it management

Der Motor für Innovation
Januar/Februar 2024

INKLUSIVE 48 SEITEN
it security

THOUGHT LEADERSHIP
AB SEITE 16
appian

DIGITALISIERUNG

Der Weg zu effizienten Workflows

Dietmar Nick, KYOCERA Document Solutions Deutschland GmbH

DATA ANALYTICS

Einfach, schnell und sicher

SAP DATASPHERE

Das Warehouse der Zukunft?

KOSTENFALLE CLOUD

Ein vermeidbares Problem

A leader is one who knows the way, goes the way, and shows the way.

John C. Maxwell

THOUGHT LEADERSHIP

2024 – HAUPTSACHE KI?

LIEBE LESERINNEN UND LESER,

Willkommen im Jahr 2024, einem Jahr, das von vielen Seiten erneut als das Jahr der KI betitelt wird. Künstliche Intelligenz weckt bei Führungskräften leuchtende Augen mit Versprechungen von gesteigerter Effizienz oder gar Personalreduktion. Wenn ich mit KI-Experten spreche, zeigt sich ein wiederkehrendes Muster: Kunden, die mit dem Wunsch an sie herantreten, „irgendetwas mit KI" zu machen, oft ohne ein konkretes Ziel dahinter.

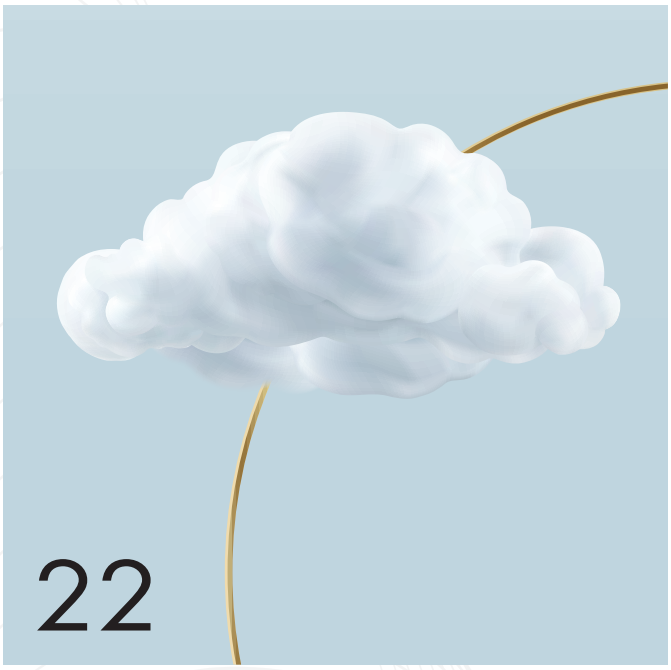
Kein Zweifel, die Künstliche Intelligenz wird ihrem Hype gerecht und die Art und Weise, wie wir arbeiten, wird sie grundlegend verändern oder hat sie an vielen Stellen bereits maßgeblich getan. Manchmal scheint es aber so, als ob KI das neue „Abrakadabra" der Geschäftswelt sei – ein magisches Wort, das alle Probleme löst.

Doch es ist wichtig, KI nicht nur um ihrer selbst willen einzusetzen, sondern ihren funktionalen Nutzen zu betonen. Dieses Jahr sollten wir deshalb KI als ein Tool sehen, das gezielt eingesetzt wird, um echte Herausforderungen zu bewältigen und Prozesse zu optimieren. Es geht also nicht um den Einsatz von Technologie als Selbstzweck, sondern um ihre intelligente Anwendung.

KI kann vieles, aber die Kunst, sie sinnvoll einzusetzen, bleibt eine menschliche Disziplin.

Herzlichst

Lars Becker | Redakteur



INHALT

COVERSTORY

10 **Der Weg zu effizienten Workflows**
Digitalisierungsschritte nicht auf die lange Bank schieben

12 **Digitalisierung ohne Schmerz**
Der einfache Weg zum digitalen Schreibtisch

THOUGHT LEADERSHIP

16 **Keeping the core clean**
Den Standard für ERP-Systeme behalten und trotzdem flexibel agieren

Farblich hervorgehobene Artikel sind von der Redaktion als besonders lesenswert empfohlen

IT MANAGEMENT

18 **Pay-per-Use**
Gebrauchsabhängige Finanzierung von Sondermaschinen

21 **LLMs im ERP-Kontext**
Mehr Struktur, bitte!

22 **Gefangen in der Microsoft-Cloud?**
Ein Befreiungs-Tipp

24 **Kostenfalle Cloud**
Die Vorteile einer umfassenden IT-Management-Lösung

26 **IT Service Management**
Die Wartungsplanung integrieren

28 **IT Service Management 2024**
Die acht wichtigsten Trends

30 **IT-Organisation 2025**
IT und Business verschmelzen zunehmend

33 **UC-Tools für Digital Workplaces**
Unified-Communications-Lösungen für den „Arbeitsplatz der Zukunft“

34 **Digitalisierungs-Booster**
Keine Digitalisierung ohne Unified Communications

36 **Kleiner Schritt, große Wirkung**
Office 4.0 dank SAP-Schnittstellen

38 Effektives SAP-Management
Datengetriebene Prozesse für Sicherheit und Lizenzen

42 Neujustierung erforderlich
SAP erkennt die Schlüsselrolle von KI und optimiert sein Portfolio

44 SAP Datasphere
Das Cloud Data Warehouse der Zukunft?

48 Transformationsstudie 2023
Mangelnde Datenhygiene gefährdet Transformationserfolge

50 Integrierter Ansatz für die digitale Transformation
Vom Wandel der Unternehmens-Digitalisierungsprojekte

54 KI in Finanzabteilungen
Ist künstliche Intelligenz der nächste große Renner?

56 Testdaten-Management (Teil 1 von 5)
Synthetische und referentiell korrekte Testdaten erstellen

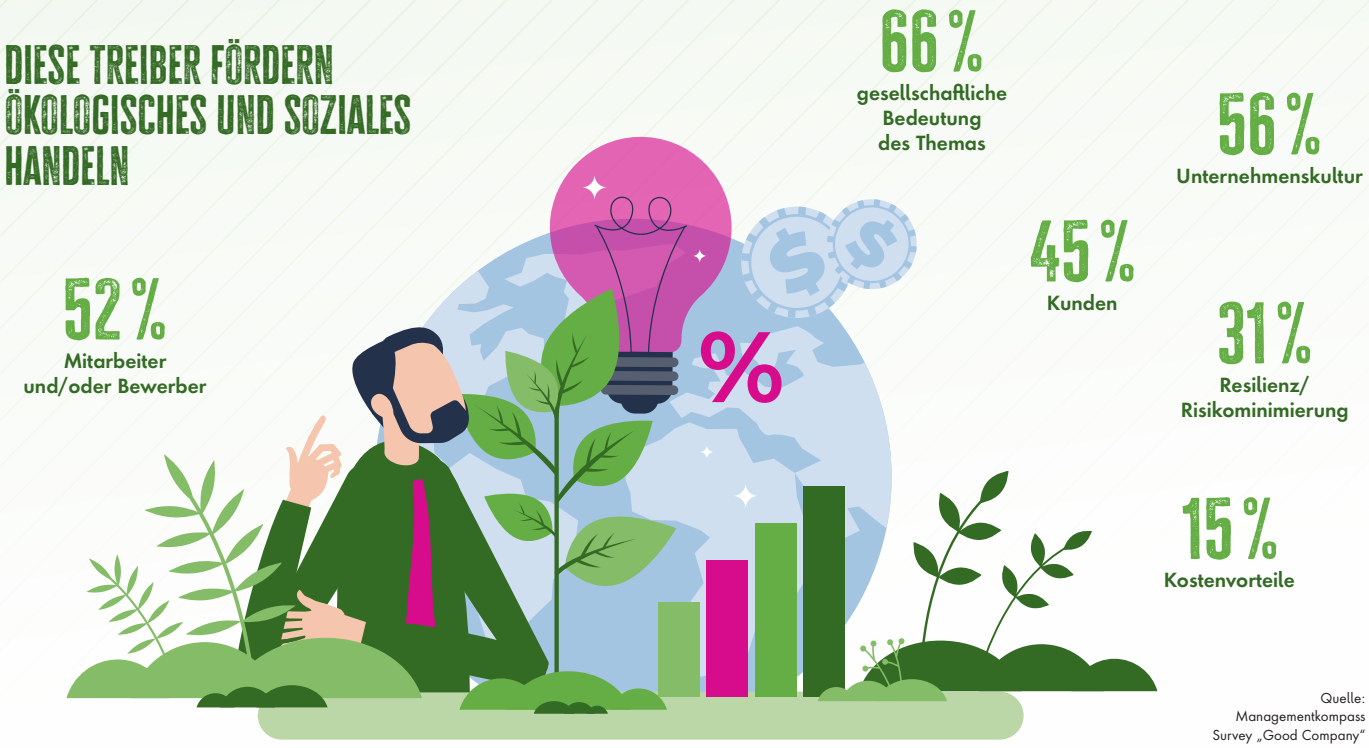
60 Data Automation
Einfach, schnell und sicher zur Data-Analytics-Lösung

