

DIGITAL BUSINESS

EXPERTENMAGAZIN FÜR DIGITALE TRANSFORMATION

CLOUD

Eine Publikation der WIN Verlag GmbH & Co. KG | Ausgabe-Nr.: 187



ENTSPANNT IN DIE

CLOUD

Schnell, einfach, effizient: So gelingt die Migration der IT

HOSTING

Container isolieren Software von ihrer Umgebung und stellen sicher, dass diese weiterhin gleichbleibend arbeitet.

RECRUITING

Next Shiny Object oder Game Changer? Wie KMU bei neuen Tools zwischen Hype und Innovation unterscheiden.

VERTRIEB

Kunden erwarten heute umfassende Beratung und Mehrwerte. Fünf aktuelle Lösungen für mehr Umsatz.



marconomy

B2B MARKETING DAYS

10. + 11. Oktober 2023

VCC Würzburg

Erhalten Sie
20% Rabatt
auf den aktuellen
Ticketpreis mit
dem Code
ECOMMERCE20

Strategien, Trends & Best Practices für B2B Marketer

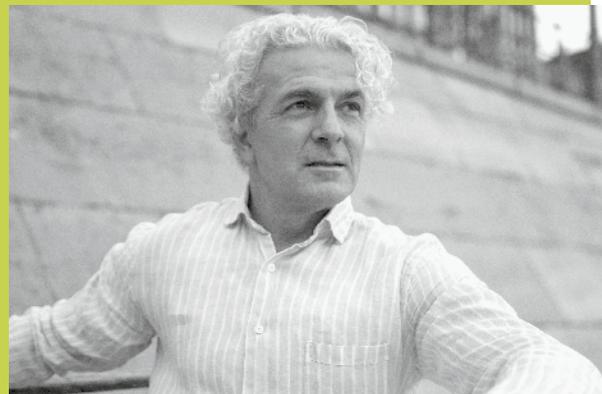
Bei den marconomy B2B Marketing Days am 10. und 11. Oktober profitieren Marketing- und Vertriebsverantwortliche aus dem Mittelstand vom Know-how-Austausch in interaktiven Formaten, lernen neue Technologien kennen und schaffen Strategien für ihr B2B-Marketing.

www.b2bdays.de



Eine Veranstaltung von **marconomy** – einer Marke der **VOGEL COMMUNICATIONS GROUP**

EDITORIAL



Liebe Leserin, lieber Leser

• Am 20. und 21. September 2023 gastierte in Köln die Digital X, die von der Telekom gehostete Plattform mit 300 Partnerfirmen, 250 Speakern und 50.000 Teilnehmern, die Deutschland in der Digitalisierung voranbringen soll. Das ist offenbar dringend nötig, wie Hagen Rickmann, Schirmherr des Events und Geschäftsführer Geschäftskunden Telekom Deutschland sichtlich zerknirscht den Journalisten offenbarte: Im europäischen Vergleich steht Deutschland aktuell auf Platz 13, 2021 Platz war es noch Platz 12. **Statt vorwärts geht es rückwärts.** „Nur ein Drittel der Unternehmen wollen mehr in Digitalisierung investieren, 2021/22 waren es noch die Hälfte“, so Hagen Rickmann. „46 Prozent der Unternehmen sprechen laut Bitkom inzwischen mehr über die Risiken als die Chancen der Digitalisierung. Das ist **ein ziemlich großes Problem.**“

Tim Höttinges, CEO der Telekom, rief die Gäste in seiner Eröffnungsrede angesichts dieses Szenarios zu Optimismus auf. Um die Dinge zum Besseren zu wenden, sei **radikale Transparenz** erforderlich. Zum Beispiel darüber, dass Deutschland als einstiger Exportweltmeister inzwischen mehr importiere als exportiere. Dass Rohstoffe wie Lithium, Getreide, Gas und Daten **wirtschaftspolitisch als Waffe eingesetzt** werden. Vor allem die Politik müsse die daraus resultierenden Auswirkungen für Wirtschaft und Gesellschaft diskutieren und klarmachen, was zu tun ist, um Deutschland wieder zu einer führenden Wirtschaftsnation zu machen. Dazu brauche es aber die passenden politischen Rahmenbedingungen. Das war zwischen den Zeilen durchaus eine **harsche Kritik an der aktuellen Politik** der Rot-Grünen Koalition.

Was ihm besonders bitter aufstieß: Bei Europas Unternehmen beträgt der Return auf das eingesetzte Kapital im Durchschnitt sechs Prozent, in den USA 14 Prozent.

Das mache es Unternehmen vergleichsweise schwerer, in die Zukunft zu investieren. Zudem werden die Kommunikationsnetze zur Verfügung gestellt, ohne das große US-Konzerne sich daran beteiligen. „80 Prozent des Datenverkehrs werden von den Hyperscalern unkontrolliert und unbezahlt benutzt“, so Höttinges und plädierte für einen **„Fair Share“**. „Für eine Infrastruktur von Welt-niveau sollten die Konzerne, die damit Kohle machen, künftig auch dafür bezahlen. Ich hoffe inständig, dass die Bundesregierung hier entsprechend agiert“, richtete er einen einigermaßen verzweifelt klingenden Apell in Richtung Berlin.

Deutschland brauche eine **Vision für die Zukunft**. Zum Beispiel von 27 Europas zu einem Europa, samt Bürokratieabbau. Von Verzögerung durch Regulierung zu schnellen Entscheidungen und schneller Umsetzung. Von systemischen Nachteilen zu einem „Level Playing Field“. Von Laissez-faire zur Leistungskultur. Aktuell sehe er keinen Plan zum Umbau einer nachhaltigen Gesellschaft angesichts extrem hoher Energiepreise. „Deutschland muss protektionistischer werden, bevor unsere Unternehmen von anderen platt gemacht werden. Dazu gehört auch, Industrien auch die Chance zu geben, mit gleichen Wettbewerbsbedingungen am Markt zu bestehen.“ Und warnte abschließend: „Wer keine Strategie hat, ist Teil der Strategie eines anderen.“

In diesem Sinne hoffe, ich, dass Sie eine Vision und eine Strategie für Ihr Unternehmen haben. Anregungen, wie digitale Tools Ihren Weg dahin unterstützen können, finden Sie wieder reichlich in der aktuellen Ausgabe. •

Ihr **HEINER SIEGER**, Chefredakteur
DIGITAL BUSINESS CLOUD
hsi@win-verlag.de



SEITE 14 – 15

Fit für den digitalen Produktpass

Das Konzept des digitalen Zwillings ist ein zentraler Baustein für mehr Nachhaltigkeit und Wettbewerbsfähigkeit.



SEITE 28 – 29

Start aus dem Stand

Container isolieren Software von ihrer Umgebung und stellen sicher, dass diese gleichbleibend arbeitet.

SEITE 6 – 12

Entspannt in die Cloud

Schnell, einfach, effizient: So gelingt die Migration der IT.



SEITE 30 – 31

Revolution im Service

Mit ihrer Fähigkeit zur Analyse komplexer Zusammenhänge verändert generative KI die Welt des Kundenservices.



SEITE 19 – 23

HR insight

- 01 Recruiting: Unterscheiden zwischen Hype und Innovation
- 02 Software-Entwickler: Gemeinsam statt einsam



DIGITAL BUSINESS CLOUD

05

	TITEL	
06	Alternative Wege in die Cloud	
08	Maßanzug statt Massenabfertigung	
10	Transparenter Fahrplan	
11	Keine Angst vorm Anbieterwechsel	
12	Das Ende unzähliger Insellösungen	
	KI	
13	Fluch oder Segen	
	DIGITAL TWIN	
14	Fit für den Digitalen Produktpass	
	KI	
16	Lernen von Hollywood Studios	
	FRISCH AUSGEPACKT	
18	News	
	HR-INSIGHT	
19	Game-Changer	
20	Jenseits des Obstkorbs	
22	Gemeinsam statt einsam	
	ECM	
24	Out of the box	
	ID-PRÜFUNG	
26	Digital mit Brief und Siegel	
	DIGITALE TRANSFORMATION	
27	Kundenfokus und Turbotempo	
	HOSTING	
28	Start aus dem Stand	
	GENERATIVE KI	
30	Revolution im Service	
	UNIFIED COMMUNICATIONS	
32	UC oder UCaaS – die optimale Lösung finden	
	CRM	
33	Prozesse konsequent zu Ende gedacht	
	VERTRIEB	
34	Fünf Gamechanger für mehr Umsatz	
	5G	
36	Der Mittelstand kann deutlich profitieren	
	SECURITY SPECIAL	
38	Ransom(every)ware?!	
40	So verderben Händler Hackern das Geschäft	
42	Im Notfall: eine „Blutwäsche“ für das AD	
44	Raus aus der Shadow-IT-Falle	
46	Sind Ihre Salesforce- und AWS-Daten wirklich sicher?	
48	Kriminelle Spiele ohne Grenzen	
50	Datenschutz ist Katastrophenschutz	
	IT & SUSTAINABILITY	
52	Nachhaltigkeit messbar machen	
03	Editorial	
51	Marketplace	
54	Vorschau	
54	Impressum	

Alternative Wege in die Cloud

Die Migration in die Cloud kann für Unternehmen eine entmutigende Aufgabe sein, die eine detaillierte Planung und viele Ressourcen erfordert. Dabei bietet die Nutzung von Cloud-Diensten Vorteile wie Kosteneinsparungen, kürzere Markteinführungszeiten, Skalierbarkeit und vieles mehr, sagt Matthias Pfützner* von Red Hat.

VON CAROLINA HEYDER

DEN GOLDENEN WEG, um die Digitalisierung im Unternehmen voranzutreiben, gibt es nicht. Wer alles In-House meistern möchte, steht oft vor einer Mammutaufgabe, die sich – aufgrund IT-Infrastruktur oder personellen Faktoren – kaum bewältigen lässt. Eine gute Möglichkeit der Herausforderung gerecht zu werden, ist auf Dienste oder Systeme in oder aus der Wolke zurückzugreifen. Einen genauen Blick darauf zu werfen, lohnt sich.

Digital Business Cloud_Die Migration in die Cloud ist für viele eine Herausforderung. Was sind, Ihrer Erfahrung nach, die häufigsten Probleme, mit denen Unternehmen kämpfen?

Matthias Pfützner_Bei einer Migration in die Cloud können potenziell vielfältige Probleme mit unterschiedlichen Ursachen auftreten. Das Wichtigste ist immer, dass ein Unternehmen zum Projektstart die Gründe für den Cloud-Einstieg genau definiert – verbunden mit einer klaren Festlegung der Ziele. Daraus folgt, dass Probleme typischerweise dann auftreten, wenn man nicht genau weiß, was man warum machen will. Prinzipiell muss im Cloud-Kontext zudem berücksichtigt werden, dass es keine Lösung für alles und alle gibt. Die Herausforderungen sind somit immer unternehmensspezifisch und die

hier gilt also: Die jeweiligen konkreten Vorteile sind immer abhängig davon, was man aus der Cloud verwendet.

Zum Beispiel: Nutzer der Microsoft Office Suite, insbesondere des Exchange-Servers, merken kaum einen Unterschied, weil die Services aus der Cloud den ehemals im eigenen Rechenzentrum angebotenen Diensten sehr ähnlich sind. Wenn aber ein Unternehmen die im eigenen Rechenzentrum betriebene SAP-Umgebung durch eine Salesforce-Implementierung ablöst, kann der Unterschied sehr viel größer sein. Die Ermittlung des Vorteils ist dann auch sehr viel schwieriger, da Aspekte wie die unter Umständen erforderliche Umschulung der Mitarbeiter hinzukommen, die über den reinen Austausch eines Exchange-Servers im eigenen Rechenzentrum durch einen Server in der Azure Cloud oder auch einer anderen Cloud hinausgehen.

Generell bestehen bei der Cloud-Nutzung deutliche Einsparpotenziale hinsichtlich der erforderlichen Ausgaben für eigene Server, des benötigten Platzes im Rechenzentrum und unter Umständen im Hinblick auf Software-Lizenzen und eigenes IT-Personal. Allerdings müssen hier dann die laufenden Kosten der Dienste aus der Cloud gegengerechnet werden, um letztlich einen etwaigen finanziellen Vorteil bestimmen zu können.

„Das Wichtigste ist immer, dass ein Unternehmen zum Projektstart die Gründe für den Cloud-Einstieg **genau definiert** – verbunden mit einer klaren Festlegung der Ziele“.

Probleme können von einer mangelnden Akzeptanz der Mitarbeitenden bis hin zu komplett gescheiterten Projekten reichen.

Digital Business Cloud_Was sind die konkreten Vorteile der Nutzung von Cloud-Diensten?

Matthias Pfützner_Unternehmen müssen sich nicht mehr um das Patchen der eigenen Systeme, Updates oder den Ersatz der Hardware im eigenen Rechenzentrum kümmern. Viele dieser Vorteile gab es aber auch schon vor der Cloud durch die Nutzung von Hosting-Angeboten. Auch

Digital Business Cloud_Wie lange dauert es, bis Unternehmen davon profitieren?

Matthias Pfützner_Dies hängt vom jeweiligen Cloud-Projekt ab. Eine pauschale Antwort auf die Frage gibt es deshalb nicht.

Digital Business Cloud_Für wen kommen Cloud-Dienste eher in Frage, für KMUs oder Großunternehmen? Sind sie für Unternehmen aller Branchen geeignet?

Matthias Pfützner_Prinzipiell gibt es hier keinen Unterschied. Sowohl KMU als auch Großunternehmen aller

Branchen können von den Diensten aus der Cloud profitieren.

Digital Business Cloud_Welchen Weg in die Cloud sollten Unternehmen bevorzugen, gibt den richtigen Weg in die Cloud?

Matthias Pfützner_Nein, einen allgemein richtigen oder effizientesten Weg gibt es nicht. Ein kleines Unternehmen etwa hat ganz andere Anforderungen an seine IT als ein großer weltweit agierender Automobilkonzern. Wichtig ist daher, dass man weiß, was man braucht, was man will und sich dabei auch gut beraten lässt.

Digital Business Cloud_Werden Cloud-Dienste attraktiver für Unternehmen, wenn es darum geht, neue Technologien wie KI(-Funktionen) zu implementieren?

Matthias Pfützner_Auch diese Frage lässt sich nicht pauschal beantworten, denn nicht jedes Unternehmen braucht immer sofort neue Technologien. Im Kontext von KI ist die Cloud aber mit Sicherheit ein guter Einstiegspunkt, da ein Unternehmen hier mit vergleichsweise geringem Aufwand Erfahrungen sammeln und lernen kann, ohne dass die mit dieser Technologie verbundenen relativ hohen Einstiegskosten anfallen.

Digital Business Cloud_Welche Best Practices sollten bei der Sicherheit bezüglich Cloud-Dienste gelten? Worauf sollten Unternehmen achten?

Matthias Pfützner_Generell kann man zunächst sagen, dass Cloud-Anbieter vielfach eine höhere Sicherheit bieten können, als es bei der Nutzung von Diensten aus dem eigenen Rechenzentrum möglich ist. Hier wären wir beim Thema Economies of Scale. Als Nutzer von Services aus der Cloud ist aber insbesondere in der EU die nun in Kraft getretene DORA (Digital Operational Resilience Act)-Verordnung zu beachten. Sie schreibt unter anderem vor, dass Unternehmen, die finanzielle Transaktionen tätigen, ausfallsicher aufgestellt sein müssen. Im Umkehrschluss bedeutet dies, dass Unternehmen eine Abhängigkeit von den Diensten eines einzigen Cloud-Providers vermeiden müssen. Eine Alternative zu einem solchen Lock-in stellt die Nutzung von hybriden Cloud-Lösungen dar.

Matthias Pfützner

ist als Senior Solution Architect bei Red Hat für das Thema Cloud in der DACH.

Digital Business Cloud_Technologie hin oder her, aber wie sollte die Belegschaft einbezogen werden?

Matthias Pfützner_Es ist immer davon abhängig, in welcher Form und in welchem Umfang Cloud-Services genutzt werden. Wenn die Belegschaft unmittelbar betroffen ist, dann sollte sie auch eingebunden werden. Wird zum Beispiel ein bisher selbst betriebenes Online-Termin-Buchungssystem durch einen fertigen Cloud-Service ersetzt, sind die Mitarbeiter nicht direkt betroffen. Wenn es aber um die Ablösung einer eigenen SAP- durch eine Salesforce-Umgebung geht, dann sollte die Belegschaft frühzeitig über die anstehenden Änderungen informiert werden.

Digital Business Cloud_Können Sie uns einen Tipp verraten für den Fall, dass Unternehmen bei der Migration in die Wolke die Nutzung von Cloud-Diensten in Anspruch nehmen wollen?

Matthias Pfützner_Unternehmen sollten sich zunächst genau überlegen, was sie wie durch was ersetzen wollen. Dabei kann die Unterstützung durch externe Consultants durchaus von Vorteil sein. Nicht zuletzt müssen Unternehmen beim Weg in die Cloud auch immer Datenschutzaspekte und die digitale Resilienz im Blickfeld behalten. •



Maßanzug statt Massenabfertigung

Planen Unternehmen ihre IT-Infrastruktur in die Cloud zu verlegen, stehen sie oft vor einer Vielzahl an Herausforderungen. Wie können Cloud-Anbieter sicherstellen, dass Kunden die Migration gelingt?

VON DANIEL ARABIÉ

DIE WAHL DES RICHTIGEN CLOUD-ANBIETERS IST – angesichts der Angebotsmenge – meist gar nicht so einfach. Für Unternehmen liegt es nahe, sich an den Großen der Branche zu orientieren. Hyperscaler sind bekannt und glänzen durch umfangreichen Service. Den großen Anbietern von Cloud-Speicherdiensten fehlt es jedoch oft an der Fähigkeit, die Probleme ihrer Kunden individuell anzugehen. Ihr wachsendes Dienstleistungsportfolio zeigt, dass sie sich nicht mehr nur auf eine Sache spezialisiert haben – nämlich Cloud-Speicher – sondern, dass sie sich darauf konzentrieren, ständig neue Produkte hinzuzufügen, um ihren Gewinn zu steigern.



Daniel Arabié
ist Country Manager Central Europe beim Hot-Cloud-Speicheranbieter Wasabi Technologies.

Wenn sich Unternehmen für Hyperscaler entscheiden, gehen sie oft langfristige Verpflichtungen ein. Zudem erschweren ihnen hohe Ausstiegskosten bei der Verlagerung von Daten die Migration von Anbieter zu Anbieter.

Cloud-Migration: Branchen und Herausforderungen

Der Umzug in die Cloud gestaltet sich nicht für jedes Unternehmen gleich, da jeder Sektor seine ganz eigenen Anforderungen an die IT-Struktur hat. So können im Finanzbereich beispielsweise die Integration von Legacy-Systemen

und das Sicherstellen von reibungslosen Transaktionsabläufen eine Herausforderung sein. Unternehmen im Finanzsektor verarbeiten sensible, personenbezogene Daten, die es um jeden Preis entlang strenger Richtlinien zu schützen gilt. Eine Cloud-Infrastruktur muss also entsprechend compliant sein.

Im Gesundheitssektor sind personenbezogene Daten nicht minder sensibel zu behandeln; Healthcare-Organisationen müssen jedoch zusätzlich sicherstellen, dass bei der Cloud-Migration immer die Interoperabilität zwischen verschiedenen IT-Systemen innerhalb der Organisation gewährleistet ist.

Industrieunternehmen stehen wiederum vor der Herausforderung, komplexe IT-Infrastruktur, die mit einer Vielzahl von Maschinen und Geräten verbunden ist, zu verlagern. Probleme bei der Migration, oder Ausfälle durch einen Service, der der Systemkomplexität nicht gewachsen ist, hätten im Ernstfall ein wirtschaftliches Desaster für das Unternehmen – und unter Umständen leere Regale beim Endkunden – zur Folge. Die Hürden neuer Cloud-Kunden lassen sich jedoch auf drei Kernherausforderungen reduzieren: Preis, Performance, Sicherheit.

Den Unterschied machen: Zeit, Expertise, Kundennähe

Unternehmen brauchen einen günstigen Cloud-Anbieter, der ihnen die beste Performance liefert und dabei alle gesetzlichen Standards einhält. Diese Situation eröffnet Cloud-Anbietern eine gute Ausgangslage, um die spezifischen Probleme ihrer Kunden zu lösen. Unternehmen sollten sich an die Cloud-Anbieter wenden, die ihren Kunden beratend zur Seite stehen, indem sie eine gründliche und vollständig personalisierte Bedarfsanalyse durchführen.

Unternehmen sollten sich an genau die Cloud-Anbieter wenden, die ihren Kunden beratend zur Seite stehen, indem sie eine **gründliche und vollständig personalisierte Bedarfsanalyse** durchführen, um die Anforderungen und Ziele des Kunden und der Branche zu verstehen.

ren, um die Anforderungen und Ziele des Kunden und der Branche zu verstehen. Kundenberater müssen jeden Geschäftsprozess kennen und die damit verbundene IT-Infrastruktur sowie die zukünftigen technischen Anforderungen, die mit der Cloud-Migration einhergehen. Sie müssen vom Cloud-Experten zum Branchenexperten werden.

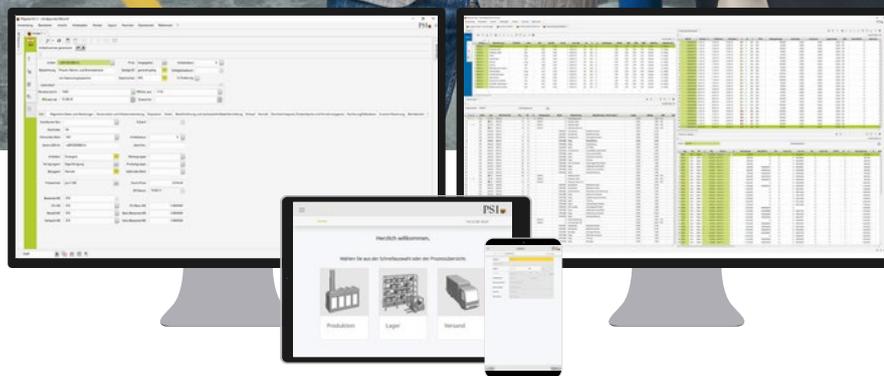
Auf Basis der Bedarfsanalyse entwickeln Cloud-Anbieter maßgeschneiderte Lösungen für den Kunden. Dies kann die Auswahl der richtigen Cloud-Plattform, Cloud-Services und Migrationsstrategien beinhalten, die den spezifischen Anforderungen des Kunden gerecht werden. Es gilt: Je individueller die Beratung, desto besser. Dabei sollten Anbieter eng mit kundeninternen, technischen Experten zusammenarbeiten, um die Anforderungen der Unternehmens genau zu verstehen und entsprechend individuelle technische Lösungen zu entwickeln. Auch der grundsätzliche Zeitmangel seitens der Hyperscaler ist ein Chancengewinn für Kundenberater kleinerer Cloud-Anbieter: Sie sollten sich die Zeit nehmen, um im Transformationsprozess Schulungen und Workshops zu organisieren. Diese bereiten auf die Cloud-Migration vor und stellen sicher, dass die Teams die neuen Technologien und Prozesse verstehen und nutzen können. Kundenberater bleiben während des gesamten Migrationsprozesses mit dem Kunden in Kontakt, um den Fortschritt zu überwachen und Feedback zu sammeln. Bei Problemen oder Hindernissen kann der Sales Manager rechtzeitig reagieren und Lösungen anbieten. Die Devise ist auch hier: Berater müssen sich die Zeit nehmen, die Hyperscaler

nicht aufbringen können und fachlich tiefe Branchenexpertise anwenden, wo sie können.

Fazit

Cloud-Migration gestaltet sich je nach Branche unterschiedlich. Daher ist es wichtig, einen Cloud-Anbieter zu wählen, der maßgeschneiderte Lösungen für die spezifischen Probleme seiner Kunden entwickelt. Cloud-Storage-Anbieter sollten beratend tätig sein und auf die individuellen Bedürfnisse ihrer Nutzer eingehen: indem sie sich Zeit nehmen, sich Branchenwissen aneignen und ihre Beratung entsprechend individuell gestalten. •

Mehr als Software
Wir stehen nicht nur für
exzellente Software, sondern
auch für kompetente Beratung
und Know-how-Transfer



www.psi-automotive-industry.de

Intelligent Production **PSI** 

Transparenter Fahrplan

Die Vorteile von Cloud-Datenbanken sind bekannt: Skalierbarkeit, Flexibilität und geringere Kosten. Schlecht vorbereitet, kann der Weg dorthin allerdings holprig sein. Unternehmen müssen vorab prüfen, auf welchem Stand und ob ihre Datenbanken schon cloud-ready sind. Toolgestützt gelingt dieser Prozess einfach und effizient.

VON MARKUS HAHN

VIELEN UNTERNEHMEN, DIE IHRE DATENBANKEN in die Cloud migrieren möchten, fehlt es (nicht zuletzt aufgrund historisch gewachsener Infrastrukturen) an der notwendigen Übersicht: über ihre Datenbank-Infrastruktur, über die Applikationen, die im Einsatz sind, und auch darüber, welche Systeme mit den Datenbanken kommunizieren. Damit das Migrationsvorhaben reibungslos

viele Unternehmen verschiedene Datenbanksysteme wie Oracle-, SQL- oder auch Db2 parallel nutzen; für jede von ihnen ist eine individuelle Migrationsstrategie erforderlich, damit entscheidende Funktionen nicht verloren gehen.

