it management

Der Motor für Innovation
Januar/Februar 2023

INKLUSIVE 48 SEITEN
it security

PROFESSIONELLES DATENMANAGEMENT

Wir investieren in die Zukunft

Christian Sohn, Managing Director, zetVisions GmbH

WIFI, LTE ODER 5G?

PoCs zeigen den Nutzen

THE NEXT BIG THING

ERP: Gehört Low-Code die Zukunft?

MACH-TECHNOLOGIEN

Microservices, APIs und Cloud

IT WELT.at is IT

IT NEWS

Der tägliche Newsletter der ITWELT.at bringt die aktuellen IT Nachrichten aus Österreich und dem Rest der Welt. Wer immer up to date sein will, bestellt den kostenlosen Newsletter itwelt.at/newsletter und ist damit jeden Tag schon am Morgen am neuesten Informationsstand.

itwelt.at

IT TERMINE

In Österreichs umfangreichster IT-Termindatenbank gibt es Termine für IT-Events wie Messen, Konferenzen, Roadshows, Seminare, Kurse und Vorträge. Über die Suchfunktion kann man Thema und Termin suchen und sich bei Bedarf auch gleich anmelden. Mit Terminkoordination und Erinnerung per E-Mail.

itwelt.at/events

IT UNTERNEHMEN

TOP 1001 ist Österreichs größte IT-Firmendatenbank. Mit einer Rangliste der umsatzstärksten IT- und Telekommunikations-Unternehmen. Die Datenbank bietet einen Komplettüberblick der TOP IKT-Firmen und ermöglicht die gezielte Abfrage nach Tätigkeitsschwer-punkten, Produkten und Dienstleistungen.

itwelt.at/top-1001

IT JOBS

Hier sind laufend aktuelle IT Job-Angebote zu finden. In Zusammenarbeit mit der Standard.at/Karriere, dem Jobportal der Tageszeitung Der Standard, findet man auf dieser Plattform permanent hunderte offene Stellen aus dem Bereich IT und Telekom. Eine aktive Jobsuche nach Tätigkeitsfeld und Ort ist natürlich möglich.

itwelt.at/jobs

IT MANAGEMENT & IT SECURITY RELOADED

LIEBE LESERINNEN UND LESER,

Hallo und herzlich willkommen zur ersten Ausgabe 2023! Sie werden es auf den ersten Blick und Touch gemerkt haben. Wir haben unsere Printausgabe einem umfangreichen Relaunch unterzogen.

Vieles ist neu: Logo, Haptik, ein voluminöseres Papier, der Heftumfang, nachhaltigere Erscheinungsweise, Bildsprache und Optik, Stilelemente. Denn wir glauben an die Printzukunft.

Und auch wenn sich unsere Online-Plattform it-daily.net prächtig entwickelt, wird Print immer eine große Rolle einnehmen – Crossmedial ist hier das Stichwort.

Und was erwartet uns 2023: Nun, hoffentlich ein Ende der diversen Krisen. Denn zu viel Abkehr von gewohnten Prozessen und Wandel fördert Ängste. Ängste, die Unternehmen daran hindern, die Digitalisierung weiter voranzutreiben. Die Welt ist komplex, anfällig für Störungen, aber trotzdem enorm resilient! Und genauso ist es, entgegen aller düsteren Prognosen, gekommen. Vielleicht müssen wir uns nur auf ein höheres Level an Störanfällen einstellen und dementsprechend agieren.

In diesem Sinne sind Sie hoffentlich gut ins neue Jahr gestartet? Denn auch die IT wird von der Evolution 2023 nicht verschont bleiben. Prognosen gibt es zuhauf und je nach Autor und Unternehmen fallen sie unterschiedlich aus. Welche Vorhaben Unternehmen jetzt priorisieren, müssen sie selbst entscheiden. In diesem Heft und auf www.it-daily.net halten wir zumindest eine Auswahl zu den Prognosen für das Jahr 2023 für sie bereit!

Herzlichst

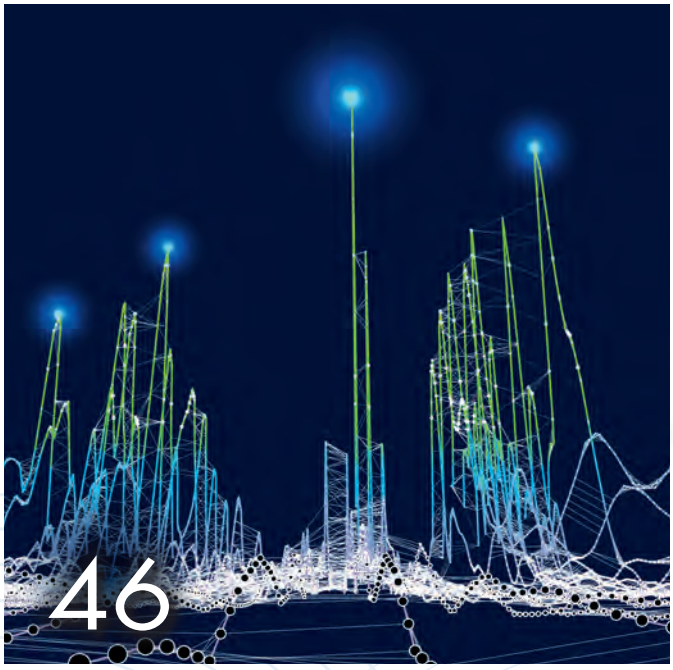
Ulrich Parthier | Publisher it management & it security

INHALT

COVERSTORY

IT MANAGEMENT

Farblich hervorgehobene Artikel sind von der Redaktion als besonders lesenswert empfohlen



Inklusive 48 Seiten IT Security

GUT ZU WISSEN

Achten Sie auf dieses Icon und lesen sie mehr zum Thema im Internet auf **www.it-daily.net**

Chief Information Officer

NEUE STRATEGISCHE ROLLE?

CIOs sind nach dem CEO die zweitwichtigste Instanz bei der Gestaltung und Umsetzung der Unternehmensstrategie und kontrollieren heute die Mehrheit der Unternehmensbudgets, so das Ergebnis einer Studie von Citrix. Die Studie basiert auf der Befragung von 3.300 Führungskräften in großen und mittelständischen Unternehmen weltweit.

CIOs und andere C-Suite-Führungskräfte im technischen Bereich haben mit einem Mangel an Fach- und Führungskräften zu kämpfen. Fast die Hälfte (46 Prozent) der C-Level-Führungskräfte in der Technologiebranche zögert ihren Ruhestand hinaus, weil sie befürchten, dass es niemanden gibt, der sie ersetzen kann. Diese Befürchtung ist angesichts ihrer derzeitigen Aufgaben sinnvoll, denn 60 Prozent geben an, dass ihre Aufgabe darin besteht, dafür zu sorgen, dass alle Mitarbeiter im Unternehmen über die erforderliche Technologie verfügen, um effektiv zu arbeiten, und die Hälfte gibt an, dass sie an der Behebung technischer Probleme der Mitarbeiter beteiligt sind. Auch wenn sich die Rolle weiterentwickelt, muss noch mehr getan werden, um sicherzustellen, dass CIOs in der Lage sind, die von zukünftigen IT-Leitern geforderte übergeordnete Geschäftsstrategie zu priorisieren.

Aus diesem Grund befinden sich die heutigen Tech-Führungskräfte in einer Zwickmühle zwischen einer „traditionellen" CIO-Rolle: Verwaltung der Infrastruktur und Leitung von Projekten zur digitalen Transformation und einer „Übergangsrolle": Definition und Verfeinerung der Arbeitsplatztechnologie und der Förderung der Geschäftsstrategie.

www.citrix.de

BEDEUTUNG DES CIOs

64 %

der Befragten geben an, dass der CIO den Großteil des Budgets ihres Unternehmens kontrolliert

76 %

der deutschen Führungskräfte geben an, dass der CIO heute nach dem CEO die zweitwichtigste Rolle bei der Gestaltung und Umsetzung der Unternehmensstrategie spielt

73 %

der Führungskräfte sind der Meinung, dass eine Zukunftsvision wichtig ist, um in der heutigen Arbeitswelt ein erfolgreicher Tech Leader zu sein

NEW WORK

HYBRIDER ARBEITSPLATZ ALS WETTBEWERBSFAKTOR

Unternehmen suchen zunehmend nach Wegen, die Vorteile des Homeoffice mit den Vorzügen des Büros als sozialem Ankerpunkt zu verbinden. New-Work-Serviceanbieter entwickeln deshalb gerade mit Hochdruck Lösungen für den hybriden Arbeitsplatz. Dies meldet die neue Anbietervergleichsstudie „ISG Provider Lens Future of Work – Services & Solutions Germany 2022", die das Marktforschungs- und Beratungsunternehmen Information Services Group (ISG) veröffentlicht hat. Der Anbietervergleich untersucht die Wettbewerbsstärke und Portfolioattraktivität von 30 Dienstleistern, die im deutschen Markt für Future-of-Work-Services und -Lösungen tätig sind.

„Hybrides Arbeiten ist in der heutigen Dimension auch für die Service-Provider im New-Work-Markt ein neues Thema. Nachhaltige Erfolgsgeschichten gibt es daher bisher kaum", sagt Roman Pelzel, Principal Consultant bei der ISG. Deshalb könnten Serviceanbieter noch große Wettbewerbsvorteile am Markt erzielen, wenn sie erfolgreiche Implementationen von Hybrid-Work-Lösungen vorweisen.

Technik vs. Kultur

Den ISG-Analysten zufolge standen bisher vor allem die digitalen und technologischen Aspekte des hybriden Arbeitens im Mittelpunkt der New-Work-Initiativen in Unternehmen, vor allem ausgelöst durch die COVID-Pandemie. Nun würden die menschenbezogenen und kulturellen Aspekte sowie Fragen der Bürogestaltung zunehmend in den Mittelpunkt rücken. Deshalb sollten neben der IT-, auch die HR-Abteilung sowie das Facility Management beim Einführen von Lösungen für hybrides Arbeiten miteinbezogen werden.

Den ISG-Analysten zufolge zeigen deutsche Unternehmen darüber hinaus erstes Interesse an der Mischung aus Realität und Virtualität, um den Nutzen für Kunden und die eigenen Mitarbeiter zu erhöhen. Noch schränke teure und unhandliche Hardware wie VR-Brillen die neuen Technologien wie zum Beispiel das Metaverse ein. Doch gebe es erste erfolgreiche Anwendungsfälle wie zum Beispiel Schulungen oder das Onboarding neuer Mitarbeiter, bei denen immersive Technologien die Effektivität gesteigert hätten.

https://isg-one.com

GUT ZU WISSEN

Die Studie kann unter folgender Adresse herunter geladen werden:
https://bit.ly/3XiQk52

SUPERCLOUD

DIE NÄCHSTE STUFE VON CLOUD COMPUTING?

Die Supercloud macht die Runde. Sie gilt als die nächste Evolutionsstufe von Cloud Computing. Bei der genauen Definition aber ist sich die IT-Szene noch nicht so ganz einig.

Der Gedanke dahinter: Supercloud steht für eine IT-Architektur, die alle Service-Level (IaaS, PaaS und SaaS) integriert. So gesehen ist die Supercloud auch mehr als das, was die Hyperscaler an IT-Services zu bieten haben, denn deren Clouds agieren immer noch als mehr oder weniger interoperable Silos. In diesem Sinne ist die Supercloud quasi eine Multi-Cloud 2.0. Daher sollte auch Edge Computing, als erweiterte Form von Cloud Computing, unbedingt dazugehören.

www.couchbase.com

DIE WICHTIGSTEN ATTRIBUTE

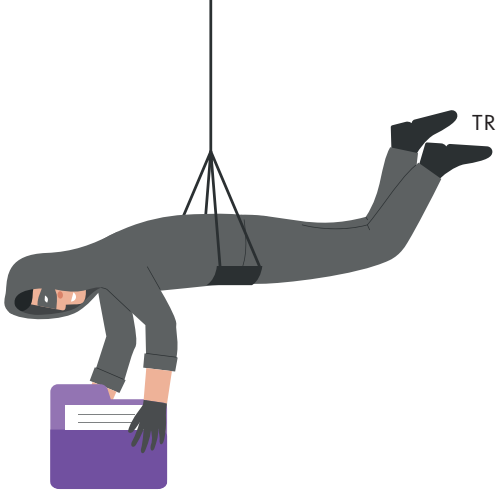
Alle Services in der Supercloud sind hochautomatisiert, egal ob es sich um Infrastruktur-, Plattform- oder Applikation-Services handelt. Das vereinfacht die Administration und die Nutzung der Services.

In der Supercloud läuft ein Set von verbrauchsbasierten Services, die aus mehr als einer Cloud kommen, sei sie nun Private oder Public. Sie orchestriert den Betrieb dieser Workloads in jeder Cloud und zwischen den Clouds.

Die Supercloud schafft damit auch eine gemeinsame Benutzeroberfläche für Entwickler und Nutzer und vereinfacht so die operative Umsetzung von wichtigen IT-Trends wie DevOps und SecOps.

Die nativen PaaS-Layer der verschiedenen Cloud-Anbieter werden in der Supercloud zu einem „Super-PaaS"-Layer abstrahiert. So entsteht eine einheitliche Plattform, in die Partner einfacher ihre spezifischen Innovationen und Lösungen einbringen können.

Sie nutzt die nativen Werkzeuge der verschiedenen Clouds in einer gemeinsamen Management-Schicht, samt integriertem Metadaten-Management. So können wichtige Parameter des Cloud-Betriebs wie Datenaustausch, Performance, Sicherheit und Kosten zentral optimiert werden.



Gestohlene Daten

DIE SECHS HÄUFIGSTEN VERSÄUMNISSE

Laut der aktuellen Studie „More Lessons Learned from Analyzing 100 Data Breaches" im Auftrag von Imperva, ist der Diebstahl von Kreditkarteninformationen und Passwortdaten rückläufig (Rückgang um 64 Prozent). Unternehmen sollten weiterhin auf folgende Punkte achten:

#1 Fehlende Multi-Faktor-Authentifizierung (MFA)

Setzen Unternehmen auf Multi-Faktor-Authentifizierung wird es für einen Angreifer viel schwieriger, mit gestohlenen Anmeldeinformationen auf sensible Daten zuzugreifen.

#2 Begrenzter Einblick in alle Datenbestände

Unternehmen benötigen eine Lösung mit einem einzigen Dashboard, das einen Überblick über eine breite Palette von Datensicherheitsfunktionen bietet. Dazu gehören Datenerkennung und -klassifizierung, Überwachung, Zugriffskontrolle, Risikoanalyse, Compliance-Management, Sicherheitsautomatisierung, Bedrohungserkennung und Audit-Berichterstattung.

#3 Unzureichende Passwortrichtlinien

Jedes Unternehmen sollte seine Mitarbeitenden regelmäßig in Schulungen darauf hinweisen, Passwörter nicht zu duplizieren und sie nicht mit Kollegen, Partnern oder Lieferanten zu teilen.

#4 Falsch konfigurierte Dateninfrastrukturen

Jede von der Cloud verwaltete Infrastruktur ist einzigartig und erfordert spezielle Fähigkeiten, um sie richtig zu verwalten. Durch die Sichtbarkeit aller in der Cloud verwalteten Datenbestände über ein einziges Dashboard ist es nicht mehr notwendig, Konfigurationen für die Datentransparenz zu pflegen.

#5 Begrenzter Schutz vor Schwachstellen

Eine Zero-Day-Schwachstelle in einem beliebten Code kann bei Zehntausenden von Unternehmen zu Sicherheitsproblemen führen. Der Laufzeitschutz (Runtime Protection) schützt Anwendungen vor Schwachstellen, ohne dass diese potenziellen Angriffen ausgesetzt werden.

#6 Nicht aus früheren Datenschutzverletzungen lernen

Unternehmen sollten maschinelles Lernen (ML) einsetzen, um anomales Verhalten genau zu analysieren und bösartige Aktivitäten zu identifizieren. Mit diesen Informationen können sie eine Basislinie für den typischen Zugriff privilegierter Benutzer festlegen.

www.imperva.com

Wir investieren in die Zukunft

MIT NEUEM SELBSTVERSTÄNDNIS AUF WACHSTUMSKURS

Seit einem Jahr führt Christian Sohn als Managing Director die Geschicke von zetVisions. Mit Sitz in Heidelberg, im Herzen des IT-Clusters Rhein-Main-Neckar, realisiert und implementiert das Unternehmen seit 2001 intuitive Softwarelösungen für das Datenmanagement. Wohin Christian Sohn zetVisions entwickeln will, berichtet er im Interview mit Ulrich Parthier, Publisher it management.

? **Ulrich Parthier:** *Herr Sohn, Sie sind nun fast 12 Monate an der Spitze von zetVisions. Wie sieht ihre persönliche Jahresbilanz aus?*

Christian Sohn: Für das Jahr 2022 hatten wir uns ein Wachstum im zweistelligen Prozentbereich vorgenommen. Und das haben wir in den meisten Bereichen erzielt.

Wir haben im zurückliegenden Jahr neue Kunden gewonnen, konnten Geschäftsfelder ausbauen, haben unser Partnernetzwerk erweitert, entwickeln ein neues Selbstverständnis mit Fokus auf den Menschen sowie unsere Unternehmenskultur und formen einen neuen Markenauftritt.

Damit sind alle geplanten Projekte für die Transformation und die Unternehmensentwicklung auf den Weg gebracht.

MEHR WERT

Weitere Infos zu zetVisions und Christian Sohn:
www.linkedin.com/company/zetvisions-gmbh
www.linkedin.com/in/christian-sohn

Ich bin sehr stolz auf die MitarbeiterInnen und sehr zufrieden mit dem, was wir als Team bis jetzt erreicht haben! Um wachsen zu können, braucht es vor allem gute und engagierte MitarbeiterInnen. Bei meinem Einstieg umfasste unser Team 80 Personen. Heute sind wir über 100 KollegInnen. 2023 und 2024 sollen jeweils 35 weitere KollegInnen an Bord kommen. Wir investieren also massiv in die Zukunft.

? **Ulrich Parthier:** *Gibt der Markt diesen Wachstumsanspruch in einer Rezessionsphase überhaupt her?*

Christian Sohn: Auch wenn digitale Transformation oder Digitalisierung abgegriffene Buzzwords sind, haben immer noch sehr viele Unternehmen in Deutschland einen erschreckend schwachen Digitalisierungsgrad. Selbst in einer Wirtschaftskrise wird hier weiter investiert werden müssen – denn hier heißt es „Do or die!"

Wenn wir über Digitalisierung sprechen, geht es stets um zwei Ebenen: Prozesse und Daten. zetVisions bietet Unternehmen auf beiden Ebenen einen entscheidenden Wertbeitrag. Nämlich die Datenlage so zu optimieren, dass Führungskräfte auf der Basis exzellenter Daten gute Entscheidungen treffen können. Und zusammen mit unserem Partnernetzwerk im gleichen Zuge die Prozesse dafür zu perfektionieren. Dies wird auch in wirtschaftlich herausfordernden Zeiten gefragt und von hohem Wert sein. Ich bin mir sicher: ganz besonders in diesen Zeiten. Deshalb: Ja, wir sehen für zetVisions große Marktchancen.

? **Ulrich Parthier:** *Wo liegen diese genau?*

Christian Sohn: zetVisions hat sich in den letzten Jahren im Wesentlichen über seine beiden Produktfelder definiert: Das Beteiligungsmanagement und das Stammdatenmanagement. Im Beteiligungsmanagement betreuen wir mehr als die Hälfte aller deutschen DAX-Unternehmen und einen großen Anteil der M-DAX und S-DAX-Unternehmen. Hier sind wir Marktführer mit einer tollen Diversifikation: Industrie, Banken, Versicherungen, öffentliche Hand. Bei diesem wichtigen Werkzeug haben wir einen loyalen Kundenstamm, den wir fokussiert ausbauen werden!

Wenn man auf das Stammdatenmanagement blickt, dann sehe ich große Potenziale. In Unternehmen bilden die Datenqualität und das Management von Daten das Fundament für die Datenstrategie. Datenqualität und Datenmanagement sind die Grundlage, um Digitalisierung voranzutreiben.

Aus dieser Perspektive entwickeln wir unser neues Selbstverständnis: Wir denken weniger in einzelnen Produkten, sondern vielmehr in ganzheitlichen und strategischen Lösungen, die wir mit unserem Partner-Ökosystem für unsere Kunden bereitstellen.

? **Ulrich Parthier:** *Wie muss man sich das vorstellen?*

Christian Sohn: Stand heute wird zetVisions vor allem wahrgenommen als Anbieter von Beteiligungs- und Stammdatenmanagementsoftware. Wir verstehen uns mittlerweile aber viel stärker als strategischer Partner unserer Kunden.

Bevor sich ein Unternehmen für eine Stammdatenmanagement-Software entscheidet, geht es um folgende Themen: 1.

Organisation & Governance; 2. Prozesse & Architektur; 3. Datenqualität und 4. das „Information Model".

Mit unserem Partnerökosystem sind wir in der Lage, Unternehmen im kompletten Lifecycle bis hin zum Softwaretool, dessen Implementierung und im Aftersales zu unterstützen. Das Netzwerk und die enge Zusammenarbeit mit unseren Technologie- und Beratungspartnern verschafft unseren Kunden Synergien und strategische Vorteile durch ganzheitliche Lösungen auf der Prozess-, Technologie- und der Produktebene.

Ein Beispiel: Gemeinsam mit einem Partner bietet wir ein methodisches Vorgehen, die „Master Data Excellence" an: ein lückenloser End-to-end Service, mit dem wir von der Beratungs- und von der Umsetzungsseite Unternehmen ganzheitlich begleiten können, um exzellente Datenqualität zu erreichen.

? **Ulrich Parthier:** *Wie sieht ihr Plan für die nahe Zukunft aus?*

> MIT UNSEREM PARTNERÖKOSYSTEM SIND WIR IN DER LAGE, UNTERNEHMEN IM KOMPLETTEN LIFECYCLE BIS HIN ZUM SOFTWARETOOL, DESSEN IMPLEMENTIERUNG UND IM AFTERSALES ZU UNTERSTÜTZEN.
>
> **Christian Sohn, Managing Director, zetVisions GmbH, www.zetvisions.de**

Christian Sohn: Unsere Kunden schätzen es sehr, mit zetVisions einen Dienstleister mit kurzen und direkten Kommunikationswegen zu haben. Wir sind offen, flexibel und reagieren schnell. Das unterscheidet uns von Konzernen. In diesem Sinne wollen wir in Zukunft unsere Angebote, Dienstleistungen und Produkte im Rahmen eines Co-Innovationsprogramms mit unseren Kunden und anhand der Marktbedürfnisse weiterentwickeln.

Neukunden wollen wir es einfacher machen, bei uns an Bord zu kommen. Wir vereinfachen unsere Lizenzmodelle und bieten neue Lizenzierungsoptionen an. Wir bringen bereits 2023 ein Produkt in die Cloud und streben an, bis 2025 das komplette Portfolio umgestellt zu haben.

Auch nach innen werden wir 2023 weiterwachsen, unsere Büroräume moderner und innovativer gestalten, die Eigenverantwortung in den Teams ausbauen, unsere NewWork-Philosophie fortführen und den Austausch und die Innovation fördern.

Wir verändern zudem den kompletten Marktauftritt von zetVisions und gehen mit einem neuen Logo, neuer Farbgestaltung, neuer Website und individueller Ansprache unterschiedlicher Zielgruppen in die Zukunft.

? **Ulrich Parthier:** *Was macht Sie nach einem Jahr so sicher, diese ehrgeizigen Ziele mit zetVisions erreichen zu können?*

Christian Sohn: Da kann ich Ihnen eine ganz einfache und ehrliche Antwort geben: unsere MitarbeiterInnen. Sie haben in den letzten Monaten unseren Veränderungsprozess begeistert unterstützt und mitgestaltet. Das Unternehmen sprudelt vor Leistungswillen und Innovationskraft.

! **Ulrich Parthier:** Herr Sohn, viel Erfolg auf Ihrem weiteren Weg.

Professionelles Datenmanagement

WAS SPRICHT DAFÜR?

Datenprobleme können tückische Folgen haben: So fanden im Frühjahr 2019 85 Kunden der Haiwaiian Airlines, die Meilen für Prämientickets eingelöst hatten, Abbuchungen zwischen 17.500 bis 674.000 Dollar auf ihren Kreditkarten. Das Reservierungssystem hatte die Kundenkonten versehentlich in Dollar statt in Flugmeilen belastete. Das Problem wurde noch dadurch verschärft, dass auch Buchungen durchgingen, die die Kreditkartenlimits deutlich überstiegen. Eine Kundin berichtete, ihr seien fälschlicherweise mehr als 150.000 Dollar in Rechnung gestellt worden, obwohl sie ein Limit von 10.000 Dollar auf ihrer HawaiianMiles-Kreditkarte hat. Und sie war nicht die einzige.

Seit zig Jahren wird über die Notwendigkeit eines professionellen Datenmanagements, über den Nutzen hoher Datenqualität etc. geredet, und doch wird man das Gefühl nicht los, alle drehen sich im Kreis. Alle sind sich einig, das Thema ist irgendwie wichtig, passieren tut aber nicht allzu viel. Und wenn etwas passiert, dann ist es bis dahin recht mühsam, im Unternehmen Akzeptanz auf der obersten Führungsebene zu finden und last but not least das erforderliche Budget genehmigt zu bekommen. Fragt man sich, woran es liegen mag, dass nach unzähligen Studien, Umfragen, Vorträgen und Fachbeiträgen, nach „Daten sind das neue Öl"-Statements das Thema Datenmanagement noch immer so stiefmütterlich behandelt wird, kommt einem der Gedanke: Viele Unternehmen haben anscheinend keine wirklichen „Schmerzen" – trotz der vorhandenen Datenprobleme. Anders ausgedrückt: Die „Schmerzen" sind offensichtlich zu klein, um die Investition in eine professionelle Datenmanagement-Lösung zu rechtfertigen.

It's the cost, stupid

Nun könnte man annehmen, die Unternehmensleitungen müssten doch für das Thema Datenmanagement zu gewinnen sein, wenn ihnen die Kosten schlechter Datenqualität transparent gemacht werden. Nur passiert das zumeist nicht: Laut dem Gartner Data Quality Market Survey messen fast 60 Prozent der Unternehmen die jährlichen finanziellen Kosten von Daten schlechter Qualität nicht. Nach der Gartner-Umfrage belaufen sich die durchschnittlichen jährlichen Finanzkosten je Unternehmen auf 15 Millionen US-Dollar. Das sind die direkten Kosten. Unternehmen sind aber nicht nur finanziell betroffen. Schlechte Datenqualitätspraktiken untergraben digitale Initiativen, schwächen ihre Wettbewerbsfähigkeit und säen Misstrauen der Kunden.

Es gibt weitere Zahlen: Thomas C. Redman, Gründer von Data Quality Solutions und in der Community als „the Data Doc" bekannt, schätzt in einem Beitrag für den Sloan Management Review des MIT, dass die Kosten schlechter Daten für die meisten Unternehmen bei 15 bis 25 Prozent des Umsatzes liegen. Dabei sind die Kosten, die Unternehmen durch wütende Kunden und Fehlentscheidungen entstehen, noch nicht einmal messbar – in jedem Fall aber enorm.

Soweit die schlechte Botschaft. Die gute lautet: Schätzungsweise zwei Drittel der messbaren Kosten können laut Redman identifiziert und dauerhaft beseitigt werden.

Dafür müssten man aber die entsprechenden Prozesse Schritt für Schritt dokumentieren und messen. Das machen die wenigsten. Davon weiß auch Jürg Hofer, Teamleiter Enterprise Architect bei der Emmi Schweiz AG, zu berichten. Nach seiner Erfahrung funktioniert das Thema Kosten als Trigger für Datenmanagement nur selten, da zum einen durch diesbezügliche Maßnahmen in der Regel keine Kosten direkt reduziert werden (Personalabbau), und zum anderen die Mitarbeiter durch Korrektureingriffe verhindern,

> SCHLECHTE DATENQUALITÄTSPRAKTIKEN UNTERGRABEN DIGITALE INITIATIVEN, SCHWÄCHEN IHRE WETTBEWERBSFÄHIGKEIT UND SÄEN MISSTRAUEN DER KUNDEN.
>
> **Christian Sohn, Managing Director, zetVisions GmbH, www.zetvisions.de**

dass schlechte Datenqualität zu Schäden führt. Im Zuge der fortschreitenden Digitalisierung wird das aber nicht mehr funktionieren. Der Grund: Die manuellen Schritte, bei denen während eines Prozesses von der Datenentstehung bis zum Vertrieb Menschen einen Blick auf die Daten hatten und korrigierend eingreifen konnten, gibt es immer weniger. „Die ‚biologischen Kontrollmechanismen' fallen weg", sagt Hofer. „Das heißt aber: Ich brauche IT-gestützte Prozesse mit entsprechenden Prüfmechanismen, die die Rolle der Menschen übernehmen, und das kostet Geld."

Argumente pro Datenmanagement

Auch wenn viele Unternehmen erfahrungsgemäß kaum in der Lage sind, die Kosten schlechter Datenqualität mit harten Fakten, also mit Zahlen zu belegen, wissen sie gleichwohl: Bei fehlerhaften Kunden- und Lieferantenstammdaten entstehen ihnen beispielsweise Kosten für Fehllieferungen und -bestellungen, Porto- und Arbeitskosten für Mailingrückläufer und hoher Arbeitsaufwand für Bereinigung und Fehlerkorrekturen. Zudem haben sie oftmals keinen Überblick über das Bestellvolumen bei demselben Lieferanten, was zu hohe Preise im Einkauf zur Folge hat. Mangelhafte Materialstammdaten erzeugen Kosten etwa durch zu niedrig ausgewiesene Rechnungsposten aufgrund fehlerhafter Stücklisten und zu hohe Logistikkosten durch falsche Gewichte. Vermehrte Reklamationen wegen fehlerhafter Lieferungen, falsche Materialbestellungen und Produktionsstillstände wegen fehlender Materialien sind weitere Kostentreiber.

Jenseits der reinen Kosten gibt es weitere Ansatzpunkte, um die Bedeutung eines professionellen Datenmanagements im Unternehmen zu verdeutlichen. Dazu zählt unter anderem das enorme Wachstum der Datenmenge. Um einmal die Dimension des Problems anschaulich zu machen, folgendes Beispiel von VW: Das Unternehmen produziert an weltweit 118 Standorten rund 40.000 Autos pro Tag. Dazu bedarf es einer Milliarde Teile (25.000 Teile pro Auto) und 1,25 Milliarden Arbeitsgänge pro Tag (fünf Arbeitsgänge pro Teil, 25 Prozent Eigenfertigungsanteil). Für jeden dieser Arbeitsgänge gibt es Auftragsdaten, Maschinendaten, Fertigungshilfsmitteldaten, Lager- und Materialdaten, Prozessdaten, Qualitätsdaten und Personaldaten. Hinzu kommen Daten zu den außerhalb der Fertigung liegenden Prozessen, wie beispielsweise für Vertrieb, Einkauf, Logistik, Verwaltung und Management. Der zentrale Punkt der Smart Factory, so heißt es folgerichtig bei Audi, ist die Beherrschung der enormen Datenströme. Allein der Karosseriebau für den Audi A3 produzierte bereits vor ein paar Jahren täglich 200 Gigabyte Daten. Wenn aber erst einmal alle Maschinen mit kognitiven Fähigkeiten ausgestattet sind, wenn alle wesentlichen Teile eines Automobils selbst wissen, dass sie in Ordnung sind und an der richtigen Stelle sitzen – dann müssen in einer unvorstellbaren Komplexität noch ganz andere Datenmengen verarbeitet werden, so Audi.

Auch die regulatorischen Anforderungen seitens des Gesetzgebers sind ein wichtiges Argument pro Datenmanagement. Die Nicht-Einhaltung von Gesetzen und Richtlinien (Compliance) kann schnell Millionen kosten, womit wir dann doch bei „Schmerzen" angekommen sind.

Folgerichtig ist für Jürg Hofer Datenmanagement für jedes Unternehmen eine unabdingbare Voraussetzung, um mit den Anforderungen der Digitalisierung seitens Behörden, der Kunden und Lieferanten mithalten zu können. Es drohen Verluste von Kunden und Marktanteilen oder empfindliche Strafen, wenn hier nicht investiert wird und die Unternehmen auf der Höhe der Zeit agieren können.

Eine Erkenntnis bleibt auch heute weiter richtig: Ein professionelles Datenmanagement kostet Geld, schlechte Datenqualität kostet schnell sehr viel mehr Geld.

Christian Sohn

WAS BRINGT PROFESSIONELLES (STAMM-)DATENMANAGEMENT

Mitarbeiterzufriedenheit

TALENTE ANZIEHEN UND BINDEN

Heutzutage haben viele Unternehmen mit einer hohen Mitarbeiterfluktuation zu kämpfen: Das neue Phänomen der stillen Kündigung, auch als Quiet Quitting bekannt, erschwert die Personalarbeit der Betriebe. In der kommenden Zeit wird sich diese Tendenz voraussichtlich eher verstärken als abschwächen. Methoden zur Mitarbeiterbindung, zur Verbesserung der Mitarbeiterzufriedenheit und zur Weiterentwicklung von Angestellten im Unternehmen werden nicht nur deshalb zur obersten Priorität der Personalabteilung: Im Gegensatz zu bisherigen Theorien hat die Zufriedenheit der Belegschaft einen erheblichen Einfluss auf die Rentabilität eines Unternehmens.

Doch wie kann man die Loyalität in Teams stärken und gleichzeitig die Effizienz von Prozessen verbessern?

1. Fokus auf Flexibilität

Die Pandemie hat unsere Arbeitsweisen und -strukturen verändert. Nach dem Ende der Einschränkungen erfreuen sich hybride Arbeitsmodelle weiterhin einer großen Beliebtheit. Inzwischen sind Angestellte, die komplett remote arbeiten, nicht länger die Ausnahme.

Wenn heute von Flexibilität die Rede ist, dann stehen längst nicht mehr nur die neuen Arbeitsmethoden im Fokus, sondern innovative Lösungen für die Herausforderungen der Arbeitswelt von morgen. Es müssen Lösungsansätze gefunden werden, die den Wandel in Unternehmen und Gesellschaft begleiten können. Mit anderen Worten: Nicht alle Geschäftsprozesse, die vor der COVID-Pandemie eingeführt wurden, sind nach der Gesundheitskrise noch effizient.

2. Autonomie für Teams und Mitarbeitende

Investitionen in die Ausbildung, die Weiterentwicklung und die Soft Skills von Angestellten sind ein weiterer Aspekt für eine zufriedene Belegschaft, der von Personalverantwortlichen nicht unterschätzt werden sollte. Es geht längst nicht mehr nur darum, Fortbildungsmaßnahmen anzubieten, die an das Fachgebiet der jeweiligen Mitarbeitenden gebunden sind. Im Jahr 2023 sollten Betriebe unbedingt verschiedene Kurse zur Entwicklung von Soft Skills und Schulungen zu wichtigen Branchenthemen anbieten.

3. Integration von Technologien

Wenn Arbeitnehmende weniger Zeit für repetitive Aufgaben benötigen, bleibt logischerweise mehr Zeit für die Aufgaben, die ihnen wirklich Spaß machen und einen Mehrwert fürs Unternehmen bringen. Dies hat nicht nur Auswirkungen auf Arbeitnehmende und deren berufliche Entwicklung, sondern auch auf die Organisation selbst. Damit die Mitarbeitenden am Ende des Monats nicht mehr mit nervigen, zeitraubenden Aufgaben beschäftigt sind, ist die Technologie entscheidend. Dank ihr lassen sich repetitive und monotone Aufgaben automatisieren. Die Belegschaft kann sich somit den wahren Herausforderungen im Arbeitsalltag widmen.

www.expensya-com/de

Gewappnet in die Zukunft

6 TIPPS FÜR EINEN NACHHALTIGEREN SERVICE

Sie möchten Ihr Unternehmen für die Zukunft wappnen? Wie wäre es mit mehr Nachhaltigkeit in Ihren Serviceabteilungen? Mit unseren 6 Tipps gelingt der Start ganz einfach.

#1 Ernennen Sie einen Nachhaltigkeitsmanager

Der 1. Schritt zu mehr Nachhaltigkeit im Service ist die Ernennung eines Nachhaltigkeitsmanagers. Er bringt die richtigen Leute zusammen, überwacht Projekte und sorgt für die Kommunikation. Sobald Ihre Mitarbeiter wissen, an wen sie sich mit Ideen wenden können, wird das Thema Fahrt aufnehmen.

#2 Machen Sie Nachhaltigkeit zu einem Teil Ihrer Marke

Jetzt sollten Sie Nachhaltigkeit zur Priorität machen. So wird sie Teil Ihrer Unternehmensmarke und -kultur. Warum? Wenn es nicht Teil Ihrer DNA ist, wird es oft nur halbherzig umgesetzt.

Aber wo fangen Sie an?

Setzen Sie sich mit allen Abteilungsvertretern und Ihrem Nachhaltigkeitsmanager zusammen, um grüne Ziele festzulegen. Alle Glühbirnen durch energieeffiziente zu ersetzen, kann ein erstes Ziel sein. Lassen Sie Ihre Teams zur Ideenfindung brainstormen. Passen Ihre Ziele und Prozesse noch zusammen? Nehmen Sie schrittweise Änderungen vor.

#3 Beziehen Sie Ihre Mitarbeiter ein

Nachhaltigkeit ist nun in Ihrem Unternehmen angekommen. Befragen Sie Ihre Mitarbeiter, welche Änderungen durch die Serviceteams umgesetzt werden sollen. Bieten Sie ihnen Fortbildungsmöglichkeiten zur Nachhaltigkeit und machen Sie Ihre Ziele zum Teil Ihrer Leistungsbeurteilungen.

Wie wäre ein Wettbewerb, den pro Team verursachten Müll zu reduzieren? Beginnen Sie mit Belohnungen zu arbeiten. So weiß jeder, dass Ihre Umweltziele genauso wichtig sind wie jeder andere KPI.

#4 Sensibilisieren Sie Ihre Mitarbeiter für ihr Handeln

Zeigen Sie Ihren Mitarbeiter zum Beispiel über ein Display wie viel Wasser sie am Tag verbrauchen. Die meisten sind sich nicht bewusst, wie leicht sie mit ein paar kleinen Änderungen zu Ihren Zielen beitragen können. IT und Facility könnten das Display erstellen und HR oder das Marketing die Initiative im Unternehmen verbreiten.

#5 Digitalisieren Sie Ihr Unternehmen

Bereit für den nächsten Schritt? Rufen Sie Ihre Serviceteam-Leiter zusammen und starten Sie eine Digitalisierungsinitiative. Sie werden überrascht sein wie viel Papier täglich verbraucht wird: Haftnotizen, Ausdrucke oder Verträge. Es gibt viele digitale Optionen weniger Papier zu nutzen.

Ihre Facility-Abteilung sollte einen kritischen Blick auf Ihren Papiervorrat werfen und alle nicht notwendigen Lieferantenverträge stoppen. Zusammen mit der IT-Abteilung können sie die Implementierung digitaler Systeme planen und die HR-Abteilung sorgt dafür anstehende Änderungen zu kommunizieren.

Wie wäre ein wiederbeschreibbares Notizbuch für alle Mitarbeiter oder Kunden? So gehen Sie mit gutem Beispiel voran und steigern Ihre Markenbekanntheit. Eine Win-Win-Situation!

#6 Denken Sie darüber nach, wie Sie Ihre Assets verwalten

Betrachten Sie Ihre Kosten für die gesamte Lebensdauer Ihrer Vermögenswerte. Was jetzt als die billigste Option erscheint, kann sich als die teuerste herausstellen, wenn sie weniger energieeffizient ist.

Brauchen Sie neue Laptops, Server oder andere Hardware? Berücksichtigen Sie Nachhaltigkeit in Ihrem Auswahlprozess. Erstellen Sie eine Liste von Lieferanten, die nachhaltig agieren und energieeffiziente Geräte anbieten. Beschränken Sie diese Auswahl nicht nur auf IT-Assets, sondern auch auf alle Bürogeräte und Materialien, von der Mikrowelle bis hin zu Toilettenpapier.

www.topdesk.de

TOPdesk

Vom CO_2-Verbrauch der IT

WARUM SICH NACHHALTIGES LIZENZMANAGEMENT LOHNT


Foto: @Manuel Emme

Pascal König ist IT-Leiter der Konstruktionsgruppe Bauen AG. Für 130 Beschäftigte managed er die Ausstattung mit Computerarbeitsplätzen, Notebooks, Tablets und Handys sowie der notwendigen Verbindungen zu den Servern. In dem Ingenieurbüro kommen vor allem Betriebssysteme und Anwendungssoftware von Microsoft zum Einsatz. Eine Lizenzierung für derart viele Geräte und User wird schnell teuer.

2016 dachte das Unternehmen deshalb erstmals über gebrauchte Microsoft-Lizenzen nach. Die sind zum einen bedeutend günstiger als die neueste Version oder Cloud-Lösungen. Zudem schonen sie die Umwelt. Denn Software-Upgrades bedingen oft die Anschaffung neuer Hardware. Den immer kürzer werdenden Lebenszyklus ihrer Computer und Server wollte man bei der Konstruktionsgruppe Bauen nicht länger mitgehen. Auch deshalb also gebrauchte Software.

Mit gebrauchter Software durchs Audit

Erste Testkäufe nahm Pascal König bei der VENDOSOFT GmbH vor. Sie zeigten eine Professionalität, die man bei anderen Gebrauchtsoftwarehändlern vermisste. König formuliert es so: „Es gibt eine Menge Anbieter gebrauchter Microsoft-Lizenzen. Viele erschienen uns unseriös. Bei VENDOSOFT war das anders." Überzeugt haben Dokumente wie die Vernichtungserklärung der Vorbesitzer sowie eine Bestätigung der Rechtmäßigkeit der erworbenen Programme durch unabhängige Wirtschaftsprüfer.

Kurz nach dem Kauf gebrauchter Office- und Visio-Lizenzen sowie eines SQL Servers durchlief die Konstruktionsgruppe Bauen ein Microsoft-Audit – und erhielt prompt die Legitimation für den Einsatz der Software. Das überzeugte vollends. Als man 2021 über einen Umstieg auf Cloud-Modelle nachdachte, war VENDOSOFT längst zu einer festen Instanz in Sachen Microsoft-Lizenzberatung geworden. Die Zusammenarbeit hatte gezeigt: Nicht nur die Beratung war hervorragend. Auch die Preise stimmten. „Ich muss nicht zehn Mal nachverhandeln, sondern bekomme gleich das beste Angebot", sagt Pascal König.

Doch der Preis ist nicht alles. Dem Ingenieurbüro ist es von jeher wichtig, bei der IT-Beschaffung so nachhaltig zu agieren, wie man es auch bei den Bauprojekten ist.

Nachhaltig – bei der IT genauso wie beim Bauen

Die Arbeit im Ingenieurbau ist längst noch nicht umweltschonend. Doch wo immer möglich, handelt die Konstruktionsgruppe Bauen ökologisch. Bis hin zur IT-Beschaffung. Mit gebrauchter Soft-

Illerbrücke bei Thanners - ein Monument der Konstruktionsgruppe Bauen

ware bleiben Systemanforderungen nun über Jahre gleich. Das verlängert die Lebensdauer der Computer, Notebooks und Server und ermöglicht, refurbished Notebooks einzusetzen, statt ihre IT wie üblich alle drei bis vier Jahre auszutauschen. Ein Denken, das allein bei den 130 PC-Arbeitsplätzen mehr als 9 Tonnen CO_2 einspart. Auf diese Zahl kommt, wer weiß, dass ein einziger Computer von der Produktion bis zur Entsorgung laut Umweltbundesministerium Emissionen von etwa 700 Kilogramm CO_2 verursacht. Das Treibhausgaspotenzial eines Notebooks mit SSD wird auf gut 600 Kilogramm CO_2 geschätzt.

CO_2- und kostensparend lizenziert

In enger Zusammenarbeit mit VENDOSOFT ließ sich auch die Umstellung auf Microsoft 365 nachhaltig gestalten: mit einer hybriden Lösung aus Cloud- und Gebrauchtsoftware. Aus der Vielzahl der Abomodelle von Microsoft empfahl der Lizenzberater Business Premium und Power BI Pro zu kombinieren. Dort, wo keine Cloud-Lösung erforderlich ist, kommt weiterhin die vorhandene Gebrauchtsoftware zum Einsatz. Mit dem hybriden Modell ist Pascal König äußerst zufrieden: „Damit haben wir alles erreicht, was uns wichtig war: eine optimale Vernetzung der acht Unternehmens-Standorte, Anbindung der remote Arbeitenden an die Cloud, Nutzung von Teams für unbegrenztes Video Conferencing und maximale Nachhaltigkeit."

Die Konstruktionsgruppe Bauen ist ein Beispiel, wie VENDOSOFT Unternehmen durch geschicktes, nachhaltiges Lizenzmanagement hilft, IT-Kosten im hohen zweistelligen Bereich UND zugleich CO_2-Emissionen einzusparen.

www.vendosoft.de

MEHR WERT

Mehr Beispiele unter
www.vendosoft.de/casestudies
Mehr Informationen unter
www.vendosoft.de/nachhaltige-it

DISRUPTION IN ACTION

TRANSFORMATION, DIGITALISIERUNG, DISRUPTION

Vielen Traditionsunternehmen gelingt der digitale Wandel nicht – warum?

Der Erfolg hängt entscheidend davon ab, ob die Managerinnen und Manager aus der Chefetage als „Change Leader" agieren oder nicht. Das ist leider häufig nicht der Fall: Etwa drei Viertel der Unternehmen scheitern bei der digitalen Transformation, so die Erfahrungswerte.

Der Grund: Die Digitalisierung stellt CEOs gleichzeitig vor drei neue Herausforderungen. Erstens: Disruptive neue Technologien mit großen Veränderungen des Geschäftsmodells bringen erhebliche Risiken mit sich. Zweitens sind umfangreiche Investitionen notwendig, die sich erst langfristig auszahlen. Und drittens gibt es keine bewährten, branchenüblichen Messgrößen, an denen man sich orientieren könnte. Die Herausforderungen sind so groß, dass Manager versucht sind, die Lösung des Problems zu delegieren.

Das führt in der Regel dazu, dass Unternehmen enorme Summen für neue Technologien ausgeben, die nicht funktionieren und anschließend jemanden bezahlen, um das Problem zu lösen. Das führt niemals zum Erfolg. Bei der Digitalisierung muss sprichwörtlich die gesamte Besatzung an Deck sein – Firmenchef oder Chefin und das gesamte Team.

Wie vorgehen?

Nun, es gibt zwar grundlegende Prinzipien, die in allen Branchen anwendbar sind. Als Beispiel geht es bei der Digitalisierung niemals um die Technologie als Selbstzweck. Vielmehr geht es darum, Leistungen für die Kunden zu verbessern. Außerdem hat die Transformation immer einen Anteil von 80 Prozent, der bei den Menschen liegt, nur 20 Prozent entfallen auf die Technologie. Denn gerade bei den Menschen liegt die echte Komplexität. Die Auswahl der Software etwa ist in den einzelnen Branchen unterschiedlich, aber das ist im gesamten digitalen Wandel nur ein Detail.

Welche Rolle spielt die IT bei der digitalen Transformation?

Die IT spielt eine Schlüsselrolle bei der digitalen Transformation und sie benötigt deshalb die Unterstützung von den anderen Geschäftsbereichen. Wenn man die digitale Transformation an die IT-Abteilung delegiert – oder noch schlimmer, an externe Berater – so wird sie scheitern. Erfolgreiche digitale Unternehmen arbeiten funktionsübergreifend, wobei alle Abteilungen zusammenarbeiten und die IT im Zentrum steht.

Disruption in Action
7 Inside stories of how global companies take on digital disruption;
Alexandra Jankovich, Tom Voskes, Adrian Hornsby;
SparkOptimus; 08-2022

Dies erfordert eine vollständige Umgestaltung des Unternehmens unter der Leitung der Unternehmensführung – deshalb sprechen wir in unserem neuen Buch „Disruption in Action" auch so viel über Leadership und Menschen und welche Fehler Unternehmen bei der digitalen Disruption machen.

Ohne Mehraufwand und Kosten

IT-OPTIMIERUNG VERBESSERT DIE ÖKOBILANZ IM UNTERNEHMEN

Kaum ein deutsches Unternehmen bleibt dieser Tage vom Lieferkettensorgfaltspflichtengesetz verschont. Das klingt nicht nur nervig, seine Erfüllung kostet auch Zeit, Geld und Ressourcen. Wichtig ist es dennoch, denn zu lang hat sich die westliche Wirtschaft eben jenen Sorgfaltspflichten entzogen, die sie entlang ihrer Lieferketten zu verantworten hat. Dabei verursachen der Herstellungsprozess und die Entsorgung von Waren vielerorts schwere Umweltschäden. Auch Menschenrechtsverletzungen sind an der Tagesordnung. Das ist uns allen beim Thema Plastik mehr als bewusst oder wenn es um Billigwaren aus Asien geht. Weniger bekannt sind die Emissionen und Müllberge, die Soft- und Hardware verursachen. Dabei sind sie massiv. Mit den folgenden IT-Management-Hacks lässt sich der ökologische Fußabdruck verbessern. In jedem Unternehmen, ohne Aufwand und auch noch kostensparend.

> UNTERNEHMEN, DIE DIE LEBENSDAUER IHRER LIZENZEN AUSNUTZEN, VERLÄNGERN AUCH DIE LEBENSDAUER IHRER COMPUTER UND SERVER.
>
> Angelika Mühleck, Fachjournalistin und Nachhaltigkeitsberaterin, www.purecontent.de

#1 Refurbished Hardware hilft CO_2 sparen

Computer, Notebooks, Server und Tablets sind Klimakiller. Das wird am Beispiel eines Desktop PCs deutlich, der im Laufe seines Produktlebens rund 700 Kilogramm CO_2 verursacht. Neue Computer für 100 Beschäftigte anzuschaffen, setzt demnach 7 Tonnen CO_2 frei. Hinzu kommen verseuchte Böden, die Gesundheitsgefährdung der Arbeiter auf den Elektroschrott-Deponien der Dritten Welt und weitere nachgelagerte Schäden. Sieben Tonnen für 100 Computer! Um allein eine Tonne der Treibhausgase aufzunehmen und zu neutralisieren, muss eine Buche etwa 80 Jahre wachsen. Liegt es da nicht nahe, voll funktionsfähige Hardware maximal lange einzusetzen, gegebenenfalls auch refurbished für einen zweiten oder gar dritten Nutzungszyklus? Im gewerblichen Kontext wird sie laut Bundesumweltamt alle drei bis vier Jahre erneuert. Dieser Turnus gehört für eine positive Klimabilanz dringend auf den Prüfstand!

#2 Software-Upgrades zwingen zu Hardware-Upgrades

Die meisten Software-Programme könnten sieben bis zehn Jahre lang genutzt werden. In dieser Zeit erhalten sie Sicherheits-Updates und werden supported. Deutlich früher jedoch bringen die Hersteller neue Lizenzen auf den Markt. Wer darauf anspringt, muss aufgrund gestiegener Systemanforderungen an Prozessoren, Arbeitsspeicher und Festplatten oft auch mit der Hardware nachziehen. Unternehmen, die die Lebensdauer ihrer Lizenzen ausnutzen, verlängern auch die Lebensdauer ihrer Computer und Server – mit oben beschriebenem Beitrag zum Klimaschutz!

#3 Trotz Cloud nicht in die Upgrade-Falle tappen

Wer ausschließlich über Cloudmodelle lizenziert ist, unterliegt meist unweigerlich den Upgrades durch die Hersteller. Ein hybrider Lizenzmix hilft, dieser Endlosspirale zu entkommen. Dabei werden nur remote arbeitende Beschäftigte und solche, die nicht ohne Tools wie Teams auskommen, über die Cloud lizenziert. Wo das nicht vonnöten ist und die Funktionalität ausreicht, können On-Premises-Lizenzen bis zum Ablauf ihrer Supportzeit verwendet werden. Die sind als Kauf- oder Gebrauchtlizenzen erhältlich und besonders günstig in der Anschaffung. Unternehmen sparen auf diese Weise hohe Abogebühren, umgehen eine zu große Abhängigkeit von den Herstellern und bestimmen den Zeitpunkt ihrer Soft- und Hardware-Upgrades selbst.