52 Potenziale freisetzen
Die Macht der IT-Unternehmensarchitektur

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**



Quelle: Managementkompass Survey „Good Company"

NACHHALTIGKEIT IN UNTERNEHMEN

ZWEI DRITTEL REAGIEREN AUF DRUCK VON AUSSEN

Wirtschaft und öffentliche Verwaltung lassen sich bei ESG-Maßnahmen vorrangig von externen Faktoren treiben. 66 Prozent der Unternehmen und Behörden in Deutschland investieren in Ethik und Nachhaltigkeit vorrangig aufgrund gesellschaftlicher Entwicklungen. Jede zweite Organisation will attraktiver für Fachkräfte werden, 45 Prozent reagieren auf Kundenerwartungen. Intrinsische Motive wie im Geschäftsmodell verankerte Werte sind seltener Treiber für Nachhaltigkeitsaktivitäten. Sie gewinnen allerdings an Bedeutung. Das zeigt die Studie Managementkompass Survey Good Company von Sopra Steria. Für die Befragung von 371 Entscheiderinnen und Entscheidern wurden regulatorische Vorgaben als Antriebsfaktoren bewusst ausgeklammert.

Ökologische, soziale und unternehmensethische Prinzipien (ESG) gewinnen an Bedeutung für Unternehmen und Verwaltung – auch abseits von Regulierungsvorschriften wie dem AI Act und dem Lieferkettensorgfaltspflichtengesetz. Für 60 Prozent der Unternehmen und Behörden sind ethische Prinzipien für strategische Entscheidungen heute wichtiger als vor zehn Jahren. Ein Paradigmenwechsel im Managementhandeln ist allerdings nicht in Sicht: Nur 37 Prozent der Befragten sehen eine grundlegende Neuausrichtung der Unternehmenssteuerung und eine Orientierung an Langfristzielen. Dazu zählen beispielsweise langfristige Partnerschaften mit Lieferanten und das bewusste Zahlen höherer Einkaufspreise, um die Kaufkraft in Zukunftsmärkten zu steigern.

Die Studienergebnisse deuten auf einen gewissen Bewusstseinswandel hin. 56 Prozent der Befragten sehen einen positiven Effekt nachhaltigen Handelns auf Umsatz und Gewinn. Die Unterstützer dieser These haben jedoch die Erkenntnis oft noch nicht in ihrer Organisation umgesetzt. Nur 15 Prozent der Befragten treiben signifikante Kostenvorteile an, wenn sie in ökologische, sozial oder unternehmerische Nachhaltigkeit investieren. Zehn Prozent handeln nachhaltig, weil eine „Good Company"-Strategie Unternehmen und Verwaltungen produktiver macht, so die Studie.

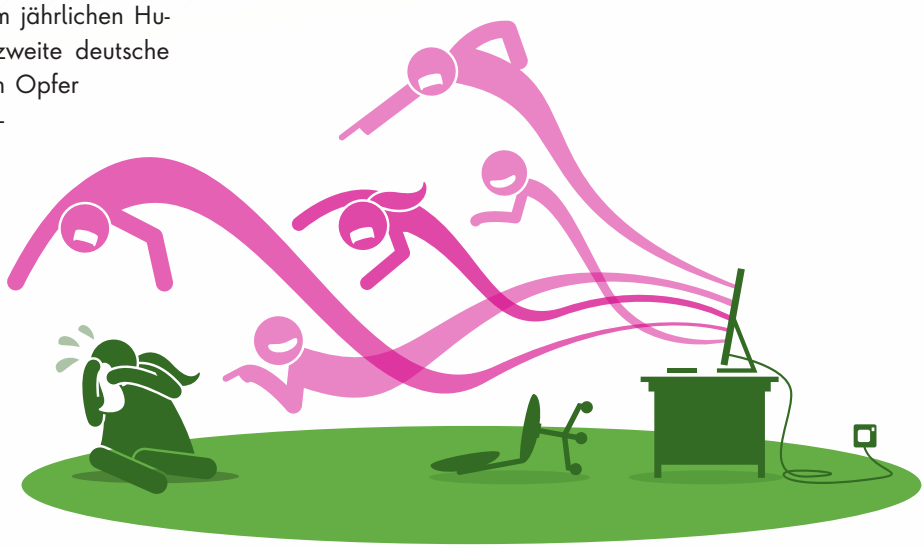
Good-Company-Geschäftsmodelle sind so konzipiert, dass durch verantwortungsvolles Handeln ein geschäftlicher Mehrwert entsteht und nicht trotz dieses Handelns. Dafür ist es wichtig, die Folgekosten eines weniger tugendhaften Verhaltens zu internalisieren oder positiv ausgedrückt: Es geht darum „gute Prinzipien" in betriebswirtschaftliche Erfolgskennzahlen zu übersetzen.

www.soprasteria.de

Cybercrime Trends 2024

DAS JAHR VON HACKTIVISMUS UND DISINFORMATION-AS-A-SERVICE

In der heutigen Zeit verschärft sich die Bedrohungslage für deutsche Unternehmen stetig. So wurde nach dem jährlichen Human Risk Review Report von SoSafe jedes zweite deutsche Unternehmen in den vergangenen drei Jahren Opfer eines Cyberangriffs (58 %). Um dieser Entwicklung entgegenzuwirken, zeigen die folgenden Trends, worauf sich Unternehmen im kommenden Jahr besonders gut vorbereiten müssen.



#1 Die Auswirkungen von generativer KI auf die Cybersicherheit werden sich erst noch zeigen.

#2 Der Trend zum Hacktivismus gewinnt in einer zunehmend fragmentierten Welt an Bedeutung.

#3 Disinformation-as-a-Service wird zu einem mächtigen Werkzeug zur Destabilisierung von Organisationen.

#4 Sicherheitsteams stehen mehr denn je unter Druck.

#5 Den öffentlichen Sektor erwarten große Herausforderungen.

#6 Der menschliche Faktor wird eine immer größere Rolle spielen.

https://sosafe-awareness.com/de

Top oder Flop?

WHATSAPP ALS MARKETINGKANAL

Dort kommunizieren, wo die Verbraucher bereits sind, gilt seit jeher als eines der wichtigsten Erfolgsrezepte im Marketing. Und doch bleibt oft vielerorts ein Kanal außen vor, der allein in Deutschland Millionen von Nutzern hat und als der beliebteste Online-Kommunikationsdienst gilt: WhatsApp.

Während Elon Musik mit X weiter herumexperimentiert, um irgendwann eine „Super App" zu schaffen, ist Konkurrent Mark Zuckerberg mit dem Instant Messenger WhatsApp inzwischen einen deutlichen Schritt weiter. Zuletzt stellte die Meta-Tochter nämlich mehrere Neuerungen vor, die nicht nur den Funktionsumfang für Unternehmen und Nutzer maßgeblich erweitern, sondern die App auch noch stärker in den Alltag integrieren soll.

WhatsApp soll zum Alleskönner werden

So können Nutzer nun sogenannten Kanälen folgen, die von Organisationen mit Inhalten gefüllt werden, und sich – wenn gewünscht – sogar per Push-Nachrichten über Neuigkeiten informieren lassen. Dies bietet für Unternehmen neue Möglichkeiten, Informationen schnell und einfach an eine größere Zielgruppe auszuspielen, die aktiv solche Informationen wünscht.

Darüber hinaus können Brands es ihren Kunden mithilfe von „Flows" ermöglichen, direkt über den Messenger Bestellungen zu tätigen, Formulare auszufüllen oder Termine zu buchen. Dadurch schaffen Unternehmen kurze Wege und senken die Wahrscheinlichkeit, dass Käufe abgebrochen werden.

Es geht um eine stimmige Kundenansprache

Unternehmen sollten jetzt allerdings nicht kurzerhand haufenweise WhatsApp-Kanäle eröffnen, Marketing Messages schreiben und Flows erstellen. Wie bei jedem anderen Marketingkanal braucht es auch hier ein überlegtes Vorgehen, das zur restlichen Strategie und Kundenkommunikation passt. Denn Kunden sind aufmerksam und merken schnell, wenn Marken nicht authentisch sind.