Die Konsequenz: Unternehmen stellen oft fest, dass ihre Datenbanken und die dazugehörigen Applikatio-

Ein Austausch sensibler Daten mit Dritten ist nicht notwendig, denn das System greift ausschließlich auf die bereitgestellten Daten über Datenbankstrukturen und Systeme zurück – ohne sich diese zu merken. Die Lösung gibt Einblicke in die Eigenschaften der IT-Systeme, zeigt Einsparpotenziale für verschiedene Cloud-Umstiegsoptionen und ermittelt Chancen und Risiken der bevorstehenden Migration.

In Eigenregie ein digitales Assessment durchführen

Diese Bandbreite wird vor allem dadurch ermöglicht, dass die Expertise unterschiedlicher Partner in die gemeinsame Lösung eingeflossen ist: Während Logicalis als Azure-Spezialist umfassendes Know-how in Datenbanken sowie die passenden Managed Services beisteuert und zudem das Projektmanagement übernimmt, stellt Microsoft die Infrastruktur in der Cloud-Umgebung bereit. Die weiteren Partner wie Prodyna, Maiborn-Wolff sowie Cybertec übernehmen weitere Leistungen rund um Applikationsmodernisierung und -transformation.

Unternehmen können dieserart in Eigenregie ein digitales Assessment ihrer Datenbankinfrastruktur durchführen und Datenbanken automatisiert in die Cloud migrieren – auf Grundlage eines transparenten Fahrplans. Sie erhöhen so die Migrationsgeschwindigkeit deutlich, halten die Kosten gering und müssen weniger personelle Ressourcen einsetzen. •



Der AUTOR
Markus Hahn

ist Chief Technology Officer der Logicalis GmbH.

gelingt, ist dieses Wissen allerdings unerlässlich. Die Verantwortlichen müssen darüber im Bilde sein, inwieweit sie ihre On-Premises-Infrastruktur anpassen müssen, und ob sie dies mit ihren internen Ressourcen abbilden können.

Überblick verschaffen und toolgerecht vorgehen

Kennen sie überhaupt die notwendigen Ressourcen, die sie für die Migration ihrer On-Premises-Datenbank in die Cloud benötigen? Und haben sie bereits einen Überblick, welche Anpassungen die bestehende IT-Infrastruktur erfordert, um auf Ihre Datenbank in der Cloud zugreifen zu können? Nicht zu vergessen ist, dass

nen noch nicht bereit für eine Migration sind und das Projekt zu viele Ressourcen beanspruchen würde. Die Migrationsprojekte verzögern sich infolgedessen oder werden gar ganz abgeblasen – zu Lasten der Wettbewerbsfähigkeit. Einen Ausweg aus diesem Dilemma bietet eine toolgestützte Herangehensweise.

Von der Analyse bis zur Migration

Tools, wie das Open Source Tool Atroposs, können den Weg in die Cloud deutlich vereinfachen. Bei Atroposs handelt es sich um eine browserunabhängige Webanwendung, die auf dem offenen W3C-Standard WebAssembly basiert und keine Installation auf Unternehmensservern benötigt.

Keine Angst vorm Anbieterwechsel

Es gibt diverse Gründe den Cloudanbieter zu wechseln.

Ein aktueller: die Preiserhöhungen großer Cloudanbieter. Doch viele scheuen die Veränderung – weil sie Angst um die Sicherheit ihrer Daten haben. Dabei könnte alles so einfach sein.

VON ANDREAS STEFFEN

JETZT HABEN WIR DEN SALAT: Immer mehr Unternehmen speichern ihre Daten in der Cloud und verleihen den Anbietern von Cloudlösungen immer mehr Macht und Einblick. So wundert es nicht, dass der ein oder andere die Gelegenheit nutzt und seine Preispolitik anpasst. Ein Beispiel: Microsoft. Der Konzern hat im April 2023 im Euroraum signifikante Preissteigerungen vorgenommen und damit nicht wenige Kunden verärgert. Viele denken deshalb über einen Anbieterwechsel nach – trauen sich aber nicht, weil sie unter anderem Angst um ihre Datensicherheit haben.

Angst ist ein schlechter Ratgeber

Es ist richtig, sich um die Datensicherheit zu sorgen. Denn die Verantwortung liegt immer beim Dateneigentümer – egal was Cloudanbieter mit ihren Security-Versprechen versuchen, zu suggerieren. Aber mit ein paar geschickten Schachzügen lässt sich dieses Thema problemlos regeln – für jetzt und immer. Datenzentrische Verschlüsselung heißt das Zauberwort. Sie sorgt dafür, dass Daten niemals als Klardaten das Unternehmen verlassen, sondern immer nur verschlüsselt. Wer auf dieses Prinzip setzt, hat die meisten Sicherheits- und Datenschutzanforderungen auf einen Schlag gelöst. Nicht nur, dass das Unternehmen sich wegen der DSGVO keine Gedanken mehr machen muss. Es kann auch den Attacken von Cyberkriminellen entspannter gegenüber treten, denn diese können mit verschlüsselten Daten nichts

anfangen. Das Unternehmen ist und bleibt Herr über seine Daten. Deshalb muss es sich auch bei der Suche nach einem neuen Cloudanbieter keine Sorgen machen.

Feel free!

Wer seine Daten also von Anfang an verschlüsselt, hat alle Freiheiten der cloudifizierten Welt. Das gilt natürlich auch für den Cloudanbieterwechsel – egal, ob dieser aus wirtschaftlichen Gründen erfolgt oder weil man unzufrieden mit dem Service ist.

Wenn Unternehmen selbständig dafür sorgen, dass ihre Daten bei egal welchem Cloud-Anbieter und unabhängig vom Standort des Rechenzentrums sicher sind, können sowohl die wirtschaftlichen als auch technischen Vorlieben voll ausgespielt werden. In Sachen Datensicherheit spielt ein Anbieterwechsel dann zumindest keine Rolle mehr. Aber worauf kommt es dabei an? Vor allem, dass bei der Datenverschlüsselung die Daten nicht erst in der Cloud verschlüsselt werden, sondern bereits ab dem Zeitpunkt, wenn sie die geschützte Umgebung des Unternehmens verlassen. Eine datenzentrische Verschlüsselung für das Arbeiten in der Cloud gelingt dann, wenn die Daten bereits innerhalb des Unternehmens mit einem dedizierten Gateway – in Form eines Proxys – verschlüsselt beziehungsweise tokenisiert werden.

Der AUTOR

Andreas Steffen ist CEO von eperi.

Verschlüsselung und Funktionalität müssen Hand-in-Hand gehen

Allerdings ist es mit einer einfachen Verschlüsselung der Daten in Verbindung mit der Cloud meist nicht getan. Entscheidend ist es, dass ein derartiges Gateway nicht nur die Verschlüsselung des reinen Dateiverkehrs unterstützt, sondern auch die Funktionalität der Anwendungen wie Microsoft 365, SharePoint, HubSpot oder Salesforce. Erst dann können die besonderen Vorteile der Cloud und der Cloud-Anwendungen trotz höchstem Datenschutz in vollem Umfang genutzt werden. So geht kompromissloser Datenschutz für jede Cloud und für maximale Freiheit beim Anbieterwechsel. •

Das Ende unzähliger Insellösungen

Die BPV GmbH aus Unna wuchs in wenigen Jahren vom Telekommunikations-Vertriebspartner zum führenden Full-Service-Partner in IT und Telekommunikation. Das Wachstum brachte Probleme mit sich: Aus einer simplen ERP-Lösung erwuchs eine heterogene IT-Systemlandschaft ohne Schnittstellen. Die Lösung: eine moderne, flexible und anpassungsfähige Cloud-ERP-Lösung.

VON UDO HENSEN

EIN EXPANDIERENDES UNTERNEHMEN benötigt die entsprechende ERP-Software, die mitwächst und unterstützt. Ist dies nicht gegeben, wird die ERP immer nur ergänzt durch Drittlösungen, was irgendwann zu einem Flickenteppich führt. Davon kann die BPV GmbH ein Lied singen. Das Unternehmen startete 2013 als Vertriebspartner für TK-Lösungen und ist jetzt einer der größ-

Mit expandierendem Produktportfolio und wachsenden Lageranforderungen stieß dieses System schnell an die Grenzen. Auch die Zahl der eingesetzten Drittlösungen wuchs deshalb rasant, es entstand eine heterogene IT-Systemlandschaft ohne Schnittstellen: CRM, Ticketsystem, Warenwirtschaft, Rechnungsstellung, Buchhaltung, Urlaubsorganisation, Projekt- und Fuhrparkmanagement

All diese Anforderungen erfüllte die ERP-Lösung von GEBRA-IT.

Testprojekt überzeugte auf Anhieb

Ein Testprojekt zur Retouren-Verwaltung überzeugte sofort, und innerhalb weniger Monate wurden alle geforderten Workflows und Prozesse mit Low-Code neu gestaltet, viele davon automatisiert.

„Die GEBRA-Suite ist einzigartig – kein vergleichbares Systemhaus lässt so eine Flexibilität zu. Unser Unternehmen und unsere Prozesse können mit keinem Standardprodukt abgebildet werden“, sagt Maximilian Limburg, Director of Operation bei der BPV-Unternehmensgruppe. „Deshalb sind wir mit dem uneingeschränkt individualisierbaren und fortlaufend anpassbaren System sehr zufrieden. Es sichert unsere Zukunft und sorgt für schnelles Wachstum ohne Verwaltungshemmnisse.“

Durch die Integration der notwendigen Schnittstellen zur DATEV, zu Lieferanten-Systemen, zu Transportdienstleistern und zu Drittlösungen wurde die heterogene IT-Systemlandschaft durch eine integrierte, hochflexible Cloud-ERP-Lösung abgelöst. Die Fehlerquote ging gegen null, Prozesse laufen größtenteils automatisiert und das Management erhält umfangreiche Reportings. Dank des Low-Code-Ansatzes können auch Nicht-Programmierer die Entwicklung mitgestalten. Die BPV GmbH profitiert nun von einer effizienten, zukunftsfähigen ERP-Lösung. •



Der AUTOR
Udo Hensen

ist Geschäftsführer der GEBRA-IT GmbH.

ten Full-Service-Partner in der IT- und Telekommunikationsbranche. Heute bietet BPV im B2B-Bereich Lösungen und Services für den Aufbau mobiler Arbeitsplätze an. Neben eigenen Lösungen hat man sich ein Netzwerk aus Hard- und Softwareherstellern, Netzbetreibern und Finanzierungspartnern aufgebaut. Mittlerweile sind mehr als 160 Mitarbeitende an vier Standorten in Europa für die BPV Unternehmensgruppe tätig.

Rasanten Wachstum führt zu heterogener IT-Systemlandschaft

Am Anfang war alles einfach. Das Unternehmen war klein, wuchs langsam. Eine simple ERP-Lösung reichte aus, um die Prozesse abzubilden.

sowie Mobilfunk- und Asset-Management bestanden als Insellösungen. Die digitalen Medienbrüche sorgten für viele manuelle Tätigkeiten, was wiederum zu Fehlern in der Abwicklung führte. Rechnungen und Retouren waren oft fehlerhaft oder wurden gar nicht geschrieben.

Ein neues ERP-System muss her

Es wurde klar: Ein neues, ganzheitliches und cloudbasiertes ERP-System muss her, das Prozesse digitalisiert, automatisiert und Schnittstellen bereitstellt. Ein System, das das Unternehmen produktiv hält, statt es zu lähmen. Ein System, das man nicht über das Unternehmen stülpt, sondern das sich anpasst und mitwächst.

Fluch oder Segen

Die Diskussion um die Einsatzgebiete von künstlicher Intelligenz erhitzt die Gemüter. Tatsache ist: Die IT-Sicherheit profitiert bereits enorm von dieser Technologie – und Hacker werden sie auf jeden Fall für ihre Zwecke missbrauchen. Die beste Antwort auf deren KI-Attacken ist daher eine KI-Abwehr.

VON MARCO EGGERLING

KÜNSTLICHE INTELLIGENZ (KI) UND IT-SICHERHEIT sind unweigerlich verbunden – und je nachdem, welchen Aspekt man betrachtet, ist die KI ein Fluch oder Segen. Auf der einen Seite kann KI einen vorrauschauenden Ansatz der IT-Sicherheit ermöglichen. Die Kehrseite der Medaille ist, dass auch kriminelle Akteure sich KI zunutze machen. So setzen Hacker-Gruppierungen bereits KI ein, um neue Mitglieder zu trainieren, Malware zu verbessern, Angriffe zu automatisieren und Phishing-Mails glaubwürdig zu gestalten. Andererseits nutzen bereits mehr als die Hälfte der Unternehmen in mindestens einem Geschäftsbereich KI. Das Potenzial, die Produktivität der Unternehmen zu steigern, besteht und KI kann auch dabei helfen, die IT-Sicherheit zu erhöhen.

Wie Kriminelle von KI profitieren

Seit ChatGPT und Google Bard am Markt sind, sehen wir eine starke Zunahme von Bots, die infizierte Computer fernsteuern. Damit lassen sich DDoS-Attacken durchführen, die mit enorm vielen Zugriffsanfragen einen Server, oder ein komplettes System lahmlegen können. Auch daher nahmen die weltweiten Cyber-Angriffe letztes Jahr um 38 Prozent zu.

Außerdem kann KI eine große Hilfe bei der Erstellung von Malware, Phishing-E-Mails, Deepfakes und der Konzipierung von Cyber-Attacken sein. Da die KI-Tools mit jeder Eingabe lernen, sind sie auch in der Lage, komplizierte Inhalte zu erstellen: Bilder, Videos oder sogar Tonaufnahmen – davon geht eine große Gefahr

für Deepfakes aus. Deepfakes zeigen einen bestimmten Menschen so, wie man es von ihm gewohnt ist, obwohl es sich dabei um eine Fälschung handelt. Mit der Technologie kann von der Mimik und Gestik bis hin zur Stimme alles optimal nachgeahmt werden.

Ein weiteres Risiko ist die einfache Bereitstellung von Schad-Software. Kleinkriminelle, die über keinerlei Programmierkenntnisse verfügen,

gen, Aufgaben, Protokollanalyse und Optimierung verringern. Sie kann auch ein höheres Schutzniveau bieten, indem sie Unternehmen in die Lage versetzt, moderne Sicherheitsmechanismen zu nutzen und den Datenverkehr eingehend zu prüfen. Besonders hervorzuheben ist, dass der Einsatz von KI den Menschen entlastet, da autonome Entscheidungen und Weichenstellungen

Der AUTOR Marco Eggerling

ist CISO EMEA bei Check Point.



haben durch KI-Tools plötzlich Zugriff auf hochentwickelte Malware, oder können Phishing-Attacken durchführen. Das führt zu einer Flut von vielen kleinen Angriffen.

KI zur Optimierung der Netzwerksicherheit

KI löst derzeit außerdem eine Begeisterung im Bereich der Netzwerksicherheit aus. Das liegt zum Beispiel daran, dass an jedem Zugangspunkt ein hohes Sicherheitsniveau aufrechterhalten werden muss, gleichzeitig aber der Verwaltungsaufwand verringert werden soll. KI kann die Komplexität der Verwaltung von Sicherheitsrichtlinien durch die Automatisierung von Richtlinienänderun-

gen durch die Technologie übernommen werden und die Systeme im besten Fall ineinandergreifen. Daneben hilft sie IT-Sicherheitsleuten mit Echtzeitdaten und -Berechnungen bei der Bedrohungsabwehr ungemein, vor allem gegen KI-Attacken.

Fazit

Die Tatsache, dass Kriminelle die zur Verfügung stehenden KI-Tools zu ihren Zwecken missbrauchen, sollte den Chancen der KI-Nutzung aber nicht im Wege stehen. Wichtig ist nur, dass KI-Programme so gestaltet werden, dass so wenig wie möglich Missbrauch stattfinden kann – beispielsweise mit individuell zugeschnittenen Tools. •

Fit für den Digitalen PRODUKTPASS

Auf produzierende Unternehmen kommen in den nächsten Jahren mit neuen Nachhaltigkeits-Regularien aus Brüssel große Herausforderungen zu. Das Konzept des Digitalen Zwillinges ist ein wichtiger Baustein, um nachhaltiger zu werden und die Wettbewerbsposition zu stärken.

VON MICHAEL HERING UND UDO RAMIN

MIT DER CORPORATE SUSTAINABILITY REPORTING Directive (CSRD) der EU werden von 2026 an auch Mittelständler ab 250 Mitarbeitenden in die Pflicht genommen, einen Nachhaltigkeitsbericht zu erstellen. Dafür sind viele Daten notwendig, die bisher nicht konsequent erhoben werden. Der Digitale Batteriepass, an dem derzeit unter Hochdruck gearbeitet wird, kann als Blaupause gesehen werden, wenn ab 2027 die Pflicht zu Digitalen Produktpässen kommt.

Nachhaltigkeit wird Wettbewerbsfaktor

Mit dem Digitalen Batteriepass will die EU im Rahmen des Green Deal erreichen, dass sämtliche Emissionen dokumentiert werden, die während des Lebenszyklus durch Herstellung, Nutzung und Recycling entstehen. Die Batterieverordnung zielt auf die Zweitverwertung und Nachnutzung ab. In der Praxis bedeutet das, für Zertifizierungsprozesse vorbereitet zu sein, die zum Beispiel die Autoindustrie bereits angestoßen hat und in wenigen Jahren von ihren Zulieferern erwartet. Das Nachhaltigkeits-Reporting wird damit zum wettbewerbsentscheidenden Faktor. Dabei rücken zum einen Kennzahlen zum CO₂-Verbrauch und zur Herkunft von Rohstoffen und Materialien in den Fokus, aber auch die Lebenszyklusdaten der Produkte. Nachweise zur Nutzung von grünem und blauem Wasserstoff gehören künftig ebenfalls dazu. Damit im Sinne der Kreislaufwirtschaft die richtigen Entscheidungen getroffen werden können, sind bessere Informationen zum jeweiligen Zustand von Produkten, Geräten, Maschinen, Anlagen und Komponenten essentiell.

Datenmodell für den gesamten Produktlebenszyklus

Um also über den Lebenszyklus eines Produktes hinweg alle relevanten Daten sowohl aus Nachhaltigkeits- als auch aus Automatisierungssicht zu sammeln, braucht es passende Datenmodelle. Hier kommt der Digitale Zwilling ins Spiel. Die Idee von Digital Twins (DT) entstand ursprünglich bei der NASA: als virtuelles Abbild von Raumfahrtobjekten, deren Zustand nicht physisch überprüft werden kann. Mittlerweile setzt sich das Konzept auch im Rahmen von Industrie 4.0 durch. So bekennt sich etwa Bosch explizit zum Digitalen Zwilling als wichtige Technologie rund um die Nachhaltigkeit, die für einen Paradig-

menwechsel steht. Der Digitale Zwilling setzt sich aus drei wesentlichen Bestandteilen zusammen: Das physische Produkt im realen Raum, das virtuelle Produkt im digitalen Raum und die Datenverarbeitung, die beide Welten verbindet. Ein Digitaler Zwilling kann dabei nicht nur das Abbild von Produkten, sondern auch von Prozessen oder Dienstleistungen sein

Jetzt schon mit dem Digital Twin starten

Die meisten kleinen und mittelständischen Unternehmen sind allerdings noch weit von diesen Themen entfernt. Traditionelle IT-Landschaften mit vielen Datensilos sind hier an der Tagesordnung. Daten werden jedoch künftig gleich für mehrere wichtige Zukunftsthemen zur treibenden Kraft. Dazu gehören auch digitale Geschäftsmodelle und Services, die häufig auf der Integration von IoT-Sensoren und KI-Analytik basieren. Digitale Services können beispielsweise den Betreibern helfen, ihre Maschinen und Anlagen immer in den jeweils optimalen Leitplanken zu fahren, Energie zu sparen und Ausschuss zu vermeiden oder mit vorausschauender Wartung für weniger Ausfälle und eine längere Produktlebensdauer zu sorgen.

Maschinen- und Anlagenbauer sollten also prinzipiell ihren Fokus von der Entwicklung und Herstellung auf den gesamten Lebenszyklus ihrer Produkte ausdehnen – und damit auf den Digital Twin. Im Expertenkreis Plattformökonomie des VDMA zeigte sich in der Diskussion, dass der geplante EU Data Act die Branche maßgeblich betreffen wird, weil sie künftig Daten zu Komponenten und Ausrüstungen in digitaler Form vorhalten muss. Das Datengesetz regelt, wie die in den Wirtschaftssektoren in der EU erzeugten Daten fair genutzt werden können. Der Verband unterstützt Initiativen wie Manufacturing X als selbstbestimmtes Datenökosystem für Industrie 4.0.

Die Datenmodelle sind vorhanden

Viele KMU nehmen den Digital Twin als Hype-Thema wahr oder befürchten, angesichts des Fachkräftemangels gerade im Bereich Data Sciences nicht an die nötigen Skills zu kommen. Doch es gibt mittlerweile pragmatische und bezahlbare Ansätze für die Umsetzung. Zunächst geht es darum, die notwendigen Daten zu identifizieren

und zu erheben, beispielsweise indem Ausrüstung, Komponenten und Maschinen digitalisiert und durch Sensorik „smart“ gemacht werden. Anschließend müssen hergestellte und verbaute Objekte mit ihren Eigenschaften in einem Datenmodell beschrieben werden, in das später weitere Informationen aus der Nutzungsphase einfließen können. Der Input dafür kommt aus Backend-Systemen wie dem ERP, aus PLM/PDM, IoT-Services oder aus Prozessleitsystemen. Damit Unternehmen schon mit den Vorbereitungen starten können, obwohl es noch keine offiziellen Standards zum Beispiel für den Digitalen Pro-



ten und KI-Technologie wie ChatGPT. Die Plattform bringt relevante Daten aus unterschiedlichsten Datenquellen zusammen und ermöglicht deren zentrale Verwaltung. Mit der DT Definition Language lässt sich jedes beliebige physische Objekt beschreiben, etwa digitale Abbilder von Produkten, Ausrüstung, Anlagen, Maschinen oder Gebäuden.



Die AUTOREN

Michael Hering

ist Industry Manager Discrete. (I.)

Udo Ramin

ist Director of Competence Center Industry 4.0 & IoT bei der COSMO CONSULT Group.

Das Nachhaltigkeits-Reporting wird zum **wettbewerbsentscheidenden Faktor**. Dabei rücken zum einen Kennzahlen zum CO₂-Verbrauch und zur Herkunft von Rohstoffen und Materialien in den Fokus, aber auch die Lebenszyklusdaten der Produkte.

duktpass gibt, sind bereits sogenannte Verwaltungsschalen als herstellernerutraler und branchenübergreifender Standard entwickelt worden. Sie geben Aufschluss über die benötigten Parameter und Eigenschaften.

Cloud-Plattform als zentrale Datendrehscheibe

So steht etwa mit Microsoft Azure eine Cloud-Plattform zur Verfügung, die das Aufsetzen von Digital Twins deutlich vereinfacht. Zusammen mit IoT- und KI-Services lässt sich mit Azure Digital Twin auch der Digitale Zwilling als Cloud-Service nutzen. Dieser Ansatz verbindet die Digital Twin Language, das Dataverse für das Handling der Da-

Wichtige Basisdaten für den Digitalen Zwilling sind die Auslegungsdaten aus den Datenblättern und die Ergebnisse vom Prüfstand bei der Inbetriebnahme von Maschinen oder Anlagen. Sie müssen in digitale Modelle eingepflegt werden: Eine Aufgabe, die sogar durch einfache Apps automatisiert werden kann. Für den Digital Twin werden meist Graphen als Datenmodelle gewählt. Die so befüllten Modellgraphen ermöglichen die Erzeugung von verschiedenen Digitalen Zwillingen, die sich wiederum für Simulationen kombinieren lassen – etwa um aus Nachhaltigkeitssicht Energieverbräuche zu optimieren. •

Lernen von Hollywood Studios

Auch in der Filmbranche werden Daten- und rechenintensiven Arbeitsprozesse wie Animationen und Rendering mithilfe einer Datenmanagement-Plattform und KI realisiert. Inzwischen profitieren weitere Branchen wie die Forschung und der Finanzhandel davon.

VON SVEN BREUNER

IN DEN BUNTEN HÄUSERSCHLUCHTEN VON Elemental City der jüngsten Pixar-Produktion „Elemental“ geht es turbulent zu. Hier leben „Feuer-, Wasser-, Erd- und Luftbewohner“ zusammen, aber zugleich getrennt, weil sich die vier Elemente nicht vermischen dürfen – oder doch? War in den Anfangszeiten des Animationsfilms die Szenerie noch sehr spartanisch, lassen die Filmemacher ihr Publikum mittlerweile in faszinierende Phantasiewelten eintauchen. Was früher nur mit Zeichentrickskünsten und jeder Menge Handarbeit mehr schlecht als recht gelang, übernimmt heute künstliche Intelligenz. Auch bei Realfilmen kommen Spezialeffekte, Actionszenen und täu-

...



Der AUTOR
Sven Breuner

ist Field CTO International bei VAST Data.

schend echt wirkende Umgebungen aus dem KI-Zauberhut, der fast grenzenlose Möglichkeiten bietet, aber auch Unmengen an Daten generiert. Hier sind die Hersteller von Storage-Lösungen gefragt.