Nachhaltigkeit in der IT ist keine Rocket Science

Die Beispiele zeigen: Nachhaltigkeit in der IT beginnt im Kleinen, hat aber große Auswirkungen. Zu hinterfragen, wer die neue Version einer Software wirklich braucht, führt bereits zu signifikanten CO_2-Einsparungen, erfüllt gesetzliche Anforderungen an nachhaltiges Wirtschaften – und eröffnet ganz nebenbei enorme Potenziale zum Kostensparen.

Angelika Mühleck

Digitale Sicherheitslandschaft

TOP-TRENDS DER KOMMENDEN FÜNF JAHRE

DXC Technology berichtet über fünf Trends, die in den kommenden fünf Jahren die digitale Sicherheitslandschaft und damit das tägliche Leben und die Geschäftswelt verändern werden.

1. Das Cyber-Security-Wettrüsten wird Fahrt aufnehmen

Sowohl Cyber-Kriminelle als auch Cyber-Security-Experten werden künstliche Intelligenz (KI) in einem immer komplexeren Wettstreit einsetzen. Im Rahmen der Cyber-Abwehr wurde KI bisher vor allem zur Erkennung verdächtiger Verhaltensmuster eingesetzt. Aufgrund des Umfangs verdächtiger Hinweise und der Anzahl von Fehlalarmen sind die Cyber-Security-Spezialisten jedoch häufig überlastet. Die gute Nachricht: Künftig werden KI-basierte Sicherheitskontrollen und Reaktionsmechanismen automatisiert arbeiten und damit schneller und präziser auf Cyber-Angriffe reagieren. Das reduziert Ausfallzeiten und hilft dabei, persönliche und geschäftskritische Daten zu schützen.

2. Wir müssen umsichtig sein, mit wem wir GLAUBEN, im Metaversum zu sprechen

2023 wird ein wichtiges Jahr für das Metaversum werden. Meta, Microsoft, Virbela und andere setzen darauf, dass virtuelle Welten sich etablieren. Aktivitäten im Metaverse können jedoch Fragen zur Legitimität aufwerfen: Woher weiß man, dass die Person, mit der man zu sprechen glaubt, auch die ist, die sie vorgibt zu sein? Digitale Zertifikate, vielleicht auf Basis von Blockchain, könnten hier Abhilfe schaffen. Diese Zertifikate könnten auch verwendet werden, um virtuelle Transaktionen im Metaversum zu sichern. Sicher ist, dass mit der Ausdehnung des Metaversums auch die Risiken zunehmen werden.

3. Geopolitische Angriffe auf die Cyber-Sicherheit werden zunehmen

Der russische Angriff auf die Ukraine hat uns in aller Deutlichkeit vor Augen geführt, dass die Kriegsführung heute hybrid ist und die Risiken geopolitisch motivierter Cyberangriffe real sind. Infolgedessen werden jetzt viele Cyber-Versicherungspolicen so aufgesetzt, dass sie Cyber-Kriegshandlungen ausschließen. Das stellt eine Herausforderung für die Minimierung von Cyber-Risiken dar.

4. Cyber-Security-Angriffe werden sich gegen KRITIS richten, die unser Zuhause versorgen

Die Operational Technology (OT) ist ein zunehmend größeres Schlachtfeld für Cyber-Angriffe auf Systeme, die Fabriken oder zivile Infrastrukturen wie Kraftwerke und Staudämme steuern.

Angesichts der geopolitischen Spannungen wird die Cyber-Bedrohungslage in Bezug auf die OT im Jahr 2023 zunehmen. Dies setzt die Industrie unter Druck: Es gilt sicherzustellen, immer einen Schritt voraus zu sein, indem die Cyber-Security-Schutzmaßnahmen in die gesamten betrieblichen Abläufe integriert werden.

5. Die Karriere-Chancen im Bereich Cyber-Security werden zunehmen

Weltweit fehlen schätzungsweise 3,4 Millionen Fachkräfte im Cyber-Security-Bereich. Angesichts der wachsenden Bedrohungen durch fortschrittliche Technologien wird diese Zahl wahrscheinlich noch steigen.

Die Lücke bei den Cyber-Kompetenzen eröffnet Karrieremöglichkeiten für Menschen jeden Alters und jeder Herkunft.

www.dxc.com

Quelle: Kyocera Document Solutions

Effizientes Dokumentenmanagement als Hebel

WIE DIGITALE LÖSUNGEN GESCHÄFTSPROZESSE NACHHALTIG GESTALTEN KÖNNEN

Digitale Technologien unterstützen Unternehmen dabei, Prozesse flexibler, sicherer und schneller zu machen – aber auch die Umwelt zu schonen. Das Thema Nachhaltigkeit hat längst alle Branchen erfasst und gewinnt durch die steigenden Anforderungen von Kunden, Mitarbeitenden, Investoren und der Politik immer größere Bedeutung für den Alltag von Unternehmen. Das hat unmittelbaren Einfluss auf unzählige Entscheidungen.

Dabei spielt nicht nur das individuelle Umweltbewusstsein eine Rolle. Unternehmen werden immer häufiger auch mit Tatsachen konfrontiert, die den Schutz von Umwelt und Klima unabdinglich machen: Ressourcen werden knapper, Energie wird teurer und globale Lieferketten werden durch Krisen erschüttert. Hinzu kommen gesetzlichen Vorgabe, die von Unternehmen eine neutrale Umweltbilanz fordern. Innerhalb der europäischen Union muss das Netto-Null-Ziel bis 2050 erreicht werden. Die CO_2-Emissionen eines Unternehmens dürfen dann also nicht größer sein als die Menge, die durch Kompensationsmaßnahmen wieder entnommen werden kann.

Das bedeutet, dass schnellstmöglich Maßnahmen auf den Weg gebracht werden sollten, die die Auswirkungen der eigenen Geschäftstätigkeit auf die Umwelt reduzieren. Das setzt die Suche nach Innovationen und neuen Lösungen hoch oben auf die To-Do-Liste – nicht nur beim produzierenden Gewerbe.

Digitalisieren statt kompensieren

Kaum ein Unternehmen steht für sich allein, sondern setzt in der Regel auf eine teils komplexe Lieferkette, die sich ebenfalls in der Umweltbilanz niederschlägt. So muss ein Händler also auch den Energieverbrauch des Lieferanten berücksichtigen, ebenso wie den Treibstoffverbrauch beim Transport der Ware. Die gesamte Lieferkette ist also gefragt, Emissionen zu reduzieren.

Viele aufwendige Prozesse, die auf dem Weg von der Herstellung zum Kunden notwendig sind, lassen sich inzwischen digital abbilden und durch digitale Technologien beschleunigen. Die Automatisierung in der Produktion spielt dabei genauso eine Rolle wie die Unterstützung mobiler Arbeitskonzepte, die den Pendlerverkehr reduzieren. Damit lässt sich CO_2 einsparen – und muss nicht im Nachhinein kompensiert werden.

Informationsmanagement als wichtiger Hebel

Damit ganzheitliche Ansätze realisiert werden können, die wirklich einen Unterschied machen, werden digitale Arbeitsumfelder benötigt, die den effizienten und nachhaltigen Einsatz von Ressourcen ermöglichen. Hier sind intelligente Lösungen gefragt, die ineinandergreifen und vollständig digitale Geschäftsprozesse erlauben. Einer der größten Hebel ist hier das Informationsmanagement. Dokumente können digital bearbeitet und unterschrieben werden. Dass ein Manager Verträge am Bildschirm prüfen und signieren kann, ist längst kein Hexenwerk mehr. Mit digitalen Dokumentenmanagement-Lösungen wie dem Kyocera Workflow Manager können die digitalen Dokumente im Unternehmen einfach, effizient und nachhaltig verwaltet und vielfältige Prozesse angestoßen werden – alles ohne physische Umlaufmappen und aufwendigen Transport von A nach B.

Wer einen echten Beitrag zum Klimaschutz leisten und den eigenen CO_2-Fußabdruck verkleinern möchte, kann mit effizientem Dokumentenmanagement die Grundlage für digitale Geschäftsprozesse schaffen und Emissionen vermeiden. Das gilt nicht nur für große Unternehmen, sondern auch für kleine Betriebe und den Mittelstand.

www.kyoceradocumentsolutions.de

Modern Workplace

VIER FRAGEN, DIE UNTERNEHMEN 2023 BESCHÄFTIGEN

Haben Sie schon den Königsweg für Ihr Unternehmen gefunden, wenn es um neue Arbeitsmodelle geht? 100 Prozent Büroarbeit, komplett remote oder irgendetwas dazwischen? Die Standardlösung gibt es hier oftmals nicht – denn Teams sind divers und unterliegen jeweils unterschiedlichen Arbeitsabläufen. Für Organisationen ist es darum wichtig Leitplanken vorzugeben, die Flexibilität zulassen – und sich mit den neuen Entwicklungen gezielt auseinanderzusetzen. Denn die neue Arbeitswelt bedeutet eben auch, agil auf sich verändernde Anforderungen reagieren zu können. Wie sehen aktuelle Trends im Bereich Modern Workplace aus und wie entwickelt sich die Zukunft der Arbeit weiter? Was sind in diesem Umfeld die wichtigsten Fragen für das neue Jahr?

#1 Remote Work – die Zukunft oder ein Auslaufmodell?

Remote Work ist aus unserer Arbeitswelt nicht mehr wegzudenken. Oder? Immer wieder wird in den Medien heiß diskutiert, dass einzelne namhafte Konzerne ihre Mitarbeitenden ins Büro zurückrufen. Dabei heben verschiedene Untersuchungen die Vorteile von Remote Work hervor. So bestätigt beispielsweise die Studie „Homeoffice Experience 2.0" des Verbundforschungsprojekts Office 21 des Fraunhofer IAO, dass die gefühlte Produktivität im Homeoffice steigt. 44 Prozent der befragten Personen gaben an, im Homeoffice produktiver zu arbeiten – dem gegenüber stehen 30 Prozent, die im Büro effizienter arbeiten. Die restlichen 26 Prozent machen keinen Unterschied. Der Work Trend Index von Microsoft zeigt, dass leitende Angestellte und Mitarbeitende die Produktivität im Homeoffice unterschiedlich wahrnehmen: 85 Prozent der Führungskräfte gaben hier an, dass es im Zuge von Hybrid Work schwierig sei, darauf zu vertrauen, dass Mitarbeitende im Homeoffice pro-

PRODUKTIVITÄT IM HOMEOFFICE

duktiv sind. 87 Prozent der Angestellten betonen jedoch, dass sie produktiv seien – und einen guten Grund dafür brauchten, um wieder ins Büro zurückzukehren. Die Erwartungen des Unternehmens reichten als Motiv dafür nicht aus.

Diese Untersuchungen verdeutlichen, wie wichtig flexible Remote-Work-Modelle für Unternehmen sind. Die flexible Arbeitsplatz- und oftmals auch Arbeitszeiteinteilung bringt große Mehrwerte: Mitarbeitende können Privates und Berufliches besser verbinden. Das steigert nicht nur die Attraktivität der Arbeitgeber, sondern auch die Zufriedenheit der Mitarbeitenden – und somit letztlich die Produktivität im Unternehmen. Junge Talente suchen außerdem gezielt Unternehmen, die flexible Arbeitsgestaltung ermöglichen. Ein wichtiger Punkt im Zeitalter des Fachkräftemangels.

DIE NEUE ARBEITSWELT BEDEUTET AUCH, AGIL AUF SICH VERÄNDERNDE ANFORDERUNGEN REAGIEREN ZU KÖNNEN.

Christian Malzacher,
Business Manager, Bechtle AG,
www.bechtle.com

#2 Arbeitszeit versus Ergebnisse. Welches Modell hat Zukunft?

Hat die 40-Stunden-Woche ausgedient? Unternehmen sollten sich zumindest die Frage offen stellen, ob Arbeit (ausschließlich) in geleisteter Zeit gemessen werden kann. Gerade in einer flexiblen, hybriden Arbeitswelt wird Transparenz immer wichtiger: Die Mitarbeitenden müssen wissen, wer im Team welche Aufgaben übernimmt, auf welche Ziele das Team hinarbeitet und welchen Beitrag jede einzelne Person dazu leistet, diese zu erfüllen. Klar wird, dass es nicht mehr allein auf die Arbeitszeit ankommt – sondern auf das Ergebnis der geleisteten Arbeit.

Teams können hier beispielsweise dazu übergehen, Rollen- statt Stellenbeschreibungen zu nutzen – und damit gezielt Aufgabenpakete offenzulegen. Rollen schaffen mehr Transparenz, was die Aufgabenverteilung angeht. Sie sind nicht mehr zwingend an eine Person gekoppelt und können nach Bedarf flexibel angepasst werden. Darüber hinaus sind Rollenwechsel jederzeit möglich, sodass Unternehmen Arbeitsspitzen und neue Bedarfssituationen besser und schneller abdecken können.

#3 Mindset oder Technik – auf was kommt es an?

Ihr Team kann auf neue, moderne Tools zugreifen – doch niemand nutzt sie? Immer wieder stehen Organisationen vor Herausforderungen, wenn es um Veränderungen geht. Zwar haben die meisten Mitarbeitenden die benötigte technische Ausstattung, um von überall arbeiten zu können. Mangelt es aber am erforderlichen Mindset, scheitern Projekte schnell. So kann keine Organisation „einfach so" von heute auf morgen hybrid arbeiten. Denn auch hier bedarf es Leitplanken, an denen sich Teams orientieren und entlang derer sie ihre eigenen, teaminternen Regeln aufstellen. Ein Umdenken in Sachen Führung, aber auch Teamarbeit ist hier gefragt. Transparenz und Kommunikation sind wichtige Grundlagen, damit eine Zusammenarbeit über Standortgrenzen hinweg funktioniert. Zusätzlich bereichern Punkte wie wertschätzendes Feedback und eine offene Fehlerkultur die hybride Arbeitswelt und bringen Teams voran.

Wenn es um die Einführung neuer Prozesse und technischer Lösungen im Unternehmen geht, ist es darüber hinaus wichtig, die Faktoren Change Management und User Adoption von Anfang an mitzudenken. Denn neue Lösungen müssen verstanden und genutzt werden – nur so steigern Unternehmen am Ende die Effizienz und Produktivität der Mitarbeitenden. Die notwendige Technik und das Verständnis der Menschen dahinter müssen somit Hand in Hand gehen. Hier bedarf es eines strukturierten Ansatzes sowie einer genauen Planung – und zwar im Vorfeld.

#4 Ersetzen Leitplanken starre Regeln?

Immer mehr Unternehmen gehen dazu über, ihren Mitarbeitenden mehr Freiräume zu geben. Agile Teams, die sich selbst organisieren, arbeiten in vielen Situationen schneller und flexibler. Starre Regeln sind hier fehl am Platz, denn sie zwängen Teams in ein enges Korsett. Dennoch braucht es Anhaltspunkte, an denen sich die Mitarbeitenden orientieren können.

Die Führungskräfte müssen den Teams Rahmenbedingungen vorgeben, in denen sich die Mitarbeitenden selbst organisieren. Darüber hinaus brauchen Teams eine klare Strategie, die sie am besten zusammen in Workshops erarbeiten. Diese muss stetig überprüft und bei Bedarf nachgebessert werden. Wichtig ist hier, dass sich Unternehmen mit dem Thema „agile Teams" auseinandersetzen und entsprechende Arbeitsmodelle dort zum Tragen kommen, wo Mehrwerte entstehen. Denn letztlich ist Flexibilität das Mittel der Wahl, um den Herausforderungen einer volatilen Arbeitswelt zu begegnen.

Gehen Sie den Wandel mit einem starken Partner an.
Alle Trends und Möglichkeiten rund um den modernen Arbeitsplatz im Blick zu

MEHR WERT

Homeoffice Experience 2.0
www.bit.ly/3Wly0qD

Hybrid Work ist just Work
www.bit.ly/3iSsX3y

behalten, ist für viele Unternehmen herausfordernd. Darum begleiten wir Sie auf Ihrer Reise hin zum Modern Workplace und haben dabei die sechs Säulen der modernen Arbeitswelt im Blick:

- **Modern Meeting:** Die User Experience steht beim Thema Meeting im Mittelpunkt – hier kommt es auf die passende Ausstattung der Meeting-Räume genauso an wie auf die Plattform, um standortübergreifende Meetings in agilen Teams zu ermöglichen.
- **Modern Communication:** Unified Communication macht es Ihrem Team so einfach wie möglich, in Kontakt zu bleiben – auch in hybriden Arbeitssituationen.
- **Digitales Büro:** Schaffen Sie einen zusammenhängenden, digital zugänglichen Arbeitsplatz. Ihr Team kann auf alle Infos und Tools einfach zugreifen – das erhöht die Produktivität und steigert die Zufriedenheit der Mitarbeitenden.
- **Extended Reality:** Ob in der Produktion, bei Schulungen und Trainings oder in der Logistik: Augmented-Reality- und Virtual-Reality-Lösungen sorgen für Interaktivität und ermöglichen modernes, produktives Arbeiten.
- **Modern Deployment und Management:** Durch cloudnatives Gerätemanagement und cloudnative Geräteverwaltung machen Sie Ihre Mitarbeitenden schnell arbeitsfähig und entlasten zusätzlich Ihre IT-Abteilung.
- **Change Management und User Adoption:** Involvieren Sie Ihre Mitarbeitenden von Anfang an strategisch durchdacht in Veränderungsprozesse – so wird Ihr Modern Workplace auf Dauer zum Erfolg.
- **Ihr Vorteil ist unser holistisches Vorgehen:** Wir verbinden unseren strategischen Ansatz mit den passenden Tools und Technologien – und holen stets Ihr Team mit ins Boot. Dabei beleuchten wir mit Ihnen den Status quo in Ihrem Unternehmen, legen individuelle Ziele fest und begleiten Sie durch den gesamten Transformationsprozess – und auch darüber hinaus. Eine durchdachte Strategie und ein detaillierter Fahrplan sind die Schlüssel zu Ihrem Erfolg. Bringen Sie Ihr Unternehmen hin zu einem modernen Arbeitsplatz, bei dem sich Ihre Mitarbeitenden voll entfalten können – und steigern Sie so Ihre Attraktivität als Arbeitgeber und die Produktivität Ihrer Teams.

Christian Malzacher

STÖRUNGEN UND FLOW-ERLEBNIS

SKALA: 1 – STIMME ÜBERHAUPT NICHT ZU , 5– STIMME VOLL UND GANZ ZU

Quelle für beide Grafiken:"
Homeoffice Experience 2.0", Verbundforschungsprojekts
Office 21 des Fraunhofer IAO

Trends der elektronischen Zeiterfassung

VERTRAUENSARBEITSZEIT WIRD DURCH MOBILE ZEITERFASSUNGS-APPS ABGELÖST

Mit der elektronischen Zeiterfassung müssen sich Unternehmen bereits seit dem EuGH-Urteil im Frühjahr 2019 befassen. Das deutsche Bundesarbeitsgericht hat im September letzten Jahres noch einmal die Dringlichkeit der Umsetzung betont und die Verpflichtung ausgesprochen, die tägliche Arbeitszeit zu erfassen; jetzt ist der Moment gekommen, dass diese Verpflichtung unstrittig ist. Folgende Trends zeichnen sich ab:

1. Boom mobiler Zeiterfassungs-Apps

Die durch die Corona-Pandemie grundlegend veränderte Arbeitswelt und die zunehmende Etablierung des Homeoffice bringen neue Anforderungen an die Erfassung der Arbeitszeit mit sich. Da ein fortschreibendes Arbeitszeitkonto für jeden Arbeitnehmer verpflichtend ist und Unternehmen es tunlichst vermeiden wollen, in die Lohnschuldfalle zu geraten, ist für das Jahr 2023 eine starke Zunahme mobiler Zeiterfassungssysteme zu erwarten. Sie bieten ein Maximum an Flexibilität und sind in der Lage sowohl am klassischen Arbeitsplatz als auch im Homeoffice die Arbeitszeiten zu erfassen. Da der Markt bereits über zahlreiche mobile Zeiterfassungssysteme verfügt, können sich die Unternehmen die Lösung aussuchen, die zu den eigenen Anforderungen am besten passt. Herkömmliches Stempeln und erst recht die traditionelle Vertrauensarbeitszeit werden zeitnah der Vergangenheit angehören.

2. Fullservice-Lösungen gehört die Zukunft

Bei der elektronischen Zeiterfassung wird der lückenlose Datenaustausch zwischen den Systemen an Bedeutung gewinnen. Sobald die Arbeitszeiten einmal digital erfasst sind, richtet sich der Fokus darauf, wie man die darin enthaltenen Informationen möglichst unkompliziert und automatisiert nutzen kann. Es geht darum, beispielsweise Überstunden zu reduzieren, Schichtpläne zu optimieren oder Urlaubsanträge besser zu koordinieren. Vor allem aber wird die digitale Verbindung zwischen Zeiterfassung und Lohnabrechnung immer mehr an Bedeutung gewinnen. Elektronische Zeiterfassungssysteme, welche die entsprechenden Schnittstellen haben sowie eine moderne Personaleinsatzplanung und Lohnabrechnung (digitaler Lohnzettel) unterstützen, werden im kommenden Jahr verstärkt zum Einsatz kommen. Der Kunde wünscht sich alles aus einer Hand.

3. Lückenlose Arbeitszeitdokumentation wird immer wichtiger

Nicht zuletzt weiß jeder, der in Zeiten der Corona-Pandemie Kurzarbeitergeld beantragt hat, wie wichtig die minutengenaue Dokumentation der Arbeitszeiten ist, zumal das Kurzarbeitergeld bis zum 31.12.2025 noch rückwirkend geprüft werden kann. Aber auch gegenüber dem Zoll, dem Finanzamt oder der Sozialversicherung sind Arbeitgeber dazu verpflichtet, bis ins Detail die Arbeitszeiten ihren Angestellten dokumentieren zu können. Jeder Unternehmer muss den Schritt in Richtung einer digitalen Zeiterfassung gehen, insbesondere, wenn er die Prüfungen bisher eher als undurchsichtiges Glückspiel empfunden hat. Je genauer die Arbeitszeitdarstellung ist und je einfacher die Erstellung sowie Handhabung eines solchen Reportings ist, desto intensiver wird die entsprechende Zeiterfassungslösung genutzt werden.

www.eurodata.de

Cyberangriffe auf die Lieferkette?

CYBERSICHERHEITSSTRATEGIE ÜBERDENKEN!

Die Digitalisierung in allen Bereichen des privaten wie auch geschäftlichen Lebens sowie die daraus resultierenden digitalen Verbindungen vergrößern die Angriffsfläche für Cyberkriminelle. So warnte auch das BSI in seinem Lagebericht zur IT-Sicherheit in Deutschland 2020 [1] vor einer stark zunehmenden Zahl von Angriffen auf die IT-Infrastruktur. Noch vor einigen Jahren kam dem Thema Cybersicherheit innerhalb der Lieferkette nicht allzu viel Bedeutung zu. Das hat sich jedoch mit dem Bekanntwerden großer Cyberangriffe geändert, denn diese haben gezeigt, wie anfällig internationale und nationale Lieferketten sind.

Trotzdem räumen Unternehmen dem Thema Cybersicherheit noch immer zu wenig Priorität ein. Das bestätigt eine aktuelle Kaspersky-Umfrage unter Entscheidern in Unternehmen in Deutschland. Cybersicherheit findet kaum Beachtung als Teil des Supply-Chain-Risiko-Managements – schlimmer noch: Entscheider haben dem Thema in den vergangenen Monaten noch weniger Bedeutung zugeschrieben als zuvor. Das ist durchaus paradox, da ein Viertel der mittelständischen und weit mehr als die Hälfte der großen Unternehmen eigenen Angaben zufolge mehr Cyberangriffen ausgesetzt waren.

Finanzielle Auswirkungen, Reputationsverlust, mangelhafte Produkte

Unternehmensentscheider sind sich der Auswirkungen eines erfolgreichen Angriffs bewusst. Denn drei Viertel aller Entscheider in Unternehmen – unabhängig von deren Größe – gehen davon aus, dass sie als Resultat eines erfolgreichen Angriffs das Vertrauen ihrer Kunden verlieren könnten. Darüber hinaus befürchten sie, dass ihre Reputation in Mitleidenschaft gezogen würde (64 Prozent der mittelständischen und 81 Prozent der großen Unternehmen) und sie sich rechtlichen Konsequenzen stellen müssten (66 Prozent der kleinen und 72 Prozent der großen Unternehmen), die sich beispielsweise aus der DSGVO ergeben.

All diese Faktoren sowie die Lieferung mangelhafter Produkte oder gar eine vollständige Unterbrechung der Produktion könnten sich schlussendlich auch auf die Beziehung zu Partnern und die Geschäftstätigkeit auswirken. So fürchten 60 Prozent der kleinen Unternehmen und 74 Prozent der Großunternehmen, dass sie im Falle eines Angriffs Partner verlieren könnten. Des Weiteren fürchten drei Viertel der Unternehmen, dass ein erfolgreicher Angriff finanzielle Auswirkungen haben könnte.

Unternehmen schützen aus den falschen Gründen

Obwohl viele Unternehmen Cybersicherheitslösungen – und der Großteil auch Threat Intelligence – einsetzen, scheinen Entscheider vor allem auf die gute Zusammenarbeit mit Partnern zu setzen. Denn nur rund drei Viertel sowohl der kleinen als auch der großen Unternehmen sind überzeugt, alle Schnittstellen und Zugriffe von Partnern ausreichend zu überwachen. Der Rest scheint auf die Vernunft ihrer Partner zu vertrauen. Dabei sind zu lasche Cybersicherheitsmaßnahmen problematisch, weil längst nicht alle Unternehmen auf Backups setzen, die den Zugriff auf Daten im Falle eines Angriffs ermöglichen würden. Denn in Deutschland sind lediglich die Hälfte (50 beziehungsweise 46 Prozent) der IT-Entscheider mittelständischer und großer Unternehmen davon überzeugt, dass in ihrem Betrieb Backups vorhanden seien.

Weiter zeigt die Kaspersky-Studie interessante Ergebnisse hinsichtlich der Hauptgründe, weshalb überhaupt Cyberschutzmaßnahmen implementiert werden. Denn diese haben wenig damit zu tun, was IT-Entscheider im Falle eines Angriffs tatsächlich befürchten. Während die meisten Cybersicherheitsmaßnahmen wählen, um ihre Daten und Kunden zu schützen sowie die Geschäftskontinuität zu ge-

währleisten, vernachlässigen viele ihr Bauchgefühl, das sich vor allem um finanzielle Schäden, Reputationsverlust sowie den Verlust von Kundenvertrauen als mögliche Auswirkungen eines erfolgreichen Cyberangriffs sorgt.

Wie sich Unternehmen umfassend schützen können

Die Umfrage zeigt eine Diskrepanz zwischen den befürchteten Auswirkungen und den Hauptgründen, warum Entscheider letztlich Cybersicherheitsmaßnahmen ergreifen. Dabei sollten sich Entscheider lieber auf ihr Bauchgefühl verlassen und auch das schützen, was ihnen am meisten Sorgen bereitet. Am besten setzen sie auf einen mehrschichtigen Cybersicherheitsansatz. Dieser sollte sowohl technische Lösungen, die sämtliche Server, Arbeitsstationen, Smartphones, Tablets und andere Geräte schützen, umfassen – zum Beispiel Kaspersky Endpoint Detection and Response [2] – als auch Experten-Services. Dazu gehören unter anderem Dienste für Threat Intelligence sowie Managed Services, die – auch bei internem Ressourcenmangel hinsichtlich Finanzen und/oder Mitarbeitern – umfassend schützen. Umfangreiche und stets aktuelle Bedrohungsinformationen ermöglichen es Unternehmen, über Tools, Techniken und Taktiken von Bedrohungsakteuren auf dem Laufenden zu bleiben und so potenzielle Risiken zu antizipieren. Hinzu kommt eine Backup-Strategie, die die regelmäßige Sicherung aller Daten vorsieht, so dass Unternehmen im Falle eines Angriffs Zugriff auf diese haben.

Neben diesem klassischen Ansatz sollte im Unternehmen klar definiert sein, wer mit wem zusammenarbeitet, um potenzielle Lücken zu entdecken und Risiken zu mindern. Dabei hilft eine ausführliche Liste aller Lieferanten und Partner: Wer hat Zugriff auf unternehmensinterne Daten? Wer auf die IT-Infrastruktur? Des Weiteren sollten die Sicherheitsmaßnahmen durch ein umfangreiches Audit bewertet werden. Denn nur so lässt sich erkennen, welche Bereiche und Schnittstellen weitere Schutzmaßnahmen benötigen. Unternehmen sollten darauf achten, dass ihre Lieferanten und Partner zertifizierte Sicherheitsmaßnahmen implementiert haben – beispielsweise eine Zertifizierung nach ISO 27001 oder ein bestandenes SOC2-Audit. Denn diese bestätigen, dass Maßnahmen zum Schutz von Daten und Systemen ergriffen und adäquat eingesetzt werden.

Waldemar Bergstreiser
www.kaspersky.de

Quellen:
[1] https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/Lagebericht2020.pdf?__blob=publicationFile&v=2
[2] https://www.kaspersky.de/enterprise-security/endpoint-detection-response-edr

Erhöhte Cybergefahr

STEIGENDES RISIKO DURCH SCHWINDENDE NETZWERKGRENZEN

Software-as-a-Service (SaaS) bietet Unternehmen große Vorteile. Ressourcen wie technische Ausstattungen, Räumlichkeiten, Know-how und Personal müssen nicht vorgehalten werden, es ist effizient und komfortabel. Aber: es entsteht damit auch ein ausgeweitetes Netzwerk, das mit klassischen Mitteln der IT-Security nicht mehr effizient abgesichert werden kann.

UM AUF CYBERANGRIFFE GUT VORBEREITET ZU SEIN, BRAUCHT ES HEUTE WEIT MEHR ALS EINE SECURITY-SOFTWARE PLUS FIREWALL.

Michael Veit, Security-Experte, Sophos, www.sophos.de

Um auf Cyberangriffe gut vorbereitet zu sein, braucht es heute weit mehr als eine Security-Software plus Firewall. Verschiedene Ansätze stehen der modernen Cybersicherheit hierbei zur Prävention vor Cybergefahren zur Verfügung. Je nach Unternehmensgröße, Budget und Mentalität lässt sich der existierende Schutz mit einer Strategie, Services und Technik inhouse oder mit externem Expertentum erweitern.

Vier Module haben sich bei der modernen IT-Sicherheit für Unternehmen etabliert: das Zero-Trust-Prinzip, ein integriertes und intelligent vernetztes Security-Ökosystem, ein zentrales Management sowie Managed Detection and Response Services. Und da es in einer vernetzten Welt nie einen hundertprozentigen Schutz geben wird, kommt dem Notfallplan eine entscheidende Bedeutung zu, um die Auswirkungen einer Cyberattacke schnell, sicher und mit möglichst geringem Schaden zu überwinden.

Zero Trust

Zero Trust ist eine Cybersecurity-Philosophie und -Architektur und fußt auf dem Prinzip: „Nichts und niemandem vertrauen, alles überprüfen". Dieser Ansatz bietet für Betriebe erheblich mehr Sicherheit als traditionelle Security-Konzepte: Alle Benutzer:innen und Geräte bilden ihren eigenen Perimeter in ihrem eigenen Mikro-Segment des Netzwerks. User:innen dürfen nur auf Anwendungen und Daten zugreifen, die explizit in den entsprechenden Richtlinien definiert sind. Dies minimiert Bewegungen im Netzwerk, so dass Cyberkriminelle, die sich über ein infiziertes Gerät oder illegal beschaffte Zugangsdaten Zugriff auf das gesamte Netz verschaffen wollen, keine Chance haben. Das Zero Trust-Modell bietet mehr Kontrolle über die gesamte IT-Umgebung, die Gleichbehandlung aller Anwender:innen, maximale Sicherheit für die Infrastrukturen und einen sehr effektiven Schutz gegen Malware und Angriffe.

Adaptives Cybersecurity Ecosystem

Das adaptive Cybersecurity Ecosystem, wie es Sophos anbietet, kombiniert die intelligente Automatisierung und Vernet-

zung der Security-Komponenten und die Einbeziehung menschlicher Expertise. Von der Notfallplanung über den präventiven Schutz mit Security-Technologie und Künstlicher Intelligenz bis hin zu menschengeführter Erkennung und Bekämpfung werden in diesem System alle Maßnahmen zentral koordiniert. Auf Basis von gesammelten Bedrohungsdaten und mit Hilfe von Künstlicher Intelligenz lernt das Ökosystem dabei kontinuierlich. Für Unternehmen liegt der entscheidende Vorteil darin, dass nicht einzelne Komponenten eingerichtet und verwaltet werden müssen, sondern sich alles über eine zentrale Oberfläche vom eigenen IT-Team (oder vertrautem externen Dienstleister als Managed Service) administrieren lässt.

Threat Hunting

Sogenanntes Threat Hunting durch ausgewiesene Spezialist:innen ist für die Abwehr der immer komplexer werdenden Cybergefahren essenziell. Kriminelle führen ihre Attacken oft über Wochen und Monate hinaus durch, teils manuell. Genau an diesem Punkt stoßen automatisierte Sicherheitsmechanismen an ihre Grenzen und es werden Expert:innen benötigt, um den Cyberkriminellen rechtzeitig auf die Schliche zu kommen. Hier gilt es abzuwägen, ob externe Expertendienste von ausgewiesenen Spezialisten-Teams unterstützen sollten, die in Kombination mit Machine-Learning-Technologien effektiv moderne Bedrohungen aufspüren können – und das rund um die Uhr.

Incident Response Plan

Ein Incident Response Plan kann Unternehmen maßgeblich dabei helfen, bei einer Cyberattacke die Kontrolle zu behalten, die Folgen eines Cyberangriffs zu minimieren und viele weitere Probleme bis hin zu Betriebsunterbrechungen im Keim zu ersticken. Auch hier können externe Dienstleister wie MDR-Provider (Managed Detection and Response) hilfreich sein. Sie bieten 24/7 Threat Hunting, Analysen und Reaktion auf Vorfälle als Managed Service.

Fazit

Für Unternehmen liegt die Aufgabe zu umfassendem Schutz vor Cyberkriminellen darin, alle neuen Aspekte der Security kontinuierlich und weitgehend zu automatisieren, in die Schutzinfrastruktur zu integrieren und durch menschliche Kompetenz und Expertise eine stetig wachsende Wissensbasis unter einem integrierten Schutzschirm aufzubauen.

Michael Veit

Das **eBook** umfasst 46 Seiten und steht zum kostenlosen Download bereit.
www.it-daily.net/download

STORAGE

WHAT`S NEW?

Daten entwickeln sich in der modernen digitalen Wirtschaft zur wichtigsten Währung. Gleichzeitig steigen Kosten, Komplexität und Bedrohungen für die Datensicherung. Ein effizienter Schutz der Daten tut Not, unabhängig davon soll der Nutz- und Mehrwert dieser „Assets" als Active Archive voll ausgeschöpft werden.

Das Backup hat sich zu einer existentiellen Anforderung für Unternehmen in der digitalen Transformation und angesichts der bekannten Cyber-Bedrohungen entwickelt. Doch wie sieht die Zukunft des Backups aus? Diese und weitere Fragen werden im eBook „Storage: What`s new?" beantwortet.

Weitere Artikel aus dem eBook

- Storage-Strategie: Der richtige Mix macht`s
- PPR: Prevention, Protection & Recovery
- Zukunftssichere Speicherinfrastrukturen
- Always on: Unveränderbare Snapshots

Transformation: Hybrid Heroes gesucht

DER MITTELSTAND BRAUCHT TRANSFORMIERER

Um die digitale Transformation in Gang zu setzen, werden Netzwerk- und IT-Sicherheitsteams mit den Anforderungen aus dem Geschäftsbetrieb konfrontiert. In der Folge ist eine komplette Neuausrichtung von zentralen Netzwerk- und Security-Komponenten erforderlich. Damit gehen ganz neue Aufgaben außerhalb der klassischen IT einher, mit denen sich gerade mittelständische Unternehmen noch schwer tun. Ihnen fehlen die dafür nötigen treibenden Kräfte im Unternehmen. Diese „Transformatoren" bringen neben dem strategischen Weitblick für die Geschäftsentwicklung auch das technische Know-How für die Einleitung von Veränderungsprozessen mit sich. Nur damit lässt sich letztendlich ein ausgewogenes Verhältnis von IT-Sicherheit, Performance und Kostentransparenz für eine digitalisierte Infrastruktur erreichen.

Jede Transformation von Abläufen und Verantwortlichkeiten als Folge infrastruktureller Veränderung erfordert einen sensiblen Balanceakt zwischen alten und neuen Welten. Unternehmen, die diesen Weg in die Transformation erfolgreich beschritten haben, waren in der Lage, zwischen IT-gesteuerten Modernisierungsbestrebungen und dem Management zu vermitteln. Sie konnten gleichzeitig die Ängste vor Veränderungen in den vorhandenen „Fürstentümern" überwinden. Denn bei jeder Transformation prallen Zielkonflikte aus verschiedenen Abteilungen aufeinander. Um diese Konflikte zu lösen, hilft eine klare strategische Ausrichtung auf die Kernbereiche des Unternehmens und die Kommunikation des Unternehmensziels quer über alle beteiligten Parteien. Denn ein Netzwerker, der das Unternehmensziel nicht kennt, kann nicht wie ein Unternehmer handeln und wird die Veränderung behindern.

Voraussetzungen für die Transformation

Für eine grundlegende Neuausrichtung der IT-Infrastruktur muss zunächst ein Problembewusstsein für den geplanten Wandel vorhanden sein. Dafür ist einerseits das Verständnis für die vorhandene Infrastruktur und deren Schwächen erforderlich, ebenso wie der strategische Weitblick mit einem klaren Zielbild, um Veränderungen auf den Weg zu bringen. Sind die Probleme genau definiert, lassen sich alternative Lösungsansätze skizzieren und deren Vorteile vermitteln. Um sich auf diese Reise zu begeben, benötigt das Unternehmen Transformatoren, die den Wandel in Gang setzen. Man könnte diese Funktion auch als Hybrid Hero be-

zeichnen, denn ein solcher fühlt sich sowohl in der alten Hardware-basierten IT-Umgebung zuhause als auch in der neuen Cloud-basierten Welt.

Die Suche nach einer solchen vermittelnden Funktion im Unternehmen, die die Transformation auf den Weg bringt, sollte in der IT-Abteilung begonnen werden. Dort ist der Druck besonders hoch, so dass ein Interesse an positiven Weiterentwicklungen besteht. Gerade in mittelständischen Unternehmen findet sich eine historisch gewachsene IT- und Netzwerkinfrastruktur, die über die Jahre an Komplexität gewonnen hat. Der Verwaltungsaufwand wächst mit jeder neuen Appliance im Ökosystem, die gewartet und gepatcht werden muss. Aufgrund des Fachkräftemangels steht die leitende IT-Funktion unter dem Druck, die nötige Administration mit einer dünnen Personaldecke in Einklang zu bringen und dabei die IT-Sicherheit nicht zu vernachlässigen.

Der Vermittler zwischen alter und neuer Welt muss zunächst als Zukunfts-Champion auftreten und die Vision für eine erfolgreiche Transformation verkaufen können. Er ist ein Profi auf dem Gebiet der bestehenden Infrastruktur und ist sich dennoch deren Limitierungen bewusst. Er hat Einblick in oftmals historisch gewachsene Infrastrukturen und ältere Anwendungen, die nicht vollständig migriert wurden. Er kennt die Unzufriedenheit mit Produkten, die nicht die gewünschte Funktionalität abbilden, ebenso wie die Workarounds, die im Unternehmen geschaffen wurden. Andererseits sieht er die Vorteile der Cloud und hat ein Verständnis dafür, wie sich die Geschäftsziele mit einem infrastrukturellen Umbau erreichen lassen.

Ein solcher Champion hat die schlechten Erfahrungen aus der Anfangsphase der Cloud bereits hinter sich gelassen. Er denkt nicht mehr in der Kategorie, dass die Cloud aus Gründen der mangelnden Nachvollziehbarkeit ein undurchdringlicher Ort ist, wo die Daten vorgehalten werden. Er hat sich mit der Thematik der Rechtssicherheit der Daten in der Cloud auseinandergesetzt und kann die Risiken und Vorteile gegeneinander abwägen. Cloud-Lösungen sind zwischenzeitlich so weit gereift, dass die Vorteile beispielsweise Zero Trust basierter Sicherheit aus der Cloud in den Vordergrund rücken für die Absicherung der Datenströme zwischen mobilen Anwendern und der Vorhaltung von Applikationen in Multicloud-Umgebungen.

Die Denkweise muss sich ändern

Das Ziel des Champions ist die Ablösung der vorhandenen Infrastruktur. Er ist mutig genug, einen Greenfield-Ansatz voranzutreiben, der mit der unternehmerischen Roadmap und langfristiger Vision in Einklang steht. Denn er ist sich bewusst, dass die Zeiten des lokalen Netzwerkbetriebs der Vergangenheit angehören, wenn sich ein Unternehmen für die Digitalisierung öffnen möchte. Das Internet hat das Unternehmensnetz abgelöst und die Cloud tritt als neues Rechenzentrum für die Vorhaltung von Anwendungen und Daten an. Da diese Wahrnehmung der Realität gerade bei den Verwaltern der existierenden Infrastruktur noch nicht angekommen ist, muss der Transformator zuerst einmal die angestammte Denkweise auf den Kopf stellen.

Anstelle des parallelen Betriebs von alten und neuen Infrastrukturen sollte die ganzheitliche Transformation in den Vordergrund treten, die von Netzwerkteams, Sicherheits-Teams und den Fachabteilungen für die Anwendungen gleichermaßen getragen wird. Oftmals gelingt Unternehmen zwar der Sprung in die Cloud für ihre Anwendungen, allerdings tun sie sich sehr viel schwerer damit, nicht mehr benötigte Infrastrukturen vom Netz zu nehmen. Der Transformierer muss sich also durchsetzen, alte Infrastruktur nicht als Rückfallebene beizubehalten, auch wenn sie noch so kostenintensiv in der Anschaffung war. Denn er weiß, dass durch ungepatchte Appliances in seiner IT-Umgebung lediglich Sicherheitslücken entstehen, wenn den Geräten nicht mehr die nötige Aufmerksamkeit für die Wartung zukommt. Durch die Einführung von Cloud-basierten Lö-

DIE FOLGENDEN VORAUSSETZUNGEN SOLLTE EIN TRANSFORMIERER BESITZEN:

- Verfügt über hohes Verständnis für Technik und ist zeitgleich in der Lage, wie ein Vorstand zu denken
- Bringt den Mindset mit, sich selbst und seinen Tätigkeitsbereich zu hinterfragen und zu erneuern
- Ist mit der technischen Entwicklung groß geworden und kann sich dementsprechend mit Erfahrungswerten verkaufen
- Erkennt, wenn die vorhandenen Lösungsansätze an ihre Grenzen stoßen
- Bringt die Neugier für die Evaluation innovativer Lösungsansätze mit und hat eine Vorstellung, wie Innovationen das Unternehmen verbessern können
- Schafft die schwierige Balance zwischen IT- Aufgaben und der Identifikation mit den übergeordneten Unternehmenszielen und verhilft damit der IT zu strategischer Bedeutung

sungen kann er der gesamten Infrastruktur die Komplexität nehmen.

Wo finden sich Transformierer?

Auf der Suche nach dem Champion, der Veränderungsprozesse erfolgreich in Gang setzt, wird ein Unternehmen oftmals in den eigenen Reihen fündig. Einerseits kann der klassische Teamleiter an einer Weiterentwicklung Richtung Cloud Interesse haben. Er hat zwar die fachliche Expertise zu internen Strukturen, hat bisher aber keine Management-Verantwortung. Als Champion kennt er die Limitierungen der vorhandenen Infrastruktur und hat die Zeichen der Zeit erkannt, auf die Cloud zu setzen. Eine andere Option für das Zugpferd der Transformation lässt sich in den Reihen der zweiten Führungsebene finden. Hier ist das Wissen um die Strategie zur Geschäftsentwicklung vorhanden, und in aller Regel bringt die Funktion die Fähigkeiten mit, die Visionen als Kommunikator intern zu vermitteln.

Unternehmen muss darüber hinaus bewusst sein, dass sie für das nötige Change-Management einer Transformation bereit sein müssen, neue Rollen zu schaffen. Diese befinden sich jenseits der traditionellen Karrierelinien-Hierachie. Sonderrollen, die die fachliche Autorität mit sich bringen, sind erforderlich, um die Hebel in Bewegung zu setzen.

Fazit

Für eine grundlegende Neuausrichtung der IT-Infrastruktur hat die Erfahrung gezeigt, dass die Vorteile einer Transformation auf verschiedenen Ebenen vermittelt werden müssen. Dafür ist das Verständnis für die vorhandene Infrastruktur und deren Schwächen ebenso erforderlich wie der strategische Weitblick, um Veränderungen einzuläuten. Ein Hybrid Hero als Transformierer hat die Aufgabe, zwischen den Ansprüchen aus den Lagern des Managements und der IT zu vermitteln und zu einem Konsens zu kommen. Er muss dazu in einem ersten Schritt Überzeugungsarbeit in den zwischengeschalteten IT-Funktionen leisten und dazu von allen Bereichen als fachliche Autorität im Transformationsprozess anerkannt werden. Letztlich muss es ihm gelingen, die IT als Follower für den Transformationsprozess zu gewinnen. Denn diese Abteilung muss das Day-to-Day-Business aufrechterhalten und zeitgleich die neue Strategie umsetzen.

Florian Rutsch

DER VERMITTLER ZWISCHEN ALTER UND NEUER WELT MUSS ZUNÄCHST ALS ZUKUNFTS-CHAMPION AUFTRETEN UND DIE VISION FÜR EINE ERFOLGREICHE TRANSFORMATION VERKAUFEN KÖNNEN.

Florian Rutsch, Solution Architect, Zscaler, www.zscaler.de

SAVE THE DATE

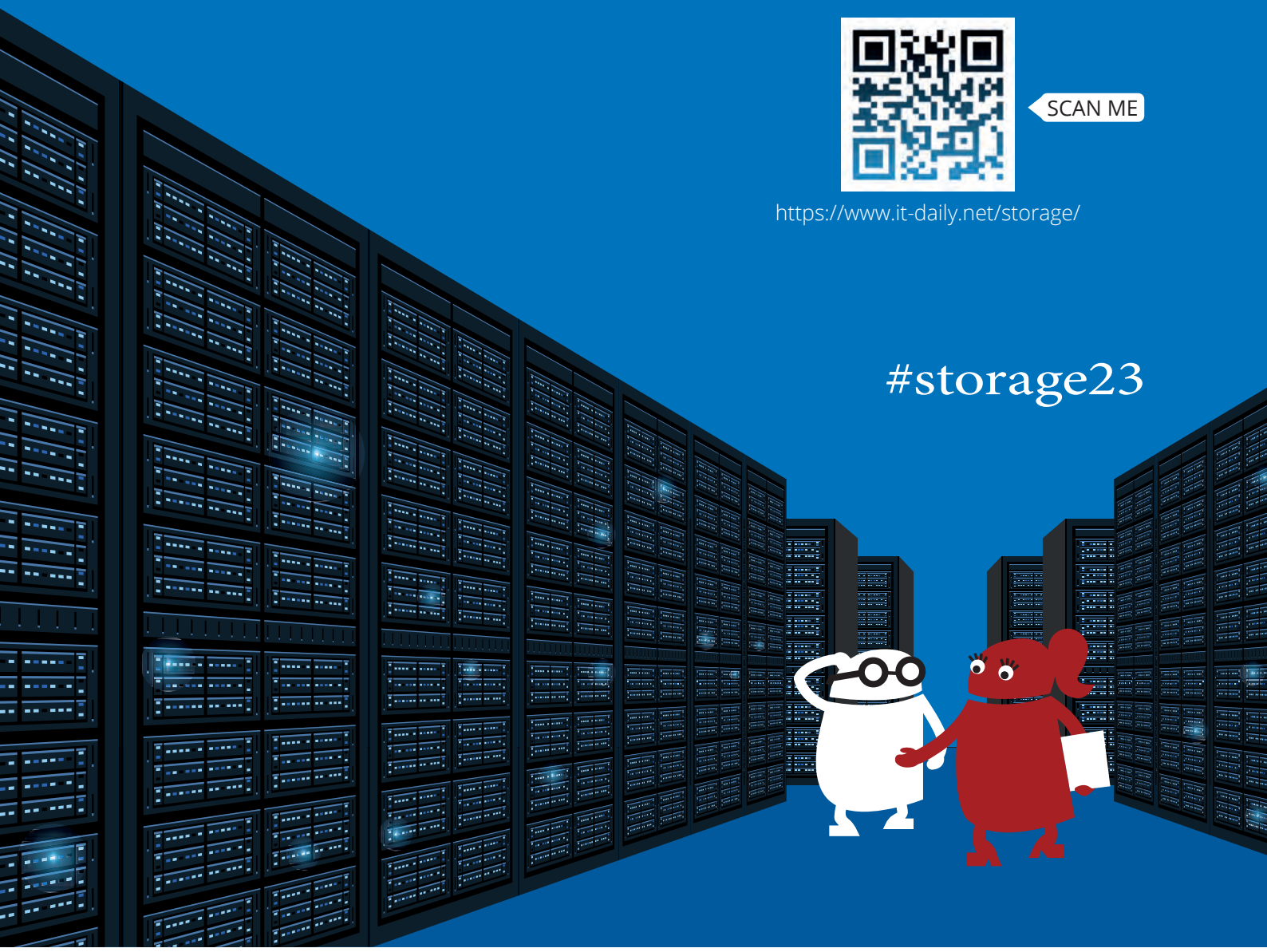
Data Protection & Storage

30. März 2023 | Digitalevent

SCAN ME

https://www.it-daily.net/storage/

#storage23



Eine Veranstaltung von itmanagement & speicherguide.de Das Storage-Magazin powered by it-daily.net

Do-It-Yourself-Cloud-Analysen

DAS JAHR DES DURCHBRUCHS?

Datenanalysen und Cloud Computing sind schon seit Jahren der Erfolgsmotor für Unternehmen. Viele wichtige Unternehmensdaten bleiben jedoch immer noch ungenutzt, was vor allem an historisch gewachsenen Bedingungen und veralteten Strategien in den Unternehmen selbst liegt. Die aktuelle wirtschaftliche Lage treibt die Notwendigkeit für Cloud Computing – und insbesondere der Analyse von Daten über die Cloud – weiter an.

Gerade jetzt, wo Unternehmen versuchen, „mit weniger mehr zu erreichen", heißt es für sie auch, alle vorhandenen Ressourcen zu nutzen und ganz nach dem Motto „Do it yourself" (DIY) ihren Mitarbeitenden die Möglichkeit zu geben, Unternehmensdaten selbstständig zu analysieren. Mit der Einbeziehung der Cloud könnte 2023 das wichtigste Jahr dafür sein, DIY-Cloud-Analysen im gesamten Unternehmen einzuführen.

Die Cloud stand bei Expert:innen, Analyst:innen und Geschäftsführer:innen in den vergangenen Jahren ganz oben auf der Liste der Technologien, die man im Auge behalten sollte. Sie wurde branchenübergreifend hoch angepriesen als Lösung mit einem großen Potenzial für Effizienzsteigerungen und Zugänglichkeit. Leider ist die Cloud auch eine bemerkenswert unzureichend genutzte Technologie. Ihr Schwerpunkt liegt vor allem auf der Datenspeicherung, während der Datenanalyse weniger Bedeutung beigemessen wird.

So konzentrierte sich auch die erste Generation der Cloud auf Storage, Apps und das Aufkommen cloud-basierter Anwendungen im Sinne von Software-as-a-Service (SaaS). Bei der zweiten Generation der Cloud modernisierten IT-Teams ihre Prozesse und Arbeitspraktiken, um leistungsfähiger zu sein. Womit wird sich also die nächste Generation der Cloud befassen?