Wie aber sollten Unternehmen dann bei der Integration der neuen WhatsApp-Funktionen vorgehen? Zunächst muss betrachtet werden, was sie in diesem Bereich – nämlich Conversational Marketing – bereits machen, wie erfolgreich sie dabei sind und inwieweit die Bedürfnisse der Kunden dabei noch nicht abgedeckt werden. Im nächsten Schritt kann dann strategisch geplant werden, wie und ob die neuen Features von WhatsApp eingesetzt werden sollen. Beispielsweise können die neuen Marketing Messages den Unternehmen die Kundenansprache erleichtern und gleichzeitig, durch eine personalisierte Anrede, die Distanz in der Kundenkommunikation verringern.

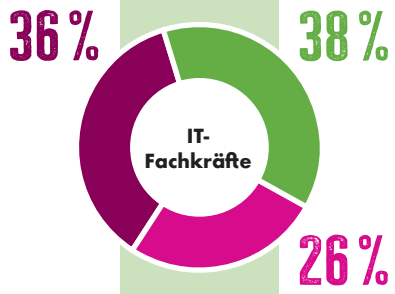
Allerdings sollten auch die Grenzen der neuen Funktionen nicht außer Acht gelassen werden. Denn bei den WhatsApp Channels handelt es sich schließlich um einen Broadcast-Channel, der nicht immer end-to-end verschlüsselt ist. Es darf also nicht voreilig gehandelt werden, sondern Unternehmen müssen wohl überlegt vorgehen und dabei ihre Datenschutzbestimmungen nicht vernachlässigen. Um auf Nummer sicher zu gehen und die Vorteile des Conversational Marketing, der Automatisierung und der Personalisierung voll auszuschöpfen, sollten Unternehmen eher auf Business Provider Lösungen zurückgreifen.

Ebenso gilt es zu beachten, dass die neuen Funktionen von WhatsApp als nützliche Tools konzipiert sind, um Marketer zu unterstützen - jedoch nicht um sie zu ersetzen. Der Schlüssel zum Erfolg ist also die Zusammenarbeit zwischen Experten, die sich auf die Erstellung origineller Inhalte und dem Management von Kunden-Chats spezialisiert haben, und modernen Tools, die punktuell den Arbeitsalltag erleichtern können.

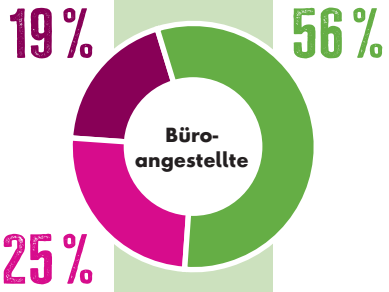
www.brevo.com

ARBEITSPLATZVERLUST DURCH KI?

DIE SKEPSIS BLEIBT



Wie besorgt sind Sie darüber, dass KI-Tools in den nächsten fünf Jahren Ihren Arbeitsplatz übernehmen könnten?



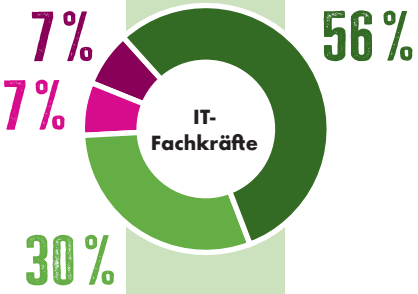
- geringfügig oder überhaupt nicht besorgt
- teilweise besorgt
- sehr besorgt

Ivanti hat die Ergebnisse seiner Studie „Getting Employees on Board for the AI Revolution" veröffentlicht. Die Studie zeigt, dass Unternehmen die Einführung von KI vorantreiben, Arbeitnehmende aber noch skeptisch sind, was die Potenziale von KI betrifft. Allerdings: Nur wenn Mitarbeitende und Unternehmen auf einer Linie sind, entfaltet KI ihre Möglichkeiten.

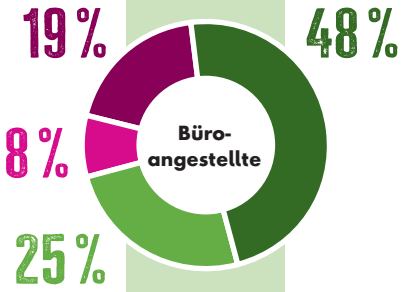
www.ivanti.com

MEHR WERT

Studie: Mitarbeitende für die KI-Revolution gewinnen



Glauben Sie, dass zukünftig vor allem Arbeitgeber oder Arbeitnehmende von KI-Tools profitieren?



- Arbeitgeber profitieren
- Arbeitgeber und -nehmer profitieren gleichermaßen
- Arbeitnehmende profitieren
- Unsicher

Der Weg zu effizienten Workflows

DIGITALISIERUNGSSCHRITTE NICHT AUF DIE LANGE BANK SCHIEBEN

Unternehmen müssen im 21. Jahrhundert auf digitale Lösungen und umweltfreundliche Technologien setzen, um erfolgreich zu sein. Davon ist Dietmar Nick, CEO von Kyocera Document Solutions Deutschland, im Gespräch mit Ulrich Parthier, Herausgeber it management, überzeugt.

Ulrich Parthier: *Während Homeoffice vor der Pandemie eher die Ausnahme war, ist es heute vielerorts fest etabliert. Heimarbeit bedeutet aber auch, dass viele Abläufe überdacht werden müssen. Wie beeinflusst sie das Informations- und Dokumentenmanagement?*

Dietmar Nick: Keine Frage, das Homeoffice ist in vielen Unternehmen und für viele Mitarbeitende zur Normalität geworden. Fest steht: Die IT gibt das heute her – technisch sind alle Anforderungen umsetzbar. Geklärt werden muss vorrangig, wie die Homeoffice-Anbindung tatsächlich sicher gestaltet werden kann. Und, richtig, Abläufe müssen neu überdacht werden. Dazu gehört, dass man Geschäftsprozesse ortsunabhängig denkt und plant. Dabei kommt uns allen entgegen, dass zu bearbeitende Dokumente in den Unternehmen heute immer digitaler werden – im Idealfall durchgängig ohne Brüche vom Posteingang bis zur Archivierung. Wenn im Homeoffice doch noch Papierausdrucke notwendig sind, dann muss geklärt werden, wie Druckertoner und Papier zuverlässig nach Hause kommen. Aber das sind definitiv lösbare Aufgaben.

> DAS NACHHALTIGSTE DOKUMENT IST DAS, WELCHES NICHT GEDRUCKT WIRD.
>
> **Dietmar Nick, CEO,**
> **Kyocera Document Solutions Deutschland GmbH,**
> **www.kyoceradocumentsolutions.de**

Ulrich Parthier: *Wie können Unternehmen ihre digitale Transformation beschleunigen? Was ist eine sinnvolle Vorgehensweise, damit ein solches Vorhaben gelingt? Was sind geeignete erste Schritte?*

Dietmar Nick: Am Anfang sollten sich die Verantwortlichen die Frage stellen, wo ihr Unternehmen künftig stehen soll. Ohne ein Ziel vor Augen ist es schwierig, in Sachen digitale Transformation einen klaren Kurs zu steuern oder gar zu beschleunigen. Eine wichtige Frage ist, wie ortsflexibel das Unternehmen und die Mitarbeitenden heute sind und in Zukunft sein sollen. Hiernach sollte geklärt werden, wie ich die IT-Infrastruktur entsprechend meiner Ziele aufbaue. Grundsätzlich sollten wir angesichts des globalen Wettbewerbs weitere Digitalisierungsschritte zeitnah einführen und nicht auf die lange Bank schieben. Ein idealer Ansatzpunkt ist dafür bei den meisten Betrieben der Posteingangsprozess. Daraus ergibt sich der Aufbau eines digitalen Dokumentenmanagements. Soll das Vorhaben nicht einfach durchgeboxt werden, sondern wirklich von den Mitarbeitenden genutzt und somit zum Erfolg werden, dann ist es unabdingbar, vor irgendwelchen Beschlüssen das Team transparent zu informieren, es abzuholen und mitzunehmen. Ich erlebe es immer wieder, dass Mitarbeitende vor solchen Schritten regelrecht Angst haben und befürchten, Aufgaben nicht mehr bewältigen zu können oder ihren Job zu verlieren. Beides ist nicht der Fall. Aber Angst kann ganze Belegschaften lähmen und einen Digitalisierungsprozess torpedieren. Das sollte unbedingt vermieden werden.

? **Ulrich Parthier:** *Neue Technik allein reicht häufig nicht aus. Sie sagen selbst: Die Mitarbeitenden müssen „mitgenommen" werden, der ganze Workflow verändert sich. Viele Unternehmen können das kaum allein bewältigen. Wo erhalten Unternehmen Unterstützung bei ihrer Transformation, an wen können sie sich wenden?*

Dietmar Nick: Änderungen technisch sicher zu stellen und umzusetzen ist eines. Unsere Fachhandelspartner sind heute aber weitaus breiter aufgestellt. Sie bieten Lösungen an, kennen die Anforderungen vieler Branchen und sie wissen durch langjährige Erfahrung auch, wo in vielen Unternehmen der Schuh drückt. Sie sind außerdem sehr regional aufgestellt, sind schnell vor Ort und sprechen die Sprache ihrer Kunden. Als Partnernetzwerk können sie auch überregional oder bundesweit aufgestellte Unternehmen beraten und betreuen. Sie verfügen durch ihre Ausbildung und kontinuierliche Schulungen über sehr viel Know-how und haben im Zweifelsfall auch schon in ähnlichen Betrieben Neuerungen begleitet. Unsere Partner sind deshalb heute in der Lage, Unternehmen ganzheitlich zu begleiten und weit über die eigentliche Technik hinaus zu unterstützen. Darüber hinaus bieten wir selbst online viele Informationen, die den Einstieg in die Digitalisierung erleichtern.

? **Ulrich Parthier:** *Kyocera engagiert sich stark im Bereich Nachhaltigkeit. Wie können Unternehmen ihren Arbeitsalltag und ihre Prozesse nachhaltiger gestalten und wo fängt man da am besten an?*

Dietmar Nick: Nachhaltigkeit ist in der Tat ein großes Thema, das von Kyocera seit der Unternehmensgründung im Jahr 1959 sehr ernst genommen wird. Als Ergebnis nutzen wir heute in unseren Hauptproduktionsstätten ausschließlich erneuerbare Energien. Für unsere Kunden gilt mit Blick auf den Bereich Dokumentenlösungen: Das nachhaltigste Dokument ist das, welches nicht gedruckt wird. Unternehmen sollten ihre Prozesse genau analysieren und klären, wo bei ihnen noch viele Papierdokumenten erstellt und bearbeitet werden. Hier sollten sie ansetzen. Fast immer ist es möglich, Dokumenten-Workflows digitaler zu denken und das dann auch zu optimieren.

? **Ulrich Parthier:** *Viele Verwaltungen und Behörden besitzen noch immer ein teils riesiges Papierakten-Archiv. Viele dieser Akten können nicht einfach vernichtet werden. Welchen Lösungsweg gibt es dafür?*

Dietmar Nick: Dieses Problem besteht fraglos und wir haben das erkannt. Die Kyocera-Tochter ALOS hat hier für sehr viele Branchen und Bereiche kluge Konzepte entwickelt. ALOS berät Unternehmen und Organisationen dabei, wie sie ihre riesigen Papierarchive praktikabel und rechtssicher abbauen können, wie sie dabei in einem Zug Aktenberge reduzieren und Büroflächen zurückgewinnen. Ein Kernbestandteil sind dabei die von unserem Partner-Netzwerk angebotenen Kyocera Scan-Services. Mit ihnen werden Kunden die vorherigen Papierakten in einem Cloud-Archiv oder direkt vor Ort digital zur Verfügung gestellt.

? **Ulrich Parthier:** *Manche Unternehmen scheuen Digitalisierungsmaßnahmen, weil die Cyberkriminalität immer mehr zunimmt und sie fürchten, dass die Digitalisierung mit neuen Security-Risiken einhergeht. Bleibt man mit Fotokopie, Papierakte & Co. nicht letztlich auf der sicheren Seite?*

Dietmar Nick: Cyberbedrohungen sind eine ernste Angelegenheit. Aber machen wir uns nichts vor: Es gibt auch für Papier Risiken. Von Feuer über Diebstahl bis hin zu Umweltereignissen ist auch die analoge Welt bedroht. Aus meiner Sicht ist man deshalb ohne Digitalisierung keineswegs sicher. Wer als Unternehmen im 21. Jahrhundert bestehen will, sollte auf digitale Lösungen und klimaschonende Technologien setzen. Nur so lassen sich Geschäftsprozesse nachhaltig, sicher und schnell gestalten. Unternehmen, die sich der Digitalisierung verweigern, werden auf mittlere Sicht ins Aus manövrieren, weil ihnen ihre Wettbewerber einfach voraus sind.

! **Ulrich Parthier:** *Herr Nick, vielen Dank für das Gespräch!*

Digitalisieren ohne Schmerz

DER EINFACHE WEG ZUM DIGITALEN SCHREIBTISCH

Die Digitalisierung ist in den meisten Unternehmen längst angekommen. Wir befinden uns bereits mittendrin in einer digitalen Lebens- und Arbeitswelt. Allerdings hat nahezu kein Unternehmen alle Prozesse und Workflows quasi über Nacht vollständig digitalisiert. Der Status quo zeigt, dass viele analoge und digitale Prozesse parallel laufen, obwohl dies alles andere als effizient ist. Doch welche Lösungen lassen sich so einfach implementieren, dass nicht der ganze Betrieb unter dauerhaften Umstrukturierungsschmerzen leidet?

Viele Unternehmen sind durchaus gewillt, weitere Entscheidungen nicht auf die lange Bank zu schieben. Sie müssen mit der Entwicklung ihrer Wettbewerber oder Partner Schritt halten und sehen sich auch aufgrund des anhaltenden Fachkräftemangels zunehmend mit sich verändernden Anforderungen an den Job konfrontiert. Bei der Digitalisierung von Prozessen empfiehlt Kyocera eine ganzheitliche Strategie. Denn ein durchgängig digitales Dokumentenmanagement beschleunigt Geschäftsprozesse spürbar und gestaltet sie effizienter.

Dokumenten-Workflows optimieren

Als Experte für die Optimierung von Dokumenten-Workflows und Geschäftsprozessen bietet die Kyocera-Gruppe sämtliche Werkzeuge für effiziente Dokumentenprozesse. Der Kyocera Workflow Manager ist speziell auf die Bedürfnisse mittelständischer Unternehmen zugeschnitten und ist der Enabler hin zur digitalen Transformation. Die Lösung erlaubt ein digitales Dokumentenmanagement mit automatisierten Abläufen. Ob Angebotserstellung, Rechnungsdurchläufe oder die Bearbeitung von Projektdokumenten: Alle Prozesse werden nachvollziehbarer – und damit auch besser kontrollierbar.

Das ist sinnvoll, wie ein Beispiel verdeutlicht. In vielen Unternehmen nutzt quasi jeder Mitarbeitende oder jedes Team ein eigenes Ablagesystem: Der eine bewahrt die eingegangenen Rechnungen noch in Papierform auf, die Kollegin speichert sie digital in einem Netzwerkordner oder in Outlook. Die Festlegung der Ordnerstruktur oder die Benennung der einzelnen Files erfolgt meist individuell. Diese Form des digitalen Wildwuchses rächt sich spätestens dann, wenn ein Mitarbeitender längere Zeit ausfällt oder das Unternehmen verlässt. Dann ist die Frage „Wo ist denn noch mal die Rechnung aus dem Oktober?" oder „Was ist der letzte Stand dieses Angebots?" für eine andere Kraft kaum zu beantworten. Die gesamte Organisation wird ausgebremst. Das ist bereits systematisch untersucht worden: Eine Umfrage unter rund 1.200 Büroangestellten in Deutschland und Österreich hat ergeben, dass Angestellte täglich bis zu zwei Stunden sparen würden, wenn ihr Unternehmen über eine digitale Dokumentenverwaltung verfügen würde.

Der Kyocera Workflow Manager bietet eine Stichwortsuche an, die das Finden von Informationen in wenigen Sekunden ermöglicht. Es reicht aus, ein Datum, die Rechnungsnummer, den Firmennamen oder auch nur einen Begriff einzugeben, um die entsprechenden Dokumente angezeigt zu bekommen. Das klingt gut, aber viele Unternehmen schrecken noch vor einer solchen Lösung zurück. Sie befürchten für die Implementierung einer DMS-Software erheblichen Customizing- und Consulting-Aufwand. Darüber hinaus sind die Unternehmen davon überzeugt, dass ein solcher Schritt in die digitale Zukunft mit beträchtlichen Kosten verbunden ist.

DMS an einem Tag

Doch es geht auch anders: Der Kyocera Workflow Manager lässt sich in wenigen Stunden einfach implementieren und kann danach ohne riesigen Schulungsaufwand sofort eingesetzt werden. Bei der Einrichtung der Lösung auf den unternehmenseigenen Servern stellt sich vor allem die Frage, welche der modularen Anwendungen installiert werden sollen. Hier helfen Kyocera und der Fachhandel bei der schnellen Identifizierung der richtigen Module. Der nächste Part ist das Zuteilen der Rechte für die Mitarbeitenden. Hierfür werden Gruppen mit Rechten erstellt und die Nutzer dann einer oder mehreren Gruppen zugewiesen. Schließlich wird der Client auf den einzelnen Rechnern eingerichtet. Das geht ganz einfach über das Setup innerhalb von kaum zehn Minuten. Anschließend werden die Anwender geschult: In rund einer Stunde werden die grundlegenden Funktionen nahegebracht. Schon kann jede und jeder Dokumente ins System bringen, sie dort verwalten und verfügbar machen. Da die

Lösung von eintönigen Aufgaben befreit und echte Zeitersparnis bringt, wird sie in der Regel schnell akzeptiert.

Das zeigt: Die Einführung einer effizienten DMS-Lösung kann schnell, modular und Schritt für Schritt erfolgen. Das Team kann sich evolutionär mit Neuerungen vertraut machen und wird nicht über Nacht mit komplett neuen Workflows konfrontiert. Dadurch bleiben die Kosten für die Implementierung im Zaum und – das ist wichtig – die Belegschaft wird auf sanfte Weise in Richtung digitaler Dokumentenzukunft geführt.

Die Software hat sich bereits bei einer Vielzahl mittelständischer Betriebe bewährt. Das verbesserte Informationsmanagement macht sich schnell durch kürzere Bearbeitungs- und Durchlaufzeiten bemerkbar. Es wird produktiver gearbeitet, es bleibt mehr Zeit für alle Kernaufgaben und Projekte. Optional ermöglicht der Kyocera Workflow Manager auch eine rechtssichere digitale Signatur, womit auch zentrale rechtliche und datenschutzbezogene Anforderungen voll erfüllt werden.

Möchten Unternehmen mit digitalen Workflows besser den Anforderungen ihrer Belegschaft an mobiles Arbeiten gerecht werden, können cloudbasierte DMS-Lösungen die richtige Antwort sein: Der Kyocera Cloud Information Manager ermöglicht als SaaS-Lösung den sicheren Zugriff auf Geschäftsdokumente über einen Webbrowser. Die Benutzer können von überall auf die Dateien zugreifen und Dokumenten-Workflows bearbeiten. Gespeichert werden alle Dokumente auf einem verschlüsselten Server, auf den nur die Benutzer mit ihren Anmeldedaten Zugriff haben. Administratoren können dabei den Zugriff nach Dokumenten- oder Benutzerkategorien verwalten, was die Plattform anwenderfreundlich und gleichzeitig hochsicher macht.

Erfolgsfaktor Archivierung

Neben der Erstellung und Bearbeitung digitaler Dokumente brennt auch das Thema Archivierung vielen Anwendern unter den Nägeln. Hier gilt es, Informationen für das gesamte autorisierte Team jederzeit verfügbar zu machen. Eine optimierte Zusammenarbeit und prozessorientiertes Arbeiten auch vom Homeoffice aus sind zentrale Anforderungen. Nicht zuletzt sorgt Kyocera mit seinen digitalen Dokumentenmanagement-Lösungen dafür, dass Unternehmen mühelos alle aktuell geltenden Sicherheitsbestimmungen einhalten und sämtliche gesetzlichen Vorgaben für Langzeitarchivierung erfüllen.

Bernd Rischer

> MIT UNSEREN DIGITALEN DOKUMENTENMANAGEMENT-LÖSUNGEN SORGEN WIR DAFÜR, DASS UNTERNEHMEN MÜHELOS ALLE SICHERHEITSBESTIMMUNGEN ERFÜLLEN UND EINHALTEN KÖNNEN.
>
> **Bernd Rischer, Group Director Sales, Kyocera Document Solutions Deutschland GmbH, www.kyoceradocumentsolutions.de**

DIE KI-ROADMAP

KÜNSTLICHE INTELLIGENZ IM UNTERNEHMEN ERFOLGREICH UMSETZEN

DIE KI-ROADMAP
– Künstliche Intelligenz im Unternehmen erfolgreich umsetzen;
Jens-Uwe Meyer,
Business Village GmbH,
10-2023

In den kommenden Jahren wird künstliche Intelligenz Unternehmen radikal verändern. Dieser Wandel betrifft Unternehmen und Beschäftigte sämtlicher Branchen.

Doch welche Technologien erwarten uns in naher Zukunft? Wie lässt sich KI in die Unternehmensprozesse integrieren? Und welche neuen Chancen entstehen durch den Einsatz von KI?

Antworten liefert Dr. Jens-Uwe Meyers neues Buch. Es illustriert, wie Sie als Unternehmen Anwendungsfälle für künstliche Intelligenz finden, die Machbarkeit evaluieren und die wirtschaftlichen Vorteile berechnen. Das kann nur gelingen, wenn Sie Ihre Organisation fit für die Zukunft machen und Beschäftigte und Führungskräfte in diese Prozesse einbinden.

Die KI-Roadmap ist das praxisorientierte Planungstool, das Sie unterstützt, die richtigen Fragen zu stellen, um die Erfolgversprechenden Antworten auf den Wandel zu finden. Dr. Jens-Uwe Meyer zählt zu den bekanntesten und einflussreichsten Vordenkern für Innovation, Digitalisierung und künstliche Intelligenz. Im Verlag Business Village sind unter anderem seine Bücher „Digitale Disruption“, „Digitale Gewinner“ und „reset – Wie sich Unternehmen und Organisationen neu erfinden“ erschienen.

PROZESSAUTOMATISIERUNG

Um wettbewerbsfähig zu bleiben, Ressourcen effizient zu nutzen, die Kundenzufriedenheit zu steigern und den sich ständig ändernden Anforderungen des Marktes gerecht zu werden, ist eine kontinuierliche Prozessoptimierung unerlässlich. Sie beruht auf Analyse, Überarbeitung und Verbesserung bestehender Geschäftsprozesse.

Doch das stellt viele Unternehmen vor enorme Herausforderungen – schon allein deshalb, weil sie oft keinen Überblick über ihre bestehenden Prozesse haben. Dazu kommen gesetzliche Vorgaben, auslaufender Support oder individuelle Anpassungen. Das Ergebnis ist oft ein Konstrukt aus Ineffizienz, Intransparenz und Mitarbeiterverzweiflung.

Bei der Prozessautomatisierung ist das Hauptziel, die menschliche Intervention zu reduzieren und manuelle und wiederkehrende Aufgaben durch den Einsatz von Technologien zu automatisieren. Doch wie kann das am sinnvollsten gelingen und welche Rolle spielt der Mensch dann noch?

Keeping the core clean

DEN STANDARD FÜR ERP-SYSTEME BEHALTEN UND TROTZDEM FLEXIBEL AGIEREN

ERP-Altsysteme müssen dringend zu moderneren Versionen und Systemen migriert werden. Das stellt Unternehmen vor große Herausforderungen. Darüber sprachen wir mit Fabian Czicholl, Regional Vice President bei Appian.

it management: *Herr Czicholl, SAP hat angekündigt, ab 2027 ältere ECC-Versionen nicht mehr zu unterstützen, sodass viele Migrations- und Transformationsprojekte zu SAP S/4HANA laufen. Das stellt einige Unternehmen vor große Herausforderungen. Mit welchen Problemstellungen haben sie aus Ihrer Sicht zu kämpfen?*

Fabian Czicholl: Immer wieder stellen wir fest, dass Altsysteme über die Jahre so stark individuell angepasst wurden, dass ein Standard im Grunde gar nicht mehr gegeben ist. Diese individuellen ERP-Ergänzungen haben in der Vergangenheit den Unternehmen Wettbewerbsvorteile gebracht, aber gleichzeitig dazu geführt, dass Updates ohne einen standardisierten Kern nicht möglich sind. Bei der Migration auf SAP S/4HANA beispielsweise möchte man diesen Fehler nicht wiederholen und den SAP-Kern „sauber" halten, damit Upgrades zukünftig möglich bleiben.

it management: *Wie kann man aber dann die Individualität und Agilität dieser ERP-Systeme beibehalten?*

Fabian Czicholl: Eine berechtigte Frage, denn ist gibt gute Gründe dafür, warum das weiterhin möglich sein sollte. Nehmen wir als Beispiel das Lieferkettensorgfaltspflichtengesetz. Das hat nicht nur den Supply-Chain-Managern einige Kopfschmerzen beschert, sondern auch der IT, die neue Governance- und Compliance-Regelungen in ihrer Architektur abbilden können muss. Dass allein hierfür bereits kleine Softwarehäuser vielfältige Ergänzungslösungen für prominente ERP-Systeme anbieten, verdeutlicht das Dilemma. Jetzt wird die EU eine deutlich strengere Lieferkettengesetzgebung auf den Weg bringen, die das deutsche Gesetz überschreiben wird. Das wird zwangsläufig dafür sorgen, dass Prozesse auch in den IT-Abteilungen der Unternehmen wieder angefasst und optimiert werden müssen.

ES BRAUCHT DEN MENSCHEN ALS NUTZER DIESER TECHNOLOGIEN, UM ZU KONTROLLIEREN UND GEGENZUSTEUERN.

Fabian Czicholl,
Regional Vice President, Appian,
www.appian.com

it management: *Wie meinen Sie das?*

Fabian Czicholl: Viele Randprozesse und Systeme sind weitgehend Spreadsheet und E-Mail-basiert, was die Zusammenarbeit mit Lieferanten und die Einhaltung von Governance- und Compliance-Vorschriften erschwert. Zudem erfordert die Verwaltung komplexer Beziehungen zu Dienstleistern eine umfassende Due-Diligence-Prüfung. Unternehmen müssen die Einhaltung von komplexen, multidimensionalen Sanktionsprüfungen in Abhängigkeit von zum Beispiel Region, Produktkategorie und Auftragsvolumen sicherstellen und das Geschäftsrisiko minimieren. Hier arbeiten viele, unterschiedliche Abteilungen teilweise auf sehr individueller Fallebene zusammen. Die oftmals manuelle Bearbeitung macht Prozesse jedoch langsam, intransparent und ineffizient. Zudem erhöht es das Risiko menschlicher Fehler. Das kann bei den komplexen Geschäftsprozessen im Supply-Chain-Management unter der Bedingung sich ändernder Regulatorik fatal sein.

it management: *Und die Updates der ERP-Systeme durch die Hersteller helfen nicht?*

Fabian Czicholl: Das würde nur bedingt helfen, denn für die Standard-Updates im Kern ist die erforderliche Individualität oft zu kleinteilig. Aus Sicht der großen ERP-Anbieter lohnen sich entsprechende Updates nicht, sodass hierfür entweder Nischenanbieter in die Bresche springen oder das ERP dahingehend angepasst wird.

Da aktuell viele Firmen mit der ERP-Migration beschäftigt sind, werden solche funktionalen Erweiterungen pausiert. Zudem zeigt sich in der Migrationsphase meist, dass in der IT-Architektur eine Brücke zwischen den Alt- und Neusystemen geschlagen werden muss.

it management: *Wie kann das funktionieren?*

Fabian Czicholl: Indem eine Plattform mit hoher Integrationsfähigkeit, diese ist entscheidend, zur Prozessorchestrierung genutzt wird. Eine solche Plattform kann als „Agilitätsschicht" an die vorhandenen Systeme angedockt werden, völlig unabhängig davon, was die Systeme darunter tun oder wie alt sie sind. Unterschiedliche Datenquellen werden miteinander verbunden, die während einer laufenden Migration flexibel austauschbar sind. Wir von Appian orchestrieren mit unserer Plattform die Prozessvariationen über Systeme hinweg, was Transparenz schafft und zur Effizienz beiträgt. Das wäre der erste Schritt. Nimmt man noch eine Prozessautomatisierung vor, verändert das die Art und Weise, wie Unternehmen mit Anbietern und Lieferanten kommunizieren, grundlegend.

it management: *Können Sie hier ein Beispiel nennen?*

Fabian Czicholl: Verknüpft man die Datenquellen der ERP-Systeme und automatisiert die Prozesse zur Fallbearbeitung erhält man dynamische Ad-hoc-Arbeitsabläufe, die Ereignisse automatisch zur Überprüfung und Bearbeitung weiterleiten. Mit den Workflow-Funktionen können Sie jeden Schritt Ihres Einzelfalls überwachen, gegensteuern, falls nötig, und effizienter gestalten. Unsere Case-Management Plattform unterstützt das Erstellen und Verwalten von Geschäftsregeln und bietet den Fallbearbeitern die Möglichkeit, Prozesse umgehend an neue Situationen anzupassen. Das Anbinden von verschiedenen Sanktionslisten oder Compliance-Anbietern für die Due-Diligence-Prüfungen beispielsweise minimiert das bereits erwähnte Geschäftsrisiko. All das hilft auch bei der Einhaltung von Compliance-Regeln, womit wir wieder bei den Lieferkettengesetzen wären. Vieles ist möglich. Schnell und flexibel in der Anwendung und Gestaltung mit einem modernen User Interface, das auch mobil sofort verfügbar ist. Durch die schnelle Umsetzung ergibt sich übrigens auch ein schneller ROI für die Unternehmen.

it management: *Kommen wir zur künstlichen Intelligenz. Diese nutzen Sie doch sicher auch, oder?*

Fabian Czicholl: Selbstverständlich. Intelligent Document Processing (IDP) als ein Beispiel für künstliche Intelligenz spielt schon seit Jahren eine große Rolle in unserem Technologie-Baukasten. KI, konkret Machine Learning, kann beispielsweise unstrukturierte Daten in strukturierte umwandeln oder auch Dokumente automatisch klassifizieren. Die neusten Entwicklungen zu generativer KI und Large Language Models sind ein weiterer technologischer Fortschritt, der uns auch in der Prozessautomatisierung hilft. Wenn es aber um die Anwendung von Anbietern wie OpenAI oder Google geht, möchte ich vehement auf die Möglichkeiten einer privaten KI verweisen.

it management: *Könnten Sie uns das bitte etwas näher erläutern?*

Fabian Czicholl: KI-Modelle sollten bestenfalls mit ausschließlich unternehmenseigenen Daten trainiert werden und Dritten den Zugang zu diesen Daten verwehren. Keine Firma möchte fremde KI-Modelle mit ihren Unternehmensdaten trainieren. Eine private KI verhindert das ganz im Sinne des Datenschutzes und den entsprechenden Policies. Alle KI-Services von Appian sind im Übrigen private KI-Services.

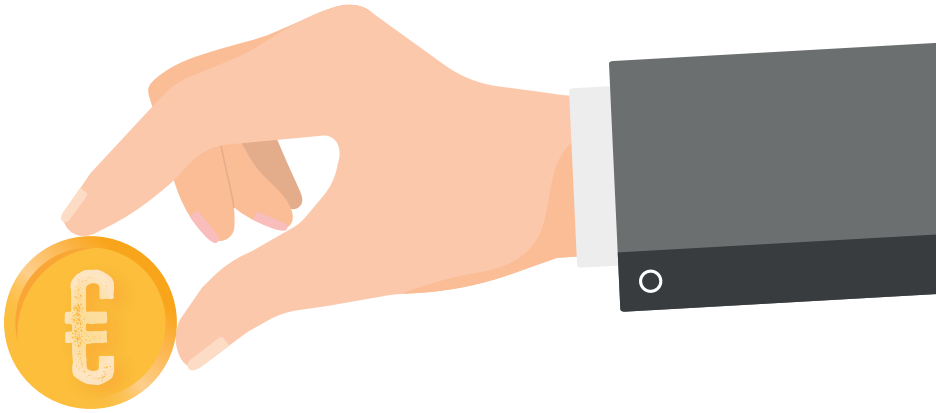
it management: *Und wo bleibt der Mensch bei aller Prozessautomatisierung auch durch KI?*

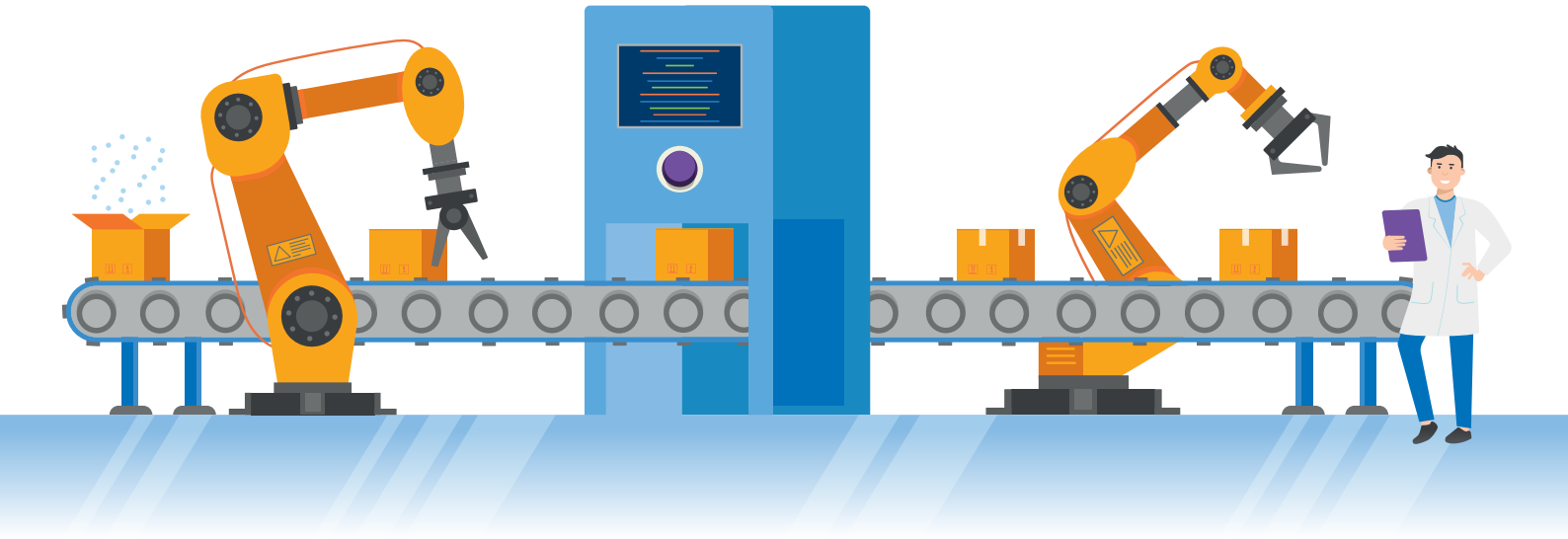
Fabian Czicholl: Der Mensch bleibt ein integrativer Bestandteil des technologischen Fortschritts. Stichwort: Human in the loop. Es braucht den Menschen als Nutzer dieser Technologien, um zu kontrollieren und gegenzusteuern. Gleichzeitig befreit eine Prozessautomatisierung die Mitarbeitenden von sinnfreien, repetitiven Tätigkeiten, da diese von einem Bot und einem Programm übernommen werden können. So ermöglicht Appian es, Freiräume für die wertvolleren Tätigkeiten an gut ausgebildete Fachexperten zu geben. Damit wird Mehrwert in einer Zeit geschaffen, in der durch Fachkräftemangel die Experten rar sind.

it management: *Herr Czicholl, wir danken für das Gespräch.*

Pay-per-Use

GEBRAUCHSABHÄNGIGE FINANZIERUNG VON SONDERMASCHINEN





Seit einiger Zeit bietet die SN Maschinenbau GmbH potenziellen Interessenten die bisher im Bereich der Einzel-, Auftrags- und Variantenfertigung nicht gebräuchliche Finanzierungsform des Pay-per-Use an. Auf diese Weise hofft der Wipperfürther Sondermaschinenbauer auf die Erschließung neuer Zielgruppen, da die Nutzung der leistungsstarken Verpackungsanlagen nun auch für solche Unternehmen eine Option wird, die die vergleichsweise hohen Anfangsinvestitionen bislang scheuten. Als Finanzierungspartner fungiert Siemens Financial Services, die gesamte kaufmännische und produkttechnische Projektabwicklung erfolgt über das ERP-System des Bergischen Mittelständlers.

Die Idee, die eigenen Maschinen im Rahmen eines flexiblen, gebrauchsabhängigen Bezahlungsmodells bereitzustellen, ergab sich aus der einige Jahre zurückliegenden Entscheidung der Firmen- und Vertriebsleitung, das seinerzeit ausschließlich hochpreisige Produktportfolio um kostengünstigere Varianten zu erweitern. Großes Renommee in seinem Marktsegment hatte das Unternehmen bis dahin durch den Bau hochindividueller Beutelverpackungsmaschinen erlangt, zu deren Abnehmern viele namhafte, oft weltweit agierende Nahrungsmittel- und Pharmaproduzenten gehören. Modular gestaltete Einstiegsmodelle mit einem größeren Anteil an standardisierten Komponenten sollten SN nun auch den Zugang zu einem deutlich erweiterten Interessentenkreis ermöglichen. Vor diesem Hintergrund war der Schritt zum Angebot von Pay-per-Use konsequent: „Dieses Konzept eröffnet uns als Hersteller neue Marktchancen, denn es ermöglicht auch kleineren Unternehmen die effiziente und nachhaltige Nutzung unserer modernen Verpackungstechnologien – auch aus wirtschaftlich schwächeren Regionen wie Osteuropa“, sagt Geschäftsführer Christian Kettler.

Flexibles Modell minimiert das finanzielle Risiko

Der Vorteil für die Maschinennutzer besteht darin, dass die hohen Anfangsinvestitionen entfallen und sie dadurch ihre Liquidität schonen. Da nur die tatsächlich produzierten Verpackungseinheiten bezahlt werden müssen, können selbst Start-ups, die noch keine langfristig planbare Auslastung einbuchen konnten, die individuell konditionierten Sondermaschinen mit geringem finanziellen Risiko in Gebrauch nehmen. Zudem wird die Auslieferung der Maschinen deutlich beschleunigt, da aufwendige Finanzierungsrunden mit den Banken entfallen. Dies hängt in großem Maße damit zusammen, dass SN potenzielle Kunden laut Christian Kettler natürlich ganz anders bewerten kann als Finanzdienstleister oder Banken. „Denn wir legen nicht allein ökonomische Bewertungskriterien und Kennzahlen zugrunde, sondern in erster Linie die Business-Erwartung. Aufgrund unserer langjährigen Branchenerfahrung können wir bestens bewerten, ob eine angedachte Applikation erfolgsversprechend ist“, konkretisiert der Geschäftsführer. Selbst wenn sich die Erwartungen nicht erfüllen sollten, entsteht den Maschinenbetreibern kein unmittelbar existenzbedrohender Schaden. Zwar zahlen sie eine monatlich fixe Grundrate, die Ge-

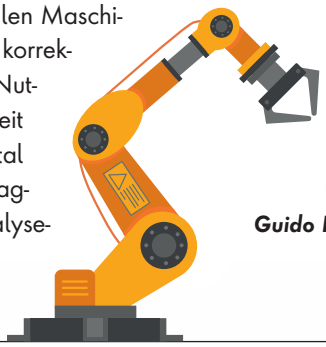
brauchskosten folgen jedoch unmittelbar der tatsächlichen Produktion. Wird wenig produziert, sinken sie entsprechend.

Natürlich muss dieser variablen Finanzform ein solides betriebswirtschaftliches Fundament zugrunde liegen. Dies gestaltet sich so, dass SN die Maschinen an Siemens Financial Services verkauft, direkt zurückleast (Sell-and-Lease-Back) und gleichzeitig die Erlaubnis besitzt, die Anlage an Dritte zu vermieten.

Technische Unterstützung durch das ERP-System

Um für sich selbst eine effiziente und wirtschaftliche Projektabwicklung zu gewährleisten, greift der Sondermaschinenbauer auf die jederzeit aktuellen Daten seines durchgängigen ERP-Systems ams.erp zurück. Dieses ist auf die besonderen Anforderungen der Einzel- und Variantenfertigung zugeschnitten und lässt dank seines integrierten Produktkonfigurators die schnelle und wirtschaftliche Auslegung der angefragten Maschinen zu. Entscheidet sich ein Kunde später dazu, eine Anlage zurückzugeben, erlaubt der Konfigurator eine unkomplizierte Neukonfiguration, um schnellstmöglich ein neues Angebot für das Rücknahmegerät zu generieren und es wiederzuverwenden.

Zur Sicherstellung der optimalen Maschinenleistung sowie auch der korrekten Abrechnung werden die Nutzungsdaten in Zusammenarbeit mit Siemens Technology digital erfasst, in Cloud-Systemen aggregiert und über eine Analyse-Software in Echtzeit ausgewertet. Siemens garantiert dabei als neutraler Partner, dass nur die von den Kunden bewilligten Daten in die Cloud gegeben werden. SN hat zur Berechnung des Pay-per-Use-Anteils lediglich monodirektionalen Zugriff auf diese freigegeben Daten.



Das große Potenzial in dem Ansatz des Pay-per-Use im Bereich des Sondermaschinenbaus sehen neben ersten Interessenten auch die Experten des ife – Netzwerk für Einzelfertiger, die der SN-Geschäftsführung im November 2023 ihren diesjährigen Innovationspreis der Losgröße 1+ verliehen.

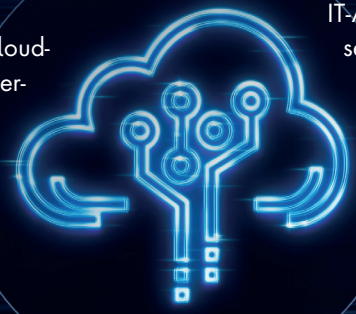
Guido Piech | www.ams-erp.com

CLOUD-NATIVE COMPUTING

SOFTWARE ENGINEERING VON DIENSTEN UND APPLIKATIONEN IN DER CLOUD

Märkte verändern sich immer schneller, Kundenwünsche stehen im Mittelpunkt – viele Unternehmen sehen sich Herausforderungen gegenüber, die nur digital beherrschbar sind. Um diese Anforderungen zu bewältigen, bietet sich der Einsatz von Cloud-native-Technologien an. Dabei reicht es jedoch nicht aus, einen Account bei einem Cloud-Anbieter anzulegen. Es geht auch darum, die unterschiedlichen Faktoren zu verstehen, die den Erfolg von Cloud-native-Projekten beeinflussen.

Das Buch beleuchtet den Cloud-native-Wandel aus unterschiedlichen Perspektiven: von der Unternehmenskultur, der Cloud-Ökonomie und der Einbeziehung der Kunden (Co-Creation) über das Projektmanagement (Agilität) und die Softwarearchitektur bis hin zu Qualitätssicherung (Continuous Delivery), Betrieb (DevOps) und Sicherheit. Anhand von realen Praxisbeispielen wird gezeigt, was bei der Umsetzung in unterschiedlichen Branchen gut und was schlecht gelaufen ist und welche Best Practices sich daraus ableiten lassen. Dabei wird auch die Migration von Legacy-Code berücksichtigt.



IT-Architekten vermittelt dieses Buch zudem das grundlegende Wissen, um Cloud-native-Technologien und die DevOps-Kultur in ihrem Projekt oder im gesamten Unternehmen einzuführen.

Cloud-native Computing
Software Engineering von Diensten und Applikationen in der Cloud;
Nane Kratzke (Hrsg.);
Carl Hanser Verlag GmbH & Co.KG; 12/2023

TRANSFORMATIONSPROJEKTE

FLUCH ODER SEGEN?

Wie treiben Unternehmen ihre digitale Transformation (DX) voran? Diese Frage untersucht Endava in einem gesponsorten IDC InfoBrief: „Leveraging the Human Advantage for Business Transformation". Im Rahmen der Untersuchung wurden Hindernisse, Maßnahmen und Ergebnisse der digitalen Transformation aufgedeckt. Zudem zeigt die Studie, welche strategischen Faktoren hierbei eine Rolle spielen und welche Ansätze Unternehmen bei der Integration wichtiger Technologien wie künstliche Intelligenz (KI) und Automatisierung verfolgen.

Unter den weltweit befragten Führungskräften und Entscheidungsträgern gibt die große Mehrheit (88 Prozent) zu, dass ihr Unternehmen in den letzten zwölf Monaten lediglich bei höchstens der Hälfte seiner DX-Projekte die erwarteten Ziele oder Ergebnisse erreicht hat. Und das hat Folgen: So geben 62 Prozent der Befragten an, dass sie aufgrund solcher Misserfolge technisch nicht so fortschrittlich sind wie ihre Konkurrenten und ihre Time-to-Market länger ist. Doch nicht nur Infrastruktur und Marktposition sind betroffen. Viele Unternehmen müssen sich infolgedessen außerdem mit frustrierten Mitarbeitern auseinandersetzen (56 Prozent) und verzeichnen einen Anstieg der Fluktuation (50 Prozent). Auch wird das Arbeitsumfeld als weniger motivierend für die Angestellten wahrgenommen (44 Prozent).

Unternehmen verlieren die Menschen aus den Augen

Der Report geht auch auf die Gründe für ausbleibende Ergebnisse und nicht erreichte Ziele bei DX-Projekten ein. Und hierbei wird deutlich, dass Unternehmen es allzu oft versäumen, die Menschen bei der Planung, Konzeption und Umsetzung digitaler Initiativen in den Mittelpunkt zu stellen. Für 39 Prozent der Führungskräfte ist beispielsweise die mangelnde Akzeptanz unter den Mitarbeitern ein Hauptgrund dafür, warum die erwarteten Ergebnisse nicht erreicht wurden. Dies deutet darauf hin, dass kulturelle Aspekte berücksichtigt werden müssen, um das Engagement und die Motivation zu erhöhen. Als weitere Gründe folgen dahinter Meinungsverschiedenheiten zwischen Führungskräften (36 Prozent) sowie fehlende interne Zusammenarbeit (33 Prozent). Scheinbar haben Unternehmen Probleme damit, interne Dynamiken erfolgreich zu steuern und alle Stakeholder in die Projekte einzubinden.

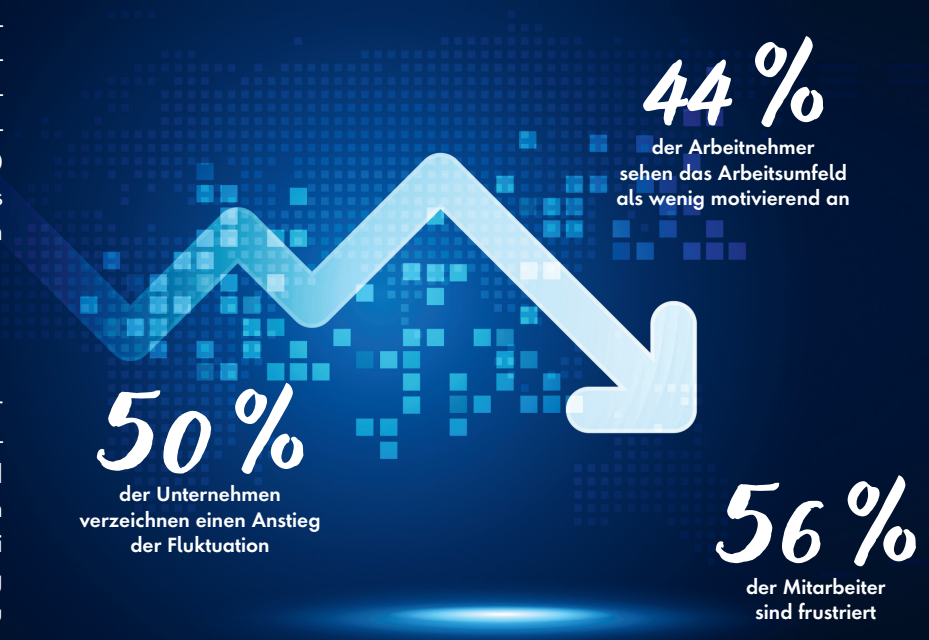
Bei der Betrachtung gescheiterter DX-Projekte stellt dann auch mehr als die Hälfte fest, dass die Investitionen besser in Projekte geflossen wären, die die Menschen in den Mittelpunkt stellen. Dazu zählen etwa Weiterbildungen für die Mitarbeiter (55 Prozent) oder die Verbesserung der Kommunikation zwischen der IT und den Fachabteilungen (50 Prozent).

Erfolgreiche DX-Projekte bringen Vorteile auf allen Seiten

Vor dem Hintergrund der großen Fortschritte der letzten Jahre im Bereich KI und dem aktuellen Boom generativer KI geht aus der Studie zudem hervor, dass bereits viele Pläne für die Implementierung und Einführung von KI haben: Jeder Zweite (49 Prozent) hat bereits KI in seinem Unternehmen eingesetzt oder ein Proof of Concept durchgeführt. Dabei ist ihnen bewusst, dass sie den menschlichen Einfluss auf den Einsatz von KI beibehalten müssen, 51 Prozent bezeichnen dies als sehr oder äußerst wichtig.

www.endava.com

WENN DAS DX-PROJEKT SCHEITERT



LLMs im ERP-Kontext

MEHR STRUKTUR, BITTE!

Ein Angebot erstellen, dazu aus unterschiedlichsten Quellen Kundeninformationen zusammensuchen, personalisierte Rabatte berücksichtigen, Sonderwünsche einarbeiten – was für einen menschlichen Mitarbeiter kein Problem ist, kann eine KI vor große Herausforderungen stellen. Damit die Möglichkeiten der jüngsten KI-Innovationen wie Large Language Models sinnvoll Einzug in die ERP-Welt halten können, braucht es KI-gerecht aufbereitete Prozessabläufe.

Es ist ein regelrechter Quantensprung, den die KI-Forschung im vergangenen Jahr vollzogen hat: Mithilfe der Large Language Models (LLM) ist es der Technologie erstmals möglich, Aufgabenstellungen nicht länger nur in einem eng umrissenen Kontext zu bearbeiten. Vielmehr ