it management

Der Motor für Innovation
Juli/August 2023

INKLUSIVE 48 SEITEN
it security

LOGICALIS
Allheilmittel Private 5G?
ab Seite 22

kobaltblau
Digitale Transformation 2.0
ab Seite 34

RECHENZENTREN

High Performance Computing

Rainer Stiller, Vertiv

THOUGHT LEADERSHIP
AB SEITE 14
BLACKLINE

DATENSTRATEGIE

Integration, Migration, Modernisierung

MODERNE CMS

Mit Headless nie wieder Updates!

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 Zu-sammenarbeit mit der Standard.at/Karriere, dem Jobportal der Tageszeitung Der Standard, findet man auf dieser Plattform perma-nent hunderte offene Stellen aus dem Bereich IT und Telekom. Eine aktive Jobsuche nach Tätigkeits-feld und Ort ist natürlich möglich.

itwelt.at/jobs

TRANSFORMATION AUF KNOPFDRUCK?

LIEBE LESERINNEN UND LESER,

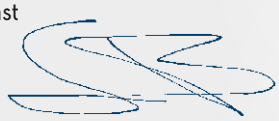
Die digitale Transformation hat sich längst von einer Buzzword-Phrase zu einer grundlegenden Notwendigkeit für Unternehmen entwickelt. Durch den Einsatz der richtigen Tools und Infrastruktur können Unternehmen Prozesse automatisieren und Kosten sparen.

So einfach ist die Theorie. Die Realität ist natürlich komplexer, denn die digitale Transformation ist nicht einfach ein Schalter, den man mit der richtigen Menge an Investitionen umlegt. Es gibt Wege, sie richtig zu machen, und Wege, sie falsch zu machen.

Wer in eine digitale Infrastruktur investiert, aber nicht weiß, wie man die vielen Möglichkeiten, die sie bietet, am besten nutzt, der hat nicht transformiert. Passend hierzu sagte George Westerman, Dozent an der Sloan School of Management des MIT : „Wenn die digitale Transformation richtig gemacht wird, ist sie wie eine Raupe, die sich in einen Schmetterling verwandelt, aber wenn sie falsch gemacht wird, ist alles, was man hat, eine sehr schnelle Raupe." In dieser Aussage steckt viel Wahrheit. Zumal es keine Einheitsgröße für alle Unternehmen gibt. Jedes Unternehmen hat seine ganz eigenen Anforderungen, Herausforderungen und Wünsche. Umso wichtiger ist es, sich rechtzeitig mit potenziellen Fallstricken auseinanderzusetzen. Schließlich kann die Umsetzung unter Umständen auch Betriebsunterbrechungen mit sich bringen – beispielsweise bei der Datenmigration.

Digitale Transformation bedeutet also mitnichten nur die bloße Einführung neuer Technologien, sondern vor allem eine Veränderung der Denkweise und Unternehmenskultur. Einen Schalter gibt es dann vielleicht doch, er wird nur ganz woanders umgelegt.

Herzlichst



Lars Becker, Redakteur

INHALT

Inklusive 48 Seiten it security

GUT ZU WISSEN

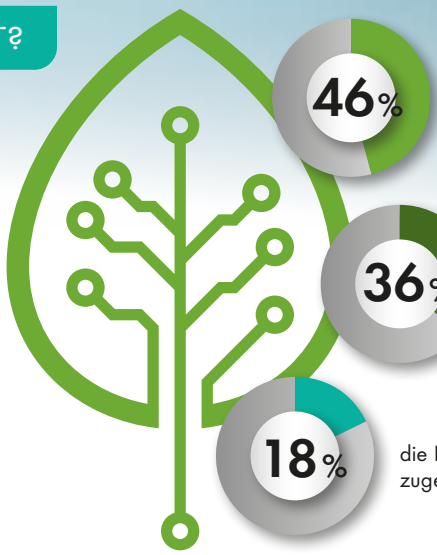
Achten Sie auf dieses Icon und lesen sie mehr zum Thema im Internet auf **www.it-daily.net**

TWIN TRANSITION

SIND DEUTSCHE UNTERNEHMEN BEREIT?

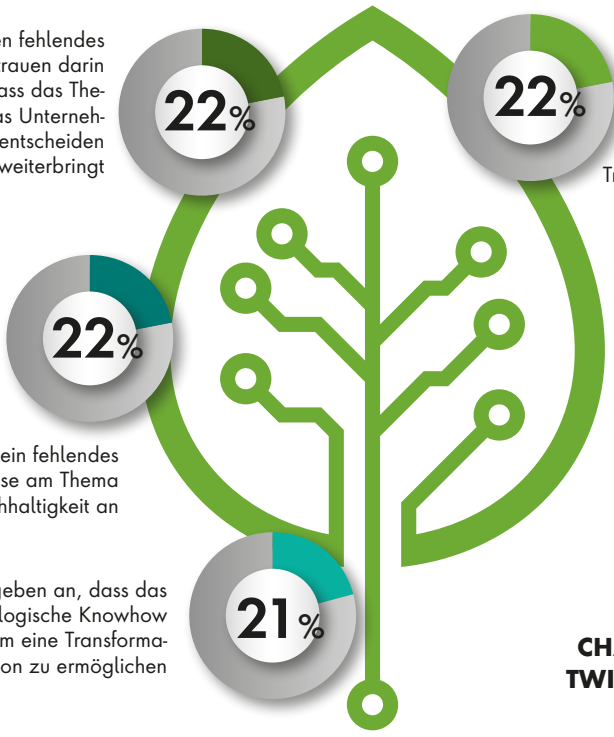
Die Twin Transition integriert Nachhaltigkeit in digitale Transformationsstrategien und ermöglicht es Unternehmen, effizienter und gleichzeitig nachhaltiger zu arbeiten.
www.futurice.com

WIE SEHR WIRD DAS THEMA NACHHALTIGKEIT VORANGETRIEBEN?



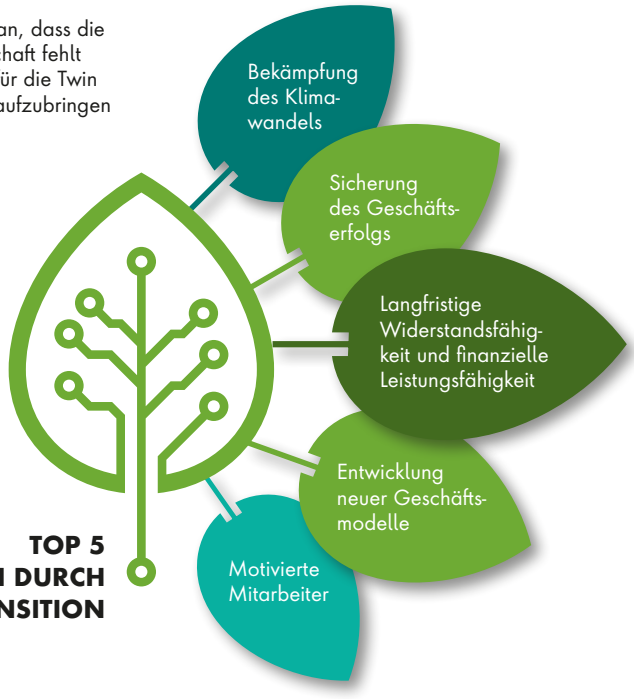
- **46%** das Investitionsvolumen ist über die letzten Jahre gleich geblieben
- **36%** die Investitionen sind zurück gegangen
- **18%** die Investitionen haben zugenommen

TWIN TRANSITION FORDERT ENTSCHLOSSENES HANDELN AUF FÜHRUNGSEBENE – DOCH WELCHE DEFIZITE GIBT ES AUF DEREN SEITE AKTUELL NOCH?



- **22%** geben fehlendes Vertrauen darin an, dass das Thema das Unternehmen entscheiden weiterbringt
- **22%** geben an, dass die Bereitschaft fehlt Budget für die Twin Transition aufzubringen
- **22%** geben ein fehlendes Interesse am Thema Nachhaltigkeit an
- **21%** geben an, dass das technologische Knowhow fehlt, um eine Transformation zu ermöglichen

TOP 5 CHANCEN DURCH TWIN TRANSITION



Schlüssel zum Erfolg

PLATFORM ENGINEERING AUF DEM VORMARSCH

Puppet by Perforce gab die Ergebnisse des globalen „State of DevOps Report: Platform Engineering Edition" bekannt. Die diesjährige Studie untersucht die steigende Popularität von Platform Engineering und dessen Vorteile. 93 Prozent der Befragten gaben an, dass der Umstieg auf Platform Teams ein Schritt in die richtige Richtung ist.

Der letztjährige State-of-DevOps-Report hat gezeigt, dass das DevOps-Konzept mit dem Ansatz über Platform Teams erfolgreicher wird. Der diesjährige Bericht befasst sich eingehender mit dem Thema und zeigt, dass eine überwältigende Mehrheit (94 %) glaubt, dass dieses Konzept ihren Unternehmen hilft, die Vorteile von DevOps besser zu verwirklichen. Platform Engineering bezeichnet das Entwerfen und Erstellen von Self-Service-Funktionen, um die kognitive Belastung der Entwickler zu minimieren und eine schnelle Softwarebereitstellung zu ermöglichen. Platform Teams stellen gemeinsam genutzte Infrastruktur-Plattformen für interne Benutzer bereit, die für die Lieferung eines Wertstroms verantwortlich sind – in der Regel Softwareentwickler und Techniker, die ihre Plattform als ein Produkt für ihre Benutzer und nicht nur als IT-Projekt betrachten.

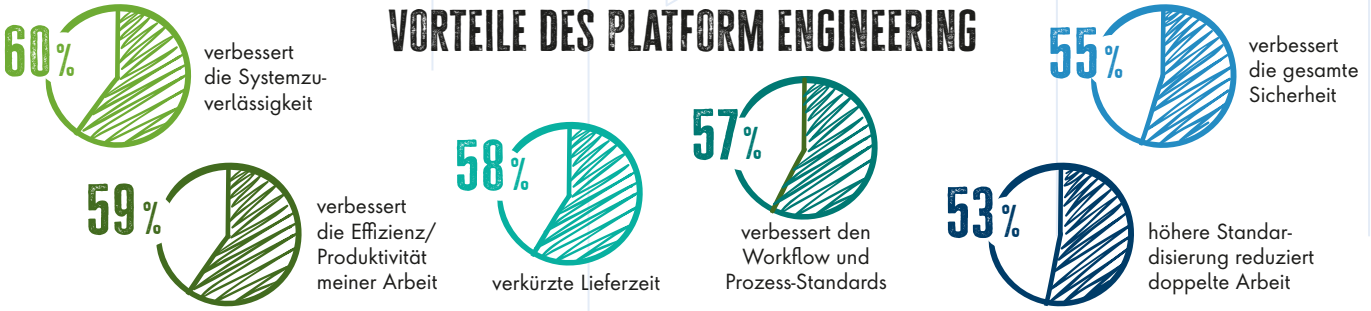
MEHR WERT State of DevOps Report: **https://bit.ly/3J1QokN**

Vorteile nutzen, Erfolge sichern

Die Ergebnisse zeigen, dass Platform Engineering über die gesamte Organisation hinweg zu bedeutenden Vorteilen führen und den DevOps-Erfolg für das Unternehmen sichern kann. Die Unternehmensführung muss jedoch kontinuierlich in das Platform Team investieren, funktionale Feedbackschleifen mit den Anwendern sicherstellen und die Produktmanagementfähigkeiten im Team weiterentwickeln, um Abläufe schneller bereitzustellen und die kognitive Belastung für die Entwickler zu senken", so Nigel Kersten, CTO von Puppet und Mitverfasser des State-of-DevOps-Report. „Wenn Unternehmen verstärkt Platform Teams einstellen, müssen sie den Schwerpunkt auf Produktmanagementfähigkeiten legen, nicht nur auf das Core Engineering."

www.puppet.com

VORTEILE DES PLATFORM ENGINEERING



DIGITALE TRANSFORMATION AUSGEBREMST?

KLUFT ZWISCHEN BUSINESS- UND IT-FÜHRUNGSKRÄFTEN

Die digitale Transformation wirkt sich weiterhin auf alle Aspekte des Geschäftslebens aus – doch allzu oft stehen sich die Führungskräfte in Wirtschaftsunternehmen und ihre IT-Fachleute gegenseitig im Weg. Denn die Transformation erfordert mehr als nur die Einführung moderner Technologien. EPAM Continuum hat einen neuen Bericht mit dem Titel „Three Ways Leaders Impede Their Company's Digital Transformation" veröffentlicht, der eine Trennung zwischen „Business" und Technologie in vielen Unternehmen aufzeigt und gleichzeitig Schlüsselstrategien für eine erfolgreiche digitale Transformation beschreibt.

„Um die digitale Transformation erfolgreich zu bewältigen, müssen Geschäftsleitung und IT aufeinander abgestimmt sein; unsere Studie zeigt jedoch, dass dies in vielen Unternehmen nicht der Fall ist", sagt Dr. Sandra Loughlin, Chief Learning Scientist und Head of Client Learning and Talent Enablement bei EPAM.

Um herauszufinden, wie es um die digitale Transformation in den verschiedenen Branchen weltweit bestellt ist, wurden im Rahmen der Studie mehr als 900 Führungskräfte aus den Bereichen Technologie, Digitalisierung, Data, Produkt, Personalwesen, Talentgewinnung sowie Lernen und Entwicklung befragt.

Zu den wichtigsten Ergebnissen gehört:

- Nur 37 Prozent der Führungskräfte in der Technologiebranche und 10 Prozent der Führungskräfte in der Wirtschaft sind über wichtige Themen der digitalen Transformation ausreichend informiert, darunter KI, maschinelles Lernen und Cloud-Migration.
- 79 Prozent der befragten Führungskräfte stimmen der Aussage zu, dass das „Business" nicht mit der Technologie spricht und die Technologie nicht mit dem Business.
- Mehr als die Hälfte der Geschäftsinhaber und C-Level-Führungskräfte sehen die IT lediglich als allgemeine Unterstützungsfunktion und nicht als Treiber des Geschäfts.

www.epam.com

WIE MAN BRÜCKEN BAUT

Um Unternehmen dabei zu helfen, die Kluft zwischen Technologie und Geschäft zu überbrücken, bietet der Bericht detaillierte Vorschläge und Ressourcen zur Verbesserung der laufenden digitalen Transformation:

- **Klärung der Rolle der Technologie im Unternehmen:** Dazu gehört die Entwicklung einer gemeinsamen Vision und eines strategischen Plans, der darlegt, wie die Technologie die Geschäftsstrategie unterstützt.
- **Schaffung obligatorischer Programme für digitale und unternehmerische Kompetenz:** Für Führungskräfte sollten die Kurse speziell auf ihre Bedürfnisse zugeschnitten sein und erörtern, wie sie ihren Mitarbeitern helfen können, neue Denk-, Verhaltens- und Arbeitsweisen zu entwickeln.
- **Verknüpfung von Lernen und Umsetzung:** Gemeinsame Ziele und eine gemeinsame Verantwortlichkeit für die digitale Transformation müssen für jeden Bereich des Unternehmens gelten, die Abläufe müssen aufeinander abgestimmt werden.

Anywhere Worker

FLEXIBEL UND UNABHÄNGIG ARBEITEN

Fiverr International hat seine zweite Anywhere Worker-Studie veröffentlicht, die aktuelle Trends von digitalen Nomaden gibt. Weltweit wurden 2.000 Anywhere Worker befragt, das heißt Menschen, die von mindestens zwei Standorten im In- oder Ausland aus arbeiten und dabei das ganze Jahr über unterwegs sind. Die Daten zeigen, dass sie immer häufiger und für längere Zeiträume reisen wollen.

Die globale Arbeitswelt entwickelt sich weiter und Fernarbeit gewinnt zunehmend an Bedeutung. Sie bleibt eine äußerst wertvolle Option, durch die Anywhere Worker das Arbeiten und Reisen nahtlos miteinander verbinden können. Die Gründe für diesen Lebensstil sind individuell und vielfältig. Sie reichen von der Sehnsucht nach mehr Flexibilität, Aufregung und Abenteuer über den Überdruss an dem typischen 9-5-Job bis hin zu dem Wunsch nach persönlicher Veränderung im Leben – oft inspiriert durch die Erfahrungen anderer Anywhere Worker. Die meisten von ihnen gehören zur Altersgruppe der Millennials, die bereits über ein gewisses Maß an Berufserfahrung verfügen und Vollzeit remote, flexibel arbeiten.

www.fiverr.de

80 %

der Anywhere Worker planen, diesen Lebensstil noch bis zu 5 Jahre lang nachzugehen

83 %

reisen alle sechs Monate mindestens einmal von einem Ort zum anderen weiter (Steigerung von 10 % innerhalb eines Jahres)

High Performance Computing in Rechenzentren

EINE FLEXIBLE UND ZUKUNFTSSICHERE KRITISCHE INFRASTRUKTUR IST DAS A UND O

Nicht nur die Pandemie hatte in den letzten Jahren massive Auswirkungen auf Rechenzentren. Durch die Zunahme generativer künstlicher Intelligenz (KI) und anderer datenintensiver Anwendungen ist der Bedarf an High-Performance-Computing (HPC)-Umgebungen drastisch gestiegen. Dies führt zu neuen Ansätzen bei der Konzeption, Erweiterung und Verwaltung von Rechenzentren. Gleichzeitig müssen Kapazitäten ausgebaut und Maßnahmen zur Reduzierung der Umweltbelastung implementiert werden. Rainer Stiller, CMO bei Vertiv, erläutert im Gespräch mit Ulrich Parthier, Publisher it management, wie sein Unternehmen Kunden bei der Anpassung an diese Veränderungen unterstützt und wie er Vertiv für die Zukunft positionieren will.

Ulrich Parthier: *Vertiv bietet Produkte für kritische digitale Infrastrukturen und Kontinuitätslösungen. Wie hat sich das Geschäft in den letzten Jahren verändert und was sind die Schlussfolgerungen daraus?*

Rainer Stiller: Die Pandemie zwang alle Unternehmen dazu, ihre Geschäftsabläufe zu modernisieren. Dadurch stiegen die Anforderungen an die Kapazität und die Infrastruktur von Rechenzentren weiter an. Zusätzlich nutzen oder planen immer mehr Betreiber hochdichte Rechenzentren, um datenintensive Anwendungen wie Cloud Computing, KI, HPC und Machine Learning zu unterstützen. Dieser Trend hat in den letzten zwei Jahren noch einmal erheblich an Dynamik gewonnen und erhöht den Bedarf an innovativen, energieeffizienten Lösungen für eine schnelle Bereitstellung von High-Density-Computing.

Ulrich Parthier: *Der Markt für kritische digitale Infrastrukturen ist hart umkämpft. Wie hebt sich Vertiv vom Wettbewerb ab?*

Rainer Stiller: Vertiv bietet ein Portfolio, das gleichermaßen auf umfassender Fachkompetenz wie einer ausgeprägten Innovationskultur beruht. Unser Schwerpunkt liegt dabei auf der Entwicklung hochverfügbarer Lösungen, die energie- und wassersparend sind. Wir helfen unseren Kunden bei der Bewältigung ihrer drängendsten Herausforderungen und unterstützen ihre Nachhaltigkeitsinitiativen durch unser Angebot an Energiemanagement, Wärmemanagement, Racks, IT-Management-Systemen, Services und integrierten Lösungen.

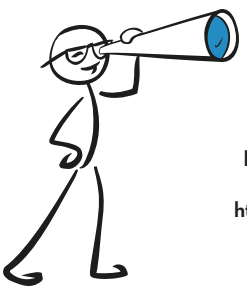
Ulrich Parthier: *Kritische digitale Infrastrukturen sind in letzter Zeit auch zunehmend in die Diskussion geraten – Stichwort Nachhaltigkeit. Wie tragen die Lösungen von Vertiv dazu bei, dass ein Rechenzentrum energie- und wassersparender wird?*

Rainer Stiller: Effizienzsteigerung und geringere Umweltbelastung sind für viele Entscheider zu Schlüsselfaktoren geworden – angetrieben durch gesetzliche Vorgaben sowie die Anforderungen von Kunden und anderen Stakeholdern. Von hocheffizienten USV-Systemen bis hin zu wassersparenden und GWP-armen Thermal-Management-Systemen bieten wir Lösungen an, die diese Ziele unterstützen. Besonders interessant sind Lösungen, mit denen die Kunden ihre Nutzung alternativer Energien steigern können. Dazu gehören Solarwandler, die solarbetriebene Telekommunikationsstandorte ermöglichen, und Lithium-Ionen-Batterien, die Energie aus alternativen Quellen speichern.

Wir informieren unsere Kunden zudem stetig darüber, wie sie ihren CO_2-Fußabdruck verringern können, beispielsweise mit dem Data Center Guide to Sustainability, der ihnen hilft, Umweltziele zu erreichen. Unser jährlicher ESG-Bericht von Vertiv enthält zudem Highlights der effizienten Lösungen von Vertiv.

Ulrich Parthier: *Wie sorgt Ihr Unternehmen dafür, dass Technologietrends wie E-Commerce, Streaming, Remote-Arbeit, KI und Machine Learning für seine Kunden optimal funktionieren?*

Rainer Stiller: Für all diese Anwendungen ist Kontinuität essenziell. Wir bieten die Infrastruktur, mit der unsere Kunden diese Dienste zuverlässig bereitstellen und ihren Betrieb skalieren können. Wir verfügen dabei nicht nur über ein globales Team von erfahrenen Ingenieuren, sondern arbeiten auch mit Innovationsführern der Branche und zukunftsorientierten Kunden zusammen. So können wir Lösungen entwickeln, die IT-Herausforderungen wie hohe Dichte, schnelles Wachstum und ökologische Ziele bewältigen.



PLUS

Data Center Guide zu Sustainability
https://bit.ly/3qrRhMY
ESG-Bericht
https://bit.ly/3WVegwe

> WIR HELFEN UNSEREN KUNDEN BEI DER BEWÄLTIGUNG IHRER DRÄNGENDSTEN HERAUSFORDERUNGEN UND UNTERSTÜTZEN IHRE NACHHALTIGKEITSINITIATIVEN
>
> **Rainer Stiller, CMO, Vertiv, www.vertiv.com**

Angesichts der Herausforderungen unserer Kunden erweist sich dieser Fokus als besonders wertvoll. Denn unser Portfolio umfasst eine Vielzahl von Lösungen. Dazu zählen Thermalmanagement-Lösungen für einen effizienten Betrieb von Server-Racks mit hoher Dichte, vorgefertigte modulare Lösungen, die Kapazitätserweiterungen innerhalb kürzester Zeit erlauben, sowie unterbrechungsfreie Stromversorgungen (USV), mit denen Kunden alternative Energiequellen bei zuverlässiger kontinuierlicher Stromversorgung nutzen können.

Ulrich Parthier: *Wie sehen einige praktische Anwendungen von KI, ML, VR und AR aus?*

Rainer Stiller: Sowohl Virtual als auch Augmented Reality werden bereits in vielen Branchen eingesetzt, um Abläufe zu optimieren und das Kundenerlebnis zu verbessern – vor allem im Verbraucher- oder Einzelhandelsbereich.

Im E-Commerce können Sie zum Beispiel virtuell Kleidung anprobieren oder ein Sofa digital in Ihrer Wohnung aufstellen. Die Kombination aus VR und AR – die Extended Reality (XR) – hat eine noch immersivere Qualität. Damit lassen sich virtuelle Umgebungen interaktiv nutzen. So können Sie beispielsweise einen Kühlschrank digital in Ihrer Küche aufstellen, die Türen öffnen und herausfinden, wie er funktioniert.

Ulrich Parthier: *Hat Vertiv KI-, ML-, VR- und AR-Anwendungen eingeführt?*

Rainer Stiller: Wir nutzen in mehreren Fabriken digitale Zwillinge, eine Form der KI, um Effizienz und Qualität zu verbessern und Kosten zu senken. Einige unserer Servicetechniker verwenden auch AR-Smart-Brillen, um Probleme virtuell zu erkennen und klare Anweisungen zu Prozessen erhalten können.

Darüber hinaus bietet unsere XR-App, das erste Tool seiner Art, ein spannendes Kundenerlebnis. Durch Augmented Reality erhalten die Nutzer der App eine realistische Darstellung des gewünschten Vertiv-Produkts am Ort ihrer Wahl – beispielsweise im Rechenzentrum oder in der Fabrikhalle. So geben wir unseren Kunden die Möglichkeit, sich die Geräte vor dem Kauf in der Einsatzumgebung anzusehen und so eine fundierte Entscheidung zu treffen. Mit der App können mehr Kunden ganz einfach virtuell mit unseren Lösungen interagieren, Türen öffnen und die Geräte so lange erkunden, wie sie wollen und wann sie wollen.

Ulrich Parthier: *Was hat Vertiv für die Zukunft geplant?*

Rainer Stiller: Die Märkte, die wir bedienen, entwickeln sich ständig weiter. Daher werden wir uns ebenfalls auf die Weiterentwicklung unserer Lösungen konzentrieren, um ihre Effizienz, Zuverlässigkeit, Intelligenz, Flexibilität und Einsatzgeschwindigkeit zu verbessern. Hierbei möchten wir unseren Kunden die bestmögliche Erfahrung bieten.

Außerdem ist es unser Ziel, in allen Bereichen unsere Umwelteinflüsse zu verringern. Dies wird in unserem kürzlich veröffentlichten ESG-Bericht ebenso ausführlich beschrieben, wie die Maßnahmen, die wir ergreifen, um Talente zur Unterstützung unserer Innovationsinitiativen und zur Aufrechterhaltung einer starken Kultur zu entwickeln. Darüber hinaus sind wir durch Partnerschaften und über unsere Kunden direkt an einer Reihe von zukunftsweisenden Projekten beteiligt. Beispielsweise arbeiten wir mit dem schwedischen RISE-Forschungsinstitut zusammen, um die Branche in eine neue Ära nachhaltiger Rechenzentren und Edge-Anwendungen zu führen. Wir beteiligen uns auch am EcoEdge Prime Power Project, das sich auf die Entwicklung umweltfreundlicher Brennstoffzellen für Rechenzentren konzentriert. Außerdem arbeiten wir mit führenden Wissenschaftlern und Forschern an den Kühltechnologien der nächsten Generation.

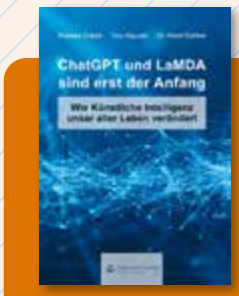
Ulrich Parthier: *Herr Stiller, wir danken für dieses Gespräch.*

ChatGPT UND LaMDA sind erst der Anfang

WIE KÜNSTLICHE INTELLIGENZ UNSER ALLER LEBEN VERÄNDERT

ChatGPT hat einen Hype um Künstliche Intelligenz (KI) ausgelöst. Eine Software, die Texte schreibt, die auf Anhieb nicht von Texten zu unterscheiden sind, die ein Mensch verfasst hat. Das ist ein Novum, ein Faszinosum und ein Angriffsziel für eine lange Reihe von Kritikern, die nicht müde werden, auf die Unzulänglichkeiten der KI-Texte hinzuweisen. Was dabei häufig übersehen wird: Wir stehen erst ganz am Anfang eine KI-Welle, die in den nächsten Jahren über uns schwappen wird. Google hat mit LaMDA über Jahre hinweg längste eine KI-Software entwickelt, die ChatGPT bei weitem übertrifft. Mit dem KI-Chatbot Bard sowie der KI-Integration in Suchmaschinen und Bürosoftware stellt 2023 ein Jahr der Zäsur für Künstliche Intelligenz dar.

Künstliche Intelligenz wird künftig alles verändern. Genauso grundlegend, wie der Personalcomputer, das Internet und das Smartphone unser Leben auf den Kopf gestellt haben. Von diesen Veränderungen wird keine Branche, kein Arbeitsplatz und kein Aspekt unseres Privatlebens verschont bleiben. Wir sind daher gut beraten, uns schon heute auf diese dramatischen Veränderungen vorzubereiten. In diesem Sinne legen die drei Autoren Andreas Dripke, Tony Nguyen und Dr. Horst Walther ein „Vorbereitungsbuch für ein Leben mit KI" vor.



ChatGPT UND LaMDA sind erst der Anfang -
Wie Künstliche Intelligenz unser aller Leben verändert

Andreas Dripke, Tony Nguyen, Dr. Horst Walther;
Diplomatic Counsil Publishing, 02-2023

ZUKUNFT VORAUS

Die Art und Weise, wie Finanzdienstleistungen erbracht werden, befindet sich in einer tiefgreifenden Transformation. Durch die Automatisierung von Prozessen wie der Kreditprüfung, der Risikobewertung oder der Betrugsprävention können Finanzinstitute Zeit und Ressourcen sparen und gleichzeitig präzisere Entscheidungen treffen. Dies ermöglicht eine schnellere Reaktion auf sich verändernden Marktbedingungen und Kundenbedürfnisse.

Doch die Automatisierung vermag viel mehr.

Quantensprung

DAS NEUE ZEITALTER DER FINANZFUNKTION BEGINNT JETZT

Es ist gut, dass es sie gibt: die zahlreichen Möglichkeiten der Automatisierung und Digitalisierung. Und je länger moderne Automatisierungs-Tools und Digitalisierungsplattformen auf dem Markt sind, umso deutlicher wird ihr Einfluss. Inzwischen zeigen zahlreiche Studien, aber auch Praxisbeispiele, wie nachhaltig die Automatisierung die Strukturen in den Unternehmen verändert und wie vorteilhaft das nicht zuletzt in Zeiten des Fachkräftemangels ist. Besonders eindrucksvoll lässt sich dieser Wandel im Finance-Segment nachvollziehen. Hier haben sich nicht nur zahlreiche Prozesse grundlegend verändert, sondern sogar ganze Stellenbeschreibungen und Rollenmodelle gewandelt.

Um die Dimension der Veränderung und vor allem deren Auswirkung auf die zukünftige Rolle der Finanzfunktion und des CFOs und dessen Team richtig erfassen zu können, ist zunächst ein kurzer Blick auf die Ausgangslage erforderlich. Zwar waren in der Vergangenheit im Finance & Accounting (F&A) bereits Softwarelösungen im Einsatz, die die klassischen Accounting-Prozesse unterstützen, aber das Automatisierungspotenzial dieser ersten Branchenlösungen war nur gering. Doch die Technologie entwickelte sich weiter und damit die Wertschöpfungsmöglichkeiten durch RPA (Robotic Process Automation)-Lösungen. Laut einer Studie von PwC aus dem Jahr 2020 werden Automatisierungslösungen vor allem in der Kreditorenbuchhaltung (72 Prozent), der Debitorenbuchhaltung (51 Prozent) sowie bei der Abschlusserstellung (28 Prozent) eingesetzt. Dadurch haben sich die Aufgaben und die Rollen der Finanzfachleute geändert. Anstatt Zahlen manuell abzugleichen und Daten händisch zu übertragen, erfolgen diese Aufgaben jetzt automatisiert im Hintergrund – basierend auf zuvor definierten Regeln. So verfügen die Finanzfachleute über mehr Kapazität für ihre eigentliche Arbeit, nämlich die Analyse der Unternehmensdaten. Laut einer Studie von McKinsey & Company ist das Potenzial enorm: Demnach können etwa 40 Prozent der Finanztätigkeiten vollständig automatisiert werden, was nicht nur zu einer weiteren Reduktion monotoner Fleißarbeit führt, sondern auch zu einem effizienten Finanzprozess. Die Untersuchung hat zudem ergeben, dass es den Unternehmen schon heute gelungen ist, mittels Automatisierung, die Kosten der Finanzfunktion durchschnittlich um 20 Prozent zu senken.

Automatisierung – der Turbo moderner Unternehmen

Durch die Automatisierung sind vor allem prozessuale Veränderungen derart grundlegend, dass die damit einhergehenden neuen Strukturen eine wesentlich breitere Basis für datenbezogene Geschäftsmodelle mit sich bringen. Am Beispiel der Accounting-Abteilung zeigt sich, dass sich die Finanzfachleute deutlich intensiver auf wertschöpfende Aktivitäten, wie etwa die Datenanalyse und

das Ableiten von Prognosen, konzentrieren können. Unternehmen, die etwa auf ein softwaregestütztes Continuous Accounting setzen, die also ihren Abschlussprozess so gestalten, dass er kontinuierlich über den Monat verteilt stattfindet und nicht erst zum Monatsende, können sogar auf Echtzeitdaten zugreifen. Das wiederum ist ein Benefit einer konsequenten Automatisierungsstrategie. Dass qualitativ hochwertige Echtzeitdaten aus der Finanzbuchhaltung in Zeiten fortwährender wirtschaftlicher Veränderungen einem Unternehmen nicht nur aus wirtschaftlicher Sicht Vorteile bringen, sondern vor allem ein Vielfaches an Agilität sowie realistischere Prognosen, versteht sich von selbst.

Die Finanzfunktion im Wandel

Stellt man diese Mehrwerte einer gezielten Automatisierung den zahlreichen Herausforderungen, die sich durch die aktuelle Wirtschaftslage ergeben, gegenüber, werden die Dimensionen der positiven Veränderung deutlich. Vor allem wenn man bedenkt, dass die Unternehmen nicht nur ihre aktuellen Aufgaben erledigen, sondern gleichzeitig auch ihre Zukunft planen müssen – egal, ob sie genügend Mitarbeiter haben oder nicht. Egal, ob diese im Homeoffice arbeiten möchten oder lieber im Büro. Und egal, welche Anpassungen Wirtschaft oder Politik in Zukunft von ihnen fordern.

Wer den Finanzprozess automatisiert, auf Continuous Accounting setzt und für einen möglichst lückenlosen Daten-Flow innerhalb der Finanzabteilung sorgt, hat vieles richtig gemacht. Denn damit werden die Voraussetzungen dafür geschaffen, dass die Finanz-Experten innerhalb kürzester Zeit auf topaktuelle Finanzdaten zurückgreifen, auf Marktveränderungen reagieren sowie das Unternehmen auf Kurs halten können.

IT & Automatisierung zieht Mitarbeiter an

Wer die Chancen der Automatisierung erkennt und die richtigen Weichen stellt, profitiert zudem davon, dass die zu erledigende Arbeit hochwertiger wird. Sobald solche Aufgaben automatisiert werden, die in der Regel wenig Freude bereiten – wie beispielsweise manuelle Abgleiche oder das Übertragen von Daten aus einem System in ein anderes – steigt die Motivation für neue Herausforderungen. Denn durch die Automatisierung sind zum einen die Unternehmensdaten in Echtzeit vorhanden, die analysiert werden können. Zum anderen haben die Finanzspezialisten auch die Zeit, ihre eigentliche Kompetenz auszuspielen. Die Automatisierung der Prozesse ist Geburtshelfer für neue Aufgabenfelder und damit auch für neue Stellenbeschreibungen und Rollen im F&A.

Der technologisch geprägte und auf Effizienz ausgerichtete Wandel sorgt also für weitaus grundlegendere Veränderungen in der Finanzabteilung als nur für eine Automatisierung der Workflows. Dank der neuen Technologie und automatisierten Tools, sind die Finanzexperten in der Lage, Real-Time-Reportings mit einer höheren Vorhersagegenauigkeit abzugeben als früher. Und sie können unterschiedliche Szenarien skizzieren, um aus diesen im Anschluss möglichst exakte Schlussfolgerungen abzuleiten und Planungen vorzunehmen. Die Automatisierung sorgt also dafür, dass überaus dynamisch und je nach Bedarf ganzheitliche Strategien entwickelt und die erforderlichen Maßnahmen abgeleitet werden können. Zusammengefasst verleiht eine strategisch durchdachte und durchgängig realisierte Automatisierung dem Finanzbereich und nicht zuletzt seinem Leiter, dem CFO, eine neue, tragende Rolle mit höherer Wertschätzung.

DURCH AUTOMATISIERUNG WIRD AUS DER TRADITIONELLEN, ADMINISTRATIVEN FINANZBUCHHALTUNG EINE STRATEGISCHE UNTERNEHMENSFUNKTION.

Ralph Weiss, Geo VP DACH, BlackLine, www.blackline.com/de

Mehr Business Consultant

Die Mehrwerte der Automatisierung sind konkret messbar. Welcher Vorstand oder welche Geschäftsführung würde es nicht begrüßen, wenn durch eine größere Genauigkeit der Finanzzahlen die Vorhersagequalität verbessert und Entscheidungsfindung unterstützt würde? Die Folge: Der CFO, der mit seinen Informationen und Analysen das Management jetzt noch zielgerichteter und wirksamer informieren

und beraten kann, wird zum gefragten Business Consultant. Nach und nach wird ihm und seinen Zahlen mehr Vertrauen entgegengebracht und er hat die Chance sich als Bindeglied zwischen der Geschäftsführung und den anderen Unternehmensbereichen zu etablieren, denn als CFO steht er automatisch im Austausch mit diesen. Das wiederum trägt zur Stärkung seiner Rolle und der Wertschätzung seiner Abteilung beziehungsweise Mitarbeiter bei. So werden der CFO und sein Team zu einem Katalysator der Wertschöpfung und Zukunftsfähigkeit im Unternehmen.

Erfolg macht attraktiv

Der Wandel durch die Automatisierung schlägt sich auch in der Finanzabteilung nieder: Die Mitarbeiter sind motiviert, weil sie wertvollere Arbeit leisten und ihre Ergebnisse eine höhere Anerkennung bekommen. Das wiederum wirkt sich positiv auf das Betriebsklima aus. Und wer zufrieden ist, kündigt nicht; ein nicht zu unterschätzender Wettbewerbsvorteil in Zeiten des Fachkräftemangels. Hinzukommt, dass diese positive Grundstimmung innerhalb des Unternehmens auch nach außen wirkt.

Dieses positive Stimmungsbild lässt sich bei der Suche nach neuen Talenten für das F & A nutzen, um sich gegenüber anderen Unternehmen in Szene zu setzen und interessante Bewerber für sich zu gewinnen. Gerade jetzt, wo Controller und Management Accountants überall gesucht werden, dürfte dieser Nebeneffekt des Automatisierungsprojekts nicht ganz unbedeutend sein. Wie jeder weiß, hat ein gutes Arbeitsklima eine große Strahlkraft. Und wenn ein Unternehmen, das im Rahmen eines Vorstellungsgesprächs vermitteln und auch noch darauf verweisen kann, dass in der Accounting-Abteilung mit den neuesten Softwarelösungen gearbeitet wird und sich die Mitarbeiter nicht mit Fleiß- sondern mit Analysearbeiten beschäftigen, dürfte das seine Wirkung kaum verfehlen.

Die Zukunft der Finanzfunktion

Die fortschreitende Automatisierung und Digitalisierung wird aus der bisher eher als passiv wahrgenommenen Finanzbuchhaltung der Unternehmen sukzessiv eine Abteilung gestalten, die intensiver in die Managementfunktionen, darunter die Unternehmensplanung, integriert sein wird. Der „Game Changer" Automatisierung wird dafür sorgen, dass das Finanzwesen zukünftig eine noch verantwortungsvollere Position einnimmt, und zwar nicht nur rückblickend und aus analytischer Sicht, sondern vor allem auch hinsichtlich der Vorhersagen. Dabei wird es keine Rolle spielen, wie ein Unternehmen strukturiert ist – sprich ob die Accountants im Büro arbeiten oder aus dem Homeoffice. Es wird egal sein, ob es sich um ein großes oder kleines Team handelt und wie oft die Geschäftsführung topaktuelle Analysen der Finanzdaten anfordert. Die modernen Tools sorgen dafür, dass manuelle Prozesse eliminiert werden und auf die Daten jederzeit und von überall zugegriffen werden kann – sicher und compliant.

Dank dieser Entlastung können sich die Verantwortlichen dem widmen, was wirklich wichtig ist: Wertbeiträge zur Unternehmenssteuerung leisten, solide Analysen durchführen, realistische Prognosen ableiten und potenzielle Szenarien skizzieren. Dieser Wandel hat in vielen Unternehmen bereits eingesetzt und zeigt eindrucksvoll, wie wichtig und dynamisierend Automatisierungsstrategien und Digitalisierungsprojekte sind – ganz zu schweigen davon, dass diese Unternehmen wesentlich bessere Chancen haben, qualifizierte und hoch motivierte Mitarbeiter für sich zu gewinnen.

Ralph Weiss

Into the Metaverse
Der unverzichtbare Leitfaden für die Chancen des Internets der Zukunft, Cathy Hackl, Plassen Verlag, 09-2023

INTO THE METAVERSE

DER UNVERZICHTBARE LEITFADEN FÜR DIE CHANCEN DES INTERNETS DER ZUKUNFT

Das Metaverse ist die nächste Generation des Internets. Doch was genau ist es, wie funktioniert es und warum wird es bald eine wichtige Rolle in Wirtschaft, Technologie und Gesellschaft spielen? Dieses Buch beantwortet alle wichtigen Fragen zum Thema und erklärt Ihnen, was das Metaverse für Ihre Marke, Ihre Organisation, Ihr Unternehmen bedeutet, wie Sie im Metaverse Geld verdienen können, indem Sie die zugrunde liegenden Konzepte wie Spiele, synthetische Medien, räumliche Datenverarbeitung und künstliche Intelligenz verstehen, wie man im Metaverse eine Führungsposition einnimmt und vieles mehr.

Cathy Hackl ist eine führende Tech-Futuristin und weltweit anerkannte Unternehmenslenkerin, spezialisiert auf Augmented Reality, Virtual Reality und Spatial Computing. Sie ist eine der ersten Chief Metaverse Officers der Welt.

Transformation im Finanzwesen

WARUM AUTOMATISIERUNG IM JAHR 2023 ENTSCHEIDEND IST

Das derzeitige globale Geschäftsumfeld bedeutet, dass Treasury-Teams im Finanzdienstleistungsbereich mit verschiedenen anspruchsvollen Herausforderungen konfrontiert sind. Diese Herausforderungen reichen von der Volatilität der Devisenmärkte bis hin zum Risikomanagement.

Die Aufgabe des Treasury-Teams besteht darin, die Finanzlage des Unternehmens durch strategische Planung zu schützen und das Risiko zu senken - oft über mehrere Bereiche hinweg. Die sich entwickelnde globale Wirtschaftslage stellt die Unternehmen jedoch vor hohe Herausforderungen in Bezug auf den Cashflow. Was können Treasurer also tun, um sich auf die kommenden Herausforderungen vorzubereiten

FÜR TREASURER ERMÖGLICHT DIE AUTOMATISIERUNG VON BACK-END-PROZESSEN EINE GRÖSSERE DATENTRANSPARENZ UND REDUZIERT GLEICHZEITIG DAS POTENZIAL FÜR MENSCHLICHE FEHLER.

Cosima von Kries,
Nintex Director, Solution Engineering EMEA,
www.nintex.de

#1 Bargeld Transparenz erhöhen

Eine Anfang 2022 veröffentlichte EACT-Umfrage ergab, dass 68 Prozent der Treasurer die Cashflow-Prognose als eines der drei wichtigsten Probleme bezeichneten. Die Gründe für die Priorisierung des Cashflows bleiben aufgrund der anhaltenden geopolitischen Situation in Europa, der weltweit steigenden Inflation und der Zinserhöhungen akut.

In diesen Zeiten brauchen Treasurer mehr Transparenz bei der Cash Visibility, um sich ein ganzheitliches Bild von der Liquiditätslage ihres Unternehmens zu machen. Erst einem vollständigen Überblick über die verfügbaren liquiden Mittel, deren Aufbewahrungsort und die erwarteten Geldströme kennen sie die Cashflow-Position ihrer Organisation wirklich.

Automatisierung ist für Treasurer wichtig. Von vielen Treasury-Abteilungen wird erwartet, dass sie typische Aufgaben wie den täglichen Cashflow, Kundentransaktionen und Mitarbeiterzahlungen verwalten und gleichzeitig strategische, langfristige Entscheidungen unterstützen. Sie jonglieren oft mit vielen Aufgaben gleichzeitig. Darüber hinaus bedeuten manuelle Prozesse, dass Treasurer nicht über Echtzeitdaten zur Cashflow-Position des Unternehmens verfügen.

Durch die Automatisierung des täglichen Liquiditätsabgleiches, der Berichterstattung über den Banksaldo und anderer Teile des Cash-Management-Prozesses automatisieren Treasurer jedoch nicht nur sich wiederholende, zeitaufwändige Arbeiten und können sich stattdessen auf strategische Aufgaben konzentrieren, sondern verfügen auch über Echtzeitinformationen auf ihren Dashboards, um zeitnahe Entscheidungen zu treffen.

#2 Die Risikostrategie neu denken

Neben dem Cash-Management ist das Risikomanagement immer wichtiger geworden. Treasurer reagieren derzeit sehr sensibel auf die Anfälligkeit ihrer Bilanzen für rasche Änderungen der Zinssätze, Währungsschwankungen, Rohstoff- und Lieferkettenrisiken, da sich die globalen Finanzbedingungen weiter verschlechtern.

Die derzeitige dynamische Finanzlandschaft hat jedoch sowohl Risiken als auch Chancen geschaffen. Treasury-Teams achten darauf, von verbesserten Renditen auf ihre kurzfristigen Anlagen zu profitieren. Die Möglichkeit, über Dashboards vollständige Transparenz und Kontrolle über Risiken und Hedging-Aktivitäten zu erhalten, ermöglicht es Treasurern Hedging-Strategien nahtlos anzupassen, beispielsweise im Falle einer hohen Marktvolatilität bei globalen Währungen im Jahr 2022.

Treasury-Teams, die in die Automatisierung investiert haben, waren schneller in der Lage, strategischere und systematischere Optionen für die Währungsabsicherung zu nutzen, um die Treasury-Richtlinien einzuhalten und günstige Absicherungsmöglichkeiten schnell und nahtlos

zu nutzen. Zu den Bereichen, die sich für die Automatisierung anbieten, gehören die Automatisierung von FX-Prozessen, wie zum Beispiel das Zusammenfassen von Anfragen, Initiierung von Preisanfragen und die Ausführung von Handelsstrategien auf der Grundlage vorteilhafter, im Voraus festgelegter Parameter.

#3 Berichtswesen verwalten

Treasurer verlassen sich bei geschäftskritischen Aufgaben oft auf manuelle Prozesse. Die Erfassung und Analyse von Daten für kritische Aufgaben wie Devisenmanagement und Risikoplanung ist zeitaufwändig. Aus diesem Grund geben viele Organisationen ihre traditionellen Prozesse auf und setzen auf Automatisierung, um ihre Arbeitsabläufe zu optimieren und Zeit für wertschöpfende Aufgaben zu gewinnen.

Beziehen Unternehmen die ESG-Berichterstattungen mit ein, bedeutet die Einführung von nicht-finanziellen Daten die Integration von noch mehr Datenquellen, was die monatliche Zusammenführung von Berichten zu einer zusätzlichen Herausforderung macht. Auch hier spielt die Automatisierung eine wichtige Rolle.

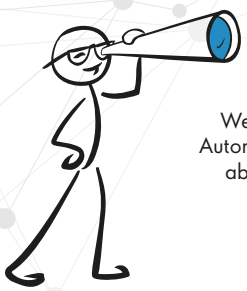
Es gibt verschiedene Möglichkeiten, die Automatisierung einzuführen – es muss keine Alles-oder-Nichts-Entscheidung sein. Die Automatisierung der Managementberichterstattung (d. h. die automatische Datenerfassung, -zusammenstellung und -eingabe in standardisierte Berichtsvorlagen) können Unternehmen beispielsweise schrittweise einführen und erhebliche Effizienzsteigerungen erreichen.

Die Rolle von Low-Code im Finanzwesen

Die Einführung dieser Automatisierungsinitiativen kann sich jedoch als schwierig erweisen, da die Ressourcen der IT-Teams knapp sind, die Budgets schrumpfen und die Lücke bei den technologischen Fähigkeiten immer größer wird. Hier werden Low-Code-Technologien und -Anwendungen alltäglich und können einen echten Unterschied machen.

Low-Code-gestützte Plattformen sind bereits ein wesentlicher Bestandteil vieler Strategien zur digitalen Transformation. Für Treasurer ermöglicht die Automatisierung von Back-End-Prozessen eine größere Datentransparenz und reduziert gleichzeitig das Potenzial für menschliche Fehler und die Verzögerung durch manuelle Eingaben. Vollständig automatisierte Treasury-Teams sind besser in der Lage, Kernprozesse im Finanz- und Rechnungswesen zu beschleunigen, menschliche Fehler zu eliminieren und Daten besser zu nutzen.

Cosima von Kries



PLUS

Weitere Informationen zur Automatisierung von Arbeitsabläufen: **bit.ly/3p7zXvV**

Biometrie statt Passwort

DER EINFACHE UND SICHERE ZUGANG ZU DIGITALEN BANKING SERVICES

Wem ist es noch nie passiert, beim Log-in plötzlich einen Black-out zu haben? Ein vergessenes Passwort ist lästig, viel kritischer ist aber die bisherige Passwort-gestützte Authentifizierung. Obgleich Banken den Umgang mit Passwörtern gut im Griff haben, wünschen sich viele Kunden einen bequemeren und trotzdem sicheren Zugang zu ihren digitalen Services. Banken können diesem Bedürfnis nachkommen – und zwar mit passwortfreier Authentifizierung durch biometrische Verfahren.

Unter den Eingabefeldern für Nutzername und Passwort steht nicht umsonst oft der Link „Passwort vergessen?" Die meist temporäre Amnesie hat auch damit zu tun, dass wir immer mehr Geräte und Kanäle nutzen und uns deren diverse Zugangsdaten merken müssen: Ein einziges Passwort für alle Zugänge verbietet sich von selbst. Als vorauseilende Hilfe bei Erinnerungslücken werden gerne Zettelnotizen in Portemonnaies oder Brieftaschen deponiert. Doch nicht nur die sind ein latentes Sicherheitsrisiko. Angesichts immer ausgefeilterer Betrugsattacken verzeichnen Banken ein ständig steigendes Risiko auch für die Kunden, die sich mit ihrem (nicht vergessenen) Passwort authentifizieren. Die von den Kunden wie den Banken gewünschte Kombination aus Sicherheit und Komfort sollte neu gedacht werden. Eine zukunftssichere und einheitliche Lösung muss diesen Zielkonflikt aufheben und beide Anforderungen parallel erfüllen.

Komfort und gleichzeitig auch Sicherheit

Banken haben verständlicherweise ein vitales Interesse daran, den Zugriff auf digitale Services zu beschleunigen, die Verweildauer der Kunden in den Apps und die Transaktionsvolumina zu erhöhen und einen unmittelbaren Mehrwert für die Nutzer zu schaffen. Die wiederum wollen schnelle, einfache und zuverlässige Anmelde- und Transaktionsfreigaben ohne Passwort-Chaos. Daraus ergeben sich drei Anforderungen an eine Authentifizierungslösung für Digital Banking: Erstens ein bequemes Log-in ohne PINs und Passwörter – und zwar für die Account-Zugänge über die diversen mobilen Apps und Browser-Applikationen hinweg. Zweitens die sichere Authentifizierung auch für risikoreiche Transaktionsarten. Und drittens die Optimierung von Bezahlvorgängen im E-Commerce durch Eliminierung von Verzögerungen und Unterbrechungen. So erhöhen beispielsweise die Wartezeiten auf Einmal-Passwörter via SMS die Abbruchraten.