Ziel ist es, den Forderungen vieler Branchen nach immer mehr Speicherplatz, noch höherer Verarbeitungsleistung, niedrigerem Energieverbrauch und mehr Nachhaltigkeit gerecht zu werden. Neue Technologien wie Hyperscale-Flash, Storage Class Memory (SCM) und Stateless-Container haben das Speichermedium Flash für viele Szenarien zur kosteneffizienten Lösung gemacht. Eine zeitgemäße „All-Flash“-Datenplattform dieser Art bietet hohe Speicherdichte und Speicherkapazität pro eingesetztem Watt Leistung. Neue Methoden der Datenreduzierung tragen zur Gesamteffizienz bei. Durch fortlaufende Flash-Optimierung gelingt es zudem, die Produktlebensdauer gegenüber herkömmlichen Lösungen zu verlängern, ohne die Hardware vollständig ersetzen zu müssen.

All-Flash rückt ins Rampenlicht

Was eine moderne All-Flash-Lösung im Produktiveinsatz leistet, zeigt ein Anwendungsbeispiel aus der Filmbranche. Die Pixar Animation Studios, Tochtergesellschaft der Walt Disney Company, nutzen VAST Data als Datenplattform, auch für „Elemental“, seit Juni im Kino. Die Plattform ist für besonders daten- und rechenintensive Anwendungen in verschiedenen Branchen geeignet.

Die Zusammenarbeit startete bereits im Jahr 2018, um neue Animationstechniken mit volumenintensivem Rendering für den Film „Soul“ anzuwenden. „Elemental“ – als aktuelle Produktion dieser Machart – setzte eine neue Art der Skalierung der detaillierten Charaktere und Umgebungen voraus. Neue Animationsmethoden und anspruchsvolle Rendering-Prozesse erforderten einen sechsmal größeren Datenumfang und Rechenaufwand als beim Vorgängertitel. Durch die Verlagerung von 7,3 Petabyte an Daten in ein einziges Datenspeicher-Cluster ist nun Datenzugriff in Echtzeit möglich. Auf diese Weise kann die Rendering-Farm von Pixar konstant Daten verarbeiten und ermöglicht gleichzeitig eine verbesserte Kontrolle und Auswertung aller Prozesse.

Die All-Flash-Plattform bietet optimierten Datenzugriff und hochgradige Ausfallsicherheit. Der parallele Datenzugriff sowie die Performance und Skalierbarkeit ermöglichen es, fast 150.000 Bildelemente zu rendern und ein neues visuelles Erlebnis zu schaffen. Zudem lassen sich nun parallel mehrere laufende Produktionen unterstützen.

Potenzial für vielfältige Anwendungsfälle

Die Filmbranche ist nur ein Beispiel für den Einsatz einer modernen All-Flash-Plattform, auch die medizinische Forschung profitiert davon. Ein Bereich ist die klinische Genetik, die der Krankheitsprävention und gezielten, personalisierten Behandlung dient. Die Suche nach den genetischen Ursachen seltener Krankheiten bringt jedoch enorm steigende Datenmengen mit sich. Jeder Genom-Sequenzierer erzeugt mehrere Terabyte an Daten, die Forscher erfassen, analysieren und interpretieren müssen. Eine All-Flash-Plattform unterstützt hierbei die anspruchsvolle Anwendungspipeline mit der nötigen Skalierung und Leistung.

Bild/Copyright: Tatiana Morozova – stock.adobe.com

Ein weiteres Beispiel ist die Finanzbranche, die traditionell hohe Anforderungen an die Dateninfrastruktur stellt. Herkömmliche Speicherumgebungen erforderten lange Zeit einen Kompromiss zwischen großer Speicherkapazität oder schneller Datenbereitstellung. Gerade im quantitativen Handel und bei der KI-gestützten Datenanalyse bestimmen heute neue Maßstäbe das Bild.

Gefragt ist eine Infrastruktur, die Echtzeitleistung für sämtliche Workloads bereitstellt und mit dem schnellen Datenwachstum skaliert. Der All-Flash-Ansatz erfüllt auch hier die Anforderungen und punktet bei Energieeffizienz und Nachhaltigkeit. Diese Aspekte gewinnen an Bedeutung, da sich immer mehr Unternehmen hier hohe Ziele setzen, zugunsten einer zeitgemäßen, makellosen Außenwirkung.

Waren Storage und Datenmanagement früher nur Themen für IT-Experten, hat sich dies im Zeitalter der digitalen

Transformation und intensiven Datennutzung grundlegend gewandelt. Eine zeitgemäße Datenplattform avanciert damit zu einer der entscheidenden Säulen für Agilität, Innovation, Effizienz und Nachhaltigkeit in unterschiedlichsten Branchen. •



KI unterstützt die Arbeitsprozesse für Animationen und Rendering bei anspruchsvollen daten- und rechenintensiven Projekten.

(Bildquelle: Pixar Animation Studios)

Waren Storage und Datenmanagement früher nur Themen für IT-Experten, hat sich dies im Zeitalter der digitalen Transformation und intensiven Datennutzung grundlegend gewandelt. Eine zeitgemäße Datenplattform avanciert damit zu einer der **entscheidenden Säulen** für Agilität, Innovation, Effizienz und Nachhaltigkeit in unterschiedlichsten Branchen.

**Kommunikation absichern,
modernisieren, konsolidieren
und cloudifizieren?**

**Prozesse digitalisieren
und automatisieren?**

**Ohne Server,
Gateways und Hubs?**

**DIE
COMMUNICATIONS
PLATFORM!**

retarus.de

KLARER TREND ZUR CLOUD

65 Prozent der MS Dynamics On-Premises-Nutzer planen eine Migration in die Cloud – mehr als die Hälfte der befragten Unternehmen setzt auf Lösungen von Drittanbietern. Das ist das wesentliche Ergebnis der 2023er Trendstudie „Einsatz von Microsoft Dynamics: Aktueller Status und zukünftige Pläne“. Diese stellte jetzt d.velop vor, ein Anbieter für Software zur Digitalisierung von dokumentenbezogenen Geschäftsprozessen. Ziel der Um-

frage, die im Frühjahr 2023 durchgeführt wurde, war es, gezielt herauszufinden, welche Betriebsmodelle (Cloud, On-Premises) derzeit im ERP-Bereich in den befragten Unternehmen zum Einsatz kommen, welche Microsoft Dynamics-Lösungen aktuell genutzt werden, und wie die zukünftigen Pläne zur Nutzung von ERP-/CRM-Lösungen im Allgemeinen und Microsoft Dynamics-Lösungen im Speziellen aussehen.

QLIK ERÖFFNET ZWEI NEUE CLOUD-STANDORTE IN EMEA

Da Unternehmen ihre Daten- und Analyse-Workloads zunehmend in die Cloud verlagern, sehen sie sich gleichzeitig mit einer Vielzahl verschärfter gesetzlicher Anforderungen konfrontiert. Qlik hat nun zwei neue Cloud-Standorte in London und Frankfurt am Main eröffnet, die ihrerseits als Zentrum zweier neuer Cloud-Regionen dienen. Damit unterstreicht das Unternehmen sein Bestreben, die wachsende Nachfrage nach Cloud-Lösungen und Innovationen weltweit und speziell in EMEA zuverlässig zu bedienen. Die neuen Standorte sind besonders für Unternehmen mit Sitz im Vereinigten Königreich und Deutschland von Bedeutung, da sie eine Anpassung an regionalspezifische Datenschutzgesetze und Anforderungen, die über die DSGVO-Richtlinien hinausgehen, benötigen. Mit den beiden neuen Regionen sind Kunden an denjenigen Standorten angebunden, die in Bezug auf diese rechtlichen Vorgaben für sie relevant sind.

NEUER ANSATZ ZUR BEWÄLTIGUNG DER RISIKEN VON CYBER-ASSETS

Forescout, ein weltweit agierender Cybersecurity-Anbieter, hat seine neue Lösung Risk & Exposure Management vorgestellt. Das cloudnative Produkt führt sämtliche Datenquellen zu den vernetzten Assets eines Unternehmens zusammen und errechnet daraus für jedes Asset einen eindeutigen Multifaktor-Risikowert, anhand dessen Unternehmen Risiken auf intuitivere, quantitative Weise priorisieren können. Um dieser Herausforderung zu begegnen, überwacht die neue Lösung Forescout Risk & Exposure Management alle Veränderungen der Sicherheitslage in einer präzisen Ansicht, die den Status für jedes einzelne Asset im Zeitverlauf darstellt. So können die Sicherheitsteams auf der Grundlage intuitiv verständlicher Erkenntnisse zu den Cyberrisiken handeln und dazu die automatisierten Security Workflows nutzen, die die Forescout Plattform bietet.

NEWS

NUR JEDER 5. SOFTWARE-ANBIETER FOLGT CLOUD-ONLY-STRATEGIE

Der Software-Experte Revenera hat den neuen Monetization Monitor zu „Software Monetization Models and Strategies 2023“ vorgestellt. Die Umfrage unter 450 Anbietern zeigt: Das Geschäft mit der Software bleibt vorerst hybrid. Zwar dominieren SaaS und Abos mittlerweile bei der Bereitstellung und Monetarisierung von Anwendungen. On-Premises hält sich nicht nur hartnäckig, sondern legt sogar etwas zu. Mit 80 Prozent ist und bleibt SaaS das am weitesten verbreitete Bereitstellungsmodell. Der Löwenanteil der Software-Anbieter (82%) hat sich bereits

in Richtung Cloud aufgemacht oder plant die Umstellung von On-Premises-Lösungen zu as-a-Service. Eine Cloud-Only-Strategie – mit ausschließlich cloudbasierten IT-Produktkatalog – findet sich jedoch nur bei jedem fünften Unternehmen (18%). Hier zeigt On-Premises Standhaftigkeit: Fast ein Drittel der Befragten (29%) bietet nach wie vor in großem Umfang lokal installierte Lösungen an. Darüber hinaus planen 46 Prozent der Softwareanbieter den Anteil an On-Premises in den nächsten 12-18 Monaten zu erhöhen.

Bild/Copyright: larui - stock.adobe.com, vachom - stock.adobe.com

GAME CHANGER

01

Jenseits des Obstkorb: Wie vor allem KMU im Recruiting zwischen Hype und Innovation unterscheiden können, ist entscheidend für die Performance am Arbeitsmarkt.

02

Gemeinsam statt einsam: Softwareentwickler müssen heute für den Unternehmenserfolg enger mit dem Management zusammenarbeiten statt allein vor Ihren Rechnern zu hocken.

JENSEITS DES OBSTKORBES

Next Shiny Object oder Game Changer? Wie vor allem kleine und mittelständische Unternehmen (KMU) im Recruiting zwischen Hype und Innovation unterscheiden können.

VON PIA TISCHER

IN DER ÄRA DER DIGITALEN TRANSFORMATION hat sich das Recruiting zu einem komplexen und dynamischen Bereich entwickelt. Software-Tools und Apps für das Recruiting sprießen förmlich aus dem Boden und präsentieren sich als die ultimativen Lösungen für die Herausforderungen der Mitarbeiterrekrutierung. Doch in diesem Ozean der Innovationen stellt sich die entscheidende Frage: Wie unterscheiden (KMU) zwischen dem „Next Shiny Object“ und einem tatsächlichen „Game Changer“ im Recruiting? Um diese Frage zu beantworten müssen Unternehmen wissen, wie sie die Basisarbeit erledigen, bevor sie sich den neuesten Trends zuwenden, und welche die wesentlichen Bausteine einer erfolgreichen und nachhaltigen Recruiting-Strategie sind.

die Basisarbeit zu erledigen. Damit meine ich, die Kernprozesse des Recruitings zu verstehen und permanent zu optimieren. Es ist wie bei einem Gebäude: Ohne ein solides Fundament können die prächtigsten Strukturen in sich zusammenfallen. Die Basisarbeit umfasst die Klärung der eigenen Unternehmenskultur und Arbeitgeberpositionierung, die ordentliche Identifizierung der Anforderungen offener Stellen, die genaue Definition der Zielgruppen auf Bewerberseite, sowie einen mehrstufigen und zügigen Recruiting-Prozess.

Die Auswahl des richtigen Tools für Ihr Unternehmen

Die Frage „Welches Tool ist denn jetzt das richtige für mein Recruiting?“ wird oft von Unsicherheit begleitet.



Die AUTORIN
Pia Tischer

ist CEO der coveto ATS GmbH, einem Spezialisten für Recruiting Software.

Ein erfolgreiches Recruiting erfordert mehr als nur eine innovative Technologie. Es braucht eine **klare Arbeitgeberpositionierung**, die das Unternehmen als attraktiven Arbeitgeber präsentiert. Es braucht eine gut durchdachte Recruiting-Strategie, die auf die Bedürfnisse der Bewerberzielgruppe zugeschnitten ist und gleichzeitig die Unternehmensziele berücksichtigt.

Die Überflutung des Recruiting-Marktes

Es fühlt sich an, als gäbe es gegenwärtig mehr Software-Tools und Apps für das Recruiting als für jeden anderen Unternehmensbereich. Dieser Boom an Technologie verspricht Effizienzsteigerung, Kostenersparnis, mehr und bessere Kandidaten. Dennoch dürfen wir nicht vergessen, dass diese Tools nur dann ihren vollen Nutzen entfalten können, wenn die grundlegenden Aspekte des Recruitings solide in unseren Unternehmen etabliert sind.

Die Grundlagen vor dem „Next Shiny Object“

Bevor wir uns dem verlockenden Glanz des „Next Shiny Object“ hingeben, ist es von entscheidender Bedeutung,

Die Antwort liegt auf der Hand: Ein Recruiting-Tool sollte in erster Linie zum Unternehmen passen und dessen Strategie unterstützen. Hilfreich ist es, einen Anbieter zu finden, der in der jeweiligen Branche und mit der Unternehmensgröße Erfahrung und Expertise hat.

Dieser Anbieter sollte einen guten, erreichbaren Support bieten, der im Preis inkludiert ist. Gerade beim Einsatz neuer Software ist es wichtig, dass Unternehmen die notwendige und zeitnahe Unterstützung erhalten, um das Produkt auch optimal nutzen zu können. Der Support sollte persönlich erreichbar sein und nicht nur aus Chatbots oder E-Mail-Nachrichten bestehen.

Die Bausteine einer innovativen und nachhaltigen Strategie

Ein erfolgreiches Recruiting erfordert mehr als nur eine innovative Technologie. Es braucht eine klare Arbeitgeberpositionierung, die das Unternehmen als attraktiven Arbeitgeber präsentiert. Es braucht eine gut durchdachte Recruiting-Strategie, die auf die Bedürfnisse der Bewerberzielgruppe zugeschnitten ist und gleichzeitig die Unternehmensziele berücksichtigt. Es braucht einen strukturierten Recruiting-Prozess, der sicherstellt, dass sowohl nicht die falschen Mitarbeiter eingestellt werden als auch Kandidaten nicht kurz vor Abschluss des Prozesses abspringen. Unternehmen sollten sich eine Lösung suchen, die diese Punkte unterstützt, bevor sie Insellösungen einsetzen.

Erfolgreiche Praxisbeispiele

Praxisbeispiele zeigen deutlich, dass der Schlüssel zum Erfolg nicht in einem einzelnen Tool oder einer App liegt, sondern in einer kohärenten Strategie, die verschiedene Elemente geschickt miteinander verknüpft. Ein Beispiel hierfür sind Recruiting-Videos, die einen authentischen Einblick in die Arbeitswelt und Kultur des Unternehmens geben. Diese Videos können die emotionale Verbindung zwischen Bewerbern und Unternehmen stärken und die Wahrscheinlichkeit erhöhen, dass sich passende Kandidaten bewerben. Ein weiteres erfolgreiches Beispiel sind besondere Benefits jenseits des Obstkorb. Einer unserer Kunden bietet seinen Beschäftigten (Handwerker) jeden Morgen ein Frühstücksbuffet an. Das hat sich schnell herumgesprochen und viele Initiativbewerbungen ausgelöst. Solche Benefits und Veranstaltungen sind einerseits Bewerbermagnete andererseits dienen sie auch dazu, die jeweilige Unternehmenskultur zu betonen und einzigartige Erfahrungen zu bieten.

Fazit: Solide Grundlagen schaffen und innovativ denken

Bevor sich kleine Und mittelständische Unternehmen auf die neuesten Technologien stürzen, sollten sie sicherstellen, dass ihr Recruiting vom Stellenanzeigenmarketing über die Kommunikation mit Kandidaten und Entscheiden bis hin zu Einstellung, Absage oder Aufnahme in den Pool digital von einer Software unterstützt wird. Eine Recruiting Software ist die Basis dafür. Eine durchdachte Arbeitgeberpositionierung, eine maßgeschneiderte Strategie und ein effektiver Prozess sind aber letztendlich entscheidend, um die besten Talente anzuziehen und langfristig zu binden. •

Bild/Copyright: vachorn – stock.adobe.com



Let's transform

**Sichern Sie sich jetzt
Ihr exklusives Abonnement!**

[www.digital-business-cloud.de/
abonnement/](http://www.digital-business-cloud.de/abonnement/)

**DIGITAL BUSINESS
CLOUD**



GEMEINSAM statt einsam

Software-Entwickler? Hocken die nicht in dunklen Zimmern bis spät in der Nacht hinter ihren Rechnern? So lautet zumindest das alte Klischee. Die Realität ist eine andere: Entwickler besetzen nicht mehr länger eine Nische in weiter Entfernung vom Management. Im Gegenteil, heute entscheiden sie direkt mit über den wirtschaftlichen Erfolg von Unternehmen.

VON SEAD AHMETOVIC

LÄNGST SIND CIO UND CTO als Tech-Experten etablierte Teile der Geschäftsleitung großer Unternehmen. Aber die Expertise von DevOps- und Entwickler-Teams geht in aller Regel noch einmal deutlich tiefer und kann heruntergebrochen werden bis auf die Codeebene des Unternehmens. Entwickler, Datenwissenschaftler, KI-Ingenieure und Cybersecurity-Experten werden deshalb immer wichtiger.

Zum Beispiel in der Automobil-Industrie: Durch die Elektromobilität verschwindet das bisherige Alleinstellungs-

Software entscheidet über wirtschaftlichen Erfolg

Heute gehören erfahrene Softwareentwickler in vielen Branchen zu den begehrtesten Talenten, die mit allen Mitteln umworben werden. Das wertet ihre Position im Unternehmen auf – mit mehr Einfluss im Management. Sie entscheiden über die künftige Weiterentwicklung von Produktportfolios und Serviceangeboten: Welche Betriebssysteme, Cloud-Plattformen und Technologien werden angeschafft und bestimmen die Zukunft des Unternehmens?



Der AUTOR
Sead Ahmetovic

ist CO-Gründer und CEO der IT-Jobplattform WeAreDevelopers.

Da Entwicklungsteams immer häufiger mitentscheiden, welche technologischen Lösungen eingeführt werden, müssen **Sales und Marketing** sich besonders an diese Stakeholder richten.

merkmal der Motortechnik, auf die der Marktführer-Status der Branche in Deutschland zurückgeht. Doch die Hardware von modernen Fahrzeugen ist mittlerweile weniger komplex als die Software.

Ähnliche Entwicklungen gibt es in der Industrie und B2B-Märkten wie dem Maschinenbau. Innovative Entwicklungen und Technologieführerschaft entstehen dort zunehmend durch innovative Software und damit verbundene Services. Wenn Unternehmen in der Lage sind, ihre Kunden mit Softwarelösungen für Condition Monitoring und Data Analytics zu versorgen, können sie neue Geschäftsmodelle schaffen und Umsätze steigern.

Software-Entscheidungen nehmen eine immer zentrale Rolle in der langfristigen Planung eines Unternehmens ein. Mit ihnen steht und fällt der Erfolg ganzer Organisationen. Das weist Software-Ingenieuren und Entwicklern eine Schlüsselrolle zu. Ihre häufig stark lösungsorientierten Ansätze ergänzen die strategischen und langfristig orientierten Denkweisen des C-Levels.

Deshalb werden im Wettbewerb der Zukunft werden vor allem die Unternehmen bestehen, in denen sich Entscheider und Entwickler zusammenschließen. Sie benötigen nicht nur Business-Expertise, ebenso ist ein tieferes Verständnis vom technischen Fach und Integrationsprozessen erforderlich.

US-Unternehmen sind die Vorreiter

Das beste Beispiel ist das Silicon Valley. Es zeigt, wie erfolgreich das Konzept „Business und Developer an der Spitze“ sein kann. Die bekannten Player Microsoft, Facebook, Apple, Google und Tesla wurden von Personen mit technischem Hintergrund gegründet. Elon Musk oder Bill Gates sind Geschäftsleute und Techniker in einem. Apple wurde zu einem der wertvollsten Unternehmen der Welt, indem sich der leidenschaftliche Entwickler Steve Wozniak mit dem Verkaufstalent Steve Jobs zusammensetzte.

Silicon-Valley-Unternehmen haben nicht nur enorme Erfolge erzielt, sondern auch die Art und Weise, wie wir leben und arbeiten, grundlegend verändert. Allein das iPhone hat unsere Gesellschaft stärker verändert als die meisten anderen Industrieprodukte. Dabei geht es

Jedes Unternehmen, das mit Software und Daten arbeitet (und das gilt heute im Grunde für jede Art von Organisation) sollte sich bemühen, die Entscheider- und IT-Ebene in Entscheidungsprozessen stärker zusammenzubringen. Besonders wichtig ist das für Tech-Unternehmen wie SaaS- oder PaaS-Provider. Ihre Kommunikation darf sich nicht nur an das C-Level in ihren Kundenunternehmen richten, sondern auch an die Entwickler.

Da Entwicklungsteams immer häufiger mitentscheiden, welche technologischen Lösungen eingeführt werden, müssen Sales und Marketing sich besonders an diese Stakeholder richten. Denn ihre Ansprüche unterscheiden sich typischerweise von denen eines Business-Entscheidungsmakers. Faktoren wie Rollout, Usability und Prozessqualität rücken in der Kommunikation mit Entwicklern in den

Das beste Beispiel ist das Silicon Valley. Es zeigt, wie erfolgreich das Konzept "**Business und Developer an der Spitze**" sein kann. Die bekannten Player von Apple bis Tesla wurden von Personen mit technischem Hintergrund gegründet.

immer um Software. Um noch einmal Elektroautos als Beispiel zu nennen: Tesla hat die traditionellen Konzepte der Automobil-Industrie so sehr auf den Kopf gestellt, wie es sich vor ein paar Jahren sicher noch niemand hätte vorstellen können.

Tesla hat erfolgreich Konzepte aus der IT-Welt in die Autoindustrie übertragen. Ein Tesla kann wie ein Computer oder Smartphone jederzeit mit zusätzlichen Funktionen erweitert werden, Updates kommen „Over The Air“ und die Bedienung erfolgt hauptsächlich über einen zentralen Touchscreen. Es besitzt nicht hunderte von getrennten Steuersystemen, sondern einen zentralen Bordcomputer mit einer einheitlichen Software.

Business und IT stärker zusammenbringen

An solchen Beispielen zeigt sich: Softwareentscheidungen werden immer teurer, langfristiger und wichtiger. Mit ihnen steht und fällt der Erfolg ganzer Organisationen. Denn nur, wer die beste Lösung zum besten Preis anbietet, kann langfristig im Wettbewerb mithalten. Gerade Märkte wie die USA oder China sind uns hier teilweise um Jahre voraus.

Vordergrund, während Faktoren wie Datenschutz, Preis und Cybersicherheit auf einem höheren Level den CTO überzeugen.

Expertise aus beiden Welten

Unternehmen brauchen Expertise aus beiden Welten, um im hochtechnisierten Wettbewerb der Zukunft mithalten zu können. Deshalb sollten Entscheider und Entwickler gemeinsam Entscheidungen treffen und an Lösungen arbeiten. Doch nicht jeder Entwickler ist gleichzeitig ein genialer Business-Entscheider. Genauso wenig muss ein erfolgreicher Unternehmer nachts im stillen Kämmerlein auch noch Billion-Dollar-Codes schreiben.

Doch mit der zunehmenden Verbreitung von künstlicher Intelligenz und anderen fortschrittlichen Technologien steigt auch die Komplexität der zu treffenden Entscheidungen. Dies erfordert vom Management ein tieferes Verständnis der Technologien und ihrer Anwendungsmöglichkeiten. Gleichzeitig müssen Entwickler in der Lage sein, komplexe technische Konzepte so zu übersetzen, dass sie Entscheidern verständlich sind. Beide müssen langfristig in der Lage sein, eine gemeinsame Sprache zu entwickeln, um wirtschaftlichen Erfolg zu erreichen. •

OUT OF THE BOX

ECM in der Cloud hat sich – u. a. befeuert durch die Pandemie – fest etabliert. Doch ist die cloudbasierte Bereitstellung von ECM-Diensten für Organisationen jeglicher Größe und Couleur auch stets die beste? Für welche Bedürfnisse die Cloud On-Prem auf jeden Fall toppen kann.