Faktencheck

Fakt ist: In den vergangenen Jahren hat sich die Unternehmenswelt schneller als je zuvor verändert – dieser Meinung sind auch 74 Prozent der deutschen Unternehmen laut einer Studie von Alteryx in Zusammenarbeit mit IDC. Interne organisatorische Veränderungen, Fachkräftemangel und sich wandelnde Wettbewerbslandschaften bremsen Unternehmen aus und machen nun den Bedarf an Datenanalysen, um wettbewerbsfähig und erfolgreich zu sein, höher denn je. Aktuell nutzen nach der Untersuchung von Alteryx und IDC jedoch 84 Prozent der deutschen Unternehmen nicht einmal ihre eigenen analytischen Erkenntnisse zur Entscheidungsfindung.

Die Fähigkeit, mithilfe von Datenanalysen gute Entscheidungen zu treffen, ist dabei von zwei Faktoren bestimmt: erstens von der Menge der zu analysierenden Daten und zweitens von dem Engpass an den für die Analyse benötigten Data Scientists. Aus diesem Grund wird sich die dritte Generation des Cloud Computing in 2023 vor allem um das Thema Zugänglichkeit drehen. Denn die Cloud-Technologie

kann viel mehr bewirken: Wenn Unternehmen die Cloud für alle ihre Mitarbeitenden zugänglich machen und sozusagen demokratisieren, legen sie auch die Datenanalysen genau in die Hände derjenigen, die am meisten davon profitieren.

Data Scientists

Letztlich ist jede Technologie nur so erfolgreich – und wirkungsvoll – wie die Person, die sie einsetzt. Das gilt auch für Cloud Computing. Am wertvollsten ist Cloud Computing, wenn es dieses menschliche Potenzial auch in einem großen Umfang nutzt. Das setzt voraus, dass Unternehmen die Zugangsanforderungen und die tatsächliche Zugänglichkeit der Cloud in Einklang bringen sowie ihre Expert:innen in den Vordergrund rücken.

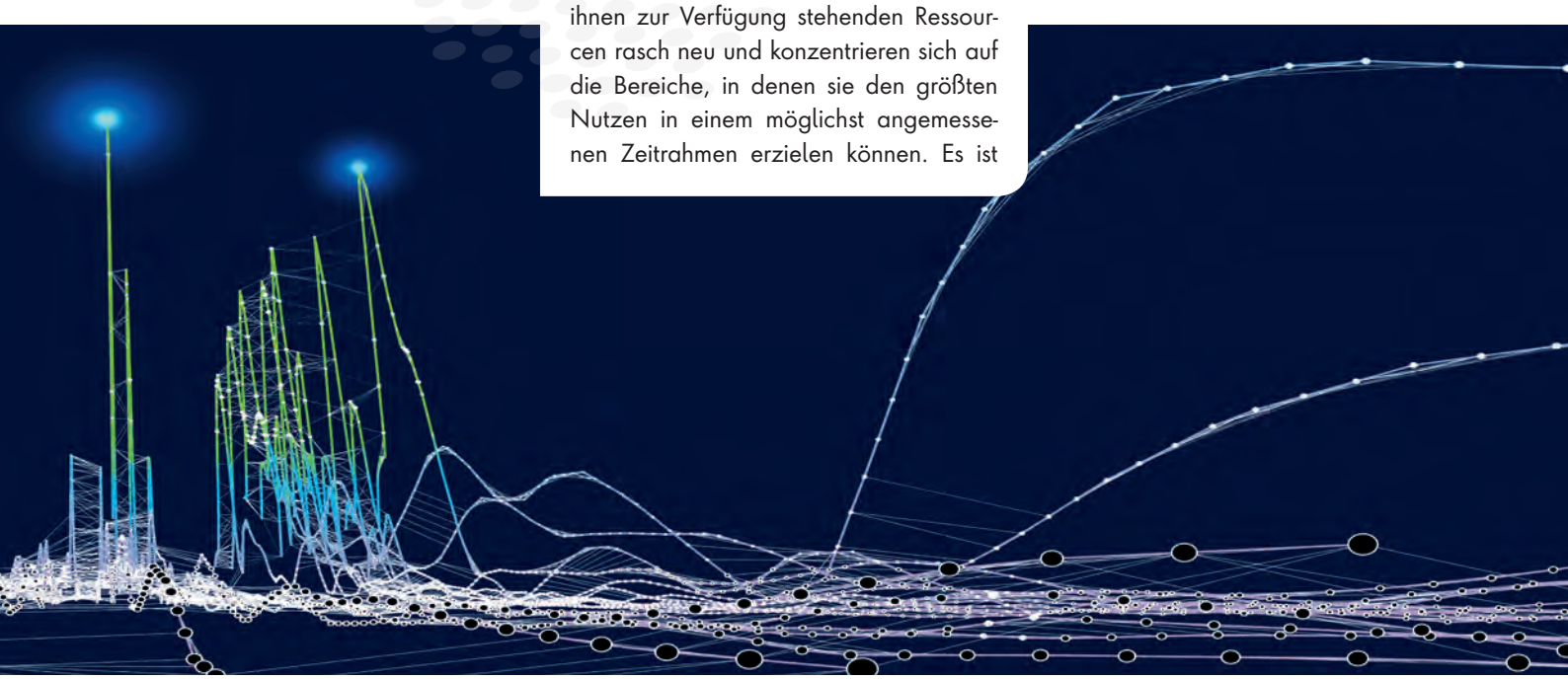
Dieser menschliche Faktor kann in vielen Fällen für Unternehmen ein Vorteil sein, weil es den Einfallsreichtum der Mitarbeitenden in der Entscheidungsfindung involviert. In anderen Fällen – so wie wir es heute bei den Data-Science-Teams sehen – kann der menschliche Faktor auch als Engpass für Unternehmen wirken. Da die täglich anfallende Datenmenge exponentiell ansteigt und Unternehmen ihre Data-Science-Teams nicht effektiv skalieren können, sind die Mitarbeitenden in diesen Teams auf der ganzen Welt aufgrund ihrer übermäßigen Arbeitsbelastung überfordert und ausgebrannt.

So belegen auch Zahlen von Gartner, dass die weltweiten Ausgaben für öffentliche Clouds im Jahr 2023 ein Volumen von 600 Milliarden US-Dollar erreichen werden. Eine Untersuchung von Statista in Fortführung der IDC-Forschung zeigt einen enormen Anstieg des Datenvolumens von bis zu 180 Zettabytes pro Jahr bis 2025. Zum Vergleich: Um nur ein Zettabyte an Daten zu speichern, wären 41,5 Millionen der weltweit größten handelsüblichen Festplatten (24 TB) erforderlich. Die wenigen Mitarbeitenden in Data-Science-Teams können mit dieser exponentiell wachsenden Datenmenge nicht Schritt halten, was zu einer Burnout-Situation führt.

Quick wins

In der Regel bewerten Unternehmen die ihnen zur Verfügung stehenden Ressourcen rasch neu und konzentrieren sich auf die Bereiche, in denen sie den größten Nutzen in einem möglichst angemessenen Zeitrahmen erzielen können. Es ist klar, dass der Wechsel zur Cloud zumindest teilweise durch Pragmatismus angesichts des exponentiellen Datenwachstums und des Bedarfs an schnellen Erkenntnissen angetrieben wurde. Im Jahr 2023 und darüber hinaus wird derselbe Pragmatismus eine wichtige Triebfeder für die verstärkte Einführung von demokratisierten Cloud-Analysen sein – eine Lösung für die Herausforderung mit den zunehmend ausgebrannten und überlasteten Data-Science-Teams, die mit dem Umfang des Datenwachstums nicht Schritt halten können.

Für Unternehmen gilt es nun nicht nur, zeitnahe Erkenntnisse aus ihren Daten zu gewinnen, sondern auch, in einem disruptiven Wettbewerbsumfeld wettbewerbsfähig zu bleiben. Dazu müssen sie das volle Potenzial von Cloud Computing ausschöpfen, indem sie Benutzerfreundlichkeit mit weitreichender Zugänglichkeit kombinieren. In der Praxis heißt das nicht



nur, dass sie mit Data Scientists die Integration moderner Cloud-Technologien erleichtern, sondern auch, dass sie Mitarbeitende in Fachabteilungen dazu befähigen, ihre eigenen Fragestellungen mit Cloud-Daten zu lösen.

Beziehung zur Cloud neu definieren

Um dieses Potenzial für 2023 und darüber hinaus zu erschließen, müssen sich Unternehmen zuallererst von der alten Vorstellung verabschieden, wie Cloud Computing funktionieren sollte. Gartner schätzt, dass wir bereits im Jahr 2019 weltweit die Grenze von einer Milliarde Knowledge Workern überschritten haben. Bei Knowledge Workern handelt es sich um Mitarbeitende, die kreativ denken und strategisch wichtige Schlussfolgerungen ziehen müssen. Knowledge Worker sind genau die Menschen, für die die Cloud-Technologie entwickelt wurde.

Cloud-Integrationen können – in vielen Fällen – aus betrieblicher Sicht enorm fortschrittlich und ausgereift sein. Unternehmen haben Multi-Cloud-Lösungen, Containerisierung und kontinuierlich lernende KI-/ML-Algorithmen implementiert, um innovative Ergebnisse zu erzielen. Doch diese Ergebnisse werden oft nicht in dem notwendigen Umfang oder mit der benötigten Geschwindigkeit geliefert, um sekundenschnelle Entscheidungen treffen zu können. Genau diese sind jedoch in der heutigen Zeit für den Erfolg eines Unternehmensbetriebs erforderlich.

ZWAR SIND DATENANALYSE UND CLOUD COMPUTING SCHON SEIT JAHREN DER ERFOLGSMOTOR FÜR UNTERNEHMEN, ABER FÜR DIE DEUTSCHEN SCHEINT ES IMMER NOCH EINE GROSSE HERAUSFORDERUNG ZU SEIN, DAS POTENZIAL IHRER DATEN ZU ERSCHLIESSEN. 2023 KÖNNTE DAS WICHTIGSTE JAHR FÜR DIY-CLOUD-ANALYSEN WERDEN.

Suresh Vittal, CPO, Alteryx, www.alteryx.com

Cloud-Demokratisierung

Damit die Cloud-Demokratisierung erfolgreich sein kann, müssen Unternehmen ihre Knowledge Worker weiterbilden und ihnen die richtigen Tools an die Hand geben. Nur so können sie das volle Potenzial ihrer eigenen Daten ausschöpfen und genau die Fachkräfte – die am besten geeignet sind, Fachfragen zu beantworten – dazu befähigen, Datenanalysen ganz nach dem Motto Do-It-Yourself „einfach mal selbst zu machen". Low-Code-No-Code-Tools können dabei einen entscheidenden Vorteil liefern: Sie ermöglichen auch ohne Expertise die Analyse von Cloud-Daten und verkörpern gleichzeitig auch die ursprüngliche Vision der Cloud-Technologie – den Menschen die Macht zu geben, die sie brauchen, um sich Gehör zu verschaffen. Die Cloud-Evolution geht also in die nächste Runde.

Suresh Vittal

CUSTOMER JOURNEY TOOLKIT

VERBESSERN SIE IHR SERVICEERLEBNIS

Sie wollen Ihre Services verbessern? Aber Sie wissen nicht, wo Sie anfangen sollen? Die Gestaltung einer Customer Journey bietet Ihnen einen schnellen Überblick über die größten Verbesserungsmöglichkeiten und einfachsten Quick Wins. Und das Beste daran? Mit dem folgenden Toolkit wird die Gestaltung einer Customer Journey zum Kinderspiel.

Laden Sie sich das TOPdesk Toolkit herunter und erhalten Sie:

- Einen interaktiven, einstündigen Workshop um Sie und Ihr Team fit für die Erstellung einer Customer Journey zu machen
- Alles was Sie zum Gestalten einer Customer Journey benötigen
- Alle Materialien und Anleitungen für die Gestaltung Ihrer Customer Journey, die Sie direkt ausdrucken können
- Eine Vorlage für die Gestaltung einer Customer Journey
- Einen einfachen Weg vom ersten Interview Ihrer Melder bis zur Verbesserung Ihrer Services.

WHITEPAPER DOWNLOAD

Der Leitfaden steht kostenlos zur Verfügung. **www.it-daily.net/Download**

WHITEPAPER DOWNLOAD

Das Whitepaper umfasst 35 Seiten und steht kostenlos zum Download bereit. **www.it-daily.net/Download**

DIE SAP S/4HANA BUSINESS TRANSFORMATION

MIT DIGITALISIERTEN END-TO-END- PROZESSEN DIE ZUKUNFT SICHERN

Es gibt viele Gründe für den Wechsel zu SAP S/4HANA. Dass Unternehmen heute immer größere Datenmengen bewältigen und ihre Geschäftsprozesse und -modelle flexibel an neue Rahmenbedingungen anpassen müssen, ist einer der wichtigsten. SAP S/4HANA ist die Antwort von SAP auf den digitalen Wandel und ein immer schnelllebigeres, global vernetztes Geschäftsumfeld.

SAP Kunden, die auf SAP S/4HANA umsteigen wollen, bleibt dafür allerdings nur noch wenig Zeit. 2027 soll der technische Support für ältere SAP ERP-Systeme auslaufen. Dieses Whitepaper beschreibt, welche Schritte dafür von der Planung bis zum erfolgreichen Abschluss notwendig sind, was es zu beachten und bedenken gilt und wie RISE with SAP bei der Transformation in die Cloud unterstützt.

Unified Communications und smarte Prozesse

DER SCHLÜSSEL FÜR DEN WORKFLOW DER ZUKUNFT

Flexible Beschäftigungsmodelle wie Homeoffice und hybrides Arbeiten sind gefragter denn je und gelten als Indikator der modernen Arbeitswelt. Zugleich sehen sich Unternehmen mit der Herausforderung konfrontiert, barrierefreie Arbeitsumgebungen zu schaffen und die nahtlose Zusammenarbeit räumlich verteilter Teams sicherzustellen. Möglich wird dies durch den Einsatz intelligenter Unified-Communications-Lösungen, mit denen sich unterschiedlichste Kommunikationsformen und -kanäle bündeln und bestehende Prozesse auch ortsunabhängig fortführen lassen.

Es ist nicht ungewöhnlich, dass sich im Laufe der Jahre verschiedenste Komponenten innerhalb der unternehmenseigenen Netzwerk- und IT-Infrastruktur ansammeln. Das Resultat ist nicht selten ein hoher Anteil an Insellösungen und heterogener Strukturen. Ein Konstrukt, dass zu Lasten der Produktivität geht und ein nahtloses und medienbruchfreies Arbeiten erschwert.

Den Verantwortlichen vieler Unternehmen ist durchaus bewusst, dass integrierte Lösungen und Systeme der Schlüssel für die Workflows der Zukunft sind. Erschwerend hinzu kommt, dass viele Digital-Workplace-Projekte eine einheitliche Anwendungsumgebung voraussetzen. Doch was tun, wenn heterogene Systeme bereits bestehen? Ist es möglich, isolierte Strukturen auch nachträglich zu bündeln? Ja, mit Unified Communications. Sind entsprechende Lösungen im Einsatz, werden alle relevanten Kommunikationsdienste in einer einheitlichen Anwendungsumgebung zusammengeführt und ein zeit- und ortsunabhängiger Zugriff auf Geräte und Informationen möglich.

Pionier im Bereich UC

Ein Unternehmen, das sich diesen Anwendungsszenarien verschrieben hat und zugleich zu den Pionieren von Unified Communications zählt, ist die Ferrari electronic AG. Ihre Entwicklung der ersten intelligenten Faxkarte im Jahr 1989 war eine Weltpremiere. Von da an war es möglich, direkt aus allen Windows-Applikationen heraus zu faxen – ein absolutes Novum für die damalige Zeit. Bis heute ist das Unternehmen seiner Vorreiterrolle treu geblieben und setzt regelmäßig neue Standards. Einer dieser Branchenstandards steckt im Kommunikationsklassiker OfficeMaster Suite. Sie ist das beste Beispiel einer konsequenten Weiterentwicklung und Adaption an die sich rasant ändernden Herausforderungen der digitalen Arbeitswelt.

Alle Kommunikationskanäle auf einer Plattform

Die OfficeMaster Suite bietet Kommunikationskanäle wie den Dokumentenaustausch, Voicemail und SMS auf einer einheitlichen Plattform, lässt sich an Dokumentenmanagement- und BPM-Systeme anbinden und stellt einen rechts- und manipulationssicheren, DSGVO-konformen Dokumentenaustausch in IP-Umgebungen sicher. Dokumente und Voicemail-Nachrichten lassen sich von allen Devices aus abrufen und weiterverarbeiten. Selbst den Herausforderungen weltweit tätiger Unternehmen ist die Lösung gewachsen. Sie erfüllt den international gültigen ITU-Standard und stellt ein verlustfreies, hybrides arbeiten auch bei global verteilten Standorten sicher.

Herzstück der OfficeMaster Suite ist der von Ferrari electronic etablierte Standard „Next Generation Document Exchange" (NGDX). Dokumente gehen damit im Original, verlustfrei und End-to-end als PDF im E-Mail-Postfach des Empfängers ein. Formatierungen, Farben und selbst hohe Auflösungen bleiben erhalten. Metadaten und Schlagworte werden ebenfalls übertragen, was eine weitere Bearbeitung in Dokumentenmanagementsystemen erleichtert. Potenziell schädliche, aktive Inhalte wie Hyperlinks oder Applikationen sind automatisch vom Transfer ausgeschlossen. Übertragen lassen sich mit NGDX auch hybride Dokumente. Papiergebundene Prozesse können so mit digitalen verbunden und das Prinzip des papierlosen Büros umgesetzt werden.

Intuitive Bedienung

Das Ziel von Unified-Communications-Lösungen sollte immer sein, dass Prozesse automatisiert, die Produktivität gesteigert und Workflows effektiver werden. Funktionieren kann dies nur, wenn die Belegschaft mit den eingesetzten Lösungen zurechtkommt und diese intuitiv bedienen kann. Hierfür entscheidend ist, dass die Nutzung über eine den Anwendern vertraute Arbeitsoberfläche realisiert wird. Dies ermöglicht die Office-

Master Suite, indem sie sich nahtlos in bereits vorhandene Groupware oder E-Mail-Clients integrieren lässt. Den Nutzern steht damit auch weiterhin die gewohnte Oberfläche zur Verfügung, welche im Hintergrund um weitere Kommunikationsformen ergänzt wurde.

Manipulationssicher dank integrierter Hashes

Gerade weil es eine der Kernaufgaben von Unified Communications ist, die nahtlose Zusammenarbeit räumlich getrennter Teams sicherzustellen, muss der manipulationssichere und datenschutzkonforme Austausch von Dokumenten höchste Priorität haben. Die OfficeMaster Suite stellt dies über eine synchrone und asynchrone Verschlüsselung sicher. Der Austausch von Schlüsseln ist nicht mehr erforderlich, die Manipulationssicherheit der Dokumente wird durch integrierte Hashes erreicht. Sind diese beim Versender und Empfänger identisch, ist sichergestellt, dass das Dokument auf dem Versandweg nicht verändert wurde.

UC über die Cloud

Ein weiterer Vorteil ist, dass sich Unified-Communications-Lösungen auch über die Cloud beziehen lassen. Gerade in Zeiten steigender Strompreise ist es wirtschaftlich oft sinnvoller, auf unternehmenseigene Rechenzentren oder vollständig On-Premises-betriebene Infrastrukturen zu verzichten und stattdessen auf Cloudlösungen zurückzugreifen. Denkbar ist dies beispielsweise im Bereich der Telefonie. Wird die OfficeMaster Suite über Azure Marketplace bezogen, lassen sich ausgewählte Rufnummern von der Telefonanlage entkoppeln, über den Provider auf die Plattform leiten und gezielt verteilen.

Der Anwender behält die Hoheit über die Abläufe, betreibt diese aber in der Cloud. Das Thema Sicherheit steht auch hier an erster Stelle: Der Austausch der Dokumente findet in einer abgesicherten Umgebung statt, die Übertragung bleibt über den gesamten Kommunikationsweg verschlüsselt. Auch die Daten selbst sind in Deutschland hinterlegt, der SIP-Trunk ist ebenfalls hier angeschlossen.

Hybride Arbeitswelten und Beschäftigungsformen werden mehr und mehr zum Standard. Dies erfordert integrierte Lösungen und Systeme, die einen reibungslosen und verlustfreien Wechsel zwischen Firmenbüro, Homeoffice und verschiedenen Unternehmensstandorten sicherstellen und bereits bestehende Strukturen in einer einheitlichen Arbeitsumgebung bündeln. Möglich wird dies durch den Einsatz intelligenter Unified-Communications-Lösungen.

https://www.ferrari-electronic.de/

Quelle: ferrari electronic/Adobe Stock/Deemerwha studio

Sind IP-Telefone zukunftsfähig?

DREI GRÜNDE, IP-TELEFONE IM ITK-BUDGET 2023 ZU BERÜCKSICHTIGEN

Es gibt einen Grund, warum VoIP immer noch auf dem Vormarsch ist: Es ist ein kostengünstiges, aber effektives Werkzeug zur Verbesserung der internen und externen Unternehmenskommunikation. Doch gilt diese Wahrnehmung auch für IP-Telefone in Zeiten des hybriden Arbeitens?

Dass die IP-Telefonie den Anforderungen an eine moderne Firmenkommunikation durch die höhere Skalierbarkeit und deutliche Kostensenkungen entspricht, ist mittlerweile eine gegebene Tatsache. VoIP hat sich seit den Anfängen enorm weiterentwickelt und lässt sich heute sogar bestens in andere aufkommende Technologietrends wie 5G oder IoT integrieren. Genau dieses Entwicklungs- und Integrationspotenzial zählt zu den Säulen des weltweiten Erfolgs der IP-Telefonie. Der große Digitalisierungsschub aus den letzten Jahren hat ebenfalls zur wachsenden Akzeptanz moderner Telekommunikationsdienste und -plattformen geführt. Demnach ist es nicht verwunderlich, dass die jüngsten Prognosen von Research & Markets dem globalen Markt für VoIP-Dienste nach wie vor ein rasantes Wachstum auf über 102 Milliarden US-Dollar bis 2026 voraussagen: Selbst konservativere Unternehmen, die zu den Early Adoptern gehörten, spüren die Notwendigkeit, auf neue Telekommunikationslösungen zu setzen. Letztere basieren auf offenen Standards und bieten eine noch engere Verzahnung mit der bestehenden Infrastruktur sowie den ERP-/CRM-Systemen. Und dies bei gleichzeitiger Erweiterung der Einsatzszenarien auf Home- und Remote-Worker.

KOMMUNIKATION UND PRODUKTIVITÄT GEHEN HAND IN HAND. DIE ERFAHRUNG AUS DEN SCHWERSTEN PHASEN DER PANDEMIE HAT GEZEIGT, WIE WICHTIG DIE VERFÜGBARKEIT GEEIGNETER KOMMUNIKATIONS-ENDGERÄTE FÜR DIE WAHRUNG DER PRODUKTIVITÄT IST.

Gernot Sagl,
CEO, Snom Technology GmbH,
www.snom.com

So kann man erwarten, dass der Ersatz bisheriger TK-Lösungen durch effizientere UCC-Plattformen im ITK-Budget 2023 vieler Unternehmen berücksichtigt sein dürfte. Besonders, nachdem das hybride Arbeiten de facto zum festen Bestandteil der Arbeitskultur geworden ist. Doch die Investition in eine neue UCC-Lösung zahlt sich erfahrungsgemäß nur bedingt in Form gesteigerter, ortsunabhängiger Produktivität aus, wenn nicht zeitgleich eine Erneuerung der eingesetzten IP-Endgeräte stattfindet: Nur zeitgemäße, per Firmware-Update auf dem neuesten Stand gehaltene IP-Telefone gewährleisten das Höchstmaß an Unterstützung der UCC-Funktionen. Doch damit nicht genug: Drei weitere Faktoren untermauern die Relevanz von IP-Telefonen für den geschäftlichen Gebrauch.

1. IP-Endgeräte: So viel mehr als nur Telefone

Mit Beginn der Einführung von Voice over IP gegen Ende der 1990er-Jahre wurden IP-PBX-Systeme gemäß den Paradigmen traditioneller Telefonanlagen entwickelt. Folglich also meistens geschlossene Systeme für einen On-Premises-Betrieb bei ausschließlicher Nutzung von Anlage und Telefonen aus einem Haus. Diese mangelnde Flexibilität führte zu hohen Kosten, wenn man die Konfiguration des Systems verändern und neue Dienste in Anspruch nehmen wollte oder zusätzliche Anschlüsse benötigte.

Heute sind solche Lösungen quasi undenkbar geworden: VoIP-Systeme sind jederzeit skalierbar und dank der eingebetteten offenen Standards für anderweitige Nutzungsszenarien einsetzbar: Mittels APIs können sowohl das VoIP-System als auch die Telefone durch einfache Updates erweitert werden. Es besteht also keine Notwendigkeit, Zeit oder Geld für die Aufrüstung von Hardware aufzuwenden. Das gilt noch weniger bei Software-basierten Telefonie-Plattformen, die heute zunehmend aufgrund ihrer Kosteneffizienz in der Cloud gehostet werden. Sie eröffnen Unternehmenskunden noch mehr Möglichkeiten bei der Auswahl des Anbieters, der Telekommunikationslösung und – zu guter Letzt – der IP-Endgeräte.

So werden bei Telefonen plötzlich andere Kriterien wie die Audio-Qualität, die Unempfindlichkeit, die Funktionsvielfalt oder das Design relevant. Erst im Anschluss daran kommt der Kostenfaktor ins Spiel, und zwar basierend darauf, welchen Funktionsumfang ein Unternehmen benötigt: Moderne IP-Telefone können beispielsweise als Schaltzentrale für die

Foto: AdobeStock

Büroautomation fungieren, als Bestandteil der Gegensprech- und Videoüberwachungsanlage oder eines Feueralarmsystems, als Basis für das Monitoring von Gegenständen und Menschen. Es ist diese Vielfalt, die die Wirtschaftlichkeit von IP-Endgeräten auch heute noch nachdrücklich belegt.

2. Nützlicher denn je

Sind IP-Telefone und die gewählte Plattform interoperabel, ist zusätzlich eine Fernkonfiguration der Geräte per Autoprovisioning möglich. Dadurch können die Telefone im Büro oder im Homeoffice direkt vom Mitarbeitenden per „Plug & Play" in Betrieb genommen und fällige Updates auch vom IT-Manager aus der Zentrale durchgeführt werden. Das bedeutet eine große Zeit- und Geld-Ersparnis für alle Beteiligten.

Als noch wirtschaftlicher erweisen sich IP-Telefone durch die Hot-Desking-Funktion. Egal in welcher Zweigstelle oder Räumlichkeit des Unternehmens sich der Mitarbeitende befindet: Beim Einloggen auf ein x-beliebiges Telefon werden alle für diese Person festgelegten Funktionen und Einstellungen bereitgestellt. Gleiches gilt entsprechend natürlich auch im Homeoffice: Fernarbeitende greifen über das am besten per VPN an der Telefonzentrale angemeldete IP-Telefon auf die geteilten Adressbücher, auf die Informationen über den Präsenzstatus der Kollegen und auf alle Merkmale, die Geschäftstelefone kennzeichne, nahtlos zurück.

3. Abgesicherte Kommunikation

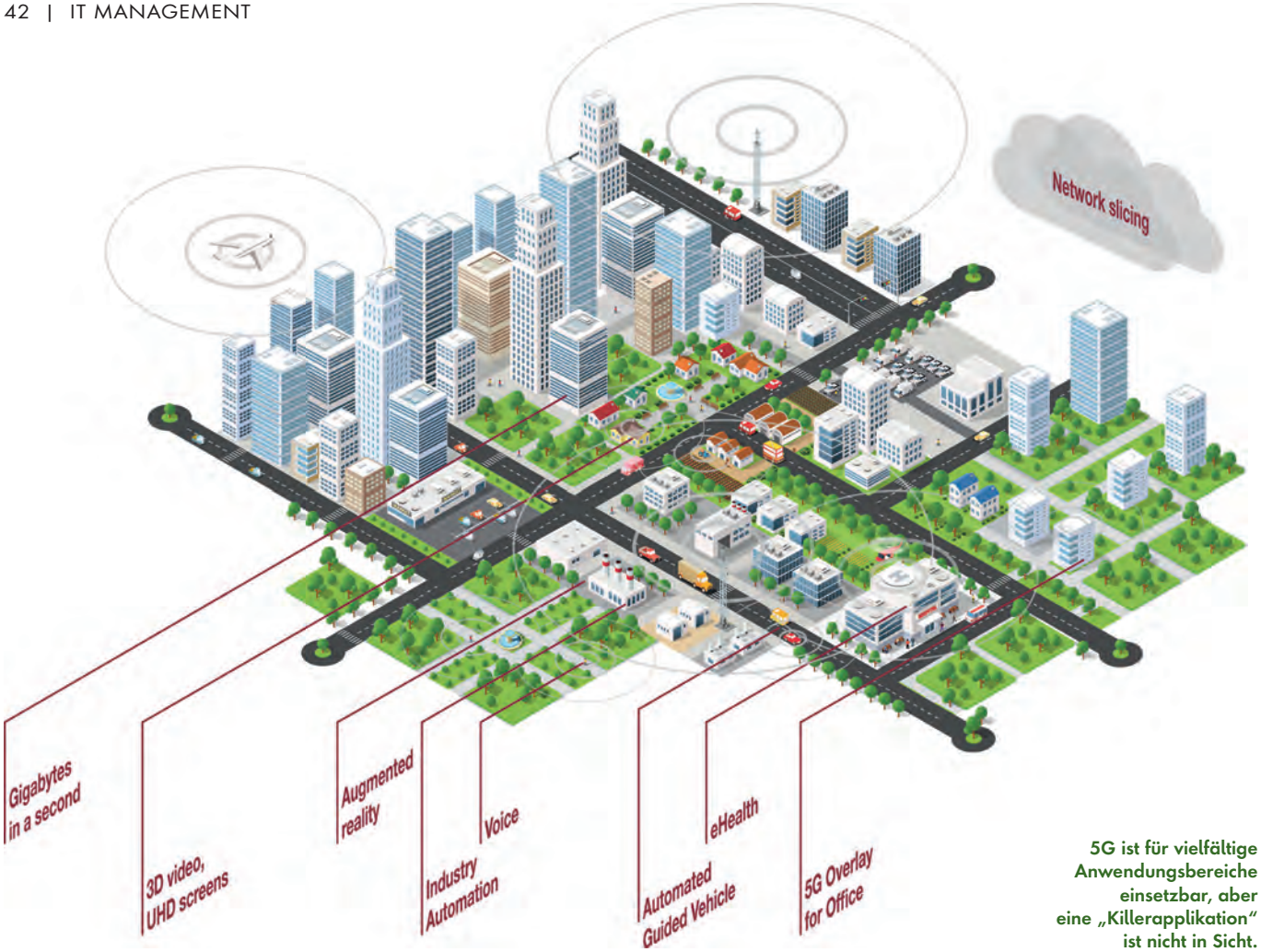
Kommunikation und Produktivität gehen Hand in Hand. Die Erfahrung aus den schwersten Phasen der Pandemie hat gezeigt, wie wichtig die Verfügbarkeit geeigneter Kommunikations-Endgeräte für die Wahrung der Produktivität ist. Eines der wichtigsten Merkmale von IP-Telefonen der jüngsten Generation sind die eingebauten Sicherheitsmechanismen. Sie gestatten nur spezifischen Geräten den Zugang zur Telefonzentrale und umgekehrt, randomisieren den Port, worüber Telefonate geführt werden, und enthalten Chiffrierungsmechanismen für den gesamten Sprachverkehr. Bei europäischen Herstellern werden zudem die in der EU und den jeweiligen Ländern gültigen Datenschutzrichtlinien „by Design" mitberücksichtigt. Somit ist es für Cyberkriminelle deutlich schwieriger, über IP-Telefone Gespräche mitzuschneiden, als über Smartphones oder herkömmliche Haustelefone.

Darüber hinaus bieten Premiumhersteller von IP-Endgeräten und -Zubehör wie Snom Technology regelmäßig kostenfreie Firmware-Updates, die einerseits der funktionellen Ausstattung der Telefone Zusatzmerkmale hinzufügen und andererseits mögliche Sicherheitslücken oder Exploits schließen. Somit können Unternehmen darauf vertrauen, dass sie Geräte auf dem neuesten Stand der Technik hinsichtlich der Sicherheit einsetzen.

Fazit

Es gibt unzählige Gründe für den unaufhaltsamen Erfolg der digitalen Kommunikation. Doch das Spielfeld teilt sich nun nicht mehr unter denen auf, die professionelle Lösungen und Endgeräte hierfür einsetzen, und denen, die es nicht tun. Auch nicht zwischen Early Adoptern und Zauderern. Die Partie um die Zukunft in der IP-Telefonie entscheidet sich zwischen denjenigen, die in dieser Technologie nur eine weitere Möglichkeit sehen, etablierte Dinge weiterhin zu tun, und jenen, die von diesen Technologien profitieren, indem sie sie nutzen, um ihre Prozesse im Unternehmen völlig neu zu denken.

Gernot Sagl



5G ist für vielfältige Anwendungsbereiche einsetzbar, aber eine „Killerapplikation" ist nicht in Sicht.

WIFI, LTE oder 5G?

INNOVATIVE FUNKTECHNOLOGIE VOR DEM MARKTDURCHBRUCH? POCS ZEIGEN IHREN NUTZEN

5G wird 2023 zum ersten Mal in große produktive IT/OT-Umgebungen der Industrie einziehen. Das ist ein echter Wendepunkt, denn es gibt erst wenige private Campus-Projekte und die meisten davon befinden sich noch in der frühen Phase des Proof of Concept (PoC). Das bedeutet: Es sind reine Testnetze ohne Anbindung an eine industrielle Fertigung, unter anderem weil es bislang an 5G-fähigen Endgeräten für die unterschiedlichen industriellen Einsatzbereiche mangelt. Die Hersteller arbeiten mit Hochdruck daran, denn der Bedarf in der Wirtschaft ist groß. Für die digitale Transformation spielen Kommunikationsinfrastrukturen und leistungsstarke Übertragungsmöglichkeiten eine wichtige Rolle, denn herkömmliche Technologien stoßen zunehmend an ihre Grenzen. Damit rückt ein bislang kaum diskutierter Aspekt in den Fokus: Die Integration von 5G in reale, bereits existierende Netzarchitekturen. Ein vielschichtiges Vorhaben!

WiFi, LTE oder 5G? Von welcher Technologie ein Unternehmen am meisten profitiert, hängt entscheidend von den betrieblichen Anforderungen und der Situation vor Ort ab. Das zeigt das Beispiel eines Fertigungsbetriebs, der seine Bauteile in einem großen Hochregallager aufbewahrt. Shuttles entnehmen die Komponenten aus den Lagerebenen und bringen sie zur Montage. Das Unternehmen wollte den Transport beschleunigen und den Lagerbestand zukünftig digital überwachen. Der erste Versuch mit einem WiFi-Netz schlug fehl. Da die Metallkonstruktion des Lagers das Funkfeld abblockte, wären sehr viele Access Points notwendig gewesen. Die zahlreichen Übergaben von einem Punkt zum nächsten hätten den Prozess erheblich verlangsamt. Deswegen beauftragte das Unter-

nehmen telent, die Gebietsabdeckung (Coverage) mit 5G zu prüfen. Dafür errichtete der Systemintegrator ein 5G-Netz, installierte Kameras in die Shuttles und prüfte so, ob die Daten in der erforderlichen Qualität übertragen werden. Innerhalb nur eines halben Tages gelang der Nachweis, dass 5G das komplette Lager funktechnisch abdeckt. Für Freigelände lässt sich dies mithilfe von Planungstools und jahrzehntelanger Erfahrung sehr exakt berechnen; für Innenbereiche braucht es zusätzlich real gemessene Daten und exakte Informationen über die Gebäudeinfrastruktur wie zum Beispiel Wandmaterial und -stärke. Doch diese Berechnung ist erst der Anfang, dem sich der PoC anschließt, wenn ein Unternehmen von der Funktionalität einer bestimmten Technologie überzeugt ist und deren Nutzen in einer längeren Testphase erproben möchte.

Die Machbarkeit prüfen

Im PoC wird getestet, ob 5G den erwarteten Nutzen tatsächlich erbringt und zwar für eine konkrete industrielle Anwendung, etwa in einer automatisierten Fertigungslinie die Steuerung der Roboter, die in Bruchteilen von Sekunden mit Informationen versorgt werden müssen. Unterstützt der Mobilfunkstandard die erforderlichen OT-Protokolle? Halten Latenz und Bandbreite in der Realität, was sie in der Theorie versprechen? Es kann Monate dauern, bis in der Testphase solche und viele weitere Fragen beantwortet sind. Großkonzerne mit spezialisiertem Fachpersonal und ausreichenden Kapazitäten können Anwendungen, wie die Steuerung der Roboterarmen via 5G, selbst testen und lassen sich nur beim Aufbau des Mobilfunknetzes von einem externen Anbieter unterstützen. Der Mittelstand kann das nicht leisten. Deswegen haben sich weltweit Industrieunternehmen, Systemintegratoren wie telent und wissenschaftliche Institute in der 5G Alliance for Connected Industries and Automation (5G ACIA) zusammengeschlossen, um die Anforderungen der Industrie in die Entwicklung und Standardisierung der 5G-Technologie frühzeitig einzubringen. Dafür bauen sie kundenspezifische Anwendungsszenarien unter realistischen Bedingungen mit der neuesten Mobilfunktechnik auf, um sie zu überprüfen und zu verbessern. Und wenn es wie im Fall der Roboterarmsteuerung noch kein 5G-fähiges Endgerät gibt, ziehen sie Spezialfirmen hinzu.

Kritische Kommunikation via 5G

Große Datenraten, kurze Verzögerungszeiten (Latenz), hohe Endgerätedichte – das sind die Leistungsmerkmale von 5G, die in sogenannten Releases schrittweise entwickelt werden. Am Markt gibt es bereits Endgeräte und Software für das 5G-Kern- sowie das Funkzugangsnetz, die der Spezifikation von Release 15 entsprechen, dem „enhanced Mobile Broadband" (eMMB) für die schnelle Datenübertragung. Die Hersteller haben zugesagt, im Laufe des Jahres Release-16-fähige Endgeräte bereitzustellen, die mit Latenzzeiten von bis zu einer Millisekunde neue Maßstäbe setzen. Das ist relevant für zeitkritische Anwendungen wie autonomes Fahren oder Predictive Maintenance. Erstmalig wird es damit auch möglich, die gesamte geschäftskritische Kommunikation (Mission Critical Communication) produktiver Offshore-Windparks wie etwa in der Nordsee über 5G abzubilden. Die Installation der Funkversorgung über großflächige, offene Wasserflächen ist eine äußerst komplexe Aufgabe ebenso wie die vielfältigen Integrationsleistungen. Sie reichen von der Netztechnik, die spezielle Schnittstellen für die Telekomunikation zwischen Windparks mit unterschiedlichen Funkstandards benötigt, bis hin zum sicheren Zusammenwachsen von IT und OT.

PRIVATE 5G-CAMPUSNETZE, DIE EXAKT AUF INDUSTRIELLE ANWENDUNGEN ZUGESCHNITTEN SIND, WERDEN DIE INDUSTRIE 4.0 VORANTREIBEN.

Ronald Janke,
Senior Manager, telent GmbH,
www.telent.de

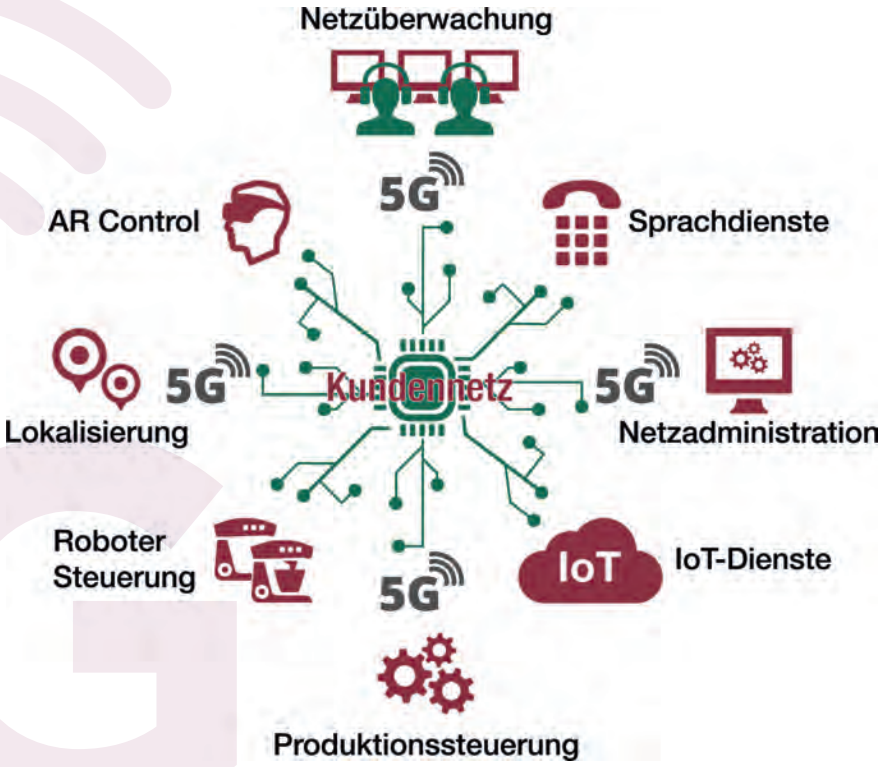
Auf dem Weg zur Industrie 4.0 bietet 5G produzierenden Betrieben viele Vorteile, wie mehr Flexibilität. Durch die drahtlose Vernetzungstechnologie können sie schneller auf geänderte Marktbedingungen reagieren, indem sie in Fertigungslinien neue Maschinen einbringen oder deren Reihenfolge ändern – ohne wie bisher aufwändig Kabel zu verlegen. Um die Vorteile eines lokalen 5G-Netzes auf dem eigenen Firmengelände voll auszuschöpfen, sollte von Anfang an ein erfahrener Dienstleister für Ende-zu-Ende-Lösungen eingebunden sein, der basierend auf einer Situationsanalyse ein optimales Netzdesign entwickelt und im Vorfeld herstellerneutral evaluiert, welche Technologien und Produkte am besten geeignet sind.

Privates versus öffentliches 5G-Netz

Auch die Betreiber öffentlicher Netze forcieren den Aufbau von 5G. So stellt sich Unternehmen die Frage, ob sie nicht diesen Service in Anspruch nehmen, um sich den Aufwand für die Bereitstellung und Wartung des 5G-Netzes zu sparen. Ob ein firmeneigenes oder ein öffentliches Netz die bessere Wahl ist, lässt sich nicht pauschal beantworten. Auch hier gilt: Es kommt auf den Anwendungsfall an. Je anspruchsvoller und spezifischer er ist, desto wahrscheinlicher ist ein firmeneigenes Netz besser geeignet. Das zeigt sich auch daran, dass für 5G bislang keine sogenannte „Killerapplikation" in Sicht ist. Damit wird in der Computertechnik eine Software bezeichnet, die viele Käufer findet, und die damit einer vorhande-

nen Technik zum Marktdurchbruch verhelfen. Das Angebotsspektrum des öffentlichen 5G-Netzes konzentriert sich vor allem auf Anwendungen, die von vielen Nutzern gewünscht sind, etwa das schnelle Streamen von Filmen. Diese Umsetzung passt jedoch nicht unbedingt zu einer bestimmten industriellen Anwendung. Dafür sind diese viel zu vielfältig. In der Industrie wird 5G deshalb in Form von individuell konfigurierten Campusnetzen überzeugen, die so individuell konfiguriert sind, dass sie genau das Problem lösen, das einem Unternehmen unter den Nägeln brennt.

Ronald Janke



Im produktiven Umfeld ermöglicht der 5G-Standard den Einsatz von IoT-Komponenten nahezu in Echtzeit.

Unversicherbare Cyberangriffe?

3 SCHRITTE, WAS UNTERNEHMEN JETZT TUN KÖNNEN

Die zunehmende Zahl von Cyberattacken und der damit verbundene Schaden haben zu einer steigenden Nachfrage nach Cyberversicherungen geführt, die jedoch einerseits von den Versicherungen selber, aber auch auf Seite der Kunden in Frage gestellt werden. Wenn Cyberangriffe bald „unversicherbar" werden, wie Mario Greco, CEO von Zurich Insurance im Interview mit der Financial Times sagte, was können Unternehmen dann tun, um diese Herausforderung zu bewältigen?

#1 **Die 3-2-1-Strategie bleibt aktuell: Isolierte Kopie der Daten vorhalten**

#2 **Silos abreißen und Daten unter Berücksichtigung von Zero-Trust zusammenführen**

#3 **Zusammenarbeit zwischen IT- und SecOps-Teams verbessern**

www.cohesity.com

CYBER ATTACKS

AI-as-a-Service, Generative AI, Metaverse

WELCHE KI-TRENDS SOLLTEN UNTERNEHMEN 2023 IM AUGE BEHALTEN?

Ob in der Softwareentwicklung, in der Automobilindustrie, bei Supply-Chain-Prognosen oder der Wartung von industriellen Maschinen – Künstliche Intelligenz (KI) hat in allen Industriesektoren Hochkonjunktur. Laut einer aktuellen Bitkom-Studie sehen 18 Prozent deutscher Unternehmen KI überwiegend als Chance für sich, 47 Prozent eher als Chance. Obwohl momentan nur 9 Prozent der Unternehmen KI-Anwendungen nutzen, planen oder diskutieren 25 Prozent der Befragten den KI-Einsatz. KI-Technologie ist also bereits in Verwendung und verspricht, in Zukunft eine noch größere Rolle zu spielen. Doch wohin könnte Unternehmen die KI-Reise im Jahr 2023 führen?

1. AI-as-a-Service

Bei Artificial Intelligence as a Service (AIaaS) outsourcen Unternehmen Leistungen im Bereich der KI an Dritte. Dadurch können sie ohne große Anfangsinvestitionen und mit geringerem Risiko KI für verschiedene Anwendungszwecke testen. In Zeiten, in denen Unternehmen sich mit dem Risiko einer drohenden Rezession auseinandersetzen müssen, kann eine Cloud-KI vor Ort, die Anschaffung der erforderlichen Hardware und Software, die Personal- und Wartungskosten, für viele Unternehmen unerschwinglich sein.

2. „Generative AI"

„Generative AI" nutzt KI und Maschinelles Lernen, um neue digitale Inhalte (Text, Video, Audio und Bilder) mit geringem menschlichem Eingreifen zu erstellen. Gartner prognostiziert, dass bis 2025 schätzungsweise 10 Prozent aller erzeugten Daten und 30 Prozent aller Marketingbotschaften großer Marken auf „Generative AI" zurückgehen werden. Marketingfachleute verzeichnen bereits erste Ergebnisse aus einer kreativen Nutzung von KI. In einer Studie verglich die KI-Kreativagentur Pencil Unternehmen, die Videowerbung mithilfe von KI-Kreativitäts-Tools erstellten, mit solchen, die ohne solche KI-Kreativitätsunterstützung arbeiteten. Durchschnittlich steigerten die erstgenannten Unternehmen die Rendite auf die Werbeausgaben (ROAS) um das Zweifache – bei einigen Kampagnen in der Studie sogar um das bis zu Siebenfache.

3. Einsatz von Chatbots & Natural Language Processing

Mit ChatGPT, dem neuen KI-gestützten Chatbot von OpenAI, hat das Forschungsgebiet um Natural Language Processing (NLP) einen weiteren signifikanten Sprung gemacht – und verspricht, weltweit bis 2030 voraussichtlich um 361,6 Milliarden USD zu wachsen. Als Teilbereich der KI zielt NPL darauf ab, Computer mit der Fähigkeit auszustatten, geschriebene und gesprochene Sprache zu verstehen und damit die Interaktion zwischen Mensch und Maschine zu vereinfachen. Sprachassistenten wie Alexa und Siri sind natürlich längst etablierte Beispiele in diesem Bereich. ChatGPT geht noch einen Schritt weiter – das Tool kann komplexe Fragen verständlich beantworten, Ideen aus verschiedenen Kontexten entnehmen und sie zusammenführen.

4. Digitale Zwillinge und das Metaverse

Das Metaverse war 2022 in aller Munde. Während der Gebrauch hauptsächlich für Gaming, Retail und Social-Media diskutiert wurde, eröffnen sich über dieses Jahr hinaus auch Möglichkeiten der Nutzung im industriellen Bereich. Dabei ist das Konzept von virtuellen Anlagen und Maschinen nicht neu – digitale Zwillinge finden in der Industrie schon seit einiger Zeit Verwendung.

In Verbindung mit dem Metaverse können diese Nutzungsmöglichkeiten anschaulicher und interaktiver gestaltet werden. So ist es denkbar, dass digitale Zwillinge fortan in eine Metaverse-Umgebung verlagert werden, wo Anwender:innen gemeinsam mit dem Kundendienst Wartungen auf virtuelle Weise durchführen können.

www.InfosysConsultingInsights.com

Metaverse

NEUE WELTEN BAUEN

Hören wir das Wort „Metaverse", denken wir sofort an Unterhaltung und Spiele. Das ist nicht völlig falsch, wenn man bedenkt, dass die Unterhaltungsindustrie mit dieser Technologie viele Innovationen hervorgebracht hat.

Das Metaversum ist jedoch mehr als nur Spaß und Spiel. Zahlreiche Branchen haben neue Wege gefunden, um es in einer Vielzahl von Prozessen zu nutzen, und tun dies auch weiterhin. Von virtuellen Schaufenstern, über Immobilien und Kundenservice sowie bis zum Marketing kann das Metaverse für moderne Unternehmen sehr nützlich sein.

Ein aktueller Forschungsbericht von Gartner sagt voraus, dass bis 2026 mindestens 25 Prozent des Online-Verkehrs etwa eine Stunde oder mehr im Metaverse verbringen wird. Die Wachstums-Prognosen für den Metaverse-Markt sind darüber hinaus erstaunliche: bis 2024 soll er auf fast 800 Milliarden Dollar anwachsen.

MIT SEINEN OFFENSICHTLICHEN VORTEILEN UND SEINER IMMENSEN REICHWEITE IST DAS METAVERSE EIN GAME CHANGER FÜR GROSSE UND KLEINE UNTERNEHMEN.

Vijay Pravin,
Gründer und Geschäftsführer,
bitsCrunch GmbH,
www.bitscrunch.com

Wozu ist das Metaverse fähig?

Setzen die großen Unternehmen der Welt die Metaverse-Technologie heute wirklich schon ein? Die Antwort ist ein klares Ja.

Infosys ist ein gutes Beispiel dafür. Das Unternehmen konzentriert sich derzeit auf eine Reihe von Metaverse-Anwendungen für reale Szenarien. Dafür wurde das Konzept der erweiterten virtuellen Realitäten auf interessante Weise weiterentwickelt. Der VR-Store für die Australian Open beispielsweise ist ein großartiges Beispiel dafür, wie das Unternehmen das Einkaufen und den Handel in eine neue digitale Welt gebracht hat. Fans der Veranstaltung wird so ein einzigartiges und unvergessliches Erlebnis geboten. Auch das Australian Open 360-Konzept bescherte den Fans ein unvergleichliches Erlebnis. Sie konnten mit ihren Freunden die Live-Übertragung eines Spiels in einem virtuellen Raum genießen, der dem tatsächlichen Stadion nachempfunden war.

Accenture setzt die Metaverse-Technologie auch für Produkttests und sogar für virtuelle Schulungen ein. Aktuell verschwimmen die Grenzen zwischen Arbeit und Leben immer mehr. Die Anwendungen des Metaversums können Remote- und Hybrid-Arbeitsverhältnisse nachhaltig verändern. Sowohl Arbeitgeber als auch Arbeitnehmer haben viel mehr Kontrolle über ihr Berufsleben, was die Arbeitsabläufe und die Effizienz insgesamt verbessert.