Für die sichere und starke Kundenauthentifizierung (SCA) gilt die Zahlungsdiensterichtlinie PSD2 der EU. Sie schreibt für den Zugang zu Online-Konten oder elektronische Zahlungen eine Multi-Faktor-Authentifizierung (MFA) vor. Grundsätzlich können dafür drei unterschiedliche Authentifizierungsfaktoren genutzt werden: Wissen, Besitz oder Merkmal. Im ersten Fall sind das beispielsweise die bereits erwähnten PINs und Passwörter. Besitz umschreibt Objekte wie externe Schlüssel, Smartcards oder Endnutzergeräte. Merkmale, sprich biometrische Eigenschaften wie Sprache, Fingerabdruck, Iris oder Gesicht dagegen sind jederzeit – kostenfrei – verfügbar und komfortabel nutzbar. Damit ist die biometrische Authentifizierung ideal für die Schnittstelle zwischen Bank und Kunde. Mit der Fast IDentity Online Technologie (FIDO) gibt es dafür einen globalen Standard, den auch Big Techs wie Apple, Google und Microsoft immer stärker unterstützen. Er arbeitet mit einer MFA-Kombination aus User Verifikation mittels Biometrie oder Wissen (erster Faktor) und Private Key (zweiter Faktor), wobei der private Schlüssel erst nach der User Verifikation genutzt werden kann.

Self-made oder Plattform?

Die Antwort auf die Vorgaben von PSD2 könnte jede Bank mit einer eigenen, selbst entwickelten Authentifizierungs-Lösung geben. Allerdings wäre der Aufwand dafür immens hoch (ausbleibende Skaleneffekte) und dies müsste auf Basis eines gemeinsamen Standards erfolgen, um die Kompatibilität der Banken-exklusiven Lösungen sicherzustellen. So hat kürzlich die Europäische Kommission in ihrer Studie über die Anwendung und die Auswirkungen der Zweiten Zahlungsdiensterichtlinie (PSD2) unter anderem mehr Standardisierung und Interoperabilität vorgeschlagen, etwa durch einheitliche Standards für zahlungsrelevante Mechanismen wie Schnittstellen oder QR-Codes – Vorschläge, die auch bei der Weiterentwicklung von PSD2 zu PSD3 noch eine wichtige Rolle spielen werden.

DURCH DIE BIOMETRISCHE AUTHENTIFIZIERUNG ENTFÄLLT DIE NUTZUNG VERSCHIEDENER PINS ODER PASSWÖRTER FÜR DIE ACCOUNT-ZUGÄNGE IN MOBILEN APPS ODER BROWSER-APPLIKATIONEN..

Quintin Stephen,
Authentication Business Lead,
Giesecke+Devrient,
www.gi-de.com/de/
(Quelle: G+D)

Wesentlich sinnvoller ist es daher, eine skalierbare digitale Plattform zu nutzen, die per APIs in die Legacy-Systeme der Banken eingebunden wird. Das macht Anwendern die biometrische Anmeldung so einfach, als würden sie ihr Smartphone entsperren. Ein Fingerabdruck oder Gesichts-Scan genügt für den sicheren, Zwei-Faktor-authentifizierten Zugang zu den persönlichen Accounts über alle Kanäle hinweg, egal ob in einer App oder in einem Browser. Gleichzeitig werden damit die drei oben beschriebenen zentralen Bedürfnisse von Banken und Finanzinstituten erfüllt. Durch die biometrische Authentifizierung entfällt die Nutzung verschiedener PINs oder Passwörter für die Account-Zugänge in mobilen Apps oder Browser-Applikationen. Auch risikobehaftete Transaktionen wie Überweisungen oder Zahlungen werden durch die biometrische Authentifizierung schnell, sicher und mit minimalem Aufwand für die Kunden erledigt. Und sie senkt die Abbruchraten in Online-Shops, da weder Passwörter oder PINs gemerkt werden müssen, noch das Warten auf Einmalpasswörter oder Verifikationscodes für Verzögerungen sorgt.

Log-in und Authentifizierung sind quasi das Tor zu Online-Banking und e-Commerce. Kundenerfahrungen beginnen immer und überall mit diesem Schritt. Und der erste Eindruck ist prägend. Deshalb sollten Banken dieser Schnittstelle besondere Aufmerksamkeit schenken, wenn sie Wert auf Kundenzufriedenheit, Loyalität und Profitabilität legen.

Quintin Stephen

Allheilmittel Private 5G?

AUF DIE RICHTIGE PLANUNG KOMMT'S AN

Sie klingen zu schön, um wahr zu sein: Die mannigfaltigen Vorteile der Private-5G-Netzwerke. Ein Narr, wer nicht auf diesen Mega-Trend aufspringt und sie für sein Unternehmen nutzt – oder nicht? Die Antwort lautet: „Ja, und ...!" Damit die Private-5G-Technik sinnvoll und gewinnbringend eingesetzt werden kann, müssen die Anforderungen an das zukünftige Netzwerk vorher klar sein. Sprich, das Private-5G-Netz muss anhand der Probleme konzipiert werden, die es zu lösen gilt, und nicht zum Selbstzweck.

Private-5G-Netzwerke sind, wie der Name schon sagt, von öffentlichen Netzen abgegrenzt. Unternehmen können also eigene Mobilfunknetze errichten und betreiben, die mittels eigener Hardware und Frequenzen vollkommen autark vom öffentlichen Mobilfunknetz funktionieren. In vielen Branchen ist Private 5G bereits im Einsatz – von der Fertigungsindustrie über die Logistik bis hin zum Bereich Healthcare. Die Vorteile, die Private-5G-Netzwerke auf dem Papier mit sich bringen, sind bestechend: Geringere Latenzen, hohe Zuverlässigkeit und Ausfallsicherheit, eine schnellere Übertragung von hohen Datenmengen sowie eine selbstbestimmte Betriebssicherheit. Nicht verwunderlich, dass Unternehmen diese Vorteile nutzen möchten. Trotzdem werden mit dem neuen 5G-Netzwerk nicht immer alle Erwartungen erfüllt. Woran liegt das?

Welches Ziel verfolge ich?

Der Wunsch, sich das Buzzword Private 5G auf die eigene Fahne schreiben zu können, bringt meist nur eines mit sich: Unternehmen preschen in die Private-5G-Welt, ohne eine konkrete Vorstellung davon zu haben, welches Problem sie überhaupt lösen möchten. Kein Wunder, denn die Anwendungsmöglichkeiten scheinen grenzenlos zu sein: Allein in der Logistik beispielsweise lassen sich Warenflüsse verfolgen, Lagerbestände überwachen oder autonome Transportsysteme koordinieren. Zahllose beschriebene Use Cases haben keinen direkten Bezug zu dem, was heute bereits umsetzbar ist. Denn 5G ist nicht gleich 5G. Ähnlich zu seinen Vorgängern (2G, 3G und 4G) wird die Technologie stufenweise von einem zentralen Gremium spezifiziert und erst anschließend von den Herstellern umgesetzt. Dadurch entsteht eine große Diskrepanz zwischen Marketing-Versprechen, die theoretische Inhalte propagieren, und der tatsächlich verfügbaren Technik. Dies führt immer häufiger zu sogenannten Proof of Concepts (PoCs) ohne „Hand und Fuß". Denn sie werden häufig ausgeschrieben, ohne dass die genauen Anforderungen an das zukünftige Netz oder die aktuelle Leistungsfähigkeit der Technik bekannt sind. Eine Vorstellung davon, wie das Ergebnis gemessen und bewertet werden könnte, fehlt meist ebenso. Unzufriedenheit, Fehlinvestitionen und Verzögerungen auf dem Weg zu einem sinnvollen Einsatz von Private 5G sind damit vorprogrammiert. Aber wie geht es richtig?

Gängige PoC-Szenarien aufbrechen

Um diesen hausgemachten PoC-Teufelskreis zu durchbrechen, gilt es, zunächst

EXTERNE EXPERTEN WIE LOGICALIS UNTERSTÜTZEN UND BEGLEITEN BEI BEDARF DEN GESAMTEN PROZESS, UM GEMEINSAM MIT DEM KUNDEN DAS RICHTIGE SETUP ZU FINDEN.

Jürgen Hahnrath, Senior Sales Executive Private 5G and Industry Solutions, Logicalis, www.logicalis.de

einmal Themenfelder mit Handlungsbedarf zu bestimmen. Sprich, wo in der Organisation und/oder bei welchen Prozessen gibt es Probleme, die gelöst werden müssen? Im nächsten Schritt geht es darum, mögliche Lösungen zu finden und (erst) dabei die Anforderungen in puncto Netz zu bestimmen.

So gibt es Anwendungsfälle, die eine Versorgung großer Flächen ohne spezielle Anforderungen beinhalten, aber auch Anwendungen, die bewegte Objekte inklusive einer hochauflösenden Aufzeichnung steuern sollen. Die Ansprüche an das Netz sind in diesen beiden Fällen grundlegend verschieden, was unterschiedliche Ausprägungen des 5G-Netzes nach sich zieht. Im Private-5G-Bereich gibt es allein bei der Frage „Indoor oder Outdoor?" massive Unterschiede, auch in puncto Mehrwert. Heißt, oftmals reicht eine Standardlösung nicht aus, um von allen Vorteilen profitieren zu können. Ein bunter Fragenkatalog entscheidet darüber, wo welche Lösung beziehungsweise Lösungskombinationen zum Einsatz kommen können und müssen. Dazu gehören Fragen zu Durchsatz, Fläche oder Nutzungsort, aber auch zu der vor Ort geltenden Rechtslage. Ein Beispiel für solche länderspezifischen Anforderungen ist der Frequenzbereich: Dieser ist für den Bereich 5G streng reguliert, jedes Land hat dafür seine eigenen Vorgaben. Während er in Deutschland zwischen 3.7 und 3.8 Gigahertz (GHz) liegt, sind es dagegen beispielsweise in Großbritannien zwischen 3.8 und 4.2 GHz. Es gilt also, sich frühzeitig mit diesen komplexen Anforderungen und Regeln zu beschäftigen.

DAMIT DIE PRIVATE-5G-TECHNIK SINNVOLL UND GEWINNBRINGEND EINGESETZT WERDEN KANN, MÜSSEN DIE ANFORDERUNGEN AN DAS ZUKÜNFTIGE NETZWERK VORHER KLAR SEIN.

Christian Freund, Solution Director 5G, Logicalis, www.logicalis.de

Standardisierungsdenken durchbrechen

Das heißt: Stellt sich bei der grundlegenden Analyse heraus, dass ein Private-5G-Netzwerk zur Lösung beitragen kann, müssen die Verantwortlichen die Anforderungen an das Netz genau bestimmen. Gleiches gilt für die KPIs zur Erfolgsmessung der Maßnahme. Erst im Anschluss an diese Maßnahmen ist es sinnvoll und zielführend, die evaluierten Schritte in einem PoC zu erproben. Dies kann je nach Anforderung in einem 5G-Testlabor oder aber direkt im Unternehmen vor Ort stattfinden. Logicalis beispielsweise bietet in seinem neuen 5G-Testlabor in Weiterstadt die Möglichkeit, Anwendungsfälle und neue 5G-Lösungen zu erproben. Ein Testnetz lässt sich dabei in zwei Bereiche aufteilen: Im Entwicklungsnetz testet das Unternehmen vorab neue Software-Versionen und die Integration von neuen 5G-Komponenten, während es im Produktionsnetz kundenspezifische Lösungen prüft.

Durchdacht schneller ans Ziel

Externe Experten wie Logicalis unterstützen und begleiten bei Bedarf den gesamten Prozess, um gemeinsam mit dem Kunden das richtige Setup zu finden – von der einzelnen Komponente und allem, was dazu gehört, bis hin zur passgenauen Lösung. Dabei ist Logicalis als Cisco Global Gold Partner einer der wenigen globalen Dienstleister, die weltweit mit Cisco 5G Szenarien umsetzen. Unternehmen, die sich dieser Vorgehensweise bedienen, kommen in der Regel schneller zu einer umsetzbaren Lösung, die einen signifikanten Beitrag zu ihrem Unternehmenserfolg leisten kann, und vermeiden Fehlinvestitionen.

Jürgen Hahnrath, Christian Freund

Die richtige Wahl für die Zukunft

WIE DIE LOGISTIK DIE VORTEILE VON 5G FÜR AUTOMATISCHE LADESHUTTLES NUTZT

5G – das Mobilfunknetz der 5. Generation – ermöglicht ein stabiles Netzwerk, das hohe Anforderungen an die Bandbreite respektive an die Anzahl der vernetzten Geräte stellt. Dass diese Vorteile nicht nur in Gaming-Anwendungen oder in der Medizin deutlich zum Tragen kommen, zeigen auch industrielle Beispiele aus der Logistik. Hier ist der 5G-Einsatz oft die richtige Wahl.

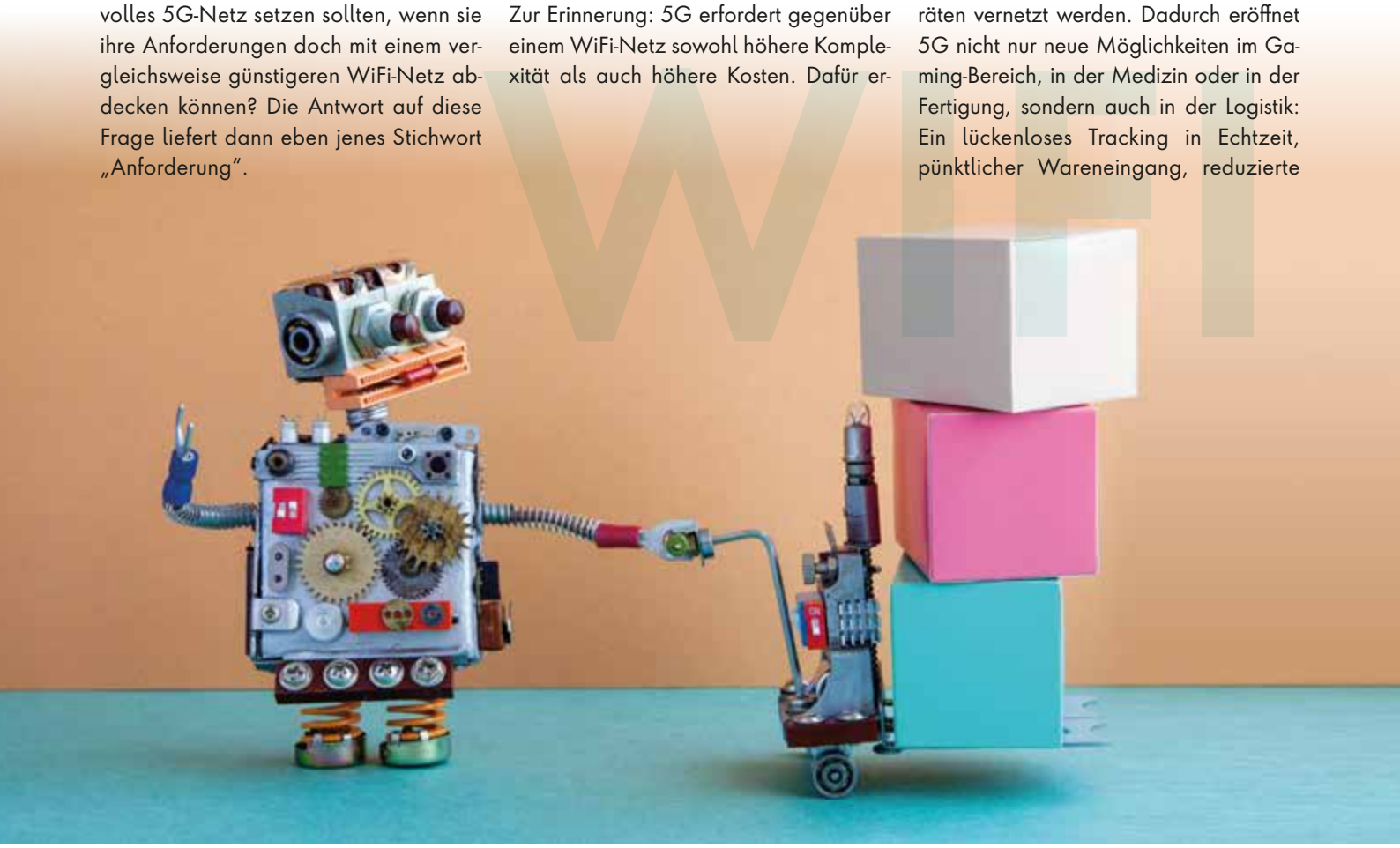
Mitunter fragen sich Unternehmende, warum sie auf ein technisch anspruchsvolles 5G-Netz setzen sollten, wenn sie ihre Anforderungen doch mit einem vergleichsweise günstigeren WiFi-Netz abdecken können? Die Antwort auf diese Frage liefert dann eben jenes Stichwort „Anforderung".

Ja, WiFi-Netze stellen je nach Anwendungsgebiet genug Datenraten. Darüber hinaus ist das Netz einfach und flexibel bereitgestellt, betrieben und gewartet. Aber: Für viele Anwendungen im modernen industriellen Umfeld kommt sogar WiFi 6 an seine Grenzen. Besonders, wenn beispielsweise die Anzahl der vernetzten Geräte von 10.000 auf 100.000 Geräte pro Quadratkilometer steigt oder die Latenzzeit enorm niedrig sein muss.

Der entscheidende Unterschied

Zur Erinnerung: 5G erfordert gegenüber einem WiFi-Netz sowohl höhere Komplexität als auch höhere Kosten. Dafür erfüllt das Netz die Anforderungen, die moderne Technologien an Bandbreite, Verfügbarkeit, Stabilität und Datendurchsatz stellen. 5G-Netzwerke bieten mehr Geschwindigkeit, weniger Latenz und mehr Kapazität. Entsprechend liegt die durchschnittliche 5G-Geschwindigkeit bei zirka 700 MBit/s, die Antwortzeit beläuft sie sich dabei nur noch auf einige Millisekunden.

Darüber hinaus können pro Quadratkilometer eine sechsstellige Anzahl von Geräten vernetzt werden. Dadurch eröffnet 5G nicht nur neue Möglichkeiten im Gaming-Bereich, in der Medizin oder in der Fertigung, sondern auch in der Logistik: Ein lückenloses Tracking in Echtzeit, pünktlicher Wareneingang, reduzierte



Lade- und Wartezeiten. Im Kontext von Industrie 4.0 macht 5G den entscheidenden Unterschied. Eben diesen macht sich die Logistik schon jetzt zu Nutze.

5.000 vollautomatische Verladeroboter

Ein Paradebeispiel hierfür sind fahrerlose Transportsysteme, sogenannte AGVs (Automated Guided Vehicles), die in Lagerhallen bis zu 50 Kilogramm schwere Waren gänzlich automatisiert aus Regalen holen und an deren Ziel transportieren. Die bis zu 5.000 AGVs bewegen sich dabei auf vertikalen und horizontalen Schienensystemen mit Geschwindigkeiten von bis zu 10 m/s. Im Vergleich: Bei einem sehr guten WiFi-6-Netz kommt es bereits ab einer dreistelligen Anzahl von Geräten zu massiven Problemen. Hier ist vor allem die Herausforderung bei Zellenwechseln hervorzuheben, welche zu Kollisionen oder gar zum kompletten Stillstand der Betriebsumgebung führen kann – eine Erkenntnis, die wir im Rahmen von eigenen Forschungsprojekten sowie bei Feldversuchen im Auftrag von Kunden mit beiden Technologien gewinnen konnten.

Dabei ermöglicht gerade erst der Einsatz automatisierter Shuttles eine effiziente Nutzung von Lagerhallen mit einer Größe von mehreren Zehntausend Quadratmetern, deren Regale bis kurz unter die Deckenwand reichen: Die maximale Nutzung von Lagerflächen bedeutet zwangsläufig eine erhöhte Brandgefahr. Als logische Konsequenz und weil Wasser als Löschmittel nicht immer in Frage kommt, reduzieren die Betreiber solcher Lagerhallen den Sauerstoffgehalt darin. Somit können Menschen nicht oder nur unter stark erschwerten Bedingungen eingesetzt werden. Hier bieten die 5G vernetzten AGVs eine ideale, fortschrittlich Lösung für den Balanceakt zwischen maximaler Sicherheit, Kosten und Verladekapazität.

Die Grenzen erreicht

Die übertragene Datenmenge der vielen Shuttles in Kombination mit den hohen Geschwindigkeiten sowie die häufigen Zellwechseln sind dabei eine technologische Meisterleistung, die aktuell nur durch ein 5G-Netz stabil und vor allem sicher unterstützt werden. Stabil und sicher heißt hier, dass bei Geschwindigkeiten von 10 Meter pro Sekunde jede Millisekunde zusätzlicher Latenzzeit zu mitunter verheerenden Konsequenzen führen kann.

5G-NETZWERKE BIETEN MEHR GESCHWINDIGKEIT, WENIGER LATENZ UND MEHR KAPAZITÄT.

Nizar Zalila, CTO, CONGIV GmbH, www.congiv.de

Durch eine intelligente Kombination von aktiven Netzelementen (Antennen) in gut zugänglichen Bereichen und passiven Netzelementen in schwer zugänglichen Bereichen wie zum Beispiel sauerstoffreduzierten Hallen oder in engen Metallregalen können die Wartungsarbeiten und somit Ausfallzeiten des Netzes auf ein absolutes Minimum reduziert werden.

Fazit

Was nach Zukunftsszenarien anmutet, ist in der Logistik inzwischen auch in Deutschland Realität! Jedoch kann nur 5G die hohen Anforderungen erfüllen, die eine derartige Kommunikation an ein Netzwerk stellt: Diese sind eine ultraniedrige Latenzzeit von unter 10 Millisekunden sowie einen stärkeren Durchsatz.

Natürlich, ob WLAN oder 5G zum Einsatz kommen, wird von Anwendungsfall zu Anwendungsfall unterschiedlich sein. Jedoch ist gerade in diesem Bereich der Logistik 5G die beste Option, da es am Ende das Ziel ist, die menschliche Interaktion möglichst zu eliminieren, um dadurch den Versand von Waren maximal zu automatisieren und zu beschleunigen.

Nizar Zalila

Revolution der Arbeitswelt

WIE KÜNSTLICHE INTELLIGENZ UNSERE ARBEITSWELT VERÄNDERT

Ob im Lehrerzimmer, auf LinkedIn oder in Leitmedien: Künstliche Intelligenz ist das Thema der Stunde. Die Veröffentlichung von ChatGPT durch Open AI im Herbst 2022 wird vielfach mit dem iPhone-Moment der Künstlichen Intelligenz gleichgesetzt. Künstliche Intelligenz wird dabei zum Treiber einer disruptiven Revolution, die unsere Arbeits- und Lebenswelt ähnlich stark wandeln wird, wie die Industrialisierung oder das Internet. Künstliche Intelligenz wird dabei Einzug in jede Branche halten. Experten erwarten ein starkes Wachstum – insbesondere bei der beruflichen Nutzung.

Große Veränderungen stehen uns durch den Einsatz von Künstlicher Intelligenz (KI) bevor, die immer stärker in unsere Arbeitswelten vordringt und diese massiv verändert. Im Bericht zur Zukunft der Arbeit des World Economic Forums geben mehr als 85 Prozent der befragten Unternehmen an, dass die verstärkte Einführung zukunftsweisender Technologien und die Ausweitung des digitalen Zugangs die Megathemen darstellen, die den Wandel in ihrem Unternehmen am stärksten vorantreiben. Dabei setzen die Unternehmen vor allem auf Big Data, Cloud Computing und künstliche Intelligenz. Mehr als 75 Prozent der Unternehmen beabsichtigen, diese Technologien in den nächsten fünf Jahren einzuführen.

ARBEIT FÄLLT DURCH DEN EINSATZ VON KI NICHT WEG, SONDERN VERÄNDERT SICH.

Lucia Falkenberg, Chief People Officer, eco – Verband der Internetwirtschaft und DE-CIX Group AG, www.eco.de

Arbeit fällt durch den Einsatz von KI nicht zwangsläufig weg, sondern verändert sich. Körperlich belastende, repetitive und monotone Tätigkeiten werden durch kreative und kommunikative Aufgaben ersetzt. Damit das gelingt, brauchen wir eine weitere kulturelle und gesellschaftliche Evolution, um Skeptiker zu überzeugen: Manche Menschen fürchten, Jobs zu verlieren. Oft ist genau das Gegenteil der Fall. Disruptive Technologien bringen neue Berufsfelder hervor, innovative Produkte und Geschäftsmodelle entstehen, führen zu Prozess- und Effizienzsteigerungen. So lautet die zentrale Botschaft des unabhängigen Rats der Arbeitswelt in seinem jüngst erschienen Bericht: Trotz des enormen Wandels der Arbeitswelt wird es in Deutschland schon allein aufgrund des demographischen Wandels nicht zwangsläufig Arbeitsplatzverluste geben. Jedoch werden die Rahmenbedingungen und Anforderungen andere sein: In der durch KI veränderten Arbeitswelt werden Diversität und lebenslanges Lernen zu Erfolgsfaktoren.

Neue Bildungskonzepte erforderlich

Unternehmen, Politik und Zivilgesellschaft müssen die Vermittlung digitaler Kompetenzen und die Teilhabe aller an der Digitalisierung als gesamtgesellschaftliche Chance annehmen und als kontinuierliche und Aufgabe verstehen. Schließlich setzt die Teilhabe an der digitalen Zukunft Aus-, Fort- und Weiterbildung in jeder Lebensphase voraus. Digitale Transformation ist ein fortlaufender Prozess, der unsere Arbeitsbedingungen in den nächsten Jahrzehnten prägen wird. Das heißt in Bezug auf Beschäftigte, dass die Halbwertszeit von Ausbildungen kürzer wird. In allen Arbeitsbereichen und Branchen, ob Handwerk, Verwaltung oder Wirtschaft, muss lebenslanges Lernen zum Standard werden. Unternehmen müssen Konzepte für die kontinuierliche Fortbildung ihrer Mitarbeiter hinsichtlich digitaler Fähigkeiten und im Umgang mit den neuen Technologien entwickeln, wenn sie sich langfristig auf leistungsfähige Teams verlassen wollen.

Lucia Falkenberg

#LiT

Das Netzwerk Ladies in Tech, kurz #LiT, setzt sich für mehr Sichtbarkeit von Frauen in Tech ein und bietet eine Plattform zum Austausch – digital und analog.
lit.eco.de

WAS BEGRÜSSEN SIE AN IP-TELEFONEN?

34 %
Funktionsvielfalt

36 %
Erreichbarkeit überall im Firmengebäude

8 %
Audioqualität des Endgerätes

Hybrid Working und Telefonie

MARKTSTUDIE WIRFT GEFÜHLTE WAHRHEITEN UM

Bedenkt man die stattfindende Veränderung herkömmlicher Arbeitsmodi hin zu hybriden oder Fully-remote-Modellen und die diesem Trend beigemessene Bedeutung, erweisen sich die Ergebnisse der jüngsten Marktstudie von Snom als verblüffend.

Der Einzug neuer Arbeitsmodelle in Unternehmen ist einer der aktuellsten Trends im B2B-Umfeld. Ob hybrid oder „fully remote", versprechen diese Arbeitsmodi eine gesteigerte Produktivität und eine verbesserte Zusammenarbeit. Sie werden von vielen als „neue Normalität" wahrgenommen. Aufgrund dessen führte das unabhängige Marktforschungsinstitut Norstat, beauftragt vom IP-Telefon-Hersteller Snom, im März dieses Jahres eine repräsentative Umfrage zum Thema Hybrid Working und Telekommunikationsausstattung durch. Gefragt wurden 4.822 Erwerbstätige (Firmenangestellte) aus Deutschland, Frankreich, Italien, Spanien und Großbritannien nach dem Besitz eines Tischtelefons im Büro, nach der Zufriedenheit mit dem IP-Endgerät, inwieweit Hybrid Working ausgeübt wird und nach dem hierfür genutzten Kommunikations-Equipment. Die Ergebnisse der Studie sind eindeutig.

Hybrid Working in Kinderschuhen

Angesichts des Hypes um das hybride Arbeiten hätte man hierzulande einen viel größeren Anteil an mobilen Arbeitenden vermutet. Doch verglichen mit den Werten Großbritanniens (56 %), Spaniens (50 %) und Italiens (45 %) behaupten in Deutschland nur 39 Prozent der Befragten, hybride Arbeitsmodelle zu leben, dicht gefolgt von Frankreich, wo gerade mal 3 von 10 Firmenangestellten mobil arbeiten. Allerdings bestätigt die Studie ebenfalls die Vorreiterrolle Deutschlands bei der Vergabe geschäftlicher Ausstattung für das Homeoffice. 67 Prozent der Hybrid Worker bestätigten, dass die eingesetzten Telekommunikationsgeräte vom Arbeitgeber gestellt wurden.

IP-Telefonbestand in Büros unverändert hoch

Die vermutete Ablösung der Bürotelefone aufgrund der gefühlt massiven Veränderung der Arbeitspraktiken blieb laut der Studie aus. Von den 1.030 befragten Erwerbstätigen aus Deutschland nutzen 64 Prozent nach wie vor ein IP-Telefon – und drei von vier sind sehr zufrieden damit. Dies spricht eher für eine komplementäre Nutzung von IP-Telefon und Smartphone zwecks geschäftlicher Kommunikation statt für eine Verdrängung. Auch weil Deutschland im Europavergleich mit 66 Prozent der Befragten den geringsten Anteil an Mitarbeitenden aufweist, die Smartphones für Geschäftstelefonate nutzen – 47 Prozent davon nur sporadisch vom Homeoffice aus.

Den wesentlichen Beitrag von IP-Telefonen in KMUs stellen Features dar, die es gestatten, das Bürotelefon nahtlos zu Hause zu nutzen, oder professionelle Geräte, die alle Kommunikationsdienste aus der Firma auch im Homeoffice abbilden. Denn damit profitieren mobile Anwender von der Flexibilität aktueller Telekommunikationssysteme, unabhängig vom Ort der Leistungserbringung, und Unternehmen von den Sicherheits-Features moderner Telekommunikationslösungen.

www.snom.com

Hybrides Arbeiten

DIE DREIFACH-FIT-FORMEL

Organisatorische, technische und kulturelle Voraussetzungen schaffen, Arbeiten am Küchentisch, virtuelle Meetings und der Abschied von der Teeküche: Der Arbeitsalltag hat sich für Millionen von Büro-Angestellten während der Pandemie radikal geändert. Dabei zeigte sich vielfach, dass ein Laptop allein noch keine gute dezentrale Zusammenarbeit ausmacht. Denn oftmals hatten die Unternehmen gar keine Chance, ihre organisatorischen Abläufe, Prozesse, Tools und Werkzeuge der neuen Realität anzupassen – von der Unternehmenskultur ganz zu schweigen. Seitdem ist einige Zeit vergangen, die Büros haben sich wieder mit Leben gefüllt. Die radikale Präsenzpflicht, wie sie Twitter & Co. wieder einführen, ist allerdings wenig beliebt bei Angestellten: Hybrides Arbeiten, also der flexible Wechsel zwischen Büro und mobiler Arbeit, setzen heute viele als Standard voraus. Doch nicht alle Unternehmen haben die Zeit genutzt, um sich fit für die neue Arbeitsrealität zu machen.

MEHR WERT

Mobilität statt Stillstand:
bit.ly/3IeJmZB

Wunsch trifft Realität

Vom gemischten Meeting mit Mitarbeitenden vor Ort und zu Hause über die funktionierende Datenablage bis zur Gleichbehandlung von Remote und Office Work: Was als schöne, neue Arbeitswelt gedacht ist, kann genau das Gegenteil bewirken, wenn die Voraussetzungen nicht stimmen. Prozesse werden langsamer, Ziele werden gerissen, Mitarbeitende werden unzufrieden oder wenden sich sogar vom Unternehmen ab. Denn beim Versuch, eine neue Arbeitsweise mittels unzureichender Tools in unpassende Strukturen zu pressen und dabei auf ein gutes Arbeitsklima zu spekulieren, sind Konflikte vorprogrammiert. Mit neuen Tools oder Regeln gegenzusteuern, ist zwar löblich – doch einzelne Maßnahmen reichen oft nicht aus. Nur durch ein gelungenes Zusammenspiel von Organisation, Technik und Kultur können Unternehmen und Angstellte gleichermaßen von hybrider Arbeit profitieren.

Organisatorische Voraussetzungen

Die Prozesse, Richtlinien und Management-Methoden bilden häufig noch starre, hierarchische Unternehmen in großen Büros ab – was gar nicht mehr der Fall ist. Stattdessen ist Flexibilität Herzstück der hybriden Arbeit, und zwar nicht nur bei der Wahl der Arbeitszeiten und -orte. Ein modernes Projektmanagement mit Objectives & Key Results (OKR) oder agilen Methoden sorgt dafür, dass die Angestellten ihr individuellen Aufgaben besser eigenständig organisieren können. Eine klare Definition von Rollen und Kompetenzen ist dabei unabdingbar, um die Arbeit im Team fair aufzuteilen. Die Etablierung von Kommunikationsrichtlinien ist ebenfalls wichtig: Gerade in hybriden Teams, die sich nicht jeden Tag an einem

Ort treffen, gilt es, Missverständnisse zu vermeiden und sicherzustellen, dass alle Mitarbeitenden stets auf dem neuesten Informationsstand sind. Auch kleine Neuerungen sollten dabei durch Schulungen und moderne Lernformate an die Mitarbeitenden herangetragen werden. Ohnehin hat lebenslanges Lernen einen festen Platz in modernen Unternehmen. So lassen sich individuelle Stärken jedes Mitarbeitenden kontinuierlich fördern, um das Unternehmen gemeinsam auf neue Herausforderungen vorzubereiten.

Die passenden Tools

Technik und Tools für hybrides Arbeiten sind heute reichlich vorhanden. Manchmal zu reichlich, um einen Überblick zu behalten. Entscheidend ist es, den Mitarbeitenden eine nahtlos integrierte digitale Umgebung zu bieten – bei der es unerheblich ist, wo und wann die Arbeit stattfindet. Ein intelligent vernetzter Arbeitsplatz bietet eine Kombination von Software und Services, die den Arbeitsalltag für alle erleichtern.

- **Infrastruktur:** Neben Laptops und Videokonferenzsystemen ist eine Plattform für den Zugang zu zentralen Daten und Ressourcen und die sichere Datenablagen unerlässlich, etwa über ein ECM-System oder Cloud-Lösungen. Alle Tools müssen miteinander interagieren können, um einen reibungslosen Arbeitsablauf zu gewährleisten.

- **Kollaborationstools:** Moderne Kollaborationstools wie Microsoft 365 ermöglichen eine effiziente Zusammenarbeit. Im Zusammenspiel mit digitalisierten Prozessen und automatisierten Workflows können viele alltägliche Arbeiten reibungslos und fehlerfrei erledigt werden.

- **Datenbasierte Entscheidungen:** Hybride Teams können besser und schneller zusammenarbeiten, wenn sie vorhandener Daten intelligent nutzen. Durch Echtzeit-Auswertungen können Teams schnell auf Marktveränderungen reagieren und fundierte Entscheidungen treffen.

- **Informationssicherheit:** Der Schutz sensibler Daten war nie wichtiger als heute. Neben technischen Schutzmaßnahmen muss aber auch die menschliche Firewall up-to-date sein: Regelmäßige Schulungen der Mitarbeitenden sind für eine umfassende Informationssicherheit unerlässlich.

- **Managed Services:** Auslagerung und Automatisierung von Aufgaben entlasten neben den Teams auch die IT-Abteilungen – ein wirksames Mittel, um Fachkräftemangel und Überlastung entgegenzuwirken.

Eine zeitgemäße Unternehmenskultur

Die organisatorischen und technischen Aspekte sind zwar entscheidend dafür, dass hybrides Arbeiten funktioniert – doch um den Arbeitsalltag wirklich besser für alle zu gestalten, muss auch ein Wandel der Unternehmenskultur spürbar sein. Moderne Unternehmen setzen auf Vertrauen zwischen Führungskräften und Mitarbeitenden, Diversität und Inklusion sowie Delegation von Verantwortung. Auch eine gute Work-Life-Balance trägt zur Zufriedenheit und Produktivität bei, wobei die Einhaltung der Grenzen zwischen Arbeit und Privatleben auch beim mobilen Arbeiten wichtig ist – Stichwort: mentale Gesundheit. Stressmanagement und Gesundheitskurse tragen zusätzlich zur Prävention bei. Ein gutes Arbeitsklima trägt letztendlich zur Resilienz des Unternehmens bei. Flexible und anpassungsfähige Teams sind langfristig belastbarer und können die Herausforderungen der volatilen Geschäftswelt gemeinsam stemmen.

Doping für die Digitalisierung

Die To-do-Liste mag lang erscheinen – doch glücklicherweise müssen die wenigsten Unternehmen bei Null anfangen. Die Grundsteine sind häufig bereits gelegt und mit kleinen Anpassungen geht es einen großen Schritt voran. Es kann sich auszahlen, an der richtigen Stelle kompetente externe Unterstützung zu holen. Zum Beispiel bei der technischen Umsetzung des intelligent vernetzten Arbeitsplatzes: Konica Minolta steht kleinen, mittelgroßen und großen Unternehmen als erfahrener Technologie- und Managed Service Provider zur Seite. Mit Beratung zu einzelnen Tools oder ganzen Digitalisierungsstrategien sowie konkreter Unterstützung bei der Umsetzung von IT-Projekten bringen die Consultants die digitale Transformation voran. Besondere Schwerpunkte bei ECM-Systemen, Cloud Printing, Microsoft 365, Dynamics 365 BC, Power Platform und Teams-Räumen. Auch Informationssicherheit, Mitarbeitenden- und Admin-Schulungen gehören zum Portfolio.

www.konicaminolta.de

CHECKLISTE:
IST IHR UNTERNEHMEN BEREIT FÜR HYBRID WORK?

Finden Sie heraus, ob Ihr Unternehmen bereits die Voraussetzungen für hybride Arbeit erfüllt:

Die Checkliste verschafft Ihnen in wenigen Minuten Klarheit – und einen Überblick zu den wichtigsten Handlungsfeldern.

Data Security & hybrides Arbeiten

SCHWUPPS, SCHON SIND DIE SENSIBLEN DATEN IN DER CLOUD

Private Endgeräte, Cloud-Tools, Ablenkung: Bei der Remote-Arbeit steigt die Gefahr versehentlicher Datenverluste enorm. Mit einer datenzentrierten Komplettlösung für IT-Sicherheit können Unternehmen kritische Informationen überall effizient schützen.

So vorteilhaft das hybride Arbeiten für Mitarbeiter und Unternehmen ist, so problematisch ist es für die IT-Sicherheitsteams. Ihre Aufgabe ist nun schwieriger als jemals zuvor. Im Homeoffice aber auch unterwegs im Café oder Hotel nutzen Mitarbeiter häufig ihre privaten Endgeräte und greifen damit auf geschäftliche Informationen im Internet, in der Cloud oder in On-Premises-Anwendungen zu. Neben offizieller, vom Unternehmen genehmigter Software, verwenden sie außerdem auch häufig private Accounts und Cloud-Tools für die Arbeit. Dadurch vergrößern sich die Angriffsflächen für Cyber-Kriminelle erheblich und Unternehmensdaten sind mehr denn je der Gefahr von Hackerangriffen ausgesetzt.

DATENZENTRIERTE KOMPLETTLÖSUNGEN ERMÖGLICHEN ES, SENSIBLE GESCHÄFTSINFORMATIONEN ÜBERALL EFFIZIENT UND GANZHEITLICH ZU SCHÜTZEN.

Frank Limberger, Data & Insider Threat Security Specialist, Forcepoint, www.forcepoint.com

Risiko für folgenschwere Missgeschicke steigt

Doch damit nicht genug. Das hybride Arbeiten erhöht ein zweites, häufig unterschätztes Risiko: versehentliche Datenverluste durch Missgeschicke von Mitarbeitern. Bereits im Büro ist es wahrscheinlich den allermeisten schon einmal passiert, dass sie in der Hektik des Alltags versehentlich eine vertrauliche Datei per E-Mail an den falschen Empfänger geschickt haben. Unter den Bedingungen des Homeoffice und des mobilen Arbeitens ist das Risiko für solche Unachtsamkeiten noch einmal deutlich höher.

Das liegt zum einen daran, dass Remote-Mitarbeiter ihre private IT für Geschäftszwecke nutzen, zum anderen fehlt ihnen durch die Vermischung von Arbeits- und Privatleben aber auch vielleicht einfach manchmal die nötige Aufmerksamkeit. Da kann es schnell passieren, dass sie ein Dokument mit personenbezogenen Daten in eine außereuropäische Cloud hochladen, eine Datei mit wertvollen Technologieinformationen unverschlüsselt auf einen USB-Stick kopieren oder ein sensibles Dokument zuhause ausdrucken und offen herumliegen lassen. Kommt es durch solche Nachlässigkeiten zu Verstößen gegen Datenschutzregularien wie der DSGVO, drohen Unternehmen empfindliche Bußgelder. Gelangt geistiges Eigentum in falsche Hände, kann das im schlimmsten Fall sogar die Existenz von Unternehmen gefährden.

Mitarbeiter mit geeigneten Systemen unterstützen

IT-Sicherheitsteams müssen sensible Geschäftsdaten deshalb vor folgenschweren Missgeschicken und Versehen der Mitarbeiter schützen. Ein wichtiges Instrument dafür sind Sicherheitsschulungen. Die Mitarbeiter sollten regelmäßig dafür sensibilisiert werden, welche Daten besonders schützenswert sind und welcher Umgang ein Risiko darstellt. Die Gefahr von Fehlern oder Unachtsamkeiten bleibt dennoch bestehen. Deshalb sollten IT-Sicherheitsteams die Mitarbeiter zusätzlich mit geeigneten Systemen unterstützen. Es kommt schließlich auch kein Unternehmen auf die Idee, auf einen Malware-Schutz zu verzichten, nur weil die Mitarbeiter geschult sind und eigentlich wissen sollten, auf welche Dateianhänge und Links sie nicht klicken dürfen.

Zum Schutz vor versehentlichen Datenverlusten stellt der IT-Sicherheitsmarkt spezielle Lösungen für Datensicherheit zur Verfügung. Solche Systeme 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 jeweiligen Kontext angemessen sind.

Damit helfen sie den Mitarbeitern beim Umgang mit Daten bessere Entscheidungen zu treffen und bewahren sie vor folgenschweren Fehlern. Das tun sie bei-

spielsweise durch das Aufpoppen einer Warnmeldung, wenn jemand im Begriff ist, kritische Daten zu versenden, in eine Public Cloud hochzuladen, zu kopieren oder auszudrucken. So verhindern sie den ungewollten Abfluss von Daten, ohne die Produktivität der Mitarbeiter unnötig einzuschränken. Sie können weiterhin moderne Cloud-Tools und ihre private IT nutzen und das sollen sie auch, denn durch sie wird ein effizienter hybrider Arbeitsalltag überhaupt erst möglich.

Heterogene Umgebungen fordern IT-Sicherheitsteams heraus

Beim Einsatz einer Software für Datensicherheit stellen aber die heterogenen und komplexen Umgebungen eine große Herausforderung dar. IT-Sicherheitsteams müssen die sensiblen Geschäftsdaten über On-Premises, Cloud, Web, gemanagte und ungemanagte Geräte hinweg schützen. Diese Herausforderung können sie am besten mit einer datenzentrierten All-in-One-Sicherheitsplattform aus der Cloud meisten. Der IT-Security-Markt stellt inzwischen zunehmend Komplettlösungen zur Verfügung, die es Unternehmen ermöglichen, alle benötigen Sicherheitsfeatures aus einer Hand als Service zu abonnieren und integriert zu nutzen. Bei datenzentrierten Komplettlösungen bildet dabei Software für Datensicherheit eine Schlüsselkomponente, die in Technologien wie Cloud Access Security Broker (CASB), Secure Web Gateway (SWG) und Zero Trust Network Access (ZTNA) integriert ist.

Solch eine Lösung befreit IT-Sicherheitsteams davon, zum Schutz der Daten für die unterschiedlichen Kanäle separate, voneinander losgelöste Punktlösungen zu nutzen, die alle ihre eigenen Managementoberflächen mit individueller Logik mitbringen. Die Folge davon wäre nicht nur eine äußerst komplizierte Verwaltung, sondern auch Inkonsistenz. Denn in unterschiedlichen Tools können IT-Security-Teams meist keine identischen Sicherheitsrichtlinien einrichten und müssen sich mit Policies zufriedengeben, die lediglich ähnlich sind. Datenzentrierte Komplettlösungen ermöglichen es ihnen dagegen, sensible Geschäftsinformationen überall effizient und ganzheitlich zu schützen. Sie können sämtliche Vorgaben mit einem einzigen Satz an Sicherheitsrichtlinien in einer einzigen Managementkonsole zentral verwalten und in der kompletten IT-Landschaft durchsetzen: von gemanagten und privaten Endgeräten bis hin zu Websites, Cloud-Diensten, Netzwerken, E-Mail-Systemen und On-Premises-Anwendungen.

Keine Angst vor ausufernden Projekten

Ausufernde Einführungsprojekte brauchen Unternehmen ebenfalls nicht zu fürchten. Sie müssen nicht zwangsläufig umfangreiche Dateiklassifizierungen vornehmen und viele Richtlinien ausarbeiten. Geeignete Lösungen können über Schnittstellen auf andere Sicherheitstools zugreifen, die bereits Datenklassifizierungen vorgenommen haben und bringen auch schon ab Werk ein großes Set an vordefinierten Richtlinien mit.

Die Mitarbeiter wiederum müssen keine Angst vor Überwachung haben. Natürlich sind übergreifende Auswertungen möglich und auch sinnvoll, um zu erkennen, ob Richtlinien angepasst werden sollten. Diese Auswertungen lassen sich aber anonymisiert durchführen, denn für das Unternehmen ist es unbedeutend, welcher Mitarbeiter versehentlich Daten in die Cloud hochladen möchte, die dort nicht hingehören. Entscheidend ist allein, es zu verhindern.

Frank Limberger

Mehr Nachhaltigkeit wagen

DIGITALER ZWILLING TRIFFT AUF TRIPLE BOTTOM LINE

Um den eigenen ökologischen Fußabdruck zu reduzieren, sind Unternehmen auf effiziente und ressourcenschonende Prozesse angewiesen. Ein digitaler Zwilling hilft nicht nur bei der Umsetzung, er unterstützt auch den ganzheitlichen Nachhaltigkeitsansatz nach dem Konzept der Triple Bottom Line.

Während sich viele Unternehmen und Organisationen gerne ein umweltschonendes und verantwortungsvolles Image in der Öffentlichkeit zuschreiben wollen, stoßen nicht wenige bei der praktischen Umsetzung schnell an ihre Grenzen. Was viele nicht bedenken: Wirkliche Nachhaltigkeit besteht nicht nur aus einzelnen Aspekten wie dem Beziehen von grünem Strom. Vielmehr setzt sie sich nach dem Konzept der Triple Bottom Line (TBL) aus drei zentralen Dimensionen zusammen: ökologisch, sozial und ökonomisch. Die Theorie geht auf den Vordenker John Elkington zurück und gründet sich auf der Idee, dass nur eine ganzheitliche Betrachtung der drei Dimensionen zu einem nachhaltigen Handeln im Einklang mit unternehmerischem Erfolg führt. Nach Elkington besitzen Unternehmen in ihrem Einflussbereich damit eine Verantwortung für die drei Ps – People (Menschen), Planet (Umwelt) und Profit (Gewinn). Eine große Aufgabe, bei deren Lösung moderne Technologie eine tragende Rolle spielt.

Digitaler Zwilling für mehr Nachhaltigkeit

Ein Konzept, das dabei immer mehr in den Fokus der Aufmerksamkeit rückt, ist der digitale Zwilling. Dabei übertragen Unternehmen mit Hilfe von Daten und Algorithmen die reale Welt in eine virtuelle – auf diese Weise können sie nicht nur Maschinen überwachen, sondern auch die Produktion sowie einzelne Prozesse effizienter gestalten und im Ergebnis Ressourcen einsparen. Digitale Zwillinge können sehr gewinnbringend sein, weil sie die Umweltauswirkungen eines Produkts, einer Anlage oder eines Prozesses simulieren und optimieren, bevor diese ihre Arbeit aufnehmen oder bereits in Betrieb sind. Je effektiver die Prozesse geplant und umgesetzt sind, desto mehr können Unternehmen Aspekte wie Energiekonsum, Materialverbrauch oder Produktionsabfall durch eine Analyse reduzieren. Aber auch bei etablierten Betriebsabläufen helfen in Echtzeit gesammelte Daten bei der Ressourcenoptimierung, zum Beispiel bei der Kreislaufwirtschaft oder der Predictive Maintenance, also der vorausschauenden Wartung von Geräten, um mittels der Analyse von Maschinen- und Produktionsdaten Ausfallzeiten zu vermeiden und Qualitätsstandards zu halten. Auch mit Blick auf die zukünftige Verpflichtung zum Verfassen von ESG-Reportings (Environmental, Social and Governance) können sich Digitale Zwillinge als nützlich erweisen, indem sie benötigte Daten zur Verfügung stellen und Prozesse transparenter machen. Umgekehrt eignen sich aber auch zentrale Datenbanken mit den gesammelten Nachhaltigkeitsdaten eines Unternehmens hervorragend als Grundlage für den Bau eines Digitalen Zwillings.

Fazit

Digitale Zwillinge sind ein wirkungsvolles Werkzeug in einer wachsenden Sammlung von Technologien und Konzepten für mehr Nachhaltigkeit. Richtig eingesetzt handelt es sich bei der Technologie um einen machtvollen Hidden Champion, der trotz seines großen Potenzials bislang noch verhalten in der Praxis zum Tragen kommt – zu Unrecht, denn das Konzept öffnet Unternehmen jeglicher Größer völlig neue Wege.

Frank Sent, www.cgi.com/de

- Aufdecken von Schwachstellen
- Optimierung von Maschinen/Prozessen
- Risiken minimieren
- Produktionseffizienz steigern
- Umweltauswirkungen reduzieren
- Predictive Maintenance
- Downtime minimieren
- Qualitätsstandards halten

Die virtuelle Repräsentation von physischen Maschinen und Prozessen hilft Unternehmen dabei, Nachaltigkeitsziele zu erreichen und effizienter zu arbeiten.
(Quelle: CGI)

Nachhaltigkeit & Innovationen

DER MITTELPUNKT DER UNTERNEHMENS-DNA

Nachhaltigkeit ist mehr denn je ein wesentlicher Faktor für die Kaufentscheidung. Dies gilt für Unternehmen, Behörden und Privatpersonen, wie fast zwei Drittel der Befragten in einer aktuellen Deloitte Studie angeben. Mehr denn je sind in Ausschreibungen klar messbare Nachhaltigkeitskriterien enthalten.

Für HP, einen der führenden Anbieter von PCs, Notebooks und Druckern, ist Nachhaltigkeit seit Jahrzehnten fester Bestandteil der Unternehmens-DNA. Das Unternehmen hat klare Nachhaltigkeitsziele und dokumentiert seit Mitte der 90er Jahre die eigenen Aktivitäten in einem Nachhaltigkeitsreport. Als eines der ersten IT-Unternehmen veröffentlicht HP einen Report zum Thema „Menschenrechte". Entsprechend geht es in den Unternehmenszielen auch um die soziale Nachhaltigkeit in der Lieferkette – den Schutz von Menschenrechten und gute Arbeitsbedingungen.

Dabei hat HP sich ehrgeizige Ziele gesetzt. Allen voran bis 2030 das nachhaltigste und gerechteste Technologieunternehmen weltweit zu werden und den Anteil von recycelten, erneuerbaren und wiederverwerteten Materialien in Produkten und Verpackungen auf 75 Prozent zu steigern – aktuell liegt der Anteil bereits bei rund 45 Prozent. Mehr noch: Nachhaltigkeit wird bereits in der Entwicklung neuer Produkte berücksichtigt. Unabhängig bestätigt wird das Engagement durch die Vielzahl an Zertifizierungen der Produkte mit Umweltsiegeln wie dem Blauen Engel, Energy Star oder dem TCO-Certified Siegel. Die Liste der Kriterien, die für die Auszeichnung mit einem dieser Siegel erfüllt werden muss, schließt eine umweltschonende Produktion unter Einhaltung klarer sozialer Standards ebenso ein wie die Schadstoffarmut, geringe Lärmemissionen, Energieverbrauch und den Einsatz von umweltverträglichen Bauteilen.