VON SASCHA LESER

GRUNDSÄTZLICH IST ZWISCHEN DREI VERSCHIEDENEN

Bereitstellungsvarianten zu unterscheiden: der On-Premise-Implementierung, einem Hosting über Managed-Services-Partner sowie dem Cloudbetrieb. Gängig ist bei letzterem das Software-as-a-Service (SaaS)-Modell. Dagegen bieten bisher nur wenige -Hersteller von Enterprise Content Management Software einen „Integration-Plattform-as-a-Service“ (iPaaS) an: Die Plattform vernetzt mit Drittanwendungen wie CRM und ERP sowie Daten aus Cloud- und On-Prem-Umgebungen. Insgesamt liegt die Cloud mittlerweile klar vorne, Tech-Giganten wie Microsoft oder SAP setzen auf Cloud-first.

Für das On-Prem-Modell spricht darüber hinaus die Unabhängigkeit von einer Internetverbindung. Das heißt, die Mitarbeiter können auch bei fehlender oder nur mäßiger Netzabdeckung jederzeit auf Informationen zugreifen. Regelmäßige Backups tun jedoch Not, um das Risiko eines Serverabsturzes und potenziellen Datenverlusts – mit gegenebenfalls verheerenden Auswirkungen – abzufedern. Für Wartung und Updates ist entsprechendes IT-Personal vorzuhalten. Der höhere Aufwand geht selbstredend mit nicht unerheblichen Kosten einher; auf der anderen Seite profitiert der Anwender von mehr Überblick und Kontrolle über seine Daten und das System.



Der AUTOR
Sascha Leser

ist Teamleiter Produktorientiertes Business Development bei ELO Digital Office.

Dennoch unterstützen auch sie traditionelle Kunden weiterhin mit Inhouse-Installationen. Es gibt also wohl doch noch gute Gründe für On-Prem.

Datenkontrolle und Customizing sprechen für On-Prem

Kandidaten für das traditionelle Modell sind zum einen kleinere Unternehmen mit nur einem Standort bzw. größere Firmen, die sich ihre eigene IT-Abteilung leisten. Zum anderen Organisationen hoch regulierter Branchen wie dem Gesundheitswesen. Zu eigen ist allen drei Zielgruppen, dass sie ihre sensiblen Daten gerne auf eigenen Servern und damit in der eigenen Obhut wissen. Überlegen ist eine On-Premise- einer Cloudlösung sicherlich in Bezug auf ihre Flexibilität bzw. das Customizing, sprich die Möglichkeit, die Software den kundenspezifischen Anforderungen anzupassen. Ein Cloudmodell punktet eher durch höhere Standardisierung, was aber nicht heißt, dass Anpassungen bis zu einem bestimmten Grad nicht möglich wären.

Viele Unternehmen scheuen jedoch die hohen Anfangsinvestitionen für die Anschaffung eines ECM-Systems inklusive dazugehöriger Hardware oder den Aufbau einer eigenen IT-Abteilung. Fehlt es aufgrund des Fachkräftemangels noch dazu an geeignetem Personal, empfiehlt es sich, den Betrieb der Software an einen zertifizierten Hosting- beziehungsweise Managed-Services-Partner auszulagern. Gegen eine Gebühr übernimmt dieser die damit einhergehenden Aufgaben, der Auftraggeber spart Personalkosten und profitiert vom Know-how des Providers.

Skaleneffekte überzeugen beim Cloudmodell

Das Cloudmodell – ob Private oder Public – verspricht dagegen höchste Flexibilität, Agilität und Skalierbarkeit, auch in Bezug auf die Kosten. Dies machen sich vor allem dezentral aufgestellte Unternehmen zunutze, die rasch neue Umgebungen für Innovationen bereitstellen oder neue Standorte aufbauen wollen. Aber auch kleinere

Betriebe oder Start-ups ohne dediziertes IT-Personal, für die Wirtschaftlichkeit, Kostentransparenz und Planungssicherheit im Vordergrund stehen – und die eine gut kalkulierbare „Out-of-the-box-Lösung“ suchen. Der Vorteil: Stets aktuelle Software und monatlich nutzungsabhängig abgerechnete Dienste (pay-per-use). Bei Ausschreibungen ist Cloudfähigkeit – ggf. auch nur als Zukunftsoption – quasi ein Muss.

Grundvoraussetzung ist jedoch eine gut funktionierende Netzausstattung, die in Deutschland noch immer nicht überall gegeben ist. Zudem ist ein prüfender Blick auf das Mietmodell ratsam, um bösen Überraschungen in Form kostspieliger Abonnements vorzubeugen. Und last but not least bietet sich mit der Hybrid Cloud auch eine Lösung, die beide Welten vereint.

Der richtige Anbieter macht den Unterschied

Die Wahl des passenden Anbieters ist das A und O. Dabei spielen Aspekte wie Kosten, Kompetenz sowie Sicherheit

standard des Bundesamts für Sicherheit in der Informationstechnik (BSI) zur Nutzung externer Clouddienste.

Datenschutz ist ein weiteres Thema. So muss speziell in hoch regulierten Branchen sichergestellt sein, dass keine Daten den europäischen Raum verlassen. Entsprechend ist der Cloud-Provider zu wählen. Deutsche Anbieter wie die Telekom bilden dies sicherlich für deutsche Standorte gut ab. Unterhält ein Unternehmen jedoch auch Standorte im außereuropäischen Ausland, empfiehlt sich eher die Beauftragung eines international ausgerichteten, zugleich aber vertrauenswürdigen Anbieters wie IBM. Deren Schwerpunkt liegt auf Finanzdienstleistungen, das heißt, sie sind verpflichtet, die technologischen und geschäftlichen Anforderungen der am stärksten regulierten Branchen zu erfüllen – ganz im Sinne von Risikobegrenzung, Compliance sowie Datenkontrolle. Kritisch ist auch die Ausfallsicherheit, die sich über Georedundanz in Form geografisch entfernter Rechenzentren (RZ) abbilden lässt. Für eine niedrige Latenz sorgt dagegen Geoproximity.

Die Wahl des passenden Anbieters ist das A und O. Dabei spielen Aspekte wie Kosten, Kompetenz sowie Sicherheit die maßgebliche Rolle. Der Provider sollte über Kompetenz im gewünschten Branchenumfeld und eine **transparente Kostenstruktur** verfügen sowie die Themen Datenschutz und Datensicherheit mit der notwendigen Sorgfalt adressieren.

die maßgebliche Rolle. Der Provider sollte über Kompetenz im gewünschten Branchenumfeld und eine transparente Kostenstruktur verfügen sowie die Themen Datenschutz und Datensicherheit mit der notwendigen Sorgfalt adressieren. Zudem sind strenge Compliance-Vorgaben unter anderem bezüglich der Dokumentation von Abläufen, Notfallplänen im Rahmen der Business Continuity sowie generell der IT-Sicherheit einzuhalten. Im Vergleich zu On-Prem wird hier ein höheres Niveau eingefordert, das abhängig von der Branche ausgestaltet ist. In der öffentlichen Verwaltung greift beispielsweise der Mindest-

Wahlfreiheit für den Kunden

Auch wenn das Cloudmodell im Fünfjahresvergleich eventuell schlechter abschneidet als On-Prem, punktet es eindeutig bei den Themen Flexibilität, Skalierbarkeit, rasche Umsetzbarkeit und Sicherheit; bei letzterer ist ein vergleichbarer Standard in der Regel aus Kostengründen lokal nicht zu gewährleisten.

Ideal ist die Wahl eines Anbieters, der für beide Bereitstellungsmodelle dasselbe Funktionsspektrum offeriert. So kann der Kunde im Zweifel problemlos wieder wechseln und hat Wahlfreiheit. •

DIGITAL mit Brief und Siegel

Kontoeröffnungen, Kredit- und Finanzierungsverträge, Versicherungsanträge und Patienteneinwilligungen – die digitale Abwicklung von Vertragsangelegenheiten wird für Kunden zur Selbstverständlichkeit. Für den Vertragspartner auf Unternehmensseite setzt dieser Trend höchste Sorgfalt und Sicherheit bei der Identitätsprüfung voraus. Digitale Verfahren setzen dabei verstärkt auf künstliche Intelligenz.

VON MAXIME HAMBERSIN

ALS PARADEBEISPIEL FÜR DEN DIGITALISIERUNGSTREND in Sachen Vertragsabwicklung gilt die Branche der Finanzdienstleister: Online-basierte Kontoeröffnungen und Darlehensvereinbarungen haben vielerorts längst die Präsenz am Bankschalter abgelöst. Nicht anders sieht es im Versicherungswesen aus. Nahezu alle Assekuranzen bieten ihre Policen online an und wickeln ihr Vertragsmanagement komplett digital ab. Auch das Personalwesen in der Privatwirtschaft nutzt immer häufiger elektronische

Vereinbarungen für das Onboarding neuer Mitarbeiter, ebenso wie das Rechtswesen für die Aufnahme neuer Mandanten und die Unterzeichnung von Geheimhaltungserklärungen. Eine Entwicklung, die nicht schwer vorherzusehen war, weil beide Seiten vom digitalen Vertragsmanagement profitieren: Kunden können Vereinbarungen unabhängig von Ort und Zeit eingehen, Anbieter wiederum erzielen Kosteneinsparungen, schnelle und fehlerfreie Prozesse und eine enge Kundenbindung. Die Voraussetzung für all das: eine hieb- und stichfeste Identitätsprüfung.

Compliance im Blick

Mit digitalen ID-Verifikationsverfahren sind Organisationen in der Lage, die Echtheit des Signierers zu überprüfen und gleichzeitig eine benutzerfreundliche digitale Erfahrung zu bieten. Wichtig dabei ist, dass entsprechende Lösungen für die digitale Ausweisprüfung den spezifischen Compliance-Anforderungen der jeweiligen Branche gerecht werden und sich nahtlos in die Geschäftsabläufe implementieren lassen. So gelten für ein Unternehmen beispielsweise die Richtlinien der EU-Verordnung eIDAS für den Umgang mit elektronischen Signaturen als besonders wichtig, während ein anderes unter Umständen Wert auf das Know-Your-Customer-Prinzip oder das Geldwäschegesetz legen muss, um Betrug vorzubeugen. Eine besondere Herausforderung dabei ist die qualifizierte elektronische Signatur (QES). Sie ist

Voraussetzung für wichtige, regulierte oder grenzüberschreitende Verträge und gilt als einzige Form der digitalen Signatur nach dem eIDAS-Gesetz in der EU als gleichwertig mit einer handschriftlichen Unterschrift. Bislang war das Identifizierungsverfahren jedoch ein zeitintensiver und umständlicher Prozess. Dank neuer KI-gestützter Lösungen können Unternehmen inzwischen sicher und aus der Ferne die Verwendung von gefälschten Dokumenten, Deep-Fakes, vorgefertigten Aufnahmen sowie Identitätsfälschungen verhindern. QES-konforme Identitätsüberprüfungen können integriert werden, ohne den schnellen, effizienten und benutzerfreundlichen Unterzeichnungsprozess zu beeinträchtigen. So kann der Signierer innerhalb von Minuten eine qualifizierte elektronische Signatur sogar auf Mobilgeräten leisten.

Unternehmen sind damit in der Lage, Geschäftsrisiken zu minimieren und die Wahrscheinlichkeit von Betrug oder Identitätsfälschung deutlich zu reduzieren, während Unterzeichner die Schritte zur Identitätsprüfung selbst durchführen können, ohne einen weniger populären Live-Videotermin mit einem Mitarbeiter vereinbaren zu müssen.

Fest steht: Neue generative KI-Systeme werden entwickelt, die ausschließlich für Verträge bestimmt sind. Wir stehen am Beginn einer Zeit, in der KI Teil eines jeden Vertragsprozesses sein wird, mit Ergebnissen, die wir uns heute noch nicht vorstellen können. •

Der AUTOR

Maxime Hambersin

ist Senior Director of Product Management International bei DocuSign.

KUNDENFOKUS und Turbotempo

Den Kunden in den Mittelpunkt stellen und einen Schritt nach dem anderen machen – so geht digitale Transformation für Dimitrios Rizoulis, Senior Vice President B2B Strategie, Transformation & Marketing bei der Deutsche Telekom Geschäftskunden GmbH. Im Interview gibt der Transformationsexperte Einblicke in seine Erkenntnisse aus 20 Jahren Transformations- und Digitalisierungserfahrung.

VON HEINER SIEGER

Oft heißt es, der Kunde steht im Mittelpunkt. Was bedeutet das für Sie als Transformationsexperte?

Dimitrios Rizoulis: Eine Transformation sollte stets mit den Kundenbedürfnissen beginnen. Es ist extrem wichtig, die veränderten Anforderungen der Kunden zu verstehen und das Geschäftsmodell entlang dieser Bedürfnisse zu transformieren. Ein konkretes Beispiel: Bis vor einigen Jahren hat ein Großteil der Mitarbeitenden aus dem Büro gearbeitet und mittels Telefonanlagen kommuniziert. Die Unternehmensdaten wurden aus dem „Datenserver im Keller“ abgerufen. Heute arbeitet ein Teil der Belegschaft von zu Hause aus, kommuniziert durch Kollaborationssysteme wie Zoom oder Webex und ruft Unternehmensdaten über das Internet aus der Cloud ab. Diese Entwicklungen müssen wir als Telekom antizipieren und unsere Produkte und Sicherheitskonzepte auf die veränderten Kundenanforderungen anpassen.

Wie haben Sie die digitale Transformation der Telekom vorangetrieben? Was waren die Schwerpunkte?

DR: Wir haben unser Geschäftskundenportfolio um neue Kundenanforderungen ausgebaut, zum Beispiel unser Repertoire mit „klassischen“ Konnektivitätsprodukten erweitert durch softwaredefinierte Netzwerke, die Standorte besonders sicher und leicht konfigurierbar miteinander vernetzen. Dazu kamen integrierte Angebote, durch die der Kunde bequem Konnektivität und Kollaborati-

onstools im integrierten Paket buchen kann. Innerhalb der Telekom statten wir unsere Vertriebsmannschaften mit den notwendigen Fähigkeiten aus, komplexe Kundenprobleme zu lösen und ihn durch den Digitalisierungs-Dschungel zu navigieren. Das nennen wir „Consultative Selling“.

Wie können Kunden und Partner der Telekom von Ihrer Transformationserfahrung konkret profitieren?

DR: Die Telekom ist der Ende-zu-Ende Digitalisierer für den Mittelstand, Großkunden und die öffentliche Hand. Auf Basis unserer eigenen digitalen Transformationserfahrung können wir unsere Kunden auf Augenhöhe beraten und sie durch ihre Transformation begleiten. Vom Vertrieb bis zur Geschäftsführung spricht bei uns jeder die Sprache der Kunden.

Wie trägt die Digital X dazu bei, die Digitalisierung nicht als Einzelkämpfer bestehen zu müssen?

DR: Europas größte Digitalisierungsinitiative bietet eine Plattform für alle, die die Digitalisierung in Deutschland und Europa beschleunigen wollen. Ein zentraler Punkt sind starke Partnerschaften. Kein Unternehmen kann die Herausforderungen der Digitalisierung allein bewältigen. Dafür haben wir die Digital X als Plattform ins Leben gerufen und sind stolz, sie auch in diesem Jahr mit mehr als 300 Partnern auf die Beine zu stellen.

Wie wichtig für die Transformation ist die Zusammenarbeit zwischen Fach-



Dimitrios Rizoulis, Deutsche Telekom

bereichen und der IT-Abteilung? Worauf sollten Unternehmen achten?

DR: Die IT spielt in jedem Aspekt der Transformation eine Schlüsselrolle – sei es im digitalen Vertrieb, im Service oder in der Produktentwicklung. IT darf nicht mehr als reiner Kostenfaktor gesehen werden, sondern sollte aktiver Mitgestalter der Transformation und Wegbereiter der Digitalisierung sein. Damit IT und Fachbereiche ineinandergreifen können, sind eine enge Zusammenarbeit und agile Entwicklungszyklen von zentraler Bedeutung.

Wie erreichen Unternehmen einfache und schnelle „Quick Wins“ bei der digitalen Transformation?

DR: Ein Geheimrezept für erfolgreiche Transformation gibt es nicht. Ich empfehle, klein und bei einem konkreten Kundenproblem anzufangen. Wurde dieses erfolgreich gelöst, sucht man nach Mustern, die sich auf andere Bereiche und Herausforderungen übertragen lassen. So wird die digitale Transformation in Scheiben schneiden geschnitten und Stück für Stück vorangetrieben. •

Start aus dem Stand

Container isolieren Software von ihrer Umgebung und stellen sicher, dass diese gleichbleibend arbeitet, auch wenn sich die Umgebung verändert. So werden Anwendungen transferierbar, ohne dass der Server heruntergefahren werden muss. Das spart Zeit und ist mit weniger Aufwand verbunden als ein Serverumzug.

VON FALKO TIMME

STELLEN SIE SICH EINE LEICHTGEWICHTIGE SCHUBLADE VOR, in der Ihre Anwendung ausgeführt wird. Diese Schublade ist abschließbar. Sie können sie einfach aus dem einen Schrank herausnehmen und in einen anderen hineinschieben. Die Funktionsweise von Containern ist in etwa vergleichbar. Sie sind einfache Hosting-Umgebungen, die Anwendungen von ihrer Umgebung isolieren und transferierbar machen, ohne dass der Server heruntergefahren werden muss. Ein Container enthält alles, was zum Ausführen der Anwendung notwendig ist. Da der Code in all seinen Abhängigkeiten gespeichert wird, ist die Anwendung schnell und zuverlässig auf den unterschiedlichsten Umgebungen lauffähig. Um zu verstehen, wie Container funktionieren, müssen wir uns zunächst vor Augen führen, dass die meisten Webanwendungen

eine Möglichkeit, um mehrere Instanzen, Webanwendungen oder Dienste isoliert voneinander den Kernel eines Servers nutzen zu lassen.

Aufgrund des gemeinsam genutzten Betriebssystems verbrauchen Container weniger Ressourcen und weniger Speicherplatz, müssen aber mit dem zugrunde liegenden Betriebssystem kompatibel sein. Demzufolge sind sie effizienter als VMs, die eigenständige Betriebssysteme auf dem Host-Server ausführen. Auf einem Server finden im Normalfall mehr Container als virtuelle Maschinen Platz. Allerdings eignen sie sich dadurch nicht für Anwendungen, die z.B. aus Sicherheitsgründen eine strikte Trennung der Anwendungen erfordern. Da nur die Komponenten ausgeliefert werden müssen, die noch nicht auf



Der AUTOR
Falko Timme

ist Gründer und Geschäftsführer von Timme Hosting.

unterschiedliche Softwarekomponenten auf dem Server voraussetzen. Liegen diese Komponenten in verschiedenen Containern, kann jede für sich gepflegt, aktualisiert und unabhängig von den anderen modifiziert werden. Zusammen ergeben die verschiedenen Container und die darauf liegenden Komponenten eine funktionale Einheit mit leicht austauschbaren Teilen.

Reibungslose und effiziente Übertragung der Anwendung

Die sogenannte Runtime bündelt die Dateien einer Anwendung zu einer Einheit. So gebündelte Dateien können als Gesamtheit verlegt und von verschiedenen Betriebssystemen ausgeführt werden. Auf diese Weise unterstützen sie eine reibungslose und effiziente Übertragung der Anwendung und ihrer Dateien zwischen verschiedenen Umgebungen.

Container ähneln in gewisser Weise einer virtuellen Maschine (VM). Anders als VMs enthalten sie allerdings keine vollständige Kopie eines Betriebssystems. Sie sind

dem Host-System laufen, starten containerisierte Anwendungen in der Regel schneller, quasi aus dem Stand.

Eine Festlegung auf den Einsatz von Container-Technologien oder VMs ist im Übrigen nicht notwendig. Im Zusammenspiel ergeben VMs und Container ein leistungsstarkes und flexibles System, um Anwendungen zu installieren und zu verwalten.

Effizientes Arbeiten mit Container-Technologie

In der Softwareentwicklung kommt die Container-Technologie bereits seit einigen Jahren zum Einsatz. Entwickler können sich auf ihren Code fokussieren, ohne die Umgebung, auf der die Software später laufen soll, ständig im Blick zu haben. Außerdem können sie von möglicherweise bereits existierenden Containern profitieren. Gern werden auch Anwendungen in Containern getestet und im Anschluss im gleichen Container in der produktiven Umgebung bereitgestellt. So werden unerwartete Probleme

Da Container Workloads voneinander isolieren, können sie leicht zwischen verschiedenen Computern verschoben werden. Dadurch lassen sich kleine **Konfigurationsänderungen problemlos** von einem Server zu einem anderen portieren. Sollte doch mal ein Serverumzug nötig sein, lässt sich dieser mit Containern unkompliziert abwickeln.

me aufgrund von Konfigurationsunterschieden zwischen Test- und Produktionsumgebung vermieden.

Anwendungen mit einer Microservices-Architektur lassen sich beispielsweise mit Containern einfach umsetzen. Für jeden Microservice erstellt der Entwickler einen separaten Container, um diese dann mit einem Orchestrierungstool und einem Service Mesh zu vollständigen Anwendungen zu verbinden. Technisch gesehen ist dies auch mit VMs oder direkt auf dem Server möglich. Allerdings sind Container mit ihrem geringen Ressourcenverbrauch und den schnellen Startzeiten hier im Vorteil.

Für Admins steht vor allem die Flexibilität im Vordergrund, die sie durch den Einsatz von Containern gewinnen sowie die potenziell reduzierte Anzahl der benötigten Systeme.

Container eignen sich für die schnelle Installation von Anwendungen beispielsweise über einen „App-Installer“ als Hilfstool. Da sie selbst kein Betriebssystem enthalten, besteht nur ein geringer Installationsaufwand. Außerdem werden Anwendungen in Containern immer auf die gleiche Weise ausgeführt. Dabei spielt es keine Rolle, wo sie implementiert sind. So werden Betriebsabläufe konsistenter.

Die Vorzüge von Containern

Da Container Workloads voneinander isolieren, können sie leicht zwischen verschiedenen Computern verschoben werden. Dadurch lassen sich kleine Konfigurationsänderungen problemlos von einem Server zu einem anderen portieren. Sollte doch mal ein Serverumzug nötig sein, lässt sich dieser mit Containern unkompliziert abwickeln.

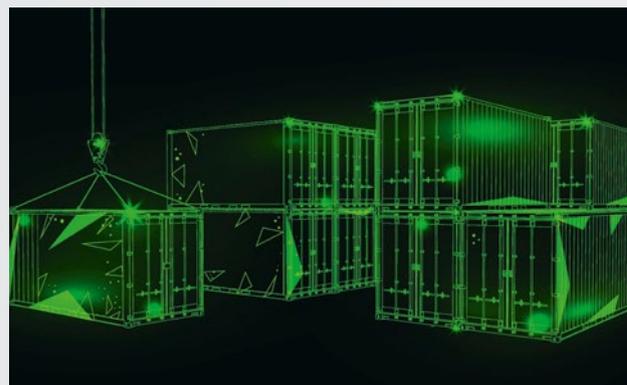
Wichtig ist hierbei nur, dass das Betriebssystem grundsätzlich kompatibel ist. So laufen dieselben Container beispielsweise problemlos auf verschiedenen Distributionsfamilien von Linux wie Ubuntu oder Debian, aber nicht unter Windows.

Außerdem stellt diese Isolierung auch die Trennung von Daten und Code sicher. Dadurch, dass Daten außerhalb des Containers gespeichert werden, ist die Aktualisierung von Containern unkompliziert möglich. Der komplette Container kann einfach durch die jeweils aktuelle Version ersetzt werden. Das dauert im Normalfall nur wenige Sekunden.

Von der Container-Effizienz profitieren

Vor allem Teams, die eine Reduzierung ihrer Infrastrukturkosten anstreben, profitieren von der Effizienz von Containern im Vergleich zu virtuellen Maschinen. Der Umstieg von VMs zu Containern führt mit einer hohen Wahrscheinlichkeit zu einem geringeren Ressourcenbedarf. Die gleichen Workloads können auf weniger Servern gehostet werden.

Anwendungen, die auf Containern laufen, können fast aus dem Stand gestartet werden. Bei VMs müssen für den Boot-Vorgang dagegen einige Minuten geopfert werden. Ein Container ist also 'just in time' nutzbar, wenn die Anwendung gebraucht wird und verschwindet anschließend wieder. Das spart nicht nur Ressourcen, sondern auch Zeit. In den meisten Fällen sind Container nicht größer als wenige hundert Megabyte. Eine VM dagegen kann mit ihrem eigenen Betriebssystem mehrere Gigabyte umfassen. •



REVOLUTION im Service

Mit ihrer Fähigkeit zur Analyse auch komplexer Zusammenhänge wird generative KI die Welt des Kundenservice komplett verändern. Bereits heute lassen sich mit Chatbot-Netzwerken sehr leistungsfähige Systeme für den effektiven Kundendialog aufbauen. Welche Mehrwerte die Integration KI-basierter Sprachmodelle wie ChatGPT bietet, zeigen bereits heute konkrete Use Cases.

VON HARALD HUBER

FÜNF TAGE HAT ES GEDAURT, BIS CHATGPT Ende vergangenen Jahres die Schwelle von einer Million Nutzern erreichte. Andere beliebte Online-Dienste benötigten hierfür zuvor wesentlich länger, Monate oder gar Jahre. Die Dynamik dieser Entwicklung spiegelt die Tatsache, dass sich inzwischen praktisch jedes Unternehmen aktiv mit den Möglichkeiten einer generativen KI auf Basis von Large Language Models (LLMs) auseinandersetzt, und permanent neue

...