Abgesehen von den großen Unternehmen und ihren virtuellen Umgebungen stellt sich die Frage, ob und welche Bedeutung das Metaverse für kleinere Unternehmen haben kann? Hier kommt das Cloud Computing ins Spiel.

Cloud Computing & Metaverse

Hybride Clouds machen das Metaversum leichter zugänglich. Die Basis dafür sind die bestehenden automatisierten Systeme sowie die in der Cloud gesicherten Daten. Die Blockchain sorgt für die robuste Datensicherheit.

Das ist eine gute Nachricht für kleine und mittlere Unternehmen. Sie können problemlos wachsen, skalieren und dabei auf die verbesserten Datenflüsse und Verarbeitungsprozesse der Blockchain setzen. Darüber hinaus kann all dies mit dem Metaverse in eine vollständige virtuelle Umgebung verpackt werden.

Das Metaversum ist umfassend darauf ausgerichtet, neue Arbeitsmöglichkeiten zu schaffen - und ein Unternehmen wachsen zu lassen.

Das Metaversum und Du

Ein weiterer aufstrebender Bereich des Metaversums sind die persönlichen Avatare. Sie sind der Kernbestandteil eines Metaverse. Persönliche Avatare sind als

physische Repräsentanten von Personen definiert, die in der realen Welt leben können oder auch nicht.

Metas jüngster Versuch, persönliche Avatare zu erstellen, mag auf Kritik gestoßen sein. Diese bezog sich jedoch ausschließlich auf die schlechte Umsetzung eines großartigen Konzeptes. So wurde beispielsweise ein Bild des digitalen Avatars von Firmengründer Mark Zuckerberg vor dem Eiffelturm mit Grafiken aus Videospielen der 90er Jahre verglichen. Das ist ein Beleg für den bedauerlichen Mangel an Qualität in der endgültigen Ausführung.

Blockchain-Domain-Namen drängen zunehmend auf den Markt. Nutzer können nun eine einzigartige Verbindung zu ihren Krypto-Geldbörsen und Profilen haben. Angesichts der Entwicklungen in der AR- und VR-Technologie ist ein personalisierter Avatar ein potenziell wichtiges Glied in der Kette des immersiven Engagements.

Das Tüpfelchen auf dem i ist, dass diese Avatare allmählich zwischen den Plattformen interoperabel werden. Der eigene Avatar kann dadurch in nahezu allen Lebensbereichen funktionieren. Er kann sowohl als Eintrittskarte für ein Konzert als auch als Sicherheitsfreigabe für das Büro dienen. Einzelhandelsgeschäfte können Preise und Produktauswahl auf der Grundlage der individuellen Einkaufshistorie ändern, die über die Cloud leicht zugänglich ist. Künstler können neue Wege finden, um ihr Publikum durch Live-Veranstaltungen und digitale Werbegeschenke zu begeistern.

Unternehmen verbessern mit den persönlichen Avataren ihrer Mitarbeiter die Sicherheit und den Datenschutz. Die Verknüpfung von Berechtigungen mit einem Avatar für Mitarbeiter macht komplizierte Sicherheitsverfahren und teure Etiketten oder Ausweise überflüssig.

Der Kundenservice ist ein weiterer Bereich, den das Metaverse verbessern kann. Jedes Unternehmen, das einen personalisierten Service für seine Kunden benötigt, kann in Echtzeit einen virtuellen Servicekiosk mit einem Avatar des Serviceleiters einrichten.

Das verbessert die Qualität von Serviceprozessen, macht sie effizienter und zugänglicher. Es wäre eine praktikable Alternative zu den langen Warteschlangen, mit denen viele Kunden in den Filialen oder am Telefon tagtäglich konfrontiert sind.

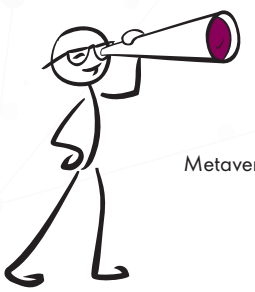
Metaverse könnte auch bei der Logistik von Trainingsprogrammen für neue und bestehende Mitarbeiter helfen. Es bietet eine außergewöhnliche Integration von Online- und Offline-Sitzungen, wie sie in dieser Weise bisher nicht möglich war. In der Tat können hybride Arbeitsabläufe von solchen Implementierungen profitieren – nach der Pandemie ist das eine willkommene Innovation für den Arbeitsplatz. Pandemie.

Ein neuer Anfang

Das Metaverse verändert jetzt schon die Landschaft vieler Branchen weltweit. Das Potenzial ist enorm. Schon die derzeitigen Anwendungen haben den Weg für weitere Verbesserungen und Innovationen geebnet.

Mit seinen offensichtlichen Vorteilen und seiner immensen Reichweite ist das Metaverse ein Game Changer für große und kleine Unternehmen.

Vijay Pravin



MEHR WERT

Mehr zum Thema Metaverse finden Sie unter:
www.it-daily.net/spezial/web3

Der Schlüssel zum Erfolg

AUCH IN KRISENHAFTEN ZEITEN DIGITALE LÖSUNGEN ZUR MARKTREIFE BRINGEN?

Energiekrise, Inflation, globale Entlassungswelle im IT-Bereich: Wie schaffen es Unternehmen, trotz der erschwerten Bedingungen innovative technologische Lösungen auf den Markt zu bringen? Die Business Area Digital von Körber, einem Technologiekonzern mit Wurzeln im Maschinen- und Anlagenbau, ist mit dieser Herausforderung vertraut. Das Geschäftsfeld nutzt künstliche Intelligenz (KI), um die Effizienz in der Produktion zu steigern und diese nachhaltiger zu gestalten. Die Strategie, die das Unternehmen anwendet, um schnell wachsende KI-zentrierte SaaS-Unternehmen aufzubauen, verbindet langjährige Erfahrung in den Märkten, wo die Lösungen eingesetzt werden sollen, mit einer Start-up-Unternehmenskultur.

Das Erfolgsrezept von Körber Digital basiert auf der richtigen Mischung aus fundiertem Branchen-Know how der Märkte, für die die Lösungen entwickelt werden und einem tatsächlich gelebten digitalen Mindset. Das bedeutet, dass nicht nur digitale Lösungen und Portfolios mit einem ergebnisorientierten Konzept entwickelt werden. Wichtig ist auch die Unterstützung der Mitarbeiter beim Aufbau von digitalen Kompetenzen. Dieses Mindset spiegelt sich darüber hinaus in der Organisationsstruktur wider, mit der eigens kreierten Digitalsparte. Körber Digital ist ein eigenständiger Geschäftsbereich, der so agieren kann wie ein unabhängiges Venture Capital-finanziertes Venture Studio. Das Geschäftsfeld fokussiert sich darauf, digitale Lösungen zur Marktreife zu bringen, die drängende Probleme von Unternehmen der produzierenden Industrie lösen.

Kundenorientierte Hilfestellung

User-Zentriertheit ist hier das Stichwort. Viele Unternehmen gehen das Thema Digitalisierung falsch an: Sie starten den Denkprozess von der Technologie-Seite her und nicht bei der Identifizierung und Lösung von akuten Problemen im Unternehmen oder avisierten Markt. Fundiertes Fachwissen bietet die perfekte Basis, um kundenorientiert Hilfestellung für die Digitalisierung in der Produktion zu bieten.

Mithilfe eines strukturierten und agilen Prozesses, der von der Problemdefinition, den Ideen zur Problemlösung, der Pro-

duktentwicklung, der Überprüfung der technischen Umsetzbarkeit sowie Identifikation von ersten Kunden für den Markteintritt durchschnittlich nur ein Jahr dauert, ist es Körber Digital bereits wiederholt gelungen, eigenständige und innovative, digital-agierende Firmen auszugründen. Erfolgreiche Beispiele sind unter anderem die Unternehmen InspectifAI mit einer KI-Lösung für die pharmazeutische visuelle Inspektion und FactoryPal, dessen digitale Lösungen zu Effizienzsteigerungen in der Produktionslinie, Maschinenleistung und Gesamtrentabilität führen.

Der Weg zum Erfolg

Bei der Entwicklung von erfolgsversprechenden digitalen Produkten mit einem möglichst schnellen Return on Invest (ROI) sind insbesondere drei Faktoren entscheidend:

Die Unternehmenssparte nutzt ihre Stärken - wo es sinnvoll ist, wird auf die Ressourcen des Mutterkonzerns zurückgegriffen. Wo es weniger Sinn macht, geht sie neue, eigenständige Wege. Zentral dabei ist die Identifizierung von Maßnahmen, die dem Unternehmen dabei helfen, den Wert seiner Portfoliofirmen zu steigern. Dies erlaubt es, in bereits vorhandenen Strukturen mit höchster Geschwindigkeit bei klarem Fokus auf Markt und Produkt voranzuschreiten. Eine Empfehlung an IT-Entscheider: Die Stärken und Ressourcen des eigenen Unternehmens genau kennen, Vorhandenes gewinnbringend einsetzen, aber auch mutig neue Pfade beschreiten. Diese Flexibilität kann erfolgsentscheidend sein in herausfordernden Marktzeiten.

Bevor sich Körber Digital dazu entscheidet, eine Firma auszugründen, ist die Idee durch einen anspruchsvollen Prozess gelaufen, der Nutzbarkeit, Erwünschtheit und Machbarkeit prüft. Management und Team verwenden viel Energie darauf, die Produkt- und Unternehmensidee zu verifizieren. Die Produktentwicklung startet erst dann, wenn erste Kunden gewonnen wurden. Bei

> KI KANN MAN ALS VEHIKEL BEGREIFEN, ALS DNA DER PRODUKTE UND LÖSUNGEN. VIEL ENTSCHEIDENDER ALS DIE TECHNOLOGIE IST ABER DAS RICHTIGE MINDSET UND DIE PASSENDE STRATEGIE.
>
> **Daniel Szabo,**
> **CEO Business Area Digital von Körber,**
> **www.koerber-digital.com/**

dieser Herangehensweise investieren Mitarbeiter und Führungskräfte bewusst mehr Energie, um das Risiko von Beginn an zu reduzieren. Alle neuen Lösungen werden vor Markteinführung über verschiedene Wege gründlich geprüft.

Neben dem richtigen Produktentwicklungsprozess ist die Unternehmenskultur der Top-Erfolgstreiber. Es gibt kein Schema F, das jedem Team und jedem Unternehmen zu einer digital ausgerichteten Unternehmenskultur verhilft. Doch wer als Manager die folgenden wichtigen Meilensteine berücksichtigt, wird mittel- und langfristig eine innovative Umgebung schaffen:

- Bestandsaufnahme der vorherrschenden Realität und konkrete Definition des Soll-Zustandes. Elementar ist es, die Mitarbeiter in den Prozess zu integrieren.
- Definition eines übergeordneten unternehmerischen Werteprinzips und dessen Übersetzung in konkrete Verhaltensprinzipien. Diese sollten so konkret wie möglich formuliert sein und die Kultur des Entrepreneurships stützen.
- Etablierung von Mechanismen, um alle Mitarbeiter verantwortlich zu halten, diese Kultur mit Leben zu füllen.

Wettbewerbsvorteil durch KI

Wettbewerbsvorteile entstehen durch eine intelligente Nutzung von Daten. Daher legt die Business Area Digital den Fokus auf KI, mit der Mission, einen tatsächlich messbaren Kundennutzen zu generieren. Dies verbindet sich mit dem Anspruch, schon heute Lösungen anzubieten, die die Kunden fit für die Zukunft machen und gleichzeitig einen positiven Effekt auf Gesellschaft und Umwelt haben. Dabei kann KI Potenziale in der Fertigung und Lieferkette freisetzen, zu denen reine Soft- und Hardware nicht fähig ist. KI dient hier dazu, den Menschen zu empowern und sie kann viele der dominanten Probleme der herstellenden Industrie adressieren wie etwa den Fachkräftemangel oder die Net Zero-Challenge.

Der Schlüssel zum Erfolg: Mindset und die richtige Strategie

KI kann man als Vehikel begreifen, als DNA der Produkte und Lösungen. Viel entscheidender als die Technologie ist aber – sowohl für den Erfolg von KI-Lösungen als auch für das Unternehmen selbst – das richtige Mindset und die passende Strategie. Dazu gehört, Strukturen zu schaffen, die Innovationskraft fördern. Dafür ist es unabdingbar, dass ein Entrepreneurdenken in der Organisation verankert wird über alle Ebenen hinweg. Darüber hinaus sollte das Management die so geschaffene Kultur mit Tools und Methodiken unterstützen, um Innovationsprozesse zu ermöglichen.

Mit diesen Ansätzen gelingt es Unternehmen auch in herausfordernden Zeiten digitale Lösungen erfolgreich zur Marktreife zu bringen und einen möglichst schnellen ROI zu erzielen.

Daniel Szabo

ERP: The next big thing

SIND LÖSUNGEN AUF LOW-CODE-BASIS DIE ZUKUNFT?

Wer den Begriff „Low-Code" hört oder liest, wird entweder aufhorchen oder fragend blicken. Diejenigen, die aufhorchen, wissen bereits, dass sich hinter „Low-Code" eine mögliche Revolution in der Softwareentwicklung versteckt. Viele sprechen schon von Low-Code als Enabler der digitalen Transformation oder von der nächsten Evolutionsstufe der Softwareentwicklung.

Diejenigen, die noch fragend blicken, werden mit dem Begriff nicht viel anfangen können. Low-Code hört sich auch irgendwie seltsam an: Wenig-Code? Ihnen sei gesagt, dass es bei Low-Code nicht um weniger Programm-Code, sondern eher um einen geringeren Codierungsaufwand geht. Mehr dazu später.

In dem folgenden Artikel möchten wir Ihnen den Low-Code-Ansatz näherbringen und zeigen, wie man damit die nächste Evolution anstoßen kann: Die Entwicklung einer flexiblen, maßgeschneiderten und passgenauen ERP-Lösung auf Basis von Low-Code anstelle der veralteten Legacy-Software.

Vom Code zum Low-Code

Jahrzehntelang wurden Softwarelösungen aufwendig von gelernten Programmierern mit Hilfe unterschiedlichster Programmiersprachen entwickelt. Die Entwicklung komplexer Software wie beispielsweise einer ERP-Software dauerte (und dauert) relativ lange und ist in der Regel kostenintensiv, weil ausgebildete und damit gut bezahlte Entwickler notwendig sind, die oftmals Wochen oder Monate an einem Projekt arbeiten. In Zeiten des Fachkräftemangels verschärfte sich die Situation für die Softwareunternehmen zusehends. Ist ein Produkt einmal fertig, wird es viele Jahre durch Updates, Ergänzungen und Erweiterungen gepflegt und damit immer komplexer. Dahinter steckt die Strategie der Hersteller, eine möglichst breite Menge von Kunden bedienen zu können.

Beispielsweise im ERP-Bereich ging man davon aus, dass alle Prozesse größtenteils standardisiert abgebildet werden

Low-Code-Entwicklung ist wie Bausteine zusammensetzen.

können. Allenfalls wurden Individualisierungen für unterschiedliche Branchen erstellt. Eine tiefere Individualisierung und Anpassung an spezifische Prozesse war nur über Sonderprogrammierung möglich, bei der das Entwicklerteam des Herstellers anrückte und in vielen Personenstunden den Programmcode anpasste. Solche Projekte wurden langwierig, teuer und führten am Ende doch nicht zu einer 100prozentigen Abdeckung aller Prozesse. Dennoch werden viele von Ihnen als Altlasten immer noch gepflegt und am Leben gehalten.

Um aus diesem Teufelskreis ausbrechen zu können, suchten Experten nach Alternativen zur klassischen Softwareentwicklung, mit denen schneller, effizienter und gegebenenfalls auch ohne – oder zumindest ohne weitreichende – Programmierkenntnisse entwickelt werden könnte. Eine dieser Alternativen ist die sogenannte Low-Code-Entwicklung (zu Deutsch geringer Codierungsaufwand).

Der Begriff Low-Code wurde bereits 2014 vom US-amerikanischen Marktforschungsunternehmen Forrester Research geprägt. Die Low-Code-Entwicklung propagiert das Erzeugen von Anwendungen nahezu ohne handgeschriebenen Programmcode durch einfaches Zusammenklicken vorgefertigter Softwarebausteine. „Konfigurieren statt programmieren" lautet die zugrunde liegende Idee. Möglich wird dies durch Low-Code-Plattformen.

Die alte Klick-Idee

Dabei bezieht sich das „low" nicht auf die Qualität des finalen Programmcodes, sondern auf die Code-Erstellung. Im Low-Code-Development werden Applikationen mithilfe einer grafischen Benutzeroberfläche aus fertigen Bausteinen in der Cloud „zusammengesteckt". Business-Applikationen wie ERP-Systeme werden im Unternehmen nach einer Art Baukastenprinzip vollständig ohne oder mit nur wenig Programmieraufwand zu einer maßgeschneiderten Lösung „konfiguriert". Der Anteil manueller Code-Entwicklung ist im Vergleich zur konfigurierten Code-Menge gering, also „low".

Softwareentwicklung per Drag & Drop. (Quelle: GEBRA-IT GmbH)

Man kann sich die „Konfiguration" vorstellen wie den Zusammenbau eines Hauses mit den Standard-Bausteinen eines dänischen Spielzeugherstellers aus Billund. Wer eine Softwareanwendung entwickeln will, erhält über Low-Code-Plattformen einen Baukasten mit vorgefertigten Formteilen, die man zu den unterschiedlichsten Systemen zusammensetzen kann.

Statt also selbst Quellcode zu schreiben und auf Basis aktueller Programmiersprachen zu codieren, bieten diese Plattformen bereits eine grafische Oberfläche (GUI), über die viele Bausteine über Pull-Down-Menüs und per „Drag-and-drop" aus dem Baukasten herausgefischt und zu individuellen Anwendungen grafisch sichtbar zusammengesetzt werden können.

Low-Code ist die logische Weiterentwicklung der Applikationsentwicklung, sozusagen die nächste Evolutionsstufe, um Business-Prozesse schneller, einfacher, flexibler und günstiger mit Software zu unterlegen. Solche Entwicklungsschritte gab es in der Softwareentwicklung regelmäßig. Denken wir an den Schritt von den Lochkarten zum Assembler zu Cobol zu C zu objektorientierten Sprachen wie Java und Python. Immer ging es um eine höhere Flexibilität, Effizienz und Einfachheit.

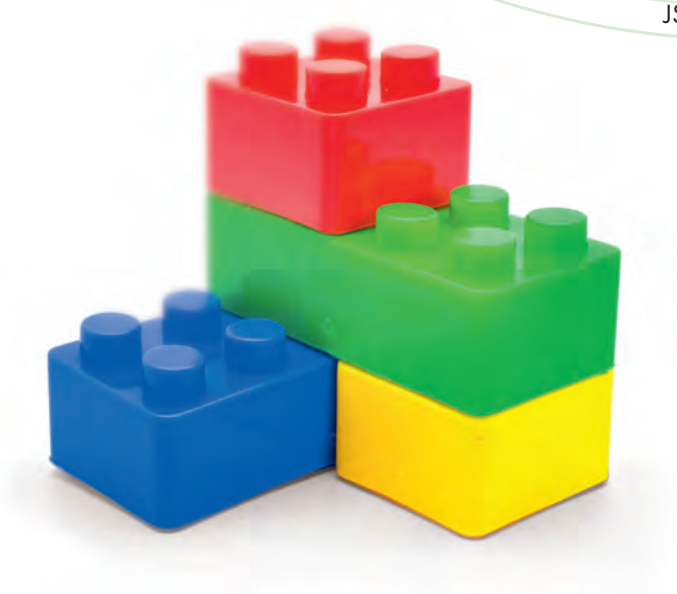
Low-Code-Plattformen

Wer Low-Code entwickeln möchte, nutzt dazu eine Low-Code-Plattform. Die Zahl der Anbieter und Lösungen ist derzeit

überschaubar, der Markt ist noch recht jung, wenn auch stark wachsend. Gartner prognostiziert beispielsweise, dass bis 2024 mehr als 65 Prozent aller Software-Programme mit Low-Code realisiert werden. Auch wenn die verschiedenen Plattformen unterschiedlichen Konzepten folgen, sind einige Punkte allen gemeinsam: Sie bieten eine Cockpit-ähnliche Entwicklungsplattform, mit der Browseranwendungen oder Apps interaktiv zusammengeklickt werden. Darunter liegt eine Geschäftslogikschicht für den Entwurf von Prozessen sowie eine Datenschicht zur Erzeugung von Geschäftsentitäten.

Die meisten Low-Code-Plattformen werden in der Cloud betrieben und sind als „Application-Platform-as-a-Service" (SaaS) konzipiert. Dies sind dann Web- oder Cloud-Dienste, die sämtliche Schritte des Low-Code-Development abwickeln können: Präsentation, Logik, Business-Integration, Datenverarbeitung und Authentifizierung oder Autorisierung. Es gibt jedoch auch Low-Code-Plattformen, die On-Premises installiert werden können.

Der wohl wesentlichste Unterschied liegt in der Art und Weise, wie der Programm-Code, der am Ende auch bei Low-Code-Plattformen vorhanden sein muss, erzeugt wird, wenn der Nutzer auf der Oberfläche seine Anwendung baut.



DIE VORTEILE VON LOW-CODE-ENTWICKLUNG GEGENÜBER KLASSISCHER ERP-ENTWICKLUNG WIEGEN SCHWER, DIE NACHTEILE SIND GUT BEHERRSCHBAR.

Frank Bärmann, freier Journalist und PR-Berater, conpublica, www.conpublica.de

Fertiger Code „wie von Geisterhand"

Bei einigen Systemen wird im Hintergrund beim Zusammenklicken der Elemente von einem Algorithmus „wie von Geisterhand" ein Code geschrieben, der kompiliert wird und dann ausführbar ist.

Rendering on the fly

Viel spannender ist jedoch die Variante, bei der zunächst kein ausführbarer Code generiert wird. Vielmehr werden alle erforderlichen Informationen in Textdateien (zum Beispiel JSON) und einer SQL-Datenbank abgelegt. Wenn der Endnutzer die Webseite aufruft, interpretiert der Webserver die Informationen und generiert den Code für den Browser „on the fly", der die finale Seite rendert. Diese State-of-the-Art-Webtechnologien kennen wir beispielsweise vom Content-Management-System WordPress.

Die Entwicklung von ERP-Lösungen mit Low-Code

Low-Code-Plattformen können für die Entwicklung verschiedenster Anwendungen eingesetzt werden. Ein Bereich, wo Low-Code bislang kaum genutzt wird, ist die Entwicklung von ERP-Lösungen. Das mag daran liegen, dass der Markt für ERP-Systeme sehr breit und vielfältig ist und einige Hersteller schon sehr viele Jahre am Markt sind und mit ihnen die eingesetzten Softwaresysteme.

Wie eingangs beschrieben, existieren ihre Lösungen zum Teil schon viele Jahre und wurden kontinuierlich weiterentwickelt, angepasst, erweitert, modernisiert und dadurch immer komplexer und schwerfälliger. Gängige ERP-Systeme decken heute nahezu alle Standard-Prozesse im Unternehmen ab, können aber nur schwer „customized" werden. Sie schleppen durch den jahrelangen Aufbau einen Ballast an Code und Funktionen mit, von dem im Einzelfall nur 20 Prozent im Kundenprojekt benötigt wird. Oft hören die Kunden den Satz "Sie müssen Ihre Prozesse leider ein wenig anpassen. Sonst wird der Aufwand für eine individuelle Anpassung der Software sehr aufwendig und teuer".

Die fortschreitende Digitalisierung zwingt Unternehmen aller Größen und Branchen aber dazu, immer flexibler auf Kundenwünsche einerseits und auf Marktveränderungen andererseits reagieren zu können. Die Anforderungen an die Unternehmen werden immer vielfältiger und komplexer. Ein modernes, schlankes, flexibles und schnell anpassbares ERP-System ist erforderlich. Hier stoßen viele der etablierten, jedoch oft veralteten Systeme an ihre Grenzen.

Mit Low-Code den Entwicklungsprozess neu denken

Diesen Mangel erkannten die Gründer der Aachener GEBRA-IT GmbH und schafften eine eigene cloudbasierte Entwicklungsplattform auf Basis von Low-Code (GEBRA Suite). Diese bietet wie alle Low-Code-Plattformen die typische intuitive grafische Benutzeroberfläche und ar-

beitet interpretativ mit modernen Technologien wie JSON, SQL und JavaScript. Auf dieser Grundlage wurde dann der gesamte Entwicklungsprozess einer ERP-Lösung umgekrempelt und neu gedacht.

Selbstverständlich haben die Gründer das „ERP-Rad" nicht komplett neu erfunden. Vielmehr flossen über 30 Jahre Erfahrung mit ERP-Projekten in die neue Lösung ein. Der Ansatz ist, auf Basis von Erfahrung und Best-Practice mit Hilfe der Low-Code-Plattform viele Grundmodule für einen Baukasten zu entwickeln, die grundsätzlich in jeder ERP-Lösung wiederkehren. „Wir beginnen nicht mit einem weißen Blatt, sondern starten bei der ERP-Lösung für Kunden mit unserem Basis-Baukasten", erklärt Geschäftsführer Udo Hensen. „Im Unterschied zur herkömmlichen ERP-Entwicklung übernehmen unsere ERP-Berater die Konfiguration der endgültigen Kundenlösung. Dies geschieht auf Basis des Baukastensystems".

Solche „Laien-Programmierer" werden in der Branche als Citizen Developer bezeichnet. Sie stehen in engem Kontakt mit dem Kunden, den Abteilungen und Mitarbeitern. Die vorhandenen Prozesse und die Wünsche des Kunden werden im Grunde „Stein für Stein" zu der ERP-Lösung zusammengebaut. Dabei sind Anpassungen, Veränderungen, Ergänzungen durch den Low-Code-Ansatz in Windeseile umgesetzt. Am Ende steht eine dem Kunden auf den Leib geschneiderte ERP-Lösung zur Verfügung.

Citizen Developer klicken eine maßgeschneiderte ERP-Lösung zusammen.
(Quelle: GEBRA-IT GmbH)

Nachteile von ERP auf Low-Code

Selbstverständlich ist Low-Code nicht der Stein der Weisheit, wenn auch die Technologie einige Vorteile gegenüber der klassischen Softwareentwicklung mitbringt. Die neue „Freiheit" bei der Entwicklung von Applikationen bedeutet auch Verantwortung. Wer völlig flexibel eine Lösung konstruieren kann, dem kommen immer neue Wünsche und Anforderungen in den Sinn. Es besteht die Gefahr, dem Kunden jeden „goldenen Henkel" zu bauen, obwohl es nicht der optimale Weg wäre. Das Beraterteam braucht Führungsstärke sowie ein großes Prozess- und IT-Wissen. Werden zu Beginn eines Projekts die Anforderungen, Ziele und Meilensteine nicht genau in einem Lastenheft definiert, besteht das Risiko, immer wieder neue Anforderungen nachzulegen und sich beim Aufbau von neuen Prozessen zu verzetteln. Daher sollte ein Lastenheft unabhängig vom Low-Code bei einem jeden ERP-Projekt vorhanden sein.

Fazit

Sicher ist Low-Code ein spannender und vielversprechender Ansatz, um zukünftig zentrale Unternehmensanwendungen schneller und flexibler zu entwickeln als bisher. Low-Code wird aber den klassischen Entwicklungsweg vorerst nicht komplett ersetzen, allein weil es viel zu viele Unternehmensanwendungen gibt, die immer noch zuverlässig ihren Dienst verrichten und vorerst nicht gelöst werden (können). Die Gartner-Prognose, dass bis 2024 mehr als 65 Prozent aller Software-Programme mit Low-Code realisiert werden, erscheint realistisch.

Für Unternehmen, die in neue Unternehmensanwendungen wie ERP-Software investieren wollen/müssen, stellt der Low-Code-Ansatz jedoch eine ernstzunehmende Alternative zu den klassischen Lösungen dar. Die Vorteile von Low-Code-Entwicklung gegenüber klassischer ERP-Entwicklung wiegen schwer, die Nachteile sind gut beherrschbar. Warten wir ab, ob Gartner recht behält.

Frank Bärmann

Quelle:
Vgl. Computerwoche vom 27.01.2022 https://www.computerwoche.de/a/booster-fuer-softwareentwickler,3552470

Datenanalysen mit Python

DER SCHLÜSSEL ZUR DIGITALEN WETTBEWERBSFÄHIGKEIT

Data Analysis und Data Science liegen im Trend. Sowohl weltweit als auch in Deutschland steigt das Such-Interesse bei Google zum Thema Datenanalyse in den vergangenen Jahren immer weiter an. Und auch auf den bekannten Jobplattformen finden sich mehr und mehr Stellenangebote, die sich mit der Auswertung und Weiterverarbeitung von Daten befassen.

Dabei ist die Analyse von Unternehmensdaten nichts Neues. Alleine die Beobachtung von Warenangebot und –nachfrage und die entsprechende Reaktion darauf – sei es durch eine Anpassung des Preises oder der Angebotsmenge – stellt eine Datenauswertung und eine darauf aufbauende Optimierung dar. Für einige Unternehmen endet die Auswertung bereits hier, dabei verbirgt sich in der Analyse ihrer Daten noch viel mehr Potential. Warum eine tiefgreifende Katalogisierung und Auswertung von Unternehmensdaten heute nahezu unverzichtbar ist und welche Tools dafür am besten in Frage kommen, möchte ich im Folgenden genauer beleuchten.

GROSSE DATENMENGEN UND WEITERVERARBEITUNG ERFORDERN SPEZIELLE ANALYSE-TOOLS. SO UMFANGREICH WIE DIE MÖGLICHKEITEN DER DATENANALYSE SIND, SO UMFANGREICH IST AUCH DAS ANGEBOT AN SOFTWARE UND PROGRAMMEN, UM DIE DATEN AUSZUWERTEN.

Prof. Dr. René Brunner, Dozent für Data Science an der Hochschule Macromedia und Kursleiter auf Udemy, www.udemy.com

Datenanalysen als Standardpraxis in deutschen Unternehmen

Viele, aber noch längt nicht alle Unternehmen haben bereits den Wert hinter ihren Daten erkannt. Laut dem Digitalisierungsindex Mittelstand 2020/2021, einer von der Telekom seit 2016 jährlich durchgeführten Benchmark-Studie zum Grad der Digitalisierung deutscher Betriebe, führen mittlerweile 76 Prozent der deutschen Unternehmen regelmäßige Datenanalysen durch.

Zu den am häufigsten analysierten Daten gehören allgemeine Geschäftsdaten wie Kunden-, Produkt- Material- und Lieferantendaten sowie Daten zur Technik und Infrastruktur, welche von 6 von 10 Unternehmen regelmäßig ausgewertet werden. Rund die Hälfte der Unternehmen analysiert zudem Transaktionsdaten, darunter Daten aus Rechnungen, Lager- und Lieferscheinen. Logdaten aus IT-Systemen (36 Prozent), externe Daten (30 Prozent), Daten aus sozialen Netzwerken (26 Prozent) und Sensordaten (17 Prozent) werden bisher noch etwas seltener ausgewertet. Dies dürfte sich aber schnell ändern. Je nach Datenkategorie geben nämlich zusätzliche 19 bis 25 Prozent der Unternehmen an, diesen Daten zukünftig in ihre Analyse miteinbeziehen zu wollen.

Kosten & Effizienz

Datenauswertungen sparen Kosten und steigern die Effizienz. Die Gründe für diese Entwicklung sind offensichtlich. Das Sammeln relevanter Daten, ihre Einordnung und Analyse ermöglichen es Unternehmen, den Geschäftsablauf auf verschiedene Arten zu optimieren. So geben Produktionszeiten und –mengen, die Nachfrage der Kunden und ihr Surfverhalten auf den unternehmenseigenen Webseiten und Online-Shops oder auch

die Auslastung der eigenen Mitarbeiter wichtige Aufschlüsse, wie man den Betrieb effizienter gestalten kann. Anhand dieser Daten lassen sich dann Vorhersagen zum zukünftigen Geschäftsbetrieb treffen – vom Kaufverhalten der Kunden, über das benötigte Angebot bis hin zur optimalen Planung der Zusammenarbeit mit Zulieferern und Transporteuren.

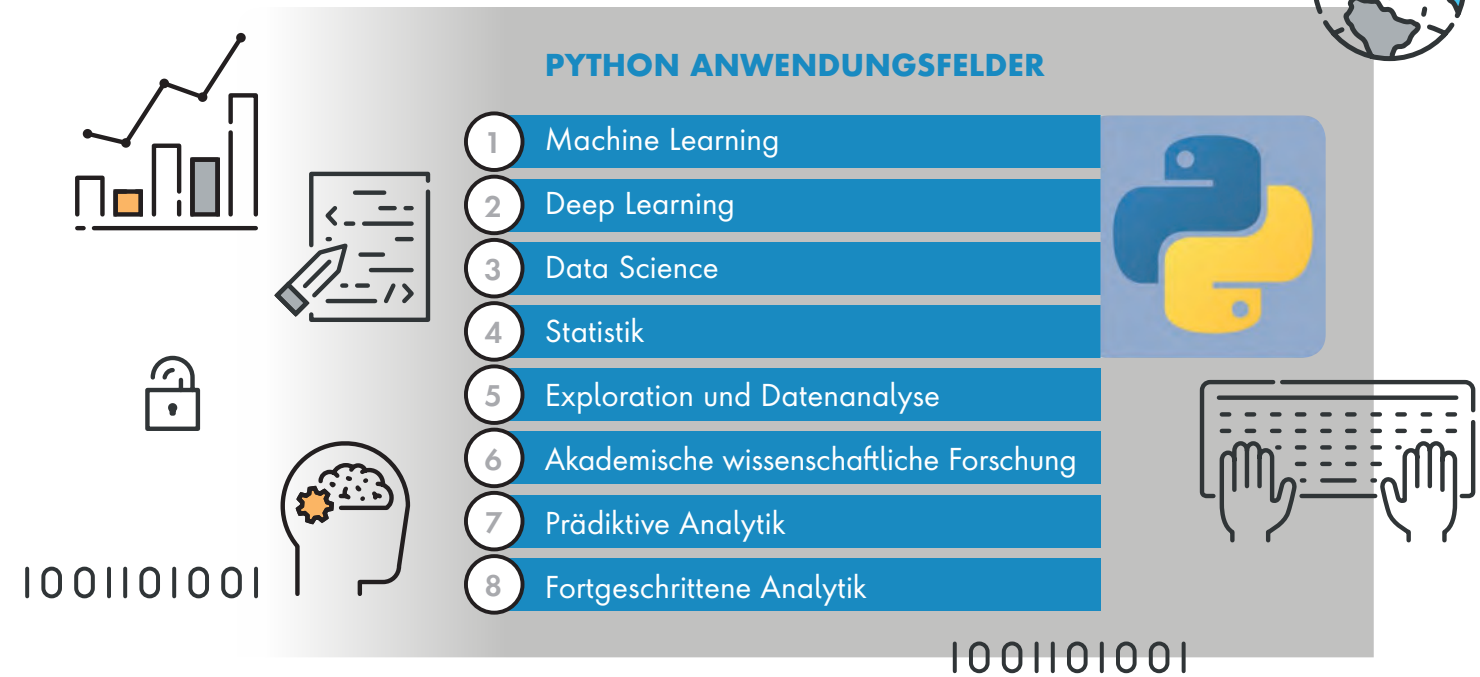
Dass sich diese Optimierungen bezahlt machen, belegt der Digitalisierungsindex. 74 Prozent der befragten Unternehmen, die Datenanalysen betreiben, konnten dadurch ihre Kosten senken, 73 Prozent haben ihren Umsatz gesteigert und 70 Prozent geben an, ihre Geschäftsprozesse verbessert zu haben. Zudem sind zwei von drei Unternehmen überzeugt davon, dass sie durch regelmäßige Datenanalysen ihre Wettbewerbsfähigkeit verbessern können.

Die Datenanalyse

Große Datenmengen und Weiterverarbeitung erfordern spezielle Analyse-Tools. So umfangreich wie die Möglichkeiten der Datenanalyse sind, so umfangreich ist auch das Angebot an Software und Programmen, um die Daten auszuwerten. Je nach Programm bieten sich dabei ganz unterschiedliche Anwendungsmöglichkeiten – von der einfachen Datenauswertung bis hin zur Visualisierung in Grafiken und Diagrammen, von allgemein zugänglichen Programmen bis hin zu spezifischen Programmiersprachen, die eine anschließende Weiterverarbeitung in Form von KI oder maschinellem Lernen ermöglichen.

Tools zur Auswertung

Eine Programmiersprache, die in diesem Zusammenhang besonders hervorsticht und sich immer größerer Beliebtheit erfreut, ist Python. Haben im Annual Developer Survey von Stack Overflow 2017 noch knapp 32 Prozent der Befragten angegeben, die Open-Source-Sprache zu nutzen, waren es bei der Umfrage im Jahr 2022 schon rund 48 Prozent. Hinzu kommt, dass Python sehr häufig von jungen Programmierern in der Ausbildung oder im Studium genutzt wird. Etwa 58 Prozent derjenigen, die das Programmieren lernen, nutzen Python. Dass die Sprache gefragt ist, zeigt sich auch im 2023 Workpla-



ce Learning Trends Report von Udemy, der Online-Plattform für Lernende und Lehrer. Laut dem Report ist Python bei Unternehmensmitarbeitern, die über Udemy Business lernen, die am häufigsten erlernte Programmiersprache und nach Amazon Web Services auch der am zweithäufigsten erlernte Skill im technischen Bereich. Der Anteil der Nutzer wird damit im Laufe der kommenden Jahre also noch weiter steigen, womit Python auf dem besten Weg ist, JavaScript als meistgenutzte Programmiersprache abzulösen.

Doch was macht die Sprache so beliebt und relevant für die Datenanalyse? Vergleicht man Python mit anderen Programmiersprachen wie JavaScript oder R so bietet Python einen deutlich schnelleren Einstieg. Durch die einfache und verständliche Syntax sowie eine geringe Anzahl an Schlüsselwörtern ist es eine der am leichtesten zu erlernenden und zu verwendenden Programmiersprachen. Zudem ist es durch seine schwache Typisierung und flexible Umwandlung von Datentypen sehr anwenderfreundlich.

Neben dem einfachen Einstieg überzeugt Python auch mit einer vielseitigen Anwendbarkeit. Dies ist vor allem der sehr umfangreichen Standardbibliothek von Paketen zu verdanken. Dank vorgefertigter Module kann Python viele verschiedene Arten von Operationen durchführen, von der Datenverarbeitung, Visualisierung und statistischen Analyse, über Webanwendungen und Automatisierung bis hin zum Einsatz von Modellen für maschinelles Lernen und künstliche Intelligenz. Hinzu kommt, dass diese Bibliothek kontinuierlich erweitert wird. Alleine in den vergangenen fünf bis zehn Jahren wurden zahlreiche Open Source Tools für Python veröffentlicht, welche seitdem stetig weiterentwickelt werden – beispielsweise Tensorflow und Pytorch für KI-Anwendungen, MLFlow und Aporia für MLOps, PySpark für Big Data oder Apache Airflow für Workflow und Pipeline Orchestration.

Diese umfangreichen Einsatzmöglichkeiten und die einfach zu integrierenden Tools sind der Grund, warum Python für Data Analysis und Data Science mittlerweile alternativlos geworden ist. Das spiegelt sich auch in Umfragen zur Nutzung der Sprache wider. Laut dem Python Developers Survey 2021 der Python Software Foundation und JetBrains setzen über die Hälfte der Programmierer, welche Python als Hauptsprache nutzen, die Sprache zur Datenanalyse ein. Auf dem zweiten und dritten Platz folgen Webentwicklung (48 Prozent) und Machine Learning (37 Prozent).

All dies zeichnet ein klares Bild von der Beliebtheit und dem breiten Anwendungsspektrum der Sprache. Unternehmen finden in Python somit ein vielseitig und leicht einsetzbares Werkzeug, mit dem sie ihre Daten auswerten, visualisieren als auch weiterverarbeiten und damit ihre Effizienz wie auch Wettbewerbsfähigkeit in einer immer stärker digitalisierten Welt steigern können.

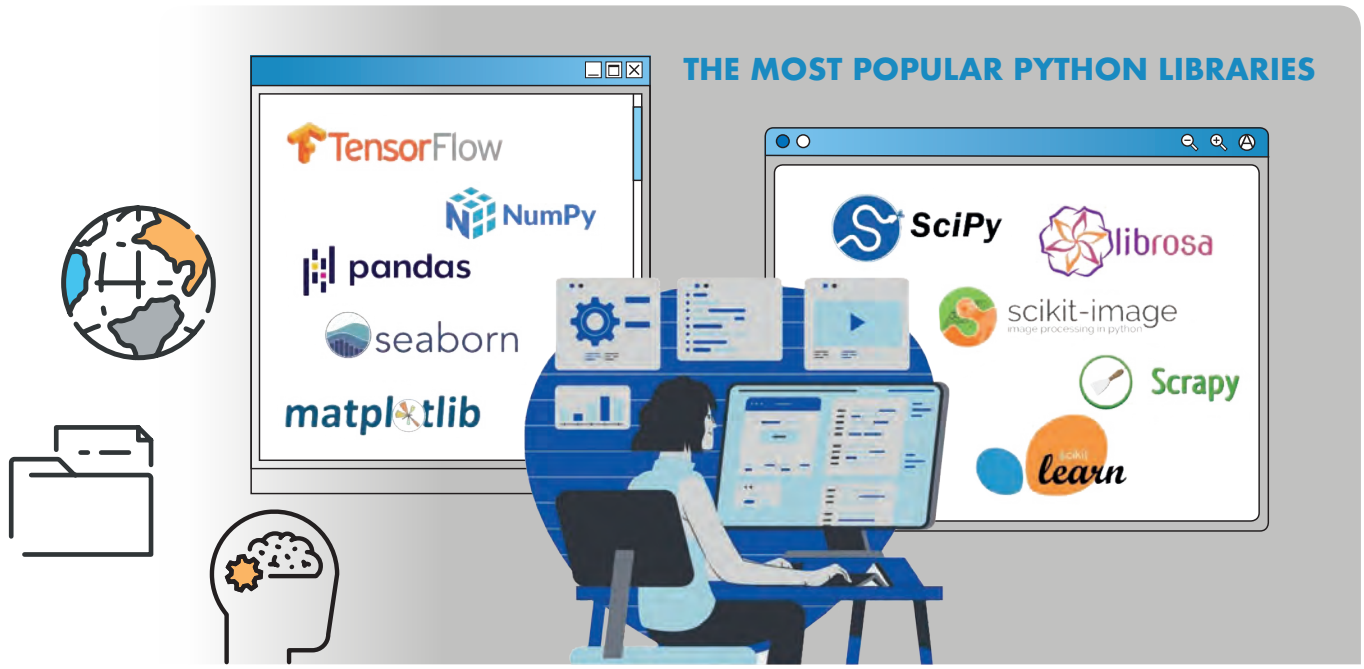
Prof. Dr. René Brunner

MEHR WERT

PYTHON

Mehr Informationen zum Einsatz von Python sowie praxisnahe Anleitungen zur Datenanalyse, Visualisierung und Machine Learning finden Sie unter **https://www.udemy.com/user/rene-brunner/**

Blog mit den Python Vorteilen: **https://bit.ly/3iVrJ73**



ZUKUNFT ODER REALITÄT?

DOKUMENTBASIERTE ANWENDUNGEN IN DER CLOUD

Wenn es um die Entwicklung und den Betrieb dokumentenbasierter Anwendungen geht, führt zukünftig kein Weg mehr an der Cloud vorbei.

Ziel der Trendstudie „Dokumentenbasierte Anwendungen in der Cloud. Zukunft oder Realität" war es, Antworten auf die folgenden Fragen zu dokumentenbasierten Anwendungen in der Cloud zu finden:

- Inwieweit denken Unternehmen heute bereits über solche Anwendungen nach und wie weit sind diese Planungen bereits fortgeschritten?
- Welche Vorteile verbinden Unternehmen mit dem Einsatz dieser Anwendungen?
- Welche Hürden und Hindernisse behindern Unternehmen bei der Verlagerung von dokumentenbasierten Anwendungen in die Cloud?
- Wie beurteilen Unternehmen den Zusammenhang zwischen Disruption und Cloud-Nutzung?

Die Ergebnisse der Umfrage wurden in einem Ergebnisbericht zusammengefasst.

WHITEPAPER DOWNLOAD

Das Whitepaper umfasst 25 Seiten und steht kostenlos zum Download bereit.
www.it-daily.net/Download

Die Zukunft von Business & IT

DAS BUSINESS BRAUCHT EINEN STRATEGISCHEN PARTNER – KEINE IT-ABTEILUNG

Alle IT-Organisationen, unabhängig ob interne oder externe Serviceprovider, sind heute stark gefordert. Nicht nur, dass es viele neue Technologien wie Cloud, künstliche Intelligenz oder Containerization zu integrieren und zu beherrschen gilt, es werden auch altbewährte Best-Practice-Verfahren hinterfragt. Mit neuen Methoden und dafür umso weniger Kontrollen wird versucht, die Innovation im Unternehmen zu fördern. Strategien, Budgets oder Pläne sind in einer VUCA-geprägten Welt (VUCA = Volatility, Uncertainty, Complexity, Ambiguity) irgendwie Makulatur geworden.

IT-Organisationen haben in den letzten Jahren viel in ihre Fähigkeiten investiert, um weg vom klassischen Technologieprovider hin zum verlässlichen Serviceprovider zu werden: Sie haben endlich einen Servicekatalog, um klar verständliche und gut strukturierte Services zu offerieren, und eine Serviceorganisation, die das verbriefte Versprechen auch einzuhalten vermag. Allerdings sind viele Organisationen noch nicht wirklich dort angekommen.

Aber auch reife IT-Organisationen hinken der Entwicklung des Business hinterher, obwohl sie von sich behaupten, über ein ausgeprägtes IT-Business-Alignment, eine auf die Business-Strategie noch so stringent ausgerichtete IT-Strategie und immer auch ein Ohr an der „Voice of the Customer" zu haben. Der Druck auf noch mehr Digitalisierung und der grundsätzlichen digitalen Transformation der Geschäftsausrichtung geht über die vorhandenen Fähigkeiten und Service-Angebote weit hinaus.

Positionierung der IT-Abteilung

Das Modell, in dem Business-Einheiten den internen IT-Abteilungen immer erklären können, was sie aktuell benötigen, um dann im sich schnell ändernden Markt rechtzeitig die richtigen Services anbieten zu können, reicht heute nicht mehr. Das Business ist selbst nicht mehr in der Lage, immer genau zu spezifizieren, was die neuen Herausforderungen sind. Es braucht heute mehr als einen Lieferanten, es braucht einen echten Partner, dem es vertraut und ohne den es keine einzige Business-Entscheidung mehr fällen wird.

CIOs müssen sich nun die zentrale Frage stellen, wie genau dies erreicht werden

kann. Wie kann sich die IT-Organisation positionieren und reorganisieren, damit ihre Rolle über die Position des Auftrag-erfüllenden IT-Organisation hinausgeht und sich zu einem konvergenten strategischen Partner verlagert und damit gemeinsam mit dem Business die Ergebnisse des Unternehmens verantwortet werden können.

Die Beziehung zu den Business-Einheiten

CIOs müssen als Erstes erkennen, dass man sich eine strategische Partnerschaft im Alltag und im erlebten Verhalten verdienen muss – sie wird nicht einfach deklariert oder vergeben. Der Wandel von der Position eines noch so ausgeprägten Serviceproviders zu einem strategischen Partner erfordert Zeit und eine klare und detaillierte Roadmap. Großangelegte agile Transformationen können vielleicht einen Beitrag leisten – aber in aller Regel beschäftigt sich die IT mit der Erlernung neuer Arbeitsmethoden damit wieder einmal primär mit sich selbst. Dabei sollten eher die Beziehungen zu den Business-Einheiten endlich im Vordergrund stehen.

Business Relationship Management (BRM) ist dabei die Schlüsseldisziplin zur Erlangung der strategischen Partnerschaft und dabei der beste Hebel, um den grössten Business-Mehrwert zu erzielen. Der CIO braucht BRM als „Change Agent", muss aber die Zusammenarbeit mit dem Business in der gesamten Organisation stärken. Er muss sich fragen, ob er weiterhin den Fokus auf die Beherrschung der komplexen Technologie legen will oder eine Kultur der Kreativität, Innovation und gemeinsamen Verantwortung im gesamten Unternehmen fördert, sodass ganzheitliche, innovative und wertorientierte Strategien entwickelt werden können, die den angestrebten Geschäftswert liefern.

Dass es in Zukunft weiterhin Provider braucht, die die Komplexität der Technologie beherrschen und obendrein auch sichere und verlässliche Services bereitstellen, steht außer Frage. Das Business braucht aber in der aktuellen Zeit eher einen glaubwürdigen Partner, der mit ihm die Roadmap der Zukunft gestaltet und Chancen wie aber auch Risiken teilt – und die verschiedenen Serviceprovider managt. Eine IT-Organisation muss sich positionieren, wo sie ihre Rolle in Zukunft sieht.

DAS BUSINESS BRAUCHT EINEN GLAUBWÜRDIGEN PARTNER, DER MIT IHM DIE ROADMAP DER ZUKUNFT GESTALTET UND CHANCEN ABER AUCH RISIKEN TEILT – UND DIE VERSCHIEDENEN SERVICEPROVIDER MANAGT.

Martin Andenmatten, Managing Director, Glenfis AG, www.glenfis.ch

Business-Alignment

Wenn es um echte Partnerschaft geht, greift das Business-Alignment allein viel zu kurz. Solange IT-Organisationen sich als Service Provider positionieren und ihre Leistungen so nahe an die Business-Bedürfnisse ausrichten wie nur möglich, solange sind sie auch nie wirklich Teil des Business und damit auch nicht gleichberechtigte Partner. Denn sie dienen dem Business primär als Support-Funktion und werden höchstens als vertrauenswürdiger Berater hinzugezogen.

Um als strategischer Partner anerkannt zu werden braucht es viel mehr als bloßer "Auftragnehmer" von Geschäftsanfragen zu sein. Strategische Partner unterstützen das Business bei der Entwicklung von Visionen und des Business-Demands sowie deren Bereitstellung in der Form, wie das Business den größten Nutzen daraus erzielt. Strategische Partnerschaft umfasst auch die Finanzplanung, die Formulierung einer gemeinsamen Strategie sowie – und das ist besonders wichtig – teilt die Verantwortung zum Erreichen der Business-Resultate. Nur so wird der CIO Teil des Business-Führungsteams und kann erfolgreich artikulieren, wie mit den Produkten und Dienstleistungen der IT die Geschäftsziele vorangetrieben werden.

Partnerschaft & innere Einstellung

Die Sprache ist dabei wichtig, weil sie direkten Einfluss darauf hat, wie wir denken und welche Botschaften wir kommunizieren. Wenn wir beispielsweise unsere Business Partnern als «Kunden» bezeichnen, so senden wir an uns und an alle, die zuhören, dass wir eine untergeordnete Beziehung haben – als Auftragnehmer und nicht eine gleichberechtigte strategische Partnerschaft. Ich möchte hier in Anlehnung an das Framework vom BRM Institute ein paar zentrale Begriffe neu positionieren:

#1 CAPABILITIES – NICHT PROZESSE

Wenn wir heute demonstrieren wollen, ob wir bestimmte Disziplinen in der IT beherrschen, verweisen wir oft auf das Vorhandensein von Prozessen: Demand Management, Portfolio Management oder Service Level Management. Wir sollten aber unser Augenmerk viel stärker auf die Capabilities legen, auf die Fähigkeit diese Disziplin im Rahmen der Bereitstellung von Produkten und Services sowohl sichtbar als auch hinter den Kulissen aktiv zu leben. Das heisst, die Mitarbeiter mit den notwendigen Kompetenzen und Skills sowie auch die notwendigen Technologien im Einsatz zu haben, diese Capabilities auch tatsächlich zu besitzen und zu beherrschen.

#2 KONVERGENZ – NICHT ALIGNMENT

Wenn wir von Business-Alignment sprechen, so sagen wir implizit auch, dass wir hinterherlaufen, um zu einem Business aufzuschliessen versuchen und um sich auf dessen Reise einzustellen. Dadurch entwickeln wir eher Silos als gemeinsame Teams. Besser wäre es, mit Hilfe von Business Relationship Management Capabilities die IT-Funktion in Business Teams zu konvergieren mit gemeinsamen Zielen und gegenseitigen Abhängigkeiten. In so einem konvergierten Status teilen sich die Teams die Ownership von Business-Strategien und Business-Ergebnissen.

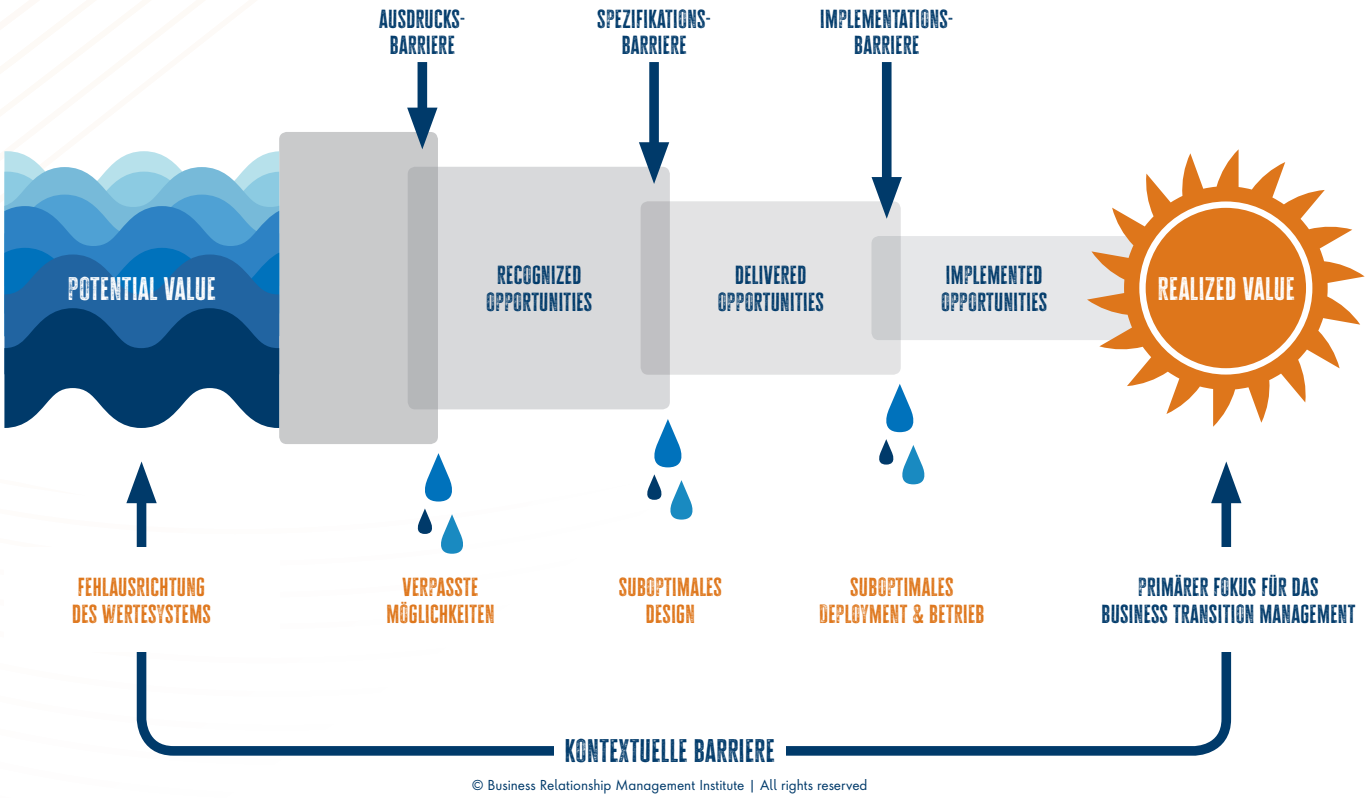
#3 SHARED OWNERSHIP – NICHT ABGEGRENZTE ACCOUNTABILITY

Echte Business Leader arbeiten heute an einer Kultur von geteilter «Ownership». Dies ist mittlerweile ein anerkannter Team-Ansatz, der den größten Business-Nutzen verspricht. Auch die IT muss Teil dieses Teams werden und jeder muss diese Ownership mittragen und damit auch den Erfolg und Misserfolg. Entsprechend hat mach auch die Entscheidungskompetenzen. Ganz im Gegensatz, dass irgendein Manager die «Verantwortung» trägt und die IT tut, was ihr gesagt wird.

#4 DEMAND SHAPING – NICHT DEMAND MANAGEMENT

Demand Management impliziert, dass man eine Methode zur Erstellung von Prognosen sowie zur Planung der Nachfrage von Produkten und Services hat. Das mag für eine Vogelperspektive notwendig und wichtig sein. Aber wenn es darum geht mit dem Business den Bedarf zu entwickeln, braucht dies viel mehr. Demand Shaping beinhaltet die Fähigkeit zwischen Demands mit hohem Business-Wert und geringeren -Wert zu differenzieren und dies mit dem Business zu erarbeiten. Das heisst auch, dass der Business-Case für das Business erarbeitet und damit die Prioritäten gesteuert werden können.

VALUE LEAKAGE ANSTELLE VALUE CREATION – WENN DIE SPRACHE NICHT BEHERRSCHT WIRD



#5 BUSINESS-CAPABILITIES – NICHT SERVICES

Service Management ist eine Schlüsseldisziplin von IT-Organisationen, um Services zuverlässig, sicher, konstant und gemäss den funktionalen Anforderungen auszuliefern. Wenn die IT dies nicht schafft, dann wird es schwierig, wenn nicht gar unmöglich, eine strategische Partnerschaft aufzubauen. Dass diese Services so funktionieren, wird aus Sicht des Business als selbstverständlich erwartet und der Wert ist so oft nicht ersichtlich. So wie wir heute den elektrischen Strom als «gegeben» betrachten, wenn wir ihn nutzen wollen, ohne uns über dessen Nutzen Gedanken zu machen.

In einer strategischen Partnerschaft oder einem konvergierten Team-Status sollten wir nicht mehr von Services sprechen, sondern von Business-Capabilities. Denn mit diesen «Business-Capabilities» hat das Business nun Fähigkeiten erworben, gewisse Geschäftspraktiken zu erbringen, welche klar identifizierten Nutzen und Mehrwert erbringen. Wichtig ist, dass das Business den Nutzen erkennt – der Service ist dann nur Mittel zum Zweck.

#6 PARTNER – NICHT KUNDEN

Der Begriff «Kunde» sollten nur noch für End-Benutzer verwendet werden. Interne Business Units sind die Partner, mit denen gemeinsam die Ziele und Geschäftserfolge erzielt werden.

#7 MEHRWERT – NICHT KOSTEN

Wenn wir bei unseren Services, respektive «Business-Capabilities» nur die Kosten gegenüberstellen, dann müssen wir uns nicht wundern, wenn das Business alles daransetzt, diese Kosten zu senken. Wir müssen lernen, den Mehrwert in Relation zu den Kosten transparent zu machen. Der Mehrwert setzt sich zusammen aus dem direkten und auch indirekten Nutzen minus die effektiven Kosten. Der Kostenfaktor sollte nicht der Schlüsselfaktor in der Diskussion mit dem Business sein. Bei der Diskussion mit dem Business muss sich alles immer um den Mehrwert drehen.

Fazit

Wenn es dem CIO nicht gelingt, das Vertrauen für eine gemeinsame digitale Zukunft zu gewinnen, dann wird sich das Business eigene Wege suchen. Vielleicht über einen neuen Chief Digital Officer, der die strategischen Initiativen stemmen darf. Dem CIO verbleibt dann die Rolle des technischen Zulieferers. Dann wird er und sein Team zur Legacy erklärt und damit zur Hypothek für das Unternehmen. Einen Kostenblock, den man lieber heute als morgen loswerden will. Die, die bleiben dürfen, sollen helfen, die Ruinen der Vergangenheit aufzuräumen. Die Zukunft gehört offenbar anderen: den verschiedenen externen Beratern und Lösungsanbietern, die unbelastet von der Vergangenheit mit neuen, disruptiven Methoden ans Werk gehen. Das muss nicht sein.

Die zunehmende Bedeutung der IT erfordert eine engere Zusammenarbeit, nicht nur als operative Ressource, sondern oft auch als strategisches Unterscheidungsmerkmal. In diesem neuen Umfeld arbeiten Unternehmen und IT nicht mehr als Dienstleistungsnehmer und -anbieter zusammen, sondern als Kollegen, die auf gemeinsame Ziele hinarbeiten. Dabei spielt die verwendete Sprache den Schlüsselfaktor. Sie kann Verhalten und Kultur in einer Organisation nachhaltig prägen. Also – was hindert uns daran, gleich damit anzufangen?

Martin Andenmatten

Microservices, APIs, Cloud & Headless

MACH-STRATEGIE: „HEADLESS“ NICHT VERGESSEN

MACH-Technologien bieten Flexibilität und stehen ganz oben auf der Tech-Agenda. Doch bei der Einführung hinkt Headless hinterher. Dabei gibt es gute Gründe, warum Unternehmen genau das nicht vergessen sollten.

Die Geschäftswelt ist schnelllebig und begünstigt Unternehmen, die sich flexibel an Veränderungen anpassen, innovativ sind und ihren Kunden stets neue und verbesserte Erfahrungen bieten können. Eine offene IT-Architektur, die das Hinzufügen und Ersetzen von Technologien erleichtert, spielt dabei eine wichtige Rolle.

Die MACH Alliance, ein Zusammenschluss unabhängiger Technologieunternehmen, hat es sich zur Aufgabe gemacht, Unternehmenstechnologien zukunftssicher zu machen und aktuelle und künftige digitale Nutzererlebnisse mit einem offenen und integrierten Technologie-Ökosystem voranzutreiben. MACH steht für Microservices, APIs, Cloud und Headless. Die Allianz unterstützt eine zusammensetzbare Architektur, in der jede Komponente austauschbar und skalierbar ist und durch agile Entwicklung kontinuierlich verbessert werden kann.

Die Beliebtheit von MACH-Technologien

Eine von der MACH Alliance in Auftrag gegebene Umfrage unter IT-Führungskräften hat gezeigt, dass die Einführung von MACH-Technologien ganz oben auf der Agenda der Technologieführer steht. Siebenundvierzig Prozent der befragten Führungskräfte gaben an, dass sie den Wechsel von monolithischen zu kombinierbaren „Best-of-Breed Lösungen“ anstreben. Ein deutlicher Anstieg im Vergleich zum Vorjahr, wo nur 36 Prozent den Wechsel anstrebten. Ferner äußerten 79 Prozent der Befragten die feste Absicht, ihrer Architektur in Zukunft mehr MACH-Komponenten hinzuzufügen. Cloud-native Anwendungen hatten mit 58 Prozent die höchste Priorität, Headless mit 23 Prozent die niedrigste.

Trotz seiner Vorteile ist es nicht überraschend, dass Headless die niedrigste Priorität hat. Für manche ist die Vorstellung, Front- und Backend-Dienste zu entkoppeln und jeden Teil separat zu betreiben und über APIs zu kommunizieren, beängstigend. Dies gilt insbesondere für IT-Mitarbeiter, die es gewohnt sind, mit einer traditionellen Software-Suite und nur einem Anbieter zu arbeiten.

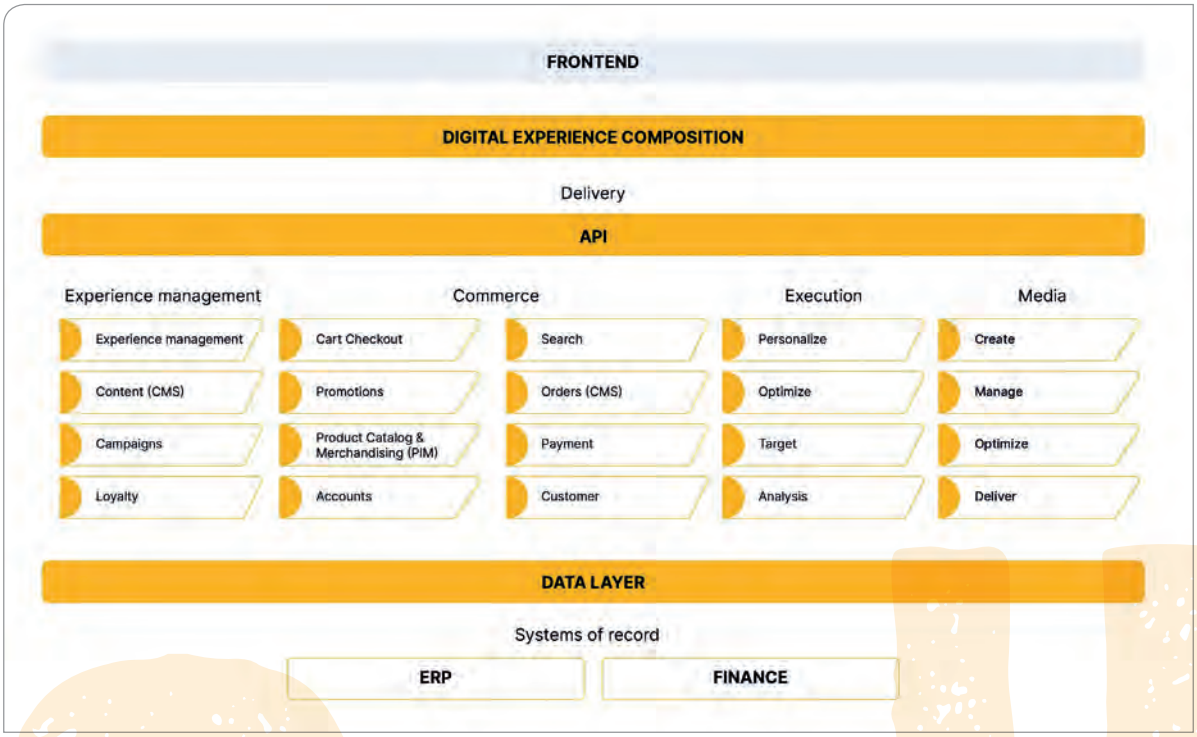
OBWOHL MACH-TECHNOLOGIEN GANZ OBEN AUF DER AGENDA VON TECHNOLOGIEFÜHRERN STEHEN, SOLLTEN CTOS UND SOFTWAREARCHITEKTEN DABEI DAS H IN MACH NICHT VERGESSEN.

Rob Daynes, VP of Strategy, Cloudinary, https://cloudinary.com

Doch der Nachteil dieses traditionellen Suite-Ansatzes ist, dass es ihm an der notwendigen Flexibilität und Anpassbarkeit mangelt. Das Hinzufügen neuer Funktionen wird schnell zu einer mühsamen, zeitintensiven Aufgabe. Technologien bei Bedarf schnell zu entfernen oder zu ersetzen ist fast unmöglich. Im Gegensatz dazu ermöglicht das Headless-Modell flexible Frontends, die nicht durch die Einschränkungen monolithischer Softwarearchitekturen eingeschränkt sind. Auch die Backend-Komponenten können gezielt an den IT-Bedürfnissen ausgerichtet werden.

Headless CMS und DAM

Zwei wichtige Anwendungsgebiete für Headless sind Content Management Systeme (CMS) und Digital Asset Management (DAM). Ein Headless CMS ist im Grunde ein Content Repository (Backend), das alle notwendigen Tools enthält, um Inhalte an einem Ort zu verwalten und sie über APIs an jedes mögliche Frontend in jeder Programmiersprache zu liefern. Bei einem CMS ist das Asset Management allerdings nur eine ergänzende Funktion und hat seine Grenzen. Etwa wenn es um die Verwendung verschiedener Formate, Größen/Auflösungen oder die Bildbearbeitung geht. Auch Funktionen wie Versionskontrolle, Berechtigungen, Tagging oder Transformationen sind oft nicht enthalten. Außerdem ist es schwierig oder unmöglich, von anderen Systemen auf die Assets zuzugreifen. An dieser Stelle kommt ein Headless DAM ins Spiel. Ein Headless DAM entkoppelt die Master-Asset-Bibliothek von der zentralisierten Schnittstelle und ermöglicht die Bereitstellung und Wiederverwendung digitaler Assets in verschiedenen Systemen über benutzerdefinierte oder



MACH-Architektur: Frontend und Backend sind voneinander entkoppelt (Headless); DAM-Aufgaben und CMS stehen als Microservices via APIs zur Verfügung.

vorgefertigte Schnittstellen. Headless DAMs ermöglichen die Speicherung aller Arten von digitalen Assets, wie etwa Bilder, 3D-Bilder, Videos oder PDFs. Über eine API können diese Assets von anderen Plattformen wie CMS, PIM, Commerce-Tools und CDNs abgerufen und an Websites oder Partner ausgegeben oder in Produktionsanwendungen wie Photoshop oder InDesign integriert werden.

Eine bessere Benutzererfahrung

Traditionell sind CMS bei der Erstellung und Verwaltung einer Website von entscheidender Bedeutung, da alle Inhalte, Daten, die Bearbeitungsoberfläche und der Code in einer einzigen Umgebung untergebracht sind. Der Headless-Ansatz erfordert auch immer noch ein CMS, um Webentwickler darüber zu informieren, wo auf einer Seite ein digitales Asset angezeigt wird. Das Headless CMS speichert die URL eines freigegebenen Assets aus dem Headless DAM. Wenn ein Asset überarbeitet oder ausgetauscht werden muss, wird diese Änderung im Headless DAM unter der Verwendung der gleichen URL vorgenommen. Sobald die Änderung durchgeführt ist, werden die Assets automatisch aktualisiert, egal wo sie verwendet werden. Da alle Assets an einem einzigen Ort gespeichert werden, ist es dank erweiterter Suche leicht, die richtigen Inhalte zu finden.

Einer der wichtigsten Gründe Headless DAM und CMS zu kombinieren, ist die mangelnde Flexibilität herkömmlicher CMS, wenn es um Management, Optimierung und Bearbeitung von Bildern und Videos geht. Beispiele wären etwa das Zuschneiden, die Wahl der Pixeldimension und der Dateigröße, das Hinzufügen von Overlays oder Filter, die Spezifikationen für verschiedene Browser und Bildschirmgrößen, die Ausrichtung und die Ladezeit. Bei einem herkömmlichen CMS-Ansatz muss jede dieser Manipulationen manuell in verschiedene Vorlagen für jeden Kanal eingegeben werden. Ein hoher Zeit- und Ressourcenaufwand, bevor eine Kampagne überhaupt gestartet werden kann.

Trotz der großen Vorteile ist die Umstellung auf Headless nicht für jedes Unternehmen geeignet, da es technische Ressourcen erfordert, die verschiedenen Softwarekomponenten zu integrieren und das Frontend anzupassen. Unternehmen, die sich bereits für ein Headless CMS entschieden haben, sollten auf jeden Fall den nächsten Schritt machen und ein Headless DAM hinzufügen. Ebenso sollten Unternehmen, die sich für eine MACH-Architektur entscheiden, ein Headless DAM einsetzen, das ihre visuellen Assets sowohl mit den alten als auch mit den neuen Teilen ihres Technologie-Stacks verbinden kann. Das Gleiche gilt für Unternehmen, wo mehrere Teams an der Erstellung von Inhalten für verschiedene Touchpoints arbeiten.

Nicht das H in MACH vergessen

Obwohl MACH-Technologien ganz oben auf der Agenda von Technologieführern stehen, sollten CTOs und Softwarearchitekten dabei das H in MACH nicht vergessen. In unserer visuell geprägten Wirtschaft spielen Bilder, Videos und Personalisierung eine entscheidende Rolle bei der Verbesserung von Nutzererlebnis, Conversions und Kundenbindung. Ohne ein Headless-System erfordert das Hinzufügen oder Austauschen von Videos und Fotos viel Zeit, Mühe und Ressourcen.

Rob Daynes

Human Experience Management

EIN MEILENSTEIN IN DER HR-TRANSFORMATION

Heutzutage – nach einer Pandemie, die neue Arbeitsweisen forciert hat – ist die Erfahrung, die Unternehmen ihren Mitarbeitern bieten, wichtiger denn je. Die Covid-19-Pandemie hat dazu geführt, dass Organisationen die archaischen Grundsätze des Personalwesens überdenken und eine integrativere und mitfühlendere Arbeitsweise entwickeln. Human Experience Management (HXM) ist der nächste Schritt in der Entwicklung von Human Capital Management (HCM)-Lösungen. Diese Anwendungen stellen den Mitarbeiter in den Mittelpunkt aller Personalfunktionen.

Menschen und ihre Bedürfnisse sollten im Mittelpunkt von HR-Funktionen stehen. Unternehmen sind dazu übergegangen, alle HR-Funktionen in einem hybriden Arbeitsmodell auf den Menschen auszurichten. Dazu gehört auch, dass die verschiedenen Phasen eines Mitarbeiters im Unternehmen erfasst und abgebildet werden. Auch wenn Covid-19 ein endemisches Stadium erreicht zu haben scheint, wird das Recruiting vielfach weiterhin remote durchgeführt – per virtuellem Gespräch oder Videokonferenz. Gleichzeitig spielt künstliche Intelligenz (KI) in allen HXM-Prozessen eine immer größere Rolle. Der Vorteil: KI kann die Vorbereitungszeit für solche Gespräche verkürzen und zum Beispiel geeignete Kandidaten identifizieren. Talente, die in die engere Wahl kommen, müssen bis zu ihrem Onboarding so nicht in die Büros kommen. Für den Kandidaten ist es bequemer und sicherer, den Einstellungsprozess ohne physischen Kontakt zu durchlaufen, bis dieser dann unbedingt erforderlich ist.

Ökosystem außerhalb der Arbeit

Es ist mittlerweile anerkannt, dass das Ökosystem der Mitarbeiter außerhalb der Arbeit eine große Rolle im Hinblick auf ihre Arbeitsleistung spielt. Immer mehr Unternehmen bieten Annehmlichkeiten wie Krippen für die Kinder ihrer Mitarbeiter an. Hinzu kommt eine höhere Flexibilität beim Arbeitsort ebenso wie bei den Arbeitszeiten an. Damit bieten Unternehmen ihrer Belegschaft die Möglichkeit, Arbeit und Privatleben zu verbinden, zum Beispiel, wenn sie ältere Menschen mit Begleiterkrankungen zu Hause pflegen.

Natürlich gab es eine Reihe dieser Angebote bereits vor der Pandemie. Aller-

dings war dies nur in ausgewählten Unternehmen der Fall. Jetzt werden sie breit angeboten – und von vielen Mitarbeitern auch verlangt. Firmen sind damit in der Lage, die Erfahrungen ihrer Angestellten zu verbessern. Selbst mit einem hybriden Arbeitsmodus haben die Mitarbeiter oft die Möglichkeit, die Tage zu wählen, an denen sie am liebsten ins Büro kommen. Der Grundgedanke dieser Praktiken besteht darin, den Komfort der Mitarbeiter zu gewährleisten sowie deren Sicherheit zu fördern.

Home-Office und hybride Arbeitsmodelle haben auch für Frauen Vorteile. Sie sind in der Lage, beispielsweise nach einer Mutterschaftspause in den Beruf zurückzukehren, und zwar in Form von Teilzeitarbeit, Gig-Work oder komplett im Home-Office – dies besteht neben dem traditionellen Beschäftigungsmodell. Es ermöglicht es den Unternehmen, sich für eine höhere geschlechtsspezifische Vielfalt in Teams und Funktionen einzusetzen.

Herausforderung Hybrid Work

Hybride Arbeitsmodelle haben jedoch ihre eigenen Herausforderungen. Es gibt keine einfachen Antworten auf die Frage, wie sich die Produktivität oder die Motivation einer dezentralisierten Belegschaft steuern lässt. Es ist außerdem nicht möglich zu kontrollieren, ob ein Mitarbeiter die Arbeitszeit nicht für einen Nebenjob nutzt.

Da sich die Unternehmenskultur auf die Strategie auswirkt, ist es von entscheidender Bedeutung, wie eine Organisation seine Arbeitskultur und -ethik in diesen Zeiten handhabt. Hier wird HR Analytics zu einem entscheidenden Faktor, da eine smarte Datennutzung und -analyse wichtig ist, um eine Vertrauenskultur zu schaffen.

Unternehmen können sich zudem überlegen, welche Funktionen sie beibehalten. Dies verringert nicht nur den Druck auf ein Unternehmen, einen Karrierepfad für eine größere Anzahl von Mitarbeitern zu entwerfen. Es gibt ihnen aber auch die Freiheit, unternehmerisch zu handeln und andere Aufgaben zu übernehmen oder sich einfach freizunehmen, solange ihr Arbeitsauftrag erfüllt ist.

Nachhaltigkeitsziele von Organisationen

Die wichtigste Herausforderung, der sich die Unternehmen stellen müssen, ist jedoch das Thema Nachhaltigkeit. Das hybride Arbeitsmodell hat die Kohlenstoffneutralitätsziele von Unternehmen möglicherweise über den Haufen geworfen. Vor der Pandemie konnten Unternehmen genaue Zahlen für den CO2-Fußabdruck vorlegen, weil die Mitarbeiter in der Zentrale sowie von den einzelnen Niederlassungen arbeiteten. Diese waren hinsichtlich der Nachhaltigkeit entsprechend ausgelegt bzw. optimiert.

Home-Office und hybride Arbeitsmodelle haben es den Unternehmen erschwert oder sogar unmöglich gemacht, die Nachhaltigkeitswerte ihrer Mitarbeiter zu ermitteln. Es könnte sogar sein, dass sich die Nachhaltigkeit durch die neue Arbeitsnormalität verschlechtert hat. Es lässt sich nicht feststellen, ob das Home-Office der Mitarbeiter genauso nachhaltig ist wie die Unternehmensstandorte – oder ob sie überhaupt nachhaltig sind. Recyceln die Mitarbeiter Wasser und Abfall, optimieren sie die Energieversorgung und vermeiden sie Plastik, wie es im Büro der Fall ist? Da die Arbeit heute an mehreren Orten stattfindet, müssen Unternehmen darauf achten, dass sich ihre Büros nicht nur an einem Standort befinden. Dies könnte bedeuten, nachhaltige Praktiken wie BYOD (Bring Your Own Device) zu fördern, um den Elektroschrott zu reduzieren.

ES GIBT KEINE EINFACHEN ANTWORTEN AUF DIE FRAGE, WIE SICH DIE PRODUKTIVITÄT ODER DIE MOTIVATION EINER DEZENTRALISIERTEN BELEGSCHAFT STEUERN LÄSST.

Pravin Kulkarni, Vice President and Delivery Head – SAP Practice, Manufacturing, Financial Services, Infosys, www.infosys.com

Auch die Personalabteilung muss sich entsprechend verändern und anpassen. Nur so kann sie dabei unterstützen, dass das Unternehmen seine Nachhaltigkeitsziele erreicht. Dies könnte beispielsweise bedeuten, dass das Belohnungs- und Anerkennungssystem erweitert wird, um über die Produktivität oder die Anzahl der von einem Mitarbeiter geleisteten Stunden hinauszugehen und „weichere" Kriterien wie Ethik und Nachhaltigkeit einzubeziehen.

Empathie und Transparenz

Das zugrunde liegende Thema im Human Experience Management ist jedoch, dass in der gesamten Organisation Empathie und Transparenz aufgebaut werden. Sie tragen dazu bei, dass Mitarbeiter sich sicher fühlen und ermutigt werden, ihre Herausforderungen und Ansichten zu kommunizieren. Unternehmen hingegen sind in der Pflicht, zu zeigen, dass sie sich um ihre Mitarbeiter kümmern. Das bedeutet entsprechend geschulte Führungskräfte, die die Motivation durch Einfühlungsvermögen steigern.

Eine solche auf den Menschen fokussierte Veränderung, die von der Personalabteilung geleitet und realisiert wird, konzentriert sich nicht nur auf eine einzelne Abteilung, sondern sie kommt der gesamten Belegschaft zugute. Das Ergebnis ist ein organisatorischer Wandel, der im gesamten Unternehmen vonstattengeht.

Pravin Kulkarni

it management

AUSGABE 3-4/2023
ERSCHEINT AM
27. FEBRUAR 2023

UNSERE THEMEN

Office 4.0 (Green IT, UC, DMS, Hybrid)
Cloud Computing
Industrie 4.0 & Nachhaltigkeit

it security

AUSGABE 3-4/2023
ERSCHEINT AM
27. FEBRUAR 2023

UNSERE THEMEN

Industrial IT Security
Ransomware
Identity & Access Management

WIR WOLLEN IHR FEEDBACK

Mit Ihrer Hilfe wollen wir dieses Magazin weiter entwickeln. Was fehlt, was ist überflüssig? Schreiben sie an u.parthier@it-verlag.de

INSERENTENVERZEICHNIS

IMPRESSUM

Geschäftsführer und Herausgeber:
Ulrich Parthier (08104-6494-14)

Chefredaktion: Silvia Parthier (-26)

Redaktion: Carina Mitzschke (nur per Mail erreichbar)

Redaktionsassistenz und Sonderdrucke: Eva Neff (-15)

Autoren: Martin Andenmatten, Frank Bärmann, Waldemar Bergstreiser, Prof. Dr. René Brunner, Rob Daynes, Roland Janke, Pravin Kulkarni, Christian Malzacher, Carina Mitzschke, Angelika Mühleck, Silvia Parthier, Ulrich Parthier, Vijay Pravin, Florian Rutsch, Gernot Sagl, Christian Sohn, Daniel Szabo, Michael Veit, Suresh Vittal

Anschrift von Verlag und Redaktion:
IT Verlag für Informationstechnik GmbH
Ludwig-Ganghofer-Str. 51, D-83624 Otterfing
Tel: 08104-6494-0, Fax: 08104-6494-22
E-Mail für Leserbriefe: info@it-verlag.de
Homepage: www.it-daily.net

Alle Autoren erreichen Sie über die Redaktion.Wir reichen Ihre Anfragen gerne an die Autoren weiter.

Manuskripteinsendungen:
Für eingesandte Manuskripte wird keine Haftung übernommen. Sie müssen frei sein von Rechten Dritter. Mit der Einsendung erteilt der Verfasser die Genehmigung zum kostenlosen weiteren Abdruck in allen Publikationen des Verlages. Für die mit Namen oder Signatur des Verfassers gekennzeichneten Beiträge haftet der Verlag nicht. Die in dieser Zeitschrift veröffentlichten Beiträge sind urheberrechtlich geschützt. Übersetzung, Nachdruck, Vervielfältigung sowie Speicherung in Datenverarbeitungsanlagen nur mit schriftlicher Genehmigung des Verlages. Für Fehler im Text, in Schaltbildern, Skizzen, Listings und dergleichen, die zum Nichtfunktionieren oder eventuell zur Beschädigung von Bauelementen oder Programmteilen führen, übernimmt der Verlag keine Haftung. Sämtliche Veröffentlichungen erfolgen ohne Berücksichtigung eines eventuellen Patentschutzes. Ferner werden Warennamen ohne Gewährleistung in freier Verwendung benutzt.

Layout und Umsetzung: K.design | www.kalischdesign.de
mit Unterstützung durch www.schoengraphic.de

Illustrationen und Fotos:
Wenn nicht anders angegeben: shutterstock.com

Anzeigenpreise: Es gilt die Anzeigenpreisliste Nr. 30.
Preisliste gültig ab 1. Oktober 2022.

Mediaberatung & Content Marketing-Lösungen
it management | it security | it daily.net:
Kerstin Fraenzke, 08104-6494-19,
E-Mail: fraenzke@it-verlag.de
Karen Reetz-Resch, Home Office: 08121-9775-94,
E-Mail: reetz@it-verlag.de

Online Campaign Manager:
Roxana Grabenhofer, 08104-6494-21, grabenhofer@it-verlag.de
Marena Avila (nur per Mail erreichbar), avila@it-verlag.de

Objektleitung: Ulrich Parthier (-14), ISSN-Nummer: 0945-9650

Erscheinungsweise: 6 x pro Jahr

Verkaufspreis: Einzelheft 20 Euro
Jahresabopreis 100 Euro (Inland), 110 Euro (Ausland)
Probeabo 20 Euro für 2 Ausgaben
PDF-Abo 40 Euro für 6 Ausgaben

Bankverbindung: VRB München Land eG,
IBAN: DE90 7016 6486 0002 5237 52, BIC: GENODEF10HC
Beteiligungsverhältnisse nach § 8, Absatz 3 des Gesetzes über die Presse vom 8.10.1949: 100 % des Gesellschafterkapitals hält Ulrich Parthier, Sauerlach.

Abonnementservice: Eva Neff,
Telefon: 08104-6494 -15, E-Mail: neff@it-verlag.de
Das Abonnement ist beim Verlag mit einer dreimonatigen Kündigungsfrist zum Ende des Bezugszeitraumes kündbar. Sollte die Zeitschrift aus Gründen, die nicht vom Verlag zu vertreten sind, nicht geliefert werden können, besteht kein Anspruch auf Nachlieferung oder Erstattung vorausbezahlter Beträge.

Bedeutet digitales Wachstum auch Nachhaltigkeit?

RETHINK
THE SYSTEM

Die Klimaziele von morgen erreichen wir nicht mit den Technologien von gestern. Lassen Sie uns deshalb gemeinsam den Status-Quo überdenken. T-Systems unterstützt Sie mit Green-IT-Lösungen und grünen Cloud-Services: für digitales Wachstum im Einklang mit nachhaltigen Umweltzielen.

Jetzt mehr erfahren unter:
rethink-the-system.de

T Systems
Let's power higher performance

it security

Detect. Protect. Respond.
Januar/Februar 2023

MODERNE VPN-LÖSUNGEN

Zero Trust & SASE-Strategien

Bernd Nüßlein, NCP engineering GmbH

Cyber-Resilience
ab Seite 10

CASB, SSE, SASE
Next Generation

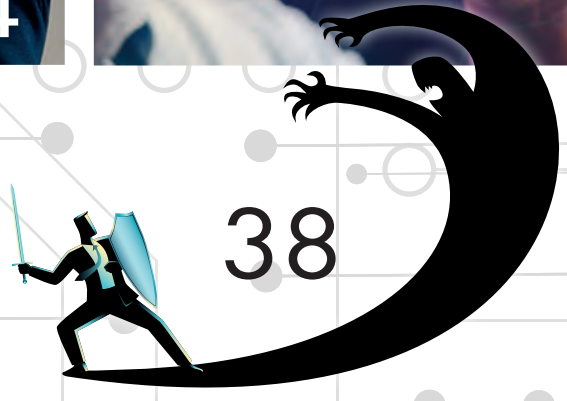
CYBER-ATTACKEN
Hilft ein Threat Navigator?

MITRE ATT&CK
Wo stehen wir heute?

Künstliche Intelligenz

Fluch oder Segen?

Inhalt



COVERSTORY

IT SECURITY

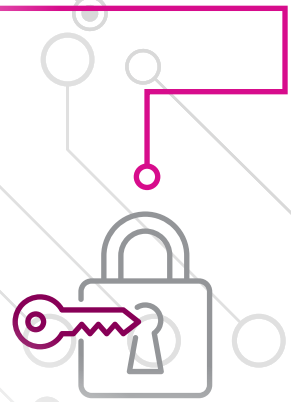
Ganzheitliche IT-Security-Konzepte im Fokus

MODERNE VPN-LÖSUNG, ZERO TRUST UND SASE-STRATEGIEN

In der IT-Sicherheit wandelt sich der Blick der Security-Verantwortlichen. Der Trend geht weg von einzelnen Tools hin zu vollumfänglichen IT-Security- & Cloud-Konzepten. Diese Entwicklung ist auch für den Nürnberger Enterprise-VPN-Anbieter NCP von großer Bedeutung. Darüber sprach Ulrich Parthier, Publisher it security mit Bernd Nüßlein, Vice President Sales & Marketing bei NCP in Nürnberg.

Ulrich Parthier: *Hallo Herr Nüßlein, kommen wir gleich zur Einstiegsfrage. Können auch Sie bei ihren Kunden einen geänderten Blickwinkel auf die IT und die IT-Sicherheitsgefahrenlage feststellen?*

Bernd Nüßlein: Hallo Herr Parthier. ja das können wir so bestätigen. Wenn es früher noch darum ging, dass man einzelne Lösungen haben musste, um von einer sicheren IT zu sprechen, sind heute eine ganze Vielzahl von Schritten nötig, um Hackern das Handwerk zu legen. Dabei ist ein ganzheitlicher Ansatz sehr wichtig, denn es nützt nichts, nur die richtigen Lösungen zu haben, sie müssen am Ende auch perfekt ineinandergreifen.



Ulrich Parthier: *In den vergangenen Jahren haben immer mehr Unternehmen ihre Anwendungen in die Cloud verschoben. Das erfordert natürlich auch einen Strategiewechsel bei den IT-Security Anbietern. Sehen Sie diese Wechsel auch bei ihren Kunden und den Toolanbietern im Allgemeinen?*

Bernd Nüßlein: Selbstverständlich gehen auch unsere Kunden und Partner diesen Weg – der eine mehr, der andere weniger schnell.

Ulrich Parthier: *Und wie lautet die NCP-eigene Antwort auf diese Frage? Welche Rolle spielt die Cloud in ihrer Lösungsstrategie?*

Bernd Nüßlein: Wir müssen darauf vorbereitet sein. Unsere Produkte müssen in die neuen Konzepte integrierbar sein. In Bezug auf die Cloud müssen wir natürlich die Trends beobachten und dort, wo es sinnvoll erscheint, neue Technologien aufgreifen.

Ulrich Parthier: *Können Sie dies etwas näher erläutern?*

Bernd Nüßlein: Das Thema „Cloud" hat in den letzten Jahren dazu beigetragen, dass IT-Security-Netzwerke immer flexibler und digitaler werden. Technologien und Standards wie SASE, Single Sign On, SD-WAN oder Zero Trust erweitern die Möglichkeiten des modernen Remote Access. Gleichzeitig steigen durch die fortschreitende Vernetzung aber auch die potenziellen Angriffsvektoren. Daher müssen Cloud-Lösungen in Unternehmen genauso lückenlos abgesichert werden wie eine On-Premises-Infrastruktur. Wir entwickeln dazu moderne VPN-Lösungen, die alle Anforderungen von Anwendern, Unternehmen und Providern gleichermaßen erfüllen und in jedes dieser Technologie-Konzepte eingebaut werden können!

Ulrich Parthier: *SD-WAN wird derzeit auch viel in Unternehmen eingeführt. Wie integriert sich ein VPN von NCP als Beispiel hier in einen software-definierten Netzwerk-Verbund?*

Bernd Nüßlein: Ein SD-WAN (Software Defined Area Network) ist im Grunde ein verzweigtes Computernetzwerk, das beispielsweise weit verteilte Standorte eines Unternehmens auf intelligente Weise miteinander verbindet. Ein solcher Zusammenschluss aus vielen Standorten und Netzwerken benötigt ein sehr hohes Sicherheitsniveau. Diese Absicherung übernehmen in einem SD-WAN die softwarebasierten IPsec-VPN-Produkte von NCP.

Der nötige Schutz gelingt durch die Kombination eines NCP Virtual Secure Enterprise VPN Servers (SES/vSES) als

Gateway und des NCP Secure Enterprise Managements (SEM) als Management-System. Hierbei liegt das Gateway in der Cloud aber nicht direkt im Internet, sondern bildet hinter der Firewall eine abgesicherte Umgebung direkt auf dem Server. Über die Management-Umgebung regeln Sie anschließend die komplette, sicherheitstechnische Administration im SD-WAN. Dies reicht von der User- und Geräte-Authentisierung, über Firewall-Konfigurationen und zentrales Update-Management bis hin zu Multifaktor-Authentifizierung oder Endpoint Policy Checks, die jeden Login-Versuch und das dazugehörige Endgerät auf seine Sicherheit hin überprüfen.

Ulrich Parthier: *Es ist sicher nicht einfach, neue Architekturkonzepte zu integrieren. Wie gelingt NCP dies beim SASE-Ansatz?*

Bernd Nüßlein: Unter SASE (Secure Access Service Edge) versteht man ein Architekturkonzept, das WAN-Services und Security-Funktionen wie Zero Trust oder VPNaaS (VPN as a Service) in einer cloudbasierten Lösung kombiniert. Die gemanagten Enterprise-Lösungen von NCP stellen dem SD-WAN den passenden IT-Security-Mitspieler an die Seite. Als 100 Prozent softwarebasiertes VPN-Produkt lässt sich unsere Lösung komplett flexibel in der Cloud betreiben und übernimmt fortan die verschlüsselte Datenübertragung zur Firmenzentrale. Jeglicher Datenverkehr wird über einen IPsec-basierten Tunnel übertragen, wodurch neben umfassender Sicherheit auch die maximale Geschwindigkeit für den Transfer sichergestellt wird.

Ulrich Parthier: *Ein großes Thema in Unternehmen ist das des Single Sign On, kurz SSO. Damit kann ein Benutzer nach einer einmaligen Authentifizierung an einem Arbeitsplatz auf alle Rechner und Dienste, für die er lokal berechtigt ist, vom selben Arbeitsplatz aus zugreifen. Welchen Part übernimmt NCP in einer SSO-/SAML-Konfiguration?*

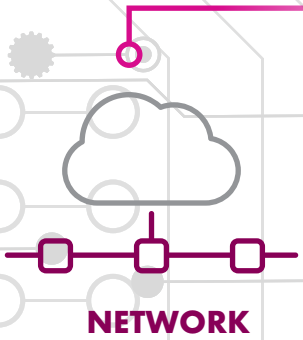
Bernd Nüßlein: Benutzerfreundlichkeit steht bei NCP seit jeher im Fokus aller Produkte. SSO haben wir seit Jahren bei unseren Lösungen im Einsatz – ist also nichts Neues.

Die Security Assertion Markup Language (SAML) ist ein offener Standard, der die Verwendung und Verifizierung von Anmeldeinformationen für mehrere Webseiten erlaubt. Mit SAML kann sich ein Nutzer mit nur einem Login-Datensatz in verschiedene webbasierte Anwendungen einwählen und die Verwaltung mehrerer Anwender entfällt. Hier nutzen wir das SSO in einem neuen Kontext und Verbinden es mit der Forderung, dass nach der Anmeldung die verschiedenen Datenströme getrennt werden können.

Das NCP-Gateway und -Management bilden hierbei gewissermaßen das Eingangstor für den Cloud-Remote-Access über SAML. Unsere Lösung übernimmt in diesem Prozess die Rolle eines Authentication Providers (AP). Wurde die Login-Anfrage des Nutzers am SSO-Portal geprüft und genehmigt, baut der NCP-Client anschließend einen VPN-Tunnel auf. Dieser Zugang gilt fortan für alle internen Dienste, während externe Cloud-Anwendungen dynamisch über Funktionen wie den NCP VPN-Bypass oder Application Based Tunneling am Tunnel vorbeigeleitet werden können. Und dank IPsec-Verschlüsselung sind alle Verbindungen zur Firmenzentrale bestens abgesichert. Dies ist ein klarer Vorteil und Security-Pluspunkt von NCP gegenüber vielen anderen Zero-Trust-Anbietern.

Ulrich Parthier: *Zero-Trust-Konzepte haben in den letzten Monaten verstärkt Einfluss auf die Planung bei IT-Security-Verantwortlichen gehalten. Wie sind sie hier aufgestellt und wie integrieren sie sich in solche Konzepte?*

Bernd Nüßlein: So ist es. Zero Trust bezeichnet einen allgemeinen IT-Sicherheitsansatz, der Nutzern nach einem



> ALS 100 PROZENT SOFTWAREBASIERTES VPN-PRODUKT LÄSST SICH UNSERE LÖSUNG KOMPLETT FLEXIBEL IN DER CLOUD BETREIBEN UND ÜBERNIMMT FORTAN DIE VERSCHLÜSSELTE DATENÜBERTRAGUNG ZUR FIRMENZENTRALE.
>
> **Bernd Nüßlein, Vice President Sales & Marketing, NCP engineering GmbH, www.ncp-e.com**

Least-Privilege-Prinzip kein blindes Vertrauen mehr ausspricht. Stattdessen erhält der Anwender nur Zugriff auf die Daten, die er für seine aktuelle Arbeit benötigt.

Die softwarebasierten Lösungen für sichere Datenkommunikation von NCP verfolgen diesen Ansatz bereits seit Jahren: Im Gegensatz zu herkömmlichen Standard-VPN-Lösungen bieten wir mehr als nur eine abgesicherte Verbindung zum Firmenserver, sondern setzen auf vollumfängliche Netzwerksicherheit.

Deshalb möchten wir uns auch von diesen Standardlösungen distanzieren und mit dem Vorurteil über VPN aufräumen. Viele ziehen den Schluss, dass VPN tot sei beziehungsweise, dass die Technologie veraltet und überholt sei. Moderne VPN-Lösungen machen eine Zero-Trust-Strategie aber besser und sicherer.

So können IT-Administratoren im NCP Secure Enterprise Management (SEM) unter anderem die Zugriffsrechte von Nutzergruppen und einzelnen Anwendern granular konfigurieren. Auf diese Weise fügt sich unsere Lösung mit ihrer zentralen Administration der Nutzerzugriffe nahtlos in den Zero-Trust-Leitgedanken ein.

Ulrich Parthier: *Nehmen wir an, Unternehmen schlagen den von Ihnen vorgezeichneten Weg zu einem ganzheitlichen IT-Security und Cloud-Ansatz ein und setzen einen Zero Trust-Ansatz um. Was bedeutet das für das IT-Sicherheitsniveau?*

SERVICE

FRAMEWORK

Bernd Nüßlein: Das Sicherheitsniveau sollte bei den richtigen Komponenten in diesen Security-Ansätzen ein weit Höheres sein, als es die sogenannten All-In-One-Anbieter propagieren. Denn kein Anbieter kann behaupten, er hätte die perfekte Zero-Trust-Lösung. Zero Trust ist ein Konzept und kein einzelnes Produkt.

Ulrich Parthier: *Zusammengefasst, niemand sucht mehr nach Einzellösungen und verteilten Features, sondern nach kompletten Lösungen. Weg vom Silogedanken hin zu 360 Grad-Lösungen. Ist das richtig so?*

Bernd Nüßlein: Exakt, dementsprechend entwickeln wir auch unsere strategische Ausrichtung weiter: Weniger Fokus auf einzelne Features, sondern lösungsorientiert. Unternehmen haben Herausforderungen/Zielsetzungen bei ihrer IT-Security – wie können wir diese individuellen Ansprüche als Gesamtlösung optimal ergänzen und verbessern?

Ulrich Parthier: *Sie haben gerade die Bereiche Sales und Marketing intern neu strukturiert. Was ist der Hintergrund und wie lauten hier ihre Ziele?*

Bernd Nüßlein: Zum einen haben die Neustrukturierung personelle Veränderungen notwendig gemacht. Zum anderen war es unserer Geschäftsleitung ein Anliegen, die Bereiche in ein und dieselben Hände zu legen und so die Ziele und Ausrichtung von Vertrieb und Marketing noch enger zusammenwachsen zu lassen. Hierbei muss es gelingen den Unternehmen, die noch auf der Suche nach den passenden Bausteinen für ihr IT-Konzept sind, die richtigen Argumente pro NCP an die Hand zu geben. Ich freue mich, dass ich dieses Vertrauen bekommen habe.

Ulrich Parthier: *Der Wechsel vom klassischen Hersteller hin zum lösungsorientierten Anbieter, wie kann der gelingen?*

Bernd Nüßlein: So viel muss sich gar nicht verändern, denn die Produkte, die wir heute haben, erfüllen schon jetzt die Kriterien für eine moderne VPN-Lösung, die Zero Trust oder SASE-Strategien verbessern. Wir müssen nur den Fokus in der öffentlichen Wahrnehmung verändern und verdeutlichen, dass wir als deutscher Hersteller von High-Level-Security ein wichtiger Baustein in diesen Konzepten sind.

Ulrich Parthier: *Welche Auswirkungen wird das auf ihre Partner und die Partnerstruktur haben?*

Bernd Nüßlein: Sowohl unsere Partner als auch Kunden können sich sicher sein, dass sie mit NCP einen verlässlichen und starken Anbieter für die Zukunft haben. Dies belegen die zahlreichen Gespräche der vergangenen Wochen und Monate. Einen deutlichen Schritt nach vorne machen wir dabei insbesondere mit unseren großen OEM-Partnern, deren Bedarf rasant nach oben geht. Gleichzeitig kommen neue Anfragen von MSSP´s (Managed Security Service Providern), die unsere ganzheitliche Enterprise- und vom BSI zugelassene VS-NfD Lösung als Service anbieten möchten. Wir werden hier, denke ich, ebenfalls noch neue Partnerschaften hinzugewinnen.

it security: *Herr Nüßlein, wir danken für das Gespräch!*

Sicherheit von A bis Z

UNTERNEHMEN BRAUCHEN STIMMIGE IT-KONZEPTE WIE SASE ODER ZERO TRUST!

Cybersicherheit war schon immer eine heikle Sache. Speziell für Unternehmen gewinnt dieses Thema jedoch zunehmend an Bedeutung. Egal, ob es um die Bestellung von Waren, die Absprache mit Lieferanten und Kunden oder die interne Datenkommunikation der Mitarbeiter geht: Ohne ein entsprechend hohes Level an IT-Security machen sich Firmen angreifbar und können nicht dauerhaft produktiv bleiben.

Wie brisant diese Thematik ist, verdeutlichen auch die Zahlen der vergangenen Jahre. So hat sich die Cyber-Bedrohungslage zuletzt so stark angespannt wie noch nie zuvor. Laut dem Bundesamt für Sicherheit in der Informationstechnik (BSI)[1] wurden allein im Jahr 2021 insgesamt 15 Millionen Meldungen zu Schadprogramm-Infektionen an deutsche Netzbetreiber übermittelt. Im gleichen Zeitraum wurden auch 20.174 Schwachstellen in Software-Produkten bekannt – ein Zuwachs von 10 Prozent gegenüber dem Vorjahr.

Entwicklungen wie diese sorgen dafür, dass sich Unternehmen ihrer eigenen „Cyber-Verwundbarkeit" immer mehr bewusstwerden. Und spätestens, wenn man selbst zum Opfer einer Cyberattacke geworden ist, stellt sich in vielen Betrieben die entscheidende Frage: Wie sichere ich meine IT-Security wirklich verlässlich ab? Oft beschäftigt man sich dann das erste Mal mit aktuellen Technologien und Standards aus dem Cybersecurity-Umfeld, die zunehmend auf dem Vormarsch sind. Dabei kristallisiert sich schnell heraus, dass man den eigenen IT-Security-Flickenteppich nicht nur mit einzelnen Features stopfen möchte, wie man es vielerorts zu Beginn der Corona-Pandemie beobachten konnte. Vielmehr suchen Unternehmen nach kompletten Security-Lösungen, die in ihrem individuellen Fall von A bis Z für Sicherheit sorgen.

Moderne Technologien für moderne Unternehmen

Zu den beliebtesten Fundamenten für eine moderne Security-Infrastruktur zählen SD-WAN und SASE. Unter einem SD-WAN (Software Defined Area Network) versteht man im Grunde ein weit verzweigtes Computernetzwerk, mittels dem zum Beispiel die Standorte eines Unternehmens miteinander verbunden werden können. Ein solcher Zusammenschluss benötigt natürlich ein sehr hohes Sicherheitsniveau, um das Netzwerk sicher vor Angreifern zu machen. Diese Absicherung können in einem SD-WAN beispielsweise softwarebasierte VPN-Lösungen übernehmen. Auf diesem Prinzip baut SASE (Secure Access Service Edge) weiter auf. Bei diesem Architekturkonzept werden WAN-Services und Security-Funktionen direkt zusammen in einer cloudbasierten Komplettlösung kombiniert, was die Einstiegshürde für interessierte Unternehmen merklich senkt.

Durch die aktuelle Bedrohungslage hat zuletzt vor allem ein IT-Security-Konzept immer weiter an Bedeutung gewonnen: Zero Trust. Hier wird die Herangehensweise, nach der Netzwerkinfrastrukturen gewöhnlich aufgebaut sind, komplett umgekehrt. Sämtliche Datenzugriffe folgen bei Zero Trust einem „Least privilege"-Prinzip. Hierbei wird Nutzern und ihren Endgeräten kein blindes Vertrauen mehr ausgesprochen, sondern nur noch Zugriff auf die Daten gewährt, die für die aktuelle Arbeit nötig sind. Um dies zu bewerkstelligen, prüft das System bei jedem Datenzugriff im Hintergrund, ob der Anwender überhaupt zum Zugriff berechtigt ist. Auf diese Weise lässt man

Cyber-Angreifern nur wenig Spielraum, da selbst ein erfolgreicher Angriff nur Zugang zu einem sehr kleinen Teil des gesamten Firmennetzwerks ermöglichen würde. Damit unbefugte Zugriffe jedoch möglichst komplett verhindert werden, muss natürlich insbesondere der Login-Aspekt einer Zero-Trust-Infrastruktur bestens abgesichert sein.

Dabei hat es oberste Priorität, dass bisherige Login-Mechanismen durch Multifaktor-Authentifizierung (MFA) abgelöst werden. Schließlich spielt MFA eine tragende Rolle im Zero-Trust-Prinzip und stellt nicht zuletzt eine der effizientesten Methoden dar, um die eigenen Zugänge effektiv vor Angreifern zu schützen. Dies ist besonders für Ansätze wie Zero Trust, bei denen sich die Anzahl der Passwörter eines Nutzers in Grenzen hält, von großem Nutzen. Gerade im Firmenkosmos erfreuen sich auch komplexere Protokolle wie SAML immer größerer Beliebtheit, mit denen die Verwendung von Anmeldeinformationen für mehrere Webseiten möglich wird. Nach dem Prinzip des Single Sign On (SSO) muss sich der User dann ebenfalls nur ein Passwort merken, mit dem er sich einmal authentifiziert und anschließend – ganz im Sinne des Zero-Trust-Gedanken – auf alle Portale und Webseiten zugreifen kann, die er für seine Arbeit benötigt.

Ein gemeinsamer Nenner

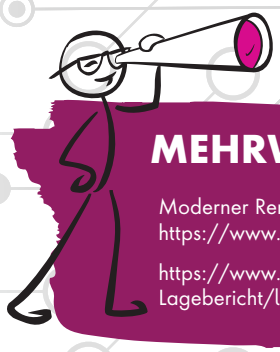
Die moderne Welt der IT-Sicherheit bietet also viele Möglichkeiten, sich vor ungebetenen Gästen zu schützen. Doch bei aller Security darf die tägliche Arbeit der Nutzer nicht durch immer neue Technologien und IT-Anwendungen eingeschränkt werden. Daher suchen Unternehmen nach IT-Security-Lösungen, die fortschrittliche Technik mit einer hohen Usability vereinen. Deshalb sollte im Zuge einer SASE-/Zero-Trust-Strategie zwingend eine moderne Lösung wie die VPN-Technologie von NCP eingesetzt werden.

Der Clou: Die zu 100 Prozent softwarebasierte NCP-Lösung kann sowohl On Premises als auch im Rechenzentrum bei Managed (Software) Service Providern zum Einsatz kommen. Diese Funktionsweise macht die NCP-Produkte von Natur aus cloudfähig, wodurch sie lückenlos in SASE-, SSE-, Zero-Trust- und SD-WAN-Konzepte integriert werden können. Den Ansatz des nutzerbasierten Datei- und Anwendungszugriffs verfolgt NCP zudem bereits seit vielen Jahren. In der Praxis funktioniert dies mithilfe granular definierter Firewall-Regeln. Der Administrator konfiguriert im NCP Secure Enterprise Management (SEM), welchen Nutzern oder Nutzergruppen welche Zugriffsrechte gewährt werden. Ergänzt wird die Lösung durch Funktionen wie Application based Tunneling oder VPN-Bypass, wodurch auch ganze Netzbereiche bei Bedarf am Tunnel vorbeigeleitet werden können. So bleibt beispielsweise eine im Firmennetz befindliche Telefonanlage weiterhin nutzbar, während diese bei einigen Zero-Trust-fähigen Produkten in der Cloud stehen müsste.

Auf diese Weise werden moderne VPN-Lösungen ein wertvoller Teil hochkomplexer Technologiekonzepte wie SASE, SSE oder Zero Trust und liefern gleichzeitig bedeutende Vorteile in Form von anwenderfreundlicher Bedienung und einfacher Administrierung. Firmen sparen sich außerdem mehrere Einzelanwendungen, indem sie eine vielseitige VPN-Lösung als Ergänzung in ihr Sicherheitskonzept einbauen, die ihre individuellen Security-Bedürfnisse erfüllt. So trägt NCP den Gedanken einer modernen, allumfassenden Netzwerksicherheit in modernen Technologien weiter, wodurch am Ende auch OEM-Partner profitieren. Nicht umsonst bezeichnet Aryaka im Zusammenhang mit ihrer SD-WAN-Lösung die VPN-Produkte von NCP als „the industry's most flexible VPN solution."

www.ncp-e.com

Quelle: 1 BSI - Die Lage der IT-Sicherheit in Deutschland 2022



MEHRWERT

Moderner Remote Access von NCP:
https://www.ncp-e.com/de/loesungen/cloud-vpn/

https://www.bsi.bund.de/DE/Service-Navi/Publikationen/Lagebericht/lagebericht_node.html

Eine Veranstaltung von itsecurity & it-daily.net
Das Online-Portal von itmanagement & itsecurity

SAVE THE DATE

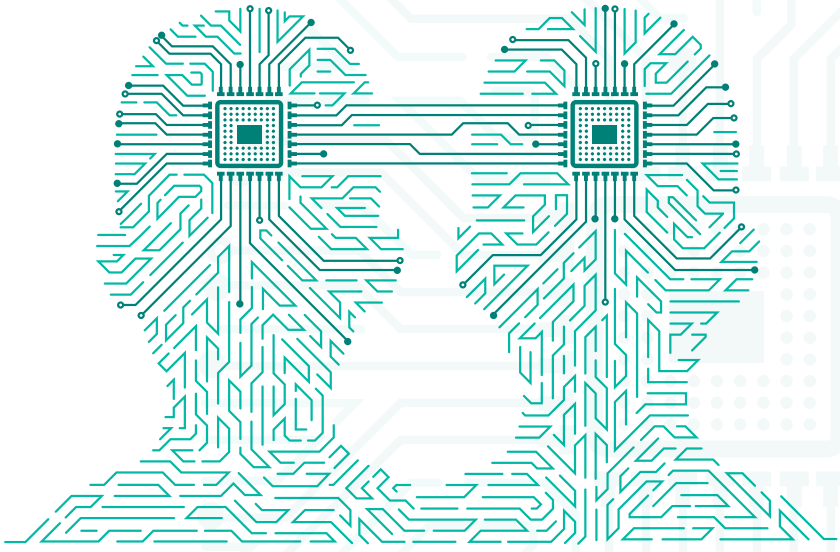
CYBERSECURITY
DIE GEFAHR AUS DEM OFF

Digitalevent
22. März 2023

#cybersec23

SCAN ME

https://www.it-daily.net/cybersecurity/



Cyber-Resilience

UNTERNEHMENSWEITE STRATEGIE ERFORDERLICH

Täglich finden Cyberangriffe statt, die Einfluss auf alle Unternehmensbereiche haben. Managementsysteme für Information Security, Business Continuity, Krisenmanagement und eine technische Absicherung der IT stellen dabei zwar starke Security-Maßnahmen dar, reichen für einen effektiven Rundumschutz jedoch nicht aus. Wie Unternehmen Cyber-Resilience erreichen können und welche besondere Rolle der Faktor Mensch dabei spielt, erläutert Florian Goldenstein, Manager IT Security Consulting & CISO, Konica Minolta Deutschland im Interview.

it security: *Herr Goldenstein, der Begriff Cyber-Resilience ist in aller Munde. Was verbirgt sich konkret dahinter?*

Florian Goldenstein: Cyber-Resilience bedeutet, dass Unternehmen auch in Krisenlagen handlungsfähig bleiben und ihr Geschäft weiterführen können. Das umfasst nicht nur einzelne, sondern sämtliche, für die Unternehmensführung relevante, Geschäftsbereiche und alle Mitarbeitenden. Denn nur, wenn alle an einem Strang ziehen, lässt sich IT-Sicherheit im Unternehmen gewährleisten. Das haben die letzten Jahre gezeigt, die von der Corona-Pandemie, der Finanzmarkt- und Energiekrise und geopolitischen Ereignissen geprägt waren. Im Zuge der Pandemie mussten im Frühjahr 2020 viele Arbeitgeber ihre Mitarbeitenden von jetzt auf gleich ins Homeoffice schicken. Das war für die IT-Abteilungen eine große Herausforderung, denn darauf war niemand vorbereitet. Bis Konzepte und Infrastrukturen an die neuen Anforderungen angepasst werden konnten ist einige Zeit vergangen. Das haben Kriminelle genutzt. Während der Fokus früher auf dem Betrieb der IT-Infrastruktur und weniger auf der Sicherheit lag, ist die Relevanz durch die bestehenden Sicherheitslücken mittlerweile deutlich gestiegen. Doch auch mit zunehmendem Fokus auf Cybersecurity, haben viele Unternehmen in diesem Punkt noch immer Nachholbedarf.

it security: *Wie können IT-Abteilungen ihre Infrastruktur zu einer nachhaltig sicheren IT-Landschaft entwickeln?*

Florian Goldenstein: Das geht nur mit effektiven Cyber-Resilience-Konzepten, die Angriffen auf die Infrastruktur trotzen und einen laufenden Betrieb auch im Angriffsfall ermöglichen. Nur so ist es möglich, Mitarbeitende und Kunden langfristig vor Datenmissbrauch, Industriespionage oder Malware zu schützen. Neben der passenden Sicherheitsstruktur und einer aktuellen Hardware spielt dabei auch der Faktor Mensch eine wichtige Rolle.

it security: *Was sind die wichtigsten Bestandteile dieser Konzepte?*

Florian Goldenstein: Cyber-Resilience ist eine Prozesskette aus fünf Phasen: „Identifizieren", „Schützen", „Detektieren", „Reagieren" und „Wiederherstellen". Im Rahmen eines Managementsystems kommt noch die „Kontinuierliche Verbesserung" hinzu. Sie rundet das Thema mit Lernprozessen ab. Diese Phasen müssen geplant und auf die Anforderungen der Informationssicherheit, die Unternehmensziele sowie die Geschäftsstrategie und das Risiko einer

PLUS

Im Whitepaper „Update für die menschliche Firewall" zeigt Konica Minolta anhand von Praxisbeispielen, wie wichtig Sensibilität für Informationssicherheit ist und wie Unternehmen mit „Security by Design" den Grundstein für eine gelungene Digitalisierung legen.

www.konicaminolta.de/sensibilisierung

außerplanmäßigen Betriebsunterbrechung ausgerichtet werden.

it security: *Wie integrieren Unternehmen solche Cyber-Resilience-Konzepte?*

Florian Goldenstein: Im Idealfall ist Cyber-Resilience ein Managementsystem, das stetig verbessert wird. Basis hierfür ist eine unternehmensweite Strategie, die durch das Risikomanagement gestützt ist und von sämtlichen Mitarbeitenden auf allen Hierarchieebenen getragen wird. Ein solches Managementsystem funktioniert aber nur dann, wenn ein organisatorischer, technischer und verhaltensorientierter Dreiklang besteht.

it security: *In den letzten Jahren waren Mitarbeitende häufig das erste Ziel einer Attacke. Welche Gründe gibt es Ihrer Meinung nach hierfür?*

Florian Goldenstein: Das liegt an zwei Faktoren: Einerseits mussten sie in vielen Unternehmen innerhalb kürzester Zeit den Umgang mit neuen Technologien, Arbeitsweisen und Prozessen lernen. Das hat einige überfordert, andere waren dadurch oftmals unachtsam. Außerdem ist vielen Mitarbeitenden nicht umfassend bewusst, dass das Thema Informationssicherheit auch sie betrifft – und zwar in vielen Situationen am Arbeitsplatz. Nicht jeder widersteht der Versuchung, einen herumliegenden USB-Stick in den Port seines Rechners zu stecken. Eine vermeintlich vom Vorgesetzten verschickte, „dringende" E-Mail wird ebenso schnell geöffnet. Man muss die alltäglichen Prozesse sehr genau überdenken, um Cyberangriffen keine Chance zu geben. Deshalb ist es so wichtig, die Menschen im Unternehmen für das Thema zu sensibilisieren und einen unachtsamen Umgang der Mitarbeitenden mit Daten zu verringern. Vor diesem Hintergrund haben Cyber-Schulungen eine elementare Bedeutung, da letztlich alle im Unternehmen die Grundlagen der Informationssicherheit kennen und täglich leben müssen.

CYBER-RESILIENCE BEDEUTET, DASS UNTERNEHMEN AUCH IN KRISENLAGEN HANDLUNGSFÄHIG BLEIBEN UND IHR GESCHÄFT WEITERFÜHREN KÖNNEN.

Florian Goldenstein, Manager IT Security Consulting & CISO, Konica Minolta Deutschland, www.konicaminolta.de

it security: *Stichwort „Social Engineering": Die Methoden der Bedrohungsakteure, um das Vertrauen von Personen zu erlangen und letztlich auszunutzen, sind hoch professionell. Wo liegen die Angriffsvektoren?*

Florian Goldenstein: Kriminelle machen sich menschliche Züge wie Hilfsbereitschaft, Angst oder Pflichtbewusstsein zunutze. Das funktioniert im Bereich Spear-Phishing sehr effektiv. Es handelt sich dabei um den gezielten Versand einer E-Mail, die zum Anklicken eines Links, zur Eingabe von Passwörtern oder dem Preisgeben von Informationen auf einer fingierten Oberfläche auffordern. Ebenfalls kommt Telefon-Spoofing häufig zum Einsatz. Dabei rufen Kriminelle Mitarbeitende an und fälschen die übermittelte Rufnummer. Der Effekt: Die angerufene Person geht davon aus, dass der Anruf aus dem eigenen Unternehmen käme und gibt im Gespräch vertrauliche Informationen preis.

Seit langem aktuell und immer wiederkehrend ist der CEO-Fraud: Hierbei werden gezielt ausführende Personen eines Unternehmens angegriffen. Kriminelle geben sich als Führungskräfte oder Management einer Firma aus. Um einen vorgeblichen Geschäftsablauf nicht zu behindern, bitten sie um Reaktion und weisen auf die Dringlichkeit hin. Das kann beispielsweise eine eilig zu tätigende Express-Überweisung sein. Deshalb ist es so wichtig, zu sensibilisieren und auf allen Ebenen zu trainieren.

it security: *Reichen Schulungen und Trainings für einen wirksamen Schutz aus?*

Florian Goldenstein: Die menschliche Firewall ist die wichtigste im Unternehmen. Hierzu bieten wir die Mitarbeiter-Sensibilisierung „as a Service" an, um auch die menschliche Firewall regelmäßig zu trainieren. Sie darf aber nicht die einzige Maßnahme zur Gefahrenabwehr darstellen. Wir unterstützen unsere Kunden daher aktiv mit Managed Services, die viele Bereiche und auch Security abdecken, beispielsweise mit Monitoring, Patch-Management oder Backups. Zudem bieten wir auch Managed Firewalls und Endpoint Protection an, denn die Sicherheit der Endgeräte – an jedem Ort – ist ein zentrales Thema. Damit legen wir den Grundstein für sichere hybride Arbeitsmodelle und eine sichere Unternehmens-IT.

it security: *Herr Goldenstein, wir danken für das Gespräch.*

THANK YOU

IT-Security-Trends

WAS 2023 WICHTIG WIRD

DURCH DIE DIGITALE TRANSFORMATION SIND DATEN HEUTE DAS WERTVOLLSTE GUT DAS UNTERNEHMEN BESITZEN, GLEICHZEITIG SIND DIE DATEN GRÖSSEREN RISIKEN AUSGESETZT ALS JEMALS ZUVOR.

Audra Simons, Senior Director of Global Products, Global Governments and Critical Infrastructure, Forcepoint, www.forcepoint.com

Die Finanzbranche rüstet sich gegen synthetischen Betrug, die aktuellen Krisen produzieren neue Insider-Risiken und Unternehmen wollen die IT-Sicherheit vereinfachen: Diese Trends werden die IT-Security im Jahr 2023 und darüber hinaus prägen.

Synthetische Identitätsdiebstähle nehmen weiter zu. Bei dieser Methode kombinieren Kriminelle gestohlene Informationen mit gefälschten persönlichen Angaben und erschaffen daraus betrügerische Identitäten, mit denen sie Konten eröffnen, Kredite beantragen und im Internet einkaufen. Um dieses Problem in den Griff zu bekommen, werden Banken, Kreditgeber und Gläubiger künftig von den Antragstellern Scans oder Fotos ihrer Pässe oder Ausweise verlangen müssen, um damit ihre Identitäten zu verifizieren. Dabei handelt es sich um Millionen von Dokumenten, die sie online entgegennehmen – und jedes dieser Dokumente ist ein potentieller Träger von Schadsoftware.

Bei der Abwehr dieser Gefahr kann ihnen die neuartige Sicherheitstechnologie Zero Trust Content Disarm and Reconstruction (CDR) helfen, die einen ganz anderen Ansatz verfolgt als herkömmliche Systeme wie Firewalls, Virenscanner oder Sandboxes. Sie durchsuchen Dokumente anhand von Signaturen nach Schadsoftware und finden deshalb nur bösartigen Programmcode den sie bereits kennen. Da Cyberkriminelle ihre Malware permanent modifizieren, sind sie immer einen Schritt voraus. Sobald eine neue Variante bekannt wir, aktualisieren IT-Sicherheitsanbieter zwar ihre Systeme, aber in diesem Zeitfenster gelingt es Angreifern immer wieder, ihre Schadsoftware an den Sicherheitssystemen vorbeizuschmuggeln.

Zero Trust CDR geht davon aus, dass grundsätzlich kein Dokument vertrauenswürdig ist und sucht deshalb erst gar nicht nach Malware. Stattdessen extrahiert sie aus den Dokumenten die Informationen, bei denen schädliche Inhalte garantiert ausgeschlossen sind und erstellt daraus in Sekundenschnelle neue, voll funktionsfähige Dateien, die vollständig frei von ausführbarem Code sind und dadurch auch keine Schadsoftware enthalten können. Zero Trust CDR alleine wird synthetischen Identitätsbe-

trug natürlich nicht gänzlich verhindern können. Aber es kann zumindest dafür sorgen, dass die zur Verifizierung von Identitäten gesammelten Dokumente sicher sind.

Politische Verhärtung erhöht Insider-Risiken

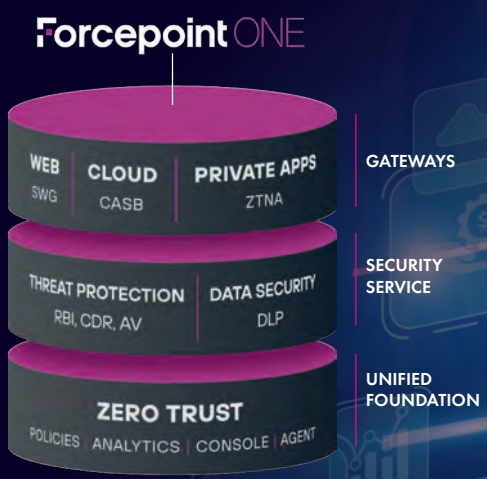
Die aktuellen Krisen führen zu einer zunehmenden Politisierung von Bürgern. Desinformationen haben dabei sogar teilweise eine regelrechte Verhärtung der Positionen und eine Radikalisierung zur Folge. Für Unternehmen entstehen daraus neue potenzielle Risiken durch Innentäter. Mitarbeiter könnten aus politischen Motiven heraus versuchen, geistiges Eigentum zu stehlen oder sensible Informationen zu exfiltrieren.

Um dieser neuen Herausforderung zu begegnen, werden Unternehmen Systeme für eine kontinuierliche Verhaltensüberwachung einführen. Der Schlüssel zum Erfolg liegt dabei in der Flexibilität der Systeme. Das Verhalten der Mitarbeiter kann sich im Lauf der Zeit ändern. Je nachdem, wie sich ihre Ansichten und Überzeugungen entwickeln, können sie nach und nach zu einem Sicherheitsrisiko werden. Die Systeme zur Überwachung von Insider-Risiken müssen flexibel genug sein, solche manchmal schleichenden Entwicklungen zu registrieren. Sie sollten es Unternehmen ermöglichen, Schwankungen in den Verhaltensmustern von Nutzern zu überwachen und mit ihrem Ausgangsverhalten zu vergleichen.

Aktuell werden solche Systeme hauptsächlich dazu verwendet, um festzustellen, ob ein Nutzer auf ungewöhnliche Weise auf Informationen zugreift. Angesichts der neuen Insider-Risiken werden Unternehmen sie künftig aber dafür einsetzen, ungewöhnliche Verhaltensmuster zu erkennen, die weit über den Zugriff auf Unternehmensdaten und -systeme hinausgehen. Mit kontinuierlicher Verhaltensüberwachung können sie beispielsweise feststellen, ob sich ein Nutzer von seinen Kollegen oder seiner Arbeit abwendet, ober ob er anfängt, ungewöhnlich große Datenmengen zu horten. Solche Erkenntnisse können Hinweise darauf liefern, dass ein User ein potenzielles Insider-Risiko darstellt. Selbstverständlich müssen solche Systeme mit den Betriebsräten abgestimmt sein. Zudem müssen sie durch eine anonymisierte Erfassung der Nutzerdaten für Datenschutzkonformität sorgen.

Unternehmen transformieren ihre IT-Sicherheit

Zur Bereitstellung von Anwendungen nutzen Unternehmen zunehmend hybride Multi-Cloud-Umgebungen, die mehrere Public Clouds, Private Clouds und On-Premises-Installationen kombinieren. Mit herkömmlichen IT-Sicherheitsarchitekturen können sie den Schutz dieser komplexen Landschaften nicht effizient managen. Diese Architekturen sind in der Regel ein Flickenteppich aus losgelösten Insellösungen, die von verschiedenen Anbietern stammen und separate Managementoberflächen mit eigener Logik haben. Die Folge ist nicht nur eine komplizierte und aufwändige Verwaltung, sondern auch Inkonsistenz. Sicherheitsteams können häufig keine identischen Sicherheitsrichtlinien einrichten und müssen sich mit Policies zufriedengegen, die lediglich ähnlich sind.



Unternehmen werden 2023 verstärkt auf integrierte All-in-One-Plattformen für IT-Sicherheit setzen. (Quelle: Forcepoint).

Unternehmen werden deshalb daran gehen, ihre IT-Sicherheit zu transformieren und auf integrierte, Cloud-basierte All-in-One-Plattformen aus der Hand eines einzigen Anbieters umsteigen. Mit solchen Komplettlösungen können sie künftig sämtliche Vorgaben mit einem einzigen Satz an Sicherheitsrichtlinien über die komplette IT-Landschaft hinweg durchsetzen und in einer einzigen Managementkonsole zentral verwalten. Dabei werden sie verstärkt auf Plattformen setzen, die einen datenzentrierten Ansatz verfolgen. Durch die digitale Transformation sind Daten heute das wertvollste Gut das Unternehmen besitzen, gleichzeitig sind die Daten durch hybride Arbeitsmodelle, mobiles Arbeiten und BYOD größeren Risiken ausgesetzt als jemals zuvor.

Diese Anforderungen machen Data Loss Prevention (DLP) zu einer Schlüsseltechnologie. DLP-Lösungen sind in der Lage, schützenswerte Informationen zu identifizieren und Aktionen mit hinterlegten Richtlinien abzugleichen. Registrieren sie Verstöße gegen die Vorgaben, machen sie die Mitarbeiter darauf aufmerksam. Moderne adaptive Systeme reagieren dabei jedes Mal mit Schutzmaßnahmen, die dem Kontext angemessen sind. So verhindern sie den ungewollten Abfluss von Daten, ohne die Produktivität der Mitarbeiter unnötig einzuschränken. Deshalb werden vor allem IT-Security-Plattformen erfolgreich sein, die Technologien Secure Web Gateway (SWG), Cloud Access Security Broker (CASB), Advanced Threat Protection (ATC) und Zero-Trust-Funktionen mit DLP integrieren. Solche Komplettlösungen ermöglichen es Unternehmen, ihre Daten über sämtliche Anwendungen und Endgeräte inklusive BYOD-Geräte hinweg zu schützen.

Audra Simons

IT-Sicherheit 2023

MASSNAHMEN GEGEN CYBERERPRESSUNG

Gute Vorbereitung ist das A und O im Kampf gegen Cyberkriminalität. Dabei stehen Unternehmen auch in diesem Jahr wieder vor einigen Herausforderungen. Denn IT-Strukturen werden in Zeiten zunehmender Digitalisierung immer vielseitiger, komplexer und damit auch anfälliger für Cyberangriffe.

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) zeigte erst kürzlich im Lagebericht zur IT-Sicherheit 2022 schwarz auf weiß: Die IT-Sicherheitslage spitzt sich zu – die Gefahr, Opfer von Cyberangriffen zu werden, war noch nie so hoch wie jetzt.

Ransomware stellt dabei die größte Bedrohung für die IT-Sicherheit deutscher Unternehmen dar. Die Trends für die IT-Sicherheit 2023 weisen deshalb gezielt auf Maßnahmen gegen Cybererpressung hin.

Hier sind die sieben wichtigsten Entwicklungen, die Unternehmen zum Thema IT Security für 2023 im Blick behalten sollten:

#1 Kritische Infrastruktur im Fokus

Ein Blick in die Medienlandschaft zeigt: Kritische Infrastrukturen sind immer häufiger das Ziel von Cyberattacken. Aktuell weist nichts darauf hin, dass beispielsweise Angriffe auf das Gesundheitswesen oder die Energieversorgung 2023 abnehmen werden. Im Gegenteil: Sie werden häufiger und gezielter.

Der Grund ist ein Trend hin zu „Cybercrime as a Service" (CaaS). Besonders „Ransomware as a Service", also Erpressersoftware, die für Attacken vermietet wird, wird immer häufiger für präzise Angriffe auf lukrative Ziele eingesetzt. Die kritische Infrastruktur ist dabei besonders anfällig und schutzbedürftig.

#2 Neue Regulierungen implementieren

In den vergangenen Jahren wurden national und international einige Gesetze und Regulierungen auf den Weg gebracht, bei denen jetzt die Umsetzungsphase beginnt. Dazu gehören zum Beispiel:

- die NIS-2-Richtlinie für EU-Mitgliedsstaaten mit strengeren Überwachungsmaßnahmen und Meldepflichten
- der Gesetzesentwurf zum European Cyber Resilience Act (CRA) für die Cybersicherheit internetfähiger Geräte und Produkte
- die EU-Verordnung zur Radio Equipment Directive (RED), die zur Cybersicherheit bei allen Wireless-Geräten (Smartphones, Tablets oder Smartwatches) verpflichtet

Dabei gilt: Selbst ist die Frau oder der Mann. Unternehmen müssen auf eigene Faust prüfen, ob sie betroffen sind. Falls

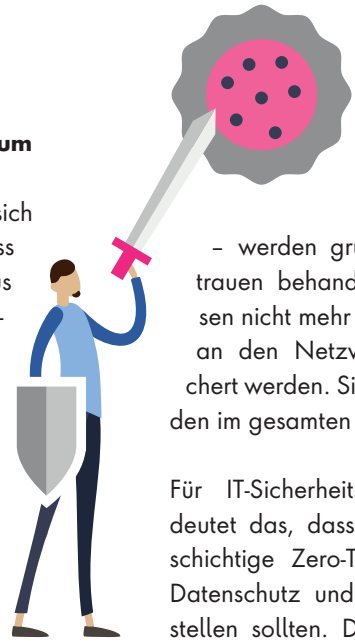
ja, müssen sie überlegen, wie sie ihre IT-Sicherheit möglichst effizient und kostengünstig anpassen können.

#3 Mehr Cyber Resilienz: Widerstandsfähigkeit stärken

Der Begriff Cyber Resilienz drückt aus, wie widerstandsfähig ein Unternehmen gegen Attacken von Cyberkriminellen ist – und ob es handlungsfähig bleibt, selbst wenn die Attacke erfolgreich ist. Es geht also um einen Notfallplan, der die sogenannte Business Continuity aufrecht und die wirtschaftlichen sowie finanziellen Verluste in Grenzen hält.

Grundlage für eine gute Cyber Resilienz ist es, dass alle im Unternehmen die Bedrohungen und eigenen Schwächen verstehen. Unternehmen können an diesem Punkt zum Beispiel mit IT-Notfallplänen und Übungsszenarien (Disaster-Recovery-Tests) effektiv vorsorgen. Reaktionen auf Angriffe sollten geplant und immer wieder geübt werden, sodass im Ernstfall alle Mitarbeiter und Mitarbeiterinnen vorbereitet sind.

#4 Zero Trust wird zum Must-have



Das Zero-Trust-Modell an sich ist nicht neu. Neu ist, dass Zero Trust durch den Fokus auf Homeoffice und Software as a Service zum neuen Standard und Must-have für Unternehmensnetzwerke wird. IT-Analysten und -Analystinnen sind sich dabei einig, dass Zero Trust künftig der einzig funktionierende Sicherheitsansatz sein wird. Unternehmen mit ausgereiftem Zero-Trust-Konzept sind deutlich besser in der Lage, Bedrohungen zu erkennen und darauf zu reagieren. Es findet also ein Paradigmenwechsel statt, der sich erheblich auf die IT-Sicherheitsarchitektur von Firmen auswirkt.

Das Zero-Trust-Modell basiert auf dem Grundsatz „never trust, always verify". Das heißt, alle Geräte, Dienste, Benutzer und Benutzerinnen – egal ob intern oder extern – werden grundsätzlich mit Misstrauen behandelt. Netzwerke müssen nicht mehr nur nach außen, also an den Netzwerkgrenzen, abgesichert werden. Sicherheitssysteme werden im gesamten Netzwerk benötigt.

Für IT-Sicherheitsverantwortliche bedeutet das, dass sie 2023 auf mehrschichtige Zero-Trust-Architekturen für Datenschutz und Cybersicherheit umstellen sollten. Dafür die technischen Weichen im Unternehmen zu stellen, kann herausfordernd und zeitintensiv sein. Eine Cloud-basierte Zero Trust Platform wie zum Beispiel von DriveLock, die mit Endpoint Security und Endpoint Protection Unternehmensdaten, Endgeräte und IT-Systeme nach modernsten Standards schützt, vereinfacht die Umstellung erheblich.

#5 Sicherheitsrisiken automatisch priorisieren

Cyber Resilienz erfordert auch eine neue Denkweise im Umgang mit Schwachstellen in der IT-Sicherheit. Es ist wichtig, dass Unternehmen im ersten Schritt alle Sicherheitslücken kennen. Um zu wissen, wo welche Gefahren lauern, sind regelmäßige Penetrationstests, laufendes Patch-Management und kontinuierliche Checks durch IT-Sicherheitsexperten und -expertinnen eher Pflicht als Kür.

Sind die Gefahren bekannt, versuchen viele Unternehmen, alle Probleme gleichzeitig zu lösen. Das ist aber nicht (mehr) zielführend. Der Trend geht stattdessen zu einem modernen Schwachstellenmanagement, das Sicherheitslücken automatisch analysiert und vor allem priorisiert. So ist der Blick immer auf die Schwachpunkte gerichtet, von denen die größte Gefahr ausgeht.

Eine solche risikobasierte Priorisierung bietet einen deutlich besseren Schutz

Foto: istockphoto/metamorworks

TOP 3-BEDROHUNGEN JE ZIELGRUPPE

Staat & Verwaltung
Ransomware
APT
Schwachstellen
Offene oder falsch konfigurierte Online-Server

Wirtschaft
Ransomware
Schwachstellen
Offene oder falsch konfigurierte Online-Server
IT-Supply-Chain

Gesellschaft
Identitätsdiebstahl
Sextortion
Fake-Shops im Internet

Quelle: bsi.bund.de

gegen Cyberkriminelle – erfordert aber auch eine grundlegend neue Vorgehensweise und die Unterstützung von erfahrenen Cybersecurity-Experten und -Expertinnen

#6 Mit smarten Tools gegen den Fachkräftemangel

Immer mehr Sicherheitsteams haben mit personellen Problemen zu kämpfen. Der IT-Fachkräftemangel wird immer sichtbarer: Eine aktuelle Bitkom-Studie zeigt, dass in Deutschland aktuell 137.000 IT-Experten und -Expertinnen fehlen. Das sind rund 10 Prozent mehr als 2019. Bei der Cybersicherheit ist die Personallücke verglichen mit 2021 sogar um fast 53 Prozent gewachsen. Das Ergebnis: überlastete und unterbesetzte IT-Sicherheitsteams, die zwangsläufig Fehler machen und weniger gut für Angriffe gerüstet sind. Vor allem kleinere und mittlere Unternehmen geraten verstärkt ins Visier von Cyberkriminellen.

In Zukunft werden Verantwortliche für die IT-Sicherheit Technologien neu bewerten und nach umfassenden Lösungen suchen müssen, mit denen sie ihre Prozesse effizienter machen können. Es braucht Tools und Plattformen, die viele Aufgaben automatisiert übernehmen und damit dünn besetzten Teams den Rücken freihalten. Der Security Service von DriveLock beispielsweise ist von Experten:Innen gemanagt, sofort einsatzbereit, ressourcenschonend, individualisierbar und maximal sicher.

#7 Anwendungsfreundliche Security in der Cloud

IT-Umgebungen werden in unserer hybriden Arbeitswelt mit verschiedensten Endgeräten, Videochats und Remote Work immer komplexer. Mehr und mehr Services wandern von On-Premises in die (Hybrid) Cloud. Viele Unternehmen werden 2023 ihre bisherige IT-Infrastruktur evaluieren und einsatzbereite Cloud-native Technologien noch mehr und vor allem strategischer einsetzen.

Mit diesem Wandel steigen auch die Anforderungen an die IT-Sicherheit. Cloud-basierte Services erfordern besondere Schutzmaßnahmen wie Confidential Computing oder hybride Firewalls. Die Kunst dabei: maximale Sicherheit für alle Geräte innerhalb eines Netzwerks zu garantieren, ohne dass die Cybersecurity-Lösungen die Nutzer:Innen im Arbeitsalltag behindern.

DriveLock hat sich Nutzerfreundlichkeit groß auf die Fahnen geschrieben und arbeitet kontinuierlich daran, die tägliche Nutzung der Lösung für Admins sowie Anwender:Innen zu vereinfachen. Zum Beispiel mit einem Self-Service-Portal, mit intelligenter Applikationskontrolle oder durch die Integration von Microsoft BitLocker Management in DriveLock.

www.drivelock.com

PLUS

IT-Sicherheit in kritischen Infrastrukturen
Lesen Sie mehr dazu in unserem Whitepaper
https://www.drivelock.com/de/lp-wp-kritis

Sicher arbeiten vom Bilderbuchstrand

SECURITY-AWARENESS-MANAGEMENT IM DIGITALEN ZEITALTER

Bei Sonnenaufgang mit nackten Füßen über lauwarmen Sand schreiten und anschließend vom klimatisierten Co-Working-Space die Kollegschaft im Online-Meeting begrüßen. Traumhaft, oder?

Im Windschatten der Pandemie locken viele Hotels mit höhenverstellbaren Tischen, Highspeed-Internet und Meerblick. Ein Paradigmenwechsel des modernen Arbeitens, „New Work". Neben Selbstverwirklichung und Potenzialentfaltung rücken auch Informationssicherheitsrisiken in den Mittelpunkt. Kritisch sind Zugriffe auf Kundschaftsdaten oder Firmennetzwerke über ungesichertes WiFi.

Schockierende 71 Prozent der befragten Führungskräfte aus der Informationssicherheit gaben in einer Forrester-Umfrage an, sie hätten nur einen geringen oder gar keinen Einblick in die Absicherung der Remote-Arbeitsplätze ihrer Angestellten.

Informationssicherheit muss Teil der Unternehmensphilosophie werden. Der erste Schritt zur Absicherung der Remote-Workforce ist eine Zero-Trust-Sicherheitsarchitektur. Dabei werden jegliche Zugriffsversuche von allen Geräten, Anwendungen, Netzwerken und Usern überwacht.

Ein weiterer Eckpfeiler ist ein kompetentes Security-Awareness-Management. Der Phishing-Attack-Simulator von Increase Your Skills beispielsweise hilft Unternehmen dabei, Angestellte gegen Social Engineering-Angriffe widerstandsfähig zu machen. Zur Auswahl stehen verschiedene, individuell erstellte Angriffsszenarien oder bereits vorhandene branchenspezifische Szenarien. Das Reporting-Modul wertet die Daten aus und gibt Aufschluss über den aktuellen Stand. Somit werden nicht nur Schwachstellen im Unternehmen analysiert, sondern langfristig auch sensible Unternehmensdaten und finanzielle Werte geschützt.

Mehr Infos und weitere Produkte für ein höheres Schutzniveau finden Sie unter:
https://increaseyourskills.com/

Praxisbuch ISO/IEC 27001
– Management der Informationssicherheit und Vorberietung auf die Zertifizierung, Michael Brenner u.a.; Carl Hanser Verlag GmbH & Co. KG; 11-2022

PRAXISBUCH ISO/IEC 27001

MANAGEMENT DER INFORMATIONSSICHERHEIT UND VORBEREITUNG AUF DIE ZERTIFIZIERUNG

Informationen zählen zum wertvollsten Kapital vieler Unternehmen. Egal ob Kunden-, Lieferanten-, Produkt-, Produktions- oder Mitarbeiterdaten – gerät davon etwas in falsche Hände, ist oft das Überleben des Unternehmens gefährdet. Wenn Sie in Ihrem Unternehmen Verantwortung für Informationssicherheits-Themen übernehmen, müssen Sie sich mit der ISO/IEC 27001 auseinandersetzen. Ein dieser Norm entsprechendes Informationssicherheits-Managementsystem ist zunehmend Voraussetzung für die Erfüllung von Kunden-Anforderungen sowie gesetzlicher und behördlicher Vorgaben, unter anderem im Rahmen des IT-Sicherheitsgesetzes.

In diesem Buch erhalten Sie die optimale Unterstützung für den Aufbau eines wirksamen Informationssicherheits-Managementsystems. Die Autoren vermitteln zunächst das notwendige Basiswissen zur ISO/IEC 27001 sowie zur übergeordneten Normenreihe ISO/IEC 27000 und erklären anschaulich die Grundlagen von Informationssicherheits-Managementsystemen.

Im Hauptteil des Buches finden Sie alle wesentlichen Teile der DIN ISO/IEC 2700:2022. Die Autoren geben Ihnen hilfreiche Erläuterungen dazu und wertvolle Praxistipps, die Ihnen bei der Umsetzung der Norm in Ihrem Unternehmen helfen.

IT-Security Herausforderungen 2023

KOMPLEXITÄT WÄCHST WEITER

IDC hat im September 2022 branchenübergreifend Security-Verantwortliche befragt, um detaillierte Einblicke in die Herausforderungen beim Aufbau und Betrieb von IT-Security-Konzepten zu erhalten. Man stellte fest, dass die Komplexität der Sicherheits-Lösungen im zweiten Jahr in Folge am häufigsten als Herausforderung genannt wurde. Deshalb ist es wichtig, bei der Auswahl von IT-Partnern auf die Kompatibilität der ausgewählten Lösungen zu achten, denn Stand-Alone-Lösungen erhöhen den Administrationsaufwand und senken die Effizienz.

Fachkräftemangel ist Engpassfaktor

Fast zwei Drittel der Befragten verzeichnen bereits einen akuten Security-Fachkräftemangel, oder erwarten diesen für das kommende Jahr. Deshalb sind Lösungen bei IT-Teams beliebt, die den Administrationsaufwand komplexer Netzwerke reduzieren. Florian Renner, Chief Information Officer, ist für alle Netzwerkthemen bei Hagleitner Hygiene International GmbH verantwortlich. Die besondere Herausforderung seiner Aufgabe liegt im ständigen Wandel und wachsender Komplexität des expandierenden Unternehmens mit den bekannten Herausforderungen an Zugangskontrolle und zeitfressender Administration des Endgeräte-Managements im Netzwerk. Renner: „Durch den Einsatz von macmon Network Access Control können wir in unserem Team zwischen 5 bis 10 Prozent Arbeitszeit einsparen. Und da der Faktor Zeit bei uns der limitierende Faktor ist, stellt das für unser Team einen signifikanten Mehrwert dar."

PLUS

Anwenderberichte aus der Praxis: **www.macmon.eu/loesungen/kunden**

Industrie erwartet Anstieg der Cyber-Angriffe

Mehr als die Hälfte der Befragten der IDC-Studie ist besorgt über die aktuelle Risikolage. 43 Prozent der Betriebe verzeichneten in den letzten 12 Monaten eine Zunahme der Cyberangriffe und für die Zukunft erwarten 51 Prozent einen weiteren Anstieg. 47 Prozent der befragten Organisationen passen wegen der geopolitischen Folgen des Ukraine-Kriegs ihre Cyberbereitschaft und -verteidigung an. Gut wer vorausschauend gehandelt hat und, wie der Schokoladenhersteller Ritter Sport, bereits sein Netzwerk absichert. Allein in der Firmenzentrale arbeiten über 1.000 Mitarbeiter, insgesamt rund 1.700 Menschen an neun Standorten, deren Endgeräte und ihre Aktivitäten im Firmennetzwerk sicher überwacht werden müssen, denn die Prozesse rund um die Produktion müssen reibungslos funktionieren. Michael Jany, Teamleitung Infrastruktur und Security: „Ziel unseres NAC-Projektes war eine komplette und sichere Überwachung und die Gewährleistung der Basissicherheit des Firmen-Netzwerkes, bei 3.400 Netzwerkknoten eine zentrale Aufgabe, um den IT-Betrieb störungsfrei zu managen.

KRITIS sollen in Zukunft besser geschützt werden

Energie, Trinkwasser, das Verkehrssystem - diese Bereiche zählen zur kritischen Infrastruktur. Die Bundesregierung hat sich zum Ziel gesetzt, diese stärker zu schützen. Zu diesem Zweck hat das Bundeskabinett im Dezember 2022 die Eckpunkte des sogenannten KRITIS-Dachgesetzes verabschiedet. Mit dem Gesetz will die Bundesregierung auf Vorfälle in den vergangenen Monaten reagieren. Außerdem sollen dadurch die Vorgaben der Richtlinie zur Resilienz kritischer Einrichtungen (CER) umgesetzt werden. Die CER-Richtlinie ist als Komplementärgesetzgebung zur ebenfalls überarbeiteten Netzwerk- und Informationssicherheits-Richtlinie (NIS2) angelegt, die Cybersicherheits-Vorgaben für kritische Infrastrukturen neu fasst und ebenfalls im kommenden Jahr in deutsches Recht umgesetzt werden soll.

Finanzwesen & Versicherungen

Banken, Kreditinstitute, Finanzdienstleister und Versicherungsunternehmen gehören zu den Institutionen mit den höchsten Anforderungen an die Informationssicherheit. Die wachsende Verwundbarkeit und Gefahr erhöht den Handlungsdruck für ein aktives IT-Sicherheitsmanagement im Finanz- und Versicherungswesen. Cyberexperten und Bankaufseher befürchten infolge des Ukraine-Krieges verstärkt Attacken

russischer Hacker auf Finanzinstitute. In gut jedem dritten Fall kämen Schadprogramme zum Einsatz, mit denen Hacker Computer und Daten verschlüsseln und Geld verlangen, um sie wieder freizugeben. Jeder zweite erpresste Finanzdienstleister hat bereits einmal Lösegeld gezahlt, zeigen Analysen des britischen IT-Anbieters Sophos. Im Durchschnitt wird ein Lösegeld von mehr als 800.000 Dollar fällig – üblicherweise zu begleichen in Bitcoins. Die meisten Banken und Finanzinstitute arbeiten heute mit hybriden Lösungen, einem Mix aus traditionellen IT-Systemen und Cloud-Applikationen. Die Kombination von NAC und Secure Defined Perimeter (SDP) bietet dafür einen optimalen Schutz, eine hohe und globale Verfügbarkeit, flexible und anpassbare Umsetzung von Compliance Vorgaben und die Erfüllung von Nachweispflichten gemäß ISO, PCI oder auch DSGVO-Vorgaben.

Öffentliche Verwaltungen im Visier von Datendieben

Behörden beherbergen eine Fülle an sensiblen Daten. Gleichzeitig müssen diese flexibel für die verschiedenen Fachverfahren nutzbar sein – auf unterschiedlichen Geräten und an multiplen Standorten. In einer Kommunalverwaltung arbeitet man mit äußerst sensiblen persönlichen Daten der Einwohner, die ein lukratives Ziel für Cyberkriminelle darstellen. Allein die Stadtverwaltung Bochum verzeichnet nach eigenen Angaben täglich 10.000 Angriffsversuche auf die Computersysteme der Verwaltung.

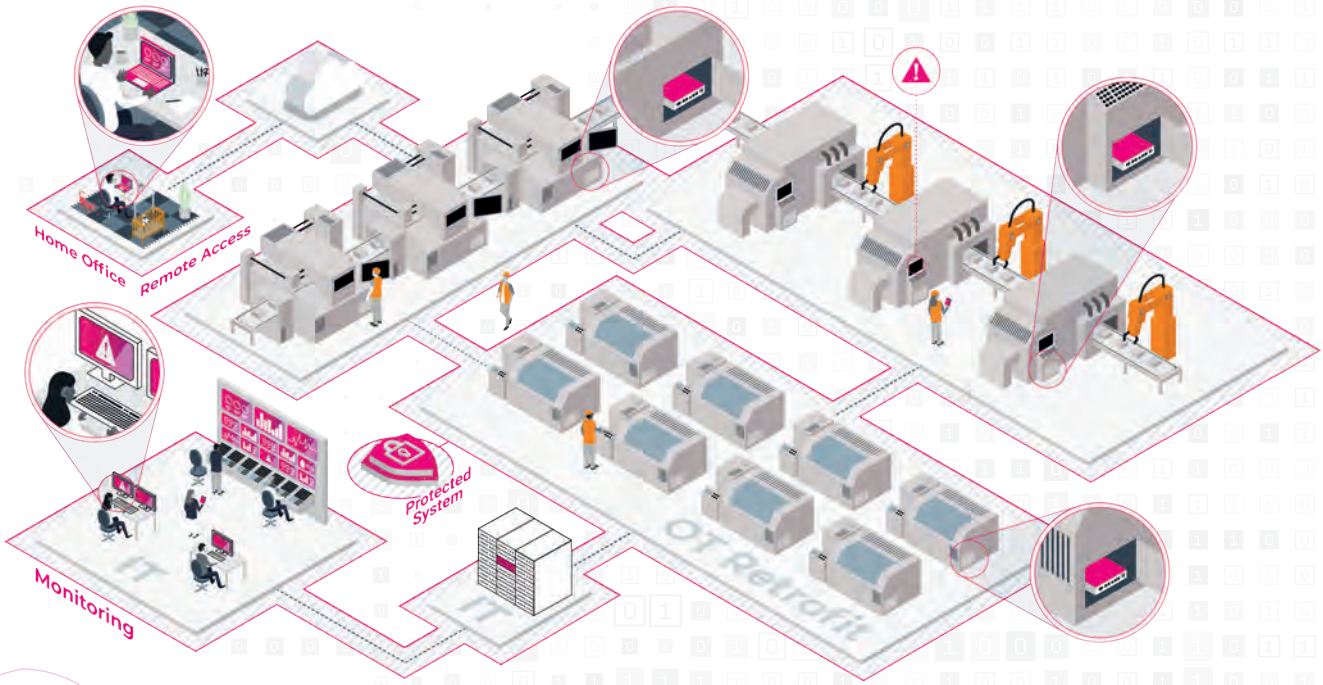
Ebenfalls finden sich in den Netzwerken der Behörden Informationen zu kritischen Infrastrukturen, wie Daten der Energieversorger oder des öffentlichen Transportwesens. Durch den Einsatz einer NAC-Lösung wissen IT-Administratoren jederzeit, welche Geräte sich im Netzwerk befinden, können sie effizient und komfortabel überwachen und kontrollieren.

Bei der Auswahl einer NAC-Lösung bietet sich eine herstellerunabhängige Sicherheitslösung an, die eine zuverlässige Überwachung auch von Netzen mit unterschiedlichsten Netzwerkkomponenten bietet.

ZTNA - Vertraue niemandem, verifiziere jeden

Die ZTNA-Philosophie bietet den Rahmen für einen intelligenten und einfachen Schutz für Netzwerke und Cloud. techconsult veröffentlichte im Juli 2022 eine mit macmon secure erstellte Studie über Cyber-Security in deutschen Unternehmen: So geben 46 Prozent der Unternehmen an, in den nächsten zwei Jahren Zero Trust einzuführen. Durch Diebstahl, Spionage und Sabotage entsteht der deutschen Wirtschaft jährlich ein Gesamtschaden von 223 Milliarden Euro, die Dunkelziffer ist hoch. Homeoffice und Digitalisierung bieten neue Angriffsmöglichkeiten, ganzheitliche Sicherheitskonzepte mit NAC und SDP sind deshalb notwendig. Das Konzept basiert auf Restriktion und Monitoring. Zusätzlich zur Sicherung lokaler Netzwerke wird der Schutz auf sämtliche Cloud-Dienste ausgeweitet. Im Unterschied zu klassischen VPNs authentifizieren sich bei Secure Defined Parameter (SDP) sowohl der Benutzer als auch der Agent am Controller. Ist die Authentifizierung erfolgreich, teilt er dem Agenten mit, ob der jeweilige Nutzer Zugriffsrechte auf die Unternehmensressourcen hat und welche das sind. Jeder einzelne Zugriff – egal ob im Firmennetzwerk oder in der Cloud – wird geprüft. Es gibt keinen Vertrauensvorschuss.

Christian Bücker | www.macmon.eu



IT-Sicherheitsgesetz

WIE DER INDUSTRIELLE MITTELSTAND PROFITIEREN KANN

Unternehmensprozesse werden nicht nur komplexer, sie werden auch digitaler. So ist die Kommunikation zwischen Maschinen inzwischen eher die Regel als die Ausnahme. Das Problem: Wachsende Ansprüche an die Cybersicherheit überfordern viele Unternehmen. Laut der Studie „Cybersecurity in Deutschland 2022", die das Research- und Beratungshaus International Data Corporation (IDC) in Zusammenarbeit mit secunet umgesetzt hat, sehen Firmen in Deutschland die Sicherheitskomplexität (27 %), Datenschutz/Privacy (21 %), Cybersecurity-Personal-/Fachkräftemangel (19 %) und die Sicherheit von vernetzten Umgebungen (18 %) als die größten Herausforderungen bei ihrer IT-Sicherheit. Fast zwei Drittel (61 %) gaben außerdem an, bereits einen akuten Fachkräftemangel zu haben oder erwarten ihn für 2023.

Das führt dazu, dass an vielen Stellen nicht genügend in die Cybersicherheit investiert wird. Die Bundesregierung hat das mittlerweile erkannt und mit dem IT-Sicherheitsgesetz 2.0 moderne Leitlinien für die IT-Sicherheit geschaffen. Es bietet Unternehmen Orientierungshilfe – egal, ob sie rechtlich davon betroffen sind oder nicht.

Das IT-Sicherheitsgesetz: Keine Pflicht, aber Vorbild für die Industrie

Das IT-Sicherheitsgesetz (IT-SiG) ist seit 2015 eines der entscheidenden Gesetze, mit denen die Bundesregierung Behörden und die Bevölkerung vor Cyberangriffen und ihren Folgen schützen will. Betroffen sind vor allem Betreiber Kritischer Infrastrukturen (KRITIS) in den Bereichen Energie, Wasser, Ernährung, Informationstechnik und Telekommunikation, Transport und Verkehr sowie Gesundheit. Mit Inkrafttreten des IT-SiG 2.0 im Jahr 2021 sind der Sektor Siedlungsabfälle und alle so genannten „Unternehmen im besonderen öffentlichen Interesse" (UBI) hinzugekommen. Diese Unternehmen werden zur strukturellen Modernisierung ihrer Cybersicherheitskonzepte verpflichtet. Angefangen bei durchdachten Netzwerkstrukturen, die Risiken bereits von vornherein berücksichtigen, umfasst dies auch eine systematische Ordnung der

Netzwerkzugänge und geeignete Mittel zur frühzeitigen Angriffserkennung.

Alles Themen und Herausforderungen, die auch in der Industrie bekannt sind. Denn die fortschreitende Automatisierung und maschinelle Kommunikation im Industriellen Internet der Dinge (IIoT) stellen auch hier hohe Ansprüche an die Cybersicherheit. Doch fehlen gerade mittelständischen Unternehmen oftmals das Know-how und das Fachpersonal, um im Schadensfall vorbereitet zu sein und schnell reagieren zu können. Deshalb empfiehlt es sich auch für sie, sich an den Standards des IT-SiG zu orientieren. Dies bietet gleich mehrere Vorteile:

1. **Effektivität:** Die umgesetzten Maßnahmen sind transparent, messbar und alltagserprobt.

2. **Planbarkeit:** Die Maßnahmen werden für mehrere Jahre und aufeinander aufbauend strukturiert, sodass Unternehmen Budgets frühzeitig definieren und verbindlich planen können. So werden Cybersicherheitsprojekte nicht zum „Fass ohne Boden".

3. **Versicherbarkeit:** Cybersicherheitsmaßnahmen dienen der Risikominimierung, können jedoch keinen einhundertprozentigen Schutz bieten. Für den Schadensfall lohnt sich deshalb eine Cyber-Versicherung. Diese greift aber nur, wenn gewisse Mindeststandards eingehalten werden.

Wie sichere ich meine Produktionsumgebung ab?

Die Basis für Cybersicherheit bildet eine Ist-Analyse. Anhand dieser lassen sich sinnvolle Maßnahmenpläne ableiten. secunet, IT-Sicherheitspartner der Bundesrepublik Deutschland, berät Unternehmen über alle Aspekte der Cybersicherheit hinweg und unterstützt diese bei der Implementierung einer professionellen und individuellen Sicherheitsinfrastruktur. In drei Schritten werden dabei zunächst bestehende Systeme, darunter auch veraltete Legacy-Geräte, vollständig erfasst. Auf Basis dessen werden Risiken bestimmt, bewertet und Anforderungen festgestellt. Im zweiten Schritt werden die passenden Maßnahmen definiert, die zur notwendigen Sicherheit der vernetzten Systeme führen. Dabei spielt auch das sogenannte Retrofitting eine Rolle, das Vernetzen bestehender und teilweise veralteter Maschinen und Anlagen. Abschließend werden die Übertragungswege zwischen Maschine und Verarbeitungsort abgesichert. Dabei handelt es sich oftmals um hybride Infrastrukturen, beispielsweise der eigenen Infrastruktur oder der Cloud. Auch kann der Einsatz einer vertrauenswürdigen „Private Cloud" sinnvoll sein, um die Vorteile der zuvor genannten Betriebsarten zu kombinieren und zudem die Datenhoheit zu behalten.

Ganzheitliche IT-Sicherheit

Neben den Maßnahmen zur Absicherung der Produktions- und Prozessumgebung braucht es ein ganzheitliches Cybersicherheitskonzept, welches das Gesamtunternehmen betrachtet. Die häufigsten Risiken, insbesondere für produzierende Unternehmen, kommen dabei aus den Bereichen, die mit dem Internet kommunizieren, also von außen erreichbar sind. Dazu zählen unter anderem der Office-Bereich oder externe Zugänge wie beispielsweise Fernwartungszugänge verschiedener Maschinen- und Anlagenhersteller.

Durch sogenannte Penetrationstests können einzelne Systeme oder Infrastrukturen auf Sicherheitslücken untersucht werden. Anhand der Ergebnisse werden im Anschluss daran effektive Maßnahmen für einen wirksamen Schutz abgeleitet. Diese beginnen bei präventiver „Basis-Security" wie Optimierungen der Firewalleinstellungen, Netzwerksegmentierungen oder Zugriffsberechtigungen. Auch Awareness-Schulungen gehören dazu, die Mitarbeiter und Führungskräfte für das Thema Cybersecurity sensibilisieren. Nicht zu vernachlässigen ist das Thema „Disaster Recovery", also das Wiederherstellen des Geschäftsbetriebs nach einem Sicherheitsvorfall. Hier sind automatisierte und funktionierende Backup-Systeme essentiell.

Eine weitergehende Maßnahme ist das sicherheitstechnische Abkoppeln veralteter Maschinen von der vernetzten Infrastruktur durch die Nutzung von gehärteten Industrial PCs („Secure Edge"). Die Maschine ist so nur noch indirekt angebunden und kann von außen nicht erkannt und kompromittiert werden. Dies trägt dazu bei, Angriffe zu erschweren und Risiken zu reduzieren. Angriffserkennungssysteme ermöglichen das frühzeitige Erkennen eines Vorfalls. Je kürzer die Erkennungszeit, desto effektiver können Schäden eingedämmt werden. Dies setzt voraus, dass das System genutzt werden kann und Reaktionsmaßnahmen und Verantwortlichkeiten vorab definiert sind. Auch hierbei bietet das IT-SiG 2.0 eine Orientierungshilfe für den effektiven Aufbau und Einsatz solcher Systeme.

Cybersecurity als Erfolgsfaktor

Langfristig können nur jene Unternehmen wettbewerbsfähig bleiben, denen es gelingt, zusätzliche Mehrwerte der Digitalisierung zu schaffen und gleichzeitig einen wirksamen Schutz vor Cyberattacken sicherzustellen. Dies trägt zudem dazu bei, die Laufzeit der Investitionsgüter zu verlängern und zum Beispiel alte Maschinen länger in Betrieb zu halten. Gerade dann entpuppt sich eine sichere und zuverlässige IT-Infrastruktur als Investition in die Zukunft.

Udo H. Kalinna | www.secunet.com

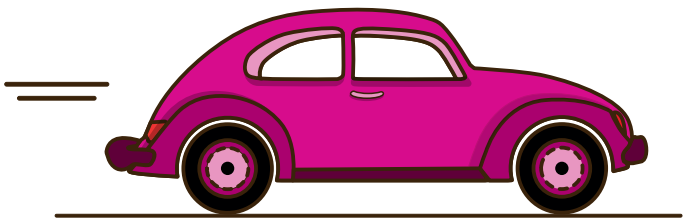
Ethisches Hacking

DER NÄCHSTE SCHRITT IHRER SICHERHEITSREISE?

1983 rief das Technologieunternehmen Hunter & Ready die erste als Bug Bounty verstehbare Initiative ins Leben. In einer cleveren Marketingkampagne mit Wortspiel wurde jeder Person, die einen Bug im hauseigenen Betriebssystem VRTX (Versatile Real-Time Executive) findet, ein Volkswagen Käfer versprochen. Wer einen Software-Bug fand, konnte also seinen eigenen Käfer (Bug) erhalten.

Die Anzeige lautete: „Es gibt jedoch einen Haken. Da VRTX das einzige Mikroprozessor-Betriebssystem ist, das vollständig mit Silikon versiegelt ist, wird es nicht einfach sein, einen Bug zu finden."

Hunter & Ready erhielten an diesem Tag ihre erste Lektion in Sachen Crowdsourced Security: Unterschätze niemals die Power der Gemeinschaft! Insgesamt wurden sieben Bugs in dem System gefunden. Die Hacker entschieden sich jedoch für die Geldprämie, nicht für das Auto.



Crowdsourced Security

Damit war der Startschuss für einen neuen Ansatz bei Sicherheitstests gefallen. Heute verdienen ethische Hacker und Hackerinnen auf der ganzen Welt durch Bug Bountys genug Geld, um davon leben zu können. Laut Intigritis Ethical Hacker Insights Report 2022 erwägen 66 Prozent der Befragten, sich in Vollzeit dem ethischen Hacking zu widmen.

Crowdsourced Security hat sich seit den Tagen interner Bug Bountys rasant weiterentwickelt. Die „Power der Gemeinschaft" lässt sich heute auf verschiedene Weise nutzen. Es gibt zahlreiche Lösungen, die den unterschiedlichen Anforderungen gerecht werden.

Dabei gelten drei Schlüsselfaktoren, die hilfreich sind, um sich für die geeignete Crowdsourcing-Lösung zu entscheiden: Zeit, Budget und der Zugang zur Community.

Jede Lösung bietet Vorteile bei mindestens zwei der Schlüsselfaktoren. Werfen wir einen genaueren Blick auf die vorhandenen Möglichkeiten.

Private und öffentliche Bug-Bounty-Programme

Während öffentliche Bug Bountys möglicherweise die bekannteste Lösung in Sachen Crowdsourced Security darstellen, sind sie nicht für alle Unternehmen gleich gut geeignet. Für Start-ups, die noch am Beginn ihrer Sicherheitsreise stehen, könnte ein öffentliches Bounty-Programm zum Beispiel zu viel Aufmerksamkeit erregen.

Hier kommen private Bug-Bounty-Programme zum Zuge. Die gezielte Auswahl bestimmter Sicherheitsexperten und -expertinnen bietet mehr Kontrolle. Private Programme eignen sich hervorragend, um mit ethischem Hacking zu starten oder neuere Assets zu testen.

Egal, ob man sich für eine öffentliche oder private Lösung entscheidet, Bug-Bounty-Programme sind individuell anpassbar. Der Umfang, das Budget und die Sichtbarkeit lassen sich auf die jeweiligen Bedürfnisse abstimmen.

Zudem sind Bug Bountys sehr kosteneffizient und daher auch für kleinere Budgets eine geeignete Lösung. Während sie zwar länger als Penetrationstests brauchen, um Ergebnisse zu liefern, profitieren die Assets von der Überprüfung durch eine Vielzahl an HackerInnen innerhalb der Gemeinschaft.

Penetrationstests als Service

Generell haben sich Penetrationstests gewissermaßen als separate Lösung zu Bug Bountys etabliert. Ein Pentest ist eine zeitlich begrenzte, simulierte Attacke auf ein Asset, bei dem häufig eine bestimmte Methode verwendet wird.

Beim Bug-Bounty-Programm handelt es sich hingegen um einen kontinuierlichen Prozess, bei dem Schwachstellen über einen längeren Zeitraum hinweg gemeldet werden. Ein Pentest wird zwar schneller durchgeführt, bietet jedoch nur eine Momentaufnahme eines bestimmten Assets zu einer bestimmten Zeit.

CROWDSOURCED SECURITY HAT SICH IMMENS WEITERENTWICKELT UND BIETET MITTLERWEILE PASSENDE LÖSUNGEN FÜR JEDEN ANSPRUCH.

Stijn Jans, CEO, Intigriti, www.intigriti.com

Angelehnt an das allgegenwärtige „Software as a Service"-Modell (SaaS), liefert Pentesting as a Service (PTaaS) skalierbare und kosteneffiziente Pentests, die den administrativen Aufwand reduzieren und Schwachstellenmeldungen in einem zentralisierten Portal anbieten.

Einige Bug-Bounty-Plattformen bieten mittlerweile erweiterte PTaaS-Services an, die auf den Fähigkeiten der Experten und Expertinnen innerhalb ihrer Gemeinschaft basieren – so auch Intigritis hybrides Pentesting.

Um auf die drei Schlüsselfaktoren zurückzukommen: PTaaS ist dann besonders sinnvoll, wenn man schnelle Resultate braucht, aber nur ein begrenztes Budget hat. Im Gegensatz zu öffentlichen Bug-Bounty-Programmen wird nicht auf die gesamte Gemeinschaft zurückgegriffen. Da der Umfang meist geringer ist und sehr spezifische Methoden notwendig sind, bietet eine große Gemeinschaft den geeigneten Pool, um spezialisierte Hacker oder Hackerinnen zu finden, die die gewünschten Fähigkeiten mitbringen.

Live-Hacking-Events

Eine weitere Lösung sind Live-Hacking-Events. Sie eignen sich besonders für alle, die eine tiefgehende Sicherheitsüberprüfung benötigen, die schnell Ergebnisse liefern muss.

In diesem Fall treffen sich ausgewählte HackerInnen zu dem Event und arbeiten gemeinsam an Angriffsstrategien. Innerhalb dieser intensiven Testperiode können zahlreiche Schwachstellenmeldungen generiert werden. Außerdem demonstrieren Unternehmen damit, dass sie eine progressive Haltung gegenüber ihrer Sicherheit einnehmen. Da der Schwerpunkt auf der Schnelligkeit liegt und die besten HackerInnen zum Einsatz kommen, sind diese Events jedoch meist kostspieliger als die anderen Lösungen.

Crowdsourced Security hat sich immens weiterentwickelt und bietet mittlerweile passende Lösungen für jeden Anspruch. Cyberkriminelle greifen auf alle möglichen Strategien zurück, was zu stetig steigenden Bedrohungen führt.

Der Einsatz ethischer HackerInnen bietet dank zahlreicher verfügbarer Lösungen eine hervorragende Möglichkeit, diesen Bedrohungen einen Schritt voraus zu sein. Unternehmen, die gerade ihr Sicherheitsbudget für das nächste Jahr planen, seien die Worte von Espen Johansen, Security Director der Softwarefirma Visma, ans Herz gelegt: 1 Dollar Investition in ein Bug-Bounty-Programm bedeutet 10–100 Dollar Ersparnis zu einem späteren Zeitpunkt.

Stijn Jans

Wie sicher ist https?

INNOVATIONEN SIND EN VOGUE, AUCH BEI HACKERN

Die Threat Labs von WatchGuard Technologies haben ihren neuen Internet Security Report (ISR) veröffentlicht. In diesem werden in gewohnter Weise die wichtigsten Malware-Trends sowie aktuell relevante Angriffsmethoden auf Netzwerke und Endpunkte ausführlich beschrieben.

Die Erkenntnisse der Forscher des WatchGuard Threat Labs zeigen, dass die größte Malware-Bedrohung für das dritte Quartal 2022 ausschließlich über verschlüsselte Verbindungen verschickt wurde. Ebenso konnten vermehrt Angriffe auf ICS- und SCADA-Systeme verzeichnet werden. Auch Computerspieler sind gefährdet, denn bei einer Minecraft-Cheat-Engine wurde eine bösartige Nutzlast entdeckt. Der ISR enthält darüber hinaus eine Vielzahl weiterer Informationen und Beispiele zur gegenwärtigen Bedrohungslage.

Fazit der Forscher: Man kann gar nicht oft genug betonen, wie wichtig die Inspektion von HTTPS-Verbindungen ist. Unternehmen sollten die entsprechende Sicherheitsfunktion unbedingt aktivieren – selbst wenn es einige Anpassungen und Ausnahmeregeln erfordert. Denn der Großteil der Malware kommt über verschlüsseltes HTTPS. Wird dieser Angriffsvektor nicht überprüft, steht Bedrohungen jeglicher Art Tür und Tor offen. Auch sollte sich das Augenmerk verstärkt auf Exchange-Server und SCADA-Managementsysteme richten. Sobald für diese ein Patch zur Verfügung steht, ist es wichtig, dieses Update sofort einzuspielen und die Anwendung zu aktualisieren. Angreifer profitieren von jedem Unternehmen, das Schwachstellen noch nicht gefixt hat.

Die überwiegende Mehrheit der Malware kommt über verschlüsselte Verbindungen

Obwohl die Malware „Agent.IIQ" in der Zeit von Juli bis September 2022 den dritten Platz in der regulären Top-10-Malware-Liste belegte, landete sie auf Platz 1 der Aufstellung für verschlüsselte Schadsoftware. Denn alle Agent.IIQ-Erkennungen wurden in HTTPS-Verbindungen gefunden. Wie die Analysen zeigen, kamen 82 Prozent der gesamten Malware über gesicherte Verbindungen, aber nur 18 Prozent unverschlüsselt. Wird der HTTPS-Datenverkehr auf der Firebox nicht überprüft, ist es sehr wahrscheinlich, dass ein großer Teil der Malware unentdeckt bleibt. In diesem Fall können Unternehmen nur darauf hoffen, dass ein wirksamer Endpunktschutz implementiert ist, um wenigstens die Chance zu haben, die Malware an einer anderen Stelle der sogenannten Cyber Kill Chain abzufangen.

ICS- und SCADA-Systeme sind weiterhin beliebte Angriffsziele

Neu in der Liste der zehn häufigsten Netzwerkangriffe im dritten Quartal 2022 ist eine Attacke vom Typ SQL-Injection, die gleich mehrere Anbieter traf. Eines dieser Unternehmen ist Advantech, dessen WebAccess-Portal den Zugriff auf SCADA-Systeme einer Vielzahl von kritischen Infrastrukturen ermöglicht. Ein weiterer schwerwiegender Angriff im dritten Quartal, der ebenfalls zu den Top 5 der einschlägigen Netzwerkbedrohungen gehörte, betraf die U.motion Builder-Software von Schneider Electric, Version 1.2.1 und früher. Dies ist ein deutlicher Hinweis darauf, dass Angreifer weiterhin aktiv versuchen, Systeme zu kompromittieren, wo immer dies möglich ist.

Schwachstellen in Exchange-Servern stellen weiterhin ein Risiko dar

Die jüngste CVE-Schwachstelle (CVE-2021-26855), die das Threat Lab entdeckte, betrifft die Remote-Code-Ausführung (RCE) von Microsoft Exchange Server bei On-Premise-Servern. Diese RCE-Schwachstelle, die eine CVE-Bewertung von 9,8 erhielt, wurde bekanntermaßen bereits ausgenutzt. Das Datum und der Schweregrad dieser Sicherheitslücke lassen ebenfalls aufhorchen, da es sich um eine von der Gruppe HAFNIUM ausgenutzte Schwachstelle handelt. Auch wenn die meisten der betroffenen Exchange-Server inzwischen gepatcht worden sein dürften, sind manche noch gefährdet und das Risiko besteht weiter.

Bedrohungsakteure, die es auf Nutzer kostenloser Software abgesehen haben

Der Trojaner Fugrafa lädt Malware herunter, die bösartigen Code einschleust. Die WatchGuard-Analysten untersuchten eine Variante, die in einer Cheat-Engine für das beliebte Spiel Minecraft gefunden wurde. Die Datei, die hauptsächlich auf Discord geteilt wurde, gibt vor, die Minecraft Cheat Engine Vape V4 Beta zu sein – aber das ist nicht al-

les, was sie enthält. Agent.FZUW weist einige Ähnlichkeiten mit Variant.Fugrafa auf, doch anstatt sich über eine Cheat-Engine zu installieren, scheint die Datei selbst geknackte Software zu enthalten. Im konkreten Fall zeigten sich zudem Verbindungen zu Racoon Stealer: Dabei handelt es sich um eine Kryptowährungs-Hacking-Kampagne, mit der Kontoinformationen von Kryptowährungsdiensten entwendet werden.

LemonDuck-Malware ist jetzt mehr als ein Cryptominer

Auch wenn die Zahl der blockierten oder verfolgten Malware-Domänen im dritten Quartal 2022 zurückgegangen ist, lässt sich unschwer erkennen, dass die Zahl der Angriffe auf ahnungslose Nutzer weiterhin hoch ist. Mit drei Neuzugängen in der Liste der Top-Malware-Domains – zwei gehörten zu ehemaligen LemonDuck-Malware-Domains und der dritte war Teil einer Emotet-klassifizierten Domain – gab es mehr neue Malware-Sites als üblich. Dieser Trend wird sich im Hinblick auf die Kryptowährungslandschaft voraussichtlich weiter verstärken, da Angreifer nach neuen Möglichkeiten suchen, um Nutzer zu täuschen. Ein wirksames Mittel dagegen ist ein aktiver Schutz auf DNS-Ebene. Damit können die Systeme der Benutzer überwacht und Hacker daran gehindert werden, Malware oder andere ernsthafte Probleme in das Unternehmen einzuschleusen.

JavaScript-Verschleierung in Exploit-Kits

Die Signatur 1132518 – als Indikator für JavaScript-Verschleierungsangriffe auf Browser – war der einzige Neuzugang in der Liste der am weitesten verbreiteten Signaturen für Netzwerkangriffe. JavaScript ist seit längerem ein gängiger Angriffsvektor und Cyberkriminelle verwenden immer wieder JavaScript-basierte Exploit-Kits, unter anderem für Malvertising und Phishing-Angriffe. Im Zuge verbesserter Verteidigungsmechanismen der Browser intensivieren auch Angreifer ihre Bemühungen, bösartigen JavaScript-Code zu verschleiern.

Anatomie der standardisierten Adversary-in-the-Middle-Angriffe

Die Multifaktor-Authentifizierung (MFA) ist zwar unbestreitbar eine immens wichtige Maßnahme im Zuge von IT-Sicherheit, aber auch kein Allheilmittel. Bestes Beispiel dafür sind der rasche Anstieg und die Kommerzialisierung von Adversary-in-the-Middle (AitM)-Angriffen. Die Untersuchung des Threat Labs zeigt, wie böswillige Akteure sich auf immer ausgefeiltere AitM-Techniken umstellen. Ähnlich wie beim zunehmend frequentierten Ransomware-as-a-Service-Angebot hat auch die Veröffentlichung des AitM-Toolkits namens EvilProxy im September 2022 die Einstiegshürde für entsprechend ausgeklügelte Angriffe erheblich gesenkt. Deren Abwehr kann nur durch die Kombination aus technischen Tools und einer Sensibilisierung der Benutzer erfolgreich aufgegleist werden.

Malware-Familie mit Verbindungen zu Gothic Panda

Bereits im Bericht des Threat Labs für das zweite Quartal 2022 fiel die Sprache auf Gothic Panda – eine Cyberspionage-Gruppe mit enger Verbindung zum chinesischen Ministerium für Staats-

GERÄTE MIT APT BLOCKIERER

50,3 %
der Malware war **Zero Day** Malware

49,7 %
der Malware war bekannte Malware

Quelle: watchguard.com/security-report

sicherheit. Interessanterweise enthält die Top-Liste der verschlüsselten Malware für das dritte Quartal eine Malware-Familie namens Taidoor, die nicht nur von Gothic Panda entwickelt wurde, sondern auch nur von Angreifern einschlägig chinesischer Herkunft eingesetzt wurde. Während sich die entsprechende Malware bisher in der Regel auf Ziele in Japan und Taiwan konzentrierte, wurde das analysierte Generic.Taidoor-Beispiel vor allem bei Organisationen in Frankreich gefunden – möglicherweise ein klarer Hinweis auf einen spezifischen, staatlich gesponserten Cyberangriff.

Neue Ransomware- und Erpressergruppen in freier Wildbahn

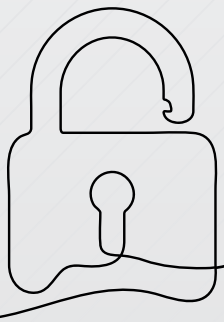
Ab sofort widmet sich das WatchGuard Threat Lab noch stärker dem Aufspüren von Ransomware-Initiativen. Dafür wurden die zugrundeliegenden Threat-Intelligence-Möglichkeiten gezielt erweitert. Im dritten Quartal 2022 führt LockBit die Liste mit über 200 einschlägigen Vorfällen an – fast viermal mehr als die Ransomware-Gruppe Basta, die von Juli bis September 2022 am zweithäufigsten von sich reden machte.

Die vierteljährlichen Forschungsberichte von WatchGuard basieren auf anonymisierten Firebox-Feed-Daten von aktiven WatchGuard-Fireboxen, deren Besitzer sich für die Weitergabe von Daten zur direkten Unterstützung der Forschungsarbeit des Threat Labs entschieden haben. Im dritten Quartal blockierte WatchGuard insgesamt mehr als 17,3 Millionen Malware-Varianten (211 pro Gerät) und mehr als 2,3 Millionen Netzwerkbedrohungen (28 pro Gerät). Der vollständige Bericht enthält Details zu weiteren Malware- und Netzwerktrends aus dem 3. Quartal 2022, empfohlene Sicherheitsstrategien, wichtige Verteidigungstipps für Unternehmen aller Größen und Branchen und vieles mehr.

www.watchguard.de

Status der IT-Security

DEUTSCHE UNTERNEHMEN KÖNNEN CYBERBEDROHUNGEN NUR BEDINGT ABWEHREN

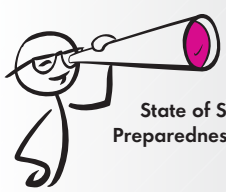


Ivanti hat die Ergebnisse der internationalen Studie „State of Security Preparedness 2023" veröffentlicht. Demnach sind deutsche Unternehmen nur bedingt in der Lage, Angriffe wirksam abzuwehren. Vor allem in den Bereichen Patch Management und der Absicherung gegen Angriffe über die Supply Chain gibt es größte Lücken.

Zweifel am Sicherheitskonzept

Viele deutsche Entscheider haben erhebliche Zweifel an ihren Sicherheitskonzepten. Jeder zehnte Manager ist davon überzeugt, dass sein Unternehmen einen schwerwiegenden Sicherheitsvorfall innerhalb der nächsten 12 Monate nicht verhindern oder stoppen kann. Damit sind die Bedenken bei deutschen Unternehmenslenkern so hoch wie in keinem anderen Land.

Diese Zweifel wirken sich auch auf die Unternehmensfinanzen aus: 9 von 10 Firmen haben bereits Rücklagen für Ransomware-Zahlungen und Kosten im Angriffsfall gebildet. Auch in diesem Punkt stehen deutsche Entscheider unangefochten an der Spitze der betrachteten Länder. Knapp die Hälfte des jährlichen Cyber-Budgets (49 %) fließt in solche Rücklagen, der Rest in Security-Tools und -Teams (43 %) sowie in Cyberversicherungen (6 %).



PLUS

State of Security Preparedness 2023

Cyberbewusstsein in der Führungsetage? Fehlanzeige

Interessanterweise sind es vor allem die C-Entscheider selbst, die es an der nötigen Portion Cyberbewusstsein mangeln lassen. Im Vergleich zu ihren Mitarbeitern im Büro werden sie etwa dreimal so häufig Opfer von Phishing-Angriffen.

Eher irritierend wirkt vor diesem Hintergrund eine Aussage der Leitungsebene zu den Gründen für die fehlende Cyber-Exzellenz des eigenen Unternehmens. Für mehr als 1/3 von ihnen (38 %) spielt ein zu großer Verlass in die eigene Belegschaft dafür eine zentrale Rolle. Ebenfalls bemängelt 1/3 der C-Ebene, dass das Sicherheitstraining für Mitarbeiter ineffizient oder unvollständig sei.

Sorgenkind Patch Management

Insgesamt verdeutlicht die Studie, dass deutsche Unternehmen zwar Vieles daran setzen, sich gegen Cyberangriffe zu wappnen, das Gros der Firmen kämpft aber immer noch mit einer reaktiven Checklisten-Mentalität. Am deutlichsten zeigt sich dies in den Prozessen der Security-Teams selbst, vor allem im Schwachstellen-Management. Heute gilt es, diejenigen Sicherheitslücken zu schließen, von denen ein tatsächliches Risiko für das individuelle Unternehmen ausgeht. Doch anstatt Schwachstellen risikobasiert zu priorisieren, versuchen deutsche Security-Teams immer noch möglichst alle Schwachstellen abzuarbeiten. Zur Verdeutlichung: Zwar geben 9 von 10 Sicherheitsexperten an, dass sie über eine Methode zur Priorisierung verfügen, doch bestätigen sie auch, dass alle Arten von Schwachstellen für sie einen gleich hohen Stellenwert haben. Im Enderfolg vergeuden sie so wertvolle Zeit, die Cyber-Angreifer ausnutzen.

Allerdings: Auf dem Weg zu einem risikobasierten Patch-Management sind deutsche Security-Teams schon einen Schritt weiter als der internationale Durchschnitt. So fokussieren sich bereits 48 Prozent der IT-Sicherheitsteams auf Angriffsvektoren, die aktiv ausgenutzt werden, als auf die jeweils neuesten Schwachstellen. Weltweit sind es durchschnittlich nur 31 Prozent.

www.ivanti.com

C-ENTSCHEIDER UND MANGELNDES SICHERHEITSBEWUSSTSEIN:

2/3 wurden im vergangenen Jahr per Phishing attackiert

1/3 hat auf Scam- und Phishing-Mails geklickt oder Zahlungen geleistet

37% haben ein Arbeitspasswort mit einer Person außerhalb des Unternehmens geteilt

71% nutzen Passwörter, die älter als ein Jahr sind

1/3 verwendet für unterschiedliche Zugänge oder Geräte das gleiche Passwort

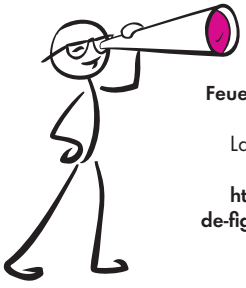
Feuer mit Feuer bekämpfen

AKTUELLE STUDIE ZUR GLOBALEN CYBERSICHERHEITSLAGE

Mit dem Report "Feuer mit Feuer bekämpfen" hat Fastly gerade eine aufschlussreiche Studie zur globalen Cybersicherheitlage in Unternehmen veröffentlicht. Im Interview erklärt Chief Product Architect Sean Leach die wichtigsten Erkenntnisse der Befragung von über 1400 IT-Entscheidern.

it security: *Herr Leach, die Cyber-Bedrohungslage scheint sich derzeit stark zu verändern. In den Medien häufen sich Berichte über immer ausgeklügeltere Cyber-Attacken, Datendiebstähle, und Unternehmen, die Opfer digitaler Erpressung werden. Müssen wir besorgter sein als noch vor ein paar Monaten?*

Sean Leach: Nicht wirklich. Natürlich entwickeln sich Angriffsmethoden weiter, neue Schwachstellen tauchen auf. Und wenn besonders prominente Unternehmen oder wichtige Verwaltungsbehörden von Attacken betroffen sind, macht das Schlagzeilen. Aber Angst ist wie so oft ein schlechter Ratgeber. Tatsächlich ist es so, dass Unternehmen und Organisationen, die die Grundlagen der Cybersicherheit richtig umsetzen, die meisten der gängigen Bedrohungen in der Regel problemlos abwehren können.



PLUS

Feuer mit Feuer bekämpfen

Laden Sie sich die Studie hier herunter:
https://learn.fastly.com/de-fighting-fire-with-fire.html

it security: *Welche Strategie ist die Sinnvollste, um sich effektiv zu schützen?*

Sean Leach: Mit einer Kombination aus bekannten Strategien und richtig umgesetzten Abwehrmechanismen wie etwa einer nicht SMS-basierten Zwei-Faktor-Authentifizierung, strengen Autorisierungsregeln, Rate Limiting zur Kontrolle von ein- und ausgehenden Anfragen und umfassenden Mitarbeiterschulungen sind Sicherheitsteams gut aufgestellt. Dies steht im Gegensatz zu der weit verbreiteten Ansicht, dass „mehr und neu" die Antwort auf Cyber-Bedrohungen sei und auch automatisch mehr Sicherheit bringe. Das ist eines der Ergebnisse unserer neuen Studie.

it security: *Reden wir über diese Analyse: Woher kam die Studienausrichtung?*

Sean Leach: Ihre Eingangsfrage hat es ja schon anklingen lassen: Seit Jahren wird die Cybersicherheitslandschaft als zunehmend komplexer gezeichnet und wahrgenommen. Außerdem werden die Auswirkungen für Unternehmen immer dramatischer, wenn sie nicht bereit oder in der Lage sind, mit den sich entwickelnden Bedrohungen Schritt zu halten. Aus Angst vor möglichen Einfallstoren kaufen die Security-Verantwortlichen deswegen so viele Sicherheitstools, wie es ihr Budget erlaubt. Was unsere Erfahrung aus Gesprächen mit Kunden aber auch zeigt:

Die alltägliche Arbeit wird nicht von einer sich entwickelnden Bedrohungslage bestimmt und die größten Bedenken von IT-Sicherheitsverantwortlichen gehen oft auf bekannte Ursachen zurück. Wir wollten daher das Szenario der zunehmenden Komplexität auf den Prüfstand stellen. Um zu verstehen, welche Herausforderungen, Faktoren, Entwicklungen und Trends die Cybersicherheit heute beeinflussen, entstand eine globale Umfrage unter mehr als 1.400 IT-Entscheidungsträgern in großen Unternehmen aus verschiedenen Branchen in Nordamerika, Europa und dem Asien-Pazifik-Raum. Darunter auch über 200 aus der DACH-Region.

it security: *Was sind Ihre Schlüsselergebnisse?*

Sean Leach: In der Studie zeigte sich, dass Unternehmen angesichts des zunehmenden Drucks anscheinend Komplexität der Einfachheit vorziehen. Statt effizienter Lösungen sehen wir oft den Aufbau übermäßig komplexer Cybersicherheitsumgebungen, die immer mehr Ressourcen binden. Dabei vernachlässigen sie einfache Schritte und Grundlagen, die das Fundament einer starken Cybersicherheitsstrategie bilden.

it security: *Was bedeutet das genau in Zahlen?*

Sean Leach: Über ein Drittel der Befragten (35 Prozent) in der DACH-Region geht davon aus, dass Phishing-Versuche in den nächsten zwölf Monaten die größte Bedrohung für die Cybersicherheit in ihrem Unternehmen darstellen werden, gefolgt von Malware (26 Prozent) sowie Datenschutzverletzun-

gen und -verlusten (25 Prozent). 69 Prozent erhöhen die Investitionen in die Cybersicherheit, um sich auf künftige Sicherheitsrisiken vorzubereiten. Das ist grundsätzlich positiv zu bewerten. Im Durchschnitt sind jedoch nur 59 Prozent der Cybersicherheits-Tools vollständig implementiert und aktiv, was ein klares Zeichen dafür ist, dass viele IT-Leiter ihr Vertrauen in eine Fülle von Tools und Technologien setzen und dann auf das Beste hoffen.

Eine weitere Herausforderung im deutschsprachigen Raum stellt das in den letzten zwei Jahren alltäglich gewordene Homeoffice-Konzept dar. Fast die Hälfte (48 Prozent) der Befragten geht davon aus, dass Cyberangriffe auf Remote-Mitarbeiter in den nächsten zwölf Monaten zu den Hauptbedrohungen für die Cybersicherheit gehören werden. Hinzu kommt, dass in der IT-Branche ein zunehmender Fachkräftemangel herrscht. Der Kampf um (Security-)Talente hat sich dabei durch neue Technologien noch verschärft. 54 Prozent geben an, dass die Verbesserung der Cybersicherheitsfähigkeiten durch Schulungen und/oder die Gewinnung von Talenten hohe Priorität für das nächste Jahr hat. Weitere 39 Prozent planen, das Thema Cybersicherheit „zugänglicher" zu machen, um eine bessere, unternehmensweite Cyber-Hygiene zu fördern.

it security: *Das Fachkräfteproblem wird sich nicht über Nacht lösen lassen – worauf sollten sich Sicherheitsteams also konzentrieren?*

Sean Leach: Da haben Sie Recht. Deswegen werden sich Unternehmen bei der Überprüfung ihrer Sicherheitsabläufe und -technologien die Frage stellen müssen: Sollten wir diese selbst verwalten oder ist es für uns sinnvoller, sie an spezialisierte Sicherheitsanbieter auszulagern? Und wenn es um die Wahl der richtigen Tools geht, sollten drei entscheidende Kriterien berücksichtigt werden: Benutzerfreundlichkeit, Observability und Kompatibilität.

IT-SECURITY-ENTSCHEIDER SOLLTEN AUF EFFIZIENZ SETZEN STATT AUF ÜBERMÄSSIG KOMPLEXE CYBERSICHERHEITSUMGEBUNGEN ZU VERTRAUEN.

Sean Leach, Chief Product Architect, Fastly, www.fastly.com

it security: *Können Sie auf diese drei Aspekte näher eingehen?*

Sean Leach: Nun, grundsätzlich müssen die Tools einfach zu bedienen sein. So ergab unsere Studie, dass 39 Prozent aller eingesetzten Sicherheitstools in Deutschland so eingestellt sind, dass sie Bedrohungen über lange Zeiträume im „Monitoring-Modus" nur protokollieren und nicht tatsächlich blockieren und damit keinen wirklichen Schutz bieten. Dies hat nach unseren Ergebnissen zwei Gründe: Zum einen gaben die Befragten an, dass 38 Prozent der erkannten Meldungen sich als Fehlalarme herausstellen. Zum anderen fanden wir heraus, dass die Angst, einen legitimen Nutzer zu blockieren, oft größer ist als die Angst, von einem böswilligen Akteur kompromittiert zu werden.

Ein weiterer wichtiger Faktor ist Observability. Sicherheitstools müssen Fachleuten klar verwertbare Einblicke liefern. Unternehmen, die wenig oder keinen Zugang zu diesen Informationen haben und Daten mehrerer Sicherheitslösungen nicht gesammelt betrachten können, werden in ihrer Sicherheitsstrategie gehindert. Einfach ausgedrückt: Wenn Sie nicht wissen, wovor Ihre Tools Sie schützen, können Sie nicht wissen, was Sie tun müssen, um geschützt zu bleiben.

Zuletzt müssen die Sicherheitslösungen leicht in bestehende Systeme integrierbar sein. Hierzu ergaben unsere Untersuchungen, dass sich durchschnittlich 41 Prozent der auf Netzwerk und Anwendungen ausgerichteten Cybersicherheitslösungen in ihrer Funktionalität überschneiden. Das ist ein deutlicher Hinweis darauf, dass Unternehmen eine Reihe von Tools kaufen, die gar nicht für eine sinnvolle Zusammenarbeit ausgelegt sind.

Entscheidend für eine zuverlässige und effiziente Cybersicherheitsarchitektur ist die Kombination dieser Faktoren.

it security: *Herr Leach, wir danken Ihnen für das Gespräch.*

MITRE ATT&CK

WO STEHEN WIR HEUTE?

Die Zahl der Cyberangriffe steigt und steigt. Die aktuelle Bedrohungslage rund um den Ukraine Konflikt hat gerade das Thema Nation-State Attacks weiter befeuert. So richten sich diese Angriffe nicht exklusiv gegen die ukrainische Infrastruktur, sondern bedrohen auch die Ukraine unterstützende Unternehmen im Westen. Wie soll man darauf reagieren? Wie soll man wissen, welche Aktoren und welche Maßnahmen für das eigene Unternehmen relevant sind?

Im Jahr 2019 haben wir auf it-daily.net einen Artikel zum MITRE ATT&CK Framework veröffentlicht der dargestellt hat, was das Framework ist und wie es uns in der Cyber Sicherheit hilft. Viel ist seitdem passiert und auch das Framework hat sich massiv weiterentwickelt. Es ist an der Zeit, die Änderungen zu beleuchten und das Framework in den Kontext der heutigen Bedrohungslage zu setzen.

CYBER SICHERHEITSTEAMS GEHEN HEUTE VIEL STRUKTURIERTER VOR UND DIE STÄNDIG WEITER ENTWICKELTE ATT&CK MATRIX WIRD ZU IMMER MEHR UND IMMER STRUKTURIERTEN SICHERHEITSTESTS FÜHREN.

Till Jäger, Leader Sales, SOC Prime, https://socprime.com/

Von V4 zu V12

So war zum Zeitpunkt unseres oben genannten Artikels die Version 4 aktuell, heute sind wir bei Version 12 angekommen. Neben vielen Änderungen im Detail, ist die PRE-ATT&CK Matrix in die Enterprise Matrix integriert worden, neben den Standard Plattformen auch Cloud, Network und Containers hinzugekommen, sowie eine neue Matrix für ICS (Industrial Control Systems) entstanden. Aus Sicht der Threat Detection Industry oder der Sicherheitsanalysten, ist sicher eine der wesentlichen Verbesserungen die Ausgliederung von Datenquellen in eigene Objekte.

Während vor drei Jahren das MITRE ATT&CK Framework („die Matrix") für

PRE-ATT&CK

Priority Definition
- Planning, Direction

Target Selection
Information Gathering
- Technical, People,Organizational

Weakness Identifikation
- Technical, People, Organizational

Adversary OpSec
Establish & Maintain Infrastructure
Persona Development
Build Capabilities
Test Capabilities
Stage Capabilities

ENTERPRISE ATT&CK

Initial Access
Execution
Persistence
Privilege Escalation
Defense Evasion
Credential Access
Discovery
Lateral Movement
Collection
Exfiltration
Command and Control

Die sieben Stufen des Cyber Attack Lifecycle, heute bekannt als die Cyber Kill Chain, erstmalig verbreitet von Lockheed Martin.

viele Sicherheitsverantwortliche noch eine mehr oder weniger theoretische Referenzarchitektur war, hat die praktische Umsetzung in freien sowie kommerziellen Produkten in den letzten Jahren massiv Fahrt aufgenommen.

Die Nutzung von MITRE ATT&CK hat einen deutlichen Wendepunkt erreicht. Während ein Großteil der Anwender ATT&CK zumindest einsetzt, um die eigene Abwehrfähigkeit zu dokumentieren, ist sie bei einem steigenden Anteil nunmehr auch ein fester Bestandteil der Sicherheitsstrategie geworden.

Auch hat sich rund um das Framework ein veritables Geschäft mit Trainings entwickelt. MITRE selbst, über die Foundation MITRE-Engenuity, spielt mit dem „MITRE ATT&CK Defender" Kursen ebenfalls auf dem Spielfeld mit.

Keine 100prozentige Sicherheit

Allerdings sollte gerade bei der Bezeichnung „Framework" immer beachtet werden, dass es sich nicht um ein vollständiges Rahmenwerk aller möglichen Angriffsvektoren handelt.

MITRE ATT&CK basiert letztendlich auf veröffentlichten, dokumentierten Vorfällen. Jedoch wird nur ein kleiner Teil der Vorfälle öffentlich gemeldet. Obwohl die Informationen in der Matrix die meisten TTPs (Tactics, Techniques and Procedures) abdecken könnten, wird dies nie dem Anspruch an Vollständigkeit gerecht. Darüber hinaus ist eine komplette Abdeckung aller TTPs auch technisch nicht möglich.

Dennoch bietet ATT&CK stand heute eines der umfangreichsten Werke an und ist nicht nur deswegen in der Branche zum de-facto Standard geworden.

ATT&CK ist eine Wissensdatenbank für gegnerische Taktiken und Techniken, die auf realen Beobachtungen basieren. Sicherheitsverantwortliche sollten sie als solches einsetzen und nicht als etwas betrachten, das es zu 100% abzudecken gilt.

Typische Anwendungsfälle:

Grundlegende Ausrichtung / Richtlinie der Cybersicherheitsstrategie

CISOs und andere Sicherheitsverantwortliche nutzen zunehmend ATT&CK um die Sicherheitsstrategie des Unternehmens daran auszurichten.

Anreichern von Warnungen im SOC / Alert-Triage

ATT&CK gibt den SOC Teams wichtige Hinweise nach welchen Indikatoren zu suchen ist, um eine Warnung besser zu klassifizieren und die gesamte Breite des Angriffs aufzudecken

Analyse & besseres Verständnis der TTPs (Taktiken, Techniken und Verfahren) der Angreifer

So interessieren sich zum Beispiel Behörden oder behördennahe Unternehmen im Besonderen für nationalstaatliche Bedrohungen wie etwa APT29. Die in MITRE ATT&CK als Bedrohungsgruppen (Threat Groups) bezeichneten Akteure sind, soweit die Information verfügbar, den jeweiligen Industriezweigen zugeordnet, so dass der Sicherheitsanalyst sich vorrangig auf die Bedrohungsgruppen konzentrieren kann, die den spezifischen Industriezweig im Fokus haben (zum Beispiel APT28, APT29 – Behörden & Militär, APT41 – Gesundheitssektor/Telekom/Spieleindustrie, APT34 – Oil & Gas Sektor).

Anreichern der Bedrohungsinformation bestehender Technologien

Werkzeuge nutzen ATT&CK zunehmend zwecks Anreicherung der produzierten Informationen. Reports werden danach ausgerichtet.

Analyse der Fähigkeiten von Sicherheitswerkzeugen

Vor dem Hintergrund der derzeitigen Einsparmaßnahmen, die auch vor der Cyber Security Industrie nicht halt macht, nutzen immer mehr Unternehmen das Rahmenwerk, um vorhandene Tools und Technologien in Ihren Abwehr Fähigkeiten abzubilden und mögliche Überschneidungen (und natürlich auch Lücken) aufzudecken. Dadurch lässt sich effektiv die Landschaft an Sicherheitswerkzeugen im Unternehmen optimieren, sowie deren Einsatz gegenüber dem Management besser argumentieren und dokumentieren.

SOC Assessments

Assessments bestehender SOCs orientieren sich zunehmend an ATT&CK und

nutzen dies um Lücken in der Abwehr oder auch in bestehenden Prozessen zu dokumentieren und zu optimieren.

SIEM Rule Mapping

Ein sehr populärer Anwendungsfall betrifft die Welt der SIEM (Security Information & Event Management) Systeme. Während vor einigen Jahren die vom Hersteller mitgelieferten Regeln noch als „der Standard" angesehen wurden, gehen Unternehmen heute deutlich analytischer vor. So wird immer häufiger das MITRE ATT&CK Framework genutzt um die für das jeweilige Unternehmen relevanten Akteure zu ermitteln, diese dann auf die verfügbaren Log Quellen abzubilden und den dafür relevanten „Detection Content" individuell zu beziehen und ausrollen. Das SIEM wird dadurch von einem generischen zu einem individuell zugeschnittenen Werkzeug. Ein Anbieter, der sich sehr früh mit diesem Thema auseinandergesetzt hat, ist die mittlerweile marktführende Plattform von SOC Prime (siehe Kasten).

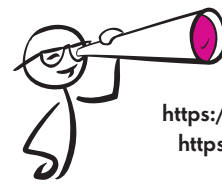
Wo geht die Reise hin? Ein Blick in die Zukunft

Cyber Sicherheitsteams gehen heute viel strukturierter vor und die ständig weiter entwickelte ATT&CK Matrix wird zu immer mehr und immer strukturierten Sicherheitstests führen. So ist die Matrix heute bereits der Goldstandard bei SOC Assessments. Die weitere Verbreitung von „Detection as Code" sowie auch von anderen Werkzeugen wie Red Teaming Tools verleihen der Matrix weiteren Vortrieb. Startups im Sicherheitsumfeld kommen um eine Unterstützung von ATT&CK nicht herum und bewerben dies aktiv. Basierend auf dem Erfolg von MITRE ATT&CK werden CISOs und SOC-Teams offener für andere MITRE-Projekte wie MITRE D3fend (A Knowledge Graph of Cybersecurity Countermeasures) und MITRE Engage (ein Framework für die Planung und Diskussion von gegnerischem Engagement und Operationen).

Till Jäger

SOC PRIME

- SOC Prime betreibt eine weltweite Plattform für kollaborative Cyberabwehr und transformiert die Erkennung von Bedrohungen auf globaler Ebene. Angetrieben von seiner Detection-as-Code-Plattform, die die Zusammenarbeit einer globalen Cybersicherheits-Community fördert, kuratiert die Lösung das weltweit größte Repository für Erkennungsinhalte, das über 200.000 Erkennungsalgorithmen basierend auf dem Sigma-Regelstandard aggregiert.
- Die Plattform bietet die aktuellsten Sigma-Regeln neben innovativen Tools für Bedrohungserkennung, Bedrohungssuche, Streaming von Erkennungsinhalten und SOC-Management bei gleichzeitiger Integration mit über 25 SIEM-, EDR- und XDR-Plattformen.
- Die Crowdsourcing-Initiative von SOC Prime, das Threat Bounty Program verbindet 600 Forscher und Threat Hunter aus der ganzen Welt, die Sigma- und YARA-Regeln erstellen, sie täglich mit Branchenkollegen teilen und ihre Beiträge monetarisieren. Die Plattform verbindet Sicherheitsexperten weltweit und stellt sicher, dass relevante Sigma-Regeln für jede kritische Bedrohung innerhalb von 24 Stunden oder weniger bereitgestellt werden.
- Die branchenweit erste Suchmaschine für Cyber-Bedrohungen bietet kostenlosen und sofortigen Zugriff auf Kontextinformationen, einschließlich Tags, MITRE ATT&CK- und CTI-Referenzen, CVE-Beschreibungen und aufschlussreichere Metadaten, die sicherstellen, dass jeder Sicherheitsfachmann relevante Informationen und Sigma-Regeln zu Cyber-Bedrohungen sofort finden kann um diese auf seine individuelle Sicherheitsinfrastruktur anzuwenden.
- Der kollaborative Cyber-Defense-Ansatz bewältigt die Herausforderung des Talentmangels mit seinem Quick Hunt-Modul, das es jedem ermöglicht, auch ohne Erfahrung auf diesem Gebiet ein Threat Hunter zu werden. Teams können automatisch nach den neuesten Bedrohungen in ihrer SIEM- oder EDR-Umgebung suchen, mit Top-Trend Threat Hunt Anfragen, die von der Empfehlungsmaschine basierend auf Information der Branchenkollegen vorgeschlagen werden. Das Continuous Content Management (CCM) / Outpost-Modul von SOC Prime ermöglicht das Streamen der aktuellsten Erkennungen, die als Inhaltslisten organisiert sind, direkt in ihre Umgebung.



MEHR WERT

https://attack.mitre.org
https://bit.ly/3Z11Tz1

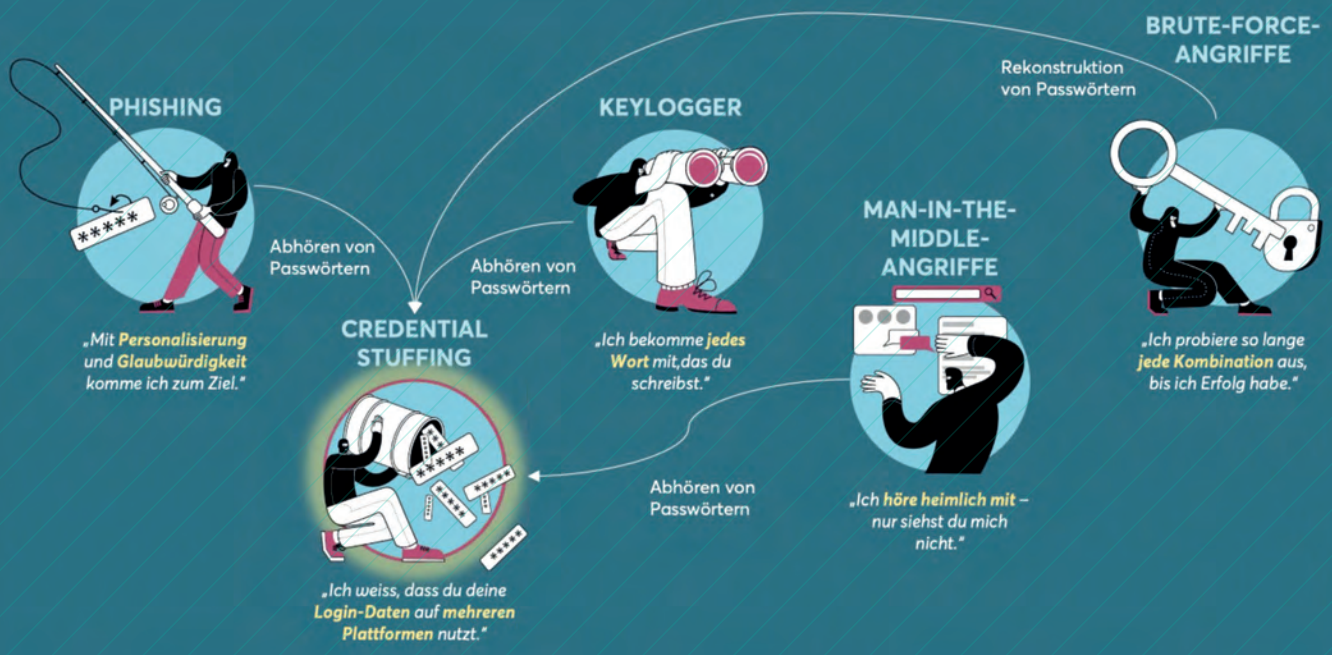
Einträgliches Business

ACCOUNT TAKEOVER

Die feindliche Übernahme von Benutzerkonten hat sich zu einem einträglichen Geschäft für Cyberkriminelle entwickelt. Durch die Nutzung des Internets und der zunehmenden Digitalisierung ist das Angriffsspektrum weit gefasst: es reicht von E-Mails, über die sozialen Netzwerke und den Online-Shops branchenübergreifend in alle Bereiche des täglichen Lebens. Das Account Takeover ist dementsprechend ein attraktiver Businesszweig für das organisierte Verbrechen geworden und Zugangsdaten sind die Basis, die sie benötigen, um bestehende Benutzerkonten zu übernehmen (engl. Account-Takeover). Nachfolgend die fünf erfolgreichsten Angriffsvektoren, die Nevis identifiziert hat.

www.nevis.net

DIE 5 ANGRIFFSVEKTOREN



Quelle: Nevis Security GmbH

Cyber-Attacken: Was hilft ein Threat Navigator?

INNOVATIVES CLIENT VISIBILITY-TOOL HILFT, DAS RISIKO VON CYBERANGRIFFEN ZU MINIMIEREN

Mit dem Threat Navigator erhalten Organisationen eine grafische Übersicht ihrer vorhandenen Sicherheitsmaßnahmen und können so besser einschätzen, wie gut sie vor den neuesten Angriffstechniken geschützt sind. Einziger Wermutstropfen: das Tool ist nicht stand-alone verfügbar, denn der Threat Navigator ist eine Kerkomponente des MDR (Managed Detection and Response) -Portals von Kudelski Security und in Fusion Detect integriert, das die Grundlage der hauseigenen XDR-Architektur darstellt.

Bei Managed-Detection-and-Response-Services wird die Angriffserkennung in der Regel mit einem Reaktionsservice kombiniert. Der Vorteil: als Service muss man als Unternehmen kein eigenes Expertenteam vorhalten.

Was unterscheidet XDR von EDR und MDR? EDR bezeichnet die endpunktbasierte Detektion und Reaktion, MDR die gemanagte Erkennung und Reaktion und XDR die erweiterte Erkennung und Reaktion auf Cybervorfälle.

Anwender erhalten damit automatisierte Empfehlungen, wie sie Bedrohungen in ihrem Umfeld besser erkennen können.

Herausforderungen

Cyberangriffe werden bekanntlicherweise immer häufiger und raffinierter. Gleichzeitig fordern Führungskräfte und Vorstände von ihren Sicherheitsteams, dass sie die Sicherheitslage klar kommunizieren. Eine der Herausforderungen für Sicherheitsteams ist die richtige Einschätzung und Kommunikation der Risiken und Möglichkeiten, um die modernen Bedrohungen und Angreifer zu erkennen. Mit dem Tool erhält man ein tieferes Verständnis darüber, welche Daten und Sicherheitstools notwendig sind, um die für ihre Branche bekannten Angreifer besser zu identifizieren.

DER THREAT NAVIGATOR ERMÖGLICHT UNSEREN KUNDEN, RISIKEN BESSER ZU VERSTEHEN UND ABWEHRMASSNAHMEN ZU PRIORISIEREN.

Jacques Boschung, Head of Kudelski Security, www.kudelskisecurity.com

Threat Navigator ist Teil der breit angelegten, auf dem Cyber Fusion Center basierenden MDR-Strategie von Kudelski Security, die Technologie, Dienstleistungen und hochoptimierte Prozesse und Verfahren kombiniert, die für jeden Kunden individuell angepasst werden. Dadurch werden bestehende MDR-Funktionen erweitert, die das bekannte MITRE ATT&CK-Framwork nutzen. Außerdem erhalten Sicherheitsverantwortliche durch die Analysen mit einer Bedrohungsmodellierung einen sofortigen Überblick über ihre Sicherheitsabdeckung.

Die Ergebnisse werden nach Relevanz gestaffelt und bieten Einblicke und Empfehlungen bezüglich der wichtigsten Sicherheitslücken. Damit können Kunden eine umfassende und rund um die Uhr aktive Strategie zur Erkennung und Abwehr von Bedrohungen implementieren, die auch Pläne zur Risikominimierung und Schwachstellenverwaltung umfasst. Unterstützt wird diese Strategie durch Threat Intelligence, Threat Hunting, effiziente Tools und Expertise in den Bereichen digitale Forensik und Incident Response (DFIR).

Die Vorteile der dynamischen Oberfläche im Überblick:

- Abgleich der aktuellen Sicherheitsabdeckung mit dem MITRE ATT&CK-Framwork, das besonders die für die jeweilige Branche relevanten Bedrohungsakteure sowie ihre Techniken priorisiert.

- Umfangreiche Wissensdatenbank mit Erkenntnissen zu Bedrohungsakteuren (einschließlich der verwendeten Techniken und angegriffenen Branchen), umfangreiche Informationen über MITRE ATT&CK-Techniken sowie Sicherheitsdaten, die von Fusion Detext, der Grundlage der XDR-Architektur, erfasst werden.

- Empfehlungen und Berichte mit vollständigen Listen priorisierter Angriffstechniken sowie Exportfunktionen.

- Für zukünftige Versionen sind branchenspezifische Funktionen geplant, um Verteidigungsstrategien zu verbessern und regelmäßig Sicherheitsempfehlungen zu geben, während sich die Bedrohungslage sowie das Cloud- und Hybrid-Unternehmensumfeld verändern.

Visualisieren, Priorisieren, Beseitigen

Die proaktive Erkennung von Bedrohungen hängt davon ab, herauszufinden, welche Bedrohungen für das jeweilige Unternehmen relevant sind, in welchem Umfang sie bereits abgedeckt sind und welche Maßnahmen man ergreifen sollte, um die Lücken zu schließen. Das Threat Navigator-Tool basiert auf dem MITRE ATT&CK-Framework und einer individuellen Bedrohungsmodellierung. Es ist vollständig in das Kundenportal von Kudelski Security integriert.

Methodik

Das Onboarding mit dem Managed Detection and Response Service von Kudelski Security ist aus gutem Grund sehr gründlich. Je mehr Informationen über das Unternehmen vorliegen, desto genauer ist das zu erstellende Bedrohungsmodell.

Definition des Cybersecurity-Bedrohungsmodell

Die Erstellung eines umfassenden Bedrohungsmodells – basierend auf der jeweiligen Angriffsfläche, den Business- und IT-Security-Experten und den potenziellen Bedrohungsakteuren – ist entscheidend, um zu verstehen, wie das Unternehmen angegriffen werden kann. Das ist der erste Schritt, um kritische Sicherheitslücken in ihrer Transparenz und Abdeckung aufzuzeigen.

Effektiv verteidigen

Ziel muss es sein, Abdeckungslücken durch priorisierte ATT&CK-Techniken automatisch zu erkennen und zu schließen. Das Threat Navigator-Tool verfolgt keinen „Alles-auf-einmal"-Ansatz, sondern hebt die Angriffstechniken hervor, die für das Unternehmen höchste Priorität haben. Durch die Zusammenführung von Datenquellen aus der jeweiligen Umgebung mit verfügbaren Erkennungsregeln und kontextbezogenen Informationen über die jeweilige Branche sowie geografische Informationen hebt der Threat Navigator die fünf wichtigsten empfohlenen Techniken für die Unternehmen hervor, um ATT&CK-Abdeckungslücken zu schließen. Die nächsten empfohlenen Angriffstechniken sind ebenfalls dokumentiert.

Datenanforderungen für die Erkennung von Angriffstechniken

Sobald die Unternehmen wissen, mit welchen Angriffstechniken ihr Unternehmen konfrontiert ist, hilft eine Daten-Checkliste dabei, das Rauschen zu reduzieren und die erforderlichen kritischen Daten zu definieren. Das Ziel ist

WIR GLAUBEN, DASS DIE TRANSPARENZ UND DAS WISSEN, DAS WIR IN UNSEREM KUNDENPORTAL ZUR VERFÜGUNG STELLEN, EIN ENTSCHEIDENDER VORTEIL FÜR UNTERNEHMEN IST.

Olivier Spielmann, First Vice President, Global Managed Detection & Response, Kudelski Security, www.kudelskisecurity.com

eine kontinuierliche, auf Bedrohungen ausgerichtete Verteidigung, um ihre allgemeine Sicherheitslage zu stärken.

Priorisierung von Angriffsabwehrmaßnahmen
Nachdem die Grundlagen geschaffen wurden, ist der Threat Navigator ein nützliches Tool, das Anwendern hilft, Prioritäten für ihre Abwehrmaßnahmen zu setzen. Sobald sie ein klares Bild von der Art der Angriffe haben, mit denen sie konfrontiert sind, können sie sich überlegen, wie sie ihre wichtigen Ressourcen am besten schützen.

Die Prioritätensetzung konzentriert sich auf drei Bereiche:

1. Die Bedrohungsakteure – und die von ihnen verwendeten Techniken – die am ehesten auf die Branche des jeweiligen Unternehmens abzielen
2. Die Daten, die von ihren Sicherheitstechnologien stammen
3. Die von Kudelski Security gepflegten Erkennungsregeln

Die Aggregation dieser Daten ermöglicht es zu verstehen, wo die Sicherheitslücken liegen und welche fünf Lücken am dringendsten geschlossen werden müssen.

Externe Daten einbinden
Anwender können den Threat Navigator zusätzlich mit Daten aktualisieren, die außerhalb der Kudelski Security MDR Services vorliegen. Sie können Datenquellen als „abgedeckt" markieren, wenn sie eine Quelle selbst überwachen oder wenn ein anderer Anbieter diese Informationen für sie bereitstellt.

Ein Security Detection Engineering Team pflegt die Erkennungen „als Code". Das bedeutet, dass die Informationen aus dem Threat Navigator genutzt werden, um Entwicklungen zu verstehen und Erkennungsaktivitäten entsprechend immer wieder neu zu priorisieren. Das geht soweit, Erkennungen automatisch der Kunden-Infrastruktur bereitzustellen soweit die Technologien unterstützt werden. Das bedeutet, dass die globale Sichtbarkeit immer berücksichtigt wird, wenn eine neue Erkennungslogik geändert wird.

THREAT HUNTING

Unter Threat Hunting versteht man die proaktive Suche nach Cyber-Bedrohungen, die unentdeckt in einem Netzwerk lauern. Die Cyber-Bedrohungsjagd gräbt tief, um böswillige Akteure in Ihrer Umgebung zu finden, die an Ihren ursprünglichen Endpunkt-Sicherheitsmaßnahmen vorbeigeschlüpft sind.
Nachdem sich ein Angreifer eingeschlichen hat, kann er monatelang unbemerkt in einem Netzwerk verbleiben, während er heimlich Daten sammelt, nach vertraulichem Material sucht oder sich Anmeldeinformationen verschafft, mit denen er sich seitlich in der Umgebung bewegen kann.
Wenn es einem Angreifer gelungen ist, sich der Erkennung zu entziehen und ein Angriff die Verteidigungsmaßnahmen eines Unternehmens durchdrungen hat, verfügen viele Unternehmen nicht über die fortschrittlichen Erkennungsfunktionen, die erforderlich sind, um zu verhindern, dass die fortschrittlichen, dauerhaften Bedrohungen im Netzwerk verbleiben. Aus diesem Grund ist die Bedrohungsjagd ein wesentlicher Bestandteil jeder Verteidigungsstrategie.

Threat Detection

Im Allgemeinen lassen sich alle Bedrohungserkennungen in vier Hauptkategorien einteilen: Konfiguration, Modellierung, Indikator, und Bedrohungsverhalten. Jede Kategorie kann unterschiedliche Anforderungen und Ansätze unterstützen, je nach den geschäftlichen Anforderungen. Wenn das Ziel ist, neuartige Angriffe zu finden und man bereit ist, einen erheblichen Aufwand zu betreiben, dann ist die Modellierung ein guter Ansatz. Wenn das Ziel darin besteht, ähnliche Angriffe mit weniger Aufwand zu finden, dann ist die Analyse des Bedrohungsverhaltens der richtige Ansatz.

Threat Intelligence

Darunter versteht man den Prozess der Identifizierung und Analyse von Cyberbedrohungen. Dabei werden als „Threat Intelligence" entweder die Daten selbst bezeichnet, die über eine potenzielle Bedrohung erfasst werden, oder der Prozess der Erfassung, die Verarbeitung und die Analyse dieser Daten, um sich ein umfassendes Bild von einer Bedrohung zu machen. Threat Intelligence-Daten werden zunächst gesichtet und im Kontext untersucht, um Probleme zu identifizieren und für jedes aufgespürte Problem eine spezifische Lösung zu entwickeln.

Threat Modeling

Bei Threat Modeling (Bedrohungsmodellierung) handelt es sich um eine sehr bewerte konzeptionelle Analysetechnik mit deren Hilfe sich potentielle Schwachstellen (bzw. Risken) bereits frühzeitig bei der Entwicklung von Anwendungen oder Diensten identifizieren und hierfür erforderliche Maßnahmen ableiten lassen.

DATENSICHERHEIT

SO SCHÜTZEN UNTERNEHMEN IHRE SENSIBLEN UND GESCHÄFTSKRITISCHEN DATEN

Betriebliche Informationsflüsse erfolgen heute zunehmend digital – und die Menge der verarbeiteten Daten steigt dabei täglich an. Für Unternehmen wächst damit auch die Gefahr, ins Visier von Cyberkriminellen zu geraten. Wie das Bundeskriminalamt im Bundeslagebild Cybercrime verlauten ließ, hat die Zahl erfasster Cyberstraftaten mit 146.363 Delikten im Jahr 2021 eine Rekordmarke erreicht. Einer Studie zufolge haben Cyberangriffe bei 90 Prozent der befragten deutschen Unternehmen seit Beginn der COVID-19-Pandemie sogar noch zugenommen.

Und hier liegt das Problem, denn eben genau wegen der Pandemie wurden bei fast allen Unternehmen Sicherheitsprojekte auf Eis gelegt – ein äußerst gefährliches Wagnis.

Um die Sicherheit von Daten zu gewährleisten, bedarf es einer ausgeklügelten Strategie, die nicht nur die rechtlichen Anforderungen abdeckt, sondern auch für das Unternehmen gangbar ist. Hier heißt es, Maßnahmen einzuführen, die es gestatten, sensible Informationen schnell, bequem und ohne Risiken auszutauschen. Zudem gilt es sicherzustellen, dass ausschließlich berechtigte Personen darauf zugreifen können.

WHITEPAPER DOWNLOAD

Das Whitepaper umfasst 35 Seiten und steht kostenlos zum Download bereit.
www.it-daily.net/Download

Das vorliegende Whitepaper gibt Ihnen deshalb Hilfestellung zu folgenden Fragen:

- Was ist Datensicherheit und welche gesetzlichen Grundlagen gibt es dazu?
- Welche Risiken ergeben sich aus mangelnder Datensicherheit?
- Welche Maßnahmen für Datensicherheit gibt es?
- Wie sieht Datensicherheit in der Praxis aus?
- Welche hochsicheren Datenraumlösungen gibt es?

Flankiert wird dies mit nützlichen Checklisten und wertvollen Tipps.

Converged Endpoint Management

ANTWORTEN AUF DIE FRAGEN EINER IMMER KOMPLEXEREN IT-BEDROHUNGSLANDSCHAFT

Nicht nur das Volumen an Cyberangriffen hat im vergangenen Jahr zugenommen, die Angriffe werden auch immer komplexer. So unterteilt der Data Breach Investigations Report 2022 von Verizon die Angriffe in mehrere übergeordnete Kategorien ein.

Die vier hervorstechendsten sind Folgende:

Hacking – Gezielte Angriffe auf IT-Systeme (Backdoor, Web Applications, DoS etc.)

Malware – Schadcode, der Änderungen am IT-System vornimmt (Ransomware, Backdoor, manipulierte Software Updates und Downloader)

Social Engineering – Täuschung und Manipulation von Mitarbeitern, um Zugriff auf die IT-Infrastruktur zu erlangen (Phishing, Emails, Social Engineering etc.)

Missbrauch – Die Verwendung von Privilegien und Rechten im Widerspruch zum ursprünglich formulierten Zweck

Jede dieser Angriffswege nutzt unterschiedliche Schwachstellen in der IT-Sicherheitsstrategie des Opfers aus. Die meisten Sicherheitslösungen konzentrieren sich jedoch auf eine bestimmte Angriffsstrategie und können daher keinen vollumfänglichen Schutz garantieren. Hinzu kommt, dass die neue Arbeitswelt durch Home-Office und Fernzugriff auf Firmendaten die Situation noch komplexer gemacht hat. Die Masse an neuen Endgeräten im Firmennetz sowie die Implementation einer Vielzahl heterogener Softwarelösungen haben ein schwer manage- und überwachbares IT-Ökosystem geformt.

> ES GIBT VIELE ANGRIFFSWEGE, ABER ALLE NUTZEN UNTERSCHIEDLICHE SCHWACHSTELLEN IN DER IT-SICHERHEITSSTRATEGIE DER OPFER AUS.
>
> **Zac Warren,**
> **Chief Security Advisor EMEA, Tanium,**
> **www.tanium.com**

Unübersichtliche Endpoint-Landschaft

Eine verteilte Belegschaft, naürlich auch pandemie-begünstigt durch das Home Office, bedeutet einen gewissen Grad an Kontrollverlust - nicht unbedingt über die Belegschaft, sondern über die Vielzahl von unsichtbaren und ungeschützten Endpunkten in der IT-Infrastruktur von Unternehmen. Daten von Tanium zeigen, dass in 94 Prozent der Organisationen mindestens 20 Prozent der Endgeräte ungeschützt sind. Hinzu kommt, dass die Daten immer mehr in fest verschlossenen Silos fragmentiert werden, was eine rechtzeitige Reaktion auf Vorfälle erschwert.

Insofern stellt Converged Endpoint Management (XEM) einen Paradigmenwechsel in der IT-Sicherheit dar. Die richtige Antwort auf die wachsende Zahl von Sicherheitsproblemen besteht nicht darin, die Zahl der Lösungen für jedes IT-Ökosystem zu erhöhen. Das Gegenteil ist der Fall: Mangelnde Kompatibilität und fehlende Synergien führen dazu, dass dieser Ansatz der IT-Sicherheitslage eines Unternehmens mehr schadet als nützt.

Fast die Hälfte der Befragten der Foundry's „Security Priorities Study" (45 Prozent) gab an, dass sie innerhalb des letzten Jahres mindestens vier neue Sicherheitslösungen zu ihrem IT-Arsenal hinzugefügt haben. Ein heutiges Unternehmen verfügt im Durchschnitt über 43 separate IT-Sicherheits- und Sicherheitsmanagement-Tools in seiner Infrastruktur, die häufig von verschiedenen Abteilungen betrieben werden. Dies schafft eine hochexplosive Mischung aus Undurchsichtigkeit und Unsicherheit, die CIOs und CISOs gleichermaßen Kopfzerbrechen bereitet.

Die Lösung: XEM

Converged Endpoint (XEM) Management wirkt diesen Tendenzen entgegen und beseitigt die Hauptursache für die meisten der heutigen IT-Vorfälle: Mangelnde Endpunkttransparenz und

schlechtes Patch-Management. XEM bietet den Sicherheitsspezialisten einen konsolidierten und hoch automatisierten Überblick über alle Endpunkte in der IT-Infrastruktur ihres Unternehmens. Es verkürzt die Reaktionszeit bei Sicherheitsverletzungen und ermöglicht eine schnelle und fundierte Reaktion, um eine Kompromittierung des Unternehmensnetzwerks durch Cyberkriminelle zu verhindern.

XEM entwirrt die verstreute IT-Infrastruktur in einer Welt verteilter Belegschaften und gibt dem Sicherheitspersonal die Kontrolle zurück, die es während einer langen Zeit der Fernarbeit sukzessive verloren hatte. Converged Endpoint Management ist in der Lage auf verschiedenen Plattformen oder in verschiedenen Softwareumgebungen reibungslos zu funktionieren. Die plattformübergreifende Kompatibilität ist ein zentraler Bestandteil der Kontrolle und Verwaltung verteilter IT-Systeme und das Fundament von XEM.

Automatisch und flexibel

Insofern bietet XEM Echtzeit-Sicherheit und passt sich an ein heterogenes IT-Ökosystem an.

Den besten Schutz bieten Lösungen, die nicht erst auf Vorfälle reagieren müssen, sondern die Sicherheit durch einen ständigen Abgleich zum optimalen System-Zustand generieren.

Durch den Einsatz von Künstlicher Intelligenz und Machine Learning kann die bestmögliche und stabilste Konfiguration vom Unternehmensnetz und all seiner Komponenten – vom zentralen Server bis hin zum entlegendsten Endpunkt – ermittelt werden. Dadurch können Abweichungen im laufenden Betrieb schnell erkannt, analysiert und bei Bedarf behoben werden.

Die riesige Menge an digitalen Prozessen kann jedoch unmöglich manuell abgearbeitet werden. Selbst eine gut ausstaffierte IT-Abteilung kann nicht jede einzelne Veränderung im System beobachten und verfolgen. Hier kommt die besondere Stärke von intelligenten und selbstlernenden Algorithmen zum Tragen. Durch die Zusammenführung aller relevanten Kriterien wie die Gesamtheit der im Firmennetz befindlichen Endpunkte, sowie deren Software- und Updatestatus auf einer zentralen Plattform, können einzelne Verantwortungsträger und Spezialisten informierte Entscheidungen in Echtzeit treffen – ganz ohne die dafür relevanten Informationen in Handarbeit zusammentragen zu müssen.

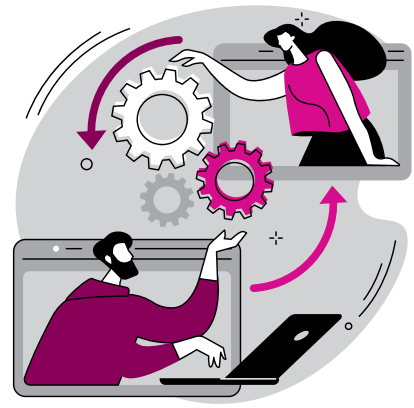
Die Vorteile von XEM auf einen Blick:

- CIOs können alle Endpunkte in wenigen Arbeitsschritten patchen und konfigurieren
- CISOs können Schwachstellen in Echtzeit erkennen und unternehmensweit beheben
- Infrastrukturteams können Cloud-Migrationen in Wochen anstatt in Jahren durchführen
- Der Einkauf kann erkennen, ob sie Software lizenzieren, die sie nicht benötigen
- Datenverwalter können sensible Daten in großem Umfang aufspüren und entfernen
- Auditoren können nachverfolgen, ob das Unternehmen Vorschriften und Compliance einhält.

Converged Endpoint Management ist die maßgeschneiderte Antwort auf ein täglich wachsendes Datenaufkommen kombiniert mit der Aufweichung klassischer Strukturen der Büroarbeit. Es stellt IT-Sicherheitsverantwortliche und Techniker vor eine große Belastungsprobe. Ein stetiger Zufluss neuer Endpunkte wird von einer – teils automatisch generierten – Datenflut flankiert und droht die begrenzte Anzahl an qualifiziertem Fachpersonal zu überfordern. Um mit dieser erhöhten Taktung im Tagesgeschäft mitzuhalten, ohne Burnouts bei Mitarbeitern oder Sicherheitslücken im System in Kauf nehmen zu müssen, benötigt es eine Abkehr von althergebrachten Methoden und eine Zuwendung zu Lösungen, die den Anforderungen der Zeit gewachsen sind.

XEM ist nicht weniger als ein Paradigmenwechsel und bietet die maßgeschneiderten Antworten auf die Fragen einer hochfrequenten und komplexen digitalen Gegenwart.

Zac Warren



Resilient Zero Trust

SCHRITT FÜR SCHRITT ZU MEHR SICHERHEIT

Es gibt viele Interpretationsvarianten für einen bestehenden Namen und immer wieder tauchen neue Begriffe auf. Zero Trust ist ein häufiger, oft unterschiedlich interpretierter Begriff. Zero-Trust-Architekturen und Zero-Trust-Network-Access werden so beispielsweise oft miteinander verwechselt.

Während ZTNA ein notwendiges Element jedes Zero-Trust-Sicherheitsansatzes ist, reicht ZTNA allein nicht aus, um Zero-Trust-Ziele zu erreichen. Es muss Teil eines integrierten Ansatzes sein.

In einem neuen Report von Absolute Software wird der Aufbau einer Grundlage für eine vollständige, integrierte Zero-Trust-Architektur erörtert. Wenn diese Puzzleteile für die Architektur richtig zusammengesetzt werden, können sie einen Großteil der Probleme lösen, die von Experten des 451 Research-Institutes genannt wurden.

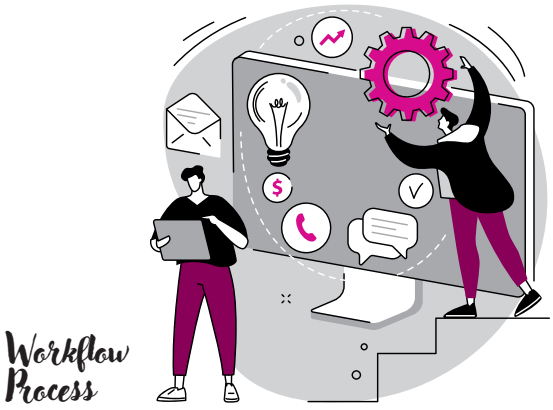
Anforderungen

Erik Hanselman, Principal Research Analyst, 451 Research, Teil von S&P Global Market Intelligence, schreibt in dem Bericht: Damit eine Zero-Trust-Umgebung wirklich belastbar ist, muss sie Endpunktsicherheit, sichere Zugriffsfunktionen, Netzwerktransparenz und -verwaltung in einem integrierten System zusammenführen. Viele Zero-Trust-Ansätze verknüpfen diese Elemente zwar, integrieren sie aber nicht wirklich. Eine integrierte Umgebung kann die Situationswahrnehmung verbessern, indem sie alle Aspekte der Geräte, ihrer Aktivitäten, des Netzwerkverkehrs und der Sichtbarkeit von Bedrohungen auf hoher Ebene zusammenführt. Zusammengenommen ist dies eine Kombination, die besser in der Lage ist, Angriffe abzuwehren und schneller eine Sanierung durchzuführen, wenn sie doch auftreten. Auf diese Weise können Unternehmen die Vorteile nutzen, die ein echtes, widerstandsfähiges Zero-Trust-System verspricht.

DIE TOP 10, DIE IT-SICHERHEITSVERANTWORTLICHEN KOPFSCHMERZEN BEREITEN.

Source: 451 Reserch's Voice of the Enterprise: Information Security, Workloads & Key Projects 2021

Was sind die drei größten Probleme Ihrer Organisation in Bezug auf die Informationssicherheit?



barkeit, Personalmanagement, Malware und Ransomware sowie Budget. Im Falle eines Angriffs wollen Unternehmen sicherstellen, dass Geräte, Systeme und Daten den Mitarbeitern so schnell wie möglich zur Verfügung gestellt werden.

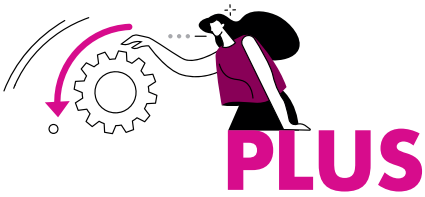
Wie in dem Bericht hervorgehoben wird, kann die Selbstheilung schneller erfolgen, wenn die Ausfallsicherheit in die Geräte eingebettet ist, so dass die Mitarbeiter schneller wieder produktiv arbeiten können.

Hanselman weist auch darauf hin, dass es zwar eine Vielzahl von Sicherheits- und Risikoproblemen gibt, mit denen Unternehmen zu kämpfen haben, dass aber Resilient Zero Trust viele der von Sicherheits- und Risikofachleuten am häufigsten angeführten Probleme lindert. Dazu gehören der Umgang mit Benutzerverhalten, Cloud-Sicherheit, Datenschutz, Phishing, Endpunktsicherheit, Fernzugriff, Sicht-

Definition und Umsetzung

Absolute Software ist ein Pionier, der nicht nur das Konzept des „Resilient Zero Trust" definiert, sondern auch die gesamte Palette der dafür erforderlichen Funktionen bereitgestellt hat. Es ist deutlich geworden, dass weit verteilte, hybride Arbeitsumgebungen auf Dauer Bestand haben werden. Daher suchen Unternehmen nach Sicherheitsansätzen, die Endpunkt- und Zugriffsbewertungen vollständig integrieren, um sicherzustellen, dass die Zero-Trust-Prinzipien bei jedem Schritt vollständig angewendet werden. Die Fähigkeit, Sichtbarkeit und Selbstheilung vom Endpunkt bis zum Netzwerkrand zu ermöglichen, bedeutet für die Unternehmen ein Mehr an Sicherheit.

Ulrich Parthier



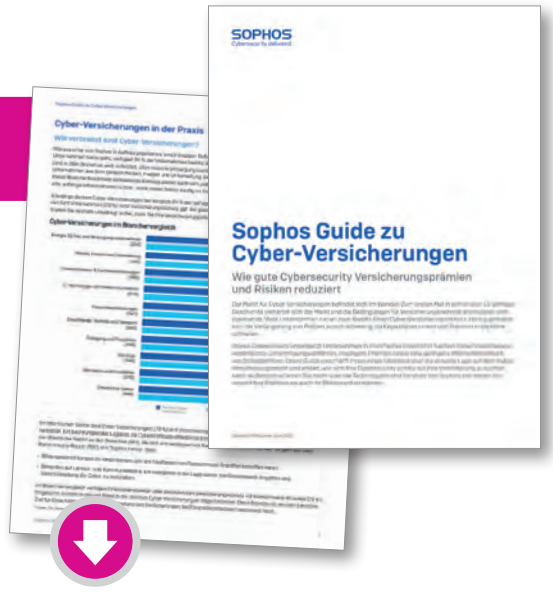
www.absolute.com/go/reports/451-research-resilient-zero-trust/

GUIDE ZU CYBER-VERSICHERUNGEN

WIE GUTE CYBERSECURITY VERSICHERUNGSPRÄMIEN UND RISIKEN REDUZIERT

Der Markt für Cyber-Versicherungen befindet sich im Wandel: Zum ersten Mal in seiner über 15-jährigen Geschichte verhärtet sich der Markt und die Bedingungen für Versicherungsnehmer erschweren sich zusehends. Viele Unternehmen haben zwar bereits einen Cyber-Versicherungsschutz. Häufig gestaltet sich die Verlängerung von Policen jedoch schwierig, da Kapazitäten sinken und Prämien in die Höhe schnellen.

Der Guide verschafft Ihnen einen Überblick über die aktuelle Lage auf dem Cyber-Versicherungsmarkt und erklärt, wie sich Ihre Cybersecurity positiv auf Ihre Versicherung auswirken kann. Außerdem erfahren Sie mehr über die Technologien und Services von Sophos, mit denen Sie sowohl Ihre Prämien als auch Ihr Risiko senken können.



WHITEPAPER DOWNLOAD

Das Whitepaper umfasst 10 Seiten und steht kostenlos zum Download bereit.
www.it-daily.net/Download

CASB, SSE, SASE

UND WAS KOMMT DANACH?

Die Verbreitung von SaaS in Unternehmen hat in den letzten Jahren rasante Ausmaße angenommen. Dieser Trend hat zwar die Produktivität der Benutzer und die Flexibilität des Unternehmens erheblich gesteigert, gleichzeitig aber auch neue Möglichkeiten für Datenschutzverletzungen und Gefährdungen eröffnet. Die Experten bei Palo Alto Networks haben sie näher mit den Ursachen beschäftigt.

Der „Schlüsselfertig"-Aspekt von Software-as-a-Service (SaaS) ist für Unternehmen verlockend, aber er kann letztlich trügerisch sein, wenn Sicherheitsrisiken eingeführt werden, die den Nutzern nicht bewusst sind.

Die Experten sehen daher im SaaS Security Posture Management (SSPM) eine zunehmend wichtige Entwicklung, um die Sicherheitsrisiken in SaaS-dominierten Umgebungen einzudämmen.

Ein großes Unternehmen verwendet in der Regel 100 oder mehr zugelassene SaaS-Anwendungen. Jede dieser Anwendungen verfügt über eigene Einstellungen, Funktionen, Versionen und Updates. Selbst wenn jede sanktionierte Anwendung zu einem bestimmten Zeitpunkt ordnungsgemäß konfiguriert ist, können Angreifer immer noch nach Sicherheitslücken suchen, die durch eine neue Funktion oder eine von einem Anwendungsadministrator vorgenommene Konfigurationsänderung entstehen.

Wenn dann noch eine neue SaaS-Anwendung ohne vorherige Genehmigung und Kontrolle zum bestehenden Portfolio sanktionierter Anwendungen hinzugefügt wird, müssen sich die Sicherheitsteams mit einer ganzen Reihe neuer blinder Flecken in der Sicherheit auseinandersetzen. Alles in allem ist jede SaaS-Anwendung – unabhängig vom Grad der Nutzung und des Schutzes – immer noch anfällig für Sicherheitslücken.

SaaS-Schwachstelle

Gartner hat vorausgesagt, dass mehr als 99 Prozent der Sicherheitsverletzungen in der Cloud auf vermeidbare Fehlkonfigurationen oder Fehler der Endbenutzer zurückzuführen sind. Heute werden SaaS-Fehlkonfigurationen schnell zu einer der Hauptursachen für Datenschutzverletzungen bei SaaS-Anwendungen. Zunächst gilt es zu klären, warum herkömmliche CASBs (Cloud Access Security Brokers) bei diesem Problem versagt haben.

Old School CASB

Herkömmliche CASBs sind so konzipiert, dass sie sensible Daten zunächst mit einer Data Loss Prevention (DLP)-Einheit schützen. Das Problem bei diesem „Schutz der Daten zuerst"-Ansatz ist,

dass der Großteil der SaaS-Angriffsfläche übersprungen wird – die Angriffsfläche, die die Sicherheit und Integrität der SaaS-Anwendung selbst darstellt. Sich auf den Schutz der Daten zu konzentrieren und dabei die Sicherheit der Anwendung selbst zu vernachlässigen, ist, als würde man auf einem rissigen Fundament bauen. Die Anwendung selbst sollte zuerst vor Schwachstellen geschützt werden, damit sie zuverlässig alle Sicherheitsgarantien, einschließlich der Datensicherheit, bieten kann.

Wenn eine SaaS-Anwendung aufgrund einer durch eine Fehlkonfiguration verursachten Schwachstelle beeinträchtigt wird, wirkt sich dies negativ auf die Gesamtsicherheit aus, so dass die Daten der Anwendung dem Risiko einer Verletzung ausgesetzt sind. Um dieses Problem zu lösen, hat sich das SaaS Security Posture Management (SSPM) schnell zu einem grundlegenden Instrument zum Schutz der Sicherheitslage von SaaS-Anwendungen entwickelt.

Was sind einige der wichtigsten SaaS-Herausforderungen, die SSPM für die SaaS-Sicherheit in Unternehmen so wichtigmachen?

Herausforderung: Die sichere Konfiguration von Tausenden von Einstellungen für Hunderte von genehmigten SaaS-Anwendungen ist keine leichte Aufgabe.

Sicherheitsteams haben bereits damit zu kämpfen, mit der ständig steigenden Nutzung von genehmigten SaaS-Anwendungen im Unternehmen Schritt zu halten. Dabei müssen sie auch sicherstellen, dass jede SaaS-Anwendung sicher konfiguriert ist. Um dies zu erreichen, müssen die Sicherheitsteams die Grundlagen verstehen. Erstens gibt es zu viele Anwendungen und jede Anwendung hat Dutzende bis Hunderte von Einstellungen, die sich auf die Sicherheit auswirken. Zweitens müssen alle Einstellungen jeder Anwendung verstanden und korrekt eingestellt werden, damit sie mit den Branchen- und Unternehmensrichtlinien übereinstimmen. Drittens müssen die Sicherheitsteams die Risiken verstehen, die selbst dann bestehen, wenn eine Einstellung versehentlich falsch konfiguriert wurde.

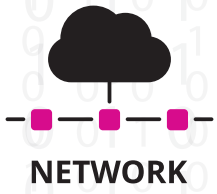
Eine beliebte Videokonferenz-App ist dafür ein gutes Beispiel. Die Anwendung scheint recht einfach zu sein, verfügt aber in Wirklichkeit über mehr als 50 Einstellungen, die sich auf die Sicherheit auswirken können – von Passwortanforderungen für Meetings bis hin zu Einstellungen für die Freigabe von Aufzeichnungen. All diese Einstellungen müssen von verschiedenen Abschnitten der Verwaltungskonsole aus verstanden werden und erstrecken sich über mehrere, verschiedene Dokumentationen.

Herausforderung: Die Behebung von Sicherheitsfehlkonfigurationen in SaaS ist schwierig – sie zu beheben ist noch schwieriger.

SaaS-Anwendungen werden in der Regel nicht nur von einem, sondern von vielen Beteiligten im gesamten Unternehmen genutzt und betrieben. Während sich diese Teams darauf konzentrieren, das Unternehmen zu unterstützen und die Zusammenarbeit zu verbessern, sind sich nicht alle von ihnen über die Sicherheitsauswirkungen der zahlreichen Einstellungen der Anwendung im Klaren, insbesondere, wenn Änderungen an der Anwendung ohne das Wissen der anderen vorgenommen werden. Darüber hinaus können die Beteiligten leicht neue SaaS einführen und zum De-facto-Eigentümer werden, obwohl sie möglicherweise nicht über das Fachwissen verfügen, um eine sichere Bereitstellung zu gewährleisten.

Letztendlich führt die mangelnde Koordination zwischen den Beteiligten aus verschiedenen Geschäftsbereichen, der IT, den Infosec- und GRC-Teams zu einer sogenannten Konfigurationsabweichung.

Das Ergebnis ist ein ineffizienter, zeitaufwändiger und langfristig nicht skalierbarer Sanierungsansatz, da immer mehr SaaS-Anwendungen für die Unternehmensnutzung zugelassen werden. Wenn Sicherheitsadministratoren keinen Einblick in die Änderungen an den Sicherheitseinstellungen einer SaaS-Anwendung haben, ist die Identi-



fizierung von Fehlkonfigurationen mit der Suche nach einer Nadel im Heuhaufen vergleichbar, und sie können die Sicherheit der Anwendung nicht gewährleisten. Sie müssen dann manuelle Anwendungsbewertungen durchführen, um nach der Möglichkeit einer Fehlkonfiguration zu suchen. Wie nicht anders zu erwarten, ist der Audit-Prozess langsam und mühsam und bietet nur punktuelle Einblicke, wenn Hunderte von sanktionierten Anwendungen betroffen sind.

Um ein Beispiel zu nennen: Wenn eine Person für eine Anwendungsbewertung eine Woche benötigt, würde es bei 200 Anwendungen 200 Wochen dauern, um eine vollständige Bewertung aller Anwendungen vorzunehmen. Selbst wenn vier Personen jeden Tag eine Anwendungsbewertung durchführen würden, würde dies ein ganzes Jahr dauern. Bis dieses Team alle Anwendungen durchgesehen hat, muss es diesen Zyklus noch einmal wiederholen, da diese Audits nur eine punktuelle Bewertung darstellen. Wenn sich etwas ändert, würde InfoSec das erst im nächsten Überprüfungszyklus herausfinden.

Es erübrigt sich zu sagen, dass es heute keine effiziente Lösung gibt, die den SaaS-Bewertungsprozess über mehrere Anwendungen hinweg automatisiert und gleichzeitig die Prüfung kontinuierlich überwacht.

Herausforderung: Die Sicherung von SaaS unterscheidet sich von der Sicherung herkömmlicher Software.

Das SaaS-Modell hat viele Vorteile gegenüber herkömmlicher Software, denn es bietet sofortige globale Verfügbarkeit und automatische Updates auf die neuesten und besten Funktionen. Doch genau diese Eigenschaften machen sie auch zu einer Herausforderung für die Sicherheit. Während herkömmliche Software im Rechenzentrum bereitgestellt wird, sind SaaS-Anwendungen direkt über das Internet zugänglich, was die Gefahr von Fehlkonfigurationen deutlich erhöht.

Es gibt ein gutes Beispiel, bei dem eine beliebte Anwendung zur Problemverfolgung den Benutzern die Option bot, ihre Dashboards mit „allen" zu teilen, was fälschlicherweise als „alle im Unternehmen" interpretiert wurde, während es in Wirklichkeit „alle im Internet" waren.

Upgrades für herkömmliche Software werden direkt vom IT-Team überwacht und durchgeführt. SaaS-Anwendungen hingegen aktualisieren sich dynamisch selbst, um neue Funktionen und Merkmale hinzuzufügen. Die häufigen Aktualisierungen verbessern die Funktionalität der Anwendung, beeinträchtigen aber auch ihre Sicherheit. Wenn eine SaaS-Anwendung angepasst wird, bieten ihre Einstellungen außerdem nicht mehr das erforderliche Sicherheitsni-

veau, was zu Konflikten mit den Compliance- und Sicherheitsrichtlinien des Unternehmens führt. Und es ist nicht nur so, dass Anpassungen zu Sicherheitslücken führen – oft sind auch die Standardeinstellungen nicht gut genug. IT-Teams in Unternehmen sollten sich an die Kerndevise von „Zero Trust" halten und niemals davon ausgehen, dass die SaaS-Anwendung standardmäßig sicher ist.

SSPM-Ansatz als nächste Stufe

Bei zeitgemäßem SSPM geht es darum, über die Einhaltung von Vorschriften hinauszugehen und alle Einstellungen zu untersuchen, die sich auf die Sicherheitslage der Anwendung auswirken. Dieser Sicherheitsansatz bietet einen vollständigen Überblick über alle Einstellungen, die sich auf die Sicherheit der Anwendung auswirken, ermöglicht eine Behebung mit nur einem Klick und verhindert das Abdriften. Darüber hinaus sollte sich SSPM nicht auf eine Handvoll Anwendungen beschränken, denn alle können ein Risiko für das Unternehmen darstellen.

Next level IT Security

Aber aufgepasst: CASB ist nur ein Teilaspekt innerhalb der IT-Security-Strategie. CASB steht auch nicht im Gegensatz zu SASE (Secure Access Service Edge), sondern ist ein Teil einer SASE-Architektur.

Gartner prägte den Begriff erstmals im Juli 2019. Näher ausgeführt haben die Analysten ihn dann in ihrem „The Future of Network Security is in the Cloud" betitelten Bericht. Seitdem wird SASE als die nächste Transformation für Unternehmensnetzwerke und deren Sicher-

FRAMEWORK

ACCESS

heit bezeichnet. Die Architektur verspricht, bestehende Technologien besser nutzen zu können. Dazu werden Netzwerk- und Sicherheitsbereiche in einem einzigen, globalen Cloud-Dienst zusammengeführt.

SASE kombiniert SD-WAN, Secure Web Gateway, Zero Trust Network Access, Firewall as a Service und Cloud Access Security Broker (CASB). Das SD-WAN sorgt dafür, dass Daten aufvdem schnellsten Weg ans richtige Ziel kommen. Greift der Endpunkt auf Cloud Services zu, schützt das Secure Web Gateway vor Gefahren aus dem Internet. Dafür setzt es zum Beispiel URL- und Web-Traffic-Filter, Anwendungskontrollen und Anti-Malware-Funktionen ein.

Firewall as a Service kontrolliert den Traffic, der nicht Web-basiert ist, während Zero Trust Network Access es ermöglicht, granulare Zugangskontrollen umzusetzen. Über einen sicheren, verschlüsselten Tunnel erhalten Nutzer nur Zugriff auf Anwendungen, wenn sie berechtigt sind. Mit dem CASB können Unternehmen zudem Schatten-IT vermeiden und sicherstellen, dass Anwender nur freigegebene Cloud Services nutzen.

Eine SASE-Plattform enthält nicht immer alle der genannten Komponenten – das muss sie auch nicht, da sich die einzelnen Services teilweise im Funktionsumfang überschneiden.Jeder Anbieter hat außerdem seine Stärken, je nachdem was sein Kerngebiet ist. Einige Hersteller sind zum Beispiel im Secure Web Gateway führend. Palo Alto Networks etwa punktet vor allem mit starken Next Generation Firewall- und ZTNA-Funktionen und bietet eine sehr gute SD-WAN-Komponente.

Natürlich gibt es am Markt zahlreiche Anbieter im Markt wie etwa Forcepoint, Zscaler, Akamai, Cisco, Cato Networks, Netskope, Versa oder Sast Solutions/Pathlock.

Ein Schmanckerl bietet Netskope mit einem kostenloses SASE-Assessment an, das in nur fünf Minuten abgeschlossen ist – mehr erfahren Sie unter www.netskope.com/sase-assessment.

Fazit

Zusammen bilden CASB (Cloud Access Security Broker), DLP (Data Loss Prevention), SWG (Secure Web Gateway) und ZTNA (Zero Trust Network Access) eine Einheit. Das verbindende Element sind das A wie Access und das Z wie Zero Trust-Gedanke, manchmal auch als perimeterlose Sicherheit bezeichnet. Es besagt, vertraue niemandem ungeprüft zu keiner Zeit. Entscheidend ist, dass niemand einen Vertrauensvorschuss für einen Zugriff erhält. Aufgrund von Kriterien wird das Vertrauen „erarbeitet“ und in einem Zero Trust-Modell mit der Anwenderidentität verknüpft, um Zugriff zu gewähren. Applikationen können sich somit überall befinden, ob im Internet, in der Private Cloud und oder im Rechenzentrum. Für private Applikationen wendet man zusätzlich das Prinzip des „Least Privilege‘“ an, also Zugriff auf Basis granularer Regeln und Rollen.

Und noch etwas: Die Konzentration dieser Aspekte auf einen Anbieter bietet eher Vorteile wie etwa ein effizientes Traffic Routing, weniger Ausschlüsse, ein verbessertes Monitoring und Troubleshooting. Dadurch wird auch die Erstellung von Sicherheitsrichtlinien vereinfacht sowie validere Metriken für Security-Management, Auditing, Governance und ein mehr an Transparenz erreicht.

Dem hat auch die Gartner Group Rechnung getragen und einen neuen Quadranten erschaffen. Er heißt Security Service Edge (SSE) und fasst alle Sicherheitskomponenten unter einem Dach zusammen. Gleichzeitig schließt er die netzwerkbezogenen Komponenten wie etwa SD-WAN, aus. Beide zusammen ergeben dann das SASE-Modell.

Ulrich Parthier

ABWEHR AKTIVIEREN

DATENSICHERHEIT IN HYBRIDEN ARBEITSUMGEBUNGEN

In unserer digitalen Welt müssen Unternehmen sich vor Cyberangriffen und dem Verlust wertvoller Daten schützen. Die Arbeit von CISOs ist anspruchsvoller denn je. Die Daten stehen als wertvolles Gut im Mittelpunkt. Das neue Normal im Zeitalter der Daten stellt Unternehmen vor die Frage, wie sie sensible Daten über den gesamten Lebenszyklus sowohl innerhalb als auch außerhalb des eigenen Firmennetzwerks im mehrdimensionalen Datenraum schützen. Unternehmen benötigen eine IT-Sicherheitslösung, die für die heutige Arbeit mit Daten geeignet ist. Eine IT-Sicherheitsplattform, die konsistent alle sensiblen Daten erkennt und schützt, unabhängig davon, wo sich diese befinden oder wie sie sich bewegen. Prävention ist immer besser als Intervention.

In diesem Whitepaper möchten wir Ihnen zeigen, welche Herausforderungen es heute für den Schutz der Daten gibt und wie ineinander verzahnte Sicherheitskontrollen entlang der Kill Chain ansetzen, um Datenverlust bereits im Vorfeld zu verhindern. Wir stellen Ihnen acht wichtige Schritte vor, die zu effektiverer Sicherheit in Ihrem Unternehmen führen.

www.it-daily.ner/download

WHITEPAPER DOWNLOAD

Das Whitepaper umfasst 10 Seiten und steht kostenlos zum Download bereit.
www.it-daily.net/Download

IMPRESSUM

Geschäftsführer und Herausgeber:
Ulrich Parthier (08104-6494-14)

Chefredaktion:
Silvia Parthier (-26)

Redaktion:
Carina Mitzschke (nur per Mail erreichbar)

Redaktionsassistenz und Sonderdrucke:
Eva Neff (-15)

Autoren:
Christian Bücker, Andrew Howard, Till Jäger, Stijn Jans, Udo H. Kalinna, Sean Leach, Carina Mitzschke, Silvia Parthier, Ulrich Parthier, Audra Simons, Oliver Spielmann, Zac Warren

Anschrift von Verlag und Redaktion:
IT Verlag für Informationstechnik GmbH
Ludwig-Ganghofer-Str. 51, D-83624 Otterfing
Tel: 08104-6494-0, Fax: 08104-6494-22
E-Mail für Leserbriefe: info@it-verlag.de
Homepage: www.it-daily.net

Alle Autoren erreichen Sie über die Redaktion.Wir reichen Ihre Anfragen gerne an die Autoren weiter.

Manuskripteinsendungen:
Für eingesandte Manuskripte wird keine Haftung übernommen. Sie müssen frei sein von Rechten Dritter. Mit der Einsendung erteilt der Verfasser die Genehmigung zum kostenlosen weiteren Abdruck in allen Publikationen des Verlages. Für die mit Namen oder Signatur des Verfassers gekennzeichneten Beiträge haftet der Verlag nicht. Die in dieser Zeitschrift veröffentlichten Beiträge sind urheberrechtlich geschützt. Übersetzung, Nachdruck, Vervielfältigung sowie Speicherung in Datenverarbeitungsanlagen nur mit schriftlicher Genehmigung des Verlages. Für Fehler im Text, in Schaltbildern, Skizzen, Listings und dergleichen, die zum Nichtfunktionieren oder eventuell zur Beschädigung von Bauelementen oder Programmteilen führen, übernimmt der Verlag keine Haftung. Sämtliche Veröffentlichungen erfolgen ohne Berücksichtigung eines eventuellen Patentschutzes. Ferner werden Warennamen ohne Gewährleistung in freier Verwendung benutzt.

Layout und Umsetzung: K.design | www.kalischdesign.de
mit Unterstützung durch www.schoengraphic.de

Illustrationen und Fotos:
Wenn nicht anders angegeben: shutterstock.com

Anzeigenpreise:
Es gilt die Anzeigenpreisliste Nr. 30.
Preisliste gültig ab 1. Oktober 2022.

Mediaberatung & Content Marketing-Lösungen it management | it security | it daily.net:
Kerstin Fraenzke, 08104-6494-19,
E-Mail: fraenzke@it-verlag.de
Karen Reetz-Resch, Home Office: 08121-9775-94,
E-Mail: reetz@it-verlag.de

Online Campaign Manager:
Roxana Grabenhofer, 08104-6494-21,
grabenhofer@it-verlag.de
Marena Avila (nur per Mail erreichbar),
avila@it-verlag.de

Objektleitung:
Ulrich Parthier (-14),
ISSN-Nummer: 0945-9650

Erscheinungsweise: 6 x pro Jahr

Verkaufspreis: Einzelheft 20 Euro
Jahresabopreis 100 Euro (Inland), 110 Euro (Ausland)
Probeabo 20 Euro für 2 Ausgaben
PDF-Abo 40 Euro für 6 Ausgaben

Bankverbindung:
VRB München Land eG,
IBAN: DE90 7016 6486 0002 5237 52, BIC: GENODEF10HC

Beteiligungsverhältnisse nach § 8, Absatz 3 des Gesetzes über die Presse vom 8.10.1949: 100 % des Gesellschafterkapitals hält Ulrich Parthier, Sauerlach.

Abonnementservice:
Eva Neff,
Telefon: 08104-6494 -15,
E-Mail: neff@it-verlag.de

Das Abonnement ist beim Verlag mit einer dreimonatigen Kündigungsfrist zum Ende des Bezugszeitraumes kündbar. Sollte die Zeitschrift aus Gründen, die nicht vom Verlag zu vertreten sind, nicht geliefert werden können, besteht kein Anspruch auf Nachlieferung oder Erstattung vorausbezahlter Beträge.

Unternehmen leben länger mit

IT-Security Schutzmaßnahmen

SCAN ME

Mehr Infos dazu im Printmagazin

itsecurity

und online auf **www.it-daily.net**