Insbesondere bei Verbrauchsmaterialien – also vor allem bei Tintenpatronen und Tonerkartuschen – ist HP einer der Vorreiter moderner Kreislaufwirtschaft. Im Planet Partners Programm wurden seit 1991 mehr als 875 Millionen Original HP Tintenpatronen und Tonerkartuschen recycelt.

HP EvoCycle Tonerkartusche

Mit den EvoCycle-Tonerkartuschen bietet HP Behörden und Unternehmen erstmals eine runderneuerte Kartusche in HP Qualität an. Eine „EvoCycle"-Kartusche enthält nach Gewicht derzeit rund 21 Prozent wiederverwendete Teile und 24 Prozent recycelte Bestandteile. Dabei besteht das recycelte Material zu 100 Prozent aus recyceltem Kunststoff aus dem HP Kreislauf. Es wird kein neuer Kunststoff hinzugefügt. Der Rest sind hauptsächlich „bildgebende" Komponenten. Diese Bestandteile der Tonerkartuschen werden grundsätzlich erneuert, um die hohen Anforderungen an die Qualität der Kartuschen – und damit der Ausdrucke – sicher zu stellen. Das bedeutet gleichermaßen, dass die Drucker in Kombination mit EvoCycle-Tonerkartuschen weiterhin die Anforderungen der Zertifizierung für den „Blauen Engel" sowie die für die Dokumentenechtheit nach DONot erfüllen.

Die runderneuerten EvoCycle-Kartuschen werden regional in einer Produktionsanlage in Liffré in der Bretagne hergestellt und unterliegen den gleichen Qualitätskontrollen wie alle Original HP-Kartuschen. Dank der Wiederverwertung der Bauteile lässt sich die CO_2-Belastung um 43 Prozent im Vergleich zu herkömmlichen Produktreihen reduzieren. Damit sind die EvoCycle-Kartuschen gleich doppelt nachhaltig: durch die Wiederverwertung von Komponenten sowie durch einen reduzierten CO_2-Abdruck bei der Herstellung. Ein wichtiger Schritt zu einer nachhaltigen Kreislaufwirtschaft.

www.hp.com

Digitale Transformation 2.0

MIT STRATEGIE ZUM NACHHALTIGEN ERFOLG

Seit zwei bis drei Dekaden gibt es technologiegetrieben immer wieder neue Phasen der digitalen Transformation. Dabei sind zahlreiche Insellösungen entstanden. Viele Unternehmen stehen jedoch noch vor der Herausforderung einer ganzheitlich geplanten digitalen Ende-zu-Ende-Transformation. it management sprach mit Martin Tydecks, Geschäftsführer der kobaltblau Management Consultants GmbH, über die Herausforderungen der digitalen Transformation.

it management: *Herr Tydecks, was bedeutet für Sie Digitale Transformation 2.0 und welche Erfahrungen haben Sie in Ihren Projekten gemacht?*

Martin Tydecks: Viele CIOs verantworten heute parallel Legacy-, hybride und zum Teil Cloud-IT-Landschaften. Einzelne Fachbereiche oder Organisationeinheiten arbeiten mit ihren digitalen Silos sehr erfolgreich. Sie sind aber untereinander maximal über Schnittstellen verbunden. Das war Digitale Transformation 1.0. Eine nahtlos digitale Transformation aller Prozesse haben bisher die wenigsten Unternehmen geschafft, was den Begriff der Digitalen Transformation 2.0 grob umreißt. Dabei geht es nun um ein Gesamtkunstwerk einer Ende-zu-Ende gedachten, strukturierten und agil arbeitenden Organisation mit einer durchgängig konsistenten digitalen Strategie. Das ist die nächste Evolutionsstufe der Digitalisierung, die nach unserer Erfahrung viele Unternehmen jetzt anstreben.

it management: *Warum ist eine solche Gesamtstrategie für die nächste Evolutionsstufe so wichtig?*

Martin Tydecks: In vielen Unternehmen besteht kein gemeinsames Verständnis darüber, welche internen und externen Prozesse schrittweise digitalisiert werden sollten, um zu diesem genannten Gesamtkunstwerk einer Ende-zu-Ende gedachten Digitalisierung zu kommen. Es fehlen oft strategische Begründungen dafür, warum und wie das Unternehmen durch eine konsequente Digitalisierung in seinem Markt bestehen und wachsen möchte, und welchen Nutzen dies für welche Zielgruppen hat. Manchmal haben sich Unternehmen unstrukturiert entlang verschiedener Digitalisierungsprojekte entwickelt. Irgendwann stellen das Management und die CIOs fest, dass es außer Schnittstellen und digitalisierten Insellösungen keine gemeinsam getragene Digitalstrategie gibt. Oftmals stoßen die Unternehmen nun an die Grenzen, die weitere Entwicklung ihrer Geschäftsfähigkeiten mit IT-Lösungen effizient zu beschleunigen.

it management: *Was führt eine Digitale Transformation 2.0 zum nachhaltigen Erfolg?*

Martin Tydecks: Ausgangspunkt für eine Digitale Transformation 2.0 sollte immer eine Strategie sein, die unterschiedlich heißen kann: Business-Strategie, IT-Strategie oder Digital-Strategie. Hauptsache, sie verfolgt einen holistischen Ansatz. Genau den verfolgen wir, in dem wir zunächst den digitalen Reifegrad unseres Kunden ermitteln. Das ist der erste von vier Schritten, die wir systematisch mit unseren Auftraggebern gehen. Sie bilden eine zielfokussierte Systematik mit Kontrollinstanzen, die den nachhaltigen Erfolg gewährleisten.

it management: *Wie ermitteln Sie den digitalen Reifegrad eines Unternehmens?*

Martin Tydecks: Wir definieren mit unseren Auftraggebern und seinen internen Stakeholdern zunächst Eingangsparameter und Business Funktionen, also Messgrößen. In Workshops, Interviews, Umfragen und Dokumentenanalyse messen wir dann, auf welchem Stand sich das Unternehmen bei diesen Parametern befindet.

Diese Parameter können sich abhängig vom jeweiligen Unternehmen auf das Geschäftsmodell, das Ökosystem beziehungsweise die Marktsicht mit Wettbewerb und Kundensegmenten, Produkte und Services, Aufbau und Ablauforganisation beziehen. Wo kommt der Kunde her, wo will er hin. Eine wichtige Größe ist dabei die digitale Ambition, also was soll erreicht werden. Auch Technologien, die aktuell und künftig zum Einsatz kommen sollen, spielen auf diesen Workshops bereits eine gewisse „enablement"-Rolle.

it management: *Wie geht es nach der Reifegrad-Analyse weiter?*

Martin Tydecks: Zusammen mit den wichtigsten Stakeholdern im Unternehmen entwickeln wir im zweiten Schritt mit einem iterativen Vorgehen basierend auf dem Design Thinking-Ansatz die neue Strategie. Diese Arbeit muss durch unseren Kunden unter unserer Anleitung geleistet werden. Sonst kann es zu einem Phänomen kommen, das früher viele Unternehmen schmerzvoll erlebten. Die Kurzfassung: „Not invented here." Das bedeutet, dass Mitarbeitende die neue Strategie und die daraus abgeleiteten Vorgaben, Prozesse und Tools weder verstehen und akzeptieren noch mit Leben füllen konnten.

it management: *Wie können Ihre Auftraggeber dieses Phänomen verhindern?*

Martin Tydecks: Durch die Beteiligung aller wichtigen Akteure im dritten Schritt unserer Arbeit. Wir nennen sie Matchmaking und Priorisierung. Dabei erarbeiten sie Ansätze, wie die Strategie heruntergebrochen werden kann, und skizzieren Initiativen für die Umsetzung. Wir moderieren dabei den Prozess der Einordnung, also welche Digitalisierungsinitiative sich auf welche Parameter auswirkt und welche Kompetenzen und Zeit, welches Budget und Kapazitäten dafür bereitgestellt werden müssen. Wir legen eine Reifegradlogik und Kontrollschleifen an, die im vierten Schritt die Umsetzung erleichtern und den Erfolg nachhaltig gewährleisten.

DIE DIGITALEN TRANSFORMATION IST EIN DAUERZUSTAND, DEN DIE UNTERNEHMEN AM BESTEN BEWÄLTIGEN, DIE AGIL STRUKTURIERT UND DIGITAL ORGANSIERT SIND.

Martin Tydecks, Geschäftsführer, kobaltblau Management Consultants GmbH, www.kobaltblau.de

it management: *Wer übernimmt die Projektsteuerung?*

Martin Tydecks: Wir etablieren für den vierten Schritt der Umsetzung mit unserem Auftraggeber ein Team, das als zentrales Transformation Management Office (TMO) sowohl Business- als auch IT-Manager:innen umfasst. Es treibt unter unserer anfänglich intensiveren Anleitung und später abnehmenden Moderation schrittweise die Implementierung voran. Es monitort den Fortschritt der einzelnen Transformationsinitiativen. Es dokumentiert und strukturiert den Prozess, sodass er nachhaltig verständlich wird. Wir achten vor allem darauf, dass wirklich alle betroffenen Stakeholder aktiv in den Prozess eingebunden sind, um den „Not invented here"-Effekt auf allen Ebenen zu verhindern.

it management: *Welche Rolle hat das TMO und wie arbeitet es?*

Martin Tydecks: Das TMO nimmt in der Transformation eine kontrollierende und coachende Rolle ein. Es sorgt für ein übergreifendes Kommunikations- und Veränderungsmanagement. Das TMO bereitet monatliche Statusmeetings vor, bei denen der Fortschritt jeder einzelnen Initiative gemessen wird. Was hat sich verändert, wo hakt es noch, wo fehlen Ressourcen oder Kompetenzen? Mit einem speziellen Value-Tracking messen wir die Ergebnisse und den Wertbeitrag und machen dadurch den Benefit der Transformation für alle Beteiligten transparent. Einmal im Quartal analysieren wir ein bis zwei Initiativen in einem detaillierten Review. Bei unserem letzten Kunden haben wir diese Analyse „Initiative Health Check" genannt. Analog zu einem Sprint in der SCRUM-Welt sollen diese Deep Dives zeigen, ob und welchen Wertbeitrag diese Initiativen für den gesamten Transformationsprozess bereits leisten und was das für das Gesamtprojekt bedeutet.

it management: *Wann ist so ein Transformationsprozess abgeschlossen oder beendet?*

Martin Tydecks: So schnell heute neue Multi-Krisen, Nachfragetrends und Technologiesprünge aufeinander folgen, ist ein Unternehmen heute immer in einem Transformationsprozess. Einige unserer Kunden machen das TMO deshalb auch zu einer Dauereinrichtung. Das ist auch die wichtigste Erkenntnis einer Digitalen Transformation: Sie ist ein Dauerzustand, den die Unternehmen am besten bewältigen, die agil strukturiert und digital organsiert sind und schneller als früher auf Veränderungen reagieren kann. Wir haben dann einen guten Job gemacht, wenn wir dafür nicht mehr gebraucht werden.

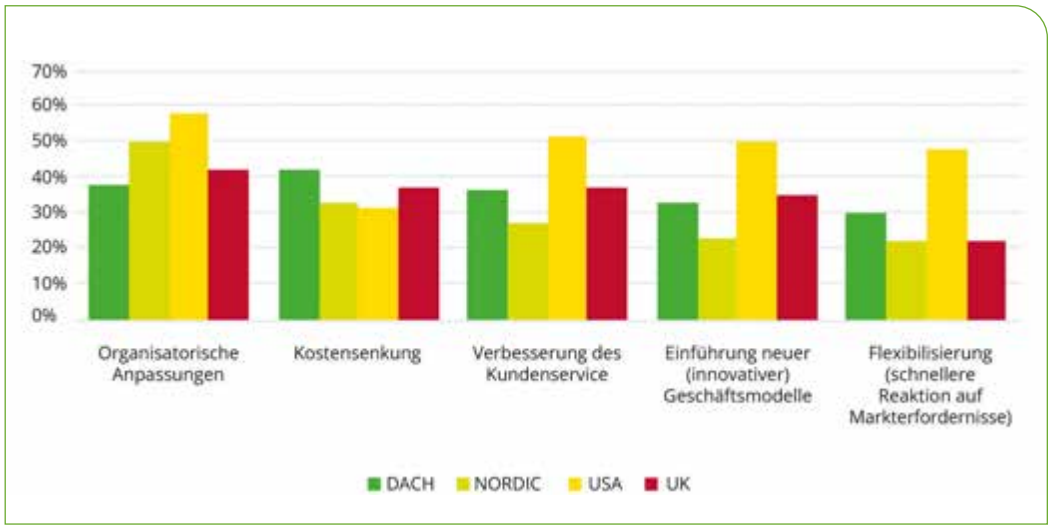
it management: *Herr Tydecks, wir danken für dieses Gespräch.*

Transformationsstudie

DEUTSCHE UNTERNEHMEN DIGITALISIEREN FÜR MEHR WIRTSCHAFTLICHKEIT – AMERIKANER STREBEN NACH INNOVATION

Strukturelle Marktveränderungen, neue Business-Chancen, Wünsche der Mitarbeiter und Kunden oder der stetig wachsende Anspruch an Wirtschaftlichkeit und Rentabilität – das alles sind maßgebliche Treiber der Digitalisierung. Für viele Unternehmen, die die Innovationskraft des digitalen Universums für ihren Erfolg nutzen, ist jetzt die Zeit gekommen, ihre Systeme aus unterschiedlichsten Gründen auf den neusten Stand zu bringen. Eine aktuelle, international angelegte Studie der Natuvion und NTT DATA Business Solutions gibt einen detaillierten Überblick über die Herausforderungen, regionalen Unterschiede, Rahmenbedingungen, Erfolge und Stolpersteine der digitalen Transformationsinitiativen.

Eines der zentralen Ergebnisse der Studie: Es bestehen zwischen den Ländern in Europa und im Vergleich von Europa zu den USA gravierende Unterschiede bei den technischen Voraussetzungen, dem Fachwissen und der Verfügbarkeit von Experten sowie in den Zielen einer digitalen Transformation. Ein Beispiel: In Europa durchlaufen Unternehmen die digitale Transformation mehrheitlich, um wirtschaftlicher zu sein und Kosten zu sparen. In den USA hingegen steht die Innovation im Fokus.



Insgesamt 630 Unternehmen weltweit haben Natuvion und die NTT DATA Business Solutions in den zurückliegenden Monaten einer repräsentativen Befragung unterzogen. Die meisten der weltweit befragten Führungskräfte nannten als Hauptgrund für die Transformation die

Die fünf meistgewählten Gründe einer Transformation

organisatorische Anpassung ihres Unternehmens. Gleich danach argumentieren 42 Prozent der deutschen Vertreter mit der Senkung von Kosten. In Amerika ist dieser Aspekt nur für ein Drittel der Unternehmen relevant. Hier sorgt man sich eher, dass man unter inkompatiblen Systemen leiden könnte, wenn man sich der Digitalisierung verschließt. Das befürchten immerhin 53 Prozent der amerikanischen Probanden. Die Hälfte (50 Prozent) der US-Unternehmen glauben zudem, innovative Geschäftsmodelle durch die Transformation zu ermöglichen und 51 Prozent sehen in der Transformation eine Chance für einen besseren Kundenservice.

Ziel nicht erreicht

Auch wenn die Unternehmen die Digitalisierung engagiert in Angriff nehmen, sind sie nicht automatisch erfolgreich. Aus weltweiter Perspektive gaben lediglich 62 Prozent an, ihre Ziele vollständig erreicht zu haben – in der DACH-Region waren es sogar nur 55 Prozent, hingegen in den USA enorm hohe 82 Prozent. Diese große Varianz lässt unterschiedliche Ursachen vermuten:

#1 Die Transformation wurde unterschätzt

Schon bei der Planung ist den meisten befragten Führungskräften die herausfordernde Komplexität des Projektes klar. Das ist in Kombination mit dem fehlenden Fachpersonal und damit einhergehendem Know-how-Mangel keine leichte Situation. Überrascht waren viele Führungskräfte zudem über das fehlende Transformationswissen der Verantwortlichen und die schlechte Datenqualität der Systeme. Diese lag zusammen mit den fehlenden Ressourcen auf Platz 2 der „unangenehmen Überraschungen" während des Transformationsprozesses. Bei der Frage danach, was man bei einem zukünftigen Digitalisierungsprojekt besser machen könnte, waren drei der wichtigsten Vorsätze „mehr Ressourcen einzuplanen", „für das Projekt mehr Zeit einzuplanen" und „sich früher mit der Thematik zu befassen".

#2 Das Housekeeping war nicht gründlich genug

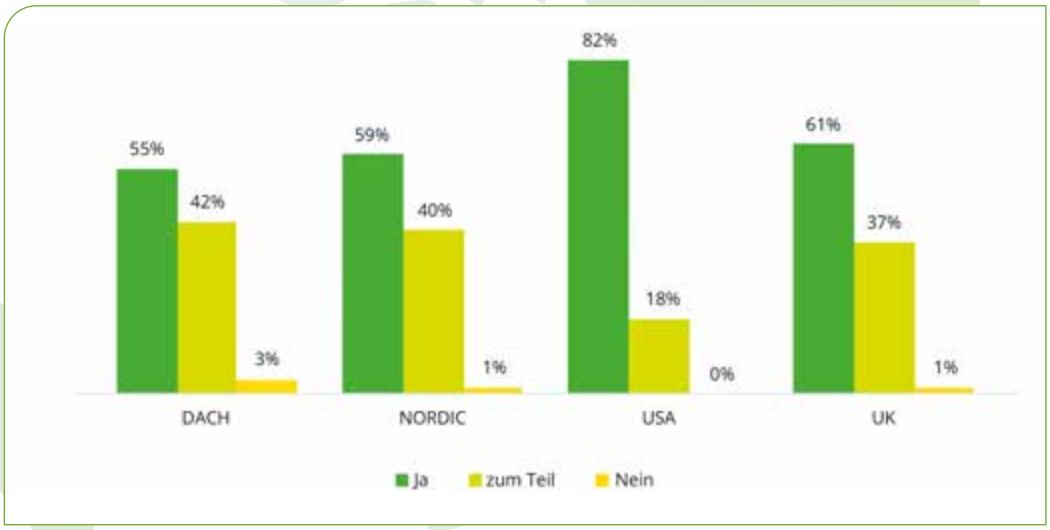
Unwissenheit schützt vor Strafe nicht – aber Wissen führt auch nicht automatisch zum Erfolg. So könnte man die Momentaufnahme zum Thema Housekeeping überschreiben. Zwar nannten die Unternehmen auf die Frage nach den Erfolgsfaktoren der Transformation die „Prüfung der Datenqualität" und die „Bestandserfassung". Aber augenscheinlich entpuppte sich erst während des Transformationsprozesses, wie schlecht die eigenen Daten faktisch sind. Nur so lässt sich erklären, dass die Befragten auf die Frage, was sie am meisten im Laufe des Transformationsprojektes überraschte, die schlechte Datenqualität nannten. In Deutschland belegt die schlechte Datenqualität mit 35 Prozent sogar mit Abstand den ersten Platz bei den „unliebsamen Überraschungen".

#3 Mangel an Transformations-Know-how

In der Studie wird deutlich, dass es an Ressourcen und Know-how fehlt. Über fehlendes Transformationswissen klagen insgesamt 40 Prozent – in den USA sogar 50 Prozent. Auf die Frage, welche organisatorische Aufgabe erfolgskritisch für das Transformationsprojekt war, nannten weltweit 46 Prozent den Aufbau neuer Kompetenzen. In der DACH-Region lag der Wert bei 54 Prozent – in Deutschland bei 57 Prozent. Die Folge: 33 Pro-

ES BESTEHEN IM VERGLEICH VON EUROPA ZU DEN USA GRAVIERENDE UNTERSCHIEDE BEI DEN TECHNISCHEN VORAUSSETZUNGEN, DEM FACHWISSEN UND DER VERFÜGBARKEIT VON EXPERTEN SOWIE IN DEN ZIELEN EINER DIGITALEN TRANSFORMATION.

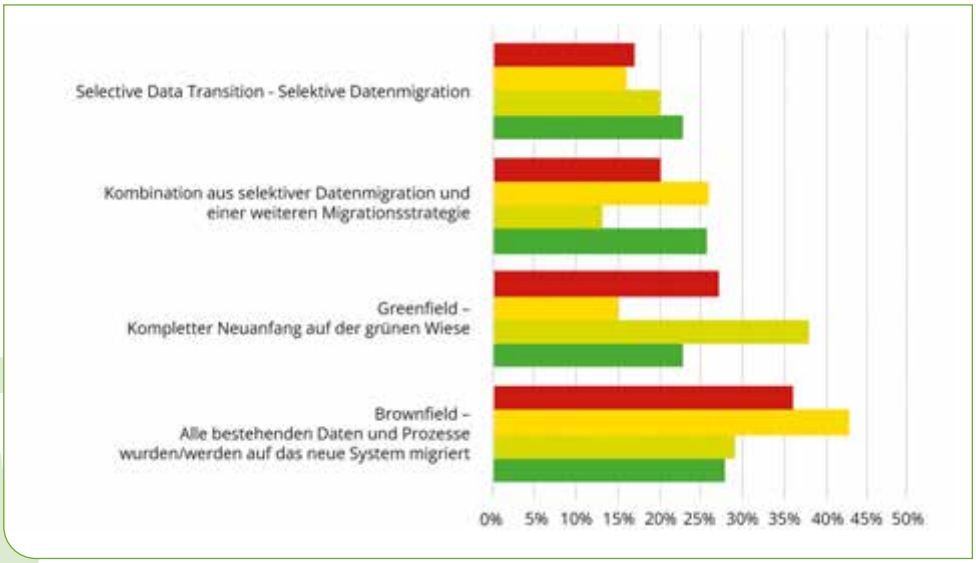
Philipp von der Brüggen, CMO, Natuvion GmbH, www.natuvion.com



Erreichung der Transformationsziele

zent der befragten Unternehmen weltweit zogen externe Berater hinzu. In DACH setzen 27 Prozent auf Hilfe von außen und in den USA 51 Prozent.

Dass es für die digitale Transformation wichtige Gründe gibt, belegt die Studie deutlich: 35 Prozent der weltweit Befragten gaben an, ihre Transformationsprojekte aufgrund der politischen Ereignisse höher priorisiert oder vorgezogen zu haben. Beschleunigend haben sich die politischen Turbulenzen insbesondere in den USA (46 Prozent) und in Großbritannien (42 Prozent) ausgewirkt. In der DACH-Region scheint die Resilienz höher zu sein. Hier hatten die Ereignisse der letzten Jahre weniger Einfluss auf die Transformations-Agenda der Unternehmen.



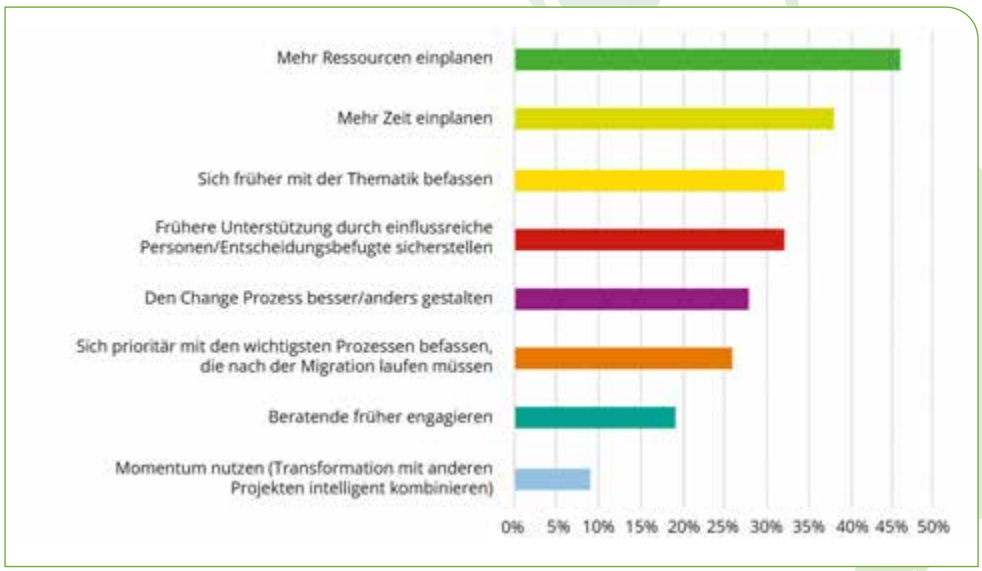
Migration mit der richtigen Methode

Eine Transformation bringt potenziell auch Betriebsunterbrechungen mit sich. Umso wichtiger ist es, sich rechtzeitig mit dieser Herausforderung auseinanderzusetzen. In der DACH-Region gaben 57 Prozent an, dass sie sich maximal eine Unterbrechung von wenigen Stunden vorstellen könnten. Wer für sein Unternehmen die am besten passende Migrationsmethode auswählt, ist in der Lage, die Unterbrechung sehr klein zu halten.

Laut Studie wird die Brownfield-Methode, bei der alle bestehenden Daten und Prozesse migriert werden, weltweit von 32 Prozent eingesetzt. Dies ist erstaunlich, da mit dieser Methode eine eher geringe Wertschöpfung von neuen Systemen erreicht wird. Auch hier unterscheiden sich die Regionen deutlich. In DACH verfolgen die Brownfield-Methode lediglich 28 Prozent, in den USA hingegen 43 Prozent. Dies könnte ein Hinweis darauf sein, weshalb die US-Unternehmen eine vergleichsweise hohe Erfolgsquote bei technischen Transformationen bestätigen. Auf einen kompletten Neuanfang mit der Greenfield-Methode setzen aus internationaler Perspektive 27 Prozent. Etwa ein Fünftel der Befragten kombiniert eine selektive Datenmigration mit der Brownfield- oder Greenfield-Methode und 21 Prozent setzen ausschließlich auf eine selektive Datenmigration.

Bevorzugte Migrationsstrategie

Vor dem Hintergrund, dass knapp 20 Prozent aller Unternehmen sagen, dass sie sich keine Unterbrechung ihres Betriebs leisten können ohne spürbare Konsequenzen für den Geschäftsbetrieb zu erleiden, ist die Wahl der Migrationsmethode ein erfolgskritischer Transformationsfaktor.



Alles in allem zeigen die Ergebnisse der Studie, dass die digitale Transformation weltweit in vollem Gange ist, es aber durchaus signifikante Unterschiede zwischen den Ländern gibt. Zudem besteht Optimierungspotenzial bei der Planung, der Datenqualität und nicht zuletzt dem Transformations-Know-how.

Philipp von der Brüggen, CMO

Was würden Sie heute im Rahmen des Transformationsprozesses anders machen?

OFFICE 4.0

NEW WAYS OF WORKING

New Work war gestern, Office 4.0 ist heute. Doch was verbirgt sich hinter diesem Begriff? Zunächst einmal: Office 4.0 hat absolut nichts mit Microsoft Office zu tun. Vielmehr stellt Office 4.0 eine neue Ära dar, in der Technologie und menschliche Interaktion zusammenkommen, um die Produktivität, Effizienz und Arbeitsqualität zu verbessern. Dabei umfasst der Begriff eine breite Palette von Aspekten, die sowohl die physische als auch die virtuelle Arbeitsumgebung betreffen. New Work, Hybrid Work oder Coworking Spaces decken dabei nur einen kleinen Teil ab. Office 4.0 spielt in den verschiedensten Unternehmensbereichen eine wichtige Rolle, angefangen in der IT, über Human Resources bis hin zum IT Service Management.

Wie Office 4.0 die Potenziale der digitalen Transformation und die Art und Weise, wie wir arbeiten, verändern kann, lesen Sie in diesem eBook.

Office 4.0 – Inhalt

- Unified Endpoint Management wörtlich genommen
- Nachhaltigkeit: Besser gebraucht!
- Future Skills to go!
- Office 4.0 & Self Service-Portale
- Zeiterfassung in Zeiten von New Work
- Führungskräfte, erweitert euren Horizont!
- Das Jahr für smarte Teamplayer
- Workation: what's that?
- Die Zukunft der Arbeitswelt baut auf Vertrauen
- Grundlegende Veränderungen:
- New Work & KI
- What's about Office 4.0?
- Neue Studien zu Hybrid Work und Women in Workplace

Das **eBook** umfasst 48 Seiten und steht zum kostenlosen Download bereit.
www.it-daily.net/download

SNP Transformation World 2023

CHANGE MANAGEMENT UND INNOVATION IN DER PRAXIS

Rund 1.100 Teilnehmende, fast 150 Vorträge zu Themen wie S/4HANA-Migration, M&A-Transformationsprozesse, Nachhaltigkeit in der Wertschöpfungskette oder Integration von Cloud und KI, darunter zahlreiche Praxisberichte von SNP-Kunden – das war die SNP Transformation World 2023 am 14. und 15. Juni in Heidelberg.

„Explore New Horizons" – das Konferenzmotto bringt auf den Punkt, worum es im Kern ging: Veränderung und wie sich diese im Business effektiv umsetzen lässt. Und auch der Eröffnungssong der Konferenz – eine der Top-5-SAP-Konferenzen europaweit, wie CEO Dr. Jens Amail bei seiner Keynote erklärte – gab diesen Sound vor: „Changes" von David Bowie.

Dass sich Veränderung nicht ausschließlich auf technologischen Wandel beschränkt, zeigte die Transformation World ganz klar. Change Management auf strategischer Ebene war ein Kernaspekt zahlreicher Vorträge, denn letztlich geht es immer wieder darum, dass technische Fähigkeiten und Projektmanagement gut zusammenspielen.

Passend dazu führte Carsten Bange, CEO und Gründer von BARC, aus, wie sich eine echte Datenkultur im Unternehmen etablieren lässt. Die Experten des Analystenhauses haben dazu ein sechs Punkte umfassendes Rahmenwerk erstellt: Data Access, Data Leadership, Data Governance, Data Communication, Data Literacy und Data Strategy sind demnach die entscheidenden Eckpunkte zum strategischen Aufbau einer Datenkultur. Lediglich zwischen einem Drittel und einem Fünftel der Teilnehmenden an einer aktuellen Befragung durch BARC hat einen diese Punkte jedoch erst implementiert.

Zwei Highlights zum Auftakt

Positive Meldungen gab es gleich zum Start der beiden Konferenztage. Zum einen vergibt SNP im Gedenken an den 2020 verstorbenen Gründer Dr. Andreas Schneider-Neureither und dessen gesellschaftliches Engagement ein Stipendium an der Universität Heidelberg im Fachbereich Physik. Zum anderen verkündete COO Gregor Stöckler am zweiten Tag den Gewinn eines Top-Kunden: Märklin, den weltweit bekannten Marktführer im Modellbahnsektor.

Zuwachs im Partner-Ecosystem: scdsoft AG

Nächste gute Nachricht: SNPs starkes Partnernetzwerk erhält Zuwachs – auf der Transformation World verkündet in Form einer Partnerschaft mit scdsoft, einem Beratungs- und Lösungsanbieter für

Eröffnung der Transformation World 2023

Der neue CEO der SNP, Dr. Jens Amail, begrüßt die TW-Gäste

SAP HCM und SAP SuccessFactors. Die beiden Unternehmen wollen ihr Know-how zukünftig bündeln und ihre Softwarelösungen kombinieren, um Kunden vereinfachte und sichere Systemtransformationen und Wechsel nach SAP S/4HANA anbieten zu können. Geplant ist zudem die gemeinsame Weiterentwicklung von HCM-Kompetenzen und innovativen HCM-Lösungen.

Was Kunden wollen

Dass Enterprise-Daten der Dreh- und Angelpunkt für Innovationen und wirtschaftlichen Erfolg sind, ist keine ganz neue Erkenntnis, wurde auf der Transformation World allerdings immer wieder durch konkrete Beispiele belegt und spezifiziert. Was Kunden heutzutage in diesem Umfeld erwarten, fasste CEO Jens Amail zusammen: Lösungen, die sich nicht auf die Systeme eines Herstellers beschränken, die Einbindung moderner Technologien wie KI, kompetente Beratung, globale Präsenz, ein breites Ökosystem und Nachhaltigkeit.

Eine zentrale Rolle übernimmt in dem Zusammenhang das Composable Enterprise. Der vom IT-Analystenhaus Gartner geprägte Begriff beschreibt ein Unternehmen, das Kompetenzen und technische Möglichkeiten so kombiniert, dass es sich schnell an geschäftliche Veränderungen anpassen kann und agil, flexibel, innovativ und resilient bleibt. Basis dafür ist ein strategisches Datenmanagement über eine leistungsstarke Plattform wie SNP CrystalBridge, die auf Langfristigkeit ausgerichtet ist, zahlreiche Use Cases ermöglicht und maximale Flexibilität schafft, sodass sich unterschiedlichste Lösungen integrieren lassen. Ein Kernstück ist dabei die BLUEFIELD-Methode der selektiven Datenmigration.

Spezialthemen im Fokus

Eingebettet in die Transformation World gab es weitere Veranstaltungen, darunter ein CPO-Panel, bei dem sich Einkaufsverantwortliche mit Fragen rund um die digitale Transformation in ihrem Bereich auseinandersetzten. Am zweiten Tag fand die erste M&A Conference by digiweek & SNP in Kooperation mit M&A Review statt. Sie widmete sich einen ganzen Tag lang der praktischen Umsetzung von M&A-Transaktionen und Carve-outs mit Vorträgen zu Target Screenings, der Bedeutung von AI und ESG sowie dem Einsatz von Software zur Vereinfachung dieser komplexen Projekte.

Ein Panel der deutschen SAP-Anwendergruppe (DSAG) diskutierte praxisnah die Umsetzung von SAP S/4HANA-Transformationen. Sebastian Westphal, Global Head of ERP Operations and Transformation bei SPS, Simone Herth, Administrative Management Digital Business & Information Technology bei Roehm, und Thomas Henzler, CIO bei Piller, berichteten aus eigener Erfahrung, was es bei Aufbau und Betrieb einer geeigneten Zielarchitektur zu beachten gilt. Eine Erkenntnis: Prozesse müssten gleich zu Beginn grundsätzlich überdacht werden.

Nachhaltigkeit als Geschäftschance

Ein Schwerpunktthema, das die Transformation World in vielen Facetten durchzog, war Nachhaltigkeit – sowie die Frage, welche Rolle dabei Technologien spielen und wie nachhaltiges Wachstum funktionieren kann. Die eigene „grüne" Transformation treibt SNP mit einer neuen Rolle voran: In der Opening-Session am ersten Tag stellte Jens Amail Nicole Burhenne vor, die ihre Arbeit als Chief Sustainability Officer und Head of Corporate Development & ESG bei SNP zum 1. Oktober 2023 aufnimmt. Ihr Tätigkeitsfeld soll die Themen Umwelt, Soziales und Unternehmensführung sowie die strategische Entwicklung von SNP zusammenführen.

Wie sich Kundenerwartungen im Hinblick auf Nachhaltigkeit erfüllen lassen, zeigte die SNP-Tochtergesellschaft EXA. Sie stellte ihre Lösung Product Environmental Footprint (PEF) vor, die angesichts der zunehmenden Wichtigkeit von ESG-Richtlinien branchenübergreifend relevant für Audits ist. Emissionen jeglicher Art können damit analysiert werden. PEF soll dabei für eine Zentralisierung sorgen. Bei diesem Ansatz werden Daten zu Material, Produktion und Transport für sämtliche Schritte der Wertschöpfungskette betrachtet – vom Lieferanten bis zum Endkunden. Diese Informationen werden unter anderem per What-if-Szenarien im Hinblick auf unterschiedlichste Kriterien ausgewertet und fließen in ein End-to-End-Reporting.

GUT ZU WISSEN

Lesen sie mehr zu diesem Thema im Internet auf **www.snpgroup.com**

Der PEF-Ansatz zahlt sich gleich doppelt aus: Zum einen schaffen Unternehmen damit einen Imageschutz gegen den Vorwurf des „Greenwashing". Sie sichern sich durch den Nachweis das Vertrauen von Kunden und anderen Interessensvertretern. Gleichzeitig ergeben sich Chancen für neue Geschäftsmodelle. Und last but not least wird ein Unternehmen, das den ESG-Richtlinien nachkommt, attraktiver für potenzielle Investoren. Immerhin schauen sich bereits 72 Prozent der PE-Unternehmen die ESG ihrer Zielunternehmen an, 76 Prozent haben diese Richtlinien bereits in ihrem Investitionsprozess verankert, zeigte eine auf der M&A Conference vorgestellte Studie.

Fazit

„Change is inevitable. Growth is optional", fasste COO Gregor Stöckler die Quintessenz im Product Plenary zum Thema „Composable Enterprise and the Future of Transformation" zusammen. SNP unterstützt den Paradigmenwechsel von einer monolithischen Architektur hin zu einem „Composable Enterprise". Indem sich SNP um die Daten kümmert, gewinnt die Business-Seite die erforderlichen Ressourcen, um sich auf die geschäftlich notwendigen Transformationen zu konzentrieren. Dass und wie es funktioniert, zeigte die Transformation World 2023 eindrucksvoll.

Application Management Services

WESENTLICHER BESTANDTEIL DER DIGITALEN TRANSFORMATION

Sie helfen Unternehmen, Software- und IT-Services effizienter zu betreiben und zu verwalten, um ihre Ziele zu erreichen: Application Management Services (AMS) bieten Unternehmen ein umfassendes Set an Dienstleistungen, um eine optimale Nutzung der Technologie zu ermöglichen und das Potenzial der digitalen Transformation voll auszuschöpfen.

Was sind AMS?

Beim Application Management geht es um die Betreuung, Optimierung und Entwicklung von Applikationen/Anwendungen im Unternehmen. Die Betreuung umfasst auch die Wartung und den Anwendersupport. Die Entwicklung umfasst die Anpassung der Applikation an aktuelle Anforderungen. Richtig gemanagt, führen die Maßnahmen zu einer stetigen Optimierung der Applikationen.

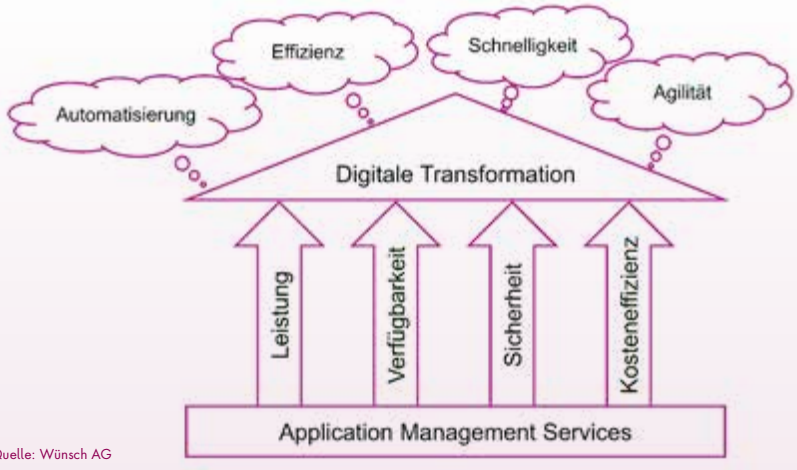
Application Management Services können Unternehmen bei der digitalen Transformation unterstützen, weil sie die Komplexität der Anwendungs- und Systemlandschaft reduzieren. Mit AMS können Unternehmen die Kontrolle über ihre Anwendungen erlangen, indem sie die Leistung, Verfügbarkeit, Sicherheit und Kosteneffizienz verbessern. Dies ermöglicht Unternehmen, schnellere und agilere Entscheidungen zu treffen, die für ihre digitale Transformation notwendig sind. Darüber hinaus können AMS dazu beitragen, Entwicklungskosten zu senken. Entwicklungszeiten lassen sich verkürzen, indem sie die Entwicklungsprozesse vereinfachen und automatisieren. AMS können auch dazu beitragen, Prozesse zu rationalisieren, weil sie redundanten Code und ähnliche Probleme beseitigen und mehr Flexibilität in den Entwicklungsprozess bringen. All dies ermöglicht es Unternehmen, schneller auf neue Markttrends und Technologien zu reagieren und sie so bei der digitalen Transformation zu unterstützen.

DURCH DIE NUTZUNG DER APPLICATION MANAGEMENT SERVICES LERNEN UNTERNEHMEN, WIE SIE IHRE ANWENDUNGEN BESSER VERWALTEN UND WIE SIE DIESE AN SICH ÄNDERNDE GESCHÄFTSBEDÜRFNISSE ANPASSEN KÖNNEN.

Petra Riepe,
Director Sales und HR,
Wünsch AG,
www.wuensch.de

Wie können AMS die digitale Transformation unterstützen?

Optimierte Applikationen und ein gut etablierter Application Management Prozess sparen Unternehmen Zeit und Geld. Beides wird benötigt, um die digitale Transformation im Unternehmen nachhaltig voranzutreiben. Ressourcen, die durch ein optimiertes Anwendungsmanagement frei werden, können sinnvoll für Zukunftsprojekte eingesetzt werden, die die Wettbewerbsfähigkeit der Unternehmen sichern.



Quelle: Wünsch AG

Faktoren für den Erfolg bei der Umsetzung der digitalen Transformation

Durch die Nutzung der Application Management Services lernen Unternehmen, wie sie ihre Anwendungen besser verwalten und wie sie diese an sich ändernde Geschäftsbedürfnisse anpassen können. Dies ermöglicht es Unternehmen, die digitale Transformation schnell und effizient umzusetzen und die Wettbewerbsfähigkeit zu steigern. Durch die Nutzung von AMS können Unternehmen ihre Anwendungen schneller entwickeln, aktualisieren und warten. Dadurch wird ein ständiger Fortschritt ermöglicht, was wiederum zu einer verbesserten Benutzererfahrung für die Kunden führt. Insgesamt kann gesagt werden, dass Application Management Services ein wesentliches Element der digitalen Transformation sind, da sie Unternehmen bei der Verwaltung ihrer Anwendungen unterstützen und Ressourcen für die digitale Transformation generieren.

Warum sind AMS für Unternehmen wichtig?

Application Management Services können Unternehmen dabei unterstützen, die digitale Transformation zu meistern. Sie bilden die Basis für eine schnelle Reaktionsfähigkeit der Unternehmen, denn es gilt diverse Herausforderungen gleichzeitig zu bedienen:

#1 Schnelle Anpassungen

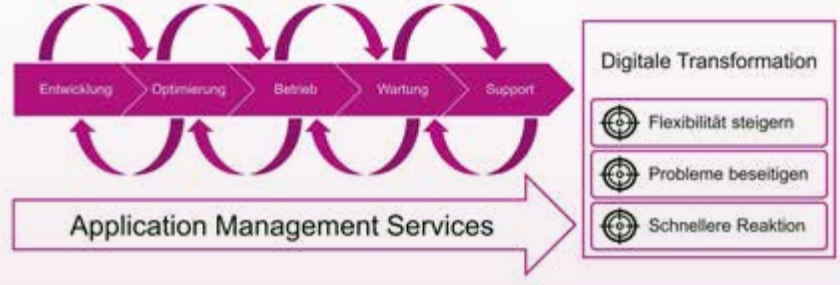
Der Prozess der digitalen Transformation erfordert mehr denn je, dass Unternehmen ihre Anwendungen und Infrastrukturen schnell an die sich ständig ändernden Anforderungen anpassen können. Ein stabiler Betrieb der Applikationen schafft freie Ressourcen. AMS bieten Unternehmen die Möglichkeit, Anwendungen und Infrastrukturen zu überwachen, zu pflegen, auf dem neuesten Stand zu halten und somit einen stabilen Betrieb zu erreichen.

#2 Kosten senken bei steigenden Anforderungen

AMS können Unternehmen dabei helfen, die Kosten zu senken, indem sie sicherstellen, dass Anwendungen und Infrastrukturen effizient betrieben werden.

#3 Erhöhung der Kundenzufriedenheit

Unternehmen können einen besseren Kunden- und Mitarbeiterservice bieten, indem Anwendungen und Infrastrukturen reibungslos funktionieren. Darüber hinaus können sie Unternehmen dabei helfen, ihre Anwendungen und Infrastrukturen zu modernisieren, um die Effizienz und die Leistung zu verbessern.



Quelle: Wünsch AG

Fazit

Es ist offensichtlich, dass Application Management Services eine zentrale Rolle bei der Unterstützung der digitalen Transformation spielen. Sie helfen Unternehmen, ihre App-Performance zu optimieren, weil sie strukturiert gewartet und bearbeitet werden.

Petra Riepe

AMS beschleunigt und sichert den Erfolg der digitalen Transformation

Bild: HZDR-Oliver Killig

Gelassen in die Zukunft

NEUE ITSM-LÖSUNG FÜR DAS HELMHOLTZ-ZENTRUM DRESDEN-ROSSENDORF

Am nordöstlichen Rand von Dresden liegt das Helmholtz-Zentrum Dresden-Rossendorf (HZDR). Was einst ein Relikt des Kalten Krieges war, ist heute ein unverzichtbarer Zukunftsstandort. Rund 1.500 Wissenschaftler forschen hier in den Gebieten Gesundheit, Energie und Materie. Damit die internen Abläufe reibungslos funktionieren, war ein neues IT-Service-Management-System dringend notwendig. Und das fanden die Verantwortlichen quasi in der Nachbarschaft.

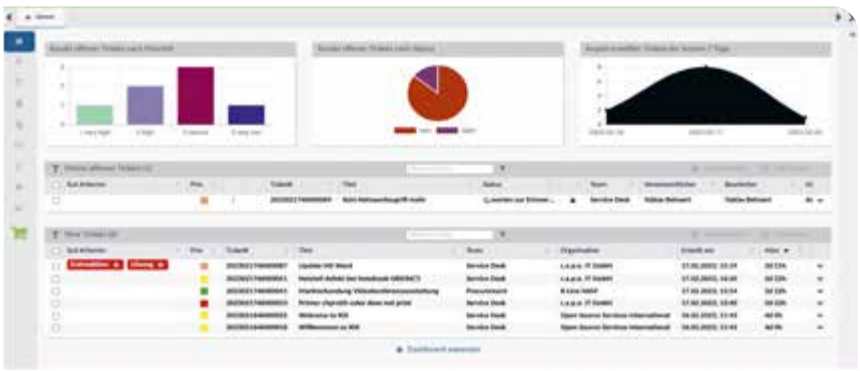
Auf ihrem Weg zur Arbeit begegnen die Mitarbeiter des HZDR jeden Tag Marie Curie, Otto Hahn oder Ernest Rutherford – die Straßen des 186 Hektar großen Areals tragen die Namen berühmter Wissenschaftler des 19. und 20. Jahrhunderts. Und auf ihren Spuren wandeln die Forscher noch heute: Sie beschäftigen sich mit Strahlenphysik, und auch Projekte zur Krebsforschung werden hier vorangetrieben. In jüngster Zeit war das HZDR auch daran beteiligt, Gegenmaßnahmen für das Corona-Virus zu entwickeln. Beispielsweise hat das Institut CASUS (Center for Advanced Systems Understanding) beim Projekt Folding@Home freie Rechenkapazitäten zur Verfügung gestellt, um die komplexen Proteinstrukturen des Virus zu entschlüsseln.

Mit der Gründung des Zentralinstituts für Kernphysik wurde 1956 der Grundstein für das heutige Areal in Rossendorf gelegt. Als Zentralinstitut für Kernforschung wurde es kurze Zeit später Teil der Akademie der Wissenschaften der DDR. Mit einer Leistung von zehn Megawatt befand sich hier unter anderem der größte Forschungsreaktor der DDR – er blieb bis 1991 in Betrieb, 2019 wurde der Rückbau abgeschlossen. Nach dem Fall der Mauer wurde der Standort als Forschungszentrum Rossendorf neu gegründet. Seit der Aufnahme in die Helmholtz-Gemeinschaft Deutscher Forschungszentren 2011 trägt er schließlich seinen aktuellen Namen. Das HZDR ist heute das größte Forschungszentrum in Sachsen und mehr denn je auf eine verlässliche IT-Infrastruktur angewiesen.

Die Lösung aus der Nachbarschaft

Das HZDR setzte viele Jahre auf ein Ticketsystem, das die IT-Mitarbeiter selbst entwickelt hatten. Mit der wachsenden Anzahl der Forschungsfelder wurden aber auch die Anforderungen an die IT immer komplexer. Die Arbeit war damit zwar noch möglich, doch die User wurden immer unzufriedener. Wichtige Features wie eine Volltextsuche oder das Erstellen von FAQs gab es nicht. Auch die Oberfläche war nicht sehr intuitiv und generell nicht mehr zeitgemäß.

Olaf Ruddigkeit, Leiter User Services am HZDR, und sein Team machten sich also auf die Suche nach einem neuen IT-Service-Management-System. Dafür erstell-



Agenten-Dashboard mit neuen Tickets inkl. SLA's, Prioritäten und Verantwortlichkeiten

ten sie im ersten Schritt ein Lastenheft, in dem sie die wichtigsten Anforderungen an das neue System zusammenfassten. Weil das HZDR eine öffentliche Einrichtung ist und diese nach Vorgabe der Bundesregierung vermehrt Open Source-Lösungen einsetzen sollen, fielen proprietäre Systeme weg. Vier ITSM-Lösungen schafften es in die engere Auswahl, und die Wahl fiel auf KIX vom Chemnitzer Unternehmen KIX Service Software.

Die Anforderungen aus dem Lastenheft wurden erfüllt, so Olaf Ruddigkeit: „Das neue System sollte alle Funktionen eines klassischen Ticketsystems haben. Jetzt können wir darüber hinaus auch die verschiedenen Mandanten abbilden, Rechte rollenbasiert verteilen und dynamische Felder frei konfigurieren, ohne auf die Hilfe des Entwicklers angewiesen zu sein." Auch aus finanzieller Sicht ist Ruddigkeit zufrieden: „Bei anderen Systemen erfolgt die Abrechnung oft nach der Anzahl der einzelnen Service-Mitarbeiter, bei der On-Premises-Variante von KIX ist die Zahl egal. Das ist wirklich ein faires Abrechnungsmodell."

Zusätzlich können die IT-Mitarbeiter verschiedene Bereiche gebündelt in einem System abbilden: „Das Incident Management, also das eigentliche Ticketsystem, sowie das Facility Management, Aufträge für das Labor und für die Forschungstechnik laufen nun alle in einem System zusammen. Das erleichtert auch die Schulungen der Mitarbeiter", so Ruddigkeit.

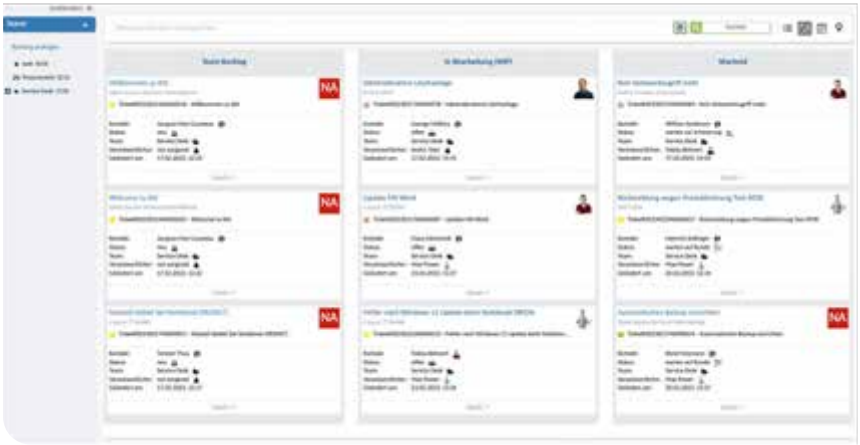
Das Herzstück des IT-Service-Managements

Beim Helmholtz-Zentrum Dresden-Rossendorf besteht das IT-Service-Management aus vier Teilen: Dem Unified Endpoint Management, einer zentralen Datenbank, der Monitoring Software Checkmk und nun KIX als Herzstück des IT-Service-Managements.

Die Inventarisierung und Patchverteilung erfolgt beim Unified Endpoint Management, auch Desktop Central genannt. Alle Assets, User, Benutzerdaten und Standorte sind in einer Datenbank hinterlegt und werden im Anschluss in KIX gemanaged. Auch die Monitoring-Software Checkmk versorgt das neue ITSM-System mit Informationen: „Hier kommen sämtliche Störungsmeldungen im Managementsystem an, etwa bei ausgefallener Hardware", erklärt Olaf Ruddigkeit. Am HZDR sind etwa 40 Mitarbeiter für die IT zuständig. Sie bearbeiten rund 14.000 Tickets pro Jahr und können auf über 50.000 Assets in der Datenbank zugreifen.

Die neue ITSM-Lösung ist auch mit einem Self Service Portal ausgestattet, mit dem die Mitarbeiter ein neues Ticket erstellen können. Durch verschiedene Kategorien lassen sich Störungen so zielgerichtet zuordnen. Die User können sich aber auch direkt an die lokalen Administratoren in den verschiedenen Instituten wenden. Sollten diese keine Problemlösung finden, landet das Ticket beim Service Desk von Olaf Ruddigkeit und seinem Team.

Besonders das integrierte Kanban-Board hat sich als sehr nützlich für die tägliche Arbeit erwiesen. Die Mitarbeiter haben damit eine visuelle Darstellung, ob ein Projekt bereits abgeschlossen ist bzw. welchen Zwischenstand es hat. Das hat vor allem die Arbeit in den Laboren vereinfacht: Aufgrund beschränkter Kapazitäten müssen die Mitarbeiter hier nach Terminen arbeiten. Verzögern sich Laboraufträge, werden sie direkt darüber informiert. Überschneidungen und doppelte Arbeiten gehören damit der Vergangenheit an.



Mit dem Kanban-Board haben die Mitarbeiter des HZDR den Überblick über alle Vorgänge

Pläne für die Zukunft

Im Moment wird das neue ITSM-System für verschiedene Bereiche eingesetzt, darunter das Störungsmanagement samt Flächenstörungen, Serviceverträge und Service Level Agreements, Knowledge- sowie Changemanagement beziehungsweise Berichtswesen. Weitere Funktionen sollen in Zukunft folgen: „Wir arbeiten bereits am Aufbau einer Gerätedatenbank. Auch das Auftragsmanagement und das Administrationstool möchten wir bald integrieren", so Ruddigkeit.

Das langfristige Ziel von ihm und seinen Kollegen ist es, den gesamten IT-Service-Katalog des HZDR in KIX abzubilden. Mit den bisherigen Ergebnissen ist er zufrieden: „Smarte Funktionen, nützliche optionale Erweiterungen, intuitive Bedienung, Open Source – jetzt haben wir ein zukunftssicheres ITSM-System. Und auch die Zusammenarbeit mit unseren Chemnitzer Nachbarn war hervorragend. Was die IT angeht, kann ich den nächsten Jahren gelassen entgegenblicken."

Julien Herrmann | www.kixdesk.com

Nur Smalltalk?

DIE MÖGLICHKEITEN UND GRENZEN VON CHATGPT IM CUSTOMER SERVICE

USU HAT MIT „BOT UNIVERSE" EIN KONZEPT ENTWICKELT, WELCHES DAS ZUSAMMENARBEITEN VERSCHIEDENER CHATBOTS ERLAUBT.

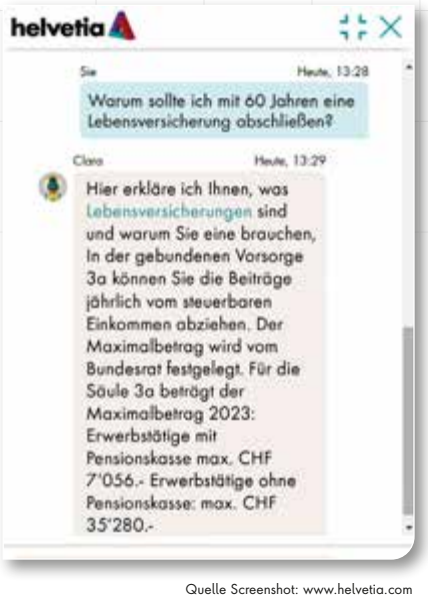
Dr. Thomas Gerick, Berater, USU Software AG, www.usu.com

Von IT-Fachzeitschriften über die großen Nachrichtenmagazine bis hin zu Fernsehreportagen und Radiosendungen: Kaum ein anderes Technologiethema hat jüngst einen derartigen Nachrichtenhype ausgelöst wie ChatGPT. Im Folgenden werden die neuen Möglichkeiten, aber auch die Grenzen von ChatGPT beim Einsatz im Kundenservice beleuchtet. Das Fazit: generative KI ist derzeit nur so gut wie der Mensch, der sie steuert. Es kommt auf den Use Case an.

ChatGPT- erste Experimente im Customer Service

Ende März 2023 kündigte die Helvetia Versicherung an, künftig ChatGPT einzusetzen, um Kundenfragen zu Versicherungen und Vorsorge zu beantworten. Clara heißt die Chatbot-Dame, die im Rahmen eines Live-Experiments Auskunft gibt. Und in der Tat liefert die digitale Assistentin auf den ersten Blick vernünftige Antworten.

Wichtig ist dabei, dass die Software auf definierte Web-Inhalte von Helvetia zurückgreift und nur allgemeine Inhalte beauskunftet, keine kritischen Themen. Auf mögliche Fehler des neuartigen Service weist die Helvetia-Website ausdrücklich hin.



Quelle Screenshot: www.helvetia.com

Denn Versicherungen gehören zu den Branchen, bei denen für den Customer Service ein ehernes Gesetz gilt: Die Antwort oder Lösung für sensible Bereiche muss immer verlässlich und qualitätsgesichert sein. Im vorliegenden Fall bringt die Antwort des Systems den Fragesteller kaum weiter. Sie greift die Frage nicht direkt auf, sondern verweist auf eine allgemein formulierte Website. Auf das Alter als Kriterium wird nicht eingegangen. Außerdem bleibt außer Betracht, dass der Fragesteller aus Deutschland kommt, aber in der Antwort auf Schweizer Rahmenbedingungen Bezug genommen wird. Insgesamt ist die Antwort auf die spezifische Frage unbefriedigend – ein Service Agent hätte besser und individueller beraten.

Viele Stichproben und Versuche haben in den letzten Monaten gezeigt, dass es die KI-Chatbots mit der faktischen Korrektheit ihrer Antworten nicht immer ganz genau nehmen. Persönlichkeiten, die zufällig denselben Nachnamen tragen, werden durcheinandergebracht, die Wahlen in der Türkei auf ein Zukunftsdatum gesetzt, deren Ergebnisse jedoch bereits halluziniert usw. Aber: trotz aller Unzulänglichkeiten lernt generative KI über menschliches Feedback extrem schnell dazu. In der Version 4 von ChatGPT, die im März 2023 vorgestellt wurde, konnten viele Fehler ausgeräumt werden.

Trotz deutlicher Verbesserungen in der Aussagequalität bleibt das Grundproblem bestehen, dass das System mit den Texten arbeitet, die verfügbar sind und daraus die „stochastisch wahrscheinlichste Antwort" zu einer bestimmten Anfrage generiert. Themen, zu denen sich nur wenige Texte finden lassen, werden daher von der KI mit höherer Wahrscheinlichkeit inkorrekt beantwortet als Bereiche, die im Internet viel diskutiert werden. Dabei ist auch die Aktualität ein Problem. So lässt sich eine defekte Sicherung laut KI an einem durchgebrannten Draht oder einer verfärbten Glassicherung erkennen. Während dies an sich korrekt ist, entspricht es jedoch bei weitem nicht mehr den Sicherungstypen, mit denen moderne Häuser und Wohnungen heutzutage ausgestattet sind – über die jedoch weniger Informationen im Internet zu finden sind. Wie aber lässt sich ChatGPT vor diesem Hintergrund nutzbringend einsetzen?

ChatGPT kann Chatbot-Services ergänzen

Chatbots im Kundendienst werden normalerweise auf Websites oder in den sozialen Medien genutzt. Sie greifen auf eine verifizierte Wissensdatenbank zurück. Bei Bedarf können sie Themen durch Rückfragen eingrenzen, um so bessere Antworten zu liefern. Für den internen Kundenservice der IT können Chatbots hingegen direkt auf dem Desktop oder den mobilen Geräten der Benutzer eingesetzt werden. Dies bietet einen entscheidenden Vorteil: Der

Chatbot kann die zur Lösung eines Problems notwendigen Aktionen direkt selbst ausführen, anstatt nur Antworten zu finden und zu liefern. Die Möglichkeiten sind nahezu grenzenlos: vom Leeren des Browser-Caches, über das Wiederherstellen der Netzwerklaufwerke, die skriptgesteuerte Installation neuer Treiber bis hin zum Einrichten eines Druckers.

Und wo lässt sich ChatGPT im Kundenservice einsetzen? Wenn es um Textzusammenfassungen, die Textklassifizierung und die Generierung von Texten bei eng begrenzten, weniger kritischen Themen und konsistent aufbereiteten Inhalten geht, kann generative KI ihre Stärken ausspielen – zum Beispiel beim Nennen von Öffnungszeiten. Auf die Frage „haben Sie am Mittwoch nachmittags geöffnet", liefert das System nicht nur die Seite mit den Öffnungszeiten, sondern antwortet konkret: „Ja, wir haben am Mittwoch auch nachmittags von 14:00 bis 16:30 geöffnet." Denkbar ist auch das automatische Vermitteln von Ansprechpartnern. Nicht zuletzt nutzt ein internationales Möbelhaus ChatGPT derzeit, um die bestehenden Texte im Service an den konzernspezifischen „tone of voice" anzupassen. Und die Entwicklung bleibt dynamisch. Wenn es gelingt, die Technologie so weiterzuentwickeln, dass sich ihre hohe Leistungsfähigkeit mit echtem Sprachverständnis und einer zuverlässigen Wissensbasis koppeln ließe, dann wären verlässliche Aussagen möglich. Eine Maschine, die mit hoher Wahrscheinlichkeit klassifizieren kann, worum es in einer Frage geht, bei Bedarf Rückfragen stellt, herausfindet, welche Daten sie dafür benötigt, diese sucht und daraus die passende Antwort generiert, inklusive verlässlicher Quellengabe – dies wäre in der Tat ein Meilenstein in die richtige Richtung.

Multibot-Architektur kann ChatGPT integrieren

Da ein einzelner Chatbot nur begrenzte Funktionen abdecken kann, entwickelte USU aus einem Forschungsprojekt heraus das Konzept von miteinander vernetzten Chatbots – eines „Bot Universe".

Ein Musikorchester ist ein gutes Bild, um die Technik-Idee für das Zusammenarbeiten verschiedener Chatbots zu beschreiben. Nach der Devise „allein stark, zusammen unschlagbar" werden mehrere unterschiedliche Chatbots auf Basis einer Multibot-Architektur zusammengeschaltet und können so auch komplexe Aufgaben lösen.

Durch die einfache Erstellung kleiner, übersichtlicher und wiederverwendbarer Chatbots ist es so möglich, mit geringem Aufwand leistungsfähige Dialogsysteme zu bauen.

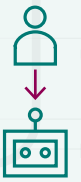
Das Konzept zu Bot Universe unterteilt Chatbots in zwei Rollen, Experten- und Lead-Bots. Dabei liefern die Expertenbots Informationen zu bestimmten Fachthemen, der Lead-Bot (= der Dirigent, um im Bild zu bleiben) fungiert als Moderator und weist dem Anwender den für sein Anliegen passenden Experten-Bot zu (der auf seinen Einsatz als Solist wartet).

Durch die beschriebene Architektur lassen sich auch ein oder mehrere ChatGPT-Bots sehr einfach integrieren. Die Inhalte für ein solches „diverses" Bot-Team werden über eine Wissensdatenbank gemanaged. Erste Service-Organisationen setzen dieses Bot-Netzwerk inklusive ChaTGPT bereits erfolgreich ein. Auf die weitere Entwicklung generativer KI darf man gespannt sein.

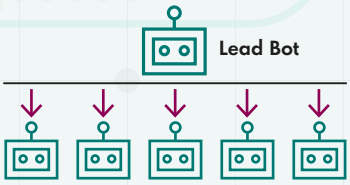
Dr. Thomas Gerick

WIE LÄUFT NUN DIE KOMMUNIKATION AB?

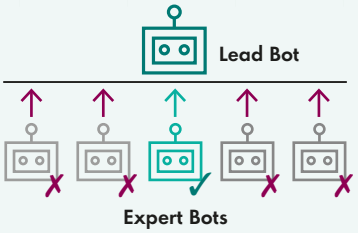
Zunächst nimmt der Lead-Bot die Anfrage des Anwenders entgegen.



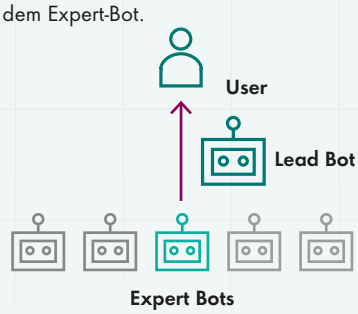
Im zweiten Schritt sendet dieser die Anfrage des Anwenders an jeden im Bot-Netzwerk registrierten Expert-Bot.



Jeder Expert-Bot ermittelt daraufhin, ob er mit der Anfrage etwas anfangen kann. Das geschieht mit Hilfe Künstlicher Intelligenz. Sollte ein befragter Expert-Bot das Thema erkennen, meldet er dies entsprechend zurück.



Anhand der Rückmeldungen entscheidet der Lead-Bot das weitere Vorgehen: Wenn sich lediglich ein Expert-Bot verantwortlich fühlt, wird die Kommunikation an diesen Expert-Bot übergeben. Wenn mehrere Bots Interesse zeigen, fragt der Lead-Bot den Anwender, für welches Thema er sich genau interessiert. Der Anwender wählt dann entsprechend aus, und der Lead-Bot baut die Verbindung zum spezifischen Expert-Bot auf. Wenn kein Bot zuständig ist, wird der Anwender um eine Spezifizierung seiner Anfrage gebeten.
Wenn eine Verbindung zu einem Expert-Bot aufgebaut wurde, kommuniziert der Anwender nun direkt mit dem Expert-Bot.



Das modular aufgebaute Chatbot-Netzwerk erlaubt eine einfache Pflege und Wartung durch die Redakteure. Kommt ein neuer Themenkomplex hinzu, wird ein weiterer Chatbot erstellt und im Netzwerk integriert. Mit dieser Architektur lassen sich mit überschaubarem Aufwand sehr komplexe Chatbot-Implementierungen betreiben.

Die nahtlos in ams.erp integrierte Projektmanagement-Software ams.project.

Systemintegration

WICHTIGER FAKTOR IM PROJEKTGESCHÄFT

Im komplexen Projektgeschäft der Einzel-, Auftrags- und Variantenfertigung kommt es wesentlich darauf an, den im Angebot kalkulierten Budgetrahmen stets im Blick zu behalten, um die Wirtschaftlichkeit der Aufträge sicherzustellen. Dabei befinden sich jene Unternehmen im Vorteil, deren Projektmanagement-Software Bestandteil ihres ERP-Systems ist. Denn dank dieser nahtlosen Integration werden etwaige Abweichungen von im ERP-System hinterlegten Budgetrahmen schnell im Projektmanagement ersichtlich.

Ein Projektmanagement-Cockpit mit umfassender ERP-Integration bietet das auf die Losgröße 1+ spezialisierte Software- und Beratungshaus ams.Solution mit ams.project. Das Modul ermöglicht die unternehmensweite Termin-, Budget- und Ressourcenplanung, was bedeutet, dass alle terminrelevanten Daten aus dem ERP-System ams.erp automatisch in der Planung berücksichtigt werden und als Meilensteine oder Vorgänge direkt in ams.project angezeigt werden.

Schneller Überblick

In der Praxis gestaltet sich der Ablauf wie folgt: Die Aufträge werden samt den budgetierten Stunden im ERP-System erfasst und sind direkt im Projektmanagement sichtbar. Auf Basis dieser Daten wird dort ein erster Terminplan erstellt. Wurden seitens des Vertriebs im ERP-System angebotsseitig 200 Stunden für die Konstruktion, 600 Stunden für die Fertigung und 200 Stunden für die Montage einer Maschine veranschlagt, die in einem Zeitraum von 12 Wochen gebaut werden soll, kann die Projektleitung dieses Stundenbudget bestmöglich und unter terminlicher Berücksichtigung aller im Hause befindlichen Aufträge einplanen.

Sollte sich im Projektverlauf herausstellen, dass das angesetzte Budget an bestimmten Punkten überschritten wird, wird dies sofort im Rahmen einer Ampelfunktionalität sichtbar. Die Projektleitung hat daraufhin die Möglichkeit, die Stunden entsprechend umzuverteilen, wenn etwa an anderer Stelle noch überschüssige Kapazitäten zur Verfügung stehen sollten. Ist diese „Quersubventionierung" nicht möglich, muss zusammen mit dem Vertrieb eine andere Lösung angestrebt werden.

Ein immenser Vorteil von ams.project gegenüber anderen Projektmanagement-Tools liegt in der Mehrstufigkeit der Planung, die von einer groben bis hinunter auf eine sehr feine Ebene möglich ist. Die Grobplanung über die Budgets kann auf eine Mittelplanung mit Bezug auf die Arbeitsplatzgruppen und bestimmte Intervalle heruntergebrochen werden, von wo aus ein weiteres „Einzoomen" auf einzelne Arbeitsplätze möglich ist. Aufgrund dieser granular gestalteten Übersicht ist schnell erkennbar, ob der Budgetrahmen eingehalten oder wo genau er gerissen wird.

Genaue Bestimmung der Kapazitätsbelastung

Interessant für mittelständische Projektfertiger ist zudem, dass sie allein auf Basis der angelegten Budgets einsehen können, wie hoch die Kapazitätsbelastung für eine bestimmte Ressource, ausfällt. Über ein Kapazitäts-Dashboard lässt sich aus den Vorgaben des Vertriebs eine Ressourcenauswertung für die Gruppe der Konstruktion aufrufen. In Form eines Kapazitätsgebirges lassen sich speziell für diese Gruppe oder auch für alle anderen Gruppen sämtliche bereits verplanten Budgetstunden einsehen. Die verfügbare Kapazitätslinie verläuft auf der x-Achse, gegen die die Aufträge mit den jeweiligen Stunden laufen. Über diverse Parameter lässt sich bei Bedarf zudem nur eine bestimmte Art von Aufträgen herausfiltern. Hilfreich ist, dass darüber hinaus auch größere Angebote mit einer Auftragswahrscheinlichkeit von über 80 Prozent in den Kapazitäts-Dashboards angezeigt werden können, um zu evaluieren, ob deren Umsetzung in einem bestimmten Zeitraum überhaupt realistisch ist.

Wenn die Einzelfertiger in einem größeren Konzernverbund oder im Rahmen internationaler Großprojekte tätig sind, können die Projektpläne zudem an Microsoft Project übergeben werden. Diese Funktionalität kommt ebenso zum Tragen, wenn den Kunden der Stand der gegenwärtigen Projektabwicklung übermittelt werden soll.

www.ams-erp.com

Strategisches Lizenzmanagement

SICHER DURCH DEN MICROSOFT-LIZENZ-DSCHUNGEL

UM KEINE UNTERLIZENZIERUNG ZU RISKIEREN, WIRD OFT BLIND ZU VIEL SOFTWARE EINGEKAUFT.

Joyce Studier, Lizenzberaterin, VENDOSOFT GmbH, www.vendosoft.de

Wer mit IT-Verantwortlichen über Microsoft-Lizenzierungen spricht, hört einen Satz besonders oft: Das ist ein Dschungel! Undurchdringlich die Lizenzmodelle, ständig neue Bestimmungen und die Preisspirale dreht sich. Kaum ein Administrator schafft es noch, lizenzrechtlich am Ball zu bleiben. Das kann teuer werden. Outsourcen ist eine Lösung. Doch an wen, wenn die Kosten nicht noch mehr explodieren sollen?

Helmut Fetsch ist IT-Leiter der Großen Kreisstadt Germering und betreut mit sieben Kollegen knapp 150 Computerarbeitsplätze. Auch er empfindet die Microsoft-Lizenzmodelle als Dschungel. „Ein Irrsinn!", sagt er. „Ständig geänderte Bestimmungen und Voraussetzungen. Da müssen wir uns externe Beratung holen."

Die hat die Stadt in dem Microsoft Solutions Partner VENDOSOFT gefunden und wird von Joyce Studier, SAM-Expertin und Microsoft Licensing Professional, betreut. Ihr Ansatz: Strategische Lizenzberatung.

Fehlende Nachweise nicht „irgendwie" ausbügeln

Der Behörde geht es wie vielen Unternehmen: Der Lizenznachweis bleibt oft ein Stiefkind. „Damit man keine Unterlizenzierung riskiert, wird gern mal eine Lizenz zu viel gekauft", erklärt Joyce Studier das Dilemma vieler IT-Abteilungen. Gut ist das nicht. Teuer allemal. Doch in der Praxis, sagt Helmut Fetsch, „sieht es so aus: Wir kaufen Software ein und geben die Rechnung ins Finanzwesen. Die liegt uns dann nicht mehr vor." Auch eine Inventarisierung erweist sich als nicht ausreichend. „Ich muss ja bei einem Arbeitsplatz wissen, ist das eine alte, upgedatete Office-Lizenz, eine OEM oder... Das bindet brutal viel Zeit." Joyce Studier erlebt das bei vielen ihrer Geschäftskunden. „Wenn man das Fortführen der Lizenzen für einige Zeit schleifen lässt, kann man von vorn anfangen."

Fallstricke bei der Microsoft-Lizenzierung

Wer den Lizenznachweis nicht hausintern koordiniert, dem hilft die strategische Lizenzberatung, wie sie die VENDOSOFT-Experten durchführen. Die kennen Fallstricke wie die ‚Upgrade-Pfade', wonach die Microsoft Windows 10 Enterprise Volumenlizenz eine Basislizenz erfordert. Ohne die ist man unterlizenziert. Neben diesem gibt es zig Beispiele, wie das Microsoft-Lizenzrecht fehlinterpretiert werden kann. Deshalb ist Organisationen ab 100 Mitarbeitern zu einer jährlichen Überprüfung der Software-Bestände geraten.

Bei der Großen Kreisstadt Germering läuft das so ab: Joyce Studier prüft zunächst einmal die Rechnungen der letzten fünf Jahre: Was ist ausreichend lizenziert, wo fehlen Lizenzen, was braucht die Stadt wirklich? „Gemeinsam stellen wir das jetzt auf gesunde Füße", sagt Helmut Fetsch.

Die zeit-, nerven- und kostensparende Lizenzberatung von VENDOSOFT bestätigen Unternehmen aus produzierendem Gewerbe, Handel, Chemie, Gesundheitswesen und dem behördlichen Umfeld.

www.vendosoft.de/casestudies

LIZENZBERATUNG ZAHT SICH AUS

Die Microsoft Licensing Professionals von VENDOSOFT erkennen Lizenz-Gaps und schließen diese günstiger als andere Anbieter – durch Einbeziehung gebrauchter Software

- **Sie empfehlen hybride Lizenzmodelle:** Cloud-Anbindung (wo nötig), gebrauchte Software (wo möglich). Das spart schnell 50 bis 60 Prozent der veranschlagten Cloud-Kosten.
- **Überschüssige Microsoft-Lizenzen sollten monetarisiert werden:** Durch Verkauf an VENDOSOFT. Das schafft liquide Mittel und dient auch noch der Nachhaltigkeit!

TEIL 2 VON 4

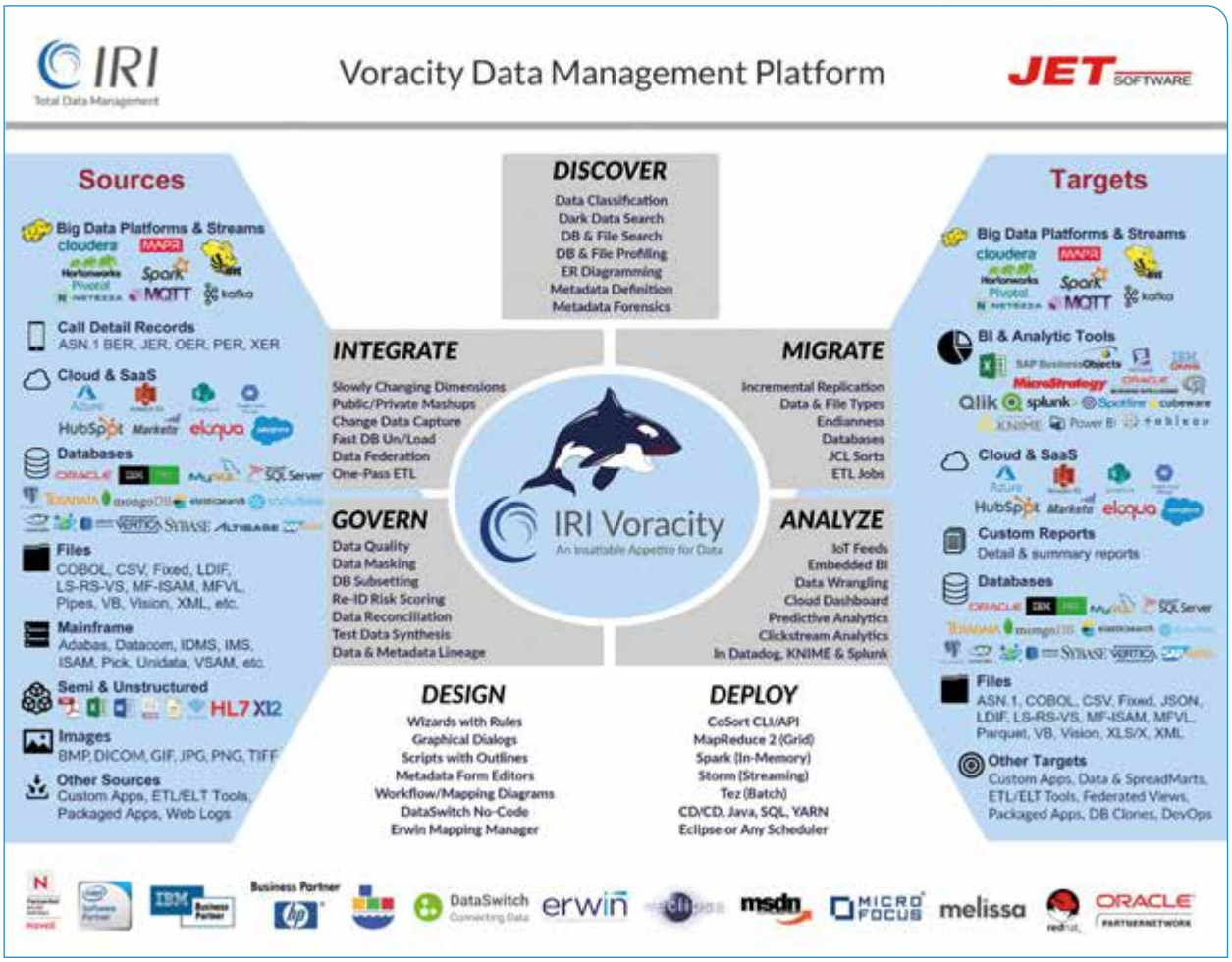
Bestandteile einer Datenstrategie

DATENINTEGRATION, -MIGRATION UND -MODERNISIERUNG

Dies ist der zweite von vier Artikeln einer Serie zum Thema End-to-End Datenmanagement. Im ersten Artikel wurde die Notwendigkeit einer umfassenden Datenverarbeitung im Zusammenhang mit der leistungsstarken und benutzerfreundlichen Plattform „IRI Voracity" vorgestellt, denn sie kombiniert die Datenerkennung, die Datenintegration und Datenmigration, mit anschließender Verwaltung und Analytik in nur einem verwalteten Metadaten-Framework. Die Verwendung von nur einer Konsole erleichtert nicht nur die Bedienung, sondern verringert die Betriebskosten einer vernetzen IT-Umgebung erheblich.

Durch eine miteinander vernetze IT-Umgebung bestehend aus Servern, Computern, anderen IoT-Geräten und Anwendungen können wertvolle Daten innerhalb des Unternehmens viel schneller integriert, ausgetauscht und gesammelt werden. Die Datenintegration bezieht sich auf den Prozess der Zusammenführung von Daten aus verschiedenen lokalen und Cloud-Quellen, um eine einheitliche und konsistente Sicht auf die Daten im Unternehmen zu schaffen. Die wesentlichen Vorteile dieser Datenintegration sind:

#1 Verbesserte Datenqualität: Durch die Integration von Daten aus verschiedenen Quellen können Duplikate, Unstimmigkeiten und Widersprüche identifiziert und korrigiert werden, das zur Verbesserung der Datenqualität führt.



#2 Bessere Entscheidungsfindung: Die einheitliche Sicht auf die gesammelten Daten ermöglicht es Unternehmen, fundiertere und bessere Entscheidungen zu treffen. Es können nicht nur Trends und Muster des Kunden, sondern auch Vorgänge im Unternehmen identifiziert werden.

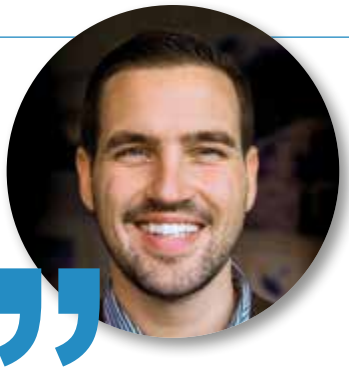
#3 Effizienzsteigerung: Durch die Integration von Daten können manuelle Prozesse automatisiert werden, was zielführend zu einer höheren Effizienz und zu Kosteneinsparungen führt.

#4 Bessere Zusammenarbeit: Eine einheitliche Sicht auf gemeinsame Daten verbessert die Zusammenarbeit zwischen verschiedenen Abteilungen und Teams. Durch den gemeinsamen Zugriff auf die gleichen Daten können die Mitarbeiter besser zusammenarbeiten und effektiver kommunizieren.

Die Datenintegration besteht aus mehreren Prozessen und beginnt mit der Identifizierung der relevanten Datenquellen. Danach folgt die Extraktion der benötigten Daten und endet mit der Umwandlung in ein einheitliches Format, damit die integrierten Daten für Analysen oder andere Zwecke bereitgestellt werden können.

Datenmigration

Die Datenmigration hingegen bezieht sich auf den Prozess, Daten von einem System, einer Plattform oder einer Datenbank auf eine andere zu übertragen. Dies kann verschiedene Gründe haben, wie zum Beispiel der Austausch von Servern oder Speichergeräten, Wartung oder Upgrades, Anwendungsmigration, Website-Konsolidierung oder die Verlagerung des Rechenzentrums beispielsweise in die Cloud. Bei der Datenmigration werden die Daten extrahiert, transformiert und in das Zielsystem geladen, wobei die Integrität und Konsistenz der Daten gewahrt werden müssen um eine einheitliche Datenverarbeitung gewähren zu können.



DURCH EINE MITEINANDER VERNETZE IT-UMGEBUNG BESTEHEND AUS SERVERN, COMPUTERN, ANDEREN IOT-GERÄTEN UND ANWENDUNGEN KÖNNEN WERTVOLLE DATEN INNERHALB DES UNTERNEHMENS VIEL SCHNELLER INTEGRIERT, AUSGETAUSCHT UND GESAMMELT WERDEN.

Amadeus Thomas, Geschäftsführer, Jet-Software GmbH, www.jet-software.com

Die Herausforderung, Informationen aus Daten zu destillieren, wächst mit deren Umfang und Vielfalt. Um dem End-to-End Datenmanagement gerecht zu werden und damit Daten in jeder Phase des Lebenszyklus kontrollieren zu können, unterstützt die Plattform IRI Voracity selbstverständlich die Integration und Verschiebung von Daten zwischen verschiedenen Systemen:

- Data Discovery (Profiling, Klassifizierung, ERDs, Dark Data)
- Datenintegration (ETL, CDC, SCD, TDM)
- Datenmigration (Dateien, Datenbanken, Datentypen, Datensatzlayouts)
- Data Governance (Maskieren, Bereinigen, MDM, EMM)
- Analytics (integrierte BI & Datenaufbereitung)

Schnelle und einfache Lösung

Die Historie geht zurück bis in die späten 1970er Jahren mit der Unterstützung von Mainframe-Daten- und Sortiermigrationen. Das Basisprogramm der IRI Voracity Plattform kann daher auf eine lange Geschichte im Bereich der Datenmigration und -modernisierung zurückblicken, einschließlich der Konvertierung von Datentypen und Dateiformaten sowie ETL-Operationen mit RDB- und NoSQL-Datenbanken. IRI Voracity bietet nun ein komplettes Set von Datenintegrations- und Migrationsfunktionen, die schneller und einfacher sind als herkömmliche Werkzeuge, ist dabei auch kostengünstiger im Betrieb und kann leichter an sich ändernde Datensätze und analytische Anforderungen angepasst werden:

#1 Um den Ort, das Layout und die Beziehungen von Daten in Datenbanken, Dateien und Dokumenten aufzudecken.

AUSBLICK

In den kommenden zwei Ausgaben wird auf die integrierten Funktionen der Plattform zum umfassenden Schutz von sensiblen Informationen eingegangen. Es werden verschiedene Methoden zur formaterhaltenden Datenverschlüsselung genannt, um Datensicherheit auf Feldebene umzusetzen. In diesem Zusammenhang werden auch die vier Möglichkeiten zur Erstellung von synthetischen und referentiell korrekten Testdaten gezeigt, nur via Zugriff auf Metadaten und nicht auf Produktionsdaten.
Dabei ist es egal, ob die Daten lokal und in der Cloud vorhanden sind, oder in welchem un/semi/strukturierten Format sie befinden – ein umfassender Schutz wird gewährleistet!

#2 Datentypen, Datensatz-Layouts, Dateiformate und Endianness neu zuordnen.

#3 Konvertieren von Spaltendaten, Layouts und Beschränkungen zwischen Datenbanken.

#4 Das Schema zu migrieren.

#5 Replizieren oder Kopieren von Daten aus einer oder mehreren Quellen auf ähnliche oder andere Ziele.

#6 Erstellen von Übergaben, persistenten Berichten oder verknüpfte Ansichten.

All diese Faktoren spielen auch eine wichtige Rolle bei der Modernisierung von Daten an sich, denn die Datenmigration ist eng mit der Datenmodernisierung verknüpft. Die Migration von Daten bietet eine Gelegenheit Datenmodernisierungsmaßnahmen umzusetzen mit dem Ziel, die Qualität, Nutzbarkeit und Wertigkeit der Daten insgesamt zu erhöhen. Indem wir Cloud-Migrationen, Datenmigrationen und Datenmodernisierung als sich stetig entwickelnde und miteinander verbundene Bereiche betrachten, können wir sicherstellen, dass die Daten für Anwendungen und Analysen geeignet sind und auch zukünftig bleiben.

Fazit

Die Datenintegration, Datenmigration und Datenmodernisierung tragen dazu bei, die Qualität, Verfügbarkeit und Wertigkeit von Daten zu verbessern. Durch die Integration von Datenquellen, die reibungslose Migration von Daten und die kontinuierliche Modernisierung von Daten können Unternehmen ihre Daten effektiver nutzen und fundierte Entscheidungen treffen, um ihre Geschäftsprozesse zu optimieren und um wichtige Wettbewerbsvorteile zu erzielen.

Amadeus Thomas

MEHR WERT Voracity`s Funktionen und Vorteile: **https://bit.ly/3o6NUdt**

WHITEPAPER DOWNLOAD

Das Whitepaper umfasst 12 Seiten und steht kostenlos zum Download bereit.
www.it-daily.net/download

MIGRATION AUF WINDOWS 11

SO KLAPPT DER UMSTIEG FÜR UNTERNEHMEN

Microsoft stellt für verschiedene Versionen von Windows 10 nach und nach den Support ein. Das offizielle End of Life für Windows datiert das Unternehmen auf den 14. Oktober 2025. Zwar ließe sich Windows 10 theoretisch auch über diesen Zeitpunkt hinaus weiterverwenden, allerdings erhält das in die Jahre gekommene Betriebssystem dann keine Sicherheitsupdates mehr – was besonders für Unternehmen ein inakzeptables Risiko darstellt.

Unternehmen sollten sich daher mit der Migration auf Windows 11 nicht allzu viel Zeit lassen, denn in vielen Fällen ist die Umstellung ein langwieriger Prozess, der auch mit der Anschaffung neuer Hardware verbunden ist.

Das Whitepaper zeigt in systematischer und chronologischer Vorgehensweise alle essentiellen Schritte von der Planung, über die Umsetzung bis zum effizienten Betrieb der aktualisierten Infrastruktur über die Migration hinaus.

THOUGHT LEADERSHIP IN DER IT

Konferenz

27. - 28. September 2023

Online via Zoom

Hier mehr erfahren

#ThoughtLeaderIT

it-daily.net

Das Online-Portal von Itmanagement & Itsecurity

Low Code

NOCH VIELE OFFENE FRAGEN

Im Trend zu Low Code steckt ein großes Versprechen, aber auch relevante offene Fragen und Risiken. Low Code heißt Anwendungsentwicklung auf Basis vorgefertigter Bausteine, die mit wenig oder keinem Hard-Coding auskommt. In der Regel kommen dafür Low-Code-Plattformen zum Einsatz, die in der Cloud residieren. Die Plattformen sind überwiegend als Entwicklungsplattformen konzipiert, die dem Platform as a Service Model (PaaS) folgen. Sie ermöglichen es Benutzern, schlüsselfertige Anwendungen zu entwickeln und unterstützen zahlreiche APIs.

Low-Code-Plattformen versprechen eine deutlich höhere Geschwindigkeit bei der Entwicklung neuer Applikationen und Services. Unternehmen setzen sie sowohl in den IT-Abteilungen als auch außerhalb ein, weil sie auch für Nicht- Programmierer, sogenannte Citizen Developer, schnell erlernbar sind. Die Herausforderungen und Risiken stecken häufig in Fragen von Governance, Infrastruktur-, Daten- und Applikationsmanagement.

Deshalb hat sich der Workstream „Low Code" des CBA Lab intensiv mit diesen Fragestellungen bei der Einführung von Low-Code-Plattformen und -Tools beschäftigt. Die teilnehmenden Unternehmen entwickelten eine detaillierte Checkliste für die Frage, ob eine Low-Code-Plattform eingeführt werden soll. Dabei geht es um Themen wie Security & Risk Management, Enterprise Architecture, Capacity Management oder Systems Integration und APIs. Eingeflossen sind die Best Practices der Low-Code-Nutzung der am Workstream beteiligten Unternehmen.

Low Code wird bereits in vielen Bereichen eingesetzt: angefangen bei Operations (etwa im Workflowmanagement), IT (zum Beispiel im Application Management), Support (etwa UI) bis hin zu Fachbereichen wie HR (Mitarbeiterumfragen), Finanzen (Reporting) oder Marketing (etwa Produktkataloge). Die Berater von Gartner rechnen damit, dass die Zahl der Citizen Developer in großen Unternehmen bis 2023 mindestens viermal so hoch sein wird wie die Zahl der professionellen Entwickler.

ERST DURCH LOW CODE WERDEN DIE VOLLEN MÖGLICHKEITEN ERSCHLOSSEN, AUS DATEN INFORMATIONEN MIT WIRKLICHEM IMPACT AUF DAS BUSINESS ZU GENERIEREN.

Uwe Weber, Botschafter des CBA Lab und Initiator des Workstreams, www.cba-lab.de

„Citizen Developer werden tendenziell in einfacheren Projekten zum Zuge kommen, während komplexere Projekte bei den Profis verbleiben. Allerdings rechnen wir auch damit, dass die Zusammenarbeit von Citizen Developern und Profis nicht nur die eigentliche Entwicklung beschleunigt, sondern auch das Anforderungsmanagement einfacher macht", erklärt Workstreamorgansiator Hendrik Grosser von Detecon.

Identifizierte Problemfelder

Dennoch sehen die Mitglieder des Workstreams noch zahlreichen Lösungsbedarfe. Dazu zählen:

- Mangelndes Verständnis von Business Usern und Citizen Developern,
- Probleme bei der Integration zur Anbindung aller relevanten Systeme, um den vollen Nutzen auszuschöpfen,
- Low-Code-Systeme sind nicht immer auf Leistung ausgelegt und können zu Ineffizienz bei der Benutzung führen,

ÜBER DAS CROSS-BUSINESS-ARCHITECTURE LAB

Das CBA Lab ist ein Anwenderverband von Unternehmen aus allen Wirtschaftszweigen, die gemeinsam neue Best Practices erschließen, erarbeiten und trainieren. Es erarbeitet mit und für seine Mitglieder innovative „Bausteine" für die Digitale Transformation, die die Architektur prägen und organisieren. Am Cross-Business-Architecture Lab beteiligen sich CIOs, CDOs und Chefarchitekten aus führenden Unternehmen und Organisationen im deutschsprachigen Raum. Die Mitglieder profitieren vom gemeinsamen Netzwerk und dem Vertrauensraum des Verbandes, der sie sehr offen Know-how und Ideen teilen lässt.

- Datenschutz- und Sicherheitsrisiken müssen beim Einsatz berücksichtigt werden,
- Abbildung des Software Development Lifecycle für Low Code (Design, Test, Deployment),
- Risiken der Fragmentierung durch den Einsatz mehrerer spezialisierter Plattformen,
- Risiko von Vendor Lock-In,
- Training von Mitarbeitenden für den Einsatz der jeweiligen Plattform und in der agilen Zusammenarbeit.

Fazit

Trotz der noch bestehenden Fragestellungen ziehen die Unternehmen im Workstream ein positives Fazit.

Die Performance steigt. Für einfache Produkte ist die Low-Code-Entwicklung hinsichtlich der Schnelligkeit und geringen Bindung von Ressourcen unschlagbar, so das Ergebnis. Allerdings sollten Unternehmen bei komplexen Produkten nicht auf klassische Programmierung verzichten und anhand der Checkliste gründlich abwägen. Die Plattformen bieten ein reiches Spektrum an Instrumenten, die zentral verwaltet werden. Durch ihre einfache Bedienung stehen sie dem gesamten Unternehmen zur Verfügung. Die IT-Abteilung wird entlastet. Durch den einfachen Einstieg der Low-Code-Plattformen können die Fachbereiche selbstständig Produkte nach ihren individuellen Bedürfnissen gestalten.

Das schafft zeitliche Freiräume für die IT-Abteilung, sodass die Developer sich auf kritische Kernanwendungen fokussieren können.

Citizen Developer sollten von einer Community und mit Datentransparenz unterstützt werden. Insbesondere für Citizen Developer sind eine Low Code Community sowie ein Center of Excellence sehr hilfreich: einerseits, um Menschen ohne Coding-Background zu ermutigen, selbstständig Produkte zu entwickeln - andererseits, um Anleitung zu bieten, die insbesondere in der ersten Phase notwendig ist. Weiterhin sollten Daten transparent auffindbar und über Access Control verwendbar sein.

Uwe Weber

ZUSAMMENFASSUNG

FÜR EINE ERFOLGREICHE LCDP-ANWENDUNG MÜSSEN ENTSCHEIDUNGEN NACH GEWISSEN KRITERIEN VON VERSCHIEDENEN ROLLEN UND GREMIEN GETROFFEN WERDEN.

Low Code-Governance @ 2023 Cross-Business-Architecture Lab e. V.

EntscheiderInnen

Entscheidungs-UnterstützerInnen

Gremien & Unternehmens-bereiche

Architektur	Infrastrukture	Plattformbetrieb	Integration	Applikationsentwicklung und -betrieb	Business Support	Business Nutzung
Führt das Unternehmen LCDPs ein oder nicht	Soll die LCDP On Prem oder cloudbasiert laufen?	Wie und von wem (in welcher Organisationsstruktur) soll die entsprechende Plattorm bereitgestellt / betrieben werden?	Welche Basissysteme dürfen angebunden werden?	Welche Pllikation soll auf welcher bestehenden Plattform entwickelt werden?	Welche Prozesse des Applikationslebenszyklus müssen durchgeführt werden?	Wer darf die Applikation wie nutzen?
Was ist der Ansatz bei LCDPs (Self Service vs. Demand Management vs. „Zwischending“) und für welche Art von Tätigkeiten?	Braucht die Organisation bei der Einführung von LCDPs zusätzliche Infrastruktur / Ausstattung?	Welche Sicherheitsvorgaben müssen beachtet werden?	Welche Daten (quellen) dürfen verwendet werden?	Welche Prozesse des Applikationslebenszyklus müssen durchgeführt werden?	Wie sind die Qualitätstandards beim Business Support?	
Welche Plattformen werden eingeführt?		Welche Trainingskonzepte soll es für Citizen Developer geben?	Wer darf auf was zugreifen?	Wie sind die Qualitätsstandards bei der Entwicklung / Betrieb?	Wer übernimmt welche Teiltätigkeiten?	
Welche Applikationen müssen in der Architektur erfasst werden?				Wer macht was (wer übernimmt welche tätigkeiten)?		

DAS NÄCHSTE LEVEL

WIE LOW CODE TECHNOLOGIE ERP-PROZESSE PERFEKTIONIERT

ERP-Systeme bilden komplexe Geschäftsprozesse ab und sind die Grundlage, um diese integriert und effizient abzuwickeln. Dabei ist es essenziell, auf individuelle Gegebenheiten von Unternehmen einzugehen, weshalb ERP-Systemeinführungen in der Regel lange und gut vorbereitet werden. Einer detailreichen Anbieterauswahl folgen hohe zeitliche und finanzielle Investitionen, um das System bestmöglich an die Anforderungen des einzelnen Unternehmens anzupassen.

In der Praxis zeigt sich dennoch: Kaum ein ERP-System bildet alle Prozessdetails wirklich optimal ab. Die letzten 10 bis 20 Prozent sind häufig nur unter immensem Ressourceneinsatz zu realisieren oder können gar nicht abgebildet werden. Doch genau in dieser „Last Mile" steckt für viele Unternehmen – speziell im Mittelstand – ihr Wettbewerbsvorteil. Ein wichtiger Grund, weshalb sie nicht darauf verzichten können und hohe Summen für individuelle ERP-Anpassungen ausgeben. Hier setzt Low Code Technologie an und verspricht einen neuen, flexiblen und effizienten Ansatz: Was in einem ERP-System nicht passt, kann Low Code noch geradebiegen.

Die ERP-Basis perfektionieren

Jeder, der im Unternehmen eine ERP-Einführung begleitet hat, weiß, dass dieser Prozess den Beteiligten oftmals zeitlich, monetär und psychisch viel abverlangt. Deshalb fühlen sich Unternehmen oft im „Lock-in", wenn Prozesse am Ende nicht so abgebildet werden, wie man es sich eingangs vorstellte. Einerseits ist der Prozess nicht optimal, andererseits sind die zeitlichen und finanziellen Ressourcen jedoch aufgebraucht. Aufbauend auf vorhandenen Systemen ermöglichen Low-Code-Plattformen in dieser Situation, ERP-Abläufe bedarfsgerecht und individuell zu perfektionieren. Beispiele hierfür sind vielfältig, von der mobilen Unterstützung im Kommissionierungsprozess über eine individuelle Vertriebsaußendienst-App bis hin zur Eliminierung letzter, noch papierbasierter Prozesse im Shopfloor. Low Code Apps können dabei einfach und anwenderorientiert umgesetzt und nahtlos mit dem ERP-System verknüpft werden – am Beispiel der Low-Code-Plattform von engomo erfolgt die Konfiguration von App-Interfaces per Drag&Drop und die Systemintegration über vorhandene REST-Schnittstellen und systemspezifische Konnektoren in wenigen Schritten. So ist gewährleistet, dass die Datenflüsse optimal abgebildet sind und keine neuen Datensilos und Insellösungen entstehen.

Wünsch Dir was

Wäre so etwas möglich, dann wäre die Antwort der Anwender sicher: Individuell und benutzerfreundlich im Frontend, datenintegriert im Backend. Für die Mitarbeiter im Unternehmen bedeutet dies, dass sie in bestimmten Prozessen ohne die Bedienung komplexer ERP-Software

auskommen, sondern ihre Aufgaben unterstützt durch intuitive, prozessorientierte Apps schneller und einfacher abwickeln können. Gleichzeitig schaffen Echtzeit-Datenübertragung und Integration mit vorhandenen Systemen die Möglichkeit, jederzeit auf aktuelle Daten aus den Backend-Systemen zuzugreifen und im Prozess anfallende Informationen auch dorthin zurückzuschreiben.

Systemübergreifende Prozesse im Fluss abbilden

Systemlandschaften in Unternehmen sind inzwischen so umfangreich und komplex, dass es kaum noch Prozesse gibt, an denen nicht mehrere Backend-Systeme beteiligt sind. Auftragsdaten kommen aus dem ERP-System, die Fertigungsplanung wird im PPS gemacht, Qualitätsdaten müssen wiederum im QS-System hinterlegt werden – Anwender haben häufig für einen Prozess verschiedene Systeme zu bedienen und der Datenaustausch zwischen diesen ist nicht automatisch gewährleistet. Low Code Technologie ermöglicht durch eine hohe Backend-Kompatibilität, dass Prozesse mit verschiedenen Systembeteiligungen im Ganzen abgebildet werden. In sogenannten „Composite Apps" können in einer Anwendung Daten aus verschiedensten Datenbanken und Systemen abgerufen und dorthin zurückgespeichert werden. Während die wenigsten Systeme in der Lage sind, miteinander zu kommunizieren, fungiert eine Low-Code-Plattform hier als zentraler Hub, der dafür sorgt, dass ein nahtloser Prozess entsteht, in dem alle relevanten Informationen vorhanden sind.

Low Code: weniger Aufwand, bessere Prozesse

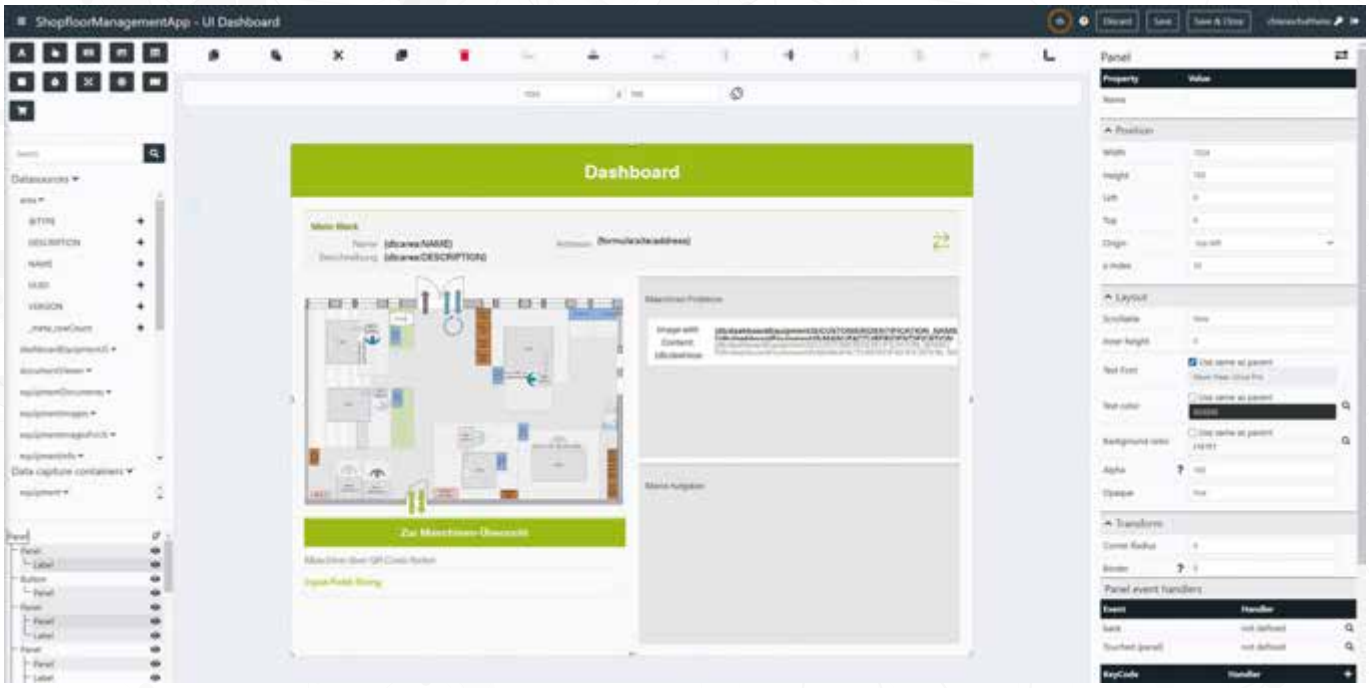
Während ERP- und andere Enterprise Systeme die individuellen Prozesse im Unternehmen bereits grundlegend abbilden und Datenstrukturen bieten, die optimal auf das Unternehmen zugeschnitten wurden, ermöglicht Low Code das nächste Level. Systemlücken werden geschlossen, noch papierbasierte Prozesse werden digitalisiert und prozessübergreifende Abläufe optimal abgebildet. Besonders daran ist, dass Low-Code-Plattformen das in viel kürzerer Zeit ermöglichen als die klassische Art der Systemintegration und Projekt-Programmierung.

MIT DEN MÖGLICHKEITEN VON LOW-CODE LASSEN SICH ERP-SYSTEME EINFACH UND SCHNELL INDIVIDUALISIEREN UND OPTIMIEREN.

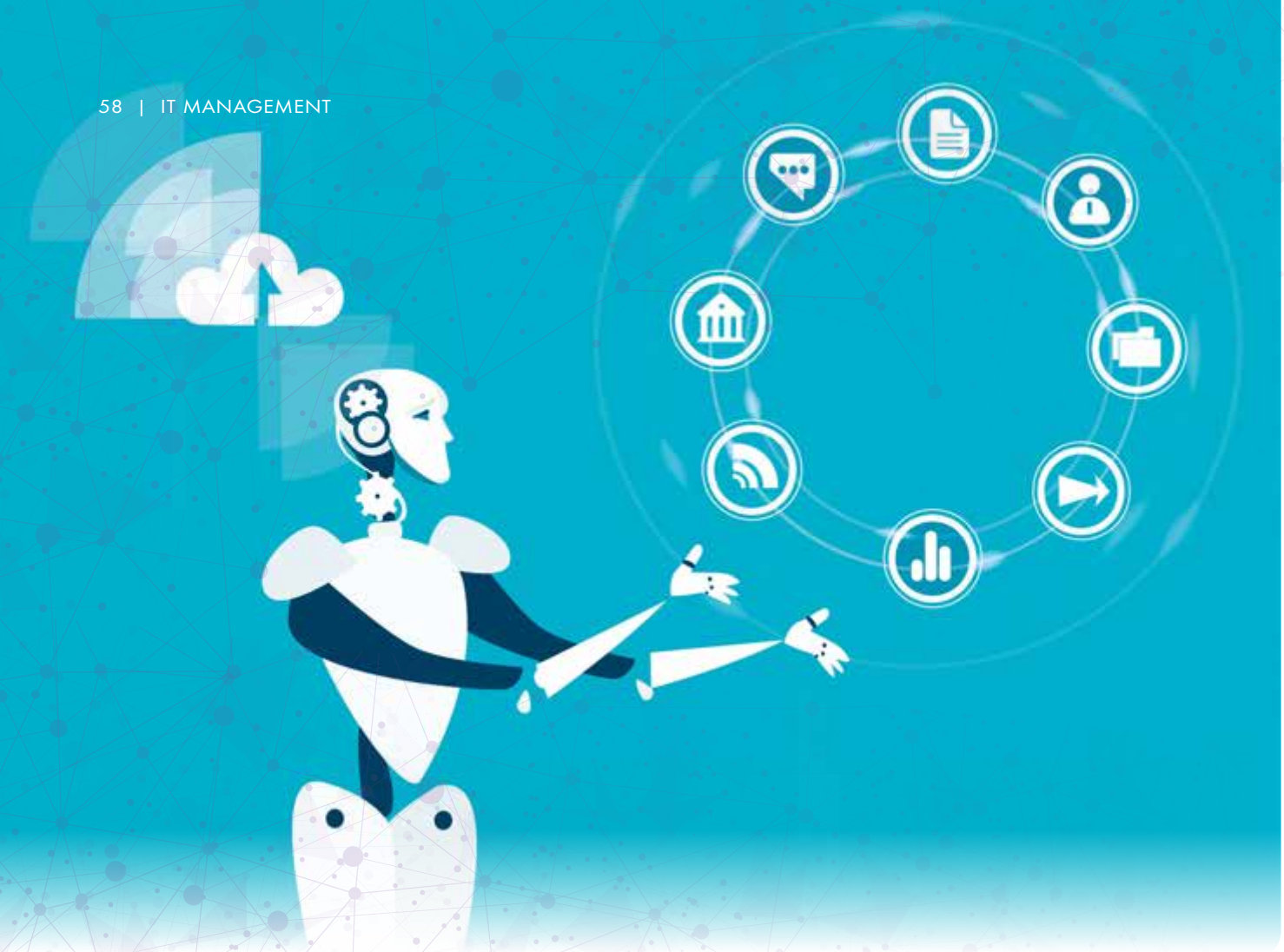
Kerstin Stier,
Mitgründerin und Geschäftsführerin,
engomo GmbH,
https://engomo.com

Das bedeutet, dass Low Code im Zusammenhang mit ERP zu deutlich reduzierten Kosten und ohne umfangreiche IT-Projekte schnelle, leichtgewichtige Lösungen und perfekte ERP-Abläufe ermöglicht.

Kerstin Stier



App-Editor für Anwendungen ohne Programmierung: **Die App-Konfigurationsoberfläche der Low-Code Plattform engomo ermöglicht das Erstellen von App-Interfaces per Drag&Drop.** (Quelle: engomo)



Auf dem Weg zur Hyperautomation

LÖSUNGSINTEGRATION AUCH JENSEITS VON RPA

Robotic Process Automation (RPA) hat sich zu einer zentralen Lösung in nahezu jedem Geschäftsumfeld entwickelt, denn damit lassen sich erhebliche Zeit- und Kosteneinsparungen erzielen und die Mitarbeiter werden produktiver und zufriedener. So ergab eine Umfrage von Deloitte, dass die Unternehmen, die RPA-Methoden erfolgreich eingeführt haben, einen ROI in weniger als zwölf Monaten erreichen. Vor allem bei einfachen und repetitiven Aufgaben kommt RPA zum Einsatz. Hier übernehmen die Bots Aufgaben, die viele Menschen häufig als lästig und überflüssig empfinden. Hinzu kommt der gegenwärtige und weit verbreitete Fachkräftemangel, sodass RPA in vielen Unternehmen hoch im Kurs steht. Laut Precedence Research soll der RPA-Markt bis 2030 auf 24 Milliarden US-Dollar anwachsen.

Viele Projekte scheitern

Doch trotz der vielen potenziellen Vorteile scheitern immer noch eine ganze Reihe an RPA-Projekten oder kommen nicht über die Anfangsphase hinaus. So ergab eine weitere Deloitte-Umfrage, dass nur drei Prozent der Unternehmen ihre „digitale Belegschaft" skalieren konnten. Die häufigsten Ursachen dafür waren mangelhafte Vorgaben und schlechte Umsetzungen. Das Problem wurde noch verschärft, weil viele Unternehmen RPA lediglich als schnelle Lösung für akute Produktivitätsprobleme einsetzen wollten. Zwar kann die isolierte Automatisierung von Teilen eines Workflows zu schnellen Erfolgen führen, doch löst das nicht die komplexeren Prozessprobleme der gesamten Organisation. Heute sind Lösungen gefragt, die weit über RPA hinaus gehen; Stichwort Hyperautomation. Laut Gartner handelt es sich dabei neben RPA um die orchestrierte Nutzung verschiedener Technologien, wie Business-Process-Management (BPM), künstlicher Intelligenz (KI), maschinellem Ler-

nen (ML), ereignisgesteuerten Softwarearchitekturen, Integration Plattform als Service (iPaaS), Low-Code/No-Code-Tools sowie andere Arten von Entscheidungs-, Prozess- und Aufgabenautomatisierungstools. Ein breites Spektrum also, das weit über RPA hinaus geht.

Pures RPA ist harmlos – Hyperautomation ist es nicht

Die erweiterte Nutzung von RPA im Rahmen der Hyperautomatisierung führt inzwischen zu immer größeren IT-Anpassungsproblemen. Das erscheint zunächst paradox, schließlich lässt sich RPA ohne Änderungen mit praktisch allen bestehenden Anwendungssystemen betreiben. Doch das stimmt nur, solange der Bot menschliche Aufgaben genau 1:1 ausführt. In diesem Fall ist der Bot gegenüber der Anwendung nur ein weiterer User. Anders ist es dagegen, wenn eigenständige Verarbeitungen, Zwischenspeicherungen, Analysen und Ausgaben erfolgen. Hier sind alle Vorgaben zur Softwareentwicklung und des korrekten Betriebs einzuhalten – inklusive der Anbindungen an die Anwendungen und Datenbanken. Wenn man jetzt noch bedenkt, dass die IT normalerweise eine heterogene und komplexe Architektur aufweist, dann ergeben sich hohe Anforderungen bezüglich Sicherheit, Skalierbarkeit, Monitoring und Auditing an RPA. Ganz generell lässt sich sagen: Je komplexer die Prozesse sind, umso mehr Abhängigkeiten entstehen, und das bedeutet mehr Dokumentationen, Fehlermöglichkeiten und auch die Gefahr von Technical Debt.

Die IT-Abhängigkeiten betreffen aber nicht nur die Bot-Erstellung, sondern noch stärker die Maintenance. Schon eine kleine Anpassung in einer Anwendung – beispielsweise im Zuge eines Updates – kann zur Folge haben, dass der Bot eine Schaltfläche nicht mehr findet – und schon läuft die gesamte RPA-Implementierung bei dieser Applikation ins Leere. Weitere Anpassungen sind auch dann erforderlich, wenn sich die Benutzeroberfläche oder der Prozessablauf ändert, für die der Bot programmiert wurde. Das zeigt die inhärente Abhängigkeit von RPA von der IT, bei der die Bot-Wartung oftmals die Kosten der ursprünglichen Erstellung deutlich übersteigt.

Schnelle Anpassung dank Low-Code

Um die Bots schnell und kostengünstig zu erstellen und deren laufende Anpassungen ohne Beeinträchtigung der Business-Performance zu ermöglichen, haben sich Low-Code-Automatisierungsplattformen auf breiter Front etabliert. Sie bilden ein effizientes Netz zwischen den Personen, den Bots und der IT-Umgebung. Über leistungsstarke Low-Code-Automatisierungsplattformen lassen sich heute alle Prozesse unter Berücksichtigung der IT-Vorgaben in kürzester Zeit und ohne Reibungsverluste abbilden. Beispielsweise können über die visuelle Konfigurationsoberfläche einer solchen Plattform kleinere Anpassungen ohne Zuhilfenahme der IT direkt von den Fachabteilungen umgesetzt werden. Moderne Low-Code-Automatisierungsplattformen sind heute ein ideales Hyperautomatisierungstool. Sie bieten viele visuelle Hilfsmittel, mit denen die User die Prozesse so einfach wie das Zeichnen eines Flussdiagramms skizzieren können. Vorkonfigurierte Komponenten, die Workflow-Aktivitäten und Automatisierungen darstellen, können per Drag & Drop in ein visuelles Prozessmodell gezogen werden. Da diese Komponenten für den Aufbau zukünftiger Workflows wiederverwendbar sind, können Teams an Agilität gewinnen – ein wichtiges Ziel der Arbeit an der digitalen Transformation. Und sie unterstützen die Nutzung smarter Technologien, wie KI und ML. Die Folgen dieser weitreichenden Nutzung einer solchen Plattform zeigen sich auch an den Zahlen. So erwartet Gartner, dass der weltweite Markt für Low-Code-Technologien in diesem Jahr ein Volumen von 27 Milliarden US-Dollar erreichen wird – 20 Prozent mehr als im Vorjahr.

Auswirkungen auf die IT-Architektur

Die Auswirkungen auf die IT durch Hyperautomation, insbesondere RPA, hängen von der Komplexität der zu automatisierenden Prozesse ab. Dabei sind drei verschiedene Komplexitätsgrade zu unterscheiden:

#1 Routineaufgaben, bei denen Daten aus unterschiedlichen Anwendungssystemen kopiert oder kombiniert werden.

#2 Strukturierte Aufgaben mit regelbasierten Entscheidungen, bei denen Daten aus unterschiedlichen Anwendungssystemen verwendet und anhand eines Regelwerks ausgewertet werden.

#3 Unstrukturierte Aufgaben und Entscheidungen, die zusätzlich zu bestehenden Daten und Regeln Erfahrungswissen erfordern.

Der erste Fall ist der klassische I/O-Bot, der sich wie ein User verhält und keine weitere Interaktion mit der IT vornimmt. Der zweite Fall muss genauer beleuchtet werden: Wo sind die Regeln gespeichert, wer definiert und kontrolliert sie, gibt es

DIE AUSWIRKUNGEN AUF DIE IT DURCH HYPERAUTOMATION, INSBESONDERE RPA, HÄNGEN VON DER KOMPLEXITÄT DER ZU AUTOMATISIERENDEN PROZESSE AB.

Dirk Pohla,
Area Vice President, Appian,
www.appian.com

Zwischenspeicherungen von Daten; falls ja, sind diese konform mit Datenschutz und Sicherheit?

Herausfordernd sind die neuen unstrukturierten Aufgaben und Entscheidungen. Hier kommen komplexe KI- und ML-Techniken zum Einsatz und das bedeutet völlig neue Implikationen für die Einbindung von RPA in die bestehende IT-Infrastruktur. So können sich durch den Einsatz dieser Technologien die Verarbeitungsweisen eines Bots signifikant ändern und somit möglicherweise die erforderliche Prozess-Transparenz und die Einhaltung von Compliance-Auflagen verloren gehen. Dem muss die IT von Anbeginn an durch entsprechende Monitoring-Maßnahmen entgegenwirken.

In allen drei Fällen besteht ein potenzielles Security-Risiko, was sich daraus ergibt, dass die Software-Roboter über ihre Präsentationsschicht mit den darunter liegenden Anwendungs-Systemen kommunizieren müssen. Das bedeutet, auch jeder Bot muss sich jeweils als Instanz des RPA-Systems vorher mit einer eigenen Benutzerkennung einloggen. Doch jedes Zugriffsrecht ist immer eine potenzielle Quelle von Datenlecks. Deshalb versucht die IT, die gewährten RPA-Berechtigungen möglichst gering zu halten sowie zusätzliche Kontrollmechanismen einzubauen, um das Risiko zu mindern – beispielsweise mithilfe von Zero Trust.

Deployment: Cloud oder On-Prem?

RPA-Bots werden normalerweise auf einer zentralen, vernetzten Infrastruktur eingesetzt. Wichtig ist dabei die Einhaltung der Sicherheitsvorgaben und die Gewährleistung der Service- und Business-Continuity des gesamten Unternehmens. Zu den zentralen RPA-Steuerungskomponenten zählen längst alle erforderlichen Funktionen, die jede unternehmensweit eingesetzte Software hinsichtlich Sicherheit, Compliance, Skalierung und Ausfallsicherheit erfüllen muss. Physisch kann das alles sowohl lokal als auch in einer sicheren Cloud-Umgebung eingerichtet werden, beispielsweise auf der besonders abgesicherten Appian-Cloud, über die dann alle Windows-, Linux-, Citrix- und Mac-Umgebungen darauf zugreifen können. Cloud-Lösungen sind unter anderem auch deshalb vorteilhaft, weil eine erfolgreiche RPA-Strategie ein Höchstmaß an Skalierbarkeit verlangt.

RPA zur IT-Automatisierung

Heute gehören zum IT-Management immer noch viele manuelle Aufgaben und Prozesse, die zur Gestaltung und zur Wartung der Infrastruktur erforderlich sind. Zukünftig sollte RPA auch für die Automatisierung dieser Prozesse zum Einsatz kommen, um so die IT-Architektur anpassungsfähiger zu machen und gleichzeitig den Administrationsaufwand zu minimieren.

Dirk Pohla

WAS SIND DIE GRÖSSTEN HINDERNISSE FÜR DIE VERBREITUNG VON RPA?

(Quelle: Deloitte: The robots are waiting; 2018)

Jeden Monat, jeweils am Wochenende, ein aktuelles Fokusthema mit spannenden Fachartikeln, interessanten Use Cases & Analysen:

Hier geht's zum neuen

it-daily Weekend

++ **April:** ChatGPT ++ **Mai:** Digital Twins ++ **Juni:** Ransomware ++ **Juli:** Quantencomputing ++

Moderne CMS

MIT HEADLESS NIE WIEDER UPDATES!

Digitalagenturen, die es seit mehr als zehn Jahren gibt, haben alle eines gemeinsam: Updates in ihren Content-Management-Systemen. Das ist lähmende Arbeit, für die Kunden oft nicht zahlen wollen, da sie keinen wirklichen Mehrwert in den Updates sehen. Entwickler verabscheuen die Arbeit ebenfalls. Mit alternativen CMS-Systemen, wie SaaS-basierte Headless CMS, gehören klassische Problemevon Updates der Vergangenheit an. Doch, wie funktioniert der Umschwung auf die neueren Systeme? Und welche Vor-/Nachteile bietet der Wechsel sonst?

„Der Wandel ist die einzige Konstante" ist eines meiner Lieblingszitate. Ich sage das, weil es die heutige digitale Welt, die von Fortschritt geprägt ist, sehr treffend definiert. Aus Erfahrung weiß ich aber auch, dass die digitale Landschaft seit Jahrzehnten eine Herausforderung für Digitalagenturen darstellt. Vor allem solche, die seit mehr als einem Jahrzehnt bestehen, haben eine ganz zentrale Herausforderung gemeinsam: Die Aktualisierungen ihrer Content Management Systeme (CMS).

Aber warum sind die Updates überhaupt ein Problem? Ganz einfach: Sie sind zeitaufwendig, teuer und werden von Kunden der Agentur oft nicht gewürdigt. Durch die Wahl neuerer CMS-Architekturen profitieren Unternehmen jedoch von einem wesentlichen Vorteil: der Abschaffung der manuellen Aktualisierungen im Content Management.

CMS-Historie

Um zu verstehen, wie wichtig es ist, die am besten geeignete CMS-Architektur für die Kunden oder auch das eigene Vorhaben zu wählen, ist es wichtig, die Geschichte und Entwicklung von CMS besser zu kennen. Das erste Konzept für systematisches Content-Management kam erstmals in den 1990er Jahren auf den Markt. Damals entwickelten Webdesigner die Anwendungen noch selbst und nutzten keine externen Lösungen. Also hatte jede Agentur ihre eigene Version eines CMS und jede kam mit eigenen Limitationen.

Im Jahr 2000, unmittelbar nach dem Dotcom-Crash, verlagerte sich der Schwerpunkt der meisten Marketingagenturen jedoch von der Code-Entwicklung auf das Design. Damit erhielt die zweite Welle von CMS-Plattformen Einzug, die nun die großen sowie kleinen Softwarehäuser entwickelten. Diese Plattformen konzent-

EIN SAAS-BASIERTES HEADLESS CMS IST EIN CONTENT-MANAGEMENT-SYSTEM, DAS NUR DEN BACK-END-DATENSPEICHER ENTHÄLT. DER INHALTSSPEICHER IST DABEI VON DER FRONT-END-PRÄSENTATIONSSCHICHT GETRENNT.

Barry D'Arcy, Vice President of Sales, Storyblok GmbH, www.storyblok.com

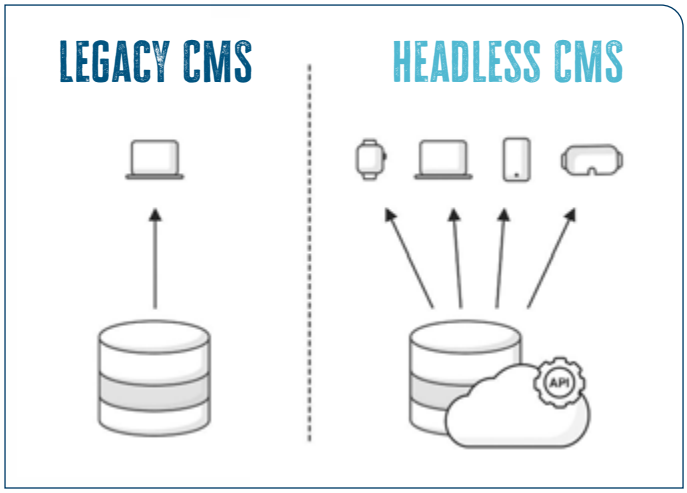


Bild 1: **Architektur eines Legacy- und eines Headless CMS im Vergleich**

rierten sich auf WYSIWYG-Textbearbeitung (What you see is what you get; visuelle Editoren), SEO und verbesserte Benutzeroberflächen. Allerdings waren sie extrem teuer und vollkommen entwicklungsabhängig.

Die in den 2000er Jahren entwickelten CMS-Plattformen waren außerdem auf die Bereitstellung von Inhalten für einen einzigen Kanal – zu der Zeit Websites – beschränkt. Mit der mobilen Revolution, dem Aufkommen des Omnichannel-Publishings und der neuen Möglichkeiten durch Skriptsprachen wie JavaScript entstand vermehrt der Bedarf an Content-Management-Systemen, die dieser Transformation gerecht werden konnten. Die Benutzer mussten ihre Inhalte schließlich dorthin bringen, wo die Zielgruppe sie auch sieht. Da zeitgleich jedoch immer mehr Endgeräte mit verschiedenen Betriebssystemen auf dem Markt erschienen, wuchs die Nachfrage nach einheitlichem Content-Management. Das war die Geburtsstunde der Headless CMS. Der Headless-Ansatz bietet eine größere Flexibilität bei der Verwaltung von Inhalten und mehr Optionen, die vielseitigen Kanäle zu bespielen.

Mit einem Headless CMS können Benutzer nun neue Technologien integrieren, sobald sich diese auf dem Markt behaupten oder generell auftauchen – das macht den Headless-Ansatz so populär.

Mittlerweile gibt es sogar Organisationen wie die MACH Alliance, die es sich zusätzlich zur Aufgabe gemacht haben, sich für die neueren und anpassbaren Alternativen zu älteren Systemen einzusetzen, um Unternehmen die heutzutage nötige Flexibilität zugänglich zu machen.

Monolithische vs. Headless CMS

In den Anfängen des Internets brauchte es nur ein System, mit dem Inhalte bereitgestellt und verwaltet werden konnten. Zu dieser Zeit erfüllten die monolithischen Content-Management-Systeme einen wichtigen Zweck. Bis heute basiert etwa ein Drittel aller Websites auf monolithischen CMS wie beispielsweise WordPress, Drupal und Joomla. Die monolithischen Content-Management-Architekturen bieten dabei ein All-in-One-System, bei dem Inhalte und Code miteinander vermischt sind. Dadurch entsteht oft eine sehr umfangreiche, dennoch hilfreiche Codebasis, die alles Notwendige für die Verwaltung und Veröffentlichung von Inhalten im Web vereint.

Da das Backend, in dem Daten gespeichert sind, und das Frontend, dass das Präsentationslayout der Daten darstellt, miteinander verbunden sind, ergeben sich bei komplexeren Websites jedoch schnell Einschränkungen. Was für einfache Firmenwebsites, Blogs und anderweitige Webauftritte viele Vorteile bieten kann, wird für E-Commerce und Co. mit geringerer Leistung und Geschwindigkeit, niedriger Datensicherheit, höheren Kosten, übermäßig notwendigen Plug-ins und

wenig Spielraum für die Kreativität der Entwickler bestraft.

Mit zunehmender Nutzung vieler Content-Kanäle, auf die vor allem der E-Commerce angewiesen ist, und den veränderten Kundenpräferenzen, die mit der Nutzung intelligenter Geräte einhergingen, bedarf es einem neuen CMS: Eines, das der Zielgruppe die Inhalte auf jede Art und Weise bereitstellen kann. Darüber hinaus besteht oft die Notwendigkeit, die Inhalte schnell, sicher und kostengünstiger bereitzustellen – spätestens dann muss der Wandel zu Headless stattfinden.

Vorteile von Headless CMS

Ein Headless CMS ist ein Content-Management-System, das nur den Back-End-Datenspeicher enthält. Der Inhaltsspeicher ist dabei von der Front-End-Präsentationsschicht getrennt. Auf die dort gespeicherten Inhalte kann also nur über APIs (Schnittstellen) zugegriffen werden. Das heißt aber nicht, dass sie unzugänglich sind, sondern eben, dass es nur einen einzigen Zugriffspunkt – die Schnittstelle – gibt, von der das Frontend die Inhalte abruft. Die Headless-Architektur für das Content Management bietet dabei eine größere Flexibilität bei der Verwaltung, vor allem wenn Inhalte schnell unübersichtlich werden, und mehr Optionen für die Veröffentlichung ebendieser über verschiedene Kanäle.

Content-Manager spielen den Content durch Headless letztendlich auf einer Website, in einer Anwendung, auf einem tragbaren Gerät oder sogar auf ausgefallenen Geräten wie High-End-Kühlschranken, aus. Da Headless CMS meist in der Cloud und somit losgelöst von Hardware-Anforderungen laufen, können Manager die Inhalte von jedem beliebigen Ort aus verändern, verwalten und veröffentlichen. Vergleicht man die beiden Architekturen, werden vor allem die großen Nachteile monolithischer CMS für anspruchsvolle Websites deutlich, die Nutzer mit dem Wechsel zu Headless beheben können

Das Headless Dilemma

Wer von CMS-Updates spricht, muss zuerst die verschiedenen Anwendungen erwähnen, in denen Content-Management-Systeme verbreitet werden. Dabei unterscheidet man generell zwischen zwei Methoden: proprietäre Software und Open-Source-Software (OSS). Bei OSS handelt es sich um Software, die mitsamt ihres Quellcodes vertrieben wird, so dass sie mit ihren ursprünglichen Rechten zur Nutzung, Änderung und Verbreitung zur Verfügung steht.

Bei proprietärer Software ist der Quellcode das Eigentum der Entwickler und kann nachträglich nicht verändert werden. Bei dieser Art von Software kauft man also nicht die Software selbst, sondern die Lizenz für ihre Nutzung. Proprietäre Software ist dafür aber in den meisten Fällen, nach kurzer Implementierung und möglicherweise Anbindung an Integrationsdienste, sofort einsatzbereit. Dadurch ist sie auch für technisch nicht versierte Personen leicht zu verwenden. Eine OSS wiederum muss mit hoher Wahrscheinlichkeit zuerst von Grund auf mit neuem Code entwickelt werden.

Vor- und Nachteile

Auch wenn OSS mehr Flexibilität und Anpassungsmöglichkeiten bietet, verzögert sich die Bereitstellung durch den zum Einsatz notwendigen Code erheblich und es entstehen zusätzliche Kosten. Darüber hinaus ist proprietäre Software wesentlich stabiler als Open-Source-Alternativen. Bevor Entwickler den Code für die Öffentlichkeit freigeben, stellen sie sicher, dass ihre Software umfangreiche Testverfahren, Qualitätssicherungsprüfungen und Schwachstellenchecks durchlaufen.

Schließlich können die Kosten für die Pflege des Supports für OSS sehr hoch ausfallen, wenn man die Ressourcen berücksichtigt, die für die Sichtung, Behebung, Prüfung und Bereitstellung von Fehlerbehebungen erst einmal erforderlich sind.

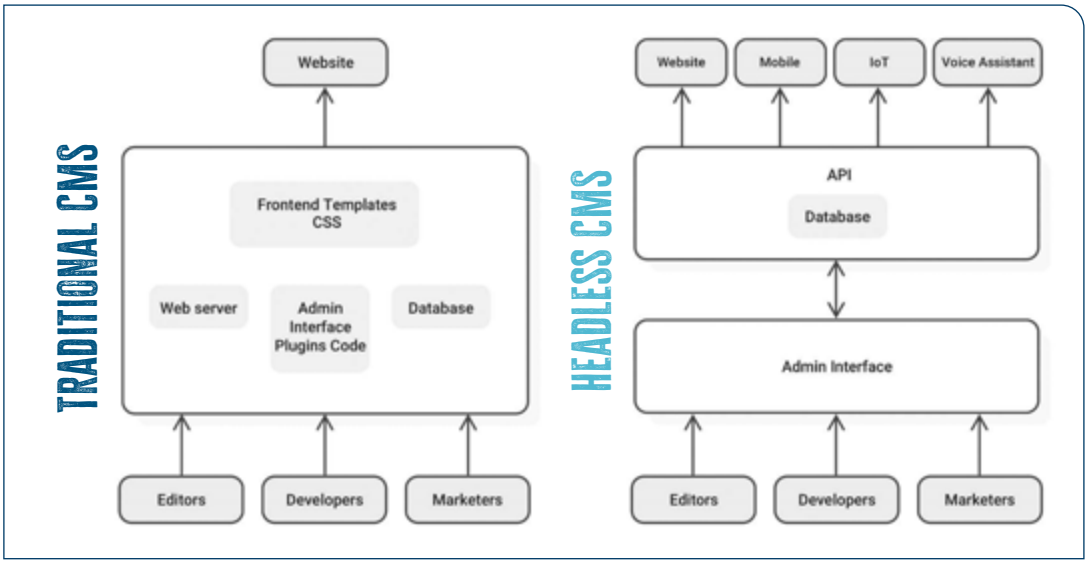


Bild 2: Architektur eines monolithischen und eines Headless CMS im Vergleich

MONOLITHISCHE CMS	SAAS-BASIERTES HEADLESS CMS
Geringere Leistung	Höhere Performance
Oft sind Plugins nötig, die die Geschwindigkeit und Leistung einer Website verringern, da jedes von ihnen einen Code hinzufügt. Die Endgeräte führen diesen Code bei jedem Website-Besuch aus, auch "Rendering" genannt.	Der API-gesteuerte Ansatz bietet leistungsstärkere Methoden für das Rendering von Seiten. Die Geschwindigkeit der Website kann sich durch den Einsatz fortschrittlicher Tools, Bibliotheken und Frameworks für Web-Technologien erhöhen.
Waterfall Management	Agiles Management
Aktualisierungen des CMS können manchmal mehrere Wochen dauern, ohne dass für Kund:innen eine sichtbare Veränderung eintritt.	Kontinuierliche Veröffentlichungen und Einbeziehung des Kundenfeedbacks bei jeder einzelnen Iteration ist durch die Trennung von Front- und Backend einfach möglich.
Hoher Kostenfaktor	Niedriger Kostenfaktor
Da Backend und Frontend gekoppelt sind, kann es lange dauern, bis Projekte zur Bereitstellung und Verwaltung von Inhalten abgeschlossen sind. Darüber hinaus sind die Entwickler:innen gezwungen, sich in die Verwendung Anbieter-spezifischer Frameworks einzuarbeiten. Das erhöht die Arbeitskosten erheblich.	Die kürzere Zeit für die Bereitstellung von Inhalten für alle Kanäle bedeutet in dem Fall, dass Vermarkter:innen Projekte in wenigen Tagen statt in mehreren Wochen abschließen können. Auch die Entwickler:innen können Projekte schneller abschließen, da sie Zugang zu fortschrittlicheren Tools haben. Die Arbeitskosten sinken.
Niedrige Sicherheit	Hohe Sicherheit
Die Inhalte werden allesamt in physischen Speichern bzw. Datenbanken und direkt zugänglich gespeichert. Datenbankgestützte Systeme sind anfällig für DDoS- und ähnliche Sicherheitsangriffe.	Verbesserter Schutz vor unerwarteten Datenverkehrsspitzen, wie beispielsweise bei DDoS-Attacken und Sicherung vor Datenverlust, da die Inhalte sicher in der Cloud gespeichert sind. Der einzige Zugangspunkt bleiben die Schnittstellen, was die Angriffsfläche für Sicherheitsangriffe aller Art verringert.
Lange Entwicklungszeiten	Kurze Entwicklungszeiten
Mit jedem Gerät und jeder Version muss ein neues Frontend erstellt werden. Dadurch benötigen auch die Inhalte für jeden neuen Kanal stets Anpassungen oder neuere Versionen. Ineffizienz bei der Entwicklung und fehlende oder fehlerhafte Inhalte sind oft die Folge.	Die API-Integration erleichtert die Einbindung, Bearbeitung und Bereitstellung von Inhalten über mehrere Kanäle. Änderungen des Contents im Backend werden sofort für alle APIs und damit auch Geräte durchgeführt.

Für Anwender ist es zudem vorteilhafter, die Wartung den Expert zu überlassen, die täglich an dem Produkt arbeiten und es auch entwickeln.

Wie erfolgt der Umstieg?

Wie weiter oben bereits erwähnt, hat sich die MACH Alliance zum Ziel gesetzt, die gesamte Branche verstärkt darüber aufzuklären, worauf bei der Umstellung von Legacy- (monolithischen) Infrastrukturen auf Headless zu achten ist – einschließlich der Frage, wann, wo und mit welchen Kriterien man beginnen und Headless-Anbieter auswählen sollte. Die Alliance ist eine herstellerneutrale Institution, die Ressourcen, Bildung und Beratung durch Branchenexperten bereitstellt, um Unternehmen bei der Migration zu neuen Lösungen zu unterstützen.

Fazit: Unvermeidlich, dafür zukunftsweisend

Der Wandel findet statt, ob man möchte oder nicht. Das bedeutet zwar, dass jeder ihn annehmen muss, aber zum Glück nicht, dass dafür Opfer nötig sind. Ganz im Gegenteil: In einer Zeit mit fortschrittlicher Technologie zu leben, die einen leichten Einstieg in die sich ständig verändernde digitale Zukunft ermöglicht, ist ein klarer Vorteil. Die Verwendung von Headless Content-Management-Systemen hilft dabei, noch geltende Einschränkungen aufzuheben, die mit monolithischen CMS einhergehen.

Durch die Entkopplung von Front- und Backend sind sie zukunftssicher, agil und skalierbar. Die Umstellung komplexerer Websites auf eine SaaS-basierte Headless-Architektur führt unter anderem zu besserer Leistung, geringeren Kosten, mehr Zeit und einer hohen Sicherheit. Zu guter Letzt können sich die Entwickler in den Agenturen oder Inhouse von teuren, zeitaufwendigen und dadurch auch oft gefürchteten CMS-Updates verabschieden, die Kunden meist ohnehin nicht schätzen. Machen Sie also ebenfalls keine Updates mehr – nutzen Sie stattdessen Ihre Ressourcen effizienter.

Barry D'Arcy

it management

AUSGABE 9-10/2023
ERSCHEINT
AM 1. SEPTEMBER 2023

UNSERE THEMEN

DSAG-Spezial
Cloud Computing
Industrie 4.0

it security

AUSGABE 9-10/2023
ERSCHEINT
AM 1. SEPTEMBER 2023

UNSERE THEMEN

it-sa-Spezial
Digitale Identitäten
Threat Intelligence

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: Lars Becker, Barry D'Arcy, Lucia Falkenberg, Christian Freund, Dr. Thomas Gerick, Jürgen Hahnrath, Julien Herrmann, Frank Limberger, Carina Mitzschke, Silvia Parthier, Ulrich Parthier, Dirk Pohla, Petra Riepe, Frank Sent, Quintin Stephen, Kerstin Stier, Amadeus Thomas, Philipp von der Brüggen, Cosima von Kries, Uwe Weber, Ralph Weiss, Nizar Zalila

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

Head of Marketing:
Vicky Miridakis, 08104-6494-15, miridakis@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.


Steampunk
Summit 2024
SAVE THE DATE
28. und 29.
Februar 2024
Heidelberg
SAP-Technikvorstand Jürgen Müller (nicht im Bild) runderneuerte die alteingesessene SAP-Programmiersprache Abap und brachte diese auf die Business Technology Platform.
Das Projekt hat bei SAP den Codenamen „Steampunk“, der in der Community begeistert aufgenommen wurde. Embedded Abap ist Steampunk.
Eine Veranstaltung vom E3 Magazin:
e3mag.com


itsa EXPO CONGRESS
PLAY HARD.
PROTECT SMART.
HOME OF IT SECURITY
JETZT GRATIS-TICKET SICHERN!
10. – 12. Oktober 2023
Nürnberg, Germany
itsa365.de/itsa-expo-besuchen
NÜRNBERG MESSE

it security

Detect. Protect. Respond.
Juli/August 2023

VULNERABILITY MANAGEMENT & THREAT DETECTION

Schwachstellen erkennen und beheben

Ralf Kempf, Pathlock Deutschland

SELBSTBESTIMMTE IDENTITÄTEN

Open-Source auf dem Vormarsch

DARKNET-TECHNOLOGIEN

Wirklich eine Bedrohung?

CYBER THREAT INTELLIGENCE

Mit dem richtigen Kontext zu mehr IT-Sicherheit

KRITIS-Betreiber und NIS2

ab Seite 20

www.it-daily.net

Unternehmen leben länger mit

IT-Security Schutzmaßnahmen

SCAN ME

Mehr Infos dazu im Printmagazin

itsecurity

und online auf **www.it-daily.net**

Inhalt

COVERSTORY

THOUGHT LEADERSHIP

SECURITY AWARENESS

IT SECURITY

Vulnerability Management und Threat Detection

SAP SECURITY: „DAS IST WIE EIN AUTO OHNE BREMSEN!“

Nach wie vor werden bei der Absicherung von SAP-Systemen die Erkennung von Bedrohungen und die Analyse von Schwachstellen oft getrennt betrachtet. Dabei ermöglicht ihre Synergie eine deutliche Verbesserung der Systemsicherheit, erklärt Ralf Kempf, CTO von Pathlock Deutschland, im Interview.

it security: *Herr Kempf, eine Teilnehmer-Umfrage zur SAP-Security im Rahmen der IT-Online-Konferenz 2023 ergab, dass gerade mal ein Drittel der Befragten beide Methodiken implementiert hat. Wie ist das zu erklären?*

Ralf Kempf: Zunächst: Das deckt sich ganz gut damit, wie der Markt gerade dasteht. Wir stellen aber schon eine verstärkte Nachfrage der Kombination beider fest. Viele Kunden haben erkannt, dass man am besten beides zusammen macht, weil die Zuständigkeiten ähnlich sind. Wir sehen dennoch häufig, dass erst mal Vulnerability Management eingeführt wird und dann Threat Detection.

it security: *Laut Expert-Talk-Umfrage gibt es immerhin 8 Prozent, die es umgekehrt machen. Kann man also genauso mit Threat Detection beginnen oder damit allein arbeiten?*

Ralf Kempf: Nun, man erhält sehr schnell sehr viele Ergebnisse, doch sind diese meist nicht verwertbar. Man muss diese Informationsflut gezielt steuern und ausbremsen, sonst fährt man sozusagen alle Vorteile für die Systemsicherheit gegen die Wand. Anders gesagt: Die Schwachstellen-Analyse ist die Grundlage für eine effektive Threat Detection, da man sonst den Wald vor lauter Bäumen nicht sieht.

it security: *Und was vernachlässigen diejenigen, die nur Vulnerability Management betreiben?*

Ralf Kempf: Beim Vulnerability-Management geht es darum, die Systeme an einem Stichtag zu untersuchen und in einen Zustand zu bringen, dass man sie sicher betreibt, das heißt, Zugangsschutz, Verfügbarkeit, Wiederherstellbarkeit und Konsistenz der Daten gewährleistet. Die Statistiken zeigen aber, dass über 80 Prozent der erfolgreichen Angriffe mit fremden Identitäten passieren. Das bedeutet, ich habe als Eindringling die Zugangskarte oder Namen und Passwort von hochprivilegierten Benutzern gestohlen. Ein Vulnerability Management allein würde mich nicht bemerken, weil ich für dieses ein qualifizierter Benutzer bin. Hier kommt dann die Threat Detection ins Spiel, deren Aufgabe es ist, auftretende Anomalien zu entdecken. In dem Moment, wenn ich etwas Sonderbares tue, etwa ungesperrte Rechner suche, kann sie Alarm schlagen.

it security: *Wo liegen denn die Herausforderungen für eine kombinierte Umsetzung?*

Ralf Kempf: Knackpunkt ist zunächst die steigende Komplexität der Systeme, auch gerade unserer SAP-Kundschaft. Man hat das klassische SAP on premise, wie ERP, S/4HANA, CRM, und mittlerweile die klassische Microsoft-IT, die Operations IT, die Produktionssteuerung. Hinzu kommen heterogene Cloudanwendungen, viele haben Personaldaten, DATEV und Shopsysteme in der Cloud. Damit wird der gesamte IT-Fokus immer komplizierter und folglich auch die Übersicht, was in den Systemen passiert, wie diese überhaupt betrieben und gehärtet werden. Das ist stets die große Herausforderung, ein einheitliches Bild zu bekommen und Zuständigkeiten zu klären.

it security: *Wie gehen Unternehmen Ihrer Erfahrung nach damit um?*

Ralf Kempf: Es gibt eigentlich zwei Strategien: Dezentral bedeutet, jeder achtet auf seine eigene Systemlandschaft. Das ist meist keine gute Idee, weil jeder froh ist, wenn es bloß irgendwie läuft. Andererseits kann man zentral darauf schauen, sollte dann allerdings wissen: Was habe ich denn für eine IT? Hier haben wir schon interessante Entdeckungen gemacht, wichtige Systeme irgendwo im Mikrokosmos der Kunden-IT, die keiner kennt, die aber irgendwie laufen. Und Kunden, die nicht wissen, wie viele SAP-Systeme sie eigentlich haben.

it security: *Aber das gilt sicherlich nicht für jedes Unternehmen.*

Ralf Kempf: Natürlich nicht, aber klar ist: Oft fehlen Experten, die diese Komplexität überhaupt überblicken können und dann noch einen SAP-Fokus haben. Ein weiteres Defizit: Dank gestiegener Komplexität betrachtet man SAP-Systeme gerne mal als Blackbox nach dem

Motto: „Lassen wir die schwarze Kiste einfach mal unbeachtet, dann wird schon alles gut gehen." Und diese Bequemlichkeit ist völlig inadäquat, hier laufen die eigentlich wichtigsten Business-Prozesse der Kunden und diese müssen entsprechend abgesichert sein.

it security: *Trotzdem wird ja vergleichsweise selten über Attacken auf SAP-Systeme berichtet, oder?*

> THREAT DETECTION OHNE VULNERABILITY MANAGEMENT IST WIE EIN AUTO OHNE BREMSEN. ZWAR SCHNELL, ABER VOR ALLEM UNSICHER.
>
> **Ralf Kempf, CTO, Pathlock Deutschland, https://pathlock.com/de/**

Ralf Kempf: Auch hier führt eine gewisse Ignoranz zu dem Trugschluss, es sei vermutlich noch nie viel passiert, man sehe ja auch nichts in den Nachrichten. Denn was publik wird, sind bekannte Attacken auf Betriebssysteme wie Heartbleed, aber es steht letzten Endes nie dabei, was genau passiert ist. Betrachtet man jedoch die Menge abhandengekommener Daten, genügt es zu überlegen, wo diese in einem Unternehmen eigentlich gespeichert sind.

it security: *Wie gelingt dann die Verbindung von Vulnerability Management und Threat Detection?*

Ralf Kempf: Zuerst muss organisatorisch geklärt werden, dass beide Komponenten korrekt zusammenspielen. Im zweiten Schritt ist es nötig, die Schnittstelle zu haben, dass das Vulnerability Management in die Threat Detection hinein reportet und so Alarme generiert und zusammengefasst werden können. Für Investigations muss man sich das Ganze über einen längeren Zeitraum anschauen können. Und diese müssen von den Teams korrekt bewertet werden können. Dazu müssen die internen Prozesse richtig aufgesetzt und Entscheidungen getroffen werden. Das ist eigentlich der größte Aufwand für ein Unternehmen, die Mitigation von Schwachstellen oder auch von Threats. Die Technologie aufzusetzen ist meist gar nicht der komplexe Teil, Unternehmen tun sich eigentlich auf der Prozess-Ebene schwerer. Und daher muss das Ganze auf jeden Fall top-down passieren. Für Mitarbeiter ist es kaum möglich, das nach oben zu arbeiten. Es wird Zeit und Geld benötigt und im Unternehmen muss einfach das Bewusstsein vorhanden sein, dass sonst Kritisches passieren kann.

it security: *Wird die Cloud das Thema Security in dieser Form nicht sowieso überflüssig machen?*

Ralf Kempf: Natürlich bemühen sich die Hoster, dass Systeme sicher betrieben werden. Das sind namhafte Firmen, aber Fehler können alle machen. Allerdings ist ihr Effekt in der Cloud-Anwendung immer größer, weil die Daten mein Gebäude ja schon verlassen haben. Und gerade die Konfiguration und Überwachung ist ein sehr schwieriges Thema. Wenn ich einen Tenant hochfahre bei einem Kunden, stellt sich die Frage, wenn ich den jetzt lösche, wird das protokolliert? Die Antwort ist Nein, dann sind auch die Logs weg. Also wird die Komplettabschaltung nicht sauber protokolliert, das merkt man dann umgehend, wenn die Anwender anrufen. Das sind Aspekte der Cloud, da müssen wir alle noch lernen. Und ich sage mal, was wir Sicherheitsberater als Berufskrankheit haben, dieses ständige Paranoia-Denken, darüber schmunzeln ja manche und spotten, was wir uns da vorstellen, das passiert alles nicht. Ich antworte dann immer, stimmt, es kommt noch viel schlimmer, als wir uns das vorstellen.

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

Schwachstellen und Bedrohungen erkennen

SAP-SICHERHEIT: VULNERABILITY MANAGEMENT UND THREAT DETECTION

Wie genau funktionieren eigentlich Bedrohungserkennung und Schwachstellen-Analyse? Warum die Synergie beider Methoden eine reduzierte Reaktionszeit bei unerwünschten Ereignissen und gleichzeitig eine optimierte Gefahrenerkennung ermöglicht, erklärt Ralf Kempf, CTO von Pathlock Deutschland, am Beispiel eines IT-Hauses.

Wie sie jeweils funktionieren und wie die zielgerichtete Verbindung aus Threat Detection und Vulnerability Management zu einer deutlichen Verbesserung der SAP-Sicherheit führt, lässt sich gut am Beispiel eines klassischen IT-Bürogebäudes veranschaulichen. Denn Schwachstellen zuverlässig zu identifizieren und Bedrohungen in Echtzeit zu erkennen, ist oftmals der entscheidende Faktor für die Systemsicherheit, sei es ein Gebäude oder SAP.

Vulnerability Management

Beim Schwachstellen- oder Vulnerability Management geht es darum, Systeme anhand der Momentaufnahme an einem bestimmten Stichtag zu untersuchen und sie hinsichtlich Zugangsschutz, Verfügbarkeit, Konsistenz und Wiederherstellbarkeit der Daten in einen sicheren Betrieb zu bringen. Kommen wir zu unserem Beispiel eines Bürogebäudes: Es gibt zunächst die Perimeter-Sicherheit. Diese beginnt bei der Zufahrt zum Gelände – hier muss man vielleicht schon mal einen PIN-Code eingeben, um in die Tiefgarage zu kommen. Mit dem Zugang über die Tiefgarage erfolgt die Kanalisierung des Traffics der Mitarbeiter. Im Eingangsbereich ist eine Tür, für die man eine Keycard benötigt. Als Gast muss man sich beim Pförtner anmelden. Ansonsten sind alle Türen optimalerweise abgeschlossen, man möchte also ganz generell unautorisierten Zugang verhindern, und Ähnliches tut man bei IT-Systemen.

Zumindest die letzten zehn Jahre war eine IT meist in einem Gebäude konzentriert: Das Rechenzentrum war im Keller, ich konnte das kontrollieren, war Herr meiner Daten, hatte eine Firewall und konnte ziemlich genau überblicken, wer reinkommt. Ich hatte zudem gut überwachte Wartungszugänge oder einen Citrix-Terminal. Solch ein IT-Haus zu betreiben ist an sich schon hochkomplex, weil es viele Zuständigkeiten gibt: den Sicherheitsdienst, den Hausmeister, die Gebäudetechnik. Ganz ähnlich ist es bei der IT: Netzwerk Management, Access Control, SAP-Basis und IT-Basis. Und genau das ist Vulnerability-Management: Wir stellen eine Liste auf – und dankenswerterweise gibt es gerade von der SAP hervorragende Vorgaben, wie man deren Systeme sichert und überwacht.

Auf dieser Liste muss man Punkt für Punkt durchgehen und sie genau wie bei einer Gebäude-Leittechnik abhaken: Sind unnötige Türen stets abgeschlossen oder ist während der Mittagspause ein Hintereingang offen, der unbemerkten Zutritt erlaubt? Vulnerability Management versucht also immer, das Mindestmaß der Stabilität, Verfügbarkeit und Erreichbarkeit zu gewährleisten. Und das nicht nur einmal, sondern wie bei einem Gebäude: Der Hausmeister macht seinen täglichen Kontrollgang und jede Nacht prüft der Schließdienst alle Türen.

Threat Detection

Begeben wir uns nun in das Gebäude: Es sind Leute im Meetingraum, andere wie üblich an ihren Arbeitsplätzen, manche unterwegs oder im Dialog auf dem Flur, also der ganz normale Büroalltag. Jetzt ist es 12:30 Uhr und wir wissen eigentlich, was in einem Unternehmen zur Mittagspause passiert: Die Leute verlassen ihre Büros und gehen in Richtung Kantine. Das heißt, wir haben hier eine ganz normale standardisierte Bewegung der Mitarbeiter.

Was wir jetzt bei der Threat Detection machen, ist vor allem, auftretende Anomalien zu entdecken, also User Behavioral Analysis zu betreiben, indem wir beobachten: Bewegt sich jemand auffällig anders im Gebäude? Wenn wir jetzt einen Eindringling haben, der mit einer gefälschten ID hinein und am Empfang vorbeigekommen ist: Sein Ziel wird jetzt eben nicht die Kantine sein, sondern er bewegt sich in genau die entgegengesetzte Richtung und durchsucht Büros, ob irgendwo ein nicht gesperrter Rechner zu finden ist. Er verhält sich ganz anders als alle anderen Mitarbeiter, zu diesem Zeitpunkt und auch generell, weil er schnell nacheinander in Raum 3, 4 und 5 schaut.

Hier müssten dann sozusagen die Alarmglocken läuten, wenn ein Benutzer plötzlich anfängt, sich jenseits üblichen Verhaltens zu bewegen. Das Auffällige können zum Beispiel andere Downloads oder andere Mengen davon sein. Oder es sind ungewöhnliche Geolocations, von denen aus sich dieser Mitarbeiter anmeldet. Oder es werden bestimmte Transaktionen in den SAP-Systemen zu sonderbaren Zeiten ausgeführt. All das ist dann eine Anomaly Detection, die sonderbares Verhalten feststellt und den ersten Alarm der Threat Detection triggert.

Wenn wir nun auf unseren Eindringling zurückkommen, kann es natürlich sein, dass er einen nicht gesperrten Rechner findet oder über eine Schnittstelle in das System gelangt und anfängt, Konfigurationsänderungen zu machen oder sich bestimmte Belege anzuschauen, zum Beispiel HR- und Kontodaten. Das heißt, hier passiert etwas im System, indem er nur die Transaktion aufruft und mit den Augen oder einer Kamera die Informationen stiehlt. Er könnte aber auch anfangen, sicherheitsrelevante Parameter im SAP-System zu verändern, Businessbelege, Mengen einer Bestellung, Steuerinformationen oder gesamte Aufträge im SAP-System manipulieren. Es gehört dann zur Threat Detection, in beiden Fällen ein solches Verhalten innerhalb des SAP-Systems festzustellen, unabhängig davon, ob eine richtige ID benutzt wurde oder von wo er reingekommen ist. Dies darf keine Rolle spielen, denn der Perimeter hat ihn nicht entdeckt, am Vulnerability Management ist er damit vorbeigekommen.

Hier stellt sich die Frage, wie erkenne ich dann Anomalien wie abweichendes Benutzerverhalten und wie kann ich es über einen längeren Zeitraum monitoren? Denn die unterschiedlichen Schritte eines Hacks geschehen meist über einen längeren Zeitraum. Sie sind dann zusammenzutragen und miteinander zu korrelieren, um sagen zu können: Im Change Documents Log habe ich dieses Ungewöhnliche gesehen, im Security Audit Log und im User Change Log jenes. Alles zusammengefasst kann ich dann feststellen, dies ist eine faktische Hacking-Attacke.

Das Beste aus zwei Welten

Also ist das, was wir im Vulnerability Management machen, vom Prinzip her erst mal die Grundlage, um später eine effektive Threat Detection umsetzen zu können, da man sonst den Wald vor lauter Bäumen nicht sieht. Anders gesagt: Was nützt ein Tool, das akribisch dokumentiert, dass jemand durch eine Tür rein und raus geht, wenn ich weder weiß, wer das ist, noch ob er diesen Raum betreten darf. Entscheidender Punkt ist, dass Kunden sich dem Vulnerability Management und der Integration von Threat Detection intensiv widmen. Wenn eine Tür offen ist, jemand eine Keycard kopiert oder die Kamera aus ist, muss ich Hinweise bekommen, und zwar zeitnah. Kein Hexenwerk, aber die Teams müssen sich abstimmen und praxisorientierte Szenarien abbilden. Prozesse müssen festgelegt sein und ihre Schnittmenge technisch so befüllt werden, dass die Daten fließen. Und hier ist es entscheidend, einen Prozess zu haben, wie man damit umgeht, wenn man eine Schwachstelle beheben will oder eine Bedrohung erkennt. Und auch, dass die Rückkopplung funktioniert, denn am Anfang steht ja häufig zunächst eine Vermutung: Wer sich entgegen dem Mitarbeiterstrom zur Kantine durch mehrere Büros bewegt, ist vielleicht auch nur der Hausmeister, der gerade Fenster wartet.

https://pathlock.com/de/

> SCHWACHSTELLEN ZUVERLÄSSIG ZU IDENTIFIZIEREN UND BEDROHUNGEN IN ECHTZEIT ZU ERKENNEN, IST OFTMALS DER ENTSCHEIDENDE FAKTOR FÜR DIE SYSTEMSICHERHEIT.
>
> **Ralf Kempf, CTO, Pathlock Deutschland, https://pathlock.com/de/**

CYBERSECURITY? CSAAS!

Das Thema Cybersecurity ist, einfach gesagt, eine endlose Wiederholung von Angriff und Verteidigung. Die Frage ist nur, wer ist besser aufgestellt: die Angreifer oder die Verteidiger? Und da beide Seiten immer weiter aufrüsten, bleibt eine Antwort offen.

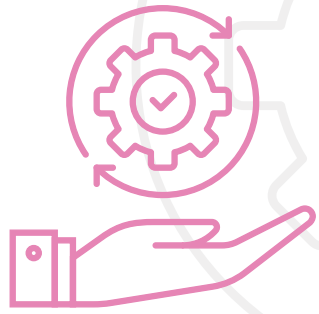
Die Welt der Cybersicherheit ist dynamisch und ständig im Wandel, Technologien entwickeln sich rasant weiter, Bedrohungen leider ebenfalls. Was also tun?

Cyber Security as a Service, eine Kombination aus technischer und menschlicher Expertise, ist aktuell die vielleicht effektivste Form sich gegen Angreifer zu schützen.

Cyber Security as a Service

HÖCHSTMÖGLICHE SECURITY FÜR MODERNE UNTERNEHMEN

Unternehmen und Organisationen sind heute anders organisiert als noch vor wenigen Jahren. Die Cloud oder intensives Homeoffice bieten eine neue Realität, die dabei hilft, dass Unternehmen und Mitarbeitende flexibler oder effizienter arbeiten können. Doch wo Licht ist, ist auch Schatten. Denn was in der Organisation im Arbeitsalltag hilft, weicht gleichzeitig traditionelle Sicherheitsstrategien und -konzepte auf. Das Resultat sind offene Flanken, welche die Cyberkriminellen kennen und für ihre Angriffe ausnutzen. Die beste Möglichkeit dieser Herausforderung zu begegnen, ist die Kombination aus technischer und menschlicher Expertise mit Cyber Security as a Service (CSaaS).

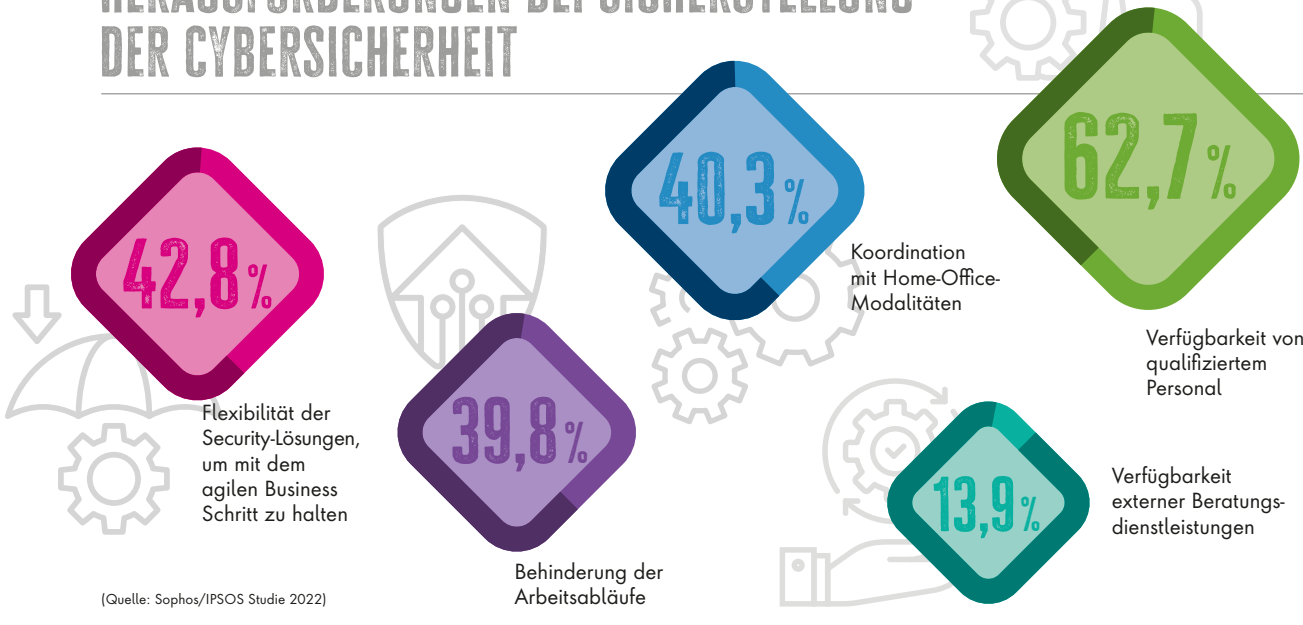


Es war einmal

Wohin die Reise der Cybersicherheit auch geht, sie ist jedenfalls durch das hohe kriminelle Potenzial der Cyberkriminellen definiert. Den Ernst der Bedrohungslage belegen die Zahlen der neuesten globalen Studie von Sophos „State of Ransomware 2023". Insgesamt wurden in Deutschland 58 Prozent der befragten Unternehmen von Ransomware angegriffen. Dies deutet darauf hin, dass die Zahl der Ransomware-Attacken trotz des vermeintlichen Rückgangs während der Pandemiejahre doch konstant hoch geblieben ist. Bei der Analyse der Ursache von Ransomware-Attacken waren die häufigsten Ausgangspunkte eine ausgenutzte Schwachstelle mit 24 Prozent sowie kompromittierte Zugangsdaten mit 36 Prozent.

Klar ist, die Gefahren für Unternehmen sind zum Teil hausgemacht und wie eine Einladung für Cybergangster. Unternehmen stehen unter dem kontinuierlichen Druck, Prozesse und Budgets zu optimieren und begeben sich dabei immer öfter in ein Ungleichgewicht zwischen Innovation, digitaler Transformation und Cybersicherheit. Immer weniger existiert das eine Netzwerk, in dem eingebundenen Systeme sicher sind, sondern stattdessen ein weit verzweigtes Ökosystem, das nicht mehr effizient

HERAUSFORDERUNGEN BEI SICHERSTELLUNG DER CYBERSICHERHEIT

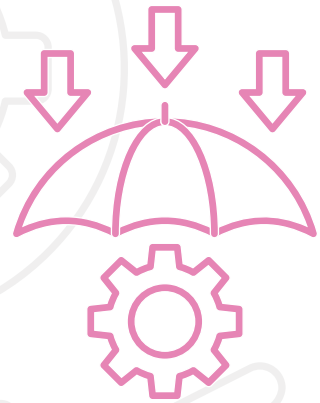


(Quelle: Sophos/IPSOS Studie 2022)

abgesichert werden kann. Das Problem liegt darin, dass klassische Sicherheitskonzepte davon ausgehen, dass mit einem ausgefeilten System von Endpoint-, Firewall-, Cloud-, Identitäts-, E-Mail- und weiteren Sicherheitselementen wie der Künstlichen Intelligenz, den Angreifern der Wind aus den Segeln genommen ist. Die bittere Realität allerdings ist, dass die Cyberkriminellen die hoch entwickelten Cyberschutzlösungen kennen und dass sie diese mit ähnlich innovativer Technologie immer wieder umgehen.

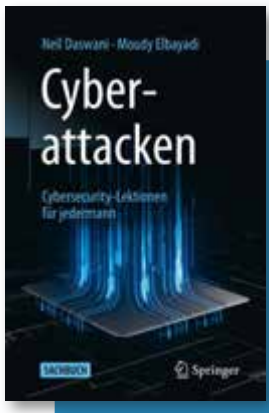
Schlüsselrolle:
Menschliche Expertise

Die Rolle menschlicher Expertise, beim Aufspüren, Identifizieren und Beseitigen von Cyberbedrohungen als Ergänzung zu Softwarelösungen gewinnt vor dem Hintergrund hoch professionalisierter Cyberkrimineller und einer gestiegenen Bedrohungslage noch mehr an Bedeutung. Ein Sicherheitsteam, das diese Disziplin vollständig beherrscht, setzt jedoch angemessenes Budget und verfügbare Fachkräfte voraus. Beides ist oft Mangelware. In einer aktuellen Management-Studie von Sophos nannten 62,7 Prozent der in Deutschland befragten Geschäftsleitungen die Verfügbarkeit von qualifiziertem Personal als die größte Herausforderung bei der Umsetzung und Sicherstellung von IT-Sicherheit. Die Lösung liegt in externen Services, beispielsweise als Cyber Security as a Service (CSaaS). Mit CSaaS haben Unternehmen die Möglichkeit, komplexe Cyberbedrohungen zu erkennen und rechtzeitig darauf zu reagieren.



CSaaS umfasst proaktive Abwehrmaßnahmen durch Spezialisten, um kritische Cybersicherheitsanforderungen zu erfüllen, wie etwa die Bedrohungsüberwachung rund um die Uhr. Damit steht fest: Die beste Lösung im Kampf gegen Cyberkriminalität sind Mensch und Maschine im Team.

Michael Veit | www.sophos.de



Cyberattacken
– Lektionen für jedermann;
Neil Daswani, Moody Elbayadi, Springer; 07-2023

CYBERATTACKEN

CYBERSECURITY-LEKTIONEN FÜR JEDERMANN

In die Cybersicherheitsbranche wurden in den letzten 15 Jahren über 45 Milliarden Dollar investiert. Hunderttausende von Arbeitsplätzen in diesem Bereich bleiben unbesetzt, und das Problem hat sich zugespitzt. Es ist an der Zeit, dass jeder – nicht nur Techniker – sich über das Thema Cybersicherheit informiert und befähigt.

In fesselnder und spannender Weise behandelt Big Breaches einige der größten Sicherheitsverletzungen und die dahinter stehenden technischen Themen wie Phishing, Malware, Kompromittierung durch Dritte, Software-Schwachstellen, unverschlüsselte Daten und vieles mehr. Cybersicherheit betrifft das tägliche Leben von uns allen, und noch nie war dieser Bereich so zugänglich wie mit diesem Buch.

Sie erhalten ein sicheres Gespür für das Insiderwissen der Branche, wie effektive Präventions- und Erkennungsmaßnahmen, die Ursachen von Sicherheitsverletzungen auf der Metaebene, die sieben entscheidenden Gewohnheiten für optimale Sicherheit in Ihrem Unternehmen und vieles mehr. Diese wertvollen Lektionen werden auf reale Fälle angewandt und helfen Ihnen dabei, herauszufinden, wie es zu den hochkarätigen Mega-Einbrüchen bei Target, JPMorgan Chase, Equifax, Marriott und anderen Unternehmen kommen konnte.

Für den Ernstfall gewappnet

SECHS SCHRITTE ZUM KRISENFESTEN UNTERNEHMEN

Krisensituationen treten immer häufiger auf und bestimmen zunehmend die Lebensrealität. Unternehmen benötigen deshalb organisatorische Resilienz, also die Fähigkeit, krisenhafte Ereignisse zu antizipieren, ihre Auswirkungen auf den Geschäftsbetrieb zu minimieren und die Sicherheit ihrer Mitarbeiter zu gewährleisten.

#1 In das Wohlbefinden der Mitarbeiter investieren.
Investitionen, die das Wohlbefinden der Belegschaft und ihre psychische Gesundheit fördern, haben oberste Priorität. Zufriedene und gesunde Mitarbeiter können besser mit Krisen umgehen und engagieren sich stärker für deren Bewältigung.

#2 Eine belastbare Unternehmenskultur entwickeln.
Unternehmen sollten die Erfolge ihrer Angestellten anerkennen, sie ermutigen, aus Fehlern zu lernen, und ihre Kooperation fördern. Dann entwickeln die Mitarbeiter ein starkes Gemeinschaftsgefühl, halten in Krisen zusammen und ziehen an einem Strang.

#3 Einen integren Führungsstil pflegen.
Die Führungskräfte müssen mit gutem Beispiel vorangehen. Wenn sie klare Vorgaben machen, realistische Erwartungen stellen und jederzeit ansprechbar sind, schaffen sie unter den Mitarbeitern ein Gefühl des Vertrauens und der Stabilität, das sich in Krisensituationen auszahlen wird.

#4 Agiles Denken und Arbeiten fördern.
Probleme schnell lösen, bei Bedarf kurzfristig neue Wege einschlagen und sich an neue Herausforderungen anpassen: Das zeichnet eine widerstandsfähige Organisation aus.

#5 Proaktives Risikomanagement betreiben.
Widerstandsfähige Unternehmen bewerten laufend potenzielle Risiken, arbeiten Notfallpläne aus und testen sie regelmäßig. Das ermöglicht ihnen dann im Fall der Fälle, die Unterbrechungen im Geschäftsbetrieb auf ein Minimum reduzieren und sich schnell von Rückschlägen zu erholen.

#6 Integrierte und intuitive Technologie einsetzen.
Unternehmen benötigen Tools für Business Continuity, Disaster Recovery und Risikomanagement, die nahtlos zusammenarbeiten und so intuitiv sind, dass sie im Krisenfall von jeder Person genutzt werden können.

www.everbridge.com/de

Awareness

DAS FUNDAMENT FÜR DIE MENSCHLICHE FIREWALL

Die Digitalisierung schreitet rasant voran. Sie bietet Unternehmen und den Menschen, die für sie arbeiten, völlig neue Möglichkeiten und Freiheiten. Der digitale Wandel birgt aber auch Risiken, die durch konsequente Maßnahmen im Bereich der Informationssicherheit entschärft werden können.

Neben Technik und Organisation stellt Informationssicherheit in unserem vernetzten, dezentralen ArbeitsÜBERALLtag vor allem für den Menschen eine neue Dimension von Herausforderungen dar. Informationssicherheit umfasst nicht nur Digitales, sondern alle schutzbedürftigen oder geheimhaltungspflichtigen Informations-Werte eines Unternehmens: von Kundendaten über Geschäftsgeheimnisse (Patente, Prototypen) bis hin zu Jahresergebnissen und Kennzahlen.

Ob diese Informationen in den Köpfen der Mitarbeitenden, auf Datenträgern oder auf Papier vorhanden sind: Zur Informationssicherheit zählen alle Konzepte, Systeme und Richtlinien, die deren Schutz sicherstellen. Die Maßnahmen müssen die technische, organisatorische und menschliche Komponente berücksichtigen. Folgerichtig spricht man vom „Dreiklang der Informationssicherheit".

MEHR WERT

Whitepaper „Update für die menschliche Firewall"
bit.ly/3WR98Jb

Neben der IT-Sicherheit hat ein Unternehmen also auch darauf zu achten, dass seine Prozesse sicher sind, also etwa Zugänge zu Informationen beschränkt sind. Die Mitarbeitenden selbst müssen wiederum durch ihr Verhalten im Geschäftsalltag sicherstellen, dass das Unternehmen die drei wesentlichen Schutzziele der Informationssicherheit erreicht:

1. Vertraulichkeit
2. Integrität
3. Verfügbarkeit

Die menschliche Firewall steht an erster Stelle

Technische Schutzmechanismen wie Firewalls, Multifaktor-Authentifizierung oder automatisierte Schwachstellen-Scans sind heute in der Regel hoch entwickelt. Kriminelle Organisationen oder Einzeltäter haben mittlerweile erkannt, dass die IT nicht mehr das primäre Einfallstor ins Unternehmen ist. Vielmehr sind die Mitarbeitenden oft das erste Angriffsziel.

Zwei Faktoren spielen Kriminellen in die Karten: In vielen Unternehmen mussten Mitarbeitende in kurzer Zeit den Umgang mit neuen Technologien, Arbeitsweisen und Prozessen lernen. Manche sind überfordert und unachtsam. Auch ist vielen Mitarbeitenden nicht bewusst, dass Informationssicherheit auch sie betrifft – und dass Sie nicht nur beim Öffnen von E-Mails aufpassen müssen.

„Man muss tägliche Prozesse genau überdenken, um Cyberangriffen keine Chance zu geben", betont Florian Goldenstein, IT-Security Consultant und CISO bei Konica Minolta Business Solutions. „Deshalb ist es so wichtig, die Menschen im Unternehmen für das Thema zu sensibilisieren. Vor diesem Hintergrund haben Cyber-Schulungen eine elementare Bedeutung, da alle im Unternehmen die Grundlagen der Informationssicherheit kennen und leben müssen."

Social Engineering und seine Methoden

Kriminelle nutzen menschliche Schwachstellen aus, um gezielt das Vertrauen bestimmter Personen oder Personengruppen zu erlangen und dieses dann für den Diebstahl oder die Manipulation von Informationen zu missbrauchen. Oft machen sie sich menschliche Züge wie Hilfsbereitschaft, Angst oder Pflichtbewusstsein zunutze. Diese kriminelle Technik nennt sich Social Engineering.

Aktuelle Studie:

WIRTSCHAFTSSCHUTZ 2022

Die Studie ergab: In jedem zweiten Unternehmen wurden im vergangenen Jahr Manipulationsversuche durch Social Engineering verzeichnet. Häufig (34%) ist eine E-Mail der erste Angriffspunkt. Noch häufiger (38%) das gute alte Telefon. Auch in beruflichen (9%) und privaten (5%) sozialen Netzwerken lauern Gefahren. Sogar im privaten Umfeld (13%) versuchen Kriminelle, an Informationen zu gelangen.

Folgende Methoden kommen besonders häufig vor:

#1 Spear-Phishing:
Eine E-Mail wird von Kriminellen an eine bestimmte Person gesendet, um sie zum Klicken eines Links, zur Eingabe von Passwörtern oder zur Preisgabe von Information auf einer fingierten Oberfläche zu bewegen. Durch Fälschung der Absenderadresse und Nutzung öffentlich zugänglicher Informationen über das Unternehmen kann eine gefälschte E-Mail täuschend echt wirken.

#2 Telefon-Spoofing:
Kriminelle rufen eine bestimmte Person an und fälschen die übermittelte Rufnummer. Die angerufene Person hat den Eindruck, dass der Anruf aus dem eigenen Unternehmen oder einem Partnerunternehmen getätigt wird. Gerade wenn sich Mitarbeitende verschiedener Abteilungen oder Standorte nicht persönlich kennen, fällt die Täuschung kaum auf.

#3 CEO-Fraud:
In einer fingierten E-Mail oder mit einem gefälschten Anruf geben sich Kriminelle als Geschäftsführende oder Management aus – also als Personen, die mehrere Hierarchiestufen über dem Opfer der Täuschung stehen. Sie geben Anweisungen, die kriminelle Handlungen begünstigen, und weisen auf Dringlichkeit und Vertraulichkeit hin: zum Beispiel eine Express-Überweisung auf ein Nummernkonto.

Lücken in der Informationssicherheit schließen

Neben klassischen Offline- und Online-Schulungen zur Informationssicherheit bietet ein Sensibilisierungs-Training mittels realistischer Simulationen maximale Lerneffekte für die Mitarbeitenden. Hierfür entwickelt ein externer Dienstleister wie Konica Minolta Business Solutions mit seinen IT-Sicherheitsexperten gezielte Awareness-Kampagnen, die auf die Mitarbeitenden abgestimmt sind.

Eine täuschend echt anmutende Phishing-Mail, ein auf dem Parkplatz liegengelassener USB-Stick, eine fremde Person in der Video-Konferenz – die „Köder" sind vielfältig. Die Mitarbeitenden fühlen sich bestätigt, wenn sie die simulierte Bedrohung erkennen oder erleichtert, wenn das „Hereinfallen" auf den CEO-Fraud ohne Konsequenzen bleibt. So oder so prägen sich die Methoden ein und schaffen ein Bewusstsein dafür, vorsichtig mit Informationen umzugehen.

Training auf mehreren Ebenen

Auch auf höheren Ebenen und in Entscheidungspositionen ist Wissen zur Informationssicherheit manchmal dünn gesät. Regelmäßige Schulungen und Trainings gewährleisten, dass die verantwortlichen Positionen im Unternehmen über Bedrohungen und Abwehrtechniken genau im Bilde sind. Effizient sind Workshops für Admins und IT-Sicherheitsbeauftragte, bei denen sie in die Rolle von Cyber-Kriminellen schlüpfen und versuchen, eigene Angriffswege zu finden. Mit dem erlangten Wissen können sie aktiv die Sicherheitslücken des Unternehmens schließen und als Multiplikatoren Bewusstsein für Informationssicherheit schaffen.

„Die menschliche Firewall ist die wichtigste im Unternehmen", weiß Konica-Minolta-Experte Goldenstein. „Daher bieten wir Awareness als Service an, um die Mitarbeitenden regelmäßig zu trainieren. Das darf aber nicht die einzige Maßnahme zur Gefahrenabwehr sein. Wir unterstützen unsere Kunden mit Managed Services, die viele Bereiche und auch Security abdecken, beispielsweise Monitoring, Patch-Management oder Backups. Zudem bieten wir Managed Firewalls und Endpoint Protection an, denn die Sicherheit der Endgeräte – an jedem Ort – ist ein zentrales Thema." So wird der Grundstein für sichere hybride Arbeitsmodelle und eine sichere Unternehmens-IT gelegt.

www.konicaminolta.de/sensibilisierung

CYBERSECURITY

INNOVATIVE LÖSUNGEN, KI & MORE

Kaum ist ein Problem gelöst, taucht (mindestens) ein neues auf. Künstliche Intelligenz (KI) drängt in alle Anwendungsbereiche des täglichen Lebens vor und stellt uns vor neue Herausforderungen.

KI und IT-Sicherheit sind eng miteinander verbunden, da KI-Systeme selbst potenzielle Angriffsziele sind, aber auch zur Absicherung von IT-Systemen eingesetzt werden können. Im nachfolgenden eBook finden Sie wichtige Aspekte, die man der Verwendung von KI in der IT-Sicherheit beachten sollte.

Cybersecurity: Innovative Lösungen, KI & more – Inhalt

Das **eBook** umfasst 82 Seiten und steht zum kostenlosen Download bereit.
www.it-daily.net/download

Messbarer Erfolg

REGELMÄSSIGKEIT UND AKTUALITÄT ALS GRUNDVORAUSSETZUNG

Security Awareness Trainings sind beim MSSP Network Box seit vielen Jahren fester Bestandteil ganzheitlicher IT-Sicherheitskonzepte. Wir sprechen mit Geschäftsführer Dariush Ansari über den konkreten Nutzen von Security Awareness, wie die Erfolge messbar werden und wie Systemhäuser ihren Kunden Security Awareness anbieten können, auch wenn sie nicht über das Know-How oder Personal verfügen.

it security: *Dariush, wie überzeugt ihr Unternehmen von der Wichtigkeit von Security Awareness?*

Dariush Ansari: Die meisten Unternehmen haben verstanden, dass Mitarbeitende angreifbar sind und die wichtigste Rolle für ganzheitlichen IT- Schutz spielen; und dass Security Awareness längst keine freiwillige Option, sondern ein Muss geworden ist. Cybervorfälle gelten als Geschäftsrisiko Nummer 1, dabei starten 90 Prozent aller Attacken beim Faktor Mensch. Viele der Unternehmen sind entweder selbst bereits Opfer gewesen und wissen daher, wovon wir sprechen, oder kennen andere Unternehmen, die einen Cyberangriff erlebt haben. Nicht ohne Grund gilt die Nachweispflicht im Rahmen der DSGVO, ISO-Standards, Cyber-Versicherer und ISMS. Vor jedem Security Awareness Training führen wir ein Onboarding-Gespräch, bei dem wir uns einen Überblick über die Unternehmenskultur, Arbeitsabläufe und Altersstrukturen verschaffen. Hier klären wir mögliche Bedenken und Fragen und entwickeln einen Awareness-Lehrplan, mit dem die Mitarbeitenden Teil des Sicherheitskonzepts werden.

it security: *Wie nutzen Cyberkriminelle die Schwachstelle Mensch denn aktuell aus?*

Dariush Ansari: Die häufigste Form der Cyberkriminalität ist und bleibt das Phishing in allen Varianten: per SMS, QR-Code oder E-Mail, als Massenmails nach dem Zufallsprinzip oder gezielte Angriffe. Cyberkriminelle nutzen dafür gerne aktuelle, emotionale Themen, die Menschen in ihrer Gutmütigkeit dazu verleiten, auf einen Angriff entsprechend „falsch" zu reagieren.

it security: *Kann man den Erfolg einer Security Awareness Schulung messen?*

Dariush Ansari: Ja, der Erfolg ist messbar. Grundvoraussetzung ist die Regelmäßigkeit und Aktualität der Trainings. Wir bieten nach unseren Phishing-Simulationen anonymisierte Auswertungen zu dem Anteil der angeklickten Links und schadhaften Anhängen, die geöffnet wurden, aber auch zu der Teilnahmequote der eLearnings. So lässt sich die Wirkung der Trainings genau belegen und ebenso zeigt sich, zu welchen Themen noch Schulungsbedarf besteht. Weiterhin geben wir den Mitarbeitenden ein Outlook-Plugin an die Hand, mit dem sie Spam und Phishing-Emails markieren können. Steigen die Markierungen, ist das ein Beleg dafür, dass die Menschen aktiver und aufmerksamer hinterfragen.

it security: *Was können Systemhäuser tun, wenn sie nicht über das Know-how oder Personal im Bereich Security Awareness verfügen?*

GRUNDVORAUSSETZUNG FÜR MESSBARE TRAININGS IST DIE REGELMÄSSIGKEIT UND AKTUALITÄT DER TRAININGS.

Dariush Ansari, Geschäftsführer, Network Box Deutschland GmbH, www.network-box.eu

Dariush Ansari: Sie suchen sich einen Managed Security Service Provider – so wie uns. Wir übernehmen den Bereich Security Awareness für mittlerweile über 500 Systemhauspartner deutschlandweit. Dazu gehört die Planung, Kontrolle und Durchführung von Phishing-Simulationen, einer eLearning-Plattform mit immer neuen Schulungsmodulen, auf Wunsch im CI des Systemhauses, Materialien am Arbeitsplatz, Newsletter und Reportings. Dabei entscheidet das Systemhaus, ob sie die Kundenkorrespondenz selbst abdecken möchten und wir im Hintergrund agieren, oder ob wir auch diesen Part übernehmen sollen.

it security: *Dariush, wir danken für das Gespräch.*

THANK YOU

Die letzte Verteidigungslinie?

DAS ABC DER SECURITY AWARENESS

Security Awareness stand lange Zeit im Schatten anderer eher technischer Themen, dabei sind Phishing-E-Mails seit Jahren eine der wichtigsten Hacking-Methoden und zielen auf Menschen ab, nicht auf die Technik um ihn herum. In den letzten Jahren hat sich dieses Nischen-Dasein jedoch grundlegend verändert. Genauso wie IT-Sicherheit sich aus der Nische der IT in das Rampenlicht gearbeitet hat, hat sich auch die Security Awareness aus der Nische der Profession ins vorderste Glied der IT-Sicherheitsstrategie entwickelt.

Oft sah die Schulung jedoch eine rasche Umsetzung des gelernten vor, das funktionierte jedoch häufig nicht, weil die Geschulten nicht verstanden hatten, worauf sie achten sollten oder aber kein Feedback mehr erhielten. Vergleichen lässt sich dies mit dem Führerschein, wer Autofahren will, muss auch eine theoretische und praktische Prüfung bestehen, die so vergleichbar ist, dass die Anzahl der Unfälle und Probleme im Straßenverkehr reduziert wurde.

Pflicht oder Kür?

Unternehmen verstanden Security Awareness zumeist als Teil der Compliance und als Anforderung, die sich mit dem Arbeitsschutz vergleichen ließen: Eine lästige Pflicht, die es nachzuweisen galt, die jedoch keine besondere Anstrengung bedarf. Die Anzahl der Cyberattacken und die Vielzahl der betroffenen Organisationen veränderten diese Haltung jedoch. Die Gefahr eines Ausfalls wichtiger IT-Services und die Androhung von Strafen durch den Verlust von Daten via DSGVO haben das Thema IT-Sicherheit auf die Geschäftsführungsebene gehoben. Security Awareness als ausdrücklich nicht technisch beladenes Thema, eignet sich besonders gut allen Mitarbeitern eines Unternehmens die Besonderheiten eines Cyberangriffs zu vermitteln, so auch der Geschäftsleitung. Budgets wurden erhöht, Trainer intern oder extern gesucht und engagiert. Erste Schulungen wurden Abteilungsübergreifend eingeführt und regelmäßig mit Anreizen durchgeführt. Die Inhalte wurden immer professioneller. Dennoch verfehlte es das Ziel, denn zielgenaue Inhalte und erste Phishing-Tests wurden in der Regel von IT-Fachleuten zusammengestellt, was vielfach für Überforderung sorgte.

> SECURITY AWARENESS WIRD MEHR UND MEHR ALS EIN DREIKLANG BETRACHTET, BESTEHEND AUS »AWARENESS«, »BEHAVIOR« UND »CULTURE«.
>
> **Jelle Wieringa,**
> **Security Awareness Advocate, KnowBe4,**
> **www.knowbe4.com**

In den letzten fünf Jahren, haben sich die Trainings, vor allem in Bezug auf die theoretischen und praktischen Grundlagen deutlich modernisiert und wurden effektiver. Darüber hinaus wurde verstanden, dass die Inhalte nicht technischer Natur sein müssen, um auch wirklich alle Mitarbeiter zu erreichen. Die Intensität und die Schulung per Frontalunterricht haben sich zu interaktiveren Seminaren in kleineren Gruppen entwickelt, ähnlich von Fortbildungsmaßnahmen. Gründe dafür sind die bessere wissenschaftliche Erfassung von menschlichem Verhalten und deren Messbarkeit sowie die bessere Erkennung von Phishing-Trends durch automatisierte Analysen. Verändert hat sich auch die Herangehensweise an die Security Awareness. Security Awareness wird mehr und mehr als ein Dreiklang betrachtet, bestehend aus „Awareness", „Behavior" und „Culture".

Was ist Awareness?

Awareness sollte dazu dienen, dass Mitarbeitende intelligentere Security-Entscheidungen treffen. Der Begriff Awareness meint, dass ein Mitarbeitender verstanden hat, dass ein vermitteltes Thema wichtig für seine Firma, aber auch ihn selbst ist. Die Geschulten sind in der Lage eine Phishing-E-Mail zu erkennen, anhand ihres erlernten Wissens durch Schulungen und anhand von Er-

SECURITY AWARENESS TRAININGS UND IHRE SCHWÄCHEN

- passive Lernmethoden
- inflexible Lerninhalte
- überkomprimierte Lehrzeit

fahrungen durch simuliertes Phishing. Am besten kann Awareness erreicht werden, wenn die Schulungen in der Muttersprache stattfinden und die Mitarbeitenden mal auditiv, mal visuell, mal ernsthafter, mal spielerisch über verschiedenste Inhaltsformen hinweg mit einem Thema konfrontiert werden. Comics, Poster, ein Quiz oder aber ein Erklärvideo helfen bei der Wissensvermittlung. Wichtig sind die Qualität und nicht die Quantität der Trainings, unwichtig ist der Ort des Trainings. Es gibt Mitarbeitende, die werden über ein Präsenztraining erreicht, es gibt jedoch auch Mitarbeitende, die sich im Home Office am besten weiterbilden und bei Rückfragen lieber mit den Verantwortlichen chatten oder telefonieren wollen. Am Ende entscheidet das Ergebnis, dass sich über simulierte Phishing-Tests in Kombination mit der Auswertung der absolvierten Schulungen am besten messen lässt.

Was ist Behavior also Verhalten?

Verhalten meint im Kontext von Security Awareness, dass Mitarbeitende die Awareness haben, ihr Verhalten den Anforderungen der Security Awareness entsprechend anzupassen. BJ Fogg, Verhaltenswissenschaftler an der Stanford University, schreibt in seinem „Fogg Behavior Model": „Verhalten entsteht, wenn Motivation, Fähigkeit und eine Aufforderung im selben Moment zusammenkommen." Die Betrachtung des Verhaltens war der nächste logische Schritt bei der Weiterentwicklung der Security Awareness. Allein betrachtet bringt es jedoch nichts das Verhalten individuell zu messen und zu verändern. Es geht darum, dass die Geschulten das Erlernte in intelligente Entscheidungen umzusetzen. Mitarbeitende mit intrinsischer Motivation zu erfüllen, dass sie einen Mehrwert sehen, sich in diesem Bereich fortzubilden und ihr Verhalten zu verändern, ist eine der zentralen Aufgaben der Trainer. Messen lässt sich Security Awareness mit simuliertem Phishing, Umfrage, einem Quiz oder anderem Content.

Was ist Culture?

Die Security-Culture umfasst laut Definition die Ideen, Eigenheiten und sozialen Verhaltensweisen einer Gruppe, die ihre Sicherheit beeinflussen. Culture ändert das und löst diese Problematik der fehlenden Vergleichbarkeit des Verhaltens auf. Eine Möglichkeit die Security Culture zu messen und mit anderen Unternehmen zu vergleichen besteht in der jährlichen Umfrage zum Security Culture Report. Im letzten Jahr wurde mit dem „Security Culture Maturity"-Modell ein erstes Reifegradmodell der Branche, das speziell auf die Messung der Sicherheitskultur (Security Culture) ausgerichtet ist, veröffentlicht.

Fazit

Die Grundidee hinter den ABCs der Security Awareness ist, dass die Awareness nachhaltiger wird, wenn sich das Verhalten ändert und die Kultur sorgt für eine Unternehmensweite Änderung der Einstellung gegenüber der Security Awareness. Alle im Verbund lassen sich messen und mit anderen Unternehmen vergleichen.

Jelle Wieringa

SO SOLLTE DAS TRAINING WIRKLICH STATTFINDEN

- Mitarbeiter aktiv in die Lernprozessse einbinden
- individuell zugeschnitten
- portioniert in Themenblöcke, die über einen längeren Zeitraum vermittelt werden

(Quelle: Der Mitarbeiter als „letzte Verteidigungslinie"; KnowBe4)

Sicherheitslücke Mensch?

CYBER SECURITY AWARENESS IM ZEITALTER VON CHATGPT

Cybergefahren stellen weltweit das größte Risiko für Unternehmen dar. Zu diesem Schluss kommt das Allianz Risk Barometer 2023. Die erfolgreichsten Angriffstaktiken sind nach dem Human Risk Review 2023 von SoSafe aktuell Malware, Phishing und Ransomware, während die häufigsten Angriffsziele IT-, Finance- und Security-Abteilungen sind. In den vergangenen drei Jahren ist jede zweite Organisation Opfer eines erfolgreichen Cyberangriffs geworden, jede dritte sogar mehr als einmal – und eine Entspannung wird nicht erwartet: 82 Prozent der Organisationen gehen davon aus, dass die Lage auch 2023 weiter angespannt bleibt.

Neue Gefahren durch generative KI

Neben der prekären geopolitischen Lage stellen auch die jüngsten Entwicklungen bei künstlicher Intelligenz neue Herausforderungen für die Cybersicherheit dar. Generative-AI-Tools wie ChatGPT sind noch nicht lange öffentlich zugänglich und haben dennoch bereits jetzt die Möglichkeiten von Cyberkriminellen erweitert. Der Trend, innovative Technologien für Cyberangriffe zu missbrauchen, ist nicht zuletzt seit den ersten Deepfakes 2017 zu beobachten. Nun hat er durch generative KI und die damit verbundenen Skalierungsmöglichkeiten für Phishing-Attacken neue Fahrt aufgenommen. Zwar steht die Technologie noch am Anfang, doch Untersuchungen von SoSafe zufolge sind KI-generierte Phishing Mails schon heute so gut, dass sich jede fünfte Person durch sie täuschen lässt und diese anklickt.

Im Moment sind von Menschen erstellte Phishing-Mails noch erfolgreicher – hier klickt jede dritte Person – allerdings werden Large-Language-Modelle wie ChatGPT sich kontinuierlich verbessern und damit das Gefahrenpotenzial durch generative KI in Zukunft weiter steigern. Insgesamt gilt für generative KI, dass sie den Aufwand für personalisierte Phishing-Angriffe senkt und sich damit häufiger und intensiver einsetzen lassen.

EIN GEFESTIGTES SICHERHEITSBEWUSSTSEIN KANN EIN BOLLWERK GEGEN CYBERANGRIFFE SEIN.

Dr. Niklas Hellemann,
CEO und Mitbegründer, SoSafe,
https://sosafe-awareness.com/de/

Social Engineering Taktiken

Phishing und andere Arten von Social Engineering stellen ein häufiges Einfallstor für weitere Angriffstaktiken wie Malware und Ransomware dar. Daher ist es nicht überraschend, dass 61 Prozent der befragten Sicherheitsverantwortlichen angeben, dass ihre Organisation über E-Mails angegriffen wurde. Schadhafte E-Mails sind nicht nur ein gängiges Angriffsmittel, sondern treten in intensiveren Wellen und kürzeren Intervallen auf.

Beim Social Engineering entscheiden zwei Faktoren darüber, ob das Angriffsopfer auf die schädlichen Inhalte klickt: Wie glaubwürdig die E-Mail wirkt und wie stark sie die Opfer emotional anspricht. Sowohl positive als auch negative Gefühle können die gewollte Reaktion hervorrufen. Noch führen Taktiken wie Lob und Hilfsbereitschaft, also solche, die auf positive Gefühle abzielen, zu höheren Klickraten. Allerdings ist ein

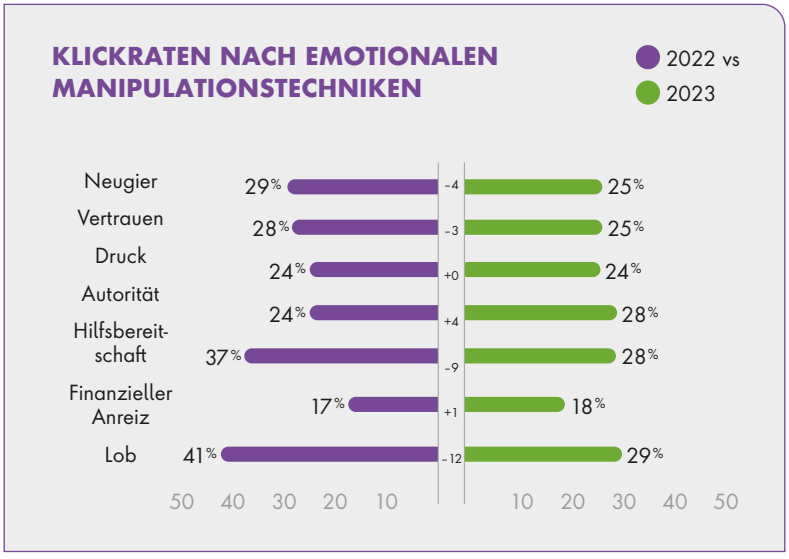
Anstieg der Klickraten bei Taktiken wie dem Einsatz von Autorität oder Druck zu beobachten, was auf eine höhere Anfälligkeit für diese Art der Manipulation hindeutet. Das liegt möglicherweise an der gestiegenen Verunsicherung durch die weltweiten Krisen und Konflikte der letzten Jahre. In den erfolgreichsten Betreffzeilen von Phishing-Mails zeigt sich dieser Trend konkret. Die Top 5 beinhalten Szenarien wie eine Beschädigung des Autos, ein Fehler in der Gehaltsabrechnung oder verpasste Teams-Nachrichten.

Social Engineering passt sich an das Zeitgeschehen an. Da es sich um einen Angriff auf emotionaler Ebene handelt, ist es besonders hilfreich, ein Bewusstsein für Angriffe solcher Art zu kultivieren. So vermeidet man Reaktionen aus dem Bauch heraus und verbessert die Schutzmechanismen unter Mitarbeitenden.

Effektiv vorbeugen – aber wie?

Welche Hebel können Organisationen also ziehen, um sich vor den neuen Gefahren der Cyberkriminalität zu schützen? Entscheidend ist es, den Menschen als Hauptfaktor zu verstehen. Schließlich zielen Phishing und andere Social-Engineering-Taktiken speziell auf den Menschen als Sicherheitslücke ab. Ein gefestigtes Sicherheitsbewusstsein bei allen Mitgliedern einer Organisation kann daher ein Bollwerk gegen Cyberangriffe sein. Maßnahmen wie bestehende Prozesse besser abzusichern, Identity und Access Management zu verbessern und bei hybriden Arbeitsmodellen die Sicherheit hochzufahren, sind essenziell für die Cybersicherheit. Doch selbst bei gründlicher Umsetzung dieser Maßnahmen bleiben Organisationen anfällig gegenüber Social Engineering. Um das Gefahrenpotential solcher Angriffe zu senken, sollten Organisationen das Sicherheitsbewusstsein der Mitarbeitenden stärken.

Grundsätzlich ist es vorteilhaft das Thema Cybersicherheit in den alltäglichen Arbeitsablauf zu integrieren. Dafür gibt es eine Vielzahl von Methoden. Um aktiv sichere Gewohnheiten zu fördern, sind Security-Awareness-Programme, die auf eine verhaltenspsychologische Methodik zurückgreifen, ideal. Organisationen setzen heute bereits erfolgreich zahlreiche verhaltenspsychologische Methoden ein.



Der aktuelle Human Risk Review von SoSafe zeigt, dass Menschen anfälliger für die Manipulation und Ausbeutung mit negativen Emotionen geworden sind. (Quelle: SoSafe)

Nudging beispielsweise ist ein Konzept, bei dem Organisationen die Umgebung so anpassen, dass sie Mitarbeitende zu erwünschten Verhaltensweisen ermutigt. So können etwa regelmäßige E-Mails an die Sicherheitsthematik erinnern und sie so präsent halten. Beim sogenannten „Spaced Learning" handelt es sich um eine Methode, bei der das Wissen mit kurzen Abständen wiederholt wird. Das hilft, die Erinnerung zu festigen. Zudem können Organisationen das Wissen über verschiedene Kanäle vermitteln, sodass die Wiederholungen verschiedene Lerntypen abdecken. Beim Micro-Learning hingegen liegt der Gedanke zu Grunde, kurze und fokussierte Lerneinheiten anzubieten. So bleibt das pro Einheit vermittelte Wissen übersichtlich und die Lerneinheiten lassen sich leicht in den Arbeitsalltag integrieren. Kontextbasierte und personalisierte Lerninhalte ermöglichen wiederum, das relevanteste und dringendste Wissen an die Mitglieder einer Organisation zu bringen.

Synergieeffekte nutzen

Jede Organisation hat unterschiedliche Sicherheitsschwachpunkte und verschiedene Mitglieder haben individuelle Vorerfahrungen und Vorwissen zum Thema Cybersicherheit. Daher gibt es keine „One-Size-Fits-All"-Lösung. Der Situation angepasste Lerninhalte sind stattdessen angemessen. Sinnvoll ist es diese Methoden, zum Beispiel auf einer Lernplattform, zu kombinieren, um den Lernerfolg so leicht wie möglich erreichbar zu machen. Sie schließen einander keinesfalls aus, sondern ergänzen sich und multiplizieren so ihre Effekte.

Es ist nicht zu verkennen: Die Cyber-Bedrohungslage ist angespannt und dynamischen Entwicklungen ausgesetzt. Die gute Nachricht ist jedoch: Es gibt schon heute effektive und erprobte Methoden, mit denen sich Organisationen und deren Mitglieder wappnen können.

Dr. Niklas Hellemann

Die IT-Aufrüstung der KRITIS-Betreiber

FRÜHZEITIG MIT NIS2 AUSEINANDERSETZEN

Spätestens mit dem Beginn des Krieges in der Ukraine haben die Angriffe auf Betreiber Kritischer Infrastrukturen (KRITIS) deutlich zugenommen. Um ein gemeinsames IT-Sicherheitsniveau unter den Mitgliedsstaaten zu etablieren, hat die EU bereits im Jahr 2016 die NIS-Richtlinie verabschiedet, auf deren Basis in Deutschland das IT-Sicherheitsgesetz 2.0 aufgebaut wurde. Allerdings gab es einige Kritik an den gesetzlichen Vorgaben und mit der Corona-Krise und einer sich verschärfenden globalen Sicherheitslage im digitalen Raum, wurden neue Schwachstellen bei der IT-Sicherheit vieler Einrichtungen offenkundig. Die NIS2-Richtlinie ist das notwendige Update, um KRITIS-Betreiber auf den aktuellen Stand zu bringen. Sie wurde im Dezember 2022 vom Europäischen Parlament und vom Europarat erlassen und muss in den EU-Mitgliedsstaaten bis 17. Oktober 2024 national umgesetzt werden.

Auch KMU können nun KRITIS-Betreiber sein

Im Vergleich zur Vorgängerrichtlinie wurde der Geltungsradius von NIS2 erweitert. Dabei sind zwei Eigenschaften entscheidend für die Einstufung der jeweiligen Organisation oder des jeweiligen Unternehmens: Die Sektorzugehörigkeit und die Unternehmensgröße. KRITIS-Betreiber ist nicht länger, wer eine bestimmte Menge an Erzeugnissen (wie Trinkwasser oder Strom) produziert, sondern wer einem bestimmten Sektor angehört. Definiert sind 18 Sektoren, die zweigeteilt sind in elf Sektoren hoher Kritikalität und sieben sonstige kritische Sektoren (siehe Tabelle).

In diesen Sektoren werden von NIS2 auch KMU (kleine und mittlere Unternehmen) adressiert. Mittlere Unternehmen beschäftigen 50 bis 250 Mitarbeiter und erzielen entweder einen Jahresumsatz von 10 bis 50 Millionen Euro oder weisen eine Bilanzsumme von höchstens 43 Millionen Euro auf. Kleine Unternehmen beschäftigen weniger als 50 Personen und haben einen Jahresumsatz oder eine Jahresbilanz von höchstens 10 Millionen Euro.

Auf Grundlage der Sektorzugehörigkeit und der Unternehmensgröße wird ermittelt, ob eine Organisation oder ein Unternehmen zu den wesentlichen (englisch: „essential") oder zu den wichtigen („important") Betreibern zählt. Mit dem Wissen um die Sektorkategorien und Kenngrößen lässt sich in einer ersten Einstufung relativ leicht ermitteln, wie eine Organisation zu kategorisieren ist: Wer zum Sektor hoher Kritikalität gehört und in die Schwellenwerte mittlerer Unternehmen fällt oder diese überschreitet, gilt als wesentlicher KRITIS-Betreiber. Als wichtig gelten alle Betreiber aus Sektoren hoher Kritikalität, die kleiner als mittlere Unternehmen sind und zusätzlich alle Einrichtungen, die zu den sonstigen

SEKTOREN MIT HOHER KRITIKALITÄT

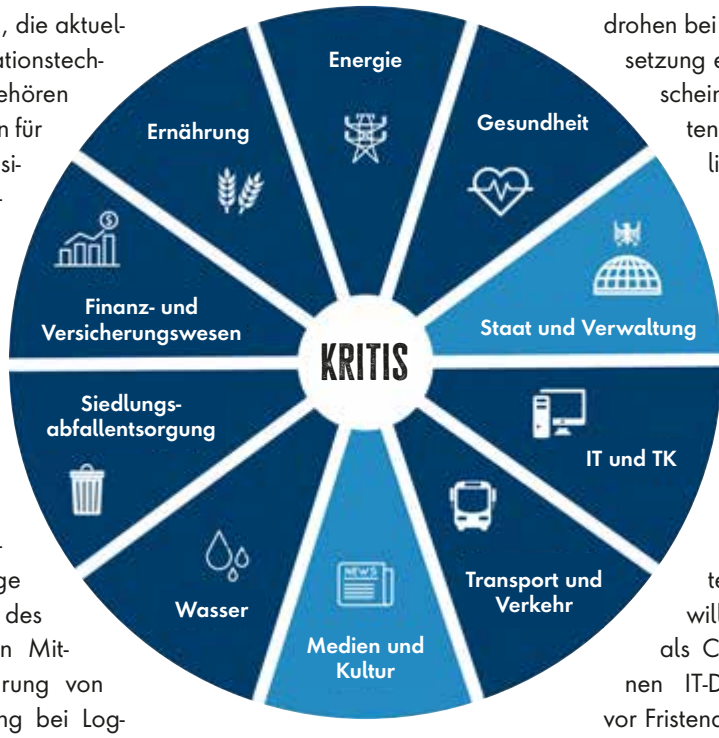
Digitale Infrastruktur	Verwaltung von IKT-Diensten (Business-to-Business)
Energie	Finanzmarktinfrastrukturen
Trinkwasser	Abwasser
Verkehr	Bankwesen
Öffentliche Verwaltung	Gesundheitswesen
Weltraum	
Sonstige kritische Sektoren	
Anbieter digitaler Dienste	Post- und Kurierdienste
Produktion, Herstellung und Handel mit chemischen Stoffen	Produktion, Verarbeitung und Vertrieb von Lebensmitteln
Verarbeitendes Gewerbe/Herstellung von Waren	Forschung
Abfallbewirtschaftung	

kritischen Sektoren gehören. Es gibt jedoch Ausnahmen: Die NIS2-Richtlinie ist auch auf Einrichtungen anzuwenden, die zum Beispiel wegen ihrer Monopolstellung oder einer speziellen Tätigkeit den wesentlichen Sektoren zugeordnet werden können. In diesem Fall spielt die Unternehmensgröße keine Rolle für die Bemessungsgrundlage.

Kampf gegen Cyberkriminelle

Um die EU-Mitgliedsstaaten „cyberresilient" zu machen, beinhaltet NIS2 eine Liste von zehn Maßnahmen, die aktuelle Standards in der Informationstechnologie abbilden. Dazu gehören beispielsweise Technologien für Disaster Recovery und Business Continuity. Das beinhaltet die Fähigkeit, Daten aus Backups wiederherstellen und so den Arbeitsbetrieb nach einem Zwischenfall zügig wieder aufnehmen zu können. Weitere Maßnahmen sind die Einrichtung von Systemen zur Prävention und Erkennung von Cybervorfällen, regelmäßige Schulungen zur Schärfung des Sicherheitsbewusstseins von Mitarbeitern oder die Einführung von Multi-Faktor-Authentifizierung bei Log-in-Prozessen. Ganz allgemein schreibt die NIS2-Richtlinie zudem Konzepte und Verfahren zur Bewertung der Wirksamkeit von Risikomanagementmaßnahmen in der IT-Sicherheit vor. Das bedeutet: KRITIS-Betreiber sollen regelmäßig evaluieren, ob die gewählten Maßnahmen noch zeitgemäß sind und angemessen funktionieren.

Kritische Infrastrukturen haben einen direkten Einfluss auf das öffentliche Leben. Sollte es zu einem Ausfall im Stromnetz oder einer Verunreinigung des Leitungswassers kommen, müssen Behörden und Bevölkerung über entsprechende Meldesysteme schnellstens informiert werden. Sicherheitsvorfälle gelten als meldepflichtig, wenn Betriebsstörungen, finanzielle Verluste oder schwerwiegende Schäden an juristischen oder natürlichen Personen drohen. Einrichtungen, die von einem solchen Fall betroffen sind, müssen dem Bundesamt für Sicherheit in der Informationstechnik (BSI) innerhalb von 24 Stunden über die Erkennung berichten und binnen 72 Stunden eine erste Bewertung inklusive einer Einschätzung



des Schweregrads abgeben. Zudem muss dem BSI spätestens einen Monat nach dem Vorfall ein Abschlussbericht vorgelegt werden.

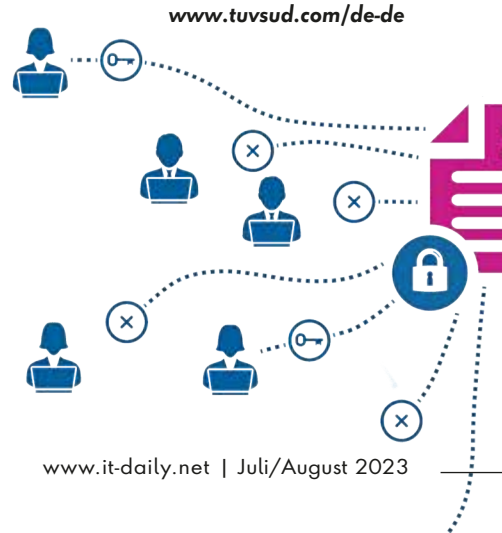
Kontrollpflicht für Lieferketten

Unternehmen sind nur sicher, wenn auch ihre Zulieferer sicher sind. Das gilt auch für KRITIS-Einrichtungen. Daher verpflichtet NIS2 die wesentlichen und wichtigen Einrichtungen dazu, die eigenen Lieferketten zu überprüfen. Allerdings sind die Detaillierungen zu diesem Punkt nicht sehr umfangreich, so dass die Einrichtungen die Angemessenheit der getroffenen Maßnahmen selbst bewerten können und müssen. Als Anhaltspunkte nennt die Richtlinie, dass auch die Beziehungen zwischen den Einrichtungen betrachtet werden sollen und dass die Gesamtqualität in Bezug auf die Cyber-Sicherheit ebenso zu bemessen ist wie ein ggf. vorhandener Entwicklungsprozess.

Mit Zertifizierungen auf der sicheren Seite

KRITIS-Betreiber sollten sich frühzeitig mit NIS2 auseinandersetzen. Betreibern drohen bei Nachlässigkeiten in der Umsetzung empfindliche Strafen. Zudem scheint es aufgrund der gesammelten Erfahrungen wahrscheinlich, dass die Bundesregierung mit der Überführung der Richtlinie in nationales Recht eine dritte Fassung des IT-Sicherheitsgesetzes verabschieden und dass dieses „IT-Sicherheitsgesetz 3.0" auch eine Verpflichtung zu Sicherheitsaudits, Prüfungen oder Zertifizierungen enthalten wird. Daher sollten KRITIS-Betreiber, die freiwillige Audits derzeit lediglich als Chance begreifen, ihre eigenen IT-Defensivmaßnahmen bereits vor Fristende im Oktober 2024 von unabhängiger Seite überprüfen lassen und gegebenenfalls an aktuelle Sicherheitsstandards und kommende gesetzliche Anforderungen anpassen.

Alexander Häußler, Thomas Janz
www.tuvsud.com/de-de



RANSOMWARE AS A SERVICE

MODELLE MIT GEWINNBETEILIGUNG

Das Ökosystem der Cyberkriminalität wird von denselben wirtschaftlichen Kräften angetrieben wie reguläre Märkte. Ein neues Geschäftskonzept oder eine neue Idee kann schnell zum neuen Standard werden. Eine dieser Revolutionen fand mit der Einführung des Ransomware-as-a-Service (RaaS)-Modells mit Gewinnbeteiligung statt. Bei diesem Modell arbeiten Ransomware-Betreiber mit Partnern zusammen, aber es handelt sich nicht um eine einfaches Abonnementmodell, wie oft beschrieben.

Wie funktioniert dieses System?
Ransomware-Betreiber entwickeln die Malware und betreiben die Infrastruktur. Die Partner sind Experten, die die Netzwerke kompromittieren. Nach einem erfolgreichen Angriff handeln die Ransomware-Betreiber das Lösegeld aus, treiben es ein und verteilen dann den jeweiligen Anteil an die Partnerunternehmen.

Heute ist es wahrscheinlicher, von einer dieser RaaS-Gruppen angegriffen zu werden, als von den älteren Ransomware-Modellen.

WHITEPAPER DOWNLOAD

Das Whitepaper umfasst 12 Seiten und steht kostenlos zum Download bereit.
www.it-daily.net/Download

Sicheres Cloud Computing

BRAINLOOP HILFT BEI DER UMSETZUNG

Die Kommunikation in Unternehmen wird heute immer häufiger von Cloudlösungen unterstützt. Diese Entwicklung macht selbst vor sensiblen Bereichen wie dem Vorstand oder dem Aufsichtsrat nicht halt. Wer hochvertrauliche Informationen dieser Gremien intern oder extern austauscht, sollte unbedingt darauf achten, dass der Anbieter einen ausgeprägten Datenschutz bieten kann. Brainloop Datenräume wurden von Anfang unter höchsten Sicherheitskonzepten entwickelt und erfüllen die Anforderungskriterien für sicheres Cloud Computing (BSI C5).

Effiziente Lösungen für erfolgreiche Board-Kommunikation

Brainloop bietet mehrere cloudbasierte Kommunikationslösungen für individuelle Anwendungsfälle. Speziell für den Bereich der hochvertraulichen Vorstands- und Aufsichtsratskommunikation ist dies das Portal Brainloop MeetingSuite. Die Lösung ist nicht nur äußerst sicher, sondern sorgt auch für zusätzliche Effizienz.

Mit Brainloop MeetingSuite lassen sich Sitzungsmappen intuitiv und automatisiert erstellen. Das Hochladen von Dokumenten erfolgt einfach mittels Drag-and-drop und Änderungen können noch bis zur letzten Minute vor Sitzungsbeginn vorgenommen werden. Aufsichtsräte und Vorstände greifen auf die Informationen mittels des favorisierten Endgerätes zu. Dabei können sie die Inhalte nicht nur online und offline lesen, sondern auch kommentieren und Notizen anbringen. Eine digitale Beschlussfassung unterstützt bei der Entscheidungsfindung und dokumentiert wichtige Ergebnisse.

Brainloop's Sicherheitskonzept für höchsten Datenschutz

Für höchste Sicherheit sorgen im Hintergrund mehrere Mechanismen. So basiert Brainloop MeetingSuite auf der Sicherheitsarchitektur Secure Dataroom, die speziell für hohe Ansprüche aufgebaut wurde. Das Konzept enthält alle Bausteine, die eine hochsichere Datenraumlösung benötigt. Hierzu zählen eine durchgängige Verschlüsselung der Daten auf dem Server, während der Übertragung und letztlich auf mobilen Geräten. Abschließend sichern ein Audit-Trail und die durchgängige Verschlüsslung die Umsetzung von Compliance-Richtlinien.

Lokales und testiertes Cloud-Computing

Als Datenraum-Anbieter hostet Brainloop seine SaaS-Plattform in ISO-27001-zertifizierten, hochverfügbaren, lokalen Datenzentren in Deutschland, Österreich und der Schweiz. Zusätzlich wurden die Brainloop Services seit 2022 nach dem C5 Kriterienkatalog des BSI (Bundesamt für Sicherheit in der Informationstechnik) testiert. Dabei stellt der Katalog nicht nur Anforderungen an die allgemeine Sicherheit des Produktes, sondern auch an sämtliche Unternehmensprozesse, die bei der Erbringung des Cloud-Service beteiligt sind. Erfahren Sie in unserem kostenlosen Whitepaper mehr über sicheres Cloud-Computing bei Brainloop.

Für Brainloop bedeuten die Anforderungen des BSI ohnehin längst Normalität. Denn seit der Gründung im Jahr 2000 bestimmen Sicherheit und Kontrolle für vertrauliche Informationen das Geschäft von Brainloop. Um auch in der heutigen Zeit Cyber-Attacken zu umgehen und die IT-Sicherheit in Unternehmen zu gewährleisten, ist es wichtig, dass IT-Grundschutz-Standards regelmäßig von internen IT-Sicherheitsbeauftragten überprüft werden. Dazu müssen Unternehmen: Erstens, ihr individuelles Cyber-Risiko genau kennen, und zweitens geeignete Tools und Maßnahmen für Cyberschutz etablieren.

www.brainloop.de

WHITEPAPER DOWNLOAD

Mit Sicherheit in die digitale Transformation

https://bit.ly/3MuOYkM

BRAINLOOP a MODERN GOVERNANCE company

Selbstbestimmte Identitäten (SSI)

OPEN-SOURCE SOFTWARE IST AUCH HIER AUF DEM VORMARSCH

Vertauschte Adressaten, offen herumliegende Gehaltszettel und mal wieder ein Philip, mit einem „P" zu viel. In Personalabteilungen kommt es immer wieder zu solchen Pannen. Obwohl die Digitalisierung in diesem Unternehmensbereich weit fortgeschritten ist, sind die Kommunikations- und Datenwege oft noch unsicher und verlaufen als Informations-Einbahnstraße.

Nachteile der gängigen Authentifizierungsverfahren

Um Betrug in sensiblen Datenräumen zu verhindern, ist es besonders wichtig, dass die Identität von externen Empfängern wie etwa Bewerbern oder ehemaligen Mitarbeitern zweifelsfrei identifiziert und authentifiziert wird. Eine gängige Methode hierfür ist das Abfotografieren oder Scannen des Ausweises, allerdings bieten diese Verfahren eine geringe Verlässlichkeit, da Sicherheitsmerkmale auf einem Foto verloren gehen können. Video- und Auto-Ident-Verfahren werden ebenfalls häufig genutzt. Während dieser Vorgänge müssen Bilddaten zwischengespeichert werden, allerdings wird oft nicht transparent offengelegt, wo und wie lange diese Daten gespeichert und verwendet werden. Informationen darüber sind oft hinter undurchsichtigen AGBs und Datenschutzerklärungen verborgen. Leider wird auch die Gefahr von Hackern und Online-Betrügern, die solche Systeme für ihre Zwecke nutzen können, immer noch unterschätzt.

Enmeshed als Praxisbeispiel für SSI

Die sogenannten selbstbestimmten Identitäten (SBI) versprechen Endnutzenden unabhängig von Identitätsdiensten Kontrolle und Hoheit, über die von Ihnen an externe Institutionen und Unternehmen übermittelten, personenbezogenen Daten. Sofern Unternehmen und Institutionen keine rechtliche Verpflichtung zur Archivierung der Daten vorliegen, geht die Verfügungsgewalt der Informationen vollständig an den Nutzenden über. Dies ermöglicht eine Übersicht der digitalen Beziehungen und der jeweiligen geteilten Daten.

Die Open-Source Software enmeshed baut ebenfalls auf der SBI-Methodologie auf. Im Gegensatz zu bestehenden Lösungen, greift die Anwendung auf eine zentrale, blockchainfreie Architektur

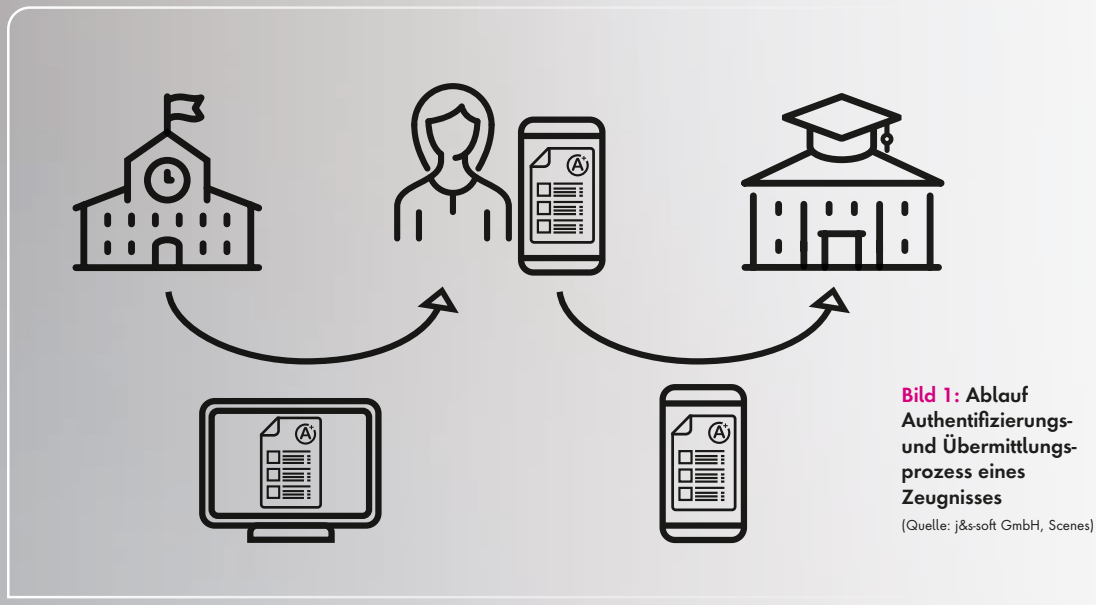


Bild 1: Ablauf Authentifizierungs- und Übermittlungsprozess eines Zeugnisses
(Quelle: j&s-soft GmbH, Scenes)

zurück. Als DSGVO-konforme SBI-Lösung kann enmeshed Praxisanwendungen vorweisen. Im Rahmen der Entwicklung des Minimum Viable Products der Nationalen Bildungsplattform bildet die Technologie als Bestandteil der Komponente „Ablage" eine Infrastruktur für einen sicheren Datentransfer und -speicherung zwischen Lernenden, Lehrenden und Bildungseinrichtungen. Besonders die niederschwellige und gleichzeitig sichere Nutzung als bidirektionale und hoch performante Ablage- und Kommunikationsmöglichkeit stellen die zentralsten Vorteile der Lösung dar. Die Anwendung konzentriert sich auf die Kommunikation im schulischen und universitären Umfeld sowie im Personalwesen in einem unternehmerischen Kontext. Beide Szenarien werden im Folgenden skizziert.

ANWENDUNGSFALL 1
Datentransfer beim Übergang Schule/Universität

Die 18-jährige Nicole (fiktiver Name) beendet im Sommer ihr Abitur am Zeppelin-Gymnasium Stuttgart und beginnt anschließend ihr Studium in International Business an der Munich Business School. Das Sekretariat ihrer Schule stellt Nicole einen QR-Code zur Verfügung, mit dem sie sich in der enmeshed App auf ihrem Smartphone mit der Schule verbinden kann. Dort wird ihr das Abitur-Zeugnis digital zur Verfügung gestellt und von ihrem Gymnasium als authentifiziert gekennzeichnet. Die Datei wird dabei auf dem lokalen Speicher von Nicoles Endgerät abgelegt. Ohne Ihre persönlichen Daten erneut eingeben zu müssen, kann sie ihr in Baden-Württemberg erworbenes Zeugnis durch Scannen des Universitäts-QR-Codes zur Immatrikulation an die Bayrische Uni weiterleiten. Über einen Backbone Layer sind Nicoles Identität und die der Universitätsverwaltung miteinander verknüpft.

PLUS
Weitere Infos unter: https://enmeshed.de

SELBSTBESTIMMTE IDENTITÄTEN FINDEN ÜBERALL DORT ANWENDUNG, WO EINE GROSSE MENGE PERSONENBEZOGENER DATEN UND DOKUMENTE AUSGETAUSCHT WERDEN.

Michael Feygelman, Senior Project & Community Manager, j&s-soft GmbH, https://enmeshed.de/

Die Normierung ihrer personenbezogenen Daten ermöglicht zudem die Übermittlung dieser in diverse IT-Systeme anderer Hochschulen für die sie sich bewerben kann. Des Weiteren werden durch die sogenannte Zero Knowledge Border ihre Angaben beim Transfer so Ende-zu-Ende verschlüsselt, dass selbst die App-Entwickelnden nicht auf Nicoles persönliche Daten zugreifen können. Sobald sie das Zeppelin-Gymnasium abschließt, kann sie zudem selbstständig entscheiden, ob ihre Schule weiterhin einen Zugriff auf Ihren Namen, ihren Wohnort oder Ihre E-Mailadresse haben soll. Ebenso kann sie bestimmen, welche Informationen die Munich Business School im Falle einer Ablehnung einbehalten darf.

Bild 2: Datenaustausch eines Unternehmens mit zukünftigen, aktuellen und vergangenen Mitarbeitenden
(Quelle: j&s-soft GmbH, Scenes)

ANWENDUNGSFALL 2
Unternehmensein und -austritte sicher managen

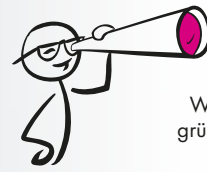
Nach 14 Jahren als Buchhalter in der j&s-soft GmbH verlässt Dominik Stein (fiktiver Name) aufgrund eines Umzugs sein Unternehmen. Die rechtliche Beziehung zwischen ihm als Arbeitnehmer und seinem Arbeitgeber läuft somit mit dem Vertragsende aus und damit auch sämtliche elektronischen Zugänge zu Postfächern, Datenbanken und allen unternehmensbezogenen Kontaktpunkten. Dennoch bestehen weiterhin bidirektionale Kommunikationsbedarfe, wie etwa die Korrektur der letzten Gehaltsabrechnung, die Übermittlung des Arbeitszeugnisses oder Abfragen zur betrieblichen Rentenversicherung. In der Vergangenheit hat die j&s-soft GmbH ihren Mitarbeitenden diese Dokumente per Post oder unverschlüsselt per E-Mail zukommen lassen. Um die Austrittskosten so niedrig wie möglich zu halten und die hochsensiblen Personaldaten sicher zu übermitteln, erstellt das Unternehmen über enmeshed eine firmeneigene selbstbestimmte Identität. Ähnlich wie beim Anwendungsfall im Bildungsbereich stellt die j&s-soft Dominik Stein einen QR-Code zur Verfügung. Über die App auf seinem Privathandy kann er nun seinem alten Arbeitgeber seine neue Adresse bestätigen sowie die erwähnten Dokumente empfangen.

Aber auch während des Bewerbungsprozesses oder der Anstellung finden selbstbestimmte Identitäten Anwendung. So müssen Bewerbende Lebensläufe, Sozialversicherungsnummern oder Krankenkassendaten nur erstmalig bei der App-Installation anlegen, bzw. durch die Verknüpfung ihres vorangegangenen Arbeitgebers bestätigen und können diese mit nur einem QR-Code Scan an Unternehmen oder Institutionen verschicken. Ebenso können Unternehmen diesen sicheren Kanal nutzen, um Push-Nachrichten zentralisiert an die Endgeräte ihrer Beschäftigen zu schicken, etwa für kurzfristige Hinweise, wie einen Bombenfund in Büronähe oder die weihnachtlichen Firmengrüße.

Erweiterung in weitere Anwendungsfelder

Selbstbestimmte Identitäten finden überall dort Anwendung, wo eine große Menge personenbezogener Daten und Dokumente ausgetauscht werden. Im hochsensiblen Bereich der Arztpraxis–Patientenkommunikation können zentrale Themen, wie die elektronische Patientenakte, aber auch vermeintlich einfache Abläufe wie Terminbuchung und -änderungen abgebildet werden. Außerdem ist der rechtskonforme Informationstransfer von Hausverwaltungen bzw. Vermietenden zu Mietenden zu nennen. Betriebskostenabrechnungen, Objektskizzen oder Ticketsysteme bilden hierbei die relevanten Anwendungsfelder. In diesem Zusammenhang lassen sich des Weiteren Rechtsdienstleistungen identifizieren, bei denen vordergründig eine digitale Interaktion zwischen Mandantschaft und Anwaltschaft für eine Beschleunigung der Bearbeitungsprozesse sorgen soll. Zusammenfassend lässt sich sagen: Um eine Akzeptanz und Verbreitung in den aktuellen sowie zukünftigen Anwendungsfällen zu gewährleisten, werden die Interoperabilität mit anderen Systemen und der Aufbau eines für jeden zugänglichen Kommunikationsökosystems für den Erfolg selbstbestimmten Identitäten maßgeblich sein.

Michael Feygelman



PLUS

Weitere technische Hintergründe zu selbstbestimmten Identitäten:
https://bit.ly/3o6r7ys

Identity Access Management

HERAUSFORDERUNGEN BEI DER IMPLEMENTIERUNG

Die Sicherheitsteams in Unternehmen stehen vor einer Reihe von Herausforderungen beim Identity Access Management (IAM). Um Firmengeheimnisse zu schützen, muss man den Zugang zu bestimmten Bereichen effektiv absichern. Die Verwaltung und regelmäßige Überprüfung von Zugriffsrechten von Mitarbeitern und Konten ist dabei unerlässlich und es wäre unrealistisch, anzunehmen, dass alle Benutzer, die auf Daten und Anwendungen im Netzwerk zugreifen, grundsätzlich vertrauenswürdig sind. Das grundlegende Zero Trust-Prinzip besagt, dass keinem Nutzer automatisch vertraut wird. Obwohl dieses Prinzip sinnvoll ist, stellt die Einführung einer IAM-Lösung für IT-Teams zahlreiche Herausforderungen dar.

Hürden abseits der Technologie

Bei der Implementierung von IAM-Lösungen hängen viele Herausforderungen eher mit Menschen und bestimmten Abläufen als mit der Technologie selbst zusammen. Identitätsmanagement ist nicht nur im Sicherheitsbereich ein zentraler Aspekt, sondern auch für alle anderen Abteilungen relevant. Oftmals sind es nicht die IAM-Teams, die entscheiden, wer welche Zugriffsberechtigung erhält. Häufig überschneiden sich Zugriffskontrollregeln, was zu großen Problemen innerhalb fragmentierter Systeme führen kann. Außerdem kommt es zu Differenzen bei der Frage, wer verantwortlich ist und ob es sich nun um ein Management-, Personal- oder Sicherheitsthema handelt.

Diese verschiedenen Interessengruppen, die sich über Umfang und Zugriff streiten, verstärken die IAM-Probleme. Zwar sollte jede der genannten Abteilungen bei der Einrichtung einbezogen werden. Geteilte Verantwortung bei der Federführung einer IAM-Lösung führt jedoch zu Problemen, denn Zugriffsrechte werden häufiger gewährt als entzogen. Dem Ansammeln nicht mehr benötigter Privilegien sollte man vor allem bei langjährigen Mitarbeitern entgegenwirken. Wenn die rollenbasierte Zugriffskontrolle (RBAC) nicht korrekt gehandhabt wird, können Verstöße gegen die Compliance-Vorschriften bei Zugriffskontrollen auftreten.

Altsysteme berücksichtigen

Eine weitere Herausforderung bei der Implementierung einer IAM-Lösung liegt darin, die Integration von veralteten Systemen zu bewerkstelligen. In einigen Unternehmen werden alte IT-Systeme nicht ganz überflüssig. Das heißt: IAM-Lösungen müssen überall funktionieren – auch in Unternehmen, die noch immer Mainframes verwenden, womöglich aber parallel modernste Cloud-Container einsetzen. Viele IAM-Strukturen in Unternehmen können damit nicht Schritt halten. Der Ausweg: ein zentralisiertes IAM-Repository zur effektiven Verwaltung von Benutzeridentitäten. Nur so kann man sich angemessen vor den Risiken des Betriebs in der Cloud schützen, wo die Identität eine zentrale Rolle spielt.

Ein gut implementiertes IAM-System stellt sicher, dass nur legitime Personen auf ein schützenswertes System zugreifen können. Wir sind an einem Punkt angekommen, an dem jedes Sicherheitskonzept Identitätslösungen beinhalten muss. Unternehmen sollten die sichere Verwaltung von Identitäten als unabdinglichen Teil der Umsetzung von Zero Trust-Modellen ansehen. Noch vor wenigen Jahren wurden IGA (Identity Governance and Administration) und IAM als Faktoren angesehen, die die Effizienz der Endbenutzer beeinträchtigen können. Doch diese Ansicht ist veraltet: Wenn IGA richtig angelegt ist und von der Organisation unterstützt und gepflegt wird, beschleunigt es die Produktivität.

Nils Meyer

IAM-LÖSUNGEN MÜSSEN ÜBERALL FUNKTIONIEREN – AUCH IN UNTERNEHMEN, DIE NOCH IMMER MAINFRAMES VERWENDEN, WOMÖGLICH ABER PARALLEL MODERNSTE CLOUD-CONTAINER EINSETZEN.

Nils Meyer, Senior Solution Engineer, Omada GmbH, https://omadaidentity.com/de/

Alles unter einem Dach

VERSCHLÜSSELN UND CYBERCRIME-ABWEHR ZENTRAL IN EINER OBERFLÄCHE

So vielfältig die Cyberbedrohungen heute daherkommen, so divers sind auch die Tools zu ihrer Abwehr. Die Unified-Endpoint-Management-Lösung ACMP vereint sie unter einem Dach. Das Resultat: mehr Übersicht und zentrale Steuerung/Auswertung.

Je stärker Unternehmen sich digitalisieren, desto intensiver vernetzen sie sich nach innen und nach außen. Damit öffnen sich neue Einfallstore für Cyberkriminelle, und die Angriffe nehmen an Komplexität zu. Erforderlich sind immer ausgefeiltere Verteidigungsmechanismen – von der Frühzeiterkennung von Viren, Schadsoftware und Spyware über die permanente Überwachung mittels Event-Überblick bis zu automatisierten Aktualisierungen der Bedrohungsdefinitionen und Festplattenverschlüsselung. Für jeden Security-Zweck gibt es Spezialsoftware, die es im Überblick zu behalten gilt.

Die Aagon GmbH fährt deshalb einen zentralisierten Ansatz: Über die Oberfläche seiner UEM-Lösung ACMP ermöglicht der Anbieter die zentrale Verwaltung des Microsoft Defender. Das von Microsoft kostenfrei mitgelieferte Tool durchsucht Dateiverzeichnisse nach bösartigem Code und Prozessen, die das System befallen und die Leistung beeinträchtigen können. Entsprechende Einstellungen vorausgesetzt, läuft dies automatisiert in bestimmten Zeitabständen im Hintergrund ab. Erkannte Malware steckt der Defender in Quarantäne und isoliert sie damit vom Kern des Betriebssystems, um weitere Schäden zu verhindern.

Sicherheitsmaßnahmen laufen automatisiert ab

Über das Modul ACMP Defender Management lässt sich Microsoft Defender in nur einer Oberfläche auf allen Clients und Servern verwalten. Das reduziert den Aufwand und sorgt für Kostenersparnisse, da keine zusätzliche Antivirenlösung mehr nötig ist. Maßnahmen und Verhalten können über die UEM-Konsole zentral vorbereitet und automatisiert ausgeführt werden, beispielsweise auf Wunsch unabhängig bzw. abhängig vom Standort. Der hohe Automatisierungsgrad wird möglich durch ein integriertes Zusammenspiel mit weiteren Modulen der UEM-Lösung für Update- und Patchmanagement, Inventarisierung, Schwachstellenmanagement und weiteren.

Analog ist über das UEM-User-Interface auch eine Festplattenverschlüsselung mit dem Microsoft BitLocker möglich. Der BitLocker ist ein kostenfreies Tool, das Microsoft zum Verschlüsseln der Festplatten in den aktuellen Betriebssystemen mitliefert. Durch die Verschlüsselung der Festplatten sind die Daten beispielweise im Falle eines Diebstahls geschützt. Mit dem ACMP BitLocker Management können IT-Admins Betriebssystem- und Festplattenverschlüsselungen des BitLockers zentral und nativ vorbereiten und automatisiert ausführen lassen – auch dies wiederum aus einer Oberfläche heraus und standortunabhängig. Bei Vorfällen werden sie umgehend informiert und haben dank Verbindung zur ACMP-Inventarisierung eine vollständige Übersicht der gesamten Infrastruktur. Monitoring- und Reportingfunktionen gestatten umfangreiche Analysen.

Fazit

Vorhandene Lösungen wie Microsoft Defender und BitLocker sind äußerst hilfreich. Wer sie über eine UEM-Konsole steuert, profitiert von noch besserem Überblick und automatisierter IT-Security. Dass dies funktioniert, beweist Aagon mit seiner ACMP Suite.

www.aagon.com

PLUS Kostenlose Testversion unter **www.aagon.com/testversion**

Managed Detection and Response

AUF WELCHE TRENDS IT-SICHERHEITSVERANTWORTLICHE JETZT REAGIEREN SOLLTEN

UNTERNEHMEN SOLLTEN SICH ZÜGIG AUF DIE SUCHE NACH GEEIGNETEN MDR-ANBIETERN MACHEN, SONST WIRD ES SCHWER, DEN GEEIGNETEN PARTNER NOCH ZU FINDEN.

Jörg von der Heydt,
Regional Regional Director DACH,
Bitdefender, www.bitdefender.de

Managed Detection and Response gehört zu den wichtigsten Trends in der IT-Sicherheit. Die Nachfrage nach solchen Diensten ist auch die Reaktion auf die Umbrüche in der Cyber-Sicherheit in den letzten Jahren. Unternehmen sehen sich gezwungen, nach externer Hilfe durch geeignete Partnern Ausschau zu halten. Drei Tendenzen spielen dabei eine entscheidende Rolle.

Auch in Deutschland wächst die Nachfrage nach Managed Security Services. Wie in anderen Ländern suchen IT-Sicherheitsverantwortliche nach einem externen Sicherheitsteam oder einem Security Operation Center (SOC). Das bestätigen die Ergebnisse des Bitdefender 2023 Cybersecurity Assessment Report: Selbst bei großen Unternehmen mit mehr als 1.000 Mitarbeitern haben 30,9 Prozent der großen Unternehmen laut eigener Aussage nicht die Kapazitäten, um mit der komplexen Bedrohungslage umzugehen. Nur ganze 1,47 Prozent sagen, dass sie weder einen solchen Dienst beanspruchen noch dies planen.

Der Markt ist den Kinderschuhen entwachsen, aber er befindet sich in einem Reifeprozess. Das wirkt sich auch auf die IT-Sicherheit aus. Unternehmen müssen reagieren. Drei Trends legen eine Reaktion nahe:

Trend 1: MDR wird zum Cyber-Versicherungsfall

Cyber-Versicherungen sehen den Mehrwert von MDR und SOC. Zugleich misstrauen sie zunehmend den Fähigkeiten von Unternehmen, für ihre IT-Sicherheit zu sorgen. Daher verlangen sie von den Versicherungsnehmern, externe Hilfe in Anspruch zu nehmen. Sie werden unter Umständen Daten der Telemetrie, zu Aktivitäten von Angreifern und andere Informationen über ihre potenziellen Versicherungsnehmer berücksichtigen, die ihnen die MDR-Dienste des Kunden liefern. Das hat einen Einfluss auf Prämien, Schadendeckung und ausgezahlte Erstattungen.

Was sollten Unternehmen tun? Sie sollten wissen, auf welche Daten des MDR-Anbieters eine Versicherung Zugriff hat und wie er sie verwendet. Sie erkundigen sich, ob sie Mitsprache bei der Weitergabe von Informationen haben.

Trend 2: Die Qual der Wahl

Mit zunehmendem Wachstum und Markreife wächst das Angebot an Managed Services. Dieses umfassen verstärkt auch weitere Angebote wie Mehrfaktor-Authentifikation, verwaltete Backups oder die Abwehr von gezielt ausgespielten Attacken auf kleine und mittelständische Unternehmen oder in bestimmten Branchen.

Was sollten Unternehmen tun? Angesichts der Auswahl sollten sie sich drei Fragen stellen: Was kann die eigene IT nicht intern abbilden? Welche Vorgaben von Compliance oder von Cyber-Versicherungen gilt es zu erfüllen? Bietet ein ausgewählter MDR-Anbieter einen umfassenden Dienst oder entsteht ein Wildwuchs verschiedener Anbieter?

PLUS Managed Detection & Response
bit.ly/43i81UZ

Trend 3: Steigende Nachfrage zu MDR

Mangel an Budget, ökonomische Unsicherheiten und Rezessionsängste setzen Entscheider unter Druck. Viele Cyber-Sicherheitsverantwortliche sehen daher in MDR eine preisgünstige Möglichkeit, ihren Schutz auszubauen.

Zudem müssen viele Unternehmen in der nahen Zukunft auf den gesetzgeberischen Druck hierzulande und in der EU, sei es durch das IT-Sicherheitsgesetz oder NIS 2, reagieren. Die Nachfrage nach MDR steigt also. Das wird die Balance zwischen Angebot und Nachfrage verändern.

Was sollten Unternehmen tun: Sie sollten sich zügig auf die Suche nach geeigneten MDR-Anbietern machen. Denn wer diese Suche zu spät startet, hat es eventuell schwer, den geeigneten Partner noch zu finden – denn auch dort sind Fachkräfte nicht leicht zu finden.

Jörg von der Heydt

Skalierbare Netzwerksicherheit

20 JAHRE IT-SICHERHEIT DURCH ÜBERBLICK UND KONTROLLE

In diesen Tagen kreisen viele berufliche und private Gespräche um das Thema Sicherheit und seine vielen Facetten. Das reicht von der (un)sicheren Rente über den bedrohlichen Krieg in Europa bis hin zum Thema Künstliche Intelligenz. Die Firma macmon secure beschäftigt sich bereits seit 20 Jahren mit einem speziellen Aspekt der Sicherheit – der Netzwerksicherheit.

Über sichere Netzwerke denken die meisten erst nach, wenn es zu einer Störung kommt, der Zugriff auf unternehmenskritische Daten nicht mehr möglich ist, das eigene Unternehmen beispielsweise zur Zielscheibe von Cyberkriminellen wurde. Im Tagesgeschäft spielen für die IT-Verantwortlichen neben dem Thema Sicherheit auch andere Aspekte eine wechselnde Rolle. In den letzten Jahrzehnten hat die Komplexität von Netzwerken immens zugenommen, man denke nur an die Menge der Endgeräte, die mittlerweile unseren Arbeitsalltag bestimmen, inklusiven BYOD-Geräten und technischen Devices wie beispielsweise einem Röntgengerät auf dessen Daten im gesamten Krankenhaus zugegriffen wird. Krankenhäuser sind mittlerweile gemischte Netzwerke, deren Kontrolle und Sicherheit essenziell sind. Eine Störung kann für Patienten lebensbedrohliche Folgen haben, beispielsweise wenn Beatmungsgeräte auf der Intensivstation gestört sind.

Jan Schmitt, Systemadministrator bei den Haßberg-Kliniken, beschreibt seine Sicherheitsanforderungen: „Die Ziele unseres IT-Sicherheitskonzepts sind der Schutz vor internen und externen Angriffen, die Gewährleistung der Funktionalität aller Systeme und natürlich das Thema Datensicherheit, da wir es hier mit hochsensiblen Patientendaten zu tun haben. Auch die Sicherheit besonders kritischer Bereiche wie den Operations- oder Aufwach-Räumen, der Labor-Abteilung und der Intensivstation gehören zu unserem Security-Konzept."

IT- und OT-Netzwerke wachsen zusammen

Heute gehört macmon secure zur globalen Belden Gruppe und sorgt mit mehr als 1.500 Kundeninstallationen für IT- und OT-Sicherheit in lokalen und digitalen Netzwerken. Das Unternehmen arbeitet im Bereich Industrial Automation Solutions (IAS), eine globale Organisation mit Hauptsitz in der Region Stuttgart, diese umfasst die führenden Netzwerk- und Konnektivität -Marken Hirschmann, ProSoft, OTN-Systems und Lumberg Automation.

Christian Bücker leitet die Geschäfte von macmon als Business Director, und treibt mit seinem 70-köpfigen Team die positive Entwicklung des Unternehmens weiter voran: „Durch die Integration in die Belden Gruppe kann man gemeinsam den globalen Kunden eine unterbrechungsfreie, sichere und skalierbare Netzwerk-Infrastruktur bieten. Dadurch sind Industrie-Kunden in der Lage die Betriebsabläufe zu revolutionieren und ihre Effizienz, Produktivität und Flexibilität zu

steigern." Effizientes Sicherheitsmanagement muss heute unter OT- und IT-Gesichtspunkten gemeinsam geplant und effizient umgesetzt werden. Die IT-Sicherheitsexperten bieten die Kompetenz als NAC-Anbieter und Belden die Expertise für industrielle Netzwerke. „Unsere enge Zusammenarbeit ermöglicht Automatisierungsprozesse und eine höhere vernetzte Sicherheit."

Das Thema IT-Sicherheit ist in der Produktion von exponentiell wachsender Bedeutung, das bestätigt auch Christof Peikert, Leiter IT, STEGO Elektrotechnik GmbH: „Die Erfassung der gesamten Infrastruktur und aller Endgeräte von STEGO als Live-Bestandsmanagement zählt zu den Kernkompetenzen von macmon. Darunter fallen beispielsweise die grafische Darstellung der Netzwerk-Topologie mit umfangreichen Analysemöglichkeiten und das Reporting der im Netzwerk ermittelten Messdaten. Durch Technologiepartnerschaften mit führenden Anbietern wie baramundi wird die NAC-Lösung bei STEGO als zentrales Sicherheits- und Management-System genutzt."

Kritische Infrastrukturen zunehmend in Gefahr

Aber auch die öffentliche Verwaltung ist im Fokus von kriminellen Cybercrime-Banden. Stefan Schönhals, Leiter Amt für Informations- und Kommunikationstechnik der Stadt Memmingen und Informationssicherheitsbeauftragter (ISB), ist sich der Bedrohungslage bewusst: „In der Stadtverwaltung von Memmingen arbeiten rund 750 Mitarbeitende mit sensiblen und personenbezogenen Daten. Zu unserem Aufgabengebiet zählt die Sicherung von Verwaltungsprozessen von Altersheimen über die Stadtwerke bis hin zum städtischen Klärwerk. Unsere umfangreichen Einwohner-Daten und Einrichtungen der kritischen Infrastruktur sind ein interessantes Ziel für Cyberkriminelle. Cyberattacken auf Kommunen sind besonders öffentlichkeitswirksam, betreffen direkt die Bürgerinnen und Bürger, sorgen für Aufsehen und die Störung öffentlicher Aufgaben."

WIR BIETEN UNSEREN GLOBALEN KUNDEN EINE UNTERBRECHUNGSFREIE, SICHERE UND SKALIERBARE NETZWERKINFRASTRUKTUR.

Christian Bücker,
Business Director, macmon secure,
www.macmon.eu

Sicherheitskonzepte wandeln sich mit den Anforderungen

Externe Netzwerkzugriffe auf Unternehmensressourcen sind heutzutage Normalität. Geräte werden weltweit genutzt und können überall und zu jeder Zeit direkt auf Cloud-Dienste, E-Mail-Applikationen und andere potenziell vertrauliche Unternehmensressourcen zugreifen. Kriminelle setzen somit an unterschiedlichen Stellen an, um ihre Ransomware in Unternehmen, Betrieben, Institutionen oder Behörden zu platzieren. 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. In traditionellen Sicherheitskonzepten wird alles, was sich im internen Netzwerk befindet, noch als vertrauenswürdig eingestuft. Zero Trust ist ein Sicherheitskonzept, bei dem prinzipiell jedem Gerät, Nutzer oder Dienst von vorneherein misstraut wird, ohne einen Unterschied zu machen, ob der Dienst, das Gerät oder der Nutzer sich innerhalb oder außerhalb des eignen Netzwerks befindet. Mit Network Access Control (NAC) und Secure Defined Perimeter (SDP) wird dieses Sicherheitskonzept für die reale und digitale Welt realisiert.

Langjährige Partnerschaften basieren auf Vertrauen

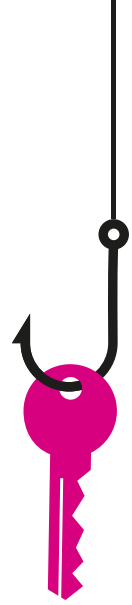
Die Lösungen werden durch erfahrene Vertriebs- und Implementierungspartner vermarktet, die die Bedürfnisse ihrer Kunden kennen. Dazu Thomas Zeller, Ettlinger IT-Systemhaus BWG, langjähriger Gold-Partner von macmon secure: „Wir haben uns auf IT-Sicherheit im Mittelstand sowie in kleinen und mittleren Unternehmen (KMU) spezialisiert. Nach der Maßgabe ‚So wenig wie möglich aber so viel wie nötig' haben wir für Ritter Sport ein bedarfsgerechtes und individuelles Konzept für die IT-Security Strategie erarbeitet und für das Thema Netzwerksicherheit das macmon Premium Bundle empfohlen, da wir mit diesem Hersteller in der Praxis sehr gute Erfahrungen sammeln konnten."

Fazit: In den vergangenen 20 Jahren hat sich die Bedrohungslage kontinuierlich gewandelt, da ist es besonders wichtig auf zuverlässige Partner zu setzen, die ihre marktführenden Technologien ständig weiterentwickeln. Das eigene Entwicklerteam und der hausinterne Support bei macmon in Berlin ermöglichen es, auch neue Kundenanforderungen erfolgreich zu erfüllen. Durch zahlreiche Technologiepartnerschaften stellt man sicher, dass Daten zwischen verschiedenen Systemen ausgetauscht, und effizient genutzt werden. Durch Übersicht und Kontrolle aller Netzwerkkomponenten wird die Sicherheit der Prozesse erhöht, und die IT-Teams sparen zudem wichtige Administrationszeit und Kosten.

Sabine Kuch

Schutz
vor Phishing Mails

WIE SICH BETRÜGERISCHE NACHRICHTEN ENTTARNEN LASSEN



Die E-Mail ist das gängigste Kommunikationsmittel der digitalisierten Geschäftswelt. Obwohl gerade seit der Pandemiezeit deutlich öfter Kollaborationstools im Einsatz sind, erhält jeder zweite Berufstätige laut Bitkom über 20 E-Mails pro Tag. Da ist es wenig überraschend, dass auch Kriminelle auf elektronische Nachrichten setzen, um einen Cyberangriff auf ein Unternehmen zu starten.

Doch auch Privatpersonen sind zunehmend von Phishing-Attacken betroffen. Laut dem BSI-Bericht zur Lage der IT-Sicherheit in Deutschland 2022 haben im letzten Berichtszeitraum vor allem die sogenannten Finance Phishing-Mails stark zugenommen. Dabei versuchen die Kriminellen, Zugangsdaten zu Bankkonten abzugreifen, indem sie dem Adressaten vorgaukeln, er müsse seine Log-In Daten aus irgendeinem Grund aktualisieren.

Bis vor einigen Jahren fielen Phishing-Mails vor allem dadurch auf, dass der Text meist in bemerkenswert schlechtem Deutsch verfasst war. Das hat sich zwischenzeitlich geändert, denn mit KI-Sprachmodellen ist es möglich, fehlerfreie Texte zu schreiben.

Trotzdem gibt es eine ganze Reihe von Anhaltspunkten, über die sich Phishing-Mails enttarnen lassen. E-Mail-Empfänger sollten vor dem Öffnen einer Mail idealerweise folgende Punkte überprüfen:

#1 Empfänger:
Wurde die Mail an mehrere Personen im Unternehmen versendet und sind darunter auch Namen, von denen der Empfänger bislang noch nie etwas gehört hat? Dann ist auf jeden Fall Vorsicht geboten.

#2 Absender:
Kriminelle tarnen ihre Absenderadressen oft hinter gefälschten oder leicht abgewandelten E-Mail-Adressen von bekannten und seriösen Organisationen. Gerne werden optisch ähnliche Buchstaben ausgetauscht, die besonders bei einer kleinen Darstellung auf dem Smartphone nicht so einfach zu erkennen sind. Im geschäftlichen Umfeld sollte sich der Empfänger in jedem Fall fragen, ob er eine Mail erwartet hat, die dem entspricht, was er im Postfach vorfindet und zwar in Bezug auf den Absender, das Thema und ob es Sinn macht, dass Links und Anhänge in der Mail enthalten sind.

#3 Datum und Uhrzeit:
Viele Phishing-Attacken werden aus Ländern gestartet, die sich in einer anderen Zeitzone befinden. Sind E-Mails zu ungewöhnlichen Uhrzeiten oder an unüblichen Tagen eingegangen, lohnt es sich, ein zweites Mal hinzusehen.

#4 Betreffzeile:
Die Betreffzeile soll Empfängern helfen, die Nachrichten gemäß ihrer Dringlichkeit zu sortieren. Phishing-Mails versuchen deshalb häufig über diese kurze Textzeile Druck aufzubauen und den Adressaten zu einem vorschnellen Öffnen zu bewegen. Sollten also Worte wie „Dringend" oder „Wichtig" auftauchen, sollten unbedingt weitere Parameter geprüft werden, bevor man die Mail anklickt.

#5 Anhänge und Hyperlinks:
Eventuell gefälschte Adressen bei einem Hyperlink lassen sich durch ein Mouse-Over enttarnen. Dafür wird der Mauszeiger über den Link gelegt OHNE zu klicken. In der Regel erscheint dann eine kleines Pop-Up Fenster oder eine Statusleiste mit der richtigen Zieladresse des Links.

#6 Inhalt:
Bezieht sich der Inhalt der Mail auf ein längst abgeschlossenes Thema, oder handelt es sich um einen unüblichen Vorgang, wie ein dringendes oder angeblich streng geheimes Projekt? Auch bei Inhalten, die nicht zu den normalen Prozessen im Unternehmen passen, sollte der Empfänger vorsichtig sein.

www.bvsw.de

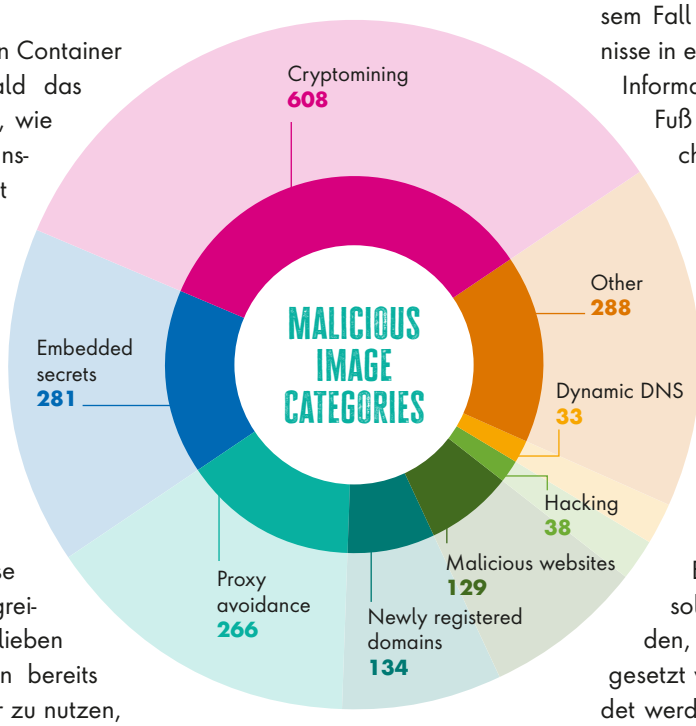
WHAT TO DO IN CASE OF ...

- erscheint einer der Punkte fragwürdig, nichts klicken oder öffnen
- bei bekannten Kontaktdaten, einfach anrufen und nachfragen
- Rechnungen oder Kundendaten erst auf der Homepage des Unternehmens prüfen

Container

DAS ULTIMATIVE TROJANISCHE PFERD

In einer idealen Welt sollten Container unveränderlich sein. Sobald das Image erstellt ist, bleibt es, wie es ist, und alle Container-Instanzen, die daraus erzeugt werden, sind identisch. Der Container ist als Code definiert, so dass seine Inhalte, Absichten und Abhängigkeiten klar definiert sind. Aus diesem Grund können Container, wenn sie sorgfältig eingesetzt werden, dazu beitragen, Supply-Chain-Risiken zu minimieren. Diese Vorteile sind jedoch bei Angreifern nicht unbemerkt geblieben und Cyberkriminelle haben bereits damit begonnen, Container zu nutzen, um bösartige Daten zu verbreiten.



Public Registries: Ein zweischneidiges Schwert

Docker Hub ist die beliebteste kostenlose, öffentlich zugängliche Container-Registry. Sie beherbergt Millionen von vorgefertigten Container-Images in praktischen, in sich geschlossenen Paketen. Public Registries sparen Entwicklern Zeit und bei solch einer großen Auswahl an Containern ist es leicht, den falschen zu erwischen. Cyberkriminelle kalkulieren, wie praktisch die Technologie für Entwickler-Workflows ist und verlassen sich darauf, dass diese nicht überprüfen, was genau installiert wird. Eine Strategie, vor der man sich in Acht nehmen sollte, ist das Typosquatting, bei dem ein Image als legitim getarnt wird, aber Schadsoftware enthält. Der Name des Images kann dabei mit nur einem Buchstaben vom echten Image abweichen. Alternativ verlässt sich der Angreifer darauf, dass ein Entwickler unvorsichtigerweise einige Anweisungen kopiert hat, die den bösartigen Pfad beinhaltet. Diese Stolperfallen verlassen sich auf die Unaufmerksamkeit der Nutzer.

Was sich wirklich im Container befindet

Das Sysdig Threat Research Team analysierte über mehrere Monate hinweg mehr als 250.000 Linux-Images. Dabei wurde festgestellt, dass davon 1.777 Images verschiedene Arten von bösartigen IPs oder Domänen und eingebettete Anmeldedaten enthalten.

Bei näherer Betrachtung stellt sich heraus, dass Kryptomining-Images der häufigste bösartige Image-Typ sind. Dies war zu erwarten, da das Mining von Kryptowährungen auf fremden Rechenressourcen heutzutage die beliebteste Art von Angriffen auf Cloud- und Container-Umgebungen ist.

Bei in Docker-Images eingebetteten Geheimnissen handelt es sich um die zweithäufigste Angriffstechnik. In diesem Fall fügen die Angreifer Geheimnisse in ein Image ein und nutzen diese Informationen, um in Ihrer Umgebung Fuß zu fassen und dann zu versuchen, sich weiter zu bewegen. So kann beispielsweise ein SSH-Schlüssel hinzugefügt werden, der einen einfachen Fernzugriff ermöglicht. Dies zeigt, dass die Verwaltung von Geheimnissen immer noch ein Kampf ist, den IT-Teams gewinnen müssen.

Fazit

Extern beschaffte Container sollten gründlich geprüft werden, bevor sie in Unternehmen eingesetzt werden, egal, wo sie verwendet werden. Statische Analysen allein reichen hier nicht aus. Die dynamische Analyse ist die einzige Methode, um einen Container zu prüfen, sobald er ausgeführt wird. Hierbei empfehlen sich Tools, die das Verhalten des Containers beobachten und Alarm schlagen oder automatisch mit entsprechenden Maßnahmen reagieren, wenn verdächtiges Verhalten festgestellt wird. Unternehmen müssen sich über die Risiken im Klaren sein, die vorgefertigte Images mit sich bringen können. Kryptominer können sehr schnell sehr teuer werden, und Backdoors können zu einer Gefährdung der gesamten Infrastruktur führen. Die Begeisterung für Container ist derzeit groß und leider gilt das auch und vor allem für Cyberkriminelle.

Stefano Chierici, www.sysdig.com

Cyber Threat Intelligence (CTI)

MIT DEM RICHTIGEN KONTEXT ZU MEHR IT-SICHERHEIT

Die Bedrohungslage in Sachen Cybersicherheit verschärft sich zusehends. CISOs und CIOs sind mit immer neuen Bedrohungen konfrontiert, die jeweils eine geeignete Strategie erfordern, um ihnen standhalten zu können.

Überlegungen, wie man dieser Situation begegnen könnte, mündeten in der Entwicklung von Cyber Threat Intelligence (CTI) beziehungsweise Threat Intelligence Services, die nach und nach eine immer größere Rolle für die IT-Sicherheit vieler Organisationen spielen. Ziel ist es, damit alle verfügbaren Informationen über Cyberbedrohungen zu sammeln und zu berücksichtigen, die bereits beobachtet wurden.

So manchem Security-Verantwortlichen ist jedoch noch immer nicht ganz klar, welcher langfristige Nutzen sich aus diesem Ansatz ergibt. An dieser Stelle sollen daher die vier wichtigsten Aspekte von CTI näher beleuchtet und Vorteile aufgezeigt werden.

Bedeutung von CTI

Eine Forrester-Studie, die unter dem Titel Automation and Unification Enable a Cohesive Attack Surface Defense 2022 erschienen ist, kommt zu dem Schluss, dass im Falle von Ransomware eine erhebliche Lücke zwischen der Erkennungsgeschwindigkeit aufseiten der Unternehmen und dem Tempo eines Angriffs klafft. Die Auswirkungen solcher Attacken auf Unternehmen (Umsatzeinbußen, Datenverluste, Rufschädigung) sind weithin bekannt. Nicht zuletzt dadurch wird deutlich, wie wichtig das Wissen um die Cyberbedrohungslage und aktuelle Taktiken der Angreifer innerhalb eines Cybersicherheitsteams ist.

Indem sie die Security-Verantwortlichen in den Unternehmen in Echtzeit mit nutzbaren Bedrohungsanalysen versorgen, helfen CTI-Teams dabei, Organisationen besser zu schützen. Hier sollten die Teams auf moderne KI-Algorithmen setzen, mit denen sich sowohl die Bedrohungen selbst als auch die Hintermänner dieser Attacken überwachen und identifizieren lassen. Dadurch werden entsprechende Angriffe frühzeitig erkannt und können so rechtzeitig eingedämmt werden, bevor größerer Schaden entsteht.

CTI als Tool zur strategischen Entscheidungsfindung

Mit CTI lässt sich das bestehende Cybersicherheitsarsenal einer Organisation um einen weiteren Baustein ergänzen. Die Vorteile dieses Ansatzes liegen auf der Hand: Zunächst bietet CTI eine

erhebliche Zeitersparnis, da die relevanten Informationen optimal genutzt werden, und unterstützt so die effiziente Entscheidungsfindung innerhalb des Security-Teams. Darüber hinaus wird mittels CTI die Kundenkommunikation sowie die Risikobewertung unterstützt und das Krisenmanagement verbessert. Auch darf nicht außer Acht gelassen werden, dass mit diesem Ansatz die durchschnittlichen Kosten eines Security-Vorfalls bedeutend gesenkt werden können.

Im Allgemeinen sind Bedrohungsdaten wertvolle Informationen, die dabei helfen, Risiken zu vermeiden oder zu reduzieren. Jedoch können nur kontextualisierte Informationen als „Intelligence" bezeichnet werden. Ohne Kontext verlieren diese Informationen ihren Wert für Security-Experten, da die relevanten Aspekte in der Datenmenge unterzugehen drohen. Mit Hilfe von künstlicher Intelligenz können CTI-Teams die verschiedene Informationsströme zusammenfassen und sie in einen Kontext rücken.

Mitarbeitern in einem Security Operations Center (SOC) hilft diese Intelligence dabei zu erkennen, wer als Bedrohung zu erachten ist, was Cyberkriminelle motiviert und welche Angriffstechniken sie anwenden. Zudem verbessert die Integration proaktiver Bedrohungsdaten im Falle von Security-Vorfällen die Reaktionsmöglichkeiten. Nur mittels der entsprechenden Informationen sind die technischen Teams in der Lage, nach den Penetrationsindikatoren zu suchen, um eine gefährliche Situation rechtzeitig zu entschärfen.

Die im Rahmen von CTI gewonnenen Informationen müssen daher den Verantwortlichen zugänglich sein und an die Betriebsumgebung angepasst werden. Hier ist eine stetige Anpassung an

MIT CTI LÄSST SICH DAS DAS BESTEHENDE CYBERSICHERHEITSARSENAL EINER ORGANISATION UM EINEN WEITEREN BAUSTEIN ERGÄNZEN.

Olaf Müller-Haberland, Head of Sales and Services DACH, TEHTRIS, https://tehtris.com/de/

sich verändernde Rahmenbedingungen erforderlich. Ein in einer Organisation vorhandenes Security Information and Event Management (SIEM) muss daher mit der CTI integriert werden. Das SOC verfügt somit über Informationen zu:

- Phishing-URLs
- Angriffsszenarien, die es ermöglichen, Schwachstellen zu beheben
- Schädlichen Domänen und IP-Adressen
- Malware-Typen und Verbreitungswege
- Command- und Controll-Infrastrukturen (C&C) von Cyberkriminellen

Mit Hilfe der Bedrohungsdaten können Korrelationen aufgedeckt und neue Erkennungsregeln entwickelt werden. Auch lassen sich damit Datenlecks frühzeitig entdecken. Das SOC profitiert also in erheblichem Umfang von CTI. Aber das SOC ist bei weitem nicht der einzige Nutznießer.

CTI als Teil des Teams

Ursprünglich war Cyber Threat Intelligence dazu gedacht, das SOC-Team einer Organisation bei der Wahrung der Cybersecurity und der Reaktion auf Vorfälle zu unterstützen. Eingebettet in eine moderne Cybersicherheitsarchitektur muss CTI heute jedoch mit verschiedenen Abteilungen innerhalb des Unternehmens zusammenarbeiten und mit unterschiedlichen Teilen der Cyber-Infrastruktur interagieren. Das reicht von den Bedrohungsanalysten des SOCs bis hin zum COMEX (Executive Committee). Die Zusammenarbeit zwischen den verschiedenen Teams gewährleistet ein einheitliches Vorgehen beim Umgang mit Vorfällen sowie der entsprechenden Reaktion darauf. Zudem müssen die gewonnenen Bedrohungsinformationen für die Überwachungsinfrastruktur herangezogen werden.

Ein CTI-Team sollte folglich mit mehreren Akteuren in Verbindung stehen und sich mit ihnen austauschen. Dazu gehören unter anderem:

Vulnerability-Operations-Center-Teams (VOC) von Partnern

CTI ermöglicht die Überwachung, Qualifizierung und Priorisierung von Schwachstellen, die in einen Kontext gestellt werden. Ohne eine entsprechende Risikobewertung sind die für den Schutz der Organisation Verant-

WAS IST CYBER THREAT INTELLIGENCE?

CTI zielt darauf ab, so viele Informationen wie möglich über die Cyber-Bedrohung zu erhalten, sowohl aus technischer als auch aus taktischer oder operativer Sicht.

wortlichen nicht in der Lage die richtigen Entscheidungen zu treffen.

Technische Teams – von Architekten bis hin zu Incident Response Managern

Durch den Austausch sind diese Teams besser gerüstet, einen Angriff zu neutralisieren. Die Kontextualisierung ermöglicht eine bessere Analyse und Antizipation von Bedrohungen je nach Tätigkeitsbereich, aktuellen Ereignissen oder neuen Technologien.

Alle kontextualisierten Informationen erhöhen die Effektivität neuer Technologien wie Anti-Spam, Anti-Malware, EPP, EDR. Analysten benötigen Echtzeit-Informationen, die auf automatisierte Weise bereitgestellt werden.

Das Management (CISO, CIO, CFO und der gesamte Vorstand)

Die bereitgestellten Informationen helfen bei der Beantwortung strategischer und operativer Fragen. Anhand nutzbarer Daten kann die Unternehmensführung Bedrohungen einordnen, die sich gegen die Organisation richten könnten. Durch die Analyse von Kampagnen, cyberkriminellen Gruppen und Schwachstellen lassen sich die Trends abbilden und bewerten. Diese Ergebnisse ermöglichen die Entwicklung einer umfangreichen Cybersecurity-Strategie, die Planung von Szenarien und die konkrete Vorbereitung. Auf diese Weise können Managementteams die Risiken langfristig reduzieren.

Threat Intelligence sollte zum Schutz aller genutzt werden

Damit die Erkenntnisse von CTI nicht nur dem eigenen Unternehmen zugutekommen, sondern auch anderen bei der Stärkung ihrer Cybersicherheit helfen können, ist es wichtig, dass entsprechende Daten mit der „Community" geteilt werden. Angesichts immer ausgeklügelterer Angriffsketten, die nicht selten auch Attacken via Unternehmen aus der Lieferkette einschließen, stärkt ein solcher Ansatz auch die eigene Sicherheit. Durch den Austausch von Wissen können sich alle besser vor Angriffen schützen und tragen so auch zur Sicherheit anderer bei. Zu solchen Communities zählen unter anderem die Cyber Threat Alliance (CTA) oder INTERCERT.

In einem nächsten Schritt gilt es die erweiterte Bedrohungsanalyse (Extended Threat Intelligence, XTI) zu implementieren, die eine Bestandsaufnahme der externen Angriffsfläche liefert und kontextbezogene Daten weitergibt. Dieser neue Ansatz bietet Transparenz ohne weiße Flecken. Denn nur durch Transparenz und Koordination werden alle gemeinsam stärker.

Keine nachhaltige Cybersicherheit ohne CTI

Um sich wirksam vor Cyberattacken schützen zu können, müssen den Security-Verantwortlichen die Angriffstechniken und -methoden der Cyberkriminellen bekannt sein. Hierzu bedarf es spezieller technischer Teams, die diese Analyse umsetzen, aber nicht nur reine Techniker sind hier gefragt. Der politische, wirtschaftliche und kulturelle Kontext von neuen Formen der Cyberkriminalität bedarf auch eines Umdenkens in Sachen Personal. Um entsprechende Erkenntnisse also in den korrekten Kontext zu rücken, müssen die Cybersicherheitsteams nun auch beispielsweise um Linguisten, Wirtschaftswissenschaftler, Politologen, Psychologen und viele andere Professionen mehr ergänzt werden.

Die eigene Perspektive auszuweiten, und diese um andere Disziplinen zu ergänzen, ist unerlässlich, die Probleme und Motivationen hinter bestimmten Bedrohungen zu verstehen. Das Konzept der Multidisziplinarität muss in Ihre Cyberstrategie integriert werden. Nur so wird sichergestellt, dass durch die gemeinsame Nutzung komplementären Wissens der Analysten und des Know-hows der einzelnen Mitglieder der Organisation ein umfassender Security-Ansatz mit verschiedenen Blickwinkeln entstehen kann.

Olaf Müller-Haberland

THREAT INTELLIGENCE ERMÖGLICHT:

- einen besseren Schutz der Informationssysteme und sensiblen Daten des Unternehmens
- ein besseres Verständnis der Bedrohung und eine bessere Antizipation von Angriffen
- eine bessere Reaktions- und Entscheidungsfähigkeit

LinkedIn-Betrugsfälle

RUFSCHÄDIGUNG ALS GRÖSSTES PROBLEM

Laut der aktuellen Studie von NordLayer wurden 65 Prozent der großen Unternehmen mindestens einmal von einem betrügerischen/gefälschten Konto auf LinkedIn kontaktiert. Darüber hinaus haben 58 Prozent der mittelgroßen und 31 Prozent der kleinen Unternehmen mindestens eine Erfahrung mit Betrugsversuchen gehabt.

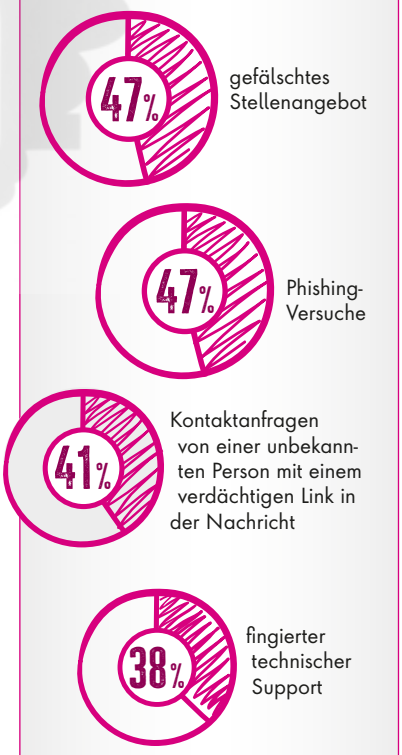
Überraschenderweise ist fast die Hälfte der Unternehmen (45 %) auch über einen Betrug auf LinkedIn informiert, bei dem der Markenname ihres Unternehmens verwendet wird. Diese Art von Betrug war bei großen Unternehmen am häufigsten (53 %), aber auch bei mittelgroßen Unternehmen ist er weit verbreitet: 53 Prozent dieser Unternehmen gaben an, dass diese Art von Betrug auch ihnen passiert ist. Nur kleine Unternehmen gaben an, dass sie fast nie von solchen Betrügereien betroffen sind (13 %).

Weitere Erkenntnisse

Als häufigste Folge von LinkedIn-Betrug nannten große Unternehmen Rufschädigung (48 %), gestohlene oder beschädigte Daten sowie einen hohen finanziellen Verlust (jeweils 40 %). Mittelgroße Unternehmen waren am häufigsten von Rufschädigung (47 %) und gestohlenen/beschädigten Kundenkontakten (45 %) betroffen. Kleinere Unternehmen, die in irgendeiner Form von Betrug betroffen waren, gaben an, dass finanzielle Verluste (67 %) sowie Betriebsunterbrechungen und gestohlenes geistiges Eigentum (jeweils 58 %) die häufigsten Folgen waren.

www.nordlayer.com/blog/linkedin-scams/

Die häufigsten Arten von LinkedIn-Betrügereien:



Sichere Videokonferenzen

NOTWENDIG UND ALLTAGSTAUGLICH?

Videokonferenzen sind für Cyberkriminelle ein beliebter Angriffspunkt geworden. Sie verschaffen sich Zugang zur Kommunikation von Firmen, greifen unbefugt Daten und geheime Informationen ab und fügen Unternehmen dadurch jährlich Schäden in Millionenhöhe zu.

Die gute Nachricht lautet: Unternehmen stehen nicht vor einer unlösbaren Aufgabe. Ganz im Gegenteil: Mit oft sehr simplen Maßnahmen können sie ihre Kommunikation zuverlässig gegen Angreifer schützen. Online-Meetings können durch den Einsatz der richtigen Technologie auch ohne erheblichen Aufwand vom offenen Tor zur abgeschirmten Festung werden.

Die gängigsten Tools sind by Design nicht sicher

Die gängigsten Lösungen im Alltag stammen von US-amerikanischen Anbietern. Jedoch unterliegen diese dem Cloud Act, der Plattformen verpflichtet, Daten über Kommunikationsströme bereitstellen zu können, falls Behörden sie anfordern. Die Vertraulichkeit ist dadurch nicht gewährleistet, es gibt „by Design" Punkte, um auf Daten zuzugreifen. Gerade Unternehmen, die hochsensible und wertvolle Inhalte kommunizieren, etwa in der Pharma- oder Finanzbranche stellt das vor ein Problem. Sie brauchen Alternativen, die „Secure by Design" sind, aus Europa stammen und in Europa gehostet werden, wie etwa die französische Plattform Tixeo. Der Standort des Anbieters ist aber nur eine der Bedingungen für geschützte Kommunikation.

Mitunter die wichtigste Rolle beim Schutz vertraulicher Inhalte kommt einer echten End-to-End-Verschlüsselung zu. Bei den meisten Lösungen erfolgt die Verschlüsselung nur vom Client zum Server, der dadurch zum Angriffspunkt für Hacker wird. Dies stammt daher, dass Sicherheit bei der ursprünglichen Entwicklung der Tools meist noch nicht im Vordergrund stand. Findet die Verschlüsselung von Client zu Client statt und wird der Schlüssel zur Entschlüsselung der Datenströme ausschließlich lokal beim User gespeichert, haben Dritte keine Chance, unbefugt mitzuhören. Ob eine Verschlüsselung wirklich sicher ist, bestätigen Zertifizierungen unabhängiger Sicherheitsbehörden.

Aufwand für die User ist keine gangbare Ausrede

Es ist gängige Alltagspraxis geworden, für den Beitritt zu Online-Meetings Zugangslinks zu versenden und zu nutzen. Diese machen es Kriminellen jedoch leicht, sich in Konferenzen einzuklinken, sie brauchen dafür lediglich den Link. Zur Teilnahme auf eine Plattform zu setzen, die vom Nutzer eine Passwortauthentifizierung sowie eine verschlüsselte und unumkehrbare Anmeldung mag zunächst gewöhnungsbedürftig sein, erhöht die Sicherheit aber drastisch. Organisatoren von Meetings behalten so jederzeit die volle Kontrolle über die Teilnehmer.

Sensible Kommunikation zuverlässig vor Attacken zu schützen, kann nicht von heute auf morgen erfolgen. Es ist aber einfacher und schneller umgesetzt als vielerorts angenommen. Basis sind die gründliche Recherche passender Anbieter und ein sorgfältiges Onboarding der Nutzer auf die neue Plattform. Die meiste Software für Videokonferenzen verfügt über ein ähnliches Interface, weshalb auch hier die Umstellung in der Regel schneller gehen dürfte als zunächst angenommen.

Online-Konferenzen sind zur zentralen Plattform für vertrauliche Inhalte geworden. Angesichts des intrinsischen Werts vieler Informationen, Gespräche sowie geteilter Dateien und Dokumente wäre es fahrlässig, sich keine Gedanken über den Schutz der Kommunikation zu machen. Videokonferenzen sind ein Punkt, den zu viele IT-Abteilungen noch übersehen. Dabei ist die Auseinandersetzung mit den Folgen erfolgreicher Cyberangriffe weit kostspieliger.

Valentin Boussin

ECHTE SECURITY BY DESIGN BEI VIDEOKONFERENZEN BIETET FAST NIEMAND – OBWOHL DIE RISIKEN ENORM SIND.

Valentin Boussin,
Country Manager DACH, Tixeo,
www.tixeo.com/de

Zero Trust in hybriden Arbeitsumgebungen

MIT PRAKTIKABLEN LÖSUNGEN ZU MEHR SICHERHEIT

In den letzten Jahren hat sich die weltweite Arbeitslandschaft grundlegend verändert, das Home Office ist selbstverständlich geworden. Damit steigen die Anforderungen an die IT-Sicherheit noch weiter – da die zu schützenden Ressourcen zumeist über mehrere Umgebungen verteilt sind, reicht es längst nicht mehr, Zugriffskontrollen am Rande eines Unternehmensnetzwerks einzurichten. Daten müssen während der Übertragung, im Ruhezustand und während der Nutzung über öffentliche und private Cloud-Umgebungen hinweg gesichert werden.

Als aktuell fortschrittlichstes Sicherheitsmodell sieht Zero Trust die Kontrolle und Authentifizierung jedes einzelnen Zugriffs auf Ressourcen oder Dienste innerhalb eines Netzwerks vor. In Echtzeit wird überprüft, ob ein Benutzer und sein Gerät zum Zugriff berechtigt sind. Jede Anfrage wird anhand von Kontextdaten zum Zeitpunkt des Zugriffs bewertet, einschließlich des Zustands und der Anmeldeinformationen des anfragenden Geräts, der Identität und Rolle des Anfragenden sowie der Sensibilität der Ressource. So kann ein sicherer Zugriff auf verteilte Unternehmensressourcen gewährleistet und das Risiko von Remote-Arbeit reduziert werden.

Der Aufbau eines Zero Trust Frameworks ist komplex. Anbieter mit umfassender Security-Expertise wie Entrust, helfen jedoch mit praktikablen Lösungen für die sichere Verwaltung von Daten, Identitäten, Berechtigungen, Schlüsseln und Zertifikaten – sei es im Multi-Cloud-, Hybrid- oder On-Premises-Betrieb. So entsteht ein übergreifendes Zero-Trust-Fundament, das sowohl hochsicheres Identitäts- und Zugriffsmanagement als auch Verschlüsselung miteinbezieht – und nebenbei die Kosten und Komplexität einer Infrastruktur reduziert.

www.entrust.com

Darknet

EIN NEUER FALL VON TECHNOLOGIE-PANIK?

In unserer Gesellschaft, in der immer mehr Lebensbereiche digitalisiert werden, nehmen auch Bedenken um die eigene Privatheit zu. So zeigen wissenschaftliche Untersuchungen zu Einstellungen rund um das Thema Privatheit, dass Menschen das Gefühl haben, diese stärker schützen zu müssen. Begleitet wird diese Debatte von Schlagwörtern wie Datenkraken, gläserner Bürger oder Post-Privacy-Gesellschaft.

Eine Möglichkeit, anonym zu bleiben und seine Privatsphäre online zu schützen, ist der Einsatz von Privacy Enhancing Technologies (PET), wie etwa Darknet-Technologien. Die bekannteste dieser Technologien ist das Netzwerk Tor (The Onion Router). Im Vergleich zu anderen Optionen zum Schutz der Privatheit im digitalen Kontext liegt der Vorteil von Tor darin, sich technisch anonym bewegen zu können, beispielsweise beim Surfen im Internet. Allerdings werden Darknet-Technologien eher negativ und als Bedrohung für die Gesellschaft wahrgenommen.

Was ist „Darknet"?

Worum handelt es sich bei Darknet-Technologie genau? Obwohl in der Medienberichterstattung und im allgemeinen Sprachgebrauch häufig von „dem Darknet" die Rede ist, gibt es dieses eine Darknet gar nicht. Stattdessen gibt es verschiedenste Darknet-Technologien. Die bekannteste und am weitesten verbreitete ist Tor, das im allgemeinen Sprachgebrauch oft synonym zum Begriff Darknet verwendet wird. Es handelt sich um ein Overlaynetzwerk, bei dem die Kommunikation über drei Tor-Knoten geroutet wird, wobei jeder Knoten nur seinen direkten Vor- und Nachgänger kennt. Betrieben werden diese Tor-Knoten von freiwilligen Unterstützenden. Somit wird technische Anonymität erreicht. Personen sind auf technischer Basis nicht identifizierbar. Zum Vergleich, bei der regulären Internetkommunikation werden die IP-Adressen im Klartext mitgesendet. Bei der Anwendung der Tor-Technologie lassen sich zwei Anwendungsfälle unterscheiden. Zum einen können auf dieser Basis Inhalte im Tor-Netzwerk angeboten und konsumiert werden, zum anderen haben Personen die Möglichkeit, mit dem Tor-Browser nicht nur auf das Tor-Netzwerk, sondern auch auf reguläre Inhalte im Clearnet (über regulären Browser erreichbar) technisch anonym zugreifen zu können.

Trotz der eingangs erwähnten Sorge um die eigene Privatheit sowie um die Akkumulation von persönlichen Daten durch Dritte, steht Darknet-Technologien eine tendenzielle Ablehnung gegenüber. Um eine bessere Vorstellung davon zu bekommen, wie diese gesellschaftlich verhandelt werden, haben jüngste Studien unter anderem die Medienberichterstattung zum Thema untersucht.

Die Medienberichterstattung

Eine Analyse der reichweitenstärksten deutschen Zeitungen ergab Themenkategorien wie Digitalisierung, Rechtsverfahren, Politik, Kinder- und Jugendschutz oder Kriminalität. Dabei fällt auf, dass Themenbereiche rund um Kriminalität viel nuancierter ausfallen als andere (siehe Bild) Ein Blick auf die Häufigkeit der verwendeten Worte unterstreicht diese Interpretation (deutsche Wortwolke).

Weitere Probleme betreffen die Verwendung der Terminologie. Der Begriff „Darknet" wurde von wenigen bis keinen Hintergrundinformationen zum Begriff selbst oder dessen Kontext begleitet. Vielmehr wurde der Begriff inflationär und verallgemeinernd eingesetzt. Dadurch entsteht implizit die falsche Aussage, es würde nur ein Darknet geben. Dieses eine Darknet wurde wiederkehrend mit Phrasen wie „die dunkle Seite", „der versteckte Teil" oder der „Schatten des Internets" beschrieben. Darüber hinaus zeigte sich ein wiederkehrendes Muster eines 3:1-Verhältnis von negativen und positiven Assoziationen im Zusammenhang mit dem Begriff. Negative Assoziationen sind zum Beispiel die Verfügbarkeit von Kinderpornografie, Waffen und Drogen. Zu den positiven Assoziationen gehört der Hinweis auf den möglichen Schutz der eigenen Daten, den Zugang zu freien Informationen für Menschen aus Regionen mit Zensur oder repressiven Regimen. Insgesamt zeichnet die Medienberichterstattung ein Bild, in dem das Darknet als geheimnisvoll und schwer fassbar dargestellt wird. Widersprüchlich ist, dass der Zugang als schwierig beschrieben wird; ein Ort für „Hacker und Profis". Anstatt von einem modifizierten Firefox-Browser ist von „spezieller Software" die Rede. Gleichzeitig beschreiben sie eine Bedrohung für die Öffentlichkeit auf Grund leichter Zugänglichkeit, durch die jeder „der Drogenhändler von nebenan" werden kann. Ähnlich paradox wird auch über die Rolle der Ermittlungsbehörden berichtet. Während ein Framing die Ermittlungsarbeiten und die behördliche Machtposition unterstreicht, wird gleichzeitig wiederkehrend über eine gewisse Hilflosigkeit der Behörden gegenüber technischer Anonymität berichtet. Der Technik wird eine kausale Schuld zugeschoben, indem sie als trei-

bende Kraft für negative Veränderungen in der Gesellschaft und als Bedrohung, insbesondere für Kinder, wahrgenommen wird.

Im Kontext der Forschungslandschaft

Zu beachten bleibt bei aller Kritik, dass sich Medienberichterstattung an Nachrichtenwerten orientiert. Sprich, die Berichterstattung wird bestimmt durch zeitliche Relevanz, Nähe und Informationswert. Doch wie gestaltet sich das Bild bei einem Blick in die Forschungsliteratur? Nachrichtenwerte sollten hier keine Rolle spielen. Oder etwa doch? Ein für die Wissenschaft sehr relevanter Faktor in diesem Zusammenhang stellt die Vergabe entsprechender Fördergelder für Forschungsprojekte dar. Während dies potenziell Einfluss auf etwaige Themenschwerpunkte geben kann, sollte es eine neutrale Betrachtung sowie die Präsentation der Ergebnisse nicht beeinflussen.

JÜNGSTE UNTERSUCHUNGEN ZEIGEN, DASS DIE NEGATIVE KONNOTATION DES BEGRIFFS „DARKNET“ ALLEIN ZU EINER ABLEHNUNG DER NUTZUNG FÜHRT.

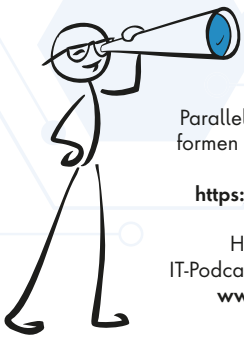
Alexandra Lux, Wissenschaftliche Mitarbeiterin, Fraunhofer-Institut SIT, promoviert an der Universität Hohenheim im Fachgebiet Medienpsychologie, www.sit.fraunhofer.de

Grundsätzlich kann man sagen, dass es sich bei Darknet-Technologien um ein Thema von internationalem Interesse handelt. Forschungsarbeiten hierzu stammen zumeist aus den Vereinigten Staaten, China sowie dem Vereinigten Königreich. Deutschland belegt Rang 6. Ein stetiger Anstieg des Interesses ist zu beobachten: Während die ersten zwei Veröffentlichungen zum Thema 2001 zu verzeichnen sind, so waren es im Jahr 2021 schon 170. Durch eine Analyse der Keywords je Jahr lässt sich eine Verschiebung beobachten. Während im Jahr 2001 „Anonymität“, „Sicherheit“ und „Privatsphäre“ die häufigsten Keywords darstellen, sind es 2019 bis 2021 „Darkweb“ und „Tor“.

Die Begriffsverwendung unterscheidet sich bei der Medienberichterstattung im Vergleich zu den wissenschaftlichen Arbeiten. Medien berichten über das „Darknet“, während bei wissenschaftlichen Arbeiten der Begriff „Darkweb“ häufiger zu finden ist. Ein möglicher Grund ist, dass in wissenschaftlichen Arbeiten Begriffe differenzierter verwendet werden. Wie schon in früheren Forschungsarbeiten konstatiert, bestätigen genauere Analysen allerdings nach wie vor das Bild, dass die Terminologie des Darknets uneinheitlich verwendet wird. Das prominenteste Beispiel betrifft hier die synonyme Verwendung der Kontexte Darknet und Darkweb sowie Deep Web. Zusätzlich werden die Zusammenhänge der Kontexte fehlerhaft erklärt und beschrieben. Einige Studien verwenden Begriffe, beschreiben aber andere. Es wird beispielsweise über das Deep Web geschrieben, inhaltlich bezieht sich die Arbeit aber auf Darkweb. Andere beschreiben das Darkweb, meinen aber Darknet oder Deep Web usw. Analog zur Medienberichterstattung führt dies unweigerlich zu Verwirrungen und Fehlinterpretation von Forschungsergebnissen.

Den Facetten des Konzepts einer Technik-Panik entsprechend, wird der Technik wiederholt eine Schuld sowie ein Bedrohungsfaktor zugeschrieben. Formulierungen, die eine enge Assoziation von Darknet und Terror, Drogen und Waffen suggerieren, finden sich nicht nur in der Medienberichterstattung wieder. In der Forschung nehmen sie mehr noch die Rolle einer Relevanzbegründung ein. Wider jegliche wissenschaftliche Norm bestehen diese Aussagen ohne weitere Referenzen. Wiederkehrend ist außerdem der Verweis auf eine Studie zu lesen, die herausfand, dass 2 Prozent der Darknet-Seiten einem kinderpornografischen Kontext zuzuordnen sind, jedoch 80 Prozent des Traffics auf diese zwei Prozent der Seiten laufen. Dieses Ergebnis wurde Jahre später in einer weiteren Studie durch eine laufende Ermittlung des FBI auf Seiten entsprechenden Typs erklärt und revidiert. Die alternative Erklärung des früheren Ergebnisses erlebt jedoch bisher nicht annähernd so viel Prominenz wie das ursprüngliche Ergebnis.

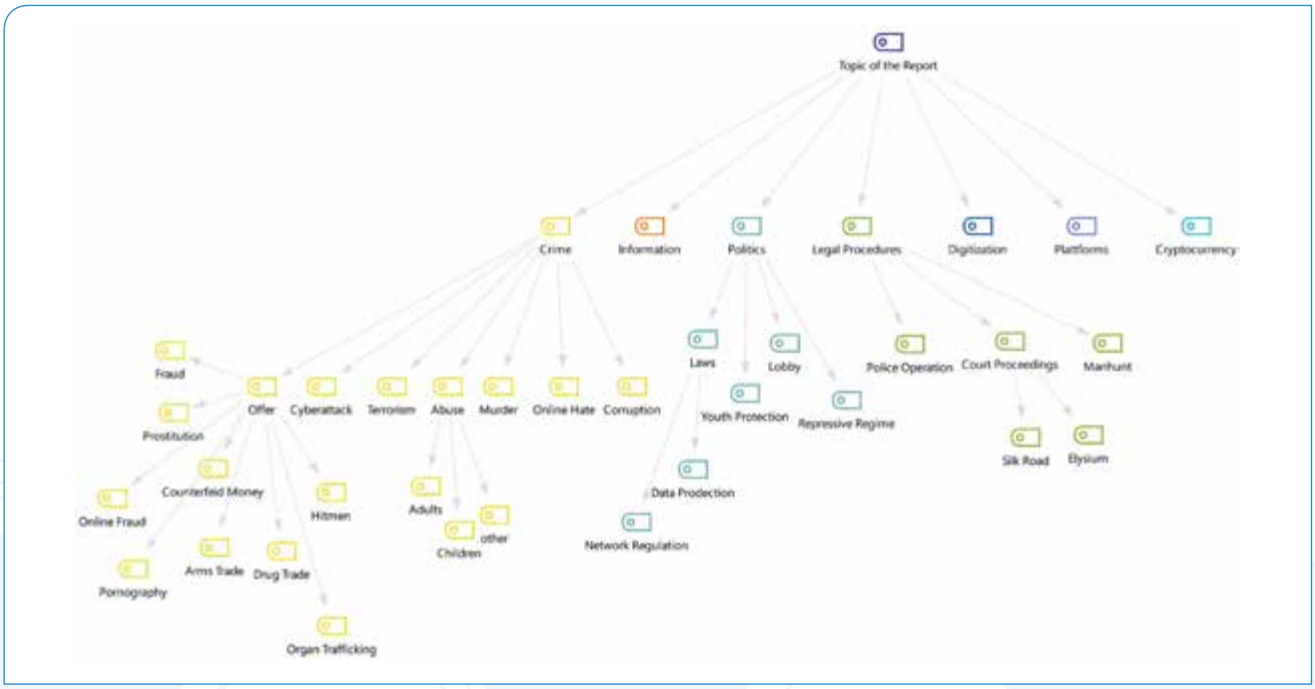
Weitere Probleme und Inkonsistenzen im Kontext der Darknet-Forschung lassen sich unter anderem durch verschiedene methodische Herangehensweisen, die im späteren Forschungsprozess nicht adäquat reflektiert werden, aufklären. Wie zum Beispiel der Umgang mit der Kurzlebigkeit der Services, der Interpretation von Duplikaten von Darknet-Seiten sowie Botnetzen spielt eine tragende Rolle.



MEHR WERT

Parallelstrukturen, Aktivitätsformen und Nutzerverhalten im Darknet (PANDA)
https://panda-projekt.de/

House of Nerds – den IT-Podcast des Fraunhofer SIT
www.sit.fraunhofer.de/houseofnerds/



Darknet-Technologien – eine andere Perspektive

Extreme Forschungsergebnisse sollten adäquat reflektiert und kritisch hinterfragt werden. Auch wenn die Ergebnisse der Erwartungshaltung entsprechen und sich mit der Medienberichterstattung decken. Viel zu selten wird allein auf die Möglichkeit eines finanziellen Betrugs bei fragwürdigen Angeboten hingewiesen. Insbesondere für den Waffenhandel konnte dies im Rahmen von Ermittlungsverfahren mehrfach festgestellt werden. Festhalten lässt sich, dass wir im Tor-Netzwerk keinen Typ von Kriminalität finden, den wir nicht auch an anderer Stelle der Gesellschaft finden oder der dort überproportional ausgeprägt ist. Ausgenommen von jeglicher Relativierung ist der Bereich der Kinderpornografie.

Vor dem Hintergrund der Bedenken rund um die eigene Privatheit ist es nicht nachvollziehbar, warum vorhandene Technologien nicht zumindest im Rahmen des anonymen Surfens im Clearnet mehr zum Einsatz kommen. Umso dissonanter, dass die Verwendung von VPN vergleichsweise weit verbreitet ist. Obwohl es hier neben dem Vertrauen in den Anbieter, dem gegenüber keine Anonymität besteht, auch oft der Bezahlung des Services bedarf. Jüngste Untersuchungen zeigen, dass die negative Konnotation des Begriffs „Darknet" allein zu einer Ablehnung der Nutzung führt. Wird die Tor-Technologie dagegen als eine Privacy Enhancing Technology präsentiert, ist die Bereitschaft, diese zu nutzen, wesentlich höher.

Wichtig bleibt zu unterstreichen, dass an dieser Stelle nicht das Vorhandensein von Kriminalität im „Darknet" grundsätzlich in Frage gestellt wird. Vielmehr geht es um einen Appell für eine ausgewogenere Berichterstattung und Betrachtung. Dies betrifft insbesondere das relative Aufkommen von Phänomenen. Nehmen wir hier beispielsweise den Drogenhandel, eines der am häufigsten beleuchteten Phänomene in der untersuchten medialen Berichterstattung sowie in der Forschung. In Relation zum Weltmarkt ist der Anteil des Drogenhandels im „Darknet" weniger als 0,1 Prozent (Europol, 2019). Dieser Markt kann außerdem zur Schadensminimierung führen, da Foren als Austauschplattform für Erfahrungsberichte zur Qualität dienen. Nicht zuletzt trägt dies auch zu einer Reduktion der Kriminalität, die mit dem Drogenhandel auf der Straße im Zusammenhang stehen, bei.

Alexandra Lux

Modulare Architektur einer KI-gestützten Datensicherheitsplattform

WIE KÖNNTE SIE AUSSEHEN?

Die KI kommt immer mehr auch in der IT-Security zum Einsatz. Velotix hat jetzt eine dreistufige Plattform mit einem stufenweisen Ansatz für automatisierte Data Governance vorgestellt.

Es beginnt mit der Datenerkennung und dem Auto-Tagging und entwickelt sich dann zu einem KI-gestützten Datenzugriff und einer automatischen Richtliniengenerierung weiter. Der stufenweise Ansatz ermöglicht es Unternehmen, die Vorteile der Automatisierung schneller zu nutzen und den regelkonformen Zugriff auf Daten mit minimalem Risiko zu kontrollieren.

Den Überblick behalten

Aufgrund des exponentiellen Datenwachstums und der heutigen sich schnell ändernden Datensicherheitsvorschriften stehen viele Unternehmen vor der Herausforderung, den Überblick darüber zu behalten, welche Daten verfügbar sind, wo sie sich befinden und wer Zugriff darauf haben sollte. Die meisten Unternehmen sind sich der Notwendigkeit der Automatisierung bewusst, um Daten leicht verfügbar zu machen und gleichzeitig die Vorschriften einzuhalten, sind jedoch nicht immer bereit, eine umfassende Datensicherheitsplattform zu implementieren. Stattdessen können sie mit dem neuen, modularen Ansatz spezifische Funktionen nutzen, die ihrem aktuellen Bereitschaftsgrad entsprechen.

Die Datensicherheitsplattform von Velotix umfasst derzeit die drei folgenden Module:

Data Discovery & Auto-Tagging

In vielen Unternehmen sind die Daten über Datenbanken, Data Warehouses und Data Lakes in verschiedenen Regionen verteilt, was eine aktuelle Bestandsaufnahme von Daten und Berechtigungen extrem schwierig macht. Das Datenerkennungsmodul kennzeichnet automatisch Daten und Metadaten, die aus bestehenden Datenbanken importiert werden, um ein einziges Repository für den Zugriff auf Informationen und die Erteilung und den Entzug von Berechtigungen zu schaffen. Datenklassifizierungsalgorithmen werden kontinuierlich angewendet, um sensible Daten zu erkennen und ein laufend aktualisiertes Dateninventar zu erstellen.

Access Management Powered by AI

Bietet die Möglichkeit, automatisch fein abgestufte Richtlinien auf Attributsebene für Einzelpersonen, Gruppen und Benutzer zu erstellen, um die rollenbasierte Zugriffsmethode zu ersetzen, die manuelle Eingaben und einen hohen Wartungsaufwand erfordert und anfällig für menschliche Fehler sein kann. KI

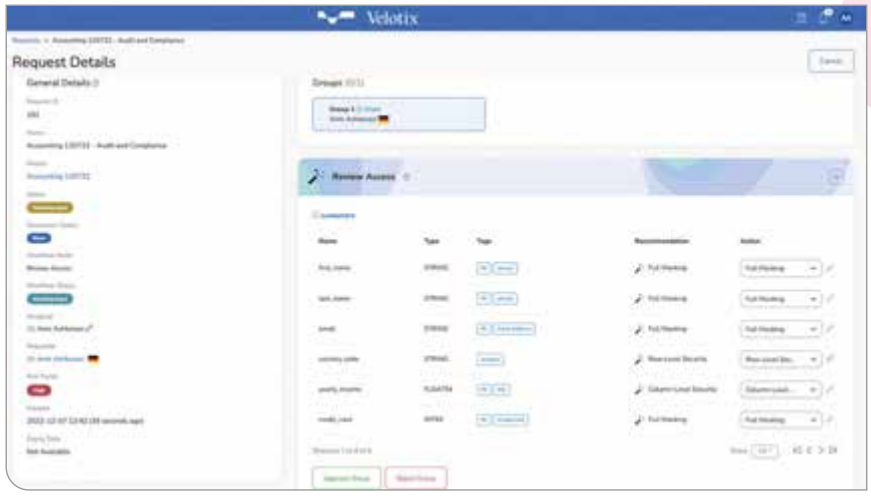
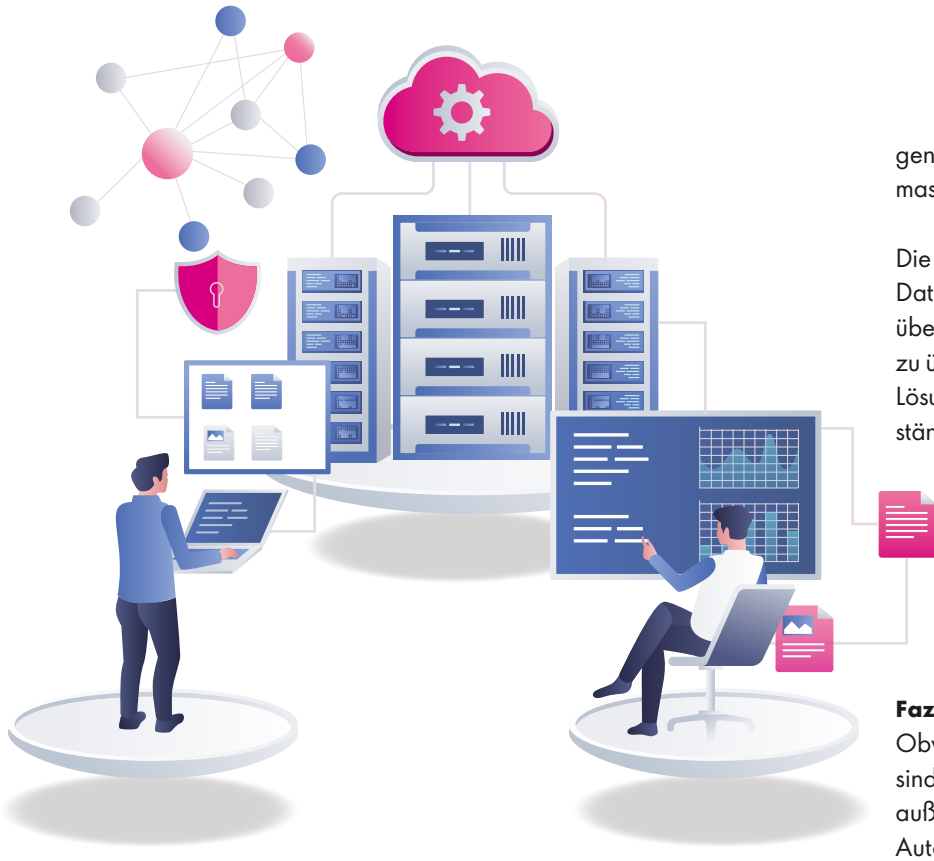


Bild 1: Anwendungsfall für die automatisierte Verwaltung von Richtlinien – Unternehmen tun sich schwer damit, eine zentrale, einzige Quelle über Unternehmensregeln und externe Richtlinien wie GDPR, HIPAA oder CCPA zu schaffen. Velotix implementiert ein automatisiertes Richtlinienmanagement, das die fehleranfällige und zeitaufwändige Arbeit der Erstellung neuer Regeln für neue Datenrichtlinien überflüssig macht und ein Regelwerk erstellt, das sicherstellt, dass Sie und Ihr Unternehmen unter Einhaltung der Regeln auf Daten zugreifen.

Quelle: www.velotix.com



wird eingesetzt, um widersprüchliche Berechtigungen automatisch zu identifizieren und Lösungen zu empfehlen.

Policy Database Management

Ermöglicht Unternehmen die Erstellung und Pflege ihrer Datenschutzrichtlinien. Der dynamische Workflow-Builder und die KI-gesteuerte Richtlinien-Engine aggregieren Datenkataloge und passen die Richtlinien mithilfe von maschinellem Lernen an, um die richtige Datenrichtlinie zu erstellen und zu pflegen. Der Richtlinienkatalog versteht die Feinheiten von Datenschutzbestimmungen wie GDPR, HIPAA und CCPA, um optimale Autorisierungsstrategien zu entwickeln.

Die integrierte Plattform bietet ein einziges Dashboard zur Verwaltung von Datenerkennung und -klassifizierung, Überwachung von Datenaktivitäten, Datenrisikoanalyse, Erkennung von Bedrohungen, Datenzugriffskontrolle und Datenmaskierung sowie sofortige Audits.

Die Erkennung und Kennzeichnung von Daten ist unerlässlich, um die Kontrolle über den Lebenszyklus des Datenzugriffs zu übernehmen, so das Credo der neuen Lösung. Unternehmen brauchen ein vollständiges Inventar seiner Datenbestände und eine modulare Architektur ermöglicht es Unternehmen, den ersten Schritt zu tun, bevor sie KI nutzen, um ihr Berechtigungsmanagement auf die nächste Stufe zu bringen.

Fazit

Obwohl sich Unternehmen bewusst sind, dass der heutige Daten-Tsunami außer Kontrolle gerät und dass sie eine Automatisierung benötigen, um Berechtigungen besser zu verwalten, kann die Implementierung einer umfassenden Lösung unpraktisch sein, so das Unternehmen. Ziel sei es, verschiedene Phasen der Datendemokratisierung mit schnellerem Nutzen anzubieten, so dass Unternehmen in einem für sie angemessenen Tempo vorankommen können, während sie Daten für Benutzer, Anwendungen und Algorithmen besser verfügbar machen.

Ulrich Parthier

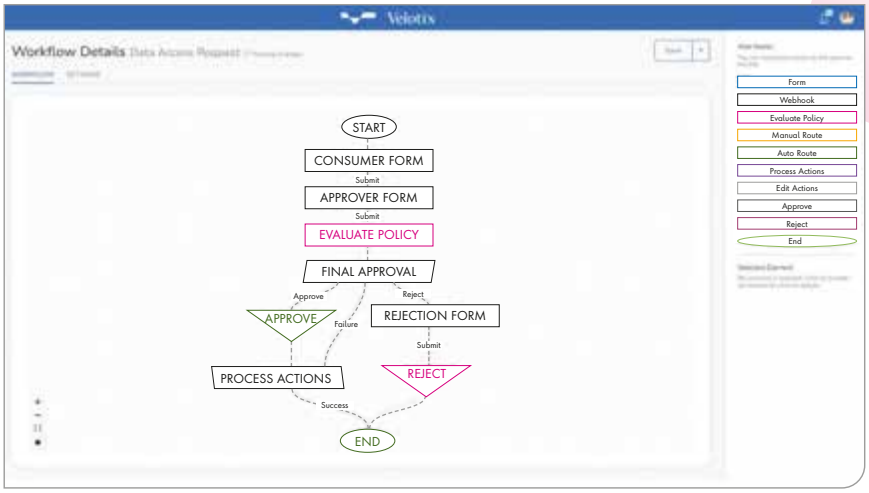


Bild 2: Anwendungsfall Datenzugriff – Datenzugriff in Echtzeit bedeutet, dass Unternehmen keine Zeit mehr damit verschwenden, auf die Genehmigung von Anfragen zu warten. Die Datenschutzplattform von Velotix bietet einen kontrollierten, föderierten und virtualisierten Zugriff auf Daten, ohne dass die Daten verschoben, repliziert oder umgewandelt werden müssen.

Quelle: www.velotix.com

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:
Valentin Boussin, Stefano Chierici, Michael Feygelman, Florian Goldenstein, Alexander Häußler, Dr. Niklas Hellemann, Thomas Janz, Sabine Kuch, Alexandra Lux, Nils Meyer, Carina Mitzschke, Olaf Müller-Haberland, Silvia Parthier, Ulrich Parthier, Michael Veit, Jörg von der Heydt, Jelle Wieringa

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

Head of Marketing:
Vicky Miridakis, 08104-6494-15,
miridakis@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.

Diversifizierte Angriffsmethoden

BEDROHUNGSAKTEURE KAPERN CHROME-BROWSER

Durch die Isolierung von Bedrohungen, die nicht von entsprechenden Tools auf PCs erkannt wurden, hat HP Wolf Security einen spezifischen Einblick in die neuesten Techniken, die Cyber-Kriminelle in der sich schnell verändernden Cyberkriminalitätslandschaft einsetzen.

- Die Chrome-Erweiterung „Shampoo" verbreitet die Chrome-Loader-Malware und bringt Anwender dazu, eine bösartige Chrome-Erweiterung zu installieren. Diese leitet die Suchanfragen des Opfers auf bösartige Websites oder Seiten um, mit denen die kriminelle Gruppe durch Werbekampagnen Geld verdient. Die Malware ist sehr hartnäckig und nutzt den Task Scheduler, um sich alle 50 Minuten neu zu starten.

- Obwohl Makros aus nicht vertrauenswürdigen Quellen mittlerweile deaktiviert sind, beobachtete HP, dass Angreifer diese Kontrollen umgehen. Sie kompromittieren ein vertrauenswürdiges Office 365-Konto, richten eine neue Firmen-E-Mail ein und verteilen eine bösartige Excel-Datei, die die Opfer mit dem Infostealer Formbook infiziert.

- OneNote-Dokumente können als digitale Sammelalben fungieren, an die sich jede beliebige Datei anhängen lässt. Angreifer machen sich dies zunutze, um bösartige Dateien hinter gefälschten „Hier klicken"-Symbolen einzubetten. Durch einen Klick auf das gefälschte Symbol wird die versteckte Datei geöffnet und Malware ausgeführt. Damit erhalten Angreifer Zugriff auf den Computer des Anwenders.

Gruppen wie Qakbot und IcedID betteten im Januar erstmals Malware in OneNote-Dateien ein. OneNote-Kits sind mittlerweile auf Cybercrime-Marktplätzen erhältlich. Sie erfordern nur geringe technische Kenntnisse – daher wird in den kommenden Monaten weiterhin mit diesen Malware-Kampagnen zu rechnen sein.

Der Bericht zeigt auch, dass Cyber-Kriminelle ihre Angriffsmethoden weiter diversifizieren – die Palette reicht dazu von bösartigen Archivdateien bis hin zum HTML-Schmuggel. Ihr Ziel ist es, E-Mail-Gateways zu umgehen. Der Grund: Bedrohungsakteure wenden sich von Office-Formaten ab.

www.hp.com


itsa EXPO CONGRESS
PLAY HARD.
PROTECT SMART.
HOME OF IT SECURITY
JETZT GRATIS-TICKET SICHERN!
10. – 12. Oktober 2023
Nürnberg, Germany
itsa365.de/itsa-expo-besuchen
NÜRNBERG MESSE