Der AUTOR
Harald Huber
ist CTO der USU Software AG

Einsatzzwecke identifiziert und evaluiert werden. Auch für die Servicewelt hat die neue Technologie disruptiven Charakter. Denn generative KI verfügt inzwischen über hoch entwickeltes Sprachwissen. Entsprechende Systeme können daher Prozesse rund um Bedeutung und Inhalte automatisieren und bieten für den Kundenservice konkrete Rationalisierungspotenzia-

Die steigende Komplexität von Alltagsprodukten wie Autos, Kaffeemaschinen, Waschmaschinen oder elektrischen Zahnbürsten erfordert einen anderen Service als den, den wir heute gewohnt sind. Large Language Modelle werden diese **Servicevolution** Wirklichkeit werden lassen und sie hat bereits begonnen.

le, z. B. minimierte Redaktions-, Pflege- und Service-Aufwände.

Die Servicewelt im Wandel

Auch wenn sich Chatbots zuletzt zu einem festen Bestandteil im Kundendienst-Alltag entwickelt haben, konnten die klassische Dialogsysteme bis heute meist nur vorab erstellte „Frage-Antwort-Szenarien“ umsetzen und einfache Fragen beantworten, z. B. zur Lieferfähigkeit von Produkten, zu Terminvereinbarungen, Versicherungspolice, Wetterdaten etc. Damit entlasten sie Service-Teams von Routine-Anfragen. Nicht mehr, aber auch nicht weniger.

Ein von internationalen Marktanalysten anerkannter Meilenstein führte ab 2022 zu einer signifikanten Leistungssteigerung von intelligenten Chatbots, die als Team agieren. Auf Basis einer Multibot-Architektur werden mehrere Chatbots zusammengeschaltet und können so auch komplexe Aufgaben lösen. Das Modell unterteilt Chatbots in zwei Rollen: Experten- und Lead-Bots. Dabei liefern die Expertenbots Informationen zu bestimmten Fachthemen, der Lead-Bot fungiert als Moderator und weist dem Anwender den für sein Anliegen passenden Experten-Bot zu.

Diese Technologie hat einen weiteren Vorteil – denn durch die beschriebene Architektur lassen sich ein oder mehrere ChatGPT-Bots sehr einfach integrieren. Entsprechend bildet ein solches Szenario die ideale Ausgangslage für verschiedene Use-Cases, die sich bereits heute mithilfe der intelligenten Technologie in der Praxis realisieren lassen.

IT-Wissen des Internets auf Knopfdruck

Beispielsweise nutzt ein IT-Dienstleister in seinem Kundenportal einen ChatGPT-Bot als zentralen Service-Baustein für allgemeine IT-Fragen. Neben den klassischen Chatbots für die Bereiche Anwendungen, Fernzugriff und Smartphone agiert der neue ChatGPT-Bot als Experte für allgemeines IT-Wissen. So antwortet er etwa korrekt auf die Frage, wie

man Netzwerklaufrerke anbindet, wie man Macros in Excel entwickelt bzw. nutzt oder mit welcher Tastaturkombination sich Smileys erzeugen lassen. Im Kontext der Frage liefert der ChatGPT-Bot das komplette IT-Wissen des Internets. Durch sein Sprachverständnis lassen sich Frage und Antwort leicht verfeinern, so dass ChatGPT in der Praxis konkret helfen kann.

Hinzu kommt ein weiterer Vorteil: Der Chatbot liefert oftmals nicht nur die Lösung des Problems, sondern führt die notwendigen Aktionen direkt selbst aus. Die Möglichkeiten sind nahezu grenzenlos: Vom Leeren des Browser-Caches oder dem Passwort-Reset über das Wiederherstellen der Netzwerklaufrerke, die skriptgesteuerte Installation neuer Treiber und die Änderung der Spracheinstellung der Tastatur bis hin zum Einrichten eines Druckers. Da diese „alltäglichen“ Anfragen erfahrungsgemäß einen großen Teil des Ticket-Aufkommens (ca. 25 %) ausmachen, führt dies zu einer deutlichen Reduktion der Helpdesk-Anfragen. Schließlich müssen Unternehmen für allgemeine IT-Fragen keine Dokumente in der Wissensdatenbank erstellen bzw. pflegen. Davon profitieren letztlich alle: das IT-Team, zahlreiche Mitarbeiter und im zweiten Schritt tausende Anwender auf Kundenseite.

FAQs automatisch erstellen

Eine weitere Einsatzmöglichkeit für generative Sprachmodelle im Service ist das Erstellen und Strukturieren relevanter Inhalte für die verschiedenen Verwendungszwecke. In der Praxis ist dies oft sehr aufwändig und damit eine der größten Hürden, eine Wissensdatenbank einzuführen. Künftig kann generative KI hierbei unterstützen, indem das System wichtige Informationen aus Tickets, Handbüchern etc. analysiert, klassifiziert und in übersichtliche Strukturen gliedert.

So setzt ein Versicherungsunternehmen den ChatGPT-Bot im Kontext seiner Wissensdatenbank auch für das automatisierte Erstellen von FAQ-Dokumenten ein. Bislang mussten Experten-Teams komplexe

Dokumente durcharbeiten sowie Fragen und Antworten möglichst verständlich formulieren – jetzt wird deren Aufwand minimiert. Dabei dienen längere Texte wie Verträge und Handbücher als Grundlage. Ein Dokument, zum Beispiel ein umfangreicher Leasingvertrag, wird hochgeladen, Agenten stellen ChatGPT Fragen und bewerten dessen Antworten im Anschluss mit Feedback (gut / schlecht), wodurch die KI lernt und sich kontinuierlich verbessert. Aus den „gut“ bewerteten Antworten wird ein Feedback-Protokoll erstellt, das wiederum die FAQs speist.

Eine neue Zeitrechnung beginnt

Mit den LLMs stehen wir am Anfang einer neuen Zeit. Diese ermöglichen neue Einsatzmöglichkeiten: Sie erlauben es, Situationen im richtigen Kontext zu erkennen und Anfragen in nicht gekannter Qualität zu beantworten – und das ohne umfangreiches Training, das in der Vergangenheit ihren Einsatz erst möglich machte. Damit wird generative KI in der Lage sein, auch im Kundenservice die Bereiche Onboarding, Systemintegration, Zusammenarbeit und Prozesse zu verändern.

Und das nicht nur im Servicecenter selbst, sondern auch im Self Service oder beim Funktionsumfang von Produkten. Beispielsweise wird es auch Services für Haushaltsprodukte wie z. B. einen Kühlschrank geben, die nicht nur bei technischen Problemen, sondern auch bei der Nutzung unterstützen: Das System lernt beispielsweise Gewohnheiten kennen, weiß über seinen „Lagerbestand“ Bescheid, kann Angebote lesen und Einkaufslisten erstellen. Bei Eskalationen unterstützt das Service Center.

Die steigende Komplexität von Alltagsprodukten wie Autos, Kaffeemaschinen, Waschmaschinen oder elektrischen Zahnbürsten erfordert einen anderen Service als den, den wir heute gewohnt sind. LLMs werden diese Servicerevolution Wirklichkeit werden lassen und sie hat – das zeigen die genannten Beispiele – bereits begonnen. •

UC oder UCaaS - die optimale Lösung finden

Die Pandemie hat die Migration in die Cloud erheblich beschleunigt und den Trend zu UCaaS (Unified Communications as a Service) gefestigt. Dabei führten insbesondere hybride Arbeitsmodelle zu einer gesteigerten Nachfrage nach Diensten, die Unternehmen ihren Mitarbeitern schnell und unabhängig vom Standort zur Verfügung stellen können.

VON JÜRGEN ENGELHARD

TROTZ DES WACHSENDEN EINSATZES VON UCAAS ist jedoch nicht automatisch jede Firma damit am besten bedient. Eine Vielzahl von UC-Lösungen wird nach wie vor eingesetzt, sei es beim Kunden gehostet, lokal betrieben oder in hybrider Form. Eine von Mittel in Auftrag gegebene Studie des Branchenanalysten TechAisle zeigt: 88 Prozent der deutschen Unternehmen setzen immer noch lokale Lösungen ein, während fast die

aus Infrastrukturen erfordern, sei es On-Premises, öffentliche Cloud, private Cloud oder eine hybride Lösung. Eine Einheitslösung ist für die meisten nicht mehr realisierbar, und oft sind On-Premises-UC-Lösungen die bevorzugte Wahl, einschließlich in einer privaten Cloud. Es gibt gute Gründe für On-Premises-

deutet darauf hin, dass Unternehmen mehr in langfristige UC-Lösungen investieren müssen. Um dies zu erreichen, müssen sie Investitionsbereiche identifizieren, die langfristigen Wert haben, und die Kostenfolgen der verschiedenen Bereitstellungsoptionen bewerten. Laut einer Studie des UC-Forschungsunternehmens Metrigy sind On-Premises-Lösungen etwa 21 Prozent kostengünstiger zu betreiben als UCaaS.



Während UCaaS in einigen Fällen erhebliche Vorteile bietet, ist es nicht automatisch die richtige Option für jedes Unternehmen. Unternehmen, die komplexe, maßgeschneiderte Kommunikation, ein hohes Maß an Kontrolle und Sicherheit sowie die Fähigkeit zur Skalierung und Zuverlässigkeit benötigen, werden möglicherweise weiterhin feststellen, dass eine vor Ort und in der privaten Cloud betriebene Kommunikationsplattform die ideale Wahl ist, möglicherweise sogar mit niedrigeren Gesamtbetriebskosten als UCaaS.

Anstatt einer Einheitslösung sollten Kunden individuell unterstützt werden, unabhängig davon, ob sie sich für lokale, hybride Modelle oder die Cloud entscheiden. Durch die Auswahl einer Bereitstellungsoption oder einer Kombination von Optionen, die ihren Bedürfnissen am besten entsprechen, werden Organisationen langfristigen Erfolg sicherstellen und ihre UC-Investitionen optimieren. •



Der AUTOR
Jürgen Engelhard
ist Business Development Manager bei Mittel Deutschland.

Hälfte (44 Prozent) entweder aktuell ihre On-Premises-Kommunikation in die Cloud verlagert oder dies in Erwägung zieht. Da On-Premises-UC weiterhin relevant ist, ist es wichtig zu verstehen, welche Vor- und Nachteile jede Bereitstellungsoption bietet.

Flexible UC-Lösungen sind gefragt

Hybrides Arbeiten ist für viele Organisationen keine Frage der Wahl mehr, und 77 Prozent der Mitarbeiter stimmen zu, dass bessere Kommunikations- und Kollaborationstools ihnen helfen, ihre Arbeit besser zu erledigen, egal wo sie sich befinden.

Aber viele Organisationen haben einzigartige Kommunikationsbedürfnisse, die eine Mischung

UC-Lösungen, da sie eine niedrigere Gesamtbetriebskosten, mehr Flexibilität und Kontrolle, eine verbesserte Integration von Kommunikation und Workflows sowie höhere Zuverlässigkeit bieten.

UC als Investitionsmöglichkeit

Unternehmen sollten sich bewusst sein, dass UC eine zentrale Komponente von Modernisierungsprozessen im Unternehmen ist und ein ebenso wichtiger Baustein für eine funktionierende hybride Arbeitsumgebung. Aber gerade hier gibt es Nachholbedarf: Die Daten von TechAisle zeigen, dass nur 47 Prozent der deutschen Unternehmen grundlegende Optionen für hybrides Arbeiten haben. Dies

Prozesse konsequent zu Ende gedacht

Neue Wettbewerber, kürzere Innovationszyklen, gestörte Lieferketten, anhaltender Kostendruck und komplexe Rahmenbedingungen: Märkte sind heute dynamischer denn je. Umso sind Unternehmen darauf angewiesen, kontinuierlich und sicher neue Chancen und damit letztlich Aufträge und Umsätze zu generieren. Moderne CRM-Lösungen sind dabei ein unverzichtbares Werkzeug. **VON GERD KUCHELMEISTER**

CRM-LÖSUNGEN SIND IM MITTELSTAND NICHTS NEUES.

In vielen Fällen handelt es sich jedoch um veraltete Insellösungen, die zwar Outlook und Excel ablösen, aber letztlich keinen großen Mehrwert bieten. Denn die Herausforderung besteht nicht darin, nur neue Leads zu generieren, sondern die richtigen Leads zu generieren. Anders formuliert: Eine moderne CRM-Lösung sollte Unternehmen dazu befähigen, bereits in der Vertriebsphase die Profitabilität von zukünftigen Verkaufsfällen zu identifizieren, und somit die rentable Auslastung von Kapazitäten in der Produktion sicherzustellen mit dem Ziel, das Unternehmenswachstum zielgerichtet zu steuern.

Kein CRM ohne ERP

Um dieses Ziel zu erreichen, sind End-to-End-Szenarien erforderlich, die vom Marketing über Sales und Auftragseingang bis zu Produktion bzw. Projektumsetzung sowie Customer Service oder Field Service den Kundenprozess durchgehend abbilden und die gesamte Kommunikation an einem Ort bündeln. Neben einem umfassenden Prozessverständnis auf Seiten des CRM-Partners ist ein automatisierter Zugriff auf das ERP-System erforderlich. Über Schnittstellen sind praktisch alle Kombinationen möglich. Besonders einfach geht dies mit Plattformen wie Microsoft Dynamics 365, die ERP, CRM, BI, DMS, Office und Teams auf

einer Plattform mit einer gemeinsamen Datenbasis verbinden. Ein weiterer Vorteil von Microsoft Dynamics 365 CRM ist eine nahtlose Integration in etablierte Tools wie Office und Teams. Das steigert die Produktivität und wirkt sich letztlich auch die Zufriedenheit der Mitarbeitenden aus

Bessere Daten

Der Vertrieb wird in die Lage versetzt, bereits in der Angebotsphase zu ermitteln, welchen Deckungsbeitrag ein potenzieller Neukunde liefern könnte. Ebenso sind klare Aussagen zu Lieferterminen und Projektvolumina möglich, wenn die Produktions- bzw. Projektplanung im ERP vom CRM systemgesteuert ausgewertet werden. Neben einer optimalen Auslastung der Ressourcen, können über das CRM die idealen Ziel- und Zukunftsdaten identifiziert werden. Unternehmen stellen damit sicher, dass sie nicht nur rentable, sondern auch zukunftsichere Marktsegmente bedienen. End-to-End-Systeme sind weiterhin für eine Automatisierung und damit Skalierung der Prozesse von Marketing und Sales unverzichtbar. Ebenso bilden sie die Basis für ein Training von KI-Funktionen, etwa für die Gewichtung von Verkaufschancen oder das Erstellen von präziseren Forecasts.

Potenziale nutzen

Branchenübergreifend haben Unternehmen Ihre Produktion bzw. Projekt-

abwicklung in den vergangenen 20 Jahren konsequent auf Produktivität optimiert. Im Sales dagegen besteht in dieser Hinsicht vielfach noch ein großes, ungenutztes Potenzial.

Moderne CRM-Lösungen tragen dazu bei, diese Chancen nutzen und das Wachstum der Unternehmen zu sichern. Gleichzeitig bieten Sie gleich in doppelter Hinsicht eine Antwort auf den Fachkräftemangel: Einerseits durch eine Professionalisierung der Sales-Prozesse inklusive Automatisierung und KI-Einsatz, andererseits durch eine Positionierung als attraktiver Arbeitgeber. Denn die eingesetzte IT-Umgebung wird zunehmend zu einem wichtigen Auswahlkriterium bei Bewerbern. •



Der AUTOR

Gerd Kuchelmeister leitet als Geschäftsführer den CRM-Bereich der KUMAVISION.

Fünf Gamechanger für mehr Umsatz

Klassisches Verkaufen mit klarem Produktfokus war gestern. Heute wird erwartet, dass der Vertrieb umfassend berät und Mehrwerte in den Vordergrund stellt. Kunden wollen sich und ihre Probleme verstanden wissen und nahtlos auf allen Kanälen individuell abgeholt werden. Zum Glück gibt es Lösungen dafür.

VON THILO KERNER

Gamechanger 1: Value based Selling

Der Klassiker im Vertrieb: Im Masterfoliensatz des eigenen Unternehmens wird eine Produktpräsentation gebastelt, welche die Top-Features herausstellt. Ein Vorgehen wie von gestern. Moderne Top-Seller gehen anders vor. Heute muss es darum gehen, den Mehrwert eines Produktes oder einer Leistung zu vermitteln – und zwar individuell für den Kunden. Dabei ist besonders wichtig: es muss für Dritte einfach nachvollziehbar sein, was dieser Mehrwert ist.

Das gelingt besser, wenn zum Beispiel das Präsentationsmaterial im Design des Kunden erstellt wird. Für das verkaufende Unternehmen auf der anderen Seite fängt Value Based Selling schon ganz einfach damit an, richtig zu qualifizieren. Das heißt: Wie man Mehrwert stiften kann, muss geklärt sein, bevor man in ein Projekt einsteigt. Dabei sollte ein Thema auch aus unterschiedlichen Blickwinkeln betrachtet und entsprechend aufgeteilt werden. Es sollte also im Verkaufsprozess geklärt werden, welche Mehrwerte Vertrieb, Business Development und Projektteam an welchem Punkt der Kundenreise konkret vermitteln können. Hier kann auch das CRM helfen, um Business Cases zu formen und dann z.B. über verschiedene Kanäle dem Kontakt unterschiedlichen Content liefern.

Gamechanger 2: KI-gestützte CRM-Systeme

Das Wichtigste in moderner Vertriebssteuerung ist die Transparenz über die Pipeline – und die Fähigkeit, daraus Maßnahmen abzuleiten. Moderne Vertriebsorganisationen nutzen dazu künstliche Intelligenz im CRM, zum Beispiel für smartes Pipeline-Management, Forecasting und Opportunity-Handling. Ein wertvoller Outcome: Mit KI können verblüffend akkurat und mit wenig Zeitauf-

wand Gaps und Risiko-Opportunitys identifiziert werden. So können Vertriebsleiter deutlich genauer abschätzen, ob Ziele erreicht werden – oder eben, ob gegengesteuert werden muss. Und vor allem: Vertriebsmitarbeiter finden entsprechend intelligente CRM-Systeme (oder ggf. einfache Add-Ons) gut, weil sie damit effizienter arbeiten, weniger Zeit im Tool verbringen und mehr Zeit mit dem Kunden haben.

Ein weiteres Beispiel, das das Vertriebsspiel gerade verändert: Guided Selling. CRM-Systeme können heute intelligent erinnern, wann was getan werden muss. Und noch mehr: sie können ebenfalls eingehende E-Mails scannen und erkennen, was der Absender wissen will, und entsprechende Antwortvorschläge machen. So wird das Vertriebsleben deutlich effizienter. Und nicht zu vergessen: Neue Mitarbeiter können schneller eingelernt werden und Ergebnisse liefern.

Die Einsatzgebiete von KI im Vertrieb sind riesig. Weitere Beispiele sind: Leadscoring, Qualifizierung von Opportunities, Touchpointanalysen und mehr.

Gamechanger 3: Social Selling

Es wird oft unterschätzt, aber: Menschen kaufen von Menschen, obwohl es abgedroschen klingt. Man muss beim Social Selling aber differenzieren. Für die eigene Strategie ist es wichtig, sich zu fragen, welcher Social-kanal Inbound- oder Outbound-Instrument ist. Dann muss der Content entsprechend aufbereitet und gut sein. Ein Tipp: Als Outbound-Kanal sollte beispielsweise LinkedIn nur genutzt werden, wenn es auch viele Touchpoints mit dem Kunden, also viele Likes etc. gibt. Ansonsten sollten sich Seller auf Inbound fokussieren und als Markenbotschaf-

Das Wichtigste in moderner Vertriebssteuerung ist die Transparenz über die Pipeline – und die Fähigkeit, daraus Maßnahmen abzuleiten. Moderne Vertriebsorganisationen nutzen dazu **künstliche Intelligenz im CRM**, zum Beispiel für smartes Pipeline-Management, Forecasting und Opportunity-Handling.

ter auftreten. Wichtig ist auch der Unterschied von Unternehmen und Person. Über das Unternehmen Events und Content-Formate zu promoten, ist heute essenziell in der Marktbearbeitung.

Gamechanger 4: Omnichannel-Vertrieb

Grundsätzlich sollte das Ziel einer Omnichannel-Vertriebsstrategie darin bestehen, ein nahtloses Kundenerlebnis über verschiedene Kanäle hinweg zu schaffen, um den Verkauf zu steigern und die Kundenbindung zu stärken. Moderne Vertriebsorganisationen nutzen diese Strategie aber für deutlich mehr.

1. Vereinfachung der Steuerbarkeit der Vertriebsaktivitäten.

Durch die Integration von Daten und Technologien kann die Vertriebsleitung beispielsweise die Leistung jedes Kanals messen und optimieren, um das Gesamtergebnis zu verbessern.

2. Verringerung der Komplexität der Vertriebsprozesse.

Richtig umgesetzt können durch die entsprechende Integration von Vertriebskanälen und die Automatisierung von Prozessen Vertriebsmitarbeiter effizienter arbeiten und sich auf wichtige Aufgaben konzentrieren.

3. Integration neuer Geschäftsmodelle

Durch CX-fokussierte Prozesse und Lösungen (wie beispielsweise Kundenportale) können völlig neue digitale Services angeboten und somit neue Einnahmequellen erschlossen werden.

Gamechanger 5: Die Verbindung von eCommerce und Sales

Die große Frage bei der Integration von eCommerce-Prozessen in die Vertriebsstrategie lautet, welche Prozesse auf welchem Kanal laufen sollten. Hier ist die große Herausforderung, den Vertrieb nicht mit digitalen Interaktionen zu überfrachten. Über ein dediziertes Customer Journey- und CX-Mapping sollten Sie sicherstellen, wann ein digitaler Kanal wirklichen Output für den Vertrieb generiert, und welche Software-Lösung dazu nötig ist.

Hier sind vier Beispiele für Synergien zwischen analogen und digitalen Prozessen:

1. Absprünge von Angeboten in den Webshop: Webshops eignen sich hervorragend für die Visualisierung auch komplexer Produkte vor Ort. Machen Sie in Angebo-

ten darauf aufmerksam. Zudem können dort personalisierte Angebote zu Cross- und Upselling-Produkten gemacht werden.

2. Produktberatung anhand von Live-Daten: Senden beispielsweise Maschinen Nutzungsdaten an ein Portal, kann ein Vertriebsmitarbeiter diese Daten verwenden, um in einem persönlichen Gespräch Cross- und Upselling-Vorschläge zu Optimierungen machen.

3. Preisvorschläge mit CPQ: Die Digitalisierung von Angebots- und Produktkonfigurationsprozessen kann nicht nur diese Prozesse effizienter und erfolgreicher machen, sondern auch zu Synergien führen. CPQ-Programme können beispielsweise Vorschläge machen, welche Discounts bei welchem Produkt am erfolgreichsten sind.

4. Perfect Store: In fortschrittlichen CRM-Systemen lässt sich abbilden, was in welchen Showrooms verfügbar ist und wie die Verkaufsräume ausgestattet sind. Ebenfalls lassen sich Engagement Maps einfügen, um die optimale Positionierung von Produkten zu erreichen und den Vertriebsmitarbeiter bei einem Kundenbesuch anzuleiten. •

Der AUTOR

Thilo Kerner

ist Chief Revenue Officer und Mitglied der Geschäftsleitung bei Sybit.



Der Mittelstand kann deutlich profitieren

Private 5G-Netze sind eine Schlüsseltechnologie, die einen wesentlichen Beitrag zur Entwicklung von Smart Factories und zur Zukunftsfähigkeit des Wirtschaftsstandortes Deutschland leistet. Die Chancen sind vielfältig.

VON MARKUS KOERNER

5G-KONNEKTIVITÄT ERFÜLLT HÖCHSTE BUSINESS-ANFORDERUNGEN bezüglich Übertragungsraten, Zuverlässigkeit und Verfügbarkeit. Bereits ein Viertel der deutschen Industrie setzt auf proprietäre 5G-Netze, so eine Bitkom-Umfrage. Laut dieser Erhebung wollen 26 Prozent der Industrieunternehmen hierzulande sogenannte Campusnetze aufbauen oder haben dies bereits getan. Prognosen zufolge könnten bis 2027 bereits 90 Prozent der Netzwerke in Fertigungsbetrieben 5G verwenden.

Vor allem OEMs und Zulieferer der Automobilindustrie werden von der neuen Technologie in Deutschland profitieren. Der Fokus auf den Ausbau der Elektromobilität begrenzt zwar aktuell die Zahl der umgesetzten privaten Netzwerke noch. Aber der Markt für 5G-Netze befindet sich in der Startphase. Und auch der deutsche Mittelstand kann deutlich profitieren. Dies zeigt ein Papier des Bundeswirtschaftsministeriums: Die Mehrzahl der rund 10.000 erwarteten 5G-Netze soll bis 2025 in kleinen und mittelständigen Unternehmen zu finden sein werden.

Die Vorteile für Unternehmen werden dafür sorgen, dass die Umsetzungszahlen in den kommenden Jahren sehr stark ansteigen werden. 5G-Netzwerke unterstützen eine signifikant höhere Anzahl vernetzter Geräte im Vergleich zu früheren Generationen von drahtlosen Netzwerken. Dadurch können nicht nur mehr Mobiltelefone pro Funkzelle zuverlässig versorgt werden, diese gesteigerte Kapazität ist auch in modernen Produktionsanlagen entscheidend, wo eine Vielzahl von Sensoren, Robotern und IoT-Geräten nahtlos kommunizieren müssen.

Vergabe der 5G-Frequenzen

Private 5G-Netzwerke funktionieren ähnlich wie herkömmliche Mobilfunknetze, sind jedoch nur in einer lokal begrenzten Umgebung wie einem Betriebsgelände oder einer Fabrik verfügbar. So können Unternehmen eine klare Trennung nach außen realisieren. Bei WLAN waren sie beispielsweise weitgehend auf Service Provider angewiesen. Private 5G-Netzwerke basieren hingegen auf Frequenzen, die ausschließlich den jeweiligen Unternehmen zur Verfügung stehen.

Dazu werden die entsprechenden Frequenzbänder für einen bestimmten Zeitraum angemietet. In Deutschland erfolgt die Vergabe der 5G-Frequenzen durch die

Bundesnetzagentur. Während die übergeordneten Frequenzbänder für die großen Mobilfunkanbieter versteigert wurden, existiert für Unternehmen ein Antragsverfahren. Darüber werden Teilbereiche der Spektren von 3,7 bis 3,8 Gigahertz und 24,25 bis 27,5 Gigahertz zugeteilt.

Unabhängigkeit, Sicherheit und Kontrolle durch Campusnetze

Der Aufbau von eigenen 5G-Infrastrukturen erlaubt es Unternehmen, sich von Telekommunikationsdienstleistern unabhängiger zu machen. Sie können nun die vollständige Kontrolle über die Verwaltung selbst übernehmen und festlegen, welche Geräte und Personen sich mit dem Netzwerk verbinden dürfen und wie das zu geschehen hat.

Diese weitreichenden Kontrollmöglichkeiten zahlen auch auf das Thema Netzwerksicherheit ein: In proprietären Mobilfunknetzen können Unternehmen SIM-basierte Authentifizierungsverfahren einsetzen. Darüber hinaus verfügen die Drahtlosschnittstellen über eine starke



Verschlüsselung. Einzelnen Geräten können dezidierte Sicherheitsrollen zugewiesen werden, was es einfacher macht, die volle Kontrolle über die Systeme zu behalten. Dieser Aspekt ist wichtig, da in einer Smart Factory das Netzwerk die zentrale Steuerungs- und Kontrollinstanz ist und ein gelungener Angriff drastische Folgen haben könnte.

Neben mehr Kontrolle und stärkeren Sicherheitsmaßnahmen helfen proprietäre 5G-Netzwerke auch dabei,

Riesiges Gelände, flächendeckende Konnektivität

Dow Chemical verfügt in Freeport, Texas, über eines der größten Fabrikgelände der Welt. Um den Betrieb zu rationalisieren, Wartungsaufgaben zu optimieren und eine zuverlässige Abdeckung des gesamten Geländes zu gewährleisten, entschied sich der Chemiekonzern für die Einrichtung eines proprietären Mobilfunknetzwerks. Die Verantwortlichen wollten sicherstellen, dass den Mitarbeitern auf dem Gelände die erforderlichen Informationen zur Verfügung stehen, damit sie präzise und zeitnah interagieren, zusammenarbeiten und Probleme lösen können.

Dow erstellte zunächst ein Proof-of-Concept und arbeitete innerhalb von 12 Monaten mit Kyndryl und Nokia zusammen, um ein privates Drahtlos- und Edge-Netzwerk in dem Industriekomplex mit einer Fläche von über einer Million Quadratmetern zu implementieren und zu skalieren. Die neue Netzwerkinfrastruktur ermöglicht



Der AUTOR Markus Koerner

ist Präsident von Kyndryl Deutschland.



Private 5G-Netzwerke werden sich in den kommenden Jahren über **viele Branchen** hinweg verbreiten. Sie können ihre Vorteile nicht nur in der Industrie, sondern auch im Handel, im Finanzsektor, dem Gesundheitswesen und weiteren Branchen ausspielen.

laufende Kosten zu senken. Die Gesamtbetriebskosten privater Netzwerke sind in der Regel deutlich geringer als die herkömmlicher Drahtlosnetzwerke.

Hinzu kommt, dass komplexe Anlagen und verwinkelte Gebäudestrukturen auf den Betriebsgeländen dazu führen können, dass „Blinde Flecken“ entstehen, also Stellen, an denen ein Signal zu schwach für zuverlässige Konnektivität ist. Sie können auch durch Interferenzen mit anderen Netzen entstehen. 5G schafft hier Abhilfe: Die Technologie garantiert wesentlich zuverlässigere Signalübertragung als WLAN und die proprietäre Bereitstellung minimiert das Interferenzproblem.

Um die Vorteile des neuen Funkstandards voll auszunutzen, sollten auch weitere innovative Technologien implementiert werden. Die Möglichkeiten des industriellen IoT (IIoT) können zum Beispiel mit Edge Computing und erweiterten Cloud Ressourcen in Kombination mit einer 5G-basierten Datenübertragung viel besser ausgeschöpft werden.

Augmented-Reality-Anwendungen, Audio- und Remote-Video-Zusammenarbeit, intelligente Verfahren in Echtzeit, Personal-Tracking vor Ort, bessere Arbeitssicherheit und Fahrzeugtelematik.

Konnektivität von morgen

Private 5G-Netzwerke werden sich in den kommenden Jahren über viele Branchen hinweg verbreiten. Sie können ihre Vorteile nicht nur in der Industrie, sondern auch im Handel, im Finanzsektor, dem Gesundheitswesen und weiteren Branchen ausspielen. Unternehmen sollten jetzt die Potenziale der Technologie evaluieren, um nicht von der Konkurrenz abgehängt zu werden.

Eine schlüsselfertige Einheitslösung für die Konnektivität von morgen gibt es allerdings nicht. Die Anforderungen an Datenübertragung unterscheiden sich je nach Branche und Unternehmen. Anbieter, die entsprechende Lösungen realisieren möchten, müssen daher verschiedene Technologien integrieren, um die Anforderungen der Kunden realisieren zu können. •

RANSOM(EVERY)WARE?!

Ransomware ist mittlerweile fast jedem ein Begriff. Die Taktiken werden jedoch raffinierter und Hacker sind keine einsamen Kleinkriminellen mehr, sondern operieren wie hochprofessionelle Unternehmen. Umso wichtiger, dass IT-Entscheider auf dem neuesten Informationsstand bleiben und den Überblick über Trends und Sicherheitsrisiken behalten.

VON IAN MCSHANE

Selbst wenn ein Opfer das Lösegeld bezahlt, gibt es keine Garantie dafür, dass Systeme „unversehrt“ bleiben oder die Bedrohungsakteure keine Kopien der Daten für zukünftige Erpressungen gespeichert haben. Jüngste Untersuchungen haben ergeben, dass **vier von fünf Ransomware-Opfern** erneut Opfer eines solchen Angriffs werden.

EREIGNISSE VON GLOBALER DIMENSION WIE KRIEGE und Wirtschaftskrisen ziehen häufig eine Flut von Cyberangriffen nach sich und hinterlassen eine Spur der digitalen Verwüstung. Trotz einiger Teilerfolge der internationalen Strafverfolgungsbehörden bleibt die Eindämmung der Cyberkriminalität jedoch schwierig. Wird wie kürzlich Qakbot, ein Malware-Netzwerk ausgeschaltet, formiert sich kurz darauf ein neues – im Zweifelsfall mit noch ausgefeilteren Angriffstaktiken. Umso wichtiger ist es, dass Unternehmen die neuesten Cyberrends im Auge behalten. Der Arctic Wolf Labs Threat Report liefert tiefe Insights in aktuelle Cyberentwicklungen, die Unternehmen in den kommenden Monaten Orientierung geben.

1. Ukraine-Konflikt: Nur vorübergehende cyberkriminelle Feuerpause

Die geopolitische Lage hat die Bedrohungsaktivität im vergangenen Jahr stark beeinflusst. Als Reaktion auf den Einmarsch Russlands in die Ukraine prognostizierten viele einen Anstieg der Internetkriminalität. Stattdessen konnten wir in diesem Zeitraum einen Rückgang bzw. eine Pause der cyberkriminellen Aktivitäten beobachten. So verzeichneten die Arctic Wolf Labs 26 Prozent weniger Ransomware-Fälle im Vergleich zum Vorjahr.

Dies wird auch durch Berichte europäischer Regierungen bestätigt, die belegen, dass weniger Unternehmen in den vergangenen zwölf Monaten Opfer von Sicherheitsverletzungen wurden. Es ist anzunehmen, dass dieser Rückgang auf einen „Fachkräftemangel“ bei Cyberkriminellen in Russland zurückzuführen ist. So haben viele jüngere

Menschen das Land verlassen, um einer Einberufung zum Kriegsdienst zu entgehen. Dennoch bedeutet diese Entwicklung keine Entwarnung für Unternehmen. Denn trotz des anfänglichen Rückgangs ist mittlerweile wieder ein Anstieg der Ransomware-Angriffe zu beobachten.

So hat sich beispielsweise die russische Ransomware-Gruppe LockBit als dominanter Player etabliert – und dabei weit mehr als doppelt so viele (248 %) erfolgreiche Attacken zu verzeichnen als die zweitaktivste Gruppe BlackCat.

2. Ransomware-as-a-Service

In den vergangenen Jahren hat Ransomware die Schlagzeilen im Bereich Cybersicherheit beherrscht. Immer wieder gab es Nachrichten über Sicherheitsverletzungen bei Unternehmen aller Größen und Branchen. Interessant ist, wie sich Ransomware-Banden inzwischen organisieren: Während Organisationen wie Lockbit in der allgemeinen öffentlichen Wahrnehmung meist noch als lose Banden betrachtet werden, ist die Analogie zu einem professionellen Franchiseunternehmen treffender. Denn diese Ransomware-as-a-Service (RaaS)-Anbieter operieren wie professionelle Unternehmen, verfügen über Abteilungen wie HR, R&D und Buchhaltung und vertreiben Ransomware-Software im großen Stil. Mithilfe dieser Provider können kriminelle Organisationen einfach und ohne spezifisches Cyber-Know How Attacken durchführen und Arbeiten an verschiedene Betreiber auslagern. Das erschwert es Behörden, die Betreiber aufzuspüren und zur Rechenschaft zu ziehen.



Der AUTOR

Ian McShane

ist Vice President of Strategy
bei Arctic Wolf.



3. Repeat Ransomware: Wer einmal Opfer wird...

Strafverfolgungsbehörden und das BSI raten davon ab, Lösegeld zu zahlen, da so die organisierte Cyberkriminalität finanziert wird. Das ist jedoch oft leichter gesagt als getan. Ob Lösegeld gezahlt wird oder nicht, ist letztlich eine geschäftliche Entscheidung, bei der viele Risiko- und Kostenfaktoren berücksichtigt werden müssen. Bevor Lösegeld gezahlt wird, sollten Opfer jedoch alle Möglichkeiten ausschöpfen und sich gegebenenfalls externe Beratung suchen.

Denn eines darf man nicht vergessen: Selbst wenn ein Opfer das Lösegeld bezahlt, gibt es keine Garantie dafür, dass Systeme „unversehrt“ bleiben oder die Bedrohungsakteure keine Kopien der Daten für zukünftige Erpressungen gespeichert haben. Jüngste Untersuchungen haben ergeben, dass vier von fünf Ransomware-Opfern erneut Opfer eines solchen Angriffs werden. Vor diesem Hintergrund sollten Unternehmen dringend in ihre aktive Cyberabwehr investieren und auch über den Abschluss einer Cyberversicherungspolice nachdenken.

Obwohl Unternehmen jeder Größe und jeder Branche von Cyberattacken betroffen sind, haben Untersuchungen des State of Cybersecurity Trends Reports von Arctic Wolf gezeigt, dass kleine und mittelständische Unternehmen (KMU) im aktuellen Wirtschaftsklima besonders stark von Cyberkriminalität betroffen sind.

Mit einer durchschnittlichen Lösegeldforderung von 500.000 US-Dollar – in der Tech-Branche sind es sogar 1,1 Mio. – kann ein Sicherheitsvorfall das Ende für kleine Unternehmen bedeuten. Trotz der verschärften Bedrohungslage bleiben die IT-Sicherheits-Budgets von KMU

in der Regel jedoch gleich oder werden sogar gekürzt. Daher bedarf es kluger Investitionen und auch die Erwägung eines externen Sicherheitspartners.

4. Business E-Mail Compromise auf dem Vormarsch

Weil Strafverfolgungsbehörden mittlerweile hart gegen Ransomware vorgehen, wenden sich Bedrohungsakteure verstärkt einer anderen lukrativen Angriffsmethode zu: Beim Business E-Mail Compromise (BEC) werden Unternehmen durch betrügerische Phishing-E-Mails an Mitarbeitende kompromittiert. Weil es für Unternehmen schwierig ist, diese „Fake-E-Mails“ zu entdecken, wenn sie ihre E-Mail-Server nicht jederzeit überprüfen, entfallen bereits mehr als ein Viertel (29 %) der Incident Response-Fälle auf BEC-Angriffe.

Die gute Nachricht: Obwohl BEC zunimmt, ist der finanzielle Schaden meist geringer als bei Ransomware-Attacken. Ein Schaden beträgt durchschnittlich „nur“ 79.000 US-Dollar. Das ist deutlich weniger als typische Ransomware-Forderungen. Wer sich schützen möchte, sollte vor allem auf Awareness-Maßnahmen für die Belegschaft setzen.

Trotz erheblicher Bemühungen, die Bedeutung einer strengen Cyberhygiene und adäquater Sicherheitspraktiken zu vermitteln, gibt es noch Handlungsbedarf. Angesichts der erwarteten weiteren Zunahme der Komplexität und des Volumens im Bereich der Cyberkriminalität müssen Unternehmen alles in ihrer Macht Stehende tun, um informiert zu bleiben und starke Incident-Response-Pläne erstellen, damit sie wirksam gegen künftige Bedrohungen geschützt sind. •

So verderben Händler Hackern das Geschäft

Ab März 2024 treten neue Schutzprotokolle des Industriestandard PCI 4.0 in Kraft. Kreditkartenindustrie und Händler sind noch nicht ausreichend für die verschärften Sicherheitsanforderungen gewappnet. Wer diese nicht einhält, gefährdet Verbraucher und sich selbst durch Hackerangriffe – und muss mit empfindlichen Strafen rechnen. **VON MICHAEL DEISSNER**

DIE ZAHLEN SPRECHEN EINE KLARE

SPRACHE: Die weltweiten Schäden durch Cyberkriminalität summieren sich im laufenden Jahr auf rund 22 Milliarden US-Dollar – pro Tag! In Deutschland beläuft sich der jährliche Schaden auf über 200 Milliarden Euro. Längst ist Cyberkriminalität ein florierender und durchorganisierter Wirtschaftszweig. Gerade die global vernetzte Finanz- und Kreditkartenindustrie, mit ihren Millionen von angeschlossenen Händlern, ist ein permanentes und lohnendes Ziel von Cyberkriminellen. Doch noch immer ist der Umgang mit hoch sensiblen Kundendaten oftmals lax und lockt Kriminelle an, die Schwachstellen auch bei Händlern gnadenlos ausnutzen.

PCI schiebt weitere Riegel vor

Diese Lücke will das Payment Card Industry Security Standard, ein allgemein anerkanntes Regelwerk der Kreditkartenorganisationen im Zahlungsverkehr, dass die Abwicklung von Kreditkartentransaktionen regelt, durch ein erweitertes Schutzprotokoll schließen. Bereits ab März 2024 treten erste Bestimmungen des neuen Sicherheitsstandards im elektronischen

Zahlungsverkehr PCI DSS V4.0 (PCI 4.0) in Kraft. Wer diese nicht einhält, gefährdet nicht nur Verbraucher und sich, sondern muss auch mit empfindlichen Strafen rechnen. Das kann bis zum Lizenzentzug zur Kreditkartennutzung gehen.

PCI 4.0 betrifft insbesondere die Bereiche Datenerkennung und -klassifizierung. Mit ihnen soll der Umgang mit Kreditkartendaten sicherer werden und mögliche Schäden für Kreditkartennutzer, Einzelhändler und Unternehmen bei Cyberangriffen ausgeschlossen bzw. minimiert werden. Dazu gehören unter anderem die fortlaufende Datenerkennung und -klassifizierung nach Risiko, ein strengeres Berechtigungsmanagement, sowie die Bestandsaufnahme aller Systemen mit Kreditkartendaten.

PCI 4.0 ist sinnvoll

Im Mittelpunkt von PCI 4.0 steht die lückenlose Bestandsaufnahme, an welchen Stellen sensitive persönliche

Kreditkarten-Daten und -Umsätze übertragen, genutzt und temporär sowie dauernd gespeichert werden. Diese Daten gilt es nach der Höhe des möglichen Schadenfalls durch Cyberangriffen zu klassifizieren. Auf dieser Basis muss der Zugang aller zu diesen Daten geregelt, überwacht und ständig angepasst werden.

Die finale Verteidigungslinie: Verschlüsselung der Daten

Entscheidend ist es jederzeit zu wissen, wo die Daten liegen, wer Zugriff darauf hat und im Fall der Fälle diese für Dritte „unbrauchbar“ zu machen. Schutz bietet die datenzentrische Verschlüsselungstechnologie. Dabei werden alle Daten über eine Tokenisierung verschlüsselt, so dass Dritte diese nicht auslesen können, aber diese weiterhin intern, in der Cloud, zur KI-Schulung sowie im Bereich IoT analysiert und genutzt werden können. Sollten im Fall der Fälle doch Datensätze in die Fänge von Hackern geraten, erhalten diese nur Datenschrott ohne jeden wirtschaftlichen Nutzen. Viele internationale Kreditkartenanbieter und Banken und auch Macys aus den USA nutzen diese Technologie bereits. Jetzt geht es darum, dass gerade auch E-Commerce-Unternehmen, die diese Daten zeitweise oder temporär in ihrer IT-Landschaft nutzen und speichern, nachziehen. Denn dann haben Hacker keine Chance mehr aus ihrem „Geschäftsmodell“ Profit zu schlagen. Insofern ist PCI 4.0 ein Weckruf an den Handel, Datensicherheit zu optimieren und Datendiebstahl endgültig einen Riegel vorzuschieben. •



Der AUTOR

Michael Deissner

ist CEO der comforte AG.



HOW ARTIFICIAL INTELLIGENCE WILL REVOLUTIONIZE CYBERSECURITY

Check Point's ThreatCloud AI
protects against the
latest cyber attacks

THREATCLOUD AI

Besuchen Sie Check Point
auf der it-sa 2023 in

Halle 6
Stand 322

Gerne stellen wir Ihnen ein kostenloses Ticket zur Verfügung.
Scannen Sie einfach den folgenden Code und registrieren Sie
sich für ein kostenloses Messticket.



Wir freuen uns auf Sie!

Im Notfall: „Blutwäsche“ für das AD

Der 25 Jahre alte Verzeichnisdienst von Microsoft, das Active Directory (AD), ist in 9 von 10 gemeldeten Ransomware-Angriffen involviert. Finden Sie heraus, wie man das eigene AD vor böswilligen Änderungen schützt und im Fall der Fälle auch per „Blutwäsche“ wieder von Malware befreit. Wie immer: eine gute Vorbereitung hilft bei jeder OP.

VON EVGENIJ SMIRNOV

DIE ZEITEN STARRER GRENZEN IN DER IT SIND VORBEI.

Spätestens seit der Covid-Pandemie kann die Perimeter-Firewall endgültig nicht mehr als die „New Work“-konforme Absicherung der Unternehmensdaten gelten. Neue Konzepte wie Zero Trust lösen das alte Schichtendenken ab. In einem Punkt sind sich die meisten Ansätze einig: Der neue Perimeter in der IT-Sicherheit ist die Identität, wobei hier sowohl die Identität eines Benutzers als auch die eines Endgeräts von Bedeutung ist. Dies haben auch die Angreifer erkannt, so dass in den vergangenen Jahren der Missbrauch von Identitäten in 9 von 10 erfolg-

derne Windows-Versionen inzwischen in der Lage sind, diese zu schließen oder deren Auswirkungen zu begrenzen. Darüber hinaus gibt es Fehlkonfigurationen, die in vielen AD-Umgebungen über alle Größen und Branchen hinweg vorkommen. Die weite Verbreitung sowohl des AD selbst als auch der Angriffstechniken, die seine bekannten Schwächen ausnutzen, führte zu der traurigen Feststellung „Hackers don't break in, they log in“, die in den vergangenen drei Jahren von einigen CSOs geäußert wurde.

Die Aufgaben der Verteidiger

Das „Cybersecurity Framework“ des US-NIST unterteilt den Sicherheits-Lebenszyklus eines IT-Systems in fünf Phasen: IDENTIFY --> PROTECT --> DETECT --> RESPOND --> RECOVER, die meistens als ein geschlossener Kreislauf dargestellt werden. Aus Sicht eines konkreten Cyberangriffs bilden diese Phasen die Zeit „vor“ (IDENTIFY + PROTECT), „während“ (DETECT + RESPOND) und „nach dem Angriff“ (RECOVER) ab. Für Identitätssysteme, die auf Active Directory basieren, kommen dem Verteidiger-Team folgende Aufgaben zu:

- Vor dem Angriff: Die Schwachstellen und offene Flanken des eigenen AD in Detail kennen und diese, sofern möglich, durch geeignete Maßnahmen schließen. Dies können Einstellungen, Richtlinien, Patches oder sogar die Abschaltung besonders anfälliger Systeme sein.
- Während des Angriffs: Zu jeder Zeit über Änderungen im Bilde sein, die im AD vorgenommen werden. Dabei die unerwünschten erkennen und den Schaden begrenzen, indem Änderungen schnell rückgängig gemacht werden, bevor der Angreifer sie für einen weiteren Schritt entlang seiner „Killchain“ einsetzen kann.
- Nach dem Angriff: War der Angreifer erfolgreich und ist es ihm gelungen, das System zu zerstören oder zumindest in Erpressungsabsicht zu verschlüsseln, muss das IT-Team in der Lage sein, die zentralen Identitätssysteme wiederherzustellen. Klassische Backups helfen dabei oft nur wenig, denn sie enthalten meistens „Spuren“ des Angreifers in Form residenter Malware – oder wurden bereits vor der finalen Angriffsphase unbrauchbar gemacht!



Der AUTOR

Evgenij Smirnov

ist Senior Solutions Architect bei Semperis.

reichen Angriffen auf Unternehmens-IT eine wesentliche Rolle spielte.

Abwärtskompatibilität vor Sicherheit

Die IT-Landschaften von Firmen und Organisationen sind vielfältig. Einige sind fest on premises verankert, andere nutzen Dienste aus der Public Cloud zur Authentifizierung und Autorisierung, dies meist in einer hybriden Konstellation. Doch in der großen Mehrheit dieser Infrastrukturen spielt eine 25 Jahre alte Technologie aus dem Hause Microsoft eine zentrale Rolle – der Verzeichnisdienst „Active Directory“ (AD). Dieses eng mit Windows und anderen Produkten verzahnte System besitzt einige bekannte Anfälligkeiten, welche größtenteils dem hohen Alter von AD geschuldet sind.

Da bis vor einigen Jahren Abwärtskompatibilität bei Microsoft noch vor Sicherheit ging, sind viele dieser Schwachstellen im Standardzustand offen, obwohl mo-



Diese Aufgaben fasste Gartner im jüngsten Cybersecurity Report zu einer neuen Disziplin „Identity Threat Detection and Response“ (ITDR) zusammen. AD- und Security-Administratoren müssen sie natürlich nicht manuell bewältigen, denn die Systeme sind so komplex und die zu verfolgenden Ereignisse so umfangreich, dass dies in der Regel gar nicht möglich ist. Verteidiger eines Active Directory sollten sich daher mit Werkzeugen ausrüsten, die ihnen das mechanische Aufbereiten der Konfigurations- und Ereignisdaten abnehmen.

Speziell bei Änderungen im AD sollte sich das Team nicht nur auf Ereignisprotokolle verlassen, denn viele typische Angriffspfade beinhalten das Umgehen der Nachverfolgung (z.B. Mimikatz, DCSshadow) oder deren temporäre Abschaltung (was ebenfalls durch DCSshadow erfolgen kann und in diesem Fall keinerlei Ereignisse ge-

neriert). Die Verfolgung der Änderungen sollte sich an den tatsächlichen AD-Daten orientieren.

Resilienz der Identitätssysteme steigern

Ist das Active Directory „gefallen“, so ist das Team in der Pflicht, die Wiederherstellung nicht nur innerhalb kürzester Zeit durchzuführen, sondern auch einen funktionierenden und schädlingfreien AD-Forest bereitzustellen, der möglichst aktuelle Identitätsdaten enthält. Gerade bei der früher sehr beliebten Mehrdomänen-Topologie ist dies ein komplexer Vorgang, der von Microsoft zwar gut dokumentiert ist, bei manueller Ausführung jedoch Tage bis Wochen dauern kann und unter Umständen zu einem Ergebnis führt, welches die vom Angreifer eingebrachte Malware dennoch beinhaltet. Spezialisierte Werkzeuge helfen auch hier, die Resilienz der Identitätssysteme zu steigern. •

Wann ist der Einsatz von Security SaaS sinnvoll?



Anzeige ///



Interview mit Uwe Dingerkus, Service Owner für SaaS Sicherheit bei GBS Europa GmbH, ein OEM für innovative Lösungen für E-Mail-Sicherheit, Governance und Compliance.

„Zum einen lohnt sich unsere SaaS-Lösung für Unternehmen mit begrenzten Ressourcen, die kaum über ein Budget und spezialisierte Fachkräfte verfügen, um ein eigenes Sicherheitsteam für die Einrichtung, Wartung, Aktualisierung und Verwaltung der Infrastruktur zu haben. Auch für große (bis zu 100.000 Nutzer) und komplexe IT-Systeme rechnet sich unsere SaaS, insbesondere wenn Multi-Mandantenfähigkeit und flexible Anpassung an Policies gefragt sind. Die Kosteneffizienz ist unbestritten. Zum einen durch die Modularität der Funktionen – es werden nur die Leistungen bezahlt, die tatsächlich genutzt werden. Zum anderen durch die Skalierbarkeit je nach E-Mail-Auslastung.

Heute ist auch die Komplexität ein Wendepunkt. Viele Unternehmen kommen mit dem dynamischen Zusammenspiel von komplexen Technologien und immer strengeren Datenschutzvorschriften nicht mehr zurecht. Vor allem, wenn sie zu einer stark regulierten Branche gehören, wo

Sicherheit und Compliance Priorität haben. Ich nenne iQ Suite SaaS gerne eine „Press and walk away“-Lösung, denn man drückt einen Knopf und sie läuft eigenständig. Damit erhält der Kunde ohne zusätzlichen Aufwand eine umfassende und erhöhte Sicherheit.

Denn im GBS-Team sitzen Spezialisten mit diversifiziertem Sicherheits-Know-how und technologischer Erfahrung, die rund um die Uhr Monitoring und Incident Response leisten. Inhouse wäre so ein Leistungspaket absolut unwirtschaftlich.“

GBS Europa GmbH

76227 Karlsruhe,
Zur Giesserei 19-27 B
+49 721 4901-0
info@gbs.com
<https://gbs.com/>



Raus aus der Shadow-IT-Falle

Um ihre Produktivität zu steigern, installieren Mitarbeitende häufig Softwarelösungen, ohne ihre IT-Verantwortlichen darüber zu informieren. Nicht selten öffnen sie dabei die Tür für Hacker, und sensible Daten werden gestohlen oder gehen verloren. Wo liegen die Herausforderungen und wie können sich Unternehmen davor schützen?

VON FRANZ SALZMANN

LAUT EINER STUDIE VON MCAFEE aus dem Jahr 2020 stieg die Cloud-Nutzung in Unternehmen während der Pandemie durch den Boom des Remote-Workings um 50 Prozent an – und damit auch die Gefahr von Datenschutzverletzungen durch Shadow-IT.

Da viele Beschäftigte im Home-Office auf ihre eigenen Endgeräte angewiesen waren, fehlte ihnen zum Teil wichtige Infrastruktur. Für die Koordination von Aufgaben installierten sie zum Beispiel Asana oder Trello und für das GIF in der Mittagspause eröffneten sie Whatsapp-Gruppen. Dateien teilten Teammitglieder über Cloud-Services wie Dropbox oder Wettransfer. Gerade zu Beginn der Pandemie war der große Vorteil dieser Tools ihre schnelle Einsatzbereitschaft und die intuitive Bedienbarkeit. Aber auch unabhängig von der Pandemie nutzen Mitarbeiter Shadow-IT, um ihre Produktivität zu steigern oder um (Kunden-) Anforderungen besser zu erfüllen. Gut die Hälfte der von McAfee befragten IT-Experten schätzt, dass die Mehrheit ihrer Kollegen Software installiert hat, von der sie nichts wissen.

Die fünf größten Shadow-IT-Probleme

Shadow-IT kann die Effizienz von Teams steigern. Schnell ein PDF komprimieren, mal eben das private Smartphone nutzen oder ein Umfragetool für eine Abstimmung herunterladen – fast jeder nutzt diese kleinen Helfer. Und sie sind nicht per se schlecht. Vielmehr müssen sich Unternehmen der Risiken bewusst sein und Mechanismen entwickeln, wie sie intern damit umgehen. Fünf Risiken sind dabei besonders hervorzuheben:

1. Kontrollverlust

Das offensichtlichste Risiko der Shadow-IT ist der Kontrollverlust der IT- und Compliance-Abteilungen. Sicherheits-Screenings können nicht durchgeführt und Compliance-Standards nicht eingehalten werden. Po-

tenzielle Sicherheitslücken und Gefährdungen werden erst spät erkannt.

2. Datenverlust und Angriffsmöglichkeiten

Zum Teil werden Gefährdungen erst entdeckt, wenn die Hacker bereits im System sind. In diesem Falle kann nur noch ein Incident-Response-Team versuchen, Datenlecks so schnell wie möglich zu stopfen und saubere Backups einzuspielen. Oft ist das mit hohen Kosten verbunden. Daten können aber auch ohne Hacker verloren gehen: Verliert ein Mitarbeiter die Zugangsdaten zu einem Shadow-IT-Programm oder wird das Programm von einer neuen firmeninternen IT-Lösung nicht mehr unterstützt, sind die dort gespeicherten Daten verloren, ohne dass die IT-Abteilung sie wiederherstellen kann.

3. Datenschutzverletzungen

Im 25. Datenschutzbericht der Landesbeauftragten für Datenschutz und Informationsfreiheit Nordrhein-Westfalen Helga Block heißt es: „Wir haben dem Arbeitgeber empfohlen, von einer Kommunikation über WhatsApp für dienstliche Zwecke generell abzusehen. Mit der Nutzung von WhatsApp sind nämlich erhebliche Risiken im Hinblick auf Zugriffe durch Unbefugte verbunden, zum Beispiel Facebook.“ Konkret ging es um die Übermittlung von Krankmeldungen über WhatsApp. Weiter heißt es: „Facebook kann auf die Verkehrsdaten (Wer kommuniziert wann mit wem?) und auf die Bestandsdaten (Wer ist für den Dienst angemeldet?) der Nachrichten zugreifen. Zudem liest die App das Adressbuch auf dem Gerät des Nutzers aus und gleicht die Daten mit den bei WhatsApp gespeicherten Daten ab, unabhängig davon, ob die Nutzer, auf die sich die Daten beziehen, davon wissen oder dies wollen.“ Dieser Fall zeigt sehr deutlich, wie schnell beispielsweise Kundendaten wie Name oder Telefonnummer an Dritte weitergegeben werden, ohne dass ein vorheriges Einverständnis eingeholt wurde.

Shadow-IT kann ein Risiko im gesamten Unternehmen sein, aber insbesondere im Finanzmanagement ist die Nutzung von ungenehmigter IT **gefährlich**.



4. Kostenfalle

Zum Teil nutzen mehrere Teams die gleichen Shadow-IT-Anwendungen und zahlen dafür mehrfach, zum Beispiel für ein monatliches Abonnement. Sinnvoller ist hier ein unternehmensweites Abo, das häufig sogar noch mehr Leistungen umfasst.

5. Ineffizienz

Eine unübersichtliche IT-Struktur führt daher unweigerlich zu Ineffizienzen. Mitarbeiter erledigen Aufgaben doppelt oder wissen nichts von den IT-Lösungen anderer und beginnen eigene Recherchen.

Shadow-IT – besonders gefährlich im Finanzmanagement

Shadow-IT kann ein Risiko im gesamten Unternehmen sein, aber insbesondere im Finanzmanagement ist die Nutzung von ungenehmigter IT gefährlich. Für das Finanzmanagement gelten strenge Vorschriften, da sensible Daten verarbeitet werden, die in den Händen Unbefugter einen hohen Schaden anrichten können. Eine schnelle WhatsApp mit den Lohndaten der Mitarbeiter an den Steuerberater oder ein Datenpaket via Cloud an den Kollegen im Home Office bergen ein hohes Risikopotenzial. IT-Verantwortliche sollten daher ein besonderes Augenmerk auf die Bedürfnisse der Mitarbeiter in der Finanzabteilung legen. Im Idealfall erfüllen die autorisierten IT-Lösungen die Bedürfnisse der Kollegen, sodass diese nicht auf Shadow-IT zurückgreifen müssen. Wenn nicht – wie es oftmals der Fall ist – müssen Präventionsmaßnahmen erfolgen.

Präventionsmaßnahmen

1. Bewusstseinsbildung und Schulung der Mitarbeiter

Häufig sind sich die Mitarbeiter der Risiken der von ihnen eingesetzten IT-Lösungen gar nicht bewusst. Eine kurze

Aufklärung und Sensibilisierung, die idealerweise bereits Teil des Onboardings ist, kann bereits sehr effizient sein.

2. Transparente Richtlinien, regelmäßige Audits

Unternehmen können Shadow-IT-Policies aufstellen, die den Umgang mit Soft- und Hardware klar regeln. Einmal aufgesetzt, sollten IT-Verantwortliche regelmäßige Audits durchführen, um sicherzustellen, dass die Richtlinien auch tatsächlich umgesetzt werden.

3. Zentrale IT-Abteilung

Vor allem in kleinen Unternehmen ist es nicht immer möglich, eine eigene IT-Abteilung aufzubauen. Dennoch sollte es eindeutige Verantwortlichkeiten geben, die die Einhaltung von IT-Standards regelmäßig prüfen. Selbst gebaute Data Lakes oder Data Warehouses sollten extern auf ihre Sicherheit geprüft werden.

4. Tools einsetzen, die die Bedürfnisse der Nutzer erfüllen

Wenn Mitarbeiter beispielsweise Reportings stets als PDF im Corporate Design des Kunden erstellen müssen, ihr Tool aber nur nicht-individualisierbare Word-Dateien erstellt, ist der Griff zu Shadow-IT schnell geschehen. Daher ist neben allen oben genannten Maßnahmen das Feedback der Mitarbeiter am wichtigsten. Kennt ein Unternehmen ihre IT-Bedürfnisse, greifen diese nicht zu unautorisierten Lösungen. •

Der AUTOR

Franz Salzmann

ist Gründer und CEO von Helu.io, einem Anbieter für einfaches und kollaboratives Finanzmanagement für Scale-ups und mittelständische Unternehmen.



Sind Ihre Salesforce- und AWS-Daten wirklich sicher?

Immer mehr Unternehmen setzen auf SaaS-Applikationen wie Salesforce oder AWS und vertrauen darauf, dass ihre Daten hier sicher sind. Insbesondere, wenn zusätzliche Security-Lösungen wie Okta eingesetzt werden. Doch wie einfach ist es für Cyberkriminelle, an sensitive Informationen zu gelangen?

Von Sebastian Mehle

UM EINEN ERFOLGREICHEN ANGRIFF DURCHZUFÜHREN, reichen oftmals schon einfache Sicherheitstools, API-Aufrufe und Skripte. Die benötigten Ressourcen sind frei zugänglich und werden in zahlreichen YouTube-Tutorials erklärt. Das klingt nicht nur besorgniserregend, sondern ist es auch.

Okta-Super-Admins als Generalschlüssel

Wie könnte ein solcher Angriff aussehen? Hierzu sind nicht unbedingt komplizierten Techniken wie spezielle Phishing-Kampagnen oder der Einsatz von Malware nö-

Um einer Entdeckung zu umgehen und einen dauerhaften Zugang sicherzustellen, wird in einem nächsten Schritt ein neuer User erstellt, unter dessen „Namen“ die weiteren Aktionen durchgeführt werden. Mithilfe von Skripten wird der neue Account nicht nur erstellt, sondern ihm auch Super-Admin-Rechte zugewiesen. Dieser Schritt ist entscheidend, da Okta als Tor zu den verbundenen Applikationen dient. Entsprechend melden sich die Angreifer nun bei Okta mit dieser Backdoor-Identität an und weisen ihr einige Anwendungen zu. Dabei verwenden sie allerdings einen Kniff: Sie weisen ihr ein anderes, legitimes Konto zu,



Der AUTOR

Sebastian Mehle

ist Account Manager von Varonis Systems.

tig. Stattdessen suchen Cyberkriminelle nach Informationen, die Unternehmen öffentlich preisgeben. In der Aufklärungsphase werden entsprechend mit einem einfachen Skript öffentlich zugängliche GitHub-Repositories nach Secrets wie API-Schlüsseln oder Zugangsdaten gescannt. Und diese finden sich öfter als man denkt. Sogar GitHub selbst musste im März dieses Jahres einräumen, dass private SSH-Keys versehentlich im eigenen Repository veröffentlicht wurden. Auf diese Weise lassen sich beispielsweise Service-Tokens finden. Diese sind direkt einem Konto zugeordnet und ermöglichen es, Aktionen durchzuführen, ohne dass bei jeder Anfrage Anmeldedaten angegeben werden müssen. Aus diesem Grund sind sie ideal für Angriffe.

Das gilt umso mehr für Okta- und/oder Super-Admin-Tokens. Finden Angreifer einen solchen, können sie mithilfe des Programms „Postman“ API-Anfragen starten und dabei Details des Kontos abrufen, das mit diesem Token verknüpft ist.

wodurch die Angreifer Berechtigungen für Box, G Suite, AWS, GitHub, Salesforce usw. erhalten. Der Angreifer gibt sich also als den Mitarbeiter aus und erhält somit dessen Zugriff auf die Anwendungen und Ressourcen.

Zugriff auf alle verbundenen Apps

Die Grundlagen sind gelegt. Jetzt geht es an das eigentliche Ziel: die Daten. Die Angreifer könnten beispielsweise mit Box beginnen, das wie OneDrive oder G Suite das Teilen von Daten sehr einfach und unkompliziert macht. Leider auch für Angreifer, die Zugang haben: Es bedarf nur eines Klicks, um die Daten zu exfiltrieren.

Bei Salesforce gestaltet sich der Datendiebstahl in aller Regel nicht ganz so einfach. Viele Salesforce-Teams leisten gute Arbeit, wenn es darum geht, den Zugriff auf Konten effektiv zu reduzieren und sie zu schützen. Jedoch wird oftmals der Schutz der Einstellungen übersehen. Die Kombination von Einstellungen, die steuern, welche



Änderungen an Benutzerkonten vorgenommen werden können, hängt von Profil- und Systemeinstellungen, Berechtigungssätzen, Freigaberegeln und anderen Variablen ab. Bei diesem sehr komplizierten Prozess kommt es entsprechend häufig zu Fehlkonfigurationen, die von Angreifern ausgenutzt werden können. Wenn beispielsweise das Kästchen „Profile und Berechtigungssätze verwalten“ aktiviert ist, können Änderungen vorgenommen werden, die einen Kaskadeneffekt haben, der den Angreifern alle Daten in Salesforce öffnet. Mit dieser einen Änderung können sie nun alle Informationen in Salesforce lesen und exfiltrieren, die mit diesen Konten verbunden sind.

Angreifer können Schlüsselrichtlinien ändern

Ein weiteres lohnendes Ziel stellen S3-Buckets dar. Um nun einen S3-Bucket öffentlich zu machen, rufen die Angreifer die S3-Konfiguration auf, suchen einen vielversprechenden Bucket und lassen mit ein paar schnellen Klicks den Lesezugriff zu. Dann wird die URL aus dem entsprechenden Ordner kopiert, wodurch Cyberkriminelle über einen Webbrowser auf die sensitiven Daten zugreifen

Eine neue Sicherheitsstrategie ist nötig

Der aufgezeigte Angriff ist sicherlich recht spezifisch. In jeder Umgebung gibt es unterschiedliche Voraussetzungen, die die Durchführung dieser Angriffsstrategien erschweren oder erleichtern können. Der springende Punkt ist jedoch, dass viele Daten in Cloud-Plattformen gespeichert sind, die sich alle über APIs verbinden. Es wurde deutlich, dass eine kleine Unachtsamkeit oder eine kleine Fehlkonfiguration einen Schneeballeffekt auslösen kann, der sich zu einem enormen Datenvorfall entwickelt. Sicherheitsverantwortliche müssen die Art und Weise, wie sie über laterale Bewegungen denken, überdenken. In einer herkömmlichen On-Premises-Umgebung verstehen wir unter lateraler Bewegung den Übergang von Rechner zu Rechner. In der Cloud hingegen bewegen wir uns von Anwendung zu Anwendung – und das geschieht oft über APIs, die gesichert werden müssen.

Sicherheitsteams müssen deshalb in der Lage sein, Änderungen zu erkennen und schnell darauf zu reagieren. Hierfür benötigen sie Transparenz bei der Authentifizie-

Die Angreifer könnten beispielsweise mit Box beginnen, das wie OneDrive oder G Suite das Teilen von Daten sehr einfach und unkompliziert macht. Leider auch für Angreifer, die Zugang haben: Es bedarf nur eines Klicks, um die Daten zu exfiltrieren.

können – von jedem Computer auf der ganzen Welt. Darüber hinaus sind in AWS-Datenbanken Unmengen von Daten gespeichert. Über den Relational Database Service (RDS) wählen die Angreifer eine interessante Datenbank aus, machen einen Snapshot davon und lagern den Inhalt in einen S3-Bucket aus.

Hier werden die Regeln für diesen neuen S3-Bucket so eingestellt, dass er öffentlich zugänglich ist und eine Exportregel hat. Zudem können die Angreifer die Schlüsselrichtlinie so ändern, dass sie Zugriff auf die Daten haben, und den Verschlüsselungsschlüssel entfernen. Auf diese Weise wird alles in Klartext exportiert.

rung, bei Änderungen der Schlüsselkonfiguration und bei verdächtigen Zugriffen. All dies muss plattform- bzw. applikationsübergreifend umgesetzt werden. Es reicht nicht aus, zu wissen, was ein Nutzer auf einer bestimmten Plattform macht. Entscheidend ist zu erkennen, wie er sich in der gesamten Umgebung verhält. Die entsprechenden Metadaten müssen in einen Kontext gebracht und korreliert werden, um Auffälligkeiten zu identifizieren und automatisch Gegenmaßnahmen einzuleiten. Nur wenn man die Daten ins Zentrum der Sicherheitsstrategie stellt, ist man in der Lage, Angriffe effektiv zu stoppen, ganz gleich über welchen Weg sie erfolgen. •

Kriminelle Spiele ohne Grenzen

Ein Report deckt Forschungswettbewerbe auf kriminellen Online-Foren für Innovationen und die Überwindung von Sicherheitshürden auf. Die Wettbewerbe konzentrieren sich auf neue Angriffs- und Ausweichmethoden und spiegeln Trends im Bereich Cyberkriminalität wider, von Command-and-Control-Infrastrukturen. **VON MICHAEL VEIT**

CYBERKRIMINELLE SIND STETS BE-MÜHT, neue Angriffs- und Ausweichmethoden zur Überwindung von Sicherheitshürden zu entwickeln. Eine neue Variante zur Erreichung dieses Ziels ist nun in kriminellen Online-Foren zu beobachten: Mithilfe von Hacker-Wettbewerben sollen neue Angriffsinnovationen vorangetrieben werden. Die Wettbewerbe ähneln dem „Call for Papers“ legitimer Sicherheitskonferenzen und bieten den Gewinnern erhebliche finanzielle Belohnungen, Anerkennung von Kollegen und Kolleginnen sowie potenzielle Arbeitsmöglichkeiten. Die Tatsache, dass Cyberkriminelle diese Wettbewerbe veranstalten, daran teilnehmen und sie sogar sponsern, legt nahe, dass es ein gemeinschaftliches Ziel gibt, ihre Taktiken und Techniken weiterzuentwickeln. Es gibt sogar Hinweise darauf, dass diese Wettbewerbe als Rekrutierungsinstrument bei prominenten Cyberkriminellen-Gruppen dienen.

Wettbewerbs-Einreichungen können sofort eingesetzt werden

Dass auf kriminellen Foren Wettbewerbe ausgerichtet werden, ist nichts

Neues, die Praxis existiert schon seit Jahren. Interessant ist jedoch, wie sie sich im Laufe der Zeit weiterentwickelt haben. Frühe Aktionen umfassten Quizfragen, Grafikdesign-Wettbewerbe und Ratespiele. Jetzt laden kriminelle Foren dazu ein, Artikel zu technischen Themen einzureichen, inklusive Quellcode, Videos und/oder Screenshots. Die gesammelten Werke werden anschließend von den Forennutzern bewertet und so der Sieger ermittelt. Die Bewertung ist jedoch nicht völlig transparent, da die Forenbesitzer und Wettbewerbs-sponsoren scheinbar spezielle Stimmrechte haben.

Viele der siegreichen Einreichungen im Rahmen der Contests haben eine breitere Anwendung. Sie zeichneten sich dadurch aus, dass sie quasi umgehend einsetzbar sein würden und zudem oftmals nicht besonders innovativ waren. Dies könnte entwe-

der die Prioritäten der Gemeinschaft offenlegen, oder auch Beleg dafür sein, dass Angreifer ihre besten Forschungsergebnisse für sich behalten wollen, um sich nicht in die Karten schauen zu lassen und ihre neuen Taktiken dann in realen Angriffen profitabel einzusetzen.

Preissummen im hohen 5-stelligen Bereich

Prominente, jährliche Wettbewerbe sind zum einen eine Veranstaltungsreihe auf dem russischsprachigen Cyberkriminalitätsforum Exploit mit einer Preissumme von 80.000 US-Dollar aus dem Jahr 2021, sowie einer weiteren Serie im sogenannten XSS-Forum mit einem Preisgeld von 40.000 Dollar. Seit mehreren Jahren haben prominente Mitglieder der Cyberkriminalitätsgemeinschaft diese Veranstaltungen gesponsert, darunter All World Cards und Lockbit.

In den jüngsten Wettbewerben konzentrierte Exploit seine Ausschreibungen auf Kryptowährungen, während XSS sich auf verschiedene Themen von sozialer Manipulation und Angriffsvektoren bis hin zu Ausweichmethoden und Betrugsangeboten konzentriert hat. Viele der Gewinnerbeiträge konzentrierten sich darauf, legitime Tools wie Cobalt Strike zu missbrauchen.

Ein Zweitplatzierteilte ein Tutorial zur Ausrichtung von Initial Coin Offerings (ICOs), um Mittel für eine neue Kryptowährung zu sammeln, und ein weiteres zur Manipulation von Privilegien, um den Windows Defender zu deaktivieren. •



Der AUTOR
Michael Veit
ist Security-Experte bei Sophos.



ECCLESIA CYBER

unterstützt Unternehmen und Versicherer

Cybercrime gehört mittlerweile zu einem der größten Risikofaktoren für Unternehmen weltweit. Eine Cyberversicherung ist daher essenziell – doch nicht immer leicht zu bekommen. Um Unternehmen noch professioneller unterstützen zu können, wurde jetzt die neue Einheit Ecclesia Cyber gegründet. Welche Vorteile sich Unternehmen und Versicherer dadurch bieten, erläutert **Robert Drexler, Leiter von Ecclesia Cyber**, im Interview.

Welche Strategie steckt hinter der Gründung von Ecclesia Cyber?

Das Thema Cybersecurity ist sehr komplex. Deshalb haben wir unter der Dachmarke Ecclesia Cyber unser langjähriges Know-how in puncto Beratung, Risikoevaluierung, Vertragsbetreuung und Schadenbearbeitung zusammengeführt, um unseren Kunden die jeweils beste Lösung anbieten zu können. Dazu trägt auch unser breit aufgestelltes und von Versicherern unabhängiges Partnernetzwerk bei, das beispielsweise aus IT-Forensikern, IT-Security-Unternehmen, Rechtsanwaltskanzleien, Krisenmanagern und weiteren Experten besteht.

Versicherungsschutz ist im Markt nicht so einfach zu bekommen. Warum ist das so und wie können Sie Unternehmen dabei unterstützen?

Bei Cyberversicherungen erleben wir seit einigen Jahren eine ausgeprägte Hartmarktphase. Das heißt, die Kapazitäten sind knapp, die Preise steigen kontinuierlich und die Anforderungen der Risikoträger an Unternehmen steigen exponentiell. Auch wenn sich die Risiken im Kern gleichen – in der Cyberbetrachtung stellen beispielsweise Krankenhäuser ein wesentlich höheres Risiko dar als ein Maschinenbauer. Damit tun sich viele Versicherer sehr schwer. Diese Negativselektion können wir durch die Konsolidierung unserer Geschäftsfelder künftig vermeiden. Hinzu kommt, dass wir die Marktanforderungen genau kennen und unsere Kunden gezielt beraten können, um Maßnahmen so zu priorisieren, dass das Risiko besser versicherbar wird.

Was kann Ecclesia Cyber, was der Wettbewerb nicht kann?

Wir bieten unseren Kunden im Cybersegment ein ganzheitliches IT-Sicherheitsmanagement und dauerhafte Versicherbarkeit ihrer IT-Risiken. Als Versicherungsmakler stehen wir ja stets auf Kundenseite. Und wenn wir Lösungen komplett abdecken können, ist unser Kunde nicht auf einzelne Versicherer oder Dienstleister angewiesen. So können wir die Rahmenbedingungen im Sinne unserer Kunden vorgeben, was ganz klar auch unsere Strategie und Zielsetzung ist. Dass wir zahlreiche versichererunabhängige Lösungen wie Bedingungswerke, Risikoberatung

oder Incident Response-Lösungen inhouse anbieten, ist schon heute unser USP.

Welche Vorteile haben die Versicherer dadurch?

Nicht nur die Unternehmen haben Vorteile, sondern auch die Versicherer, da wir Anforderungen auch mittels Auditierungen so klar darstellen, dass sie deutlich weiterentwickelte und saubere Risiken in ihre Bücher nehmen können. Denn mit unserem gemanagten Portfolio bilden wir in Teilen das Underwriting-Know-how des Versicherers bei uns ab. Das spiegelt sich bei einigen Produktgruppen auch ganz klar in den niedrigen Schadenzahlen wider. Da unsere Versicherer wissen, dass sie es bei Ecclesia mit Profis zu tun haben, bringen sie uns dieses Vertrauen auch entgegen.



Robert Drexler
Leiter von Ecclesia Cyber.

**CYBERRISIKEN
ABSICHERN**

– mit Deutschlands führendem Versicherungsmakler.

**ECCLESIA
CYBER**

- Maßgeschneiderte Versicherungskonzepte
- Risikomanagement
- 24/7-Notfall-Service
- Unterstützung im Ausbau der Cyber-Sicherheit
- Internationales Expertennetzwerk

Mehr Informationen finden Sie auf www.ecclesia-cyber.de

Ecclesia – Deutschlands führender Versicherungsmakler für Unternehmen und Institutionen

Datenschutz ist Katastrophenschutz

Werden kritische Infrastrukturen von Hackern angegriffen, kann das dramatische Folgen haben. Doch während Rechenzentren oft Hochsicherheitstresoren gleichen, lassen sich Schaltbefehle etwa von Bahnunternehmen, Energieversorgern oder Wasserwerken leicht manipulieren. Nur hochsichere Verschlüsselungstechnologien schützen vor Angriffen. **VON SASCHA KEGREISS**

DIE SATELLITENGESTÜTZTE KOMMUNIKATION von Windrädern in ganz Deutschland wurde im Februar 2022 durch einen Hackerangriff für mehrere Wochen unterbrochen. Die Störung hatte zwar keinen direkten Einfluss auf die Stromproduktion, aber im Falle eines gravierenden Problems hätte dieses nicht aus der Ferne behoben werden können. Nur Monate später hatten Unbekannte Glasfaserkabel der Deutschen Bahn durchtrennt. Der Zugverkehr im Norden und Westen Deutschlands kam zum Erliegen.

Diese Vorfälle machen deutlich, wie verheerend die Auswirkungen sind, wenn kritische Infrastrukturen (KRITIS) sabotiert werden. Und diese Angriffe gelangen, weil die betroffene Infrastruktur unzureichend geschützt war. Genauso wie die Daten, die die Befehle für Weichen oder Signalanlagen übertragen.

Unverschlüsselte Daten als Gefahrenquelle

KRITIS-Unternehmen sind gesetzlich dazu verpflichtet, angemessene organisatorische und technische Vorkehrungen zum Schutz ihrer IT-Systeme zu treffen. Wenn aber zwischen ver-

schiedenen Standorten oder Rechenzentren hochsensible Informationen übertragen werden, sind diese Daten häufig nicht oder nur unzureichend vor Manipulationen geschützt. Oftmals ist die vorhandene Netzwerkinfrastruktur oder die Systeme veraltet und daher angreifbar. In so einem Fall haben Hacker ein leichtes Spiel: Sie können Informationen mitlesen, eigene einspeisen oder die Datenübertragung stören. Im Schienennetz, bei Schaltbefehlen zum Beispiel, kann dies zu Bahnunfällen führen. Verhindern lässt sich eine solche Manipulation nur, indem man Daten verschlüsselt. Wenn nur Sender und Empfänger Zugriff auf den Inhalt einer Nachricht haben. Und wenn Letzter sicher sein kann, dass die erhaltenen Kommandos vom Sender stammen.

Netzwerkverschlüsseler ist ein Muss

Wer die Integrität und Vertraulichkeit seiner Informationen schützen

will, wenn diese das Firmengelände verlassen, benötigt einen Netzwerkverschlüsseler. Dieser bewahrt vor Spionage und Trickerei bei der Übertragung. Aber worauf sollen Unternehmen dabei achten?

Ein wesentliches Leistungsmerkmal ist die Latenz (also die Zeitspanne, die die Informationen im Gerät verbleiben müssen, um ver- oder entschlüsselt zu werden). Zum Beispiel: Verschlüsselungsgeräte, die auf Daten im OSI Layer 2 arbeiten – sie werden L2 genannt –, bieten eine minimale Latenz im μ s-Bereich.

Entscheidend für die Wahl des richtigen Netzwerkverschlüsselers ist ebenfalls, dass dieser selbst vertrauenswürdig ist. Denn manipulierte Apparate stellen eine steigende Bedrohung bei der Herstellung von Hardwarekomponenten dar. Aus diesem Grund sind nur diejenigen empfehlenswert, die vollständig in Deutschland hergestellt wurden.

Weitere wichtige Leistungsmerkmale sind Robustheit der Geräte (bezogen auf unterschiedliche Industriestandards), sowie kundenspezifischer Anpassbarkeit. Die Wahl des richtigen Verschlüsselers kann sich schwierig gestalten. Denn neben den genannten Auswahlkriterien ist insbesondere im Umgang mit kritischen Daten auf die Nutzung behördlich geprüfter Produkte zu achten. Mit Netzwerkverschlüsselern, die vom BSI zugelassen wurden, sind Unternehmen bestens ausgestattet und für Angriffe gerüstet. Nur so gelingt eine effiziente Absicherung der kritischen Infrastruktur und ohne Performanceverlust. •



Der AUTOR Sascha Kegreiß

ist Director Product Management & Business Development
Rohde & Schwarz.





xSuite Group GmbH
Hamburger Str. 12
22926 Ahrensburg
+49 4102 88380
info@xsuite.com
www.xsuite.com

xSuite Group entwickelt und vermarktet Anwendungen zur Automatisierung dokumentenbasierter Geschäftsprozesse. Wir sind Experte für das Kernthema „Eingangsberechnungsverarbeitung in SAP“ und bieten dazu alle Softwarekomponenten. Über 200.000 Anwender verarbeiten mit xSuite bereits über 60 Mio. Rechnungen pro Jahr. Ergänzt wird unser Portfolio mit einem durchgängigen P2P-Prozess (Beschaffen und Bezahlen). Die Lösungen werden in der Cloud, hybrid oder on-premises angeboten und sind zertifiziert.



Softeq Development GmbH
Bretonischer Ring 12
85630 Grasbrunn
+49 89 800 32780
www.softeq.com

Softeq wurde 1997 in Houston gegründet und hat ein EU-Office in München. Es bietet innovative Full-Stack-Komplettlösungen und unterstützt Unternehmen bei der digitalen Transformation. Das Leistungsspektrum umfasst maßgeschneiderte Softwareentwicklung, Embedded Software Development und Hardware Design, Cloud-Anwendungen, Entwicklung (Frontend- & Backend), UX / UI-Design, DevOps Teams, Wartung und Support, Qualitätssicherung und Schutz vor Cyberangriffen.



Dell GmbH
Unterschweinstiege 10
60549 Frankfurt am Main
www.delltechnologies.com

Dell Technologies unterstützt Organisationen und Personen dabei, ihre Zukunft digital zu gestalten und Arbeitsplätze sowie private Lebensbereiche zu transformieren. Das Unternehmen bietet Kunden das branchenweit umfangreichste und innovativste Technologie- und Services-Portfolio für das Datenzeitalter mit dem Ziel, den menschlichen Fortschritt voranzutreiben – darunter Laptops, Desktops, Server, Netzwerke, Speichersysteme, Hybrid-Cloud-Lösungen und vieles mehr.



Kendox AG
Bahnhof-Strasse 7
CH-9463 Oberriet SG
T +41 (71) 552 34 00
info@kendox.com
www.kendox.com

Kendox ist Experte für digitales Dokumentenmanagement und die Automatisierung von Prozessen in Büro und Verwaltung. Die Dokumenten- und Prozessautomatisierungslösungen der Kendox sind mit Microsoft 365, mit führenden ERP-Lösungen sowie mit vielen weiteren Fachanwendungen integriert. Für den Betrieb in der Cloud werden die Anwendungen von Kendox in eigenen, virtuellen Rechenzentren in Deutschland und der Schweiz bereitgestellt und betrieben. Dabei basieren die Softwarelösungen auf zukunftssicheren Technologien und erfüllen die Anforderungen an Sicherheit und Datenschutz.



Esker Software Entwicklungs- und Vertriebs-GmbH
Dornacher Straße 3a
85622 Feldkirchen
info@esker.de
www.esker.de

Esker ist eine Cloud-Plattform, die einen strategischen Mehrwert für Finanz- und Kundendienstabteilungen schafft und die Zusammenarbeit zwischen Unternehmen durch Automatisierung des Cash-Conversion-Cycles stärkt. Unsere Mission ist die Schaffung einer Grundlage für positives Wachstum: Höhere Produktivität, verbesserte Mitarbeitermotivation und größeres Vertrauen zwischen Unternehmen. Mit der Entwicklung von KI-gesteuerten Technologien und der Automatisierung von Order-to-Cash- und Procure-to-Pay-Cycles, befreit Esker Finanz- und Kundendienstabteilungen von zeitaufwendigen Aufgaben.



Sinequa
Walter-Kolb-Straße 9-11
60594 Frankfurt/Main
+49 69 962 176 608
info@sinequa.com
www.sinequa.com

Sinequa ist ein unabhängiger Softwareanbieter, der großen und komplexe Organisationen eine intelligente Unternehmenssuch- und Analyseplattform bereitstellt. Die Beschäftigten der Sinequa-Kunden erhalten dadurch verwertbare Informationen in ihrem jeweiligen Arbeitsumfeld, gewinnen neue Einblicke, treffen bessere Entscheidungen und steigern ihre Produktivität – das Unternehmen wird informationsgetrieben. Sinequa entwickelt seine Expertise und sein Geschäft weltweit mit einem breiten Netzwerk von Technologie- und Geschäftspartnern.



d.velop AG
Schildarpstraße 6-8
48712 Gescher
+49 2542 9307-0
info@d-velop.de
www.d-velop.de

Die d.velop-Gruppe entwickelt und vermarktet Standard-Software zur durchgängigen Digitalisierung von dokumentenbezogenen Geschäftsprozessen und bietet diese zur SaaS-, On-Premises- und Hybrid-Nutzung an. Das Produktportfolio reicht vom Compliance-fähigen Dokumenten-Repository bzw. Archiv und digitalen Akten über die interne Kollaboration bis zur externen Zusammenarbeit über Organisationsgrenzen hinaus. Produkte von d.velop sind aktuell bei mehr als 13.350 Geschäftskunden mit über 3,25 Millionen Anwender:innen im täglichen Einsatz.

MARKETPLACE

05

Nachhaltigkeit messbar machen

Ab 2024 müssen Unternehmen mehr Energie einsparen und das durch regelmäßige Audits dokumentieren. Zwar erfasst die Mehrheit schon Nachhaltigkeitsdaten. Doch beim Sammeln, Aufbereiten und Auswerten der Informationen hapert es, laut einer Studie von Lufthansa Industry Solutions.

VON MORITZ RÖDER

WENN IM JANUAR DAS ENERGIEEFFIZIENZGESETZ (EnEg) der Bundesregierung wie geplant in Kraft tritt, ist es für Konzerne und Mittelständler keine Frage mehr, ob sie Energie sparen wollen. Sie sind dazu verpflichtet. Damit die Energiewende gelingt, soll der Verbrauch bis 2030 zunächst um 26,5 Prozent gegenüber 2008 sinken. Das bedeutet für Unternehmen, dass sie Energiemanagementsysteme betreiben und Energieaudits durchzu-

führen müssen, um nachhaltiger zu wirtschaften.

Energieeffizienz als ökologischer und ökonomischer Hebel

Der aktuelle „Reifegradindex IT & Sustainability 2023“ von Lufthansa Industry Solutions (LHIND) zeigt, dass gesetzliche Vorgaben zwar der größte Treiber für Investitionen in Nach-

- der Hälfte fehlt die geeignete Datenbasis;
- zwei von drei Unternehmen sorgen sich um die Datensouveränität;
- für mehr als zwei Drittel (68%) ist zudem die Zusammenführung heterogener Daten ein Problem; so die Ergebnisse der Studie.

Das Energieeffizienzgesetz ist hier keine weitere administrative Belastung, sondern eine Chance und der benötigte Impuls, Datensilos aufzubrechen und mehr Transparenz zu schaffen. Unternehmen, die diese Herausforderung so begreifen, erkennen, dass Nachhaltigkeit mehr ist als eine Vorschrift: Sie ist auch ein wirtschaftlich relevanter Faktor.

In Zeiten hoher Kosten sind solche Regularien für viele Unternehmen vor allem ein ökonomischer Hebel: LED-Leuchten, energetische Sanierungen, das Schließen von Druckluft-Leckagen sowie Strom aus erneuerbaren Energien schaffen Einsparpotenziale. Gleichzeitig profitieren die Betriebe auch ökologisch, denn die Maßnahmen reduzieren die CO₂-Emissionen. Nachhaltigkeit ist als Wirtschafts- und Wettbewerbsfaktor zu betrachten.

Unternehmen aller Größen haben in den vergangenen Jahren bereits Schritte in diese Richtung unternom-



Der AUTOR
Moritz Röder

ist Associate Director Supply Chain Management & Sustainability bei Lufthansa Industry Solutions.

(Bild-Quelle: Lufthansa Industry Solutions)

halten müssen, um nachhaltiger zu wirtschaften.

Neben Daten für vorgeschriebenen Nachhaltigkeitsbericht und das Lieferkettengesetz müssen sie nun auch Informationen zum Energiekonsum liefern. Zum Beispiel für Gebäude, Beleuchtung, Heizung, Pumpen, Druckluft, industrielle Prozesse und Transport. Für viele Firmen stellt das eine zusätzliche Herausforderung dar,

halten sind. Aber unabhängig von regulatorischen Verpflichtungen erstellt die Hälfte der Unternehmen bereits einen Nachhaltigkeitsbericht, weil ihnen das Thema so wichtig ist. Nichtsdestotrotz müssen sie noch immer hohe Hürden überwinden, um diese Aufgabe zu bewältigen:

- Vier von fünf Unternehmen (80%) bemängeln die Datenqualität;

Zusätzliche Einsparungen sind nur mit einer sauberen Datenbasis und einer geeigneten Strategie möglich, in der **klar definierte Ziele** auch umgesetzt werden.

Link zur Studie <https://www.lufthansa-industry-solutions.com/de-de/studien/pac-it-sustainability-reifegradindex-2023>

NEWS LETTER

öffnen

AUGEN

Welche KPIs zur Nachhaltigkeit werden erfasst oder sollen erfasst werden?



„Weiß nicht/keine Angabe“ nicht angezeigt, geringfügige Abweichungen von 100% aufgrund von Rundungen möglich, n=92 (Filter: Unternehmen, die Daten zur Nachhaltigkeit ihres Unternehmens anhand konkreter KPIs bereits erfassen oder dies planen), des Weiteren wurde „gemeinschaftliches Engagement“ often genannt © PAC 2023

men. Vor dem Hintergrund des neuen Gesetzes müssen sie aber nicht nur den Status-quo dokumentieren, sondern den nächsten Schritt gehen und ihren Energieverbrauch künftig weiter absenken.

Datenbasiertes Nachhaltigkeitsmanagement

Zusätzliche Einsparungen sind allerdings nur mit einer sauberen Datenbasis und einer geeigneten Strategie möglich, in der klar definierte Ziele auch umgesetzt werden. Laut der LHIND-Studie haben jedoch nur vier von zehn Unternehmen Nachhaltigkeitsziele formuliert, die mit Hilfe definierter KPIs erreicht werden sollen. Neben den CO2-Emissionen (92%) gehört die Energieeffizienz (82%) zu den am häufigsten erfassten Kennzahlen.

Eine strategische Sicht auf Sustainability ermöglicht Unternehmen erst, die KPIs mit finanziellen Faktoren zu verknüpfen, um auf dieser Basis Investitionsentscheidungen, Produktentwicklungen oder Standortwahlen zu treffen. So können zum Beispiel Daten zur Effizienz helfen, das Risiko volatiler Energiepreise zu verringern und sich für die Zukunft resilient aufzustellen.

Kein Unternehmen hat jedoch Zeit und Personal, um die notwendigen Informationen manuell zu sammeln und auszuwerten. Ohne ein effizientes Datenmanagement und mit einer möglichst weitgehenden Automatisierung ist die Aufgabe nicht zu bewältigen. Denn ein auf Nachhaltigkeitsdaten spezialisiertes Analysetool hilft Unternehmen dabei, Datensilos aufzulösen und Daten effizient zu verarbeiten. Es führt Daten aus verschiedenen Quellen zusammen, berechnet die aktuelle Performance, ermöglicht eine transparente Darstellung und die Definition von Zielwerten.

Durch gesetzliche Regularien benötigte Informationen lassen sich einfach bereitstellen, bereinigen und auswerten, was sich positiv auf die Berichterstellung – Aufwand und Nutzen – auswirkt. Kurzum: Ein solches Werkzeug unterstützt Unternehmen beim Aufbau eines datenbasierten Nachhaltigkeitsmanagements, um nicht nur ihre Energieeinsparziele, sondern auch ihre Klimaziele insgesamt zu erreichen. •



Sichern Sie sich jetzt
Ihren wöchentlichen kostenfreien
Newsletter!

www.digitalbusiness-cloud.de/newsletter

DIGITAL BUSINESS
CLOUD

WIN
VERLAG

IMPRESSUM

DIGITAL BUSINESS CLOUD Magazin
www.digitalbusiness-cloud.de

Herausgeber und Geschäftsführer:
Matthias Bauer, Günter Schürger

So erreichen Sie die Redaktion:
Chefredaktion: Heiner Sieger (hsi), hsi@win-verlag.de
v. i. S. d. P. Tel.: 0 81 06 / 3 50-183
Redaktion: Stefan Girschner (stg), stg@win-verlag.de

Mitarbeiter dieser Ausgabe:
Maxim Habersin, Markus Hahn, Udo Hensen, Michael Hering,
Harald Huber, Sascha Kegreiß, Thilo Kerner, Markus Koerner,
Gerd Kuchelmeister, Sascha Leser, Ian McShane, Sebastian Mehle,
Matthias Pfützner, Udo Ramin, Dimitrios Rizoulis, Moritz Röder,
Evgenij Smirnov, Franz Salzmann, Andreas Steffen,
Falko Timme, Pia Tischer, Michael Veit

Stellvertretende Gesamtanzeigenleitung:
Bettina Prim, bp@win-verlag.de, Tel.: 08106/350-223

Anzeigendisposition:
Chris Kerler (08106 / 350-220, dispo@win-verlag.de)
Sabine Immerfall (08106 / 350-131, dispo@win-verlag.de)

So erreichen Sie den Abonentenservice:
Leserservice „WIN-Verlag“
Postfach 13 63, 82034 Deisenhofen
Tel.: +49 (0) 89 / 85 853 – 866
Fax: +49 (0) 89 / 85 853 – 62866
win-verlag@cover-services.de

Vertrieb:
Sabine Immerfall, (si@win-verlag.de), Tel.: 0 81 06 / 350-131

Produktion/Herstellung:
Jens Einloft (-172; je@win-verlag.de)

Artdirection/Titelgestaltung:
DesignConcept Dagmar Friedrich-Heidbrink

Bildnachweis/Fotos:
stock.adobe.com, shutterstock.com, Werkfotos

Vorstufe + Druck:
C. Maurer GmbH & Co. KG, Geislingen/Steige
Anschrift Anzeigen, Vertrieb und alle Verantwortlichen:
WIN-Verlag GmbH & Co. KG,
Johann-Sebastian-Bach-Str. 5, 85591 Vaterstetten,
Telefon 0 81 06 / 350-0

Verlags- und Objektleitung:
Martina Summer (08106 / 306164, ms@win-verlag.de)

Bezugspreise:
Einzelverkaufspreis: 11,50 Euro in D, A, CH und 13,70 Euro
in den weiteren EU-Ländern inkl. Porto und MwSt. Jahresabonnement
(6 Ausgaben): 69,00 Euro in D, A, CH und 82,20 Euro in den weiteren
EU-Ländern inkl. Porto und MwSt. Vorzugspreis für Studenten, Schüler,
Auszubildende und Wehrdienstleistende gegen Vorlage eines Nachweises
auf Anfrage. Bezugspreise außerhalb der EU auf Anfrage.

27. Jahrgang
Erscheinungsweise: 6-mal jährlich

Einsendungen: Redaktionelle Beiträge werden gerne von der
Redaktion entgegen genommen. Die Zustimmung zum Abdruck und zur
Vervielfältigung wird vorausgesetzt. Gleichzeitig versichert der
Verfasser, dass die Einsendungen frei von Rechten Dritter sind und nicht
bereits an anderer Stelle zur Veröffentlichung oder gewerblicher
Nutzung angeboten wurden. Honorare nach Vereinbarung. Mit der
Erfüllung der Honorarvereinbarung ist die gesamte, technisch
mögliche Verwertung der umfassenden Nutzungsrechte durch den Ver-
lag – auch wiederholt und in Zusammenfassungen – abgegolten.
Eine Haftung für die Richtigkeit der Veröffentlichung kann trotz Prüfung
durch die Redaktion vom Herausgeber nicht übernommen werden.
Copyright © 2023 für alle Beiträge bei der WIN-Verlag GmbH & Co. KG

Kein Teil dieser Zeitschrift darf ohne schriftliche Genehmigung
des Verlages vervielfältigt oder verbreitet werden. Unter dieses Verbot fällt
insbesondere der Nachdruck, die gewerbliche Vervielfältigung per Kopie,
die Aufnahme in elektronische Datenbanken und die Vervielfältigung
auf CD-ROM und allen anderen elektronischen Datenträgern.

ISSN 2510-344X, VKZ B31383F
Dieses Magazin ist umweltfreundlich
auf chlorfrei gebleichtem Papier gedruckt.

Außerdem erscheinen beim Verlag:
AUTOCAD Magazin, BAUEN AKTUELL, r.energy,
DIGITAL ENGINEERING Magazin, DIGITAL MANUFACTURING,
e-commerce Magazin, DIGITAL BUSINESS CLOUD,
DIGITAL PROCESS INDUSTRY, DIGITAL HEALTH INDUSTRY,
virtual-reality-magazin.de

DIGITAL BUSINESS CLOUD

06

/// BIG TECH

Muss das weg?

Die Digitalkonzerne sind dabei, Wirtschaft und Demokratie zu zerstören. Sind sie noch zu stoppen, und wenn ja: wie?

/// DATENSOUVERÄNITÄT

Vorfahrt für Sicherheit

Im Umgang mit Daten wird Sicherheit wichtiger denn je. Was müssen Firmen bei exponentiell steigenden Datenmengen beachten?

/// INNOVATION

Mehrwert schaffen – aber wie?

Deutschlands Unternehmen hinken bei der Investition in Innovationsprojekte hinterher. Neben Mut fehlen Budget und Ressourcen.

/// AGILE UNTERNEHMEN

Erfolgreich ohne Struktur?

In Zeiten digitaler Transformation ist Tempo ein zentraler Erfolgsfaktor. Doch ohne agiles Mindset gibt es keine Höchstgeschwindigkeit.

Die nächste Ausgabe erscheint am 13.11.2023

REDAKTIONELL ERWÄHNTE FIRMEN

Arctic Wolf, Check Point, comfote,
CosmoConsult, coveto ATS, Docusign, d.velop,
ELO Digital Office, Eperi, Forescout, Gebra-IT,
Helu.io, Kumavision, Kyndryl Deutschland,
Logicalis, Lufthansa Industry Solutions,
Mittel Deutschland, Qlik, Red Hat, Revenera,
Rohde&Schwarz, Semperis, Sophos, Sybit,
Telekom, Timme Hosting, USU Software, Varonis
Systems, Vast Data, Wasabi, WeAreDevelopers





WE ARE HIRING

MEDIABERATER M/W/D



UNSER TEAM SUCHT VERSTÄRKUNG

Unser Verlagshaus ist einer der Pioniere und einer der führenden Fachzeitschriftenverlage im Bereich der Digitalen Transformation. Unsere B2B-Zeitschriften sind innovativ und gehören in ihren Bereichen jeweils zur Spitzengruppe.

Sie möchten mit Ihrer Kreativität den Erfolg unserer Fachmagazine mitgestalten? Dann sind Sie bei uns richtig. Derzeit suchen wir engagierte Mediaberater (m/w/d) in Voll- oder Teilzeit.

Wir freuen uns auf Ihre aussagekräftige Bewerbung unter
<https://win-verlag.de/karriere/>

WIN
VERLAG



Kennen Sie schon unser **Sonderheft Logistik** vom e-commerce magazin?

Logistik ist heute das zentrale Thema der Weltwirtschaft. Wir informieren über die neuesten Entwicklungen in der Logistik und bei den Logistik-Immobilien, fragen bei Experten nach und zeigen aktuelle Lösungen anhand von Best Practice Beispielen.

- Erscheinungstermin: 20.10.23
- Redaktionsschluss: 20.09.23
- Auflagen: Print und ePaper: ca. 20.000
- Verbreitung: Abonnenten, Deutsche Bahn, Veranstaltungen und Direktversand
- Veröffentlichung als Print- und Digital-Beilage zur Ausgabe 5/2023 e-commerce magazin

