richtigen Treiber vorhanden sind. Ist das gegeben, können die Endnutzer ihre Druckaufträge an den lokalen Printserver schicken, der sie in die jeweilige Warteschlange für die einzelnen Geräte weiterleitet. Im Falle von Cloud-basierten Drucklösungen kann es hingegen sein, dass nur ein Treiber nötig ist, der sämtliche Betriebssysteme und Geräte mit der Druckflotte verbindet – vom Windows-Laptop über ein Android-Tablet bis hin zum iPhone. Diese Verbindung läuft dann über einen zentralen Cloud-Server, den zugangsberechtigte Clients über das Internet erreichen und der die lokalen Printserver möglicherweise sogar ersetzen kann.

Druckbefehl von überall

Die Verbindung über das Web ermöglicht es Nutzern darüber hinaus, ortsunabhängig drucken zu können. Im Zweifel ist es dabei auch möglich, private Geräte zu verwenden. Mit einem Gast-Account können Unternehmen ihre Druckflotte in vielen Fällen zudem externen Personen wie Kunden oder Freelancern zur Verfügung stellen. Eine Web-basierte Benutzeroberfläche für die Administratoren ist in den meisten SaaS-Paketen enthalten. Sie soll die Verwaltung der Druckinfrastruktur durch die IT-Abteilung vereinfachen.

Cloud-Lösungen gehen aber auch mit veränderten Sicherheitsanforderungen einher. Hier kann es vor allem helfen, einen Zero-Trust-Ansatz zu implementieren und nur jenen Clients Zugriff auf die Funktionen und die verschiedenen Bereiche zu gewähren, die sie wirklich benötigen. Zudem muss die Ende-zu-Ende-Verschlüsselung der gesamten Kommunikation zwischen Cloud-Server und Hardware zum Sicherheitsstandard entsprechender Lösungen gehören. Eine automatisierte Sicherung sämtlicher Daten in der Cloud kann darüber hinaus im Worst Case vor Verlusten schützen.

Ein für viele Unternehmen relevantes Merkmal Cloud-basierter Lösungen ist ihre Skalierbarkeit, von der auch Drucklösungen profitieren können. Wächst ein Unternehmen, erhöht sich meist auch die an Nutzern und Geräten, die auf die Druckflotte zugreifen müssen. Statt nun neue Server-Ressourcen selbst bereitzustellen, können Unternehmen bei ihrem jeweiligen Anbieter mehr Speicherplatz und Rechenleistung in der Cloud hinzubuchen. Gleichermaßen können sie gegebenenfalls ihren Verbrauch wieder herunterfahren, sollten sich Änderungen ergeben, die die Anzahl an verknüpften Geräten oder die Datenlast verringern.

Daniel Taylor ist Geschäftsführer bei Apogee

WACHSENDES INTERESSE

➤ Cloud-Printing wird immer beliebter. Laut der Studie „Cloud Print Services 2022" des Marktforschungsunternehmens Quocirca haben 43 Prozent der befragten Unternehmen bereits eine Cloud-Druckmanagement-Plattform implementiert. Deutschland liegt hier allerdings mit 32 Prozent hinter Großbritannien (40 Prozent), Frankreich (43 Prozent) und den USA (56 Prozent) zurück. Der Finanzsektor zeigt sich dabei mit 56 Prozent als die am weitesten fortgeschrittene Branche. Ein wichtiger Aspekt für Unternehmen, sich für eine Cloud-Druckplattform zu entscheiden ist die Sicherheit. 52 Prozent der Befragten halten das Drucken in der Cloud als sicherer als eine Plattform vor Ort. *(SN)*

WARUM SOLLTE MAN EIGENTLICH...

Autor: Alexander Haugk Redaktion: Diana Künstler

➤ Windows 11 ist seit mehreren Monaten verfügbar und mittlerweile eine echte Option für die Unternehmen. Doch warum sollte gerade jetzt umgestellt werden? Insbesondere, wo doch mit Windows 10 auch noch das aktuelle Betriebssystem ordnungsgemäß läuft. 14 Prozent der Nutzer haben sogar immer noch Windows 7 im Einsatz. Da momentan kein Zeitdruck herrscht – Unterstützungsende für Windows 10 ist offiziell 2025 – kann jetzt in Ruhe die Migration vorangetrieben werden. Momentan lassen sich die Systeme auch nebeneinander betreiben, wodurch bei etwaigen Schwierigkeiten keine allzu großen Betriebsausfälle zu erwarten wären. Gleichzeitig sollte sich jedoch auch nicht zu viel Zeit gelassen werden, da es voraussichtlich keine Feature-Updates für Windows 10 mehr geben wird. Deswegen lohnt es sich, die Migra-tion frühzeitig anzustoßen, bevor der Stichtag der Abschaltung naht. Viele Unternehmen scheuen jedoch den Wechsel, da sie in der Vergangenheit zum Beispiel schlechte Erfahrungen mit Migrationen von Betriebssystemen gemacht haben.

In Wellen updaten

Eine solche Umstellung gestaltet sich jedoch nicht so schwierig wie in Vergangenheit, da sich Windows 10 und Windows 11 deutlich ähnlicher sind als ihre Vorgänger. Etwaige Kompatibilitätsprobleme sind dementsprechend selten, sollten jedoch frühzeitig durch Tests aufgespürt und behoben werden, vorzugsweise noch während der Migrationsplanung. Insbesondere proprietäre Lösungen oder Eigenentwicklungen müssen Unternehmen besonders im Auge behalten. Aber auch Datenbanken sind oftmals kritisch.

Damit das Upgrade erfolgreich verläuft, sollte es in Wellen ausgerollt werden: In Phase 1 wird die Migration auf einem Testaccount simuliert. In Phase 2 erfolgt die Umstellung ausgewählter Key User, verteilt auf unterschiedliche Abteilungen, sodass bei Problemen nicht gleich die komplette Abteilung ausfällt. In der abschließenden Phase 3 findet dann der eigentliche Roll-out statt. Selbstverständlich sollte während jeder einzelnen Phasen immer wieder untersucht werden, ob Probleme auftreten, um für diese zeitnah Lösungen zu finden.

Vorsicht beim Umzug

Eine OS-Migration hat stets den positiven Nebeneffekt, dass Unternehmen selten genutzte oder obsolete Software entfernen können. Es bietet sich die Gelegenheit, die Systeme auch in dieser Hinsicht auf einen einheitlichen Stand zu bringen. Hier können jedoch Reibungspunkte entstehen: Endnutzer könnten beispielsweise das neue Layout ablehnen. Das lässt sich jedoch umgehen, indem dieses vorkonfiguriert wird, damit die Unterschieder der Benutzeroberfläche möglichst gering ausfallen. Bei einer Migration ist zudem zu beachten, dass Windows 11 höhere Anforderungen als die Vorgängerversionen an die CPU stellt. Das heißt, dass selbst die verfügbaren Chips der letzten drei bis fünf Jahre nicht automatisch unterstützt werden. Und auch mit Blick auf SSDs erhöht Microsoft zusehends die Anforderungen; so lässt der Anbieter Windows 11 nur vorinstallieren, wenn das Betriebssystem von der SSD booten kann. Dies lässt sich jedoch zum Beispiel durch den Einsatz des Windows-11-Enterprise-eigenen Long Term Servicing Channel (LTSC) umgehen. Hier bietet Microsoft zehn Jahre Support an, ohne Features upzugraden – ein Plus bei besonders empfindlichen und kritischen Systemen. Für eine saubere Migration werden hier sechs bis zwölf Monate benötigt, insbesondere, wenn ein Unternehmen eine Vielzahl von Geräten mit unterschiedlichen Softwareversionen unterhält. Auch der Aufwand, die richtigen

...JETZT AUF WINDOWS 11 MIGRIEREN?

Tools zu finden, um beispielsweise die Software-Kompatibilität zu überprüfen, kann mitunter groß sein. Es lohnt sich aber zumeist, da der geringere Supportbedarf die vorher getätigten Zeitinvestitionen wieder wettmachen kann.

Lohnend – aber für wen?

Doch bei all diesen Faktoren stellt sich wiederum die Frage: Für wen lohnt sich die Migration via Unified Endpoint Management (UEM)? Allen voran für die, die noch über kein UEM verfügen und mindestens 50 Endgeräte betreiben. Ab dieser Zahl ist die Wahrscheinlichkeit hoch, dass durch die gesparte Arbeitszeit der finanzielle Aufwand für die Einrichtung einer UEM-unterstützten Migration geringer ausfällt als bei einer händischen Einrichtung. Darüber hinaus werden durch die automatisierte Softwareinstallation Fehlkonfigurationen deutlich unwahrscheinlicher. Der Mensch ist meist der größte Unsicherheitsfaktor. Daher bringt eine händische Migration aller Geräte erhebliche Risiken mit sich. Mithilfe einer zentralen Verwaltung des Bitlocker lässt sich zudem unter anderem die Passwortstärke – eine der häufigsten Schwachstellen – definieren. Hierfür kann zum Beispiel der Einsatz einer PIN und ihre erforderliche Stärke voreingestellt und kontrolliert werden.

Alexander Haugk, Senior Product Manager Baramundi Software

Bild: Mitel

MARKUS HENK,
Managing Director von Mitel Germany:

„UC-Lösungsanbieter und Reseller müssen als ‚Enabler' funktionieren. Denn es ist deutlich, dass der Erfolg von hybridem Arbeiten mit der Collaboration-Lösung steht und fällt."

„ES GIBT IN DER GESCHÄFTSKOMMUNIKATION KEIN ONE-SIZE-FITS-ALL"

Die Unternehmenskommunikation hat einen erheblichen Anteil am Erfolg und am Wachstumspotenzial eines Unternehmens. Nach fast 50 Jahren im Geschäft weiß auch UCC-Spezialist Mitel davon zu berichten und blickt im Interview mit funkschau auf Entwicklungen und Trends im Bereich der Unternehmenskommunikation.

Interview: Diana Künstler

➤ ***funkschau:*** *Herr Henk, Sie sind nun seit knapp zwei Jahren Deutschlandchef von Mitel. Seitdem hat sich einiges getan in Sachen Unternehmenskommunikation. Wie schätzen Sie die Entwicklungen am Markt in den letzten zwei Jahren ein?*

Markus Henk: Angesichts der Pandemie und der vielen Herausforderungen, mit denen sich Unternehmen in den vergangenen zwei Jahren konfrontiert sahen, sind UCC-Lösungen heute eine entscheidende Komponente für den Erfolg und das Wachstum von Unternehmen. Eine aktuelle globale Studie, die von Mitel gesponsert wurde, bestätigt, dass 74 Prozent der deutschen Unternehmen der Meinung sind, dass die Unternehmenskommunikation entscheidend ist, um ungenutztes Wachstumspotenzial freizusetzen. Sie zeigt aber auch, dass obwohl die Pandemie weithin als Katalysator für die digitale Transformation angesehen wird, die letzten zwei Jahre zu einer Verlangsamung von Unternehmensmodernisierungen geführt haben. Vor allem in Deutschland sahen sich 36 Prozent der Unternehmen gezwungen, ihren Schwerpunkt auf andere Prioritäten zu verlagern. Nur 29 Prozent der deutschen Unternehmen haben während der Pandemie eine Beschleunigung ihrer Modernisierungspläne festgestellt.

funkschau: *Inwiefern unterstützt Mitel hier?*

Henk: Mitel unterstützt seine Kunden auf jedem Schritt ihrer Kommunikationsreise. Wir wissen, dass Unternehmen die Flexibilität benötigen, ihren eigenen Weg zu wählen, sei es vor Ort, in der Cloud oder in einer Kombination aus beidem. Es gibt keinen einheitlichen Ansatz für die Unternehmenskommunikation, der für alle passt. So stellt Mitel sein flexibles, modernes Portfolio auch auf unterschiedliche Art und Weise zur Verfügung, sei es über ein CapEx- oder OpEx-Modell. Anfang dieses Jahres hat Mitel zudem abonnementbasierte Angebote für alle Flaggschiff-Plattformen seines globalen Portfolios eingeführt. Um unser Portfolio zu komplettieren, sind wir eine strategische Partnerschaft mit Ringcentral, dem Marktführer im Bereich UCaaS, eingegangen.

Als Teil seiner Unternehmensstrategie legt Mitel auch einen Schwerpunkt auf das Customer Lifecycle Management (CLM), welches eine Schlüsselrolle im Auswahlprozess von UC-Lösungen spielt. Denn es unterstützt Unternehmen bei der Auswahl eines geeigneten Stacks auf Basis ihrer Bedürfnisse. Mitel arbeitet daher eng mit Vertriebspartnern zusammen und nutzt Daten und Analysen, um festzustellen, wo die Kunden sich auf ihrer Lifecycle-Management-Reise befinden.

funkschau: *Welche Learnings und Entwicklungsschritte haben das Unternehmen zu dem gemacht, was es heute ist? Schließlich feiert man im kommenden Jahr 50-jähriges Bestehen.*

Henk: Das stimmt, wir sind sehr stolz darauf. Es gibt nicht viele Unternehmen in der Technologiebranche, die so lange dabei sind. Bei Mitel blicken wir auf eine lange Innovationskultur zurück: Als langjäh-

riger Akteur in der Kommunikationsumfeld hat Mitel in den fast 50 Jahren seiner Geschäftstätigkeit bei zahlreichen Technologien Pionierarbeit geleistet, sei es das Angebot von offenen Schnittstellen, die Kommunikation zwischen Telefonen und PCs über USB, hybriden Cloud-Lösungen oder antimikrobiellen DECT-Handsets. Auch heute treiben wir innovative Produkt- und Markteinführungsmodelle voran, um unseren Kunden auf der ganzen Welt die flexibelsten und zukunftssichersten Lösungen anbieten zu können.

Im Laufe der Jahre haben wir ein tiefgreifendes Verständnis für die Bedürfnisse von Unternehmen und die Branchen, in denen sie agieren, entwickelt. Wir sind der Überzeugung, dass es in der Geschäftskommunikation keine „One-Size-fits-all"-Lösung gibt und dass wir unsere Kunden nur durch die Bereitstellung von Auswahlmöglichkeiten am besten beim Erreichen ihrer Geschäftsziele unterstützen können.

Nicht zuletzt möchte ich die Teamkultur bei Mitel hervorheben. Unsere Teams auf der ganzen Welt und in Deutschland sind definitiv eine unserer Stärken. Sie bringen ein hohes Maß an Leidenschaft für ihre Arbeit und Technologie im Allgemeinen mit. Einige von ihnen arbeiten schon seit vielen Jahren zusammen und haben starke Beziehungen zu ihren Kollegen und unserer Partner-Community aufgebaut, was die tägliche Arbeit reibungslos macht.

funkschau: *Vor Kurzem hat Mitel die Ergebnisse einer Tech Aisle-Studie bekanntgegeben, die die Modernisierung des Arbeitsplatzes von rund 1.300 Unternehmen in Australien, Frankreich, Deutschland, Großbritannien und den USA beleuchtet. Was sind die Haupterkenntnisse der Befragung, die übergreifend für alle Länder zutreffend sind?*

Henk: Ein zentrales, länderübergreifendes Ergebnis der Studie ist, dass sich trotz der gesammelten Erfahrungen der letzten beiden Jahre noch immer keine „Hybrid First"-Denkweise durchgesetzt hat: Gerade einmal elf Prozent der befragten Unternehmen legen eine solche an den Tag. Dabei wünschen sich 44 Prozent der Mitarbeiter, an mindestens drei bis vier Tagen in der Woche von zuhause zu arbeiten. Es zeigt sich also, dass der Weg zu einem dauerhaften hybriden Modell noch lange nicht beschritten ist. Es gibt immer noch Hindernisse zu überwinden. Unternehmen müssen zudem mehr in die UC-Modernisierung investieren, um hybride Arbeitsmodelle zu unterstützen.

Dies ist umso wichtiger vor dem Hintergrund, dass die Umfrage auch eine Diskrepanz zwischen Arbeitgebern und Arbeitnehmern in Bezug auf die Wahrnehmung und die Auswirkungen des hybriden Arbeitens auf ihr Berufs- und Privatleben ergab.

funkschau: *Worauf ist diese Diskrepanz in Nachfrage und Angebot Ihrer Meinung nach zurückzuführen?*

Henk: Auffällig ist hier, dass die Erwartungen und Wahrnehmung von hybriden Arbeiten zwischen Arbeitgebern und -nehmern stark auseinander gehen. 51 Prozent der Arbeitnehmer sind besorgt um ihre Work-Life-Balance, doch nur 24 Prozent der Arbeitgeber teilt diese Sorge. 36 Prozent der Arbeitgeber befürchten hingegen Produktivitäts- und Konzentrationsverluste, eine Wahrnehmung, die wiederum von nur 26 Prozent der Arbeitnehmer geteilt wird.

Obwohl es eine übereinstimmende Auffassung darüber gibt, dass Collaboration-Tools der Schlüssel zu einem effektiven hybriden Modell sind, ist das Konzept der hybriden Arbeit für viele Unternehmen noch sehr neu. Auch gibt es immer noch Hindernisse, die eine breitere und schnellere Umsetzung von wirkungsvollen Modernisierungsinitiativen verhindern. So führt die Komplexität zu einer gewissen Entscheidungsträgheit, da die Kunden versuchen, die beste Wahl zwischen einer Vielzahl von Lösungen, Technologien und Kaufmodellen zu treffen. Der Mangel an betrieblicher Flexibilität, die Angst vor Sicherheitslücken und Unfähigkeit, Anwendungen und Systeme in die Cloud zu migrieren, sind ebenfalls entscheidende Hindernisse für die UC-Modernisierung.

funkschau: *Was zeichnet speziell die befragten Unternehmen mit Sitz in Deutschland aus?*

Henk: In den meisten Punkten unterscheiden sich die Antworten deutscher Unternehmen oft nur um wenige Prozentpunkte von den internationalen Ergebnissen. Insgesamt sehen sich deutsche Unternehmen ähnlich gut aufgestellt in Sachen Heimarbeit und die dafür benötigten Voraussetzungen wie andere internationale befragte Unternehmen. In Deutschland sehen sich sogar 47 Prozent der Befragten (44 Prozent international) mit den benötigten Kompetenzen ausgestattet, um flexible Heimarbeit zu ermöglichen. Sie messen dieser jedoch auch einen höheren Stellenwert bei als im internationalen Vergleich. So bewerten 53 Prozent der Unternehmen Flexibilität der Arbeitszeiten als eine der wichtigsten Initiativen zur Förderung produktiver Mitarbeiter, gegenüber nur 46 Prozent international. Auf der anderen Seite sind deutsche Arbeitgeber im Vergleich besorgter, was ihre Fähigkeiten im Hinblick auf das Management von Mitarbeitern im Homeoffice angeht (55 Prozent in Deutschland gegenüber 50 Prozent weltweit).

funkschau: *Was sollten zeitgemäße Lösungen für die Unternehmenskommunikation leisten können, um Firmen bei der Bewältigung ihrer drängendsten Herausforderungen unterstützen zu können?*

Henk: UC-Lösungsanbieter und Reseller müssen hier als „Enabler" funktionieren. Denn es ist deutlich, dass der Erfolg von hybridem Arbeiten mit der Collaboration-Lösung steht und fällt. So geben 77 Prozent der befragten Arbeitnehmer an, dass bessere Kommunikations- und Collaboration-Tools ihnen helfen, ihre Arbeit effektiver und zielführender zu erledigen, während nur 34 Prozent der Arbeitgeber der Ansicht sind, ausgereifte Maßnahmen für die Heimarbeit zu haben.

Eine wichtige Erkenntnis in diesem Zusammenhang ist, dass es keine fertige Patentlösung gibt. Jedes Unternehmen hat, abhängig von Branche, Größe und anderen Faktoren, unterschiedliche Bedürfnisse. Die Komplexität bei der Auswahl der passenden Lösung kann überwältigend sein – von der Umsetzung hybrider Arbeitsformen über die Auswahl der richtigen Kommunikations- und Collaboration-Tools bis hin zur Schaffung einer Kultur, die dafür sorgt, dass Mitarbeiter zufrieden und engagiert bleiben.

Hier kommen UC-Lösungsanbieter zusammen mit Channel-Partnern ins Spiel: Sie sind nicht nur diejenigen, die Lösungen bereitstellen, sondern auch Kunden bei der Suche nach einer maßgeschneiderten Lösung helfen. In ihrer Funktion als Wegbegleiter können sie Unternehmen bei ihrer Modernisierungstransformation unterstützen. Diese sollte eine UC-Lösung mit fünf Schlüsselattributen umfassen: agil, anpassungsfähig, transformativ, flexibel und befähigend.

EIN ENDE DER EWIGEN WARTESCHLEIFE

Bild: AdobeStock-Australianimage

Warten, warten, warten: So erleben viele Verbraucher die ganz normale Schadensregulierung bei der Hotline ihrer Versicherung. Der qualvolle Prozess verdeutlicht: Die traditionelle Schadensregulierung ist veraltet. Verbraucher verlangen schnelle Lösungen, am besten rund um die Uhr. Ein digitales und automatisiertes Claim Management soll diese Erwartungen erfüllen.

Autor: Rasmus Lynge ***Redaktion: Diana Künstler***

➤ Versicherte, die versuchen, einen Schadensfall zu melden, kennen das: lange Wartezeiten am Telefon, dann Unterlagen und Fotos per Mail oder Kontaktformular einreichen, wieder anrufen, wieder warten, nochmal fehlende Unterlagen schicken, erneut anrufen und wieder warten – bis die Versicherung dann endlich den Betrag auszahlt. Genau diese langwierigen Prozesse führen dazu, dass sich Verbraucher eine alternative Assekuranz suchen, schließlich wirken sich mangelnde Erreichbarkeit und zunehmende Wartezeiten besonders negativ auf die Customer Journey aus.

Um die riesige Lücke zu schließen, die zwischen den Erwartungen der Verbraucher und der Schadensregulierung klafft, müssen Versicherungen ihre Prozesse automatisieren und beschleunigen. Eine mögliche Lösung ist ein digitales Claim Management, das alle Schritte des Schadenmanagments effizienter gestalten soll – von der Aufnahme des Vorfalls bis hin zur Abwicklung der Zahlung. Digitales Claim Management kommt den Gewohnheiten der Versicherten entgegen, weil sie in Customer-Self-Service-Angeboten Schäden melden können, ohne dafür lange Zeit in einer Warteschleife zu hängen.

Auch für die Versicherung bietet das digitale Claim Management gegebenenfalls Vorteile, denn das Verfahren erleichtert in vielen Fällen die Dokumentation des Schadenfalles. Dieser wird direkt digital erfasst und die Informationen stehen allen Beteiligten zur Verfügung. Die strukturierte Speicherung von Daten erlaubt einerseits ein ausführliches Reporting der Schadensfälle für die Geschäftsführung und entlastet andererseits die Mitarbeiter der Versicherung.

Unterstützung durch KI

Ein wichtiger Beschleuniger des digitalen Schadensmanagement ist der Einsatz von Künstlicher Intelligenz. Das gilt vor allem für das automatisierte Erkennen von Betrugsversuchen. Durch moderne Technologien ist das System in der Lage, gescannte oder digitalisierte Dokumente in vordefinierte Kategorien einzuordnen und selbstständig relevante Informationen zu selektieren, die für die Bearbeitung des Schadensfalls erforderlich sind. Dadurch entfallen papierbasierte und vor allem manuelle und fehleranfällige Evaluierungsvorgänge. Die ML-Frameworks verfügen zudem meist über eine so große Datengrundlage, dass Betrugsversuche schneller aufgedeckt werden, weil das System bei verdächtigen Daten Alarm schlägt und menschliche Interaktion einfordert. Mitarbeiter müssen bei automatisierten Vorgängen somit nur noch eingreifen, wenn das System etwa wegen eines Betrugsversuchs Warnung schlägt.

Kapazitäten skalieren

Allerdings sollte nicht nur die Entlastung des Personals für Versicherungen ein Anreiz sein, in die Digitalisierung der internen Abläufe zu investieren. So können sich beispielsweise cloudbasierte Systeme für das Schadensmanagement flexibel skalieren lassen. Gibt es also gerade ein besonders hohes Aufkommen an Schadensmeldungen, zum Beispiel durch extreme Wetterlagen, können Versicherungen die Kapazitäten ihres digitalen Claim Managements entsprechend anpassen.

Rasmus Lynge ist Chief Product & Technology Officer bei Fadata

WENN DER LIEFERANT ZUM SICHERHEITSRISIKO WIRD

Autor: Jonas Rahe Redaktion: Stefan Adelmann

➤ In Deutschland waren gemäß einer aktuellen Untersuchung von Trend Micro bereits 43 Prozent der Unternehmen von einem Ransomware-Angriff in der Lieferkette betroffen, weltweit sogar über die Hälfte. Dass die Supply Chain immer stärker in den Fokus von Cyberkriminellen gerät, hat einen guten Grund: Sie greifen häufig das schwächste Glied einer Kette an.

Bild: Cisco

JONAS RAHE,
Direktor Öffentliche Hand und verantwortlich für IT-Security in der Geschäftsleitung von Cisco Deutschland.

Im Vergleich zu ihren Großkunden sind deren Lieferanten oft kleine und mittelständische Unternehmen, deren IT-Systeme nicht perfekt abgesichert sind. Mit größer werdendem Zulieferer-Netz steigt also auch das Risiko einer Infiltration durch eigentlich vertraunenswürdige Partner. Für Angreifer ist das doppelt attraktiv, da sich so mit vergleichsweise wenig Aufwand ein Angriff skalieren und großer Schaden anrichten lässt. So wirkte sich im letzten Jahr zum Beispiel ein Ransomware-Angriff auf VSA, die Software für Remote Management der Firma Kaseya, auf 1.500 bis 2.000 Unternehmen aus. Unter anderem musste die Supermarktkette Coop Läden schließen, da die Kassensysteme ausfielen.

Mindestmaß an Sicherheit nötig

Schon 2011 hat Wendy Nather, heute Head of Advisory CISOs bei Cisco, auf Basis dieses Zusammenhangs das Konzept der „Armutsgrenze für Cybersicherheit“ entwickelt. Es besagt, dass in einem vernetzten System jedes Mitglied ein Mindestmaß an Sicherheit erfüllen muss. Wer es nicht erreicht, fällt unter die Armutsgrenze und gefährdet damit das gesamte System. Um nicht unbemerkt unter die Cybersicherheits-Armutsgrenze zu rutschen, sollten Unternehmen auf folgende vier Bereiche achten:

Budget: Eigentlich sollte im reichen Deutschland die Absicherung von IT-Systemen keine Geldfrage sein. Doch viele Unternehmen haben knappe Gewinnmargen oder schreiben sogar Verluste. Diese investieren nur selten in hochentwickelte Cybersicherheitssysteme.

Fachwissen: Wer ausreichend Budget bereitstellt, verfügt nicht automatisch auch über die erforderliche Expertise. Zwar lassen sich externe Partner einbinden. Jedoch muss das Unternehmen selbst genügend Know-how besitzen, um zwischen zielführenden Vorschlägen und Geschäftemacherei unterscheiden zu können.

Fähigkeit zur Umsetzung: Die besten Ideen nützen wenig, wenn sie sich nicht umsetzen lassen. Inkompatible Software und Hardware verhindern oft den Einsatz moderner Security-Systeme. Cloud-basierte Sicherheitslösungen dürfen zum Teil aus Compliance-Gründen nicht genutzt werden.

Marktposition. Während Konzerne meist günstige Bedingungen aushandeln, müssen kleine Unternehmen die regulären Preise zahlen. Vor allem die individuelle Anpassung der Lösungen an die eigenen Bedürfnisse bleibt dann auf der Strecke – oder erfolgt in Eigenregie. Das kann aber zu neuen Schwachstellen führen.

Dieser Überblick zeigt, dass die Cybersicherheits-Armutsgrenze kein Problem ist, dass man nur mit Geld lösen kann. Im Gegenteil: Sogar im gut aufgestellten Deutschland kann und wird das viele Unternehmen treffen. Aus verschiedenen Gründen schaffen sie es nicht, die erforderlichen Mindeststandards für Sicherheitsmaßnahmen umzusetzen. Aber das gefährdet nicht nur sie selbst, sondern aufgrund der umfassenden Vernetzung auch das Gesamtsystem, insbesondere ihre Partner und Kunden.

Eine umfassende Security-Strategie muss nicht nur Angriffe abwehren, sondern auch ungewollte Kompromittierungen durch Partner-Unternehmen erkennen.

Geeignete Maßnahmen

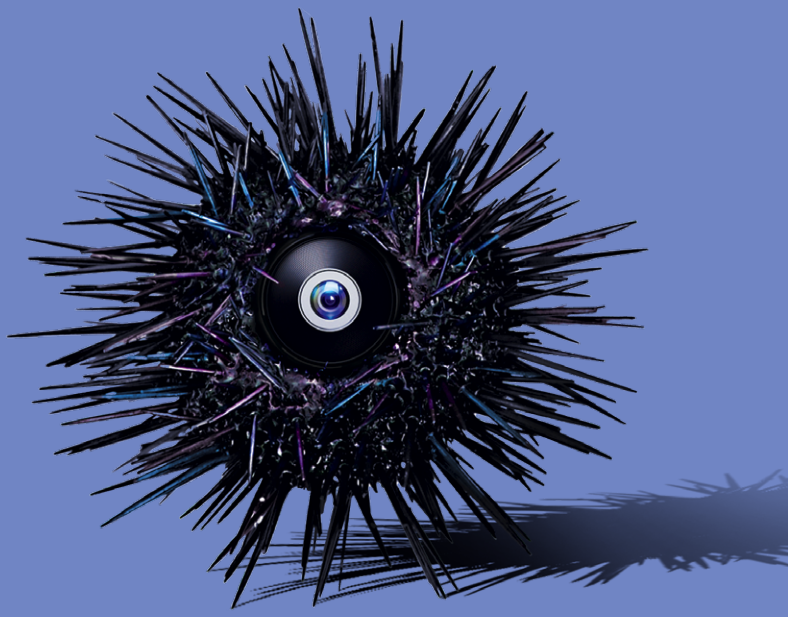
Diese Einschätzung bestätigen auch Ciscos IT-ForensikerInnen von Talos. Ihre Empfehlung: Jedes Unternehmen sollte davon ausgehen, früher oder später erfolgreich angegriffen zu werden. Daher muss eine umfassende Security-Strategie nicht nur Angriffe abwehren, sondern auch ungewollte Kompromittierungen durch Partner-Unternehmen erkennen, etwa durch ungewöhnlichen Datenverkehr. Darum sollten Unternehmen nicht nur die eigene IT-Security im Blick behalten, sondern auch die ihrer Geschäfts- und Netzwerkpartner.

Gerade für den eng verwobenen Channel ist das Thema zentral. Darum braucht es eine konzertierte Aktion von IT-Industrie, Partnern und Distributoren. Nur so können alle Elemente der IT-Wertschöpfung abgesichert werden.

GELEBTE SICHERHEIT

Die IT-Sicherheit ist ständig bedroht, Unternehmen und Organisationen zu schützen eine Daueraufgabe. Um dies zu bewältigen, sind Lösungen nötig, die eine produktive Symbiose zwischen IT-Security-Teams und der verwendeten Technologie ermöglichen.

Autorin: Tanja Hofmann ***Redaktion: Diana Künstler***



➤ Unternehmen sehen sich großen Sicherheitsherausforderungen gegenüber. Nach einer aktuellen Pressemeldung des Branchenverbandes Bitkom entstehen in Deutschland allein 203 Milliarden Euro Schaden durch Cyber-Angriffe. Neun von zehn Unternehmen sind von Attacken aus dem digitalen Raum betroffen. Dabei werden die Angriffe laut den Daten professioneller: 2022 wurden bereits 51 Prozent von ihnen von Kriminellen und Banden begangen – ein Jahr zuvor waren es noch 29 Prozent. Das bedeutet: Die Angriffe werden gezielter, komplexer und professioneller. Wenig verwunderlich, sehen sich im Schnitt 42 Prozent der Anwender in Zukunft stärker bedroht als heute – von den Unternehmen, die zur kritischen Infrastruktur zählen, glauben dies sogar 51 Prozent.

Fachkräfte, die fehlende Ressource

Um dieser Bedrohungslawine Herr zu werden, sind zwei harmonisch zusammenwirkende Faktoren erforderlich: Geschulte, motivierte IT-Security-Teams und anpassbare Lösungen, die ihnen die Arbeit erleichtern. Tools allein können niemals entscheiden, ob ein Angriff oder eine Sicherheitslücke tatsächlich substantiell und bedrohlich ist. Menschen allein sind mit der Flut der Angriffe und der daraus resultierenden Anzahl von Events hingegen schlicht überfordert.

Doch um beide Faktoren steht es heute nicht zum Besten. Zum einen fehlen Fachkräfte. Eine Untersuchung von Vanson Bourne, die das Marktforschungsunternehmen im Auftrag von Trellix bei Unternehmen in der ganzen Welt durchführte, kam zu einem alarmierenden Ergebnis: 85 Prozent der Befragten glauben, dass durch den Mangel an IT-Sicherheitspersonal die Sicherheit ihres Unternehmens gefährdet ist. Eine aktuelle Studie zum globalen IT-Security-Arbeitsmarkt, die vom weltweiten Verband der IT-Security-Spezialisten (ISC)² durchgeführt wurde, kommt wiederum zu dem Ergebnis, dass vor allem Spezialisten für sichere Bereitstellung von Systemen und Apps, Analyse, Schutz und Abwehr fehlen. Jeweils knapp die Hälfte der Befragten bezeichnete diese Qualifikationen als besonders rar. Das führe unter anderem zu Fehlkonfigurationen (32 Prozent), unzutreffenden Risikoeinschätzungen (30 Prozent), verzögertem Patching (29 Prozent) und anderen Problemen, die es Angreifern leicht machen.

Doch auch die verwendeten Produkte sind nur partiell hilfreich. In den meisten Unternehmen stehen zahlreiche Punkt-Werkzeuge für Spezialaufgaben unverbunden nebeneinander. Jedes mit eigener Bedienphilosophie, Alerts, Lizenzen und Wartungsverträgen. Die Folge: Überlastete Teams kommen mit der Arbeit nicht mehr hinterher. Statt strategische Überlegungen anzustellen, befassen sie sich damit, Alert-Massen abzuarbeiten. So bleiben Angriffe oft viel zu lange unentdeckt.

Gegenmaßnahmen müssen an beiden Seiten ansetzen: Zwar ist die Motivation der Security-Teams laut der Trellix-Untersuchung sehr hoch – 92 Prozent sagen, dass IT-Security motivierend, sinnvoll und geistig anspruchsvoll sei. Doch ein gutes Drittel der Befragten fühlt sich wenig wertgeschätzt. Besondere Bedeutung messen die Befragten der Aus- und Weiterbildung bei. So wünschen sich 85 Prozent mehr Unterstützung bei der Weiterentwicklung ihrer Fähigkeiten. Doch selbst wenn diese gewährt wird, kann das den akuten Mangel nicht beseitigen, denn Aus- und Weiterbildung brauchen Zeit.

Intelligenz und Lernfähigkeit bringen das IT-Team vor die Welle

Deshalb ist der am schnellsten wirksame Hebel zur Erleichterung der Sicherheitsprobleme die Implementierung möglichst effektiver Sicherheitslösungen. Zu nennen sind hier insbesondere XDR-Plattformen (Extended Detection and Response). Diese neue Systemklasse entstand aus Endpoint-Security-Lösungen, erweitert sie aber um viele neue Funktionen. Vor allem machen XDR-Lösungen aber Schluss mit dem Stückwerk in der Security-Toolbox vieler Unternehmen. Sie bringen meist zahlreiche fortschrittliche Funktionen mit. Gleichzeitig sollten entsprechende Lösungen aber offene Schnittstellen besitzen, über die bereits vorhandene Sicherheitsprodukte so in die Gesamtlösung eingebunden werden können, dass sie mit der gesamten IT-Security-Landschaft des Unternehmens unter dem Dach der Plattform synergistisch zusammenwirken – statt jeweils alleine vor sich hinzuarbeiten.

Die wichtigste neue Funktionsklasse, die sich in zahlreichen XDR-Lösungen findet, ist die Nutzung von AI (Artificial Intelligence, Künstliche Intelligenz) und ML (Maschinelles Lernen). Durch diese Mechanismen können die Systeme Vorfälle in einen Kontext setzen und aus den gesammelten Daten lernen. Denn nur Softwareintelligenz und Lernfähigkeit ermöglichen es, sicher einzuschätzen, ob eine Abweichung vom normalen Betrieb der Systeme oder ein Alert Besorgnis erregen sollte oder aber ignoriert werden kann, weil kein geschäftsrelevantes Risiko ersichtlich ist. Nur so lässt sich mit der großen Veränderungsrate digitaler Schädlinge mithalten.

Vor allem aber wird durch solche Mechanismen verhindert, dass sich kriminelle Elemente längere Zeit unentdeckt in der Infrastruktur ausbreiten können und dann im ungünstigsten Moment zuschlagen – etwa, indem sie Systeme und Back-ups mit Ransomware verschlüsseln. Gleichzeitig ermöglicht intelligente Software schon im Vorfeld zu erkennen, an welchen Stellen relevante Risiken lauern könnten, sodass das Unternehmen diese bestenfalls entschärfen kann, bevor ein sicherheitsrelevanter Zwischenfall eintritt.

Automatisierung und Schutz digitaler Assets

Ein weiterer Pluspunkt entsprechender Systeme sind vordefinierte Playbooks und Automatisierungsroutinen. Sie helfen den IT-Spezialisten, im Angriffsfall nicht irgendetwas zu tun, sondern genau das Richtige. Vor allem wird durch schnelle und treffende Reaktionen ohne große Vorbereitung verhindert, dass Eindringlinge weiteren Schaden anrichten können: Die XDR-Lösung isoliert Angreifer respektive Angriffsvektoren, verfolgt sie zurück soweit möglich und hält sie insbesondere von werthaltigen Ressourcen fern.

Besonders wichtig ist in einer Zeit, in der Daten als „das neue Gold“ gelten, dass ein XDR-System die vorhandenen digitalen Assets schützt. Dazu dienen DLP (Data Loss Prevention)-Funktionen. Sie sind gewissermaßen das Wachportal am Zugang zu allen digitalen Daten mit Wert. DLP-Funktionen sollten alle Daten-Assets innerhalb des Unternehmens selbständig entdecken und qualifizieren können. Sie sollten imstande sein, nach einem unternehmensspezifischen Regelwerk Zugriffsrechte durchzusetzen oder aber zu sperren und alle Aktionen, die sich auf entsprechende Dokumente beziehen, zu protokollieren. Außerdem ist es unerlässlich, dass die DLP-Funktion innerhalb eines XDR-Systems Berichte entsprechend den einschlägigen Sicherheits- und Compliance-Normen, etwa der GDPR (General Data Protection Regulation oder auch Datenschutz-Grundverordnung), automatisiert und schnell erstellen kann. Dann sind Compliance-Prüfungen kein Schreckgespenst mehr am Horizont.

Mit solchen Werkzeugen und unter solchen Bedingungen können Security-Teams anstehende Anforderungen besser bewältigen. Tools, die die Aufmerksamkeit auf das wirklich Relevante lenken, schaffen Raum für sinnvolle strategische Planungen, den Schutz wertvoller Daten und die Sensibilisierung aller Mitarbeiter für eine Aufgabe, zu deren Lösung letztlich jeder im Unternehmen beitragen muss: dem Schutz der IT-Infrastruktur und der digitalen Assets.

Tanja Hofmann, Lead Security Engineer bei Trellix

Die größten Herausforderungen für Cybersicherheit und Risikominderungsinitiativen laut CROs & CISOs (n = 607)	Rang
Fähigkeiten zur Verwaltung, Entwicklung und Unterstützung von Cybersicherheitstechnologie	1
Änderungen/Anforderungen der Belegschaft (z.B. Arbeiten von zu Hause aus, BYOD usw.)	2
Bewertung von Cyberrisiken und Kalkulation relevanter Kosten	3
Vertrauen in alte IT-Systeme	4
Akkumulierte Komplexität eigener Geschäftsprozesse und -operationen	5
Schwierigkeiten beim Nachweis der Rendite von Cybersicherheitsinvestitionen	6
Mangelnde Zusammenarbeit zwischen den Unternehmenseinheiten (Geschäft, IT und Sicherheit)	7
Mangelnde Diversität (einschließlich Denken und Erfahrung) bei Mitarbeitern, die Cyberrisiken und -bedrohungen bewerten	8
Schwierigkeiten bei der Vorgabe, dass derzeitige Anbieter fortschrittliche Technologien und Richtlinien übernehmen	9
Budgetbeschränkungen	10
Gegensätzliche Interessen mit Blick auf Vorstand oder Geschäftsleitung	11
Veraltete, isolierte und nicht integrierte Sicherheitstools	12

Quelle: Cybersecurity Study – Master Report, 2022

Mit der zunehmenden Digitalisierung steigt auch die Bedrohung durch Cyberangriffe. Daher sind IT-Sicherheitsexperten aktuell besonders gefragt: Der „Risk & Cybersecurity Studie 2022“ des IT-Beratungsunternehmens Tata Consultancy Services (TCS) zufolge sehen Unternehmen die größte Herausforderung im Bereich Cybersicherheit nicht etwa im Budget, sondern im Mangel an Fachkräften mit einschlägiger Expertise. Chief Risk Officers (CROs) und Chief Information Security Officers (CISOs) berichten in der Umfrage, dass es ihnen bereits im vergangenen Jahr schwerfiel, Talente mit Kenntnissen in den Bereichen Cyberrisiken und -sicherheit für sich zu gewinnen (44 Prozent) und zu halten (42 Prozent). Als zweitgrößte Hürde nennen die CROs und CISOs die Anforderungen an das Arbeitsumfeld wie beispielsweise das Homeoffice und die damit verbundenen Risiken. So mussten den Mitarbeitern aufgrund der Pandemie und dem daraus folgenden Wechsel ins Homeoffice unter anderem kurzfristig zahlreiche Fernzugriffe auf die Systeme und Datenbanken ihres Arbeitgebers ermöglicht werden. Das eröffnet für Cyberkriminelle neue Angriffspunkte. Die diversen Sicherheitsrisiken zu bewerten sowie ihre Kosten zu quantifizieren, stellt für die Befragten die drittgrößte Herausforderung dar.

FRISCHER ANSTRICH FÜR DEN PENTEST

Um Maßnahmen für die Cybersicherheit auf die Probe zu stellen, sind Pentests eine bewährte Methode. Mithilfe dieser Tests lässt sich praxisnah prüfen, wie gut ein Unternehmen gegen Cyberangriffe gewappnet ist. Beim klassischen Pentest arbeiteten rote und blaue Teams meist getrennt voneinander. Anders hingegen beim Purple Teaming: Diese Methode hebt den Pentest auf eine neue Stufe, indem sie auf Transparenz und Kollaboration anstelle isolierter Teams setzt.

Autor: Gergely Lesku

Redaktion: Diana Künstler

➤ Managed Security beinhaltet heute viele verschiedene Komponenten und Methoden. Wer seine Security-Infrastruktur dabei nicht nur in der Theorie, sondern auch in der Praxis auf Herz und Nieren prüfen möchte, greift häufig aufs Pentesting zurück. Denn auch die am besten durchdachten Sicherheitsmaßnahmen können Schwachstellen aufweisen. Diese lassen sich nur durch einen praktischen Test erkennen. Das Pentesting hat sich dabei als geeignete Bewährungsprobe erwiesen. Doch auch Altbewährtes muss weiterentwickelt werden. Das Purple Teaming-Verfahren tritt an, den nächsten Entwicklungsschritt für das Pentesting zu gehen.

Klassisches Pentesting: realitätsnah durch isolierte Teams

Das Grundprinzip eines Pentests war bislang so einleuchtend wie erprobt: Es wurde ein möglichst realitätsnahes Angriffsszenario durchgespielt und die Sicherheitsmaßnahmen hinsichtlich Effektivität und Reaktionsgeschwindigkeit getestet. Eine Gruppe aus ethischen Hackern nahm dabei die Rolle der „Angreifer“ ein. Ihr Ziel war es, die Schutzmauern zu überwinden, die von einer Gruppe aus Sicherheitsexperten, dem blauen Team, verteidigt wurde. Verschiedene Pentests unterschieden sich vor allem in den getesteten Angriffsmustern oder darin, wie viel das rote Team über die Sicherheitsstrukturen im Vorfeld wissen sollte (Blackbox vs. Whitebox). Eines hatten aber so gut wie alle Pentestmethoden gemeinsam: Red Team und Blue Team agierten unabhängig voneinander und verdeckt, um das Szenario möglichst nah an der Realität zu halten. Diese Art der Tests lieferte vorrangig Aussagen über die technische Bereitschaft der geprüften Systeme.

Trotz aller Vorteile ist es nicht das Ziel, herkömmliche Pentests durch Purple Teaming zu ersetzen. Je nach Situation kann es auch sinnvoll sein, dass die Teams eigenständig arbeiten und die Testumgebung so näher an der Realität liegt. Vielmehr entwickelt das Purple Teaming das traditionelle Pentesting weiter.

Größerer Lerneffekt durch Kooperation

Die Grundidee des Purple Teamings versteckt sich bereits im Namen. Denn anders als beim klassischen Pentest wird beim Purple Teaming das Kooperationsverbot zwischen rotem und blauem Team aufgeweicht. Anstatt beide Gruppen isoliert voneinander arbeiten zu lassen, agieren beim Purple Teaming beide transparent. Macht das rote Team also den ersten Schritt und beginnt mit dem Angriff, informiert es das blaue Team dabei über die verfolgte Strategie und die eingesetzten Techniken. Das blaue Team kann nun erkennen, wie gut die eingesetzten Security-Tools funktionieren und ob die für einen solchen Fall geschaffenen Abläufe sinnvoll und effektiv geplant sind. Dabei misst es bestimmte Werte, die als Indikatoren dienen. Die gesammelten Metriken werden nun mit der Incident Response-Strategie aus der Theorie abgeglichen und ihre Effektivität in der Praxis evaluiert.

Der Vorteil dieser neugewonnen Transparenz liegt in der Genauigkeit der Auswertung. Denn natürlich wird auch beim traditionellen Pentest die Wirkungskraft der eigenen Strukturen analysiert, das ist schließlich Sinn und Zweck der gesamten Methode. Purple Teaming erreicht jedoch ein neues Level an präziser Aussagekraft. Denn anstatt nur zu überprüfen, ob ein Angriff funktioniert hat, ist direkt erkennbar, wo die Schwachstellen liegen und in welcher Phase der Attacke das System durchlässig war. Teilt das rote dem blauen Team während des Angriffs direkt mit, wo eine Sicherheitslücke liegt, spart es dem blauen Team Zeit und Energie, da das blaue Team direkt die existenten Schwachstellen beseitigen kann.

Ein weiterer Pluspunkt des Purple Teamings liegt in der Wiederholbarkeit. Denn liegen alle Angriffspläne offen, können diese gezielt wiederholt werden und die Verteidiger können im zweiten Anlauf testen, ob ihre aktualisierte Vorgehensweise die Eindringlinge stoppt. Zu guter Letzt bringt Purple Teaming einen enormen Lerneffekt mit sich.

DAS WHO IS WHO DER HACKER:

WER STECKT HINTER APT29?

➤ Das National Cyber Security Centre (NCSC) des Vereinigten Königreichs und das Communications Security Establishment (CSE) Kanadas gehen davon aus, dass es sich bei APT29 – auch bekannt als „The Dukes“ oder „Cozy Bear“ – um eine Cyber-Spionagegruppe handelt, die mit hoher Sicherheit zu den russischen Geheimdiensten gehört.

Entstanden ist die Gruppierung vermutlich im Jahr 2014, als Russland die Krim völkerrechtswidrig annektiert hat. Es kann aber sein, dass die Gruppe schon zuvor aktiv war – Kaspersky Lab beispielsweise hat festgestellt, dass die frühesten Exemplare der „MiniDuke“-Malware, die der Gruppe zugeschrieben werden, aus dem Jahr 2008 stammen. Es wird überdies vermutet, dass die Gruppierung vom Auslandsgeheimdienst (SVR) gesponsert wird. Dafür gibt es jedoch keine handfesten Beweise.

Was als sicher gilt, ist die Tatsache, dass die Spionagegruppe APT29 das Ziel hat, Projekte anzugreifen, die Interessen der USA vertreten. So gehören unter anderem die Nato und deren Partner zu den Angriffszielen der russischen Spionagegruppe APT29. Diese wiederum setzt nach Angaben des Pentest-Anbieters Prosec eine Vielzahl von Instrumenten und Techniken ein, um vorwiegend Ziele in den Bereichen Regierung, Diplomatie, Think Tanks, Gesundheitsfürsorge und Energie anzugreifen, um nachrichtendienstliche Erkenntnisse zu gewinnen.

Zuletzt machte APT29 Schlagzeilen, weil sie vermehrt Angriffe auf Microsoft 365-Accounts startete. Dabei nutzte die Gruppe ihre Fähigkeiten, um Lizenzen zu deaktivieren und die Multi-Faktor-Authentifizierung (MFA) anzugreifen. Die Gruppe hat sich vor allem auf Unternehmen spezialisiert. Private NutzerInnen sind also selten betroffen. Zielobjekte sind Unternehmensdaten, die später weiterverwendet oder manipuliert werden können. *(DK)*

Denn das rote Team unterrichtet die Verteidiger nicht nur über eingesetzte Strategien oder Technologien, sondern erläutert auch Schritt für Schritt, warum sie sich für genau diesen Ablauf entschieden haben. Das blaue Team lernt also auch die Angreifer kennen und ihr Mindset zu verstehen. Etwaiger Betriebsblindheit wird so effektiv entgegengewirkt.

Wie Purple Teaming gelingt

Um Purple Teaming zielführend einzusetzen, müssen einige Aspekte beachtet werden:

▸**Technisches Expertenwissen rund um die Methoden:** Anbieter sollten sich mit den Verfahren sowohl blauer als auch roter Teams auskennen. Darunter fallen etwa die Sicherheitsüberwachung und die Reaktion auf Angriffe, die sogenannte Incident Response, beim blauen oder auch automatisierte Attacken beim roten Team. So können Anbieter final auch die richtigen Content-Einstellungen aufzeigen und andere systemspezifische Tipps geben.

▸**Teamführung und -management:** Da beim Purple Teaming der Lernerfolg im Vordergrund steht und regelmäßig geprüft werden muss, ob sich Fortschritte zeigen, sind bei Anbietern ebenso Kompetenzen in der Führung und im Management von Teams gefragt.

▸**Planung:** Damit die Übung gelingt, ist wie bei allen Pentesting-Methoden auch beim Purple Teaming ein präziser Plan wichtig. Ist das Team besonders gut vorbereitet, haben die Ergebnisse eine höhere Qualität und eine höhere Aussagekraft. Damit das blaue Team bei der finalen Übung eine Idee davon hat, was es erwartet, nutzen die Teams meist eine mehrstufige Cyber Kill Chain bekannter APT-Angreifer, etwa APT29 (siehe Kasten anbei).

Gemeinsam zum Erfolg

Wie sich zeigt, ist es für den Erfolg von Purple Teaming evident, dass beide Teams eng und vollkommen transparent zusammenarbeiten. Dazu gehört zum einen, dass das rote Team offenlegt, wie es warum und mit welchen Verfahren vorgeht. Auf diese Weise lernt das blaue Team die Angreifer und ihre Verhaltensmuster besser kennen. Gleichzeitig sollte das blaue Team direkt vermitteln, welche Fehler es gemacht hat und wo es sein Verhalten noch verbessern kann. Arbeiten die Teams so Hand in Hand, wirkt die Übung nachhaltig und hilft, die Sicherheit zu erhöhen.

Trotz aller Vorteile ist es aber nicht das Ziel, herkömmliche Pentests durch Purple Teaming zu ersetzen. Je nach Situation kann es auch sinnvoll sein, dass die Teams eigenständig arbeiten und die Testumgebung so näher an der Realität liegt. Vielmehr entwickelt das Purple Teaming das traditionelle Pentesting weiter. Vorteilhaft ist beim Purple Teaming auch der Einsatz eines SOC-Anbieters: Dieser hat zusätzlich die Möglichkeit, den Test in eine umfassendere Strategie einzubinden. Mit einer hohen Expertise im Bereich Cybersecurity sowie aktuellen Tools und Methoden kann der SOC-Anbieter das Vorgehen genau auf das jeweilige Unternehmen abstimmen und so das volle Potenzial des Purple Teamings nutzbar zu machen.

Gergely Lesku, Head of International Operations, Socwise

WER'S VORHER WEISS, DEN MACHT'S NICHT HEISS

Bild: iqoncept-123rf

Wie Observability geschäftsschädigende Ausfälle in Unternehmen verhindern kann.

Autor: Christian Deponte Redaktion: Diana Künstler

➤ Server down : Nicht nur dieser Worst Case, sondern auch kleinere IT-Störungen gehören in Deutschland zum Unternehmensalltag. Das zeigt der „Observability Forecast Report 2022" von New Relic. Pro Woche erleben 89 Prozent der Befragten demnach einen IT-Ausfall kritischen Ausmaßes, 33 Prozent sogar täglich. Hochgerechnet bedeutet das einen Verlust von circa 2.000 Euro pro MitarbeiterIn und Jahr – das gilt für Deutschland, USA, Großbritannien und Frankreich. Ein wichtiger Faktor bei der Fehlerbehebung ist Observability: die Fähigkeit, den Tech-Stack möglichst ganzheitlich zu überwachen. Und – kaum verwunderlich – fast 80 Prozent der Befragten wünschen sich mehr davon.

IT-System mit Überblick

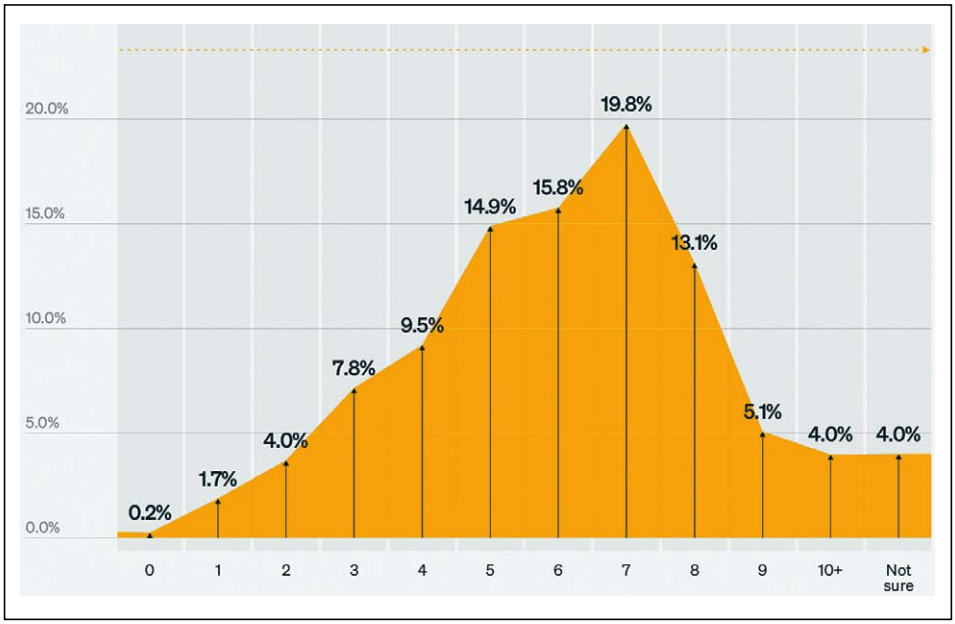
Die meisten Unternehmen nutzen viele verschiedene Tools und Services von unterschiedlichen Anbietern. Diese erzeugen eine Menge Daten: Events, Metrics, Logs und Traces. Bei deren Auswertung von Hand landet man schnell in einem Wirrwarr, in dem sich die Fehlerquelle und die passende Lösung nur schwer identifizieren lassen. Und genau hier setzt Observability an. Entsprechende Lösungen sammeln anfallende Daten von Ende zu Ende, werten sie aus und setzen sie in Kontext. Monitoring gibt hingegen oft nur Bescheid, wenn etwas schiefläuft, häufig verteilt auf viele verschiedene Dashboards. Observability soll es IT-Teams hingegen ermöglichen, die Frage nach dem Warum in einer Ansicht zu beantworten. Probleme, Ursachen und Symptome sind idealerweise auf einen Blick sichtbar.

Laut dem „Observability Forecast" sehen 78 Prozent in Observability eine wichtige Voraussetzung für das Erreichen zentraler Geschäftsziele und 75 Prozent der Führungsebene befürworten Observability. 42 Prozent der befragten Unternehmen wollen mehr Geld in Observability investieren. Denn nur 27 Prozent überblicken mit Tools aktuell ihren gesamten Tech-Stack, und nur rund fünf Prozent geben an, eine ausgereifte Observability-Strategie zu haben. Die meisten Unternehmen (82 Prozent) nutzen vier oder mehr verschiedene Anwendungen. Dabei wünscht sich knapp die Hälfte, sie wäre nur auf eine einzige angewiesen. Etwa ein Drittel findet Fehler zum Großteil noch von Hand oder durch Beschwerden.

Vom Problem- hin zum IT-Management

Dem Anwendungsbereich entsprechend geben 36 Prozent der Befragten weniger Downtime und eine bessere Verlässlichkeit des IT-Systems als wichtigsten Kernfaktor von Observability an. Viele der Befragten sehen sie zudem als Möglichkeit, Teams zu entlasten und sinnvoller einzusetzen.

Bild: Observability Forecast 2022, New Relic



Anzahl der Tools, die für Observability-Funktionen verwendet werden: Auf die Frage nach der Anzahl der Tools, die sie verwenden, um den Zustand ihrer Systeme zu überwachen, gaben die Umfrageteilnehmer einer New Relic-Studie mit großer Mehrheit an, mehr als eines zu verwenden. Die meisten (82 Prozent) verwendeten vier oder mehr Tools. 94 Prozent verwendeten zwei oder mehr. Jeder Fünfte verwendete sieben Tools, die am häufigsten gemeldete Zahl. Nur 2 Prozent nutzten nur ein Tool, um ihre Observability-Anforderungen zu erfüllen. Der Zustand der Observability ist heute also meistens multitoolfähig – und daher fragmentiert – und wahrscheinlich von Natur aus komplex zu handhaben. Tatsächlich gaben 25 Prozent der Umfrageteilnehmer an, dass zu viele Überwachungstools eine primäre Herausforderung darstellen, die sie daran hindert, eine vollständige Beobachtbarkeit zu erreichen.

Observability ist darüber hinaus eine Möglichkeit, um zeitintensive Arbeit und damit Druck von den Schultern der IT-Teams zu nehmen. KI-Systeme helfen gegebenenfalls dabei, die Kapazitäten der Fachkräfte auf die Vorfälle zu konzentrieren, die tatsächlich relevant sind und nehmen ihnen durch intelligente Empfehlungen gegebenenfalls die Sorge, ob sie bei der Implementierung der Monitoring-Software auch alles bedacht haben. Unternehmen können so die Erfahrung und das Wissen ihrer Belegschaft im Idealfall effizienter und zielgerichteter einsetzen.

Monitoring gibt oft nur Bescheid, wenn etwas schief läuft, häufig verteilt auf viele verschiedene Dashboards. Observability hingegen ermöglicht den IT-Teams, die Frage nach dem Warum zu beantworten, in einer zusammenfassenden Ansicht.

Fehlende Fachkräfte ersetzen

Ein besseres, vor allem schnelleres und konkreteres Verständnis für unternehmensinterne Softwareprozesse kann Reaktions-, Identifizierungs- und Reparaturzeiten verringern. Und das nicht nur bei internationalen Tech-Giganten, wie der Observability Forecast zeigt. Auch kleine und mittelständische Unternehmen wissen um die Möglichkeiten der Technologie und wollen auch in Zukunft mehr investieren. Gerade für sie bietet Observability die Option, trotz des drohenden Fachkräftemangels mit der technischen Entwicklung Schritt zu halten: Künstliche Intelligenz ersetzt Fachkräfte, die händisch die Unmengen von Daten durchwühlen und nach einer Lösung suchen. Fachkräfte können dann effizienter eingesetzt und ihre Fähigkeiten besser genutzt werden.

Christian Deponte, Vice President EMEA Central, New Relic

➤ Observability, zu deutsch „Beobachtbarkeit", ist die Fähigkeit, die Leistung eines Systems zu messen und Probleme und Fehler auf Grundlage seiner Ausgabewerte zu identifizieren. Diese externen Ausgaben sind Telemetriedaten (Metriken, Ereignisse, Protokolle und Ablaufverfolgungen). Datengesteuertes Engineering nutzt Telemetriedaten wiederum, um Maßnahmen voranzutreiben.

Observability erfordert Instrumentierungssysteme, um verwertbare Daten zu sichern, die einen Fehler identifizieren und detailliert angeben, wann, warum und wie ein Fehler auftritt. Observability beinhaltet auch das Sammeln, Analysieren, Ändern und Korrelieren dieser Daten, um die Verfügbarkeit und die Leistung zu verbessern. Software-Engineering, Entwicklung, Site Reliability Engineering, Operations und andere Teams nutzen Observability, um das Verhalten komplexer Systeme zu verstehen und Daten in maßgeschneiderte Erkenntnisse umzuwandeln.

▸ Eine Teilmenge der Observability ist das **Monitoring** (Überwachung), welche reaktiv ist und anzeigt, was falsch ist und wann ein Fehler aufgetreten ist. Observability hingegen bestimmt proaktiv, warum und wie ein Fehler aufgetreten ist – zusätzlich zu den Fragen Was und Wann.

▸ Die Fähigkeit, alles im Tech-Stack zu sehen, was sich auf das Kundenerlebnis auswirken könnte, wird als **Full-Stack-Observability** oder End-to-End-Observability bezeichnet. Es basiert auf einer vollständigen Sicht auf alle Telemetriedaten. *(DK)*

WIRD DIE USV ZUM EINFALLSTOR?

Energiemanagement, Remote-Wartung, Grid-interaktive Geräte – USV-Anlagen müssen zunehmend intern wie extern kommunizieren. Doch diese Vernetzung kann auch zur Gefahrensituation werden. Denn die Anlagen brauchen – wie IT-Geräte – ausreichende Cybersecurity-Maßnahmen.

Autor: Simon Feger ***Redaktion: Lukas Steiglechner***

Bild: herman4429-123rf

➤ Sicherheit der Infrastruktur im Datacenter ist entscheidend. Dazu gehört auch die Cybersicherheit von USV-Anlagen. Um zu verstehen, warum diese Geräte überhaupt online sind, muss das Grundprinzip der USV verstanden werden. Bei Rechenzentren gelten Online- beziehungsweise Doppelwandleranlagen mittlerweile vielerorts als Standard. Das Grundprinzip der unterbrechungsfreien Stromversorgung, nach dem bereits die ersten auf dem Markt angebotenen Anlagen aufgebaut waren, basiert auf drei Komponenten: Gleichrichter, Batterie und Wechselrichter. Durch alle Komponenten fließt im regulären Betrieb kontinuierlich Energie. Da die Wechselspannung an der Ausgangsseite des Geräts immer aus dem Zwischenkreis der USV erzeugt wird, lässt sich dadurch eine saubere, sinusförmige Spannung garantieren. Eventuell problematische Frequenzabweichungen des Netzes werden so ebenfalls von der sensiblen Elektronik ferngehalten. Kommt es nun zu einer Unterbrechung oder einem Stromausfall, wird die Ausgangsseite vollständig und unterbrechungsfrei aus der Batterie versorgt.

Allerdings versursacht der Dauerbetrieb von Gleichrichter, Batterie und Wechselrichter einen relativen hohen Energieverlust und ist in Gegenden wie Europa nicht zwingend notwendig, da die Stromversorgung die meiste Zeit eine ausreichende Qualität besitzt. Viele Doppelwandleranlagen bieten daher neben dem klassischen Online-Modus oft auch weitere Betriebsmodi an. Diese können die Effizienz von etwa 95 bis 97 Prozent im Onlinebetrieb auf bis zu über 99 Prozent erhöhen. Das wird beispielsweise dadurch erreicht, dass die USV-Anlage nur bei Bedarf in den Doppelwandler- oder Batteriebetrieb wechselt und die Netzspannung ansonsten zu den Verbrauchern durchschleift. Wahlweise lassen sich auch einzelne redundante Leistungsmodule automatisiert de- und reaktivieren, um die Effizienz zu erhöhen, ohne auf den höchstmöglichen Schutz der Online-Technik zu verzichten.

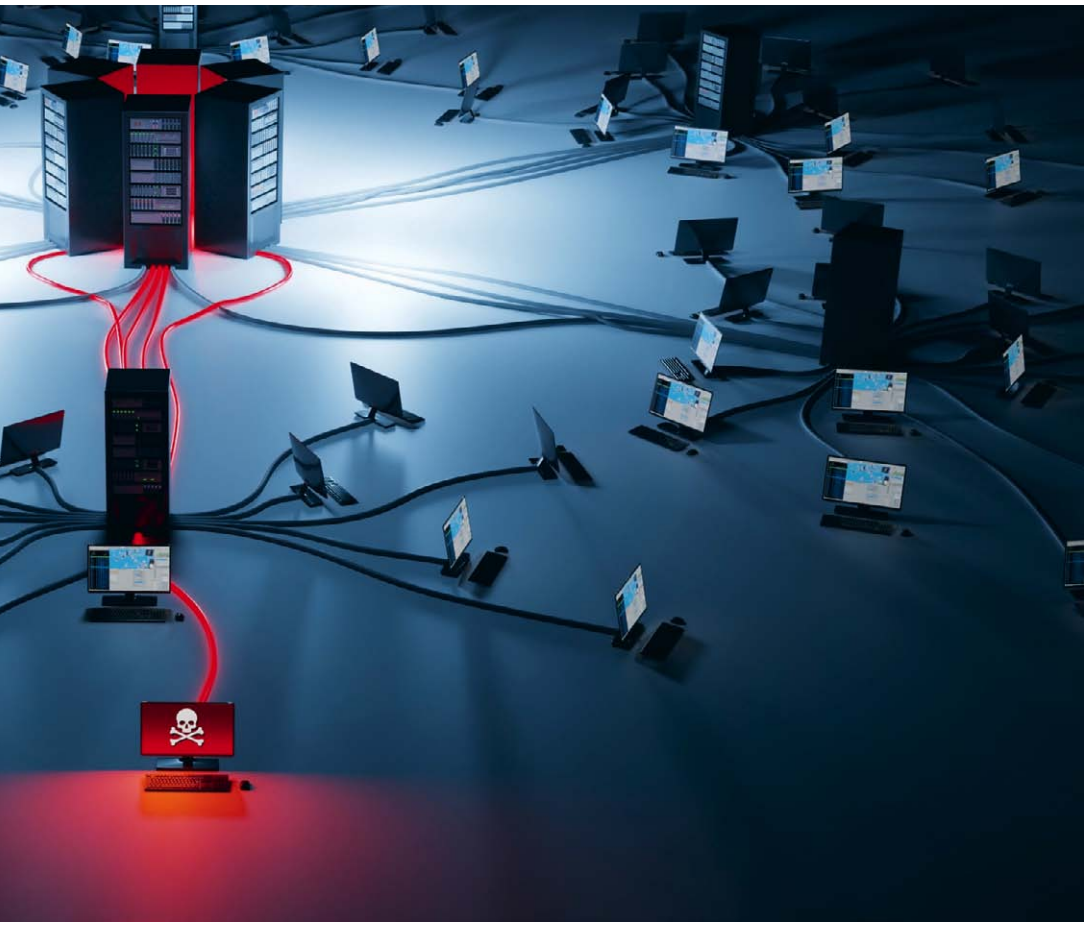
Informationen und Vernetzung

Um die IT-Infrastruktur keiner Gefahr auszusetzen, muss das Umschalten sehr schnell erfolgen. Zusätzlich müssen Sensoren ständig die Eingangsspannung überwachen und beim Über- oder Unterschreiten von Schwellenwerten reagieren. Auch der Zustand der Batterien muss regelmäßig geprüft werden, da diese nicht mehr durchgehend geladen werden, sondern nur noch bei Bedarf. Dieses Ladeverfahren verlängert die zu erwartende Lebensdauer der Batterien, lässt sich aber auch optional auf die klassische Konstantladung umschalten.

So entsteht bei den USV-Anlagen eine große Menge an Informationen. Aus dem Wunsch heraus, diese Daten zu sammeln und die Anlagen zentral zu steuern, kommt der Bedarf nach Vernetzung. Betreiber können beispielsweise den aktuellen Betriebsmodus, den Ladezustand der Batterie oder anstehende Alarme im Auge behalten, und detaillierte Pläne für den Notfall ausarbeiten, die sich auf verschiedene Bereiche der eigenen Infrastruktur konzentrieren. Unkritische Systeme können beispielsweise direkt gezielt heruntergefahren werden, um kritische Systeme länger am Laufen zu halten.

Die Grid-interaktive USV

Die Batterien einer USV sind bei guter Netzqualität die meiste Zeit ungenutzt. In diesen Phasen können sie eine stabilisierende Funktion für die Netzfrequenz wahrnehmen und zusätzliche Einnahmen für die Betreiber generieren. Die Batterien stellen in diesem Kontext als Flexibilitätsreserve kurzfristige Regelenergie zur Verfügung, die der Netzbetreiber benötigt, um die Frequenz stabil zu halten. Das kann im



positiven wie im negativen Bereich geschehen: Die Batterien werden entweder automatisch geladen oder entladen.

Der Bedarf an dieser kurzfristigen Regelleistung wächst vor allem durch die Zunahme der Solarstromerzeugung. Da die Photovoltaikmodule Gleichstrom liefern, muss die Wechselspannung für das Netz erst erzeugt werden. Die Batterien der Rechenzentren können bei diesem Prozess eine wichtige Pufferfunktion wahrnehmen. In der konventionellen Stromerzeugung mit Generatoren stellt die rotierende Masse dieser Maschinen und die darin gespeicherte kinetische Energie diesen Puffer dar. Je mehr von diesen Kapazitäten vom Netz gehen, desto wichtiger werden andere Formen des Ausgleichs, zum Beispiel Batterien.

Um an dieser Frequenzregelung partizipieren zu können, müssen die Batterien sehr schnell reagieren und gezielt angesteuert werden können. Eine Vernetzung der einzelnen Anlagen ist daher notwendig. Dabei müssen die Anlagen auch mehr leisten als den internen Informationsaustausch. Die Anlagen müssen auch nach außen kommunizieren können, sodass Ladung und Entladung – innerhalb gewisser, definierter Schwellenwerte – direkt vom Energieversorger gesteuert werden kann.

USV-Anlagen wie IT-Geräte behandeln

Wie überall bedeutet auch im Bereich der USV-Anlagen die Öffnung nach außen ein mögliches Gefahrenpotenzial. Dabei geht es aber nicht nur darum, dass Hacker Zugriff auf Informationen der Stromversorgung erlangen könnten, im schlimmsten Fall könnte ihnen die USV als Point of Entry für Kernsysteme dienen. Mit einem Angriff auf die USV ließe sich eventuell auch die Stromversorgung komplett lahmlegen, was ernsthaften Schaden anrichten kann. USV-Anlagen, die zur Kommunikation vernetzt werden sollen, müssen also entsprechend abgesichert werden wie IT-Geräte. Allerdings sieht die Realität leider oft noch so aus, dass bei peripheren oder OT-Geräten die Sicherheit zweitrangig behandelt wird. Deshalb suchen Hacker auch oft gezielt solche Devices als Angriffsvektor aus.

Unternehmen, die über vernetzte USV-Anlagen verfügen, oder ein derartiges System aufbauen wollen, sollten darauf achten, dass die verwendeten Netzwerkkarten strengen Sicherheitsstandards genügen, wie beispielsweise IEC 62443-4-2 und UL 2900-2-2. So kann sichergestellt werden, dass sie starke Verschlüsselung unterstützen, über konfigurierbare Passwortrichtlinien verfügen und verschiedene signierte digitale Sicherheitszertifikate verwenden. Die US-amerikanische Cybersecurity and Infrastructure Security Agency (CISA) rät außerdem dazu, die USV-Anlagen in ein virtuelles privates Netzwerk (VPN) einzubinden und Multifaktorauthentifizierung anzuwenden. Weiterhin sollten starke und ausreichend lange Passwörter verwendet werden. Auf keinen Fall sollte die Werkeinstellung der Geräte hinsichtlich Passworts und Nutzernamen beibehalten werden. Um den größtmöglichen Nutzen aus den vernetzten USV-Anlagen zu ziehen, haben Unternehmen in der Regel auch eine Power-Management-Software im Einsatz. Dabei sollten sie allerdings darauf achten, dass sich auch hier keine Sicherheitslücken einschleichen können und die Lösung mit der Hardware kompatibel ist.

Vernetzte USV-Anlagen können Unternehmen Vorteile bieten – von der schnellen Reaktion im Ernstfall bis hin zur Teilnahme am Regelenergiemarkt mit den Grid-interaktiven Geräten. Doch gilt auch für die unterbrechungsfreie Stromversorgung, dass Vernetzung ohne Absicherung unweigerlich zur Gefahr wird. Daher sollten Verantwortliche die USV-Anlagen wie IT-Geräte behandeln und die gleichen hohen Sicherheitsanforderungen bei der Auswahl zu Grunde legen. Nur so können sie alle Vorteile der vernetzten Geräte nutzen, ohne dadurch Schwachstellen in ihren Infrastrukturen zu schaffen.

Simon Feger, Produkt Support Manager, Eaton

SICHERHEITSKOPIEN? HABEN WIR DOCH…

Bild: deagreez-123rf

Eine zeitgemäße Datensicherheit ist wichtig, weil sie darüber entscheidet, ob und wie schnell Unternehmen ihre Systeme nach einem Cyberangriff wiederherstellen können. Voraussetzung dafür ist, dass Kriminelle das Back-up nicht kompromittiert, verschlüsselt oder gelöscht haben. Was muss die Cybersicherheit leisten, um nach einem Vorfall eine komplette Wiederherstellung zu ermöglichen und welche Rolle spielt Zero Trust Data Security dabei?

➤ Es ist ein Horrorszenario, vor dem sich jedes Unternehmen fürchtet: Plötzlich funktionieren wichtige Geschäftsanwendungen nicht mehr, weil Kriminelle oder andere Unbefugte Systeme verschlüsselt haben. Notgedrungen fahren Verantwortliche die IT weitgehend runter, um eine Ausbreitung der Ransomware zu verhindern. In Folge stehen viele Geschäftsprozesse still. Vielleicht sind auch Kunden oder Lieferketten betroffen.

Je länger es dauert, den Cyberangriff zu bewältigen und das Unternehmen wieder betriebsfähig zu machen, desto größer ist der Schaden. Laut einer Studie aus dem Jahr 2021 brauchen Organisationen rund einen Monat, um ihre Systeme nach einer Ransomware-Attacke komplett wiederherzustellen. Die durchschnittlichen Kosten für die Behebung der Folgen liegen demnach bei 1,4 Millionen US-Dollar – mögliche Lösegeldzahlungen nicht eingerechnet. Das Lösegeld ist meistens ohnehin nicht der größte Kostenfaktor.

Rarer Notfallplan für Cyberattacken

Umso erstaunlicher ist es, dass knapp die Hälfte der Unternehmen in Deutschland noch schlecht auf die Angriffsbewältigung vorbereitet ist, wie wiederum eine aktuelle Bitkom-Studie zeigt. Nur 54 Prozent der Befragten haben einen Notfallplan, der Abläufe und Sofortmaßnahmen im Falle einer erfolgreichen Cyberattacke regelt.

Bisher konzentrieren sich die meisten Unternehmen auf die Frontend-Sicherheit: Sie investieren in Endpunkt-, Netzwerk-, E-Mail- und Cloud-Security-Lösungen, um Cyberattacken bestmöglich abzufangen. All das ist wichtig und richtig, hilft aber nicht weiter, wenn trotzdem ein Angriff erfolgreich ist. Was dann neben einer schnellen Detection and Response zählt, ist ein funktionierendes Backup, mit dem man die Systeme zeitnah wiederherstellen kann.

Dass ein Unternehmen ein Konzept für Datensicherheit braucht, ist weithin bekannt. In der Regel schließt eine Sicherheitsstrategie zum Beispiel Back-ups ein. Früher auf Bändern, die dann an einem geheimen Ort hinter dicken Stahltüren gelagert wurden – manche Unternehmen machen das auch heute noch so. Entsprechend lange dauert es, insbesondere bei verteilten Standorten, Sicherheitskopien von Daten und Systemen anzulegen oder diese wiederherzustellen.

Heute befinden sich Back-ups deshalb meist auf Servern, sodass sie bei Bedarf schnell zur Verfügung stehen. Aber wie sicher sind diese, wenn sie nicht physisch von der Infrastruktur getrennt werden? Was, wenn auch sie bereits verschlüsselt, kompromittiert oder gar gelöscht wurden? Wie lange dauert der Cyberangriff schon an und wie weit muss man zurückgehen, um das letzte, saubere Back-up zu finden? All das sind wichtige Fragen, weil sich Cyberangriffe über mehrere Monate erstrecken können.

Autor:
Michael Pietsch
Redaktion:
Diana Künstler

Auch Back-ups müssen abgesichert werden.

Oft verhält sich die eingedrungene Malware zunächst ruhig, um möglichst unbemerkt zu bleiben. Nach und nach spionieren die Hacker das Netzwerk aus, identifizieren sensible Daten und verschaffen sich privilegierte Rechte. So können sie Sicherheitskontrollen schrittweise aushebeln, um immer weiter vorzudringen. Zu den Zielen von Ransomware-Angriffen zählt, den Daten- und Systemwiederherstellung auszuschalten. Denn dann erhöht sich die Zahlungsbereitschaft der Opfer deutlich. Erst ganz zum Schluss erfolgen dann der Datendiebstahl und die Verschlüsselung.

Wie Cyberkriminelle die Wiederherstellung kompromittieren

Ein Weg der Angreifer besteht darin, dass die Malware im System ruht und sich unbemerkt ins Back-up kopieren lässt. Spielen die Verantwortlichen die Sicherungskopie später ein, kann sie erneut zuschlagen. Eine andere Angriffstechnik besteht zum Beispiel darin, Network-Time-Protocol-(NTP)-Server zu kompromittieren. Diese Server versorgen die angeschlossenen IT-Systeme mit Datum und Uhrzeit. Häufig laufen sie noch auf alten Betriebssystemen und sind nur unzureichend geschützt. Wenn nun ein manipulierter NTP-Server eine Zeit meldet, die drei Jahre in der Zukunft liegt, trickst er die Back-up-Software aus: Sie hält aktuelle Sicherungen für alt und löscht diese. Um Zeit-Manipulation zu vermeiden, sollte sich das Back-up-System nicht auf einen NTP-Server verlassen, sondern Zeitstempel von einer Monotonic Clock erhalten. Diese läuft stringent vorwärts und erlaubt keine Zeitsprünge.

Grundlagen für Datensicherheit und -Wiederherstellung

Damit Back-ups auch im Ernstfall wirklich zuverlässig, sicher und verfügbar sind, sollten Verantwortliche sie vor Cyberangriffen schützen. Dabei empfiehlt sich die Umsetzung eines Sicherheitskonzepts, das auf Zero Trust Data Security basiert. Dieser Ansatz begrenzt den Zugriff auf die Unternehmensdaten und -systeme auf ein Minimum an Nutzern und Geräten und beschränkt die Dauer eines privilegierten Zugriffs. Wenn Malware in das Unternehmensnetzwerk eindringt, dann erschwert Zero Trust die Ausbreitung der Schadsoftware deutlich. Das Risiko, dass sie bis zum Back-up gelangt, sinkt.

Cyberkriminelle entwickeln Malware kontinuierlich weiter und jedes System könnte von bisher unbekannten Schwachstellen betroffen sein. Deshalb zählen unveränderliche Back-ups zu den wichtigen Bausteinen der eigenen Sicherheitsstrategie. Unveränderlichkeit bedeutet, dass einmal geschriebene Daten von niemandem verändert oder gelöscht werden können. Da die Verschlüsselung der Sicherheitskopien eine Veränderung darstellt, können Ransomware-Angriffe auf Back-ups diese nicht verschlüsseln.

Für bessere Datensicherheit empfiehlt es sich zudem, Back-ups regelmäßig auf sensible Daten und Malware zu scannen. Ersteres hilft dabei, schlecht geschützte Daten zu identifizieren und Gegenmaßnahmen zu ergreifen. Letzteres stellt sicher, dass das Back-up auch wirklich sauber ist. Mit dieser Maßnahme verhindern Unternehmen, Malware aus einer infizierten Back-up-Version wiederherzustellen. Außerdem unterstützen solche Scans bei der forensischen Untersuchung, falls es zu einem erfolgreichen Cyberangriff kommt. Sie können zum Beispiel dabei helfen, Eintrittszeitpunkt und Eintrittsort der Malware zu bestimmen.

Datensicherheit Teil des Security-Konzepts

Fakt ist: Ein Cyberangriff kann alle treffen. Selbst mit den besten Abwehrmaßnahmen sind Unternehmen nie hundertprozentig sicher. Die meisten Cyberkriminellen verfolgen das Ziel, Geld zu verdienen. Solange sie mit ihrer Strategie erfolgreich sind, werden sie das Geschäftsmodell Ransomware weiter ausbauen. Gerade kleinere und mittelständische Unternehmen verfügen oft nur über beschränkte Ressourcen für ihre Cybersicherheit und geraten deshalb zunehmend in den Fokus. Umso wichtiger wird es, neben der Frontend-Sicherheit auch die Datensicherheit besser ins Security-Konzept zu integrieren und sich näher mit Zero Trust Data Security zu beschäftigen. Daten sind oft das wichtigste Gut von Unternehmen. Verantwortliche sollten sie schützen, um kostenintensive Ausfallzeiten zu verhindern und die Geschäftskontinuität zu erhalten.

Michael Pietsch, GM and Country Manager Germany bei Rubrik

GRÖSSERE UNTERNEHMEN BEREITEN SICH BESSER VOR ALS KLEINERE

➤ Hacker, die sich auf den Unternehmensservern herumtreiben, der Abfluss von wichtigen Geschäftsdaten oder Ransomware, die Festplatten verschlüsselt und die IT-Nutzung unmöglich macht: Auf solche Cyberattacken sind viele Unternehmen in Deutschland immer noch unzureichend vorbereitet. Nur gut jedes zweite (54 Prozent) verfügt über einen Notfallplan mit schriftlich geregelten Abläufen und Ad-hoc-Maßnahmen für den Fall von Datendiebstahl, Spionage oder Sabotage. Das ist das Ergebnis einer im September vorgestellten Studie im Auftrag des Bitkom, für die 1.066 Unternehmen aus allen Branchen repräsentativ befragt wurden. „Bei der Abwehr eines Cyberangriffs ist Zeit eine ganz entscheidende Komponente. Alle Unternehmen sollten entsprechende Vorbereitungen treffen und einen klar geregelten Notfallplan aufstellen, um im Fall der Fälle nicht wertvolle Zeit zu verschwenden“, sagt Simran Mann, Referentin Sicherheitspolitik beim Bitkom. Aktuell ist die Vorbereitung auf Cyberangriffe auch eine Frage der Unternehmensgröße. Große Unternehmen mit 100 bis 500 Beschäftigten (71 Prozent) sowie 500 und mehr Beschäftigten (78 Prozent) haben deutlich häufiger einen Notfallplan aufgestellt als kleinere mit zehn bis 99 Beschäftigten (51 Prozent). Mann erklärt: „Jedes Unternehmen kann Opfer von Cyberattacken werden, unabhängig von Branche und Größe. Ist die Firmen-IT erst einmal infiziert oder lahmgelegt, entstehen den Unternehmen hohe Kosten, die bis hin zu wochenlangen Produktionsausfällen gehen können.“ *(DK)*

USB-STICK IST NICHT GLEICH USB-STICK

Bild: photovs-123rf

Der Einsatz von USB-Sticks wird im Unternehmensumfeld oft stiefmütterlich behandelt und verkompliziert. Dabei kann die Lösung so einfach wie sicher sein.

Autoren: Christian Marhöfer und Daniel Döring
Redaktion: Diana Künstler

➤ Standortunabhängige und flexible Arbeitsmodelle, Homeoffice-Regelungen, reduzierte Büroflächen und offene Bürogemeinschaften – die Art und Weise, wie, wo und wann wir arbeiten, hat sich nicht zuletzt in den vergangen zweieinhalb Jahren nachhaltig verändert. Mitarbeiter, die selbstorgansiert und ortsungebunden tätig sind, müssen jedoch auch von unterwegs auf Unterlagen und Arbeitsmaterialien zugreifen und Informationen austauschen können. Daten aller Art – ein grundlegendes Gut vieler moderner Unternehmen – sind vermehrt in Bewegung und werden nicht zuletzt häufig auf mobilen Datenträgern transportiert. Mit den falschen Geräten stellt dies ein Risiko für sensible Kundeninformationen und Betriebsgeheimnisse dar. Dabei sind moderne USB-Geräte nicht nur ein bedeutender Teil eines ganzheitlichen Datenschutzkonzeptes – sondern auch eine unkompliziert einführbare Möglichkeit, Remote Work sicher zu gestalten.

Aktuell wie eh und je

Man möchte glauben, dass Wechseldatenträger und allen voran USB-Sticks zu einer aussterbenden Gattung von Speicherlösungen gehören – tatsächlich ist das Gegenteil der Fall. Statista-Erhebungen belegen, dass in Deutschland in der Gesamtheit noch immer elf Millionen Geräte innerhalb eines Jahres verkauft werden. Ein Blick in den internationalen Industriesektor bestätigt diesen Trend auf der B2B-Seite: Laut einer Honeywell-Studie aus dem Jahr 2021 kamen in Produktionsstätten 30 Prozent mehr USB-Datenträger zum Einsatz als im Vorjahr. Gerade in diesem Bereich kann ein Verlust nicht ausreichend geschützter Daten verheerende Folgen für das betreffende Unternehmen haben.

Vorfälle wie der Fund eines Sticks mit Informationen rund um den Sicherheitsapparat des Londoner Flughafens Heathrow im Jahr 2018 oder der kürzlich bekannt gewordene Fall eines verlorenen USB-Sticks mit Daten aller Einwohner der japanischen Stadt Amagasaki (siehe Infokasten) verdeutlichen, welche sensiblen Daten auch im öffentlichen Bereich unter Umständen in falsche Hände geraten können. Die Krux mit den USB-Sticks: Mit ihnen existiert eine simple, praktische Lösung für den Transport und Austausch von Daten. Gleichzeitig stellt der Einsatz falscher Geräte jedoch auch eine enorme Gefahr für Unternehmen und deren Kunden dar – denn USB-Stick ist nicht gleich USB-Stick.

Von Äpfeln und Birnen

Tatsächlich ist ein Großteil der genutzten Wechseldatenträger für die Verwendung im Unternehmens- und Behördenumfeld ungeeignet. Häufig kommen einfache, für den Endverbraucher gedachte und schlimmstenfalls private USBs zum Einsatz. Vor einigen Jahren – 2016, um genauer zu sein – betrug der Anteil an in Unternehmen verwendeten privaten Sticks fast 60 Prozent. Ein Blick in aktuelle Statistiken des Speicherexperten Kingston Technology verrät, wie wenig sich daran geändert hat: Nur 5,8 Prozent der in Deutschland im B2B-Markt verkauften USB-Sticks sind Hardware-verschlüsselte Speichermedien, die speziell für den professionellen Einsatz entwickelt wurden und ein enormes Sicherheitsplus für die Unternehmen bieten.

Warum also vernachlässigen Unternehmen und öffentliche Stellen diesen Teil ihres Sicherheitskonzepts? Neben schlicht fehlender Kenntnis hinsichtlich verfügbarer Optionen wird häufig das Kostenargument angeführt – gerade in kleinen und mittelständischen Unternehmen ein wichtiger Punkt. Normale USB-Sticks aus dem Technikfachgeschäft kosten nur einen Teil der professionellen Datenträger, verfügen aber gleichzeitig über keinerlei Sicherheitsvorkehrungen. Abhilfe wird oft in der Verwendung diverser Softwarelösungen zur Verschlüsselung gesucht. Diese können zwar in bestimmten Fällen eine Alternative darstellen, haben jedoch auch ihre Schwachstellen. Unter anderem sind sie immer nur so sicher wie die Geräte, auf denen sie verwendet werden, sie beeinflussen die Leistung und Geschwindigkeit der Datenträger und sind häufig wenig benutzerfreundlich.

Entscheidend mit Blick auf die Diskussion ist außerdem: Die sichere Implementierung sogenannter Commodity-Sticks in die Unternehmens-IT bedeutet in Summe einen deutlich höheren und anhaltenden Aufwand bei nicht vergleichbaren Sicherheitsgarantien. Softwarelösungen benötigen regelmäßige Wartung und Updates, Mitarbeiter müssen geschult werden und die IT-Abteilung muss anhaltend Hintertürchen recherchieren und überprüfen. Umso komplexer der Pro-

zess und die Anwendung im Alltag, desto größer ist außerdem die Gefahr, dass Mitarbeiter wieder auf die erwähnten privaten Datenträger zurückgreifen, die letztendlich ein zusätzliches, nicht kalkulierbares Risiko darstellen und alle Richtlinien hinfällig machen.

Hardware-verschlüsselte Datenträger

Im Gegensatz dazu bieten Hardware-verschlüsselte, speziell für den Unternehmenseinsatz konzipierte Datenträger dank eigenen, direkt im Laufwerk integrierten Prozessoren quasi aus der Verpackung heraus hohe Datensicherheit und Schutz vor den häufigsten Angriffsarten, darunter Cold-Boot-Attacks und Brute-Force-Angriffe. Für die Verantwortlichen bleibt als To-do die optionale Kombination mit einem Whitelisting-Tool, das gegebenenfalls die Verwendung externer Datenträger verhindert und so eine zusätzliche Sicherheitsebene für das Unternehmen schafft. Weitere Aufwände, Updates oder wiederkehrende Wartungen sind in der Regel nicht notwendig.

Über die Hardware-basierte Verschlüsselung hinaus bieten professionelle USB-Sticks meist eine Reihe an sicherheitsrelevanten Funktionen, die sie von herkömmlichen Datenträgern unterscheiden und für Unternehmen und Behörden mit hohen Sicherheitsansprüchen relevant machen. Dazu zählt unter anderem eine direkt auf dem Gerät verbaute Tastatur, die das Entsperren des Sticks ohne zusätzliche virtuelle Eingabe auf dem Rechnern ermöglicht. Eine weitere entscheidende Rolle spielt die sogenannte FIPS-Zertifizierung, eine von der US-Regierung definierte Reihe an Anforderungen an Endgeräte und Informationstechnologien im Allgemeinen. Um die aktuelle Zertifizierung, FIPS 140-3 Level 3, zu erhalten, müssen USB-Sticks unter anderem vor physischen Zugriffen geschützt sein. In der Praxis wird das beispielsweise durch mit Epoxid beschichtete Schaltkreise realisiert. Hinzu kommen Merkmale wie eine mit einer Polymer-Schutzschicht überzogene Tastatur für USBs mit PIN-Eingabe, bestimmte Regeln hinsichtlich der PIN-Länge oder ein automatisches Abschalten der Geräte bei ungewohnten Hitze- und Spannungsverhältnissen. Nicht zuletzt stellt die Verwendung von FIPS-zertifizierten Wechseldatenträgern außerdem sicher, dass Anforderungen der DSGVO erfüllt und Unternehmen so vor etwaigen rechtlichen Konsequenzen und gleichzeitig Imageschäden geschützt sind. Denn geht ein FIPS-zertifizierter Stick verloren, muss dies nicht öffentlich gemacht werden.

Nicht am falschen Ende sparen

Trotz der wachsenden Bedrohungen durch diverse Formen der Cyberkriminalität ist der Klassiker des verlorenen USB-Sticks nach wie vor – und nicht zuletzt aufgrund der erhöhten Datenmobilität – eine Gefahr für die Datensicherheit in Unternehmen, öffentlichen Stellen und Behörden. Überall, wo Remote Work und verwandte Konzepte eine Rolle spielen, sollte der Bedarf an entsprechend sicheren Datenträgern geprüft und die Lösungen in die Security-Konzepte integriert werden. Den Kosten und Aufwänden gilt es, rechtliche Folgen und Schäden durch den Datenverlust gegenüberzustellen. Wer mehrere tausend Euro in eine Firewall investiert, sollte auch in puncto Datenträger gegebenenfalls nicht am falschen Ende sparen.

Christian Marhöfer, Regional Director DACH, Nordics & Benelux, bei Kingston Technology sowie Daniel Döring, Managing Director Egomind

LOST IN JAPAN

➤ Im Juni 2022 sorgte ein Vorfall in Japan für Aufsehen: Ein USB-Stick mit personenbezogenen Daten der Einwohner von Amagasaki im Westen Japans war verloren gegangen. Nach Angaben der Stadt hatte der Mitarbeiter des IT-Dienstleisters Biprogy die Daten der über 460.000 Einwohner im Informationszentrum der Stadtverwaltung auf den Stick gezogen, um sie an anderer Stelle zu verarbeiten. Nach Feierabend hätte er die Tasche mit dem Stick verloren. Einen Tag später wurde der Stick als verschwunden gemeldet; tags darauf informierte die Stadt Amagasaki die Öffentlichkeit. Schließlich tauchte der USB-Stick nach vier Tagen wieder auf.

Daten von 460.000 Menschen

Grund für den Verlust des Daten-Sticks war Medienberichten zufolge, dass der Mann nach Feierabend in einem Restaurant eingekehrt war und Alkohol trank – zu viel, denn er sei anschließend auf der Straße eingeschlafen. Das berichtete die japanische Rundfunkgesellschaft NHK und berief sich dabei auf Angaben des IT-Dienstleisters. Als der Mann erwachte, sei die Tasche mit dem USB-Stick verschwunden gewesen. Der Mitarbeiter hätte dann den Verlust auch bei der Polizei angezeigt. In Zusammenarbeit mit dieser habe er die Tasche mit dem Stick ein paar Tage darauf dann wiedergefunden, nachdem sie sein Handy geortet hatten, wie NHK berichtete. Auf der Webseite der Stadt hieß es zudem, Aufgabe des IT-Dienstleisters bei der Stadt sei es, vorübergehende Leistungen an von der Wohnsteuer befreite Haushalte auszuzahlen. Konkret sind damit Beihilfen für Menschen gemeint, die stark von der Corona-Pandemie betroffen seien, berichtete NHK. Der Stick hätte daher grundlegende Melderegisterinformationen über alle Bürgerinnen und Bürger von Amagasaki enthalten, also von 465.177 Menschen. Im Einzelnen seien das unter anderem Name, Postleitzahl, Adresse, Geburtsdatum, Geschlecht und Datum des Einzugs der einzelnen Personen. In 360.573 Fällen seien es auch Informationen zur Wohnsitzsteuer gewesen, von 86.000 Haushalten mit Sozialhilfe oder Kindergeld wiederum zusätzlich Kontoinformationen.

Nachdem der Stick wieder aufgetaucht war, berichtete die Stadt, man würde die Daten gemeinsam mit den Behörden untersuchen. Der Stick sei passwortgeschützt und die Daten darauf verschlüsselt, kein Datenleck sei bis dato bekannt. Die Stadt Amagasaki hatte in Folge vor Betrugsfällen im Zusammenhang mit dem zwischenzeitlich verlorenen USB-Stick gewarnt. Betrügerinnen und Betrüger könnten die Angst der Menschen vor einem Verlust ihrer Daten ausnutzen und ihnen etwa die Löschung ihrer Daten anbieten. Auf ihrer Webseite stellte die Stadt klar, dass weder die Polizei noch Mitarbeiter der Stadt oder des betroffenen IT-Unternehmens im Kontext des Vorfalls einzelne Menschen anrufen oder per Mail kontaktieren würden. Bis dato sind keine Konsequenzen des USB-Verlustes bekannt geworden. *(DK)*

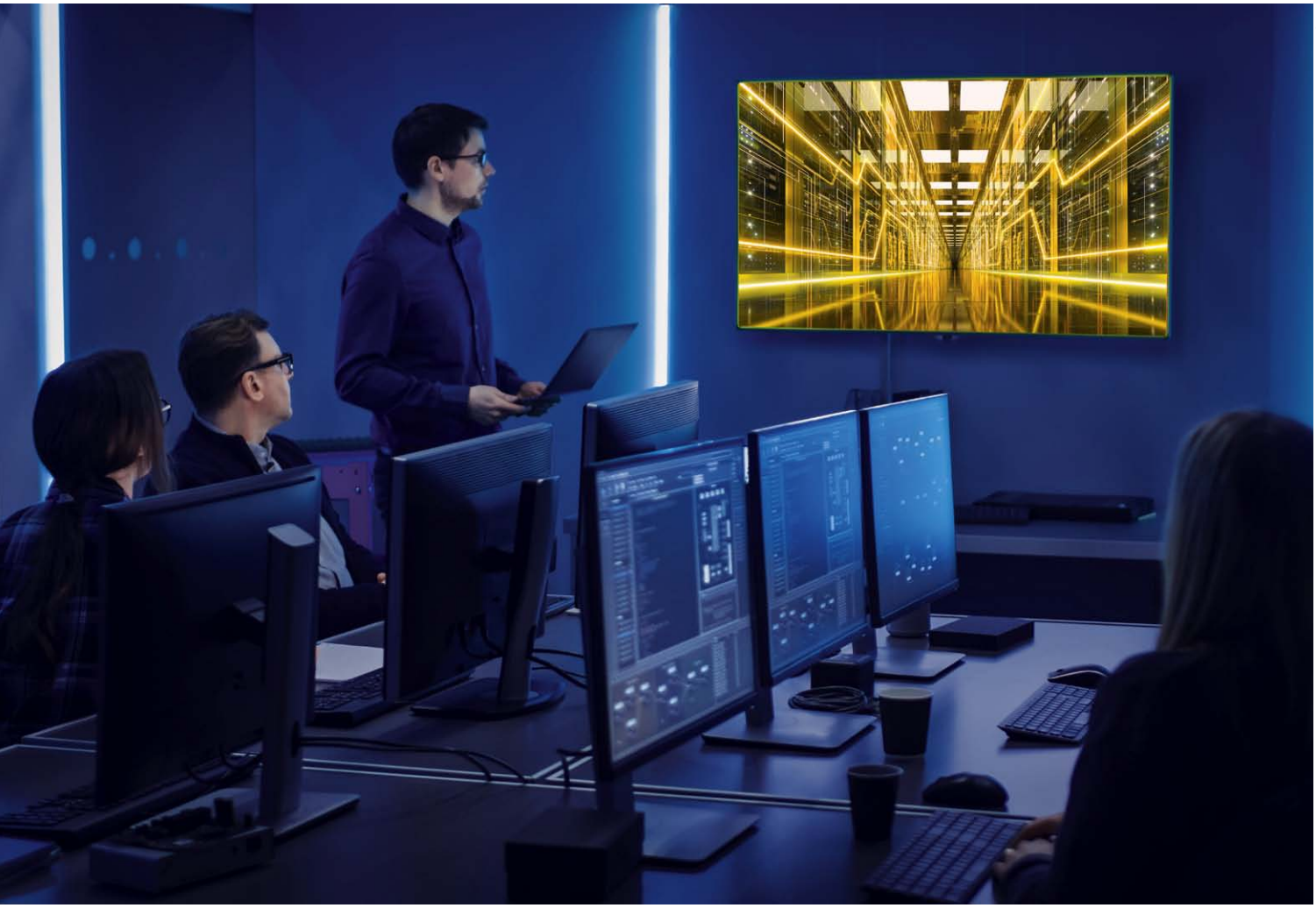


Bild: gorodenkoff - 123rf

WAS DEUTSCHE RZ-BETREIBER VON DEN NORDICS LERNEN KÖNNEN

Mit Blick auf den Datacenter-Betrieb sind die skandinavischen Länder Vorreiter in Hinblick auf Effizienz und Nachhaltigkeit. Zwar sind die lokalen klimatischen Bedingungen dabei ein entscheidender Faktor, dennoch können auch deutsche Betreiber von den Nordics lernen – vor allem in puncto Abwärmenutzung.

Autor: Lukas Steiglechner

➤ Beim Betrieb von Rechenzentren nehmen die Themen Nachhaltigkeit und Energieeffizienz einen immer größeren Stellenwert ein. In Deutschland verläuft diese Entwicklung aber oft noch schleppend – vor allem im Vergleich zu den nordeuropäischen Ländern. Ob Norwegen, Schweden oder Island – die Nordics haben zahlreiche Datacenter bereits auf erneuerbare Energien, natürliche Kühlung und effiziente Abwärmenutzung getrimmt.

Doch viele Faktoren liegen nicht in den Händen der Betreiber. Die nordischen Länder haben ihre Stromerzeugung und -netze beispielsweise bereits stark auf regenerative Energien ausgerichtet, während fossile Brennstoffe in Deutschland trotz aller positiven Entwicklungen der vergangenen Jahre noch einen bedeutenden Anteil ausmachen. So sei es noch „eine Utopie, Datacenter rein mit Ökostrom zu unterhalten – das gibt der Energiemix hierzulande einfach nicht her“, sagt

Michael Endres, Sales Director DACH von Atnorth, einem Rechenzentrumsdienstleister mit Sitz in Island. Das Problem: Während Deutschland bei der Energiewende zu wenig Tempo an den Tag legt, steigt parallel dazu jedoch der Stromverbrauch der Rechenzentren. Beispielsweise auch, weil Branchen wie die Automobil- und die Finanzindustrie zusehends auf High Performance Computing setzen. So werden immer mehr Daten generiert und mit den Hochleistungsrechnern verarbeitet – und der Energiebedarf steigt.

Lokale RZ-Betreiber benötigen vor diesem Hintergrund auch hierzulande innovative Konzepte, um einen nachhaltigen Betrieb zu ermöglichen. Beispiele sind laut Endres Generatoren, die mit E-Fuel oder Wasserstoff arbeiten. Und „auch am Einsatz nachhaltiger Materialien für den Bau von Rechenzentren führt kein Weg vorbei“, so der Sales Director. „Insgesamt gilt es nicht nur Datacenter zu bauen, die möglichst umfassend erneuerbare Energien nutzen, sondern sie müssen auch für die Arbeitslasten von morgen ausgelegt sein und weniger Energie verbrauchen.“

Gesetzlicher Rahmen entscheidet

Datacenter nachhaltiger und effizienter zu betreiben, wird zusehends zur gesetzlichen Vorgabe. Schon ab 2024 soll laut dem Entwurf des Energieeffizienzgesetzes beispielsweise eine Abwärmenutzung von 30 Prozent verpflichtend sein, bis 2027 steigt dieser geforderte Anteil auf 40 Prozent weiter an. Laut Michael Endres sei dies – mit Verweis auf eine Stellungnahme der German Datacenter Association (GDA) – allerdings „unrealistisch“. Denn für die GDA steht fest: Entsprechende Konzepte scheitern oft noch an technischen Hemmnissen und der Wirtschaftlichkeit aktueller Lösungen. An Motivation soll es den Rechenzentrumsbetreibern hingegen nicht mangeln.

Konkret ist die Abwärmetemperatur aus Rechenzentren mit 25 bis 35 Grad Celsius zu niedrig für die jetzigen Fernwärmenetze. Sie muss vor dem Einsatz also nochmals erhöht werden. Außerdem sei die Fernwärmenetzinfrastruktur derzeit nicht ausreichend ausgebaut und es mangele an passenden Abnehmern, kritisiert die GDA. „Zielgenaue politische Maßnahmen wären wünschenswert, doch da schießt der Gesetzgeber leider viel zu oft am eigentlichen Ziel vorbei“, unterstreicht auch Endres. Aus Sicht der GDA sollten sich die Verpflichtungen im Rahmen des Gesetzentwurfs daher weniger an die Rechenzentrumsbranche richten, sondern vor allem die Energieversorger in den Fokus rücken, zum Beispiel mit einer Abnahmepflicht.

Kreative Abwärmenutzung

Kreative Konzepte sind gefragt, wie sie in vielen skandinavischen Ländern bereits umgesetzt wurden – beispielsweise in der Landwirtschaft oder im Zuge der Beheizung von Büro- und Wohnräumen. „Die Abwärme der Rechenzentren kann für die Fernwärmeversorgung von kommunalen Einrichtungen wie Schwimmbädern, für Privatwohnungen und auch Gewerbegebäude eingesetzt werden“, erklärte Bitkom-Präsident Achim Berg im Juli 2022. „Dieses Potenzial sollten wir nicht weiter brachliegen lassen.“

Laut Berechnungen könnten durch Datacenter-Abwärme in Deutschland jährlich rund 350.000 Wohnungen versorgt werden. Die Bitkom-Studie „Rechenzentren in Deutschland“ hat zudem gezeigt, dass die Abwärmenutzung zu den potenziellen Maßnahmen mit dem größten Nachhaltigkeitspotenzial zählt. Dennoch leiten fast drei Viertel der Betreiber die Abwärme ihrer Rechenzentren nicht weiter. Und nur fünf Prozent nutzen mehr als die Hälfte ihrer Abwärme. Begründet wird das abermals mit fehlenden Abnehmern, fehlender wirtschaftlicher Nutzung und im ersten Schritt auch mit zu hohen Investitionskosten.

Bild: atNorth

MICHAEL ENDRES,
Sales Director DACH bei Atnorth

„Zielgenaue politische Maßnahmen wären wünschenswert, doch da schießt der Gesetzgeber leider viel zu oft am eigentlichen Ziel vorbei.“

Wissensaustausch zwischen Unternehmen

Auch hier kann Deutschland von skandinavischen Konzepten lernen, obwohl sich die Voraussetzungen in vielerlei Hinsicht unterscheiden und Use Cases stets individuell gefunden werden müssen. So kann Island beispielsweise auf ein großes Vorkommen an heißem Wasser zurückgreifen und benötigt in diesem Bereich keine weitere Energie. Daher brauche es in jedem Land vor allem den individuellen Austausch mit anderen Unternehmen, „um die Möglichkeiten für die Beheizung von Gewächshäusern, Fischzuchtanlagen und anderen Branchen zu erkunden“, betont Endres von Atnorth.

Trotz aller Hürden gibt es aber auch in Deutschland erste spannende Ideen und Modelle. Beispielsweise hat der Betreiber Windcloud in Schleswig-Holstein eine Algenfarm auf das Dach seines Rechenzentrums gebaut, die er mit der Abwärme der IT-Systeme versorgt. Doch wie die Zahlen zeigen, sind die ungenutzten Potenziale aktuell noch gewaltig.

1

WIE SIEHT DIGITALISIERUNG IN IHREM UNTERNEHMEN KONKRET AUS?

2

WELCHE ZIELE VERFOLGEN SIE MIT DER DIGITALISIERUNG IN IHREM UNTERNEHMEN/ IHRER ORGANISATION?

3

WIE SCHÄTZEN SIE DEN DIGITALISIERUNGSGRAD IHRER BRANCHE EIN?

4

WELCHE RATSCHLÄGE WÜRDEN SIE MIT DEN VON IHNEN GEMACHTEN ERFAHRUNGEN ANDEREN UNTERNEHMEN GEBEN, DIE ERST AM BEGINN IHRER DIGITALISIERUNG STEHEN?

Redaktion: Diana Künstler

Bild: W&H Dentalwerk

THOMAS LANG

ist Vice President Product Innovation bei W&H Dentalwerk. Die internationale W&H-Gruppe mit Headquarter in Bürmoos (Österreich) entwickelt Medizintechnikprodukte und stellt sie her. Mehr als 1.200 Mitarbeiter sorgen für die Bereitstellung von Hard- und Softwareprodukten, die in der Dental-, Medizin- und Veterinärbranche zum Einsatz kommen.

Bild: Debeka

PATRICK SCHNEIDER

ist Hauptabteilungsleiter IT bei der Debeka. Die deutsche Versicherungsgruppe mit Hauptsitz in Koblenz umfasst unter anderem eine private Krankenversicherung, eine Bausparkasse und die Debeka BKK als Krankenkasse.

Bild: Wempe

FRANK HENNIGFELD

ist Chief Digital Officer bei Wempe. Das 1878 gegründete Hamburger Familienunternehmen steht für feine Uhren und Juwelen und hat weltweit 32 Niederlassungen, unter anderem in New York, Paris und London.

Bild: John Deere

STEFAN STAHLMECKE

ist Regional Director Intelligent Solutions Group bei John Deere. Das ist die Hauptmarke des US-amerikanischen Industrieunternehmens Deere & Company. Das Unternehmen ist Hersteller von Landtechnik; weitere Produkte sind forstwirtschaftliche und Baumaschinen sowie Geräte zur Rasen- und Grundstückspflege.

1

Lang: In der W&H Gruppe ist Digitalisierung ein wesentlicher Teil der Unternehmensstrategie. Es geht um die Vernetzung der Produkte, Predictive Maintenance, Prozessoptimierungen und darum, einfache Lösungen für medizinische Anwendungen zu gestalten. Die intuitive Bedienbarkeit der Software spielt dabei eine ebenso wichtige Rolle wie die Dokumentation der Behandlung beziehungsweise die Nachvollziehbarkeit der Aufbereitung zwischen den Behandlungen. Bei unseren Produktionsstandorten in Österreich und Italien setzten wir vor allem auf die Digitalisierung der Produktionsprozesse, welche stark geprägt von Automatisierung sind und somit eine individualisierte Auftragsabwicklung ermöglichen.

Schneider: Die Debeka hatte schon immer die Philosophie, dass wir unsere Mitglieder und Kunden in den Mittelpunkt unseres Handelns stellen. Deshalb betrachten wir Digitalisierung immer nur aus einer Perspektive: Wie können wir durch Digitalisierung den besten Service für unsere Mitglieder und Kunden liefern, die Teil unserer Gemeinschaft sind? Konkret heißt das, wir nutzen digitale Services zur Vereinfachung und Beschleunigung unserer Prozesse. Wir möchten für unsere Mitglieder und Kunden immer erreichbar sein. Egal ob persönlich oder digital. Hierfür stellen wir uns im Bereich der digitalen Kanäle, von Homepage über Apps bis zu Social Media, zukunftsfähig auf. Und natürlich bleiben wir unserer Linie treu, kompetente Beratung und besten Service auch im persönlichen Kontakt zu bieten. Wir sind uns sicher, so das Erlebnis für unsere Mitglieder und Kunden zu liefern, das von einem modernen Traditionsversicherer erwartet wird.

Hennigfeld: Wempe ist ein Familienunternehmen mit langer Tradition. Das Kerngeschäft stützt sich auf den Verkauf hochwertiger Uhren und Schmuck sowie Serviceleistungen. Mit 32 Niederlassungen in deutschen und internationalen Standorten ist die Kundeninteraktion vor allem durch den persönlichen Kontakt geprägt. KundInnen finden bei Wempe eine intensive und tiefgehende Beratung. Daher standen die digitalen Fähigkeiten lange nicht im Vordergrund. Mit den veränderten Kundenanforderungen ist der Bedarf immer größer geworden. 2019 wurde ein umfassender Relaunch des Online-Shops durchgeführt. Im selben Jahr wurden der weitere Ausbau der IT nochmals intensiviert und eine umfassende Digitalisierungsstrategie verabschiedet.

Stahlmecke: John Deere ist eine Smart Industrial Company. Den Schritt dorthin haben wir in einer der größten Umstrukturierungen in der Firmengeschichte vollzogen und uns mit den drei Geschäftsfeldern Produktionssysteme, Technologie-Lösungen und Lebenszyklus-Lösungen neu aufgestellt. Wir betrachten Traktor, Mähdrescher und Co. nicht mehr als einzelne Maschine, sondern schauen auf das ganze Produktionssystem inklusive der dahinterliegenden Software. Wir sind überzeugt: Daten sind die Bauernregeln von morgen; sie ermöglichen bessere Entscheidungen auf dem Acker und in der Fabrik. Hierbei helfen Sensorik, GPS-Technologie und KI. Die Digitalisierung hilft der Landwirtschaft nicht nur bei der Optimierung der Produktion, sie unterstützt auch bei der Dokumentation der durchgeführten Maßnahmen.

2

Lang: Unser Ziel ist es, für unsere Kunden die tägliche Arbeit zu erleichtern. Manuelle Prozesse digital abzubilden. Die cloudbasierten Systeme bei unseren Produkten sind zukunftsweisend. Die UserInnen können egal von wo und wann auf die vernetzten Geräte zugreifen, das führt zu mehr Effizienz und Produktivität im Praxisteam. Bestmögliche Beratung der Patient:innen inbegriffen, ob bei der Implantatsstabilität, welche Falldaten zur Verbesserung von Zahnimplantatsbehandlungen liefert, oder bei den Sterilisationsgeräten, welche mit Activation Codes ein individuelles Upgrade bekommen und ein umfangreiches Monitoring gewährleisten.

Schneider: Ziel soll es vor allem sein, die Kundenerwartungen zu bedienen. Und diese verändern sich rasanter denn je. Die Pandemie hat sich hier als eine Art „Katalysator“ gezeigt und das Verständnis und den Bedarf an digitalen Services und Produkten in der Gesellschaft verändert. Dies haben wir erkannt und richten unserer Service- und Produktlandschaft konsequent nach dem digitalen Bedarf unserer Mitglieder und Kunden aus. Sei es durch einfach online abschließbare Produkte oder neuen Self Services, die „convenient“ also bequem konsumiert werden können. Darüber hinaus ist Digitalisierung auch ein wichtiger Treiber für die moderne Arbeitswelt. Haben wir vor der Pandemie noch von „New Work“ gesprochen, befinden wir uns längst im „New Normal“. Ob mobil, hybrid oder in unseren aktivitätsbezogenen Raumkonzepten. Durch digitale Lösungen können unserer MitarbeiterInnen frei entscheiden, wie sie ihren collaborativen Arbeitstag gestalten wollen.

Hennigfeld: Die Digitalisierung bei Wempe dient vor allem dazu, die Kernkompetenzen im Kundenkontakt zu stärken und durch neue Service-Angebote zu ergänzen. Daher steht die bessere Unterstützung der Verkaufsberater*innen mit digitalen Werkzeugen an erster Stelle. Aber auch der Ausbau der Omni-Channel-Prozesse, die ein noch besseres Einkaufserlebnis über stationäre und digitale Touchpoints hinweg ermöglichen, stehen im Vordergrund. Bei der Digitalisierung verfolgt Wempe einen langfristigen und nachhaltigen Ansatz, bei dem die IT-Landschaft insgesamt modernisiert wird, damit diese die notwendige Leistungsfähigkeit von übermorgen bieten kann. Daher wurde auch die IT-Infrastruktur umfassend erneuert.

Stahlmecke: Jeder Tropfen, jedes Korn zählt. Das ist das Motto von Precision Farming. Die Digitalisierung trägt dazu bei, den Einsatz von Düngemitteln, Pflanzenschutzmitteln und Treibstoff zu reduzieren und dennoch einen höheren Ertrag zu erzielen. Dies schützt die Umwelt und sichert die Ernährung. Dafür müssen wir nicht mehr in einzelnen Arbeitsschritten, sondern mit Blick auf das gesamte Produktionssystem von der Aussaat bis zur Ernte denken. Mit der Leap Ambition haben wir als erster Landmaschinenproduzent eine Nachhaltigkeitsagenda aufgestellt. Bis 2030 wollen wir 75 Prozent der Betriebe hierzulande ermöglichen, sich mit ihren Feldern zu vernetzen und nachhaltiger zu wirtschaften. Gleichzeitig unterstützt John Deere die Landwirte dabei, die politischen Forderungen des Green Deals zu erfüllen.

3

Lang: Da kommt es sicher auf den Bereich an. In der Industrie sind die Digitalisierung und Automatisierung bereits auf einem hohen Grad fortgeschritten. Für den Vertrieb geht es nicht nur um schlanke CRM Tools und einen integrierten Sales Funnel, sondern auch um Segmentierung in der Kundenansprache. Das ist ohne digitale Unterstützung nicht mehr möglich. In der Dentalbranche steht man eher am Beginn der Digitalisierung. Da gibt es unglaublich viel Potenzial für die AnwenderInnen und dadurch auch für die PatientInnen. Die Zeiten, wo es rein um die Geschwindigkeit bei der Umdrehung ging, sind vorbei. Es werden vermehrt nachhaltige Lösungen für den jeweiligen Bedarf der ÄrztInnen nachgefragt.

Schneider: Generell sehe ich Nachholbedarf in unserer Branche. Sicherlich gibt es hier Mitbewerber, die einen guten Reifegrad im Rahmen der Digitalisierung erreicht haben. Das findet vor allem dort statt, wo es darum geht, bestehende Prozesse und Services zu digitalisieren. Häufig kommen hier Themen wie „Erhöhung der Dunkelverarbeitung“ oder „KI im Bereich Fraud“ zur Sprache. Der Kundenbedarf geht allerdings in eine andere Richtung. Es wird erwartet, dass auch im Bereich Versichern und Finanzieren, durch Digitalisierung Innovation im Bereich der Produkte und Services stattfindet. Dies passiert aktuell aber leider eher selten. Und gerade in unserer Branche ist durch die große Produktspannbreite ein hohes Potenzial vorhanden. Allein in den Themen Smart Home, IoT, Data Analytics & Co. steckt das Potenzial, Versicherungsunternehmen vom reinen Risiko-Manager zum Fürsorger weiterzuentwickeln.

Hennigfeld: Die Luxusbranche zählt nicht unbedingt zu den Vorreitern in der Digitalisierung im Vergleich zu anderen Branchen. Das stationäre Einkaufserlebnis und die persönliche Beratung sind maßgebend. Darüber hinaus sind die Produkte sehr beratungsintensiv und begeistern KundenInnen, wenn diese anprobiert und gefühlt werden können. Die Branche hat aber längst erkannt, dass die Digitalisierung Möglichkeiten bietet, um KundInnen noch umfassender über Produkte informieren und mit neuen Services mehr Komfort bieten zu können. Hierzu zählt auch das Online-Shopping. Auch der Pre-owned-Markt mit Online-Pure-Playern hat eine weitere Dynamik in der Branche erzeugt.

Stahlmecke: Pflügen, Aussaat, Ernte und Co. sind bereits viel digitaler als viele meinen. Aber es gibt auch Hürden: Anders als in der Automobilindustrie ist etwa die Elektrifizierung von Landmaschinen derzeit nur bedingt möglich. Batteriebetriebene Konzepte für mittlere und große Traktoren sind noch nicht realisierbar, die Leistungsdichte der Batterien noch zu gering. Als Brückentechnologie, bis vollelektrische Landmaschinen auch in höheren Leistungsklassen verfügbar sein werden, setzt John Deere auf den Einsatz von Biokraftstoffen. In den unteren Leistungsklassen treibt das Unternehmen die Elektrifizierung weiter voran. Bis 2026 wird John Deere in jeder Produktfamilie von Rasen- und Grundstückspflegegeräten und kompakten Nutzfahrzeugen eine elektrische Antriebsalternative auf den Markt bringen. So ist ein autonomer, batteriebetriebener Elektrotraktor in der Klasse unter 100 PS geplant.

4

Lang: Eine schwierige Frage. Am ehesten einfach mutig sein. Es wird nicht immer alles perfekt beim ersten Versuch gelingen und Digitalisierung ist nie fertig produziert, das ist laufende Weiterentwicklung und Optimierung. Da braucht es Beharrlichkeit genauso wie Veränderung.

Schneider: Wichtig ist vor allem zu verstehen, dass Digitalisierung kein reines Thema der IT ist oder es hier nur um Technik geht. Digitalisierung rückt den Mensch in den Fokus allen Handels. Gute Digitalisierung funktioniert nur, wenn man das Problem des Kunden versteht und es dann mit sinnvollen digitalen Services löst. Man sollte nicht in digitale Lösungen investieren, nur damit es am Ende „fancy“ und in einer App ist. Damit wird Digitalisierung lediglich zu einem Kostentreiber im Unternehmen. Digitalisierung sollte als Weiterentwicklung des eigenen Geschäftsmodells verstanden werden. Dazu ist es wichtig, ein klares Alignment zwischen den Business und IT-Bereichen zu erzeugen. Denn Digitalisierung kommt nur dann optimal beim Kunden an, wenn Digitalisierung im Unternehmen von allen Bereichen gelebt und vorangetrieben wird.

Hennigfeld: Die Digitalisierung ist eine Aufgabe, die für viele gewaltig groß erscheint. Gerade für den Mittelstand, der vielleicht nicht immer die Priorität auf Investitionen in die IT-Fähigkeiten gelegt hat. Da fragt man sich schnell: Wo fangen wir am besten an? Wie sollen wir das überhaupt schaffen? Sind wir nicht sowieso schon zu spät? Trotz der hohen Dynamik halte ich es für sinnvoll, einen langfristigen Plan zu verfolgen, bei dem auch Basis-Probleme in der IT adressiert werden. Die Priorität der einzelnen Projekte sollte sich zudem am Mehrwert der Nutzer orientieren. Ein System zur Verbesserung der internen Kommunikation für alle Mitarbeitenden kann mehr wert sein als ein Augmented Reality Edge-Case.

Stahlmecke: Bis zum Durchbruch der Digitalisierung in der Landwirtschaft war es ein langer Weg. Beim GPS-basierten Spurführungssystem AutoTrac hat es beispielsweise circa 20 Jahre gedauert. Heute gehört diese Technologie zur Standardausstattung bei den mittleren und großen Traktoren. Gleichzeitig nimmt die technische Weiterentwicklung immer schneller Fahrt auf. Vor allem kleinere Unternehmen können diese Herausforderung daher oft nicht allein stemmen. Hier helfen Kooperationen mit spezialisierten Unternehmen und Start-ups. Sie sind agil sowie äußerst innovativ und in der Lage digitale Lösungen sehr schnell zu entwickeln. Wir arbeiten zum Beispiel in der landwirtschaftlichen Branche mit über 120 Partnern zusammen. Sie erstellen beispiesweise Applikationskarten mit Hilfe von Drohnen- beziehungsweise Satellitenaufnahmen, bieten digitale Wetterstationen an oder entwickeln spezielle Softwareanwendungen. Darüber hinaus haben wir vor einigen Jahren die Firma Blue River übernommen, die die Entwicklung der Pflanzenschutztechnologie See & Spray zur Serienreife vorangetrieben hat. Ein weiteres Beispiel ist die Firma Bear Flagg, mit der wir den ersten autonomen Großschlepper entwickelt haben.

45%

der befragten IT-Entscheider sehen die digitale Geschäftsfähigkeit ihres Unternehmens aufgrund gestiegener Strompreise unter anderem auch bei Rechenzentren in Gefahr. Die hohen Energiekosten sind insbesondere für kleine und mittelständische Betreiber existenzgefährdend.

Das Meinungsforschungsinstitut Civey hat im Auftrag des Eco-Verbandes rund 1.000 privatwirtschaftliche IT-Entscheider zu diesem Themenkomplex befragt.

2.036.189 US-Dollar

zahlten Unternehmen aus Fertigung und Produktion weltweit im Durchschnitt als Lösegeld bei Ransomware-Attacken. Dieser Sektor zahlt damit durchschnittlich mehr als das Doppelte im Vergleich zu anderen Branchen. Dort werden im Durchschnitt 812.360 US-Dollar an die Erpresser gezahlt.

Dies ist ein Ergebnis aus der Studie „State of Ransomware 2022“ des Security-Unternehmens Sophos. Für diesen wurden 5.600 IT-Experten in mittelständischen Unternehmen in 31 Ländern befragt, darunter 419 aus der Fertigungs- und Produktionsbranche.

57%

der befragten IT-Entscheider in Deutschland sind der Meinung, dass ihr Unternehmen nicht weiß, was notwendig ist, um die Digitale Transformation innerhalb der Belegschaft voranzutreiben. Gleichzeitig finden 62 Prozent der Angestellten, dass ihr Unternehmen bei der Planung von Transformationsprogrammen nicht ausreichend auf die eigene Belegschaft eingeht.

Das zeigt Dells „Breakthrough“-Studie. Für diese wurden weltweit 10.500 Führungskräfte, IT-Leiter sowie Mitarbeitende, die an der Digitalen Transformation beteiligt sind, befragt. 400 Teilnehmer kamen aus Deutschland.

4 von 10

befragten IT-Entscheidungsträgern in Deutschland haben Sicherungs- und Wiederherstellungssysteme für alle Remote-Mitarbeiter ihres Unternehmens eingerichtet. Mehr als ein Fünftel (22 Prozent) der Befragten gab an, solche Lösungen für keinen ihrer Remote-Mitarbeiter im Einsatz zu haben.

Diese Studienergebnisse hat Arcserve, Anbieter von Datensicherungslösungen, vorgestellt. Insgesamt haben 1.121 IT-Entscheidungsträger in elf Ländern an der Umfrage teilgenommen.

1/3

der befragten Internetnutzer verwendet dasselbe Passwort für verschiedene Online-Dienste. Vier von fünf Umfrageteilnehmern geben an, bei der Passwort-Erstellung einen Mix aus Buchstaben, Zahlen und Sonderzeichen zu verwenden.

Der Bitkom hat 1.014 Personen ab 16 Jahren in Deutschland zum Thema Passwörter befragt.

Redaktion: Lukas Steiglechner

JEDER 2.

befragte deutsche Cybersicherheitsexperte ist der Meinung, dass die Geschäftsleitung der digitalen Sicherheit nicht genügend Aufmerksamkeit schenkt. In Deutschland ist eine große Mehrheit (95 Prozent) der Fachleute für Cybersicherheit überzeugt, dass die Verantwortung für Cyberrisiken auf Vorstands- und Managementebene klar definiert ist.

Die Studie „XDR: Redefining the future of cybersecurity“ von Trellix gibt Aufschluss über dieses Thema. Im Rahmen der Studie wurden 9.000 Cybersicherheitsexperten aus Unternehmen mit 500 oder mehr Mitarbeitenden befragt, darunter 500 Teilnehmer aus Deutschland.

7 MONATE

bleibt eine offene Stelle für IT-Fachkräfte im Durchschnitt unbesetzt. Im Vorjahr war dieser Zeitraum noch einen halben Monat kürzer. Derzeit fehlen in Deutschlands Unternehmen 137.000 IT-Experten quer durch alle Branchen. Die Zahl liegt sogar über dem Vor-Corona-Jahr 2019 mit 124.000 unbesetzten Stellen.

Dies ist das Ergebnis einer Umfrage des Bitkom. Für diese wurden 854 Unternehmen ab drei Beschäftigten in Deutschland befragt.

Mehr als die Hälfte

der befragten IT-Fachkräfte plant, sich innerhalb des nächsten Jahres nach einer neuen Stelle umzusehen. Gleichzeitig geben zwei Drittel der IT-Entscheider an, Qualitätslücken in ihren Teams zu sehen. Die Bereiche, die am schwierigsten zu besetzen sind, sind Cloud Computing, Data Science und Cybersicherheit.

Der „IT Skills & Salary Report 2022“ von Skillsoft hat dies ermittelt. Befragt wurden 7.952 IT-Entscheider und IT-Mitarbeitende weltweit.

EIN KOMPLEXES THEMA KOHÄRENT VERMITTELT

Datenschutzverletzungen sind immer noch an der Tagesordnung: 2021 kam es in der Europäischen Union zu 356 Verstößen täglich und es wurden Bußgelder von insgesamt einer Milliarde Euro verhängt. Einer der häufigsten Gründe, unter anderem auch in Deutschland: Der fehlerhafte Umgang mit personenbezogenen Daten. Um diesen zu entgehen und Daten rechtskonform zu verarbeiten, können Unternehmen mit E-Learning-Angeboten zum Thema Datenschutz Mitarbeitende sensibilisieren.

Autor: Philipp von Bülow ***Redaktion: Diana Künstler***

➤ Seit Einführung der DSGVO sind knapp fünf Jahre vergangen und noch immer stellt sie Unternehmen und NutzerInnen vor Herausforderungen. Insbesondere bei der datenschutzkonformen Verarbeitung von personenbezogenen Daten lauern viele Fallstricke, die Unternehmen teuer zu stehen kommen können. Das Risiko und die Höhe der Bußgelder bei Datenschutzverstößen werden dabei oft unterschätzt: Die Verordnung droht mit einer Geldbuße von bis zu 20 Millionen Euro oder im Fall eines Unternehmens mit bis zu vier Prozent des weltweit erwirtschafteten Jahresumsatzes im vorangegangenen Geschäftsjahr – je nachdem, welcher Betrag höher ist.

Laut DSGVO-Portal ist häufig falsche und unrechtmäßige Datenverarbeitung Grund für Bußgelder. Prominentes Beispiel ist eine Bremer Wohnungsbaugesellschaft, die im März 2022 ein Bußgeld in Höhe von 1,9 Millionen Euro zahlen musste. Der Grund: Mitarbeitende erhoben unrechtmäßige Daten zu Mietinteressenten – unter anderem zum Geschlecht, zum Beziehungsstatus und zur sexuellen Orientierung.

Enger Nutzungsrahmen für personenbezogene Daten

NutzerInnen, die mit personenbezogenen Informationen arbeiten beziehungsweise diese verarbeiten, müssen wissen, wie sie mit ihnen umzugehen haben. Die DSGVO gibt Unternehmen und Usern einen strengen Nutzungsrahmen vor. Unter diesen fallen zum Beispiel die Rechte betroffener Personen, die Art und Weise, wie Daten an dritte Organisationen weitergeleitet werden dürfen, und was bei Löschfristen personenbezogener Daten zu beachten ist.

Zur DSGVO gehören aber nicht nur Vorgaben zum Umgang mit personenbezogenen Daten. Die Verordnung regelt auch Maßnahmen und Reaktionen auf Datenschutzvorfälle, die sich in Unternehmen ereignen. Dazu gehört die Benachrichtigung der betroffenen Personen in klarer und einfacher Sprache. Zudem müssen Unternehmen innerhalb von 72 Stunden die zuständige Aufsichtsbehörde über den Vorfall informieren.

Laut Umfrage des Branchenverbands Bitkom (siehe auch Grafik rechts) haben viele Menschen eine differenzierte Meinung zur DSGVO: 73 Prozent der Befragten gaben an, die DSGVO mache Geschäftsprozesse in ihrem Unternehmen komplizierter. Gleichzeitig gaben 74 Prozent an, die DSGVO setze weltweit Maßstäbe für den Umgang mit personenbezogenen Daten. Und ganze 78 Prozent fühlen sich unsicher hinsichtlich ihrer genauen Auslegung. Verwunderlich ist dies nicht, schließlich beinhaltet die Verordnung in elf Kapiteln 99 Paragrafen mit unterschiedlich vielen Absätzen. Um diese nachhaltig zu vermitteln, bedarf es anschaulicher Schulungen.

Vorteile von E-Learning

Online-Schulungen sollen dabei helfen, Mitarbeitenden den sicheren und rechtskonformen Umgang mit sensiblen Daten auf leicht ver-

ständliche Art und Weise näherzubringen. Besonders die vorangegangene Pandemie hat den Bedarf an digitalen Lerninhalten, die unabhängig von Zeit und Ort stattfinden können, wachsen lassen: Seminare, in denen sich TeilnehmerInnen vor Ort einen oder gar mehrere Tage zusammenfanden, waren und sind aus gesundheitstechnischen Gründen seither oft nicht mehr erste Wahl.

E-Learning-Angebote bringen den Vorteil mit sich, dass Betriebe nicht mehr abteilungs- oder teamweise ihre Mitarbeitenden von Projekten und Aufgaben abziehen müssen. Störungen des Betriebsablaufs und organisatorische Aufwände (Terminfindung oder Bereitstellung von Räumlichkeiten) lassen sich so idealerweise vermeiden. Neben Datenschutzschulungen für Berufsfelder wie Führungskräfte oder für Mitarbeitende in Praxen und Krankenhäusern können E-Learning-Angebote zum Komplex DSGVO beispielsweise Informationen zu folgenden Themen vermitteln:

- Umgang mit Datenpannen: Was im Falle eines Datenlecks zu tun ist
- Weitergabe personenbezogener Daten: In welchen Fällen personenbezogene Daten weitergegeben werden dürfen
- Verarbeitung personenbezogener Daten in unterschiedlichen Ländern: Schulungen zu lokalen Datenschutzgesetzen wie PIPL (China) und LGPD (Brasilien)
- Löschpflichten im Datenschutz
- Rechtskonformer Datenaustausch zwischen EU und USA

Faktoren für Lernkonzepte

EntscheiderInnen, die über die Einführung von E-Learnings für ihre Mitarbeitenden nachdenken, sollten jedoch bei der Auswahl eines geeigneten Anbieters ein paar Dinge beachten:

❶ Verständliche Struktur

Das Thema Datenschutz ist komplex, ein kohärenter Aufbau des E-Learning-Angebotes ist deshalb entscheidend: Fragen wie „wann, von wem und wie dürfen Daten verarbeitet werden?" und die Bestimmung von Datenschutzrisiken sollten erläutert werden. Auch Santkionen sollten die Inhalte beleuchten.

❷ Multimedia-Ansatz

Bleiwüsten sowie einfache Multiple-Choice-Tests sorgen dafür, dass Lernende schnell das Interesse verlieren und Informationen nicht im Gedächtnis bleiben. E-Learning-Angebote sollten Informationen deshalb auf anschauliche Weise darstellen. Dazu gehören zum Beispiel interaktive Videos, die Lerninhalte anhand von Alltagssituationen und Praxisbeispielen darstellen.

❸ Kurze Sessions

Da der Datenschutz bei vielen Prozessen im Arbeitsalltag eine Rolle spielt, müssen Mitarbeitende nachhaltig lernen, welches Verhalten in welcher Situation datenschutzkonform ist – und welches nicht. Allerdings dürfen E-Learning-Angebote nicht zu lange dauern: Schließlich sollen sie Teilnehmende entsprechend in ihren Arbeitsalltag integrieren können.

❹ Mehrsprachigkeit

Im Zuge der Globalisierung sind immer mehr Unternehmen international aufgestellt und beschäftigen Mitarbeitende mit verschiedenen ethnischen Hintergründen. In diesen Fällen bieten sich E-Learning-Dienste an, die mehrere Sprachen zur Verfügung stellen. Das ermöglicht individualisierte Kurse und eine bessere Nutzerfreundlichkeit.

❺ Überprüfung des Gelernten

Kurze Tests in E-Learnings helfen dabei, das Gelernte zu überprüfen beziehungsweise aufzuzeigen, wo Lernende noch einmal wiederholen müssen. Dabei kann es sich beispielsweise um ein Dialogspiel handeln, in dem Teilnehmende in die Rolle von einer Datenschutzbeauftragten schlüpfen und Fragen zur DSGVO-konformen Arbeit mit Kundeninformationen beantworten.

Die hohen Bußgelder und die Häufigkeit, mit der diese verhängt werden, zeigen den Bedarf nach regelmäßigen Lehrangeboten zum Thema Datenschutz und DSGVO auf. Sie müssen Mitarbeitenden vermitteln, wie sie personenbezogene Daten rechtskonform verarbeiten können und helfen, Unternehmen vor harschen Konsequenzen und Reputationsschäden zu schützen.

Philipp von Bülow, CEO von Lawpilots

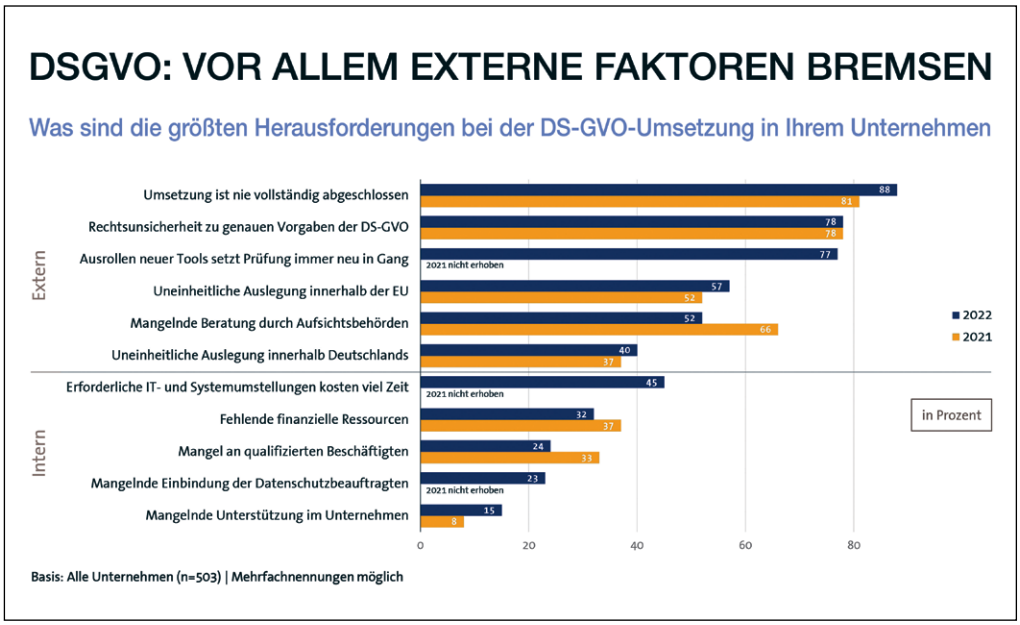


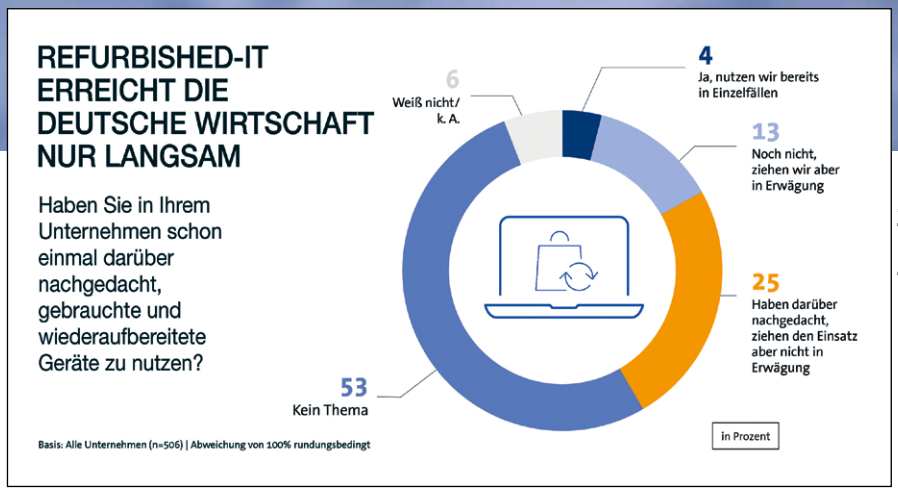
Bild: Datenschutz in der deutschen Wirtschaft: DS-GVO & internationale Datentransfers, Bitkom 2022

Dass die Umsetzung der DSGVO noch nicht weiter ist, liegt nach Ansicht vieler Unternehmen überwiegend an Gründen, die sie nicht selbst zu verantworten haben. Sie sehen sich vor allem mit Rechtsunsicherheit und einer widersprüchlichen Auslegung der Datenschutzvorgaben innerhalb Europas und zwischen den Bundesländern konfrontiert. „Datenschutz darf nicht zum Selbstzweck werden", sagt Bitkom-Hauptgeschäftsführer Bernhard Rohleder. „Aus Sicht der Unternehmen ist es der DSGVO bislang nicht gelungen, den Datenschutz zu vereinheitlichen, weder innerhalb der EU noch innerhalb Deutschlands. Deutschland kann sich auf Dauer nicht 18 verschiedene Datenschutz-Auslegungen leisten. Ob in München oder Hamburg, in Köln oder Schwerin: zumindest innerhalb Deutschlands müssen die gleichen Datenschutzregeln gelten."

KREISLAUFWIRTSCHAFT FÜR EINE LÄNGERE LEBENSDAUER

Die IT-Branche verursacht weiterhin Unmengen an Elektroschrott. Daher braucht es ein radikales Umdenken, wie mit IT-Geräten umgegangen wird. Recycling ist nicht ausreichend, die Grundsätze der Circular Economy können hingegen weitreichendere Veränderungen erzielen.

Autor: Emanuel Lippmann ***Redaktion: Lukas Steiglechner***



Quelle: „Digitalisierung und Klimaschutz in der Wirtschaft" Bitkom e.V.

Lediglich vier Prozent der befragten Unternehmen nutzt bereits in Einzelfällen refurbished Hardware. 13 Prozent ziehen dies immerhin in Erwägung. Allerdings ist die Nutzung von wiederaufbereiteten Geräten für drei Viertel entweder kein Thema oder ziehen den Einsatz nicht in Erwägung.

➤ Eine nachhaltigere IT ist keine neue Forderung. Darunter sammeln sich sämtliche Maßnahmen, die den technologischen Fortschritt mit Umweltschutz verbinden. Seit vielen Jahren schränkt der Gesetzgeber bereits die Verwendung zahlreicher schädlicher Substanzen in den Komponenten von IT-Geräten ein oder verbietet sie sogar ganz. Hinzu kommen Vorschriften für das Recycling von Elektroschrott. So wird das noch immer gängige Verschiffen von ausgemusterten Geräten in Entwicklungsländer, wo diese dann unter umwelt- und gesundheitsschädlichen Bedingungen zerlegt werden, inzwischen erschwert – zumindest auf dem Papier.

Lineares Wirtschaftsmodell dominiert weiter

Dennoch, das dominierende Wirtschaftsmodell ist nach wie vor linear: Natürliche Ressourcen werden genommen und daraus Produkte hergestellt, die weggeworfen werden, wenn sie nicht mehr gebraucht werden. Die Folgen liegen auf der Hand: Rohstoffe werden schneller abgebaut als sie zur Verfügung stehen. Einmal ausrangierte Produkte werden als Abfall verbrannt oder auf Deponien gelagert, was zum Verlust wertvoller und knapper natürlicher Ressourcen führt. Sowohl die Herstellung als auch der Transport von Produkten führen zudem zu Umweltverschmutzung und hohem Energieverbrauch.

Dem Circularity Gap Report zufolge entstehen rund 70 Prozent aller Treibhausgase während der Materialumschlags- sowie -nutzungsphase. Dieser hohe Anteil erklärt sich dadurch, dass eine große Menge der erzeugten Energie direkt oder indirekt in die Herstellung fließt. Entsprechend groß ist auch der Hebel einer Kreislaufwirtschaft: Gerade einmal 8,6 Prozent der weltweit im Einsatz befindlichen Rohstoffe werden nach Gebrauch wiederverwendet oder einem Recyclingprozess zugeführt. Eine Erhöhung dieser Quote würde laut dem Bericht bei dem Ziel helfen, die Erderwärmung bis 2032 unter zwei Grad zu drücken.

Kreislaufwirtschaft bedeutet mehr als Recyceln

Grundsätzlich bezeichnet Kreislaufwirtschaft oder Circular Economy ein Modell, bei dem Wirtschaftswachstum nicht mit der Ausbeutung und dem Verbrauch von natürlichen, nicht-regenerativen Rohstoffen einhergeht. Stattdessen werden Ressourcen möglichst lange im Wirtschaftskreislauf gehalten. Wird dieses Prinzip auf die IT gemünzt, bedeutet es, Geräte zu reparieren, sie aufbereitet wiederzu-

Bild: ipopba-123rf

verwenden und erst dann, wenn die Lebensdauer maximal ausgereizt ist, die Komponenten, Materialien und Rohstoffe fachgerecht zu recyceln. Das hat einen handfesten Grund: Basis-Kunststoffe beispielsweise erkennen mechanische Sortiermaschinen recht zuverlässig. Jede Verpackung und jedes Gehäuse hat allerdings in der Regel seine eigenen Additive, mit denen die Maschinen oft nicht zurechtkommen. Mit Hilfe des chemischen Recyclings – also dem Herunterbrechen der Kunststoffe auf ihre einzelnen Bausteine – lassen sich recycelte Kohlenstoff-Moleküle zwar einfacher wieder in die Wertschöpfungskette einbringen als Granulat aus dem konventionellen Recycling. Dieser Prozess ist aber sehr energieintensiv und belastet die Umwelt massiv. Eine weitere Herausforderung ist das sogenannte „Downcycling“: Im Vergleich zum Ausgangsmaterial haben wiederaufbereitete Stoffe oftmals eine schlechtere Qualität.

Umso wichtiger ist es, die Produkt- und Materiallebensdauer bereits in der Designphase zu berücksichtigen: Die Komponenten müssen leicht trennbar sein und dürfen keine gefährlichen Substanzen enthalten, die sie für das Recycling und die Verwendung in neuen Produkten ungeeignet machen. Zudem können etwa Platinen aus Flachsfasern oder Gehäuse aus Bio-Kunststoffen bestehen, die aus Abfällen bei der Papierherstellung gewonnen werden. Ein weiterer Punkt ist der Lebenszyklus von Geräten: Auch wenn PCs, Notebooks oder andere Hardware in Firmen ausgemustert werden, sind sie längst noch nicht reif für den Schrott, sondern können nach einer Wiederaufbereitung einen neuen Besitzer finden. Das Interesse an aufbereiteten Notebooks, Tablets oder auch Smartphones ist zwar da, erreicht die deutsche Wirtschaft aber trotzdem nur langsam. Die Bitkom-Studie „Digitalisierung und Klimaschutz in der Wirtschaft“ zeigt, dass nur vier Prozent der Unternehmen in Einzelfällen wiederaufbereitete Geräte nutzen. 13 Prozent tun dies noch nicht, erwägen es aber.

Nachhaltigkeit mit Software-Unterstützung

Wenn es um IT-Lösungen für Unternehmen geht, spielen neben der Verfügbarkeit von Ersatzteilen für Reparaturen einfache Möglichkeiten zum Upgrade eine wichtige Rolle. Durch die Nutzung von Support-Optionen wie Proactive Maintenance lassen sich mögliche Probleme zudem frühzeitig erkennen, sodass entsprechende Maßnahmen rechtzeitig eingeleitet und schwerere Schäden oder sogar Ausfälle vermieden werden können. Ein automatisierter Maintenance-Support vereinfacht in solchen Fällen das proaktive Identifizieren von Hardware- und Softwareproblemen. Daneben unterstützt auch die Verwendung von Software-Tools die längere Lebensdauer eines Geräts. Das ist beispielsweise dann der Fall, wenn die Upgrades von Firmware oder Security-Programmen frei verfügbar sind. So können auch Nutzer ohne Servicevertrag ihre Geräte jederzeit auf dem aktuellen Softwarestand halten und deren Sicherheit wie auch Kompatibilität gewährleisten. As-a-Service-Angebote wiederum, bei denen der Zugang zu Wartung, Reparatur und Upgrades in einer Dienstleistung enthalten ist, garantieren ebenfalls, dass ein Produkt länger im Einsatz ist.

Eine möglichst abfallfreie Kreislaufwirtschaft zu erreichen, klingt ehrgeizig – und das ist es auch. Das Erreichen des Ziels erfordert einen grundlegenden Wandel in der Art und Weise, wie über Produktdesign nachgedacht, welche Produkte gekauft und wie sie genutzt werden.

Emanuel Lippmann, Global Program Manager ESG, Dell Technologies

„DER KUNDE WILL EINE SCHLÜSSELFERTIGE LÖSUNG“

Mit steigender IT-Komplexität nehmen Systemhäuser eine neue Rolle an der Seite ihrer Kunden ein. IT-Haus-Geschäftsführer Thomas Simon erklärt im Interview, wie sich die Zusammenarbeit verändert hat, wo neue Schwerpunkte liegen und wie sich eine optimale Zusammenarbeit gestaltet.

Redaktion: Stefan Adelmann

➤ ***funkschau:*** *Herr Simon, wie hat sich in den vergangenen Jahren Ihre Rolle als IT-Systemhaus verändert? Sind Sie „nur“ externer Dienstleister oder im Zuge der Digitalisierung stärker in Geschäfts- oder sogar Entscheidungsprozesse involviert?*

Thomas Simon: Die Rolle des klassischen Systemhauses unterliegt einem ständigen Wandel. Waren wir im IT-Haus früher eher externer Dienstleister im Projekt oder für SLA-/Wartungs- oder Outsourcing-Themen, so nimmt der As-a-Service-Teil ebenso wie der Managed-Service-Anteil der Dienstleistungen stetig zu.

Bild: IT-Haus

THOMAS SIMON,
CEO des Systemhauses IT-Haus

funkschau: *Das hat sicherlich auch Einfluss auf Ihre Zusammenarbeit mit den internen IT-Abteilungen. Wie gestaltet sich diese heutzutage?*

Simon: Waren die IT-Abteilungen kundenseitig früher in der Make-Situation, so hat sich dies stark in Richtung „buy“ verändert. Einerseits aufgrund der Komplexität und Vernetztheit der heutigen Lösungen, andererseits aufgrund der Personal- und Ressourcenknappheit beim IT-Personal des Kunden. Heute möchte der Kunde eine weitgehend schlüsselfertig in seine IT integrierte Lösung in den Eigenbetrieb übernehmen oder diese als Service einkaufen.

funkschau: *Oft wird dazu geraten, Standardprozesse nach außen zu geben und die interne IT-Abteilung hingegen auf komplexe Transformationsthemen auszurichten. Ist diese Strategie sinnvoll?*

Simon: Der eigentliche Wert der internen IT ist – neben dem Betrieb unternehmensspezifischer Apps, für die es keinen oder nur wenig Standard(-betrieb) durch Dritte gibt – die Kenntnis der prozessualen und organisatorischen Abläufe des jeweiligen Unternehmens zu Nutzung und Wertbeitrag in digitalen Transformations- und Automatisierungsprozessen.

funkschau: *Sehen Sie sich als Systemhaus wiederum in der Rolle des Impulsgebers für komplexere Digitalisierungsvorhaben?*

Simon: Wir treiben Digitalisierungsthemen aktiv an. Das Systemhaus von heute ist Impulsgeber für viele Arten von Digitalisierungs- und Automatisierungsvorhaben wie Managed Print Solutions mit Roll-Out, automatisierter Überwachung und Belieferung sowie Service und Roll-Back, Digitale Signage Solutions, Device as a Service, automatisierte Betankungsverfahren für OS, Apps und Updates sowie MDM-Verwaltung – bis hin zur standardisierten Bereitstellung aller IT-Ressourcen.

funkschau: *Wo sehen Sie vor diesem Hintergrund grundsätzlich die wichtigsten Kernthemen, die Sie besetzen wollen?*

Simon: Absolute Kernthemen sind nach wie vor der Modern Workplace und das Arbeiten von überall aus, die Bereitstellung von Standard-Apps aus der Cloud und somit die Ankopplung der lokalen IT an die Cloud und die Bereitstellung der Core und Hybrid Infrastructure – egal ob On Prem, hybrid oder in der Cloud. Hinzu kommt die Integration von IT-Security-Asses vom Gateway bis zum Endpoint sowie die automatisierte Überwachung der IT-Netze, Apps und Services.

funkschau: *Hätten gerade kleine und mittelständische Unternehmen das Know-how und die Ressourcen, um diese Themen und die steigende Komplexität der IT überhaupt noch ohne externe Unterstützung stemmen zu können? Oder ist das ohne einen IT-Partner grundsätzlich nicht mehr möglich?*

Simon: Kleine und mittelständische Unternehmen treffen heute aus gutem Grund immer häufiger die „Buy-Entscheidung“. Sie lösen durch IT-Stellen gebundene Ressourcen auf und setzen diese gezielt für ihre hoch standardisierten Digitalisierungs- und Automatisierungsvorhaben ein. Der IT-Partner wird – zusammen mit der auf den Alltagsbetrieb spezialisierten internen IT – mehr und mehr zum Business Enabler und Business-Treiber.

funkschau: *Was sind wiederum die größten Herausforderungen und Hürden in der Zusammenarbeit mit Ihren Kunden und wie würde sich im Gegenzug eine ideale Zusammenarbeit gestalten?*

Simon: Die Zusammenarbeit mit unseren Kunden läuft umso besser, je besser wir die Kunden und ihre spezifischen Needs verstehen und der Kunde aufgeschlossen ist für „den neuen Weg der IT“. Ideal wird die Zusammenarbeit, wenn beide Seiten ein gutes Verständnis von robuster und resilienter IT entwickelt haben.

Matchmaker+

Business Netzwerk ITK

WEKA PRODUCTS & CONTENT

Unsere Premiumanbieter

ARCTIC WOLF | AvePoint | audiocodes | baramundi | datto | Delinea – Defining the boundaries of access

Draka – A Brand of Prysmian Group | dtm group – IT MANUFAKTUR | d.velop | ECOM | EKINOPS | enreach

EPOS | estos | G DATA – TRUST IN GERMAN SICHERHEIT | Gamma | getronics | GERMAN DATACENTER ASSOCIATION

GoTo | infopulse | ITscope | Jabra GN | kiwiko eG | littlebit TECHNOLOGY

NCP – SECURE COMMUNICATIONS | ninjaOne | PANDUIT | RingCentral | RITTAL | [sysob]:::

MC TECHNOLOGIES | UNICON | VERTIV | IHR LOGO JETZT BUCHEN!

Kontakt: itksales@weka-fachmedien.de Tel.: +49 (0)89.255 56-1390

matchmaker.funkschau.de

REDAKTION

Anschrift: Redaktion funkschau, WEKA Fachmedien GmbH, Richard-Reitzner-Allee 2, 85540 Haar, Telefon: (089) 25556-1351,Telefax: (089) 25556-1656, Internet: www.weka-fachmedien.de

Chefredakteur: Stefan Adelmann (STA) (V.i.S.d.P.), E-Mail: sadelmann@weka-fachmedien.de
Chefin vom Dienst: Dipl.-Ing. (FH) Alexandra Hose (AH), E-Mail: ahose@weka-fachmedien.de
Ressorts:
Dipl.-Journ. Diana Künstler (DK): Call- und Contact-Center, Netzwerke, Security, IoT, Messtechnik, E-Mail: dkuenstler@weka-fachmedien.de
Dr. Sabine Narloch (SN): UCC, Business Software, Cloud-Lösungen, Drucker
E-Mail: snarloch@weka-fachmedien.de
Lukas Steiglechner (LS), Datacenter
E-Mail: lsteiglechner@weka-fachmedien.de
Titel und Layout: Norbert Preiß,
E-Mail: npreiss@weka-fachmedien.de

Manuskripte, Programme, Tipps & Tricks, Leserbriefe bitte an die Anschrift der Redaktion. Für unverlangt eingesandte Manuskripte und Datenträger sowie Fotos übernimmt der Verlag keine Haftung. Die Zustimmung zum Abdruck wird vorausgesetzt. Das Verwertungsrecht für veröffentlichte Manuskripte, Fotos und Programme liegt ausschließlich beim Verlag. Mit der Honorierung von Manuskripten und Programmen erwirbt der Verlag die Rechte daran. Insbesondere ist der Verlag ohne weitere Honorierung berechtigt zur weltweiten und uneingeschränkten Veröffentlichung auf Papier und elektronischen Trägermedien. Der Autor erklärt mit der Einsendung, dass eingereichte Materialien frei sind von Rechten Dritter. Eine Haftung für die Richtigkeit der Veröffentlichung kann trotz sorgfältiger Prüfung durch die Redaktion vom Herausgeber nicht übernommen werden. Für veröffentlichte Manuskripte übernimmt der Verlag weder Gewähr noch Haftung. Schaltungen und verwendete Bezeichnungen müssen nicht frei sein von gewerblichen Schutzrechten. Die geltenden Bestimmungen sind zu beachten. Nachdruck, Übersetzung sowie Vervielfältigung oder sonstige Verwertung von Texten sind nur mit schriftlicher Genehmigung des Publishers erlaubt. Namentlich gekennzeichnete Beiträge geben nicht in jedem Fall die Meinung der Redaktion wieder.

MEDIABERATUNG

Sales Director: Eric Weis (Anschrift wie Verlag), Tel.: (089) 25556-1390
Account Manager: Sofie Steuer, Tel.: (089) 25556-1452; Nicole Wawrzinek, Tel.: (089) 25556-1087; Gina Gießmann, Tel.: (089) 25556-1576; Christine Philbert, Tel.: (089) 25556-1465;
Sales Operations Specialist: Christina Gottwald Tel.: (089) 25556-1351
Disposition: Jeanette Blaukat, Tel.: (089) 25556-1014
Anzeigenpreise nach Preisliste gültig ab 1.1.2021

VERLAG

Anschrift: WEKA Fachmedien GmbH, Richard-Reitzner-Allee 2, 85540 Haar, Telefon: (089) 25556-1000, Telefax: (089) 25556-1199, E-Mail: info@weka-fachmedien.de

Alleinige Gesellschafterin der WEKA Fachmedien GmbH ist die WEKA Group GmbH, Kissing
Geschäftsführer: Kurt Skupin, Matthäus Hose
Vertriebsleitung: Marc Schneider (089) 25556-1509
Herstellungsleitung: Marion Stephan
Sonderdrucke: Alle Beiträge können für Werbezwecke als Sonderdruck hergestellt werden.
Anfragen an: Melanie Griesbach, Tel.: (089) 25556-1440, E-Mail: mgriesbach@wekanet.de
Druck: L.N.Schaffrath, Marktweg 42-50, 47608 Geldern

Die funkschau erscheint monatlich (12 Ausgaben im Jahr).
95. Jahrgang
ISSN 0016-2841,
Vertriebskennzeichen ZKZ 3108

HIER KÖNNEN SIE BESTELLEN

Bestell- und Abonnement-Service: WEKA Fachmedien GmbH, c/o Zenit Pressevertrieb GmbH, Postfach 810640, 70523 Stuttgart, Tel: +49 (0) 711 7252 210; Fax: +49 (0) 711 7252 333, E-Mail: abo@weka-fachmedien.de

Bankverbindung: Postbank München, BLZ 70010080, Konto-Nr 9339809

Abonnementpreise:
Erscheinungsweise: 12 Ausgaben
Jahresabonnement Print Inland: 142,00 €, davon 112,60 € Heft, 29,40 € Versand
Jahresabonnement Print Ausland: 152,20 €, davon 112,60 € Heft, 39,60 € Versand
Einzelausgabe Print: 12,00 € inkl. der aktuellen MwSt., zzgl. 3,00 € Versandkosten
Jahresbezug digitales E-Paper: (Inland/Ausland) 58,00 € inkl. der aktuellen MwSt., ohne Versandkosten
Einzelausgabe digitales E-Paper: (Inland/Ausland) 4,99 € inkl. der aktuellen MwSt., ohne Versandkosten
shop.weka-business-communication.com

IHRE ANSPRECHPARTNER DER FUNKSCHAU

➤ STEFAN ADELMANN
Chefredakteur
Tel.: +49 89 25556-1352
sadelmann@weka-fachmedien.de

Advertorials, Sonderpublikationen
➤ ALEXANDRA HOSE
Leitende Redakteurin/CvD
Tel.: +49 89 25556-1354
ahose@weka-fachmedien.de

Security, Netzwerke/IoT, Call- und Contact-Center, Messtechnik
➤ DIANA KÜNSTLER
Stellv. Chefredakteurin
Tel.: +49 89 25556-1361
dkuenstler@weka-fachmedien.de

Cloud-Dienste/Managed Services, Software, Drucker
➤ DR. SABINE NARLOCH
Redakteurin
Tel.: +49 89 25556-1355
snarloch@weka-fachmedien.de

Datacenter
➤ LUKAS STEIGLECHNER
Redakteur
Tel.: +49 89 25556-1514
lsteiglechner@weka-fachmedien.de

➤ NATASCHA SCHÖNEMANN
Redaktionsassistenz
Tel.: +49 89 25556-1511
nschoenemann@weka-fachmedien.de

➤ NORBERT PREISS
Mediengestalter
Tel.: +49 89 25556-1365
npreiss@weka-fachmedien.de

INSERENTEN

funkschau

KOMMENDE AUSGABEN IM ÜBERBLICK

02/23 17. Februar 2023

Cloud-Dienste & Managed Services

Die hohe Nachfrage nach Managed Services ist laut aktuellem ISG-Index ungebrochen. So lag der jährliche Vertragswert der neu abgeschlossenen Managed-Services-Verträge im deutschsprachigen Raum, der größten Teilregion von EMEA, bei 1,1 Milliarden US-Dollar und übertraf damit den Vorjahreswert um mehr als das Doppelte. Das Wachstum ist auf die Stärke der ADM- und Infrastruktursegmente zurückzuführen. Doch der Mix aus steigenden Zinsen, zunehmender Energieknappheit, Problemen in den Lieferketten und einem Anhalten der Inflation werde aus Sicht von ISG dazu beitragen, dass sich die Nachfrage der Unternehmen nach IT- und Business-Diensten abschwächt. funkschau nimmt diese und weitere Entwicklungen im Markt für Managed Services unter die Lupe.

Und außerdem:

- Unified Communications
- IT-Dienstleister
- Drucker & Dokumentenmanagement

03/23 17. März 2023

Aus- und Weiterbildung

Die Kluft wächst: Auf der einen Seite ist die Digitalisierung von Prozessen und Geschäftsmodellen für Unternehmen überlebenswichtig, doch auf der anderen Seite ist der IT-Arbeitsmarkt nach wie vor leergefegt. Die Lösung für dieses Dilemma können Citizien Developer sein. Also IT-fremde Fachkräfte, die Software in standardisierten Entwicklungsumgebungen programmieren, ohne dafür Coding-Kenntnisse mitbringen zu müssen. Der Ansatz klingt vielversprechend – wirft aber auch einige Fragen für die Umsetzung auf.

Und außerdem:

- Datacenter
- Unternehmenssoftware
- Business Intelligence
- Branchenspezial: Medien

01/23 20. Januar 2023

Bild: dmitr3d-123rf

Trends 2023

Globaler Wettbewerbsdruck, zyklische Absatzmärkte und schneller technischer Wandel kennzeichnen die Hightech-Branche – und nicht nur diese. Laut Lever X sind Tools aus Bereichen wie dem Internet der Dinge (IoT), Blockchain, AR/VR, Metaverse oder Mobile LMS (Learning Management System) vielfältig und werden immer gefragter. Im Idealfall tragen sie zur Verbesserung von Geschäftsprozessen in Bereichen wie Fertigung, HR, Einzelhandel und Gesundheitswesen bei. Diese und weitere spannende Themen des kommenden Jahres im Überblick.

Cybersecurity-Prognosen

Welche Erkenntnisse mit Blick auf die Cybersicherheit von Unternehmen hat das Jahr 2022 gebracht? Und was erweist sich als die größte Cybersecurity-Bedrohung für 2023? Diese und weitere sicherheitsrelevante Fragen stellen sich derzeit. Zehn Security-Anbieter haben geantwortet und geben Einblick in ihre Erfahrungen und Einschätzungen.

Modern Workplace

Mit einer Contract Lifecycle Management-Software werden Verträge digital abgewickelt. Welche Schritte ein solches System übernimmt und was das für Vereinbarungen, wie zum Beispiel Bestellungen und Lieferantenverträge, in der Praxis bedeutet.

Server & Storage

Um mit wachsenden Datenmengen zurechtzukommen, braucht es immer mehr Speicherplatz. Doch wie lässt sich Storage auch nachhaltig gestalten? Mit Flash-Speicher kann der Stromverbrauch gesenkt und Energie gespart werden.

Branchenspezial
Öffentlicher Sektor

Änderungen aus aktuellem Anlass möglich.

business-netzwerk-itk.de

Eric Weis, Sales Director, Telefon +49 (0)89 25556-1390, eweis@weka-fachmedien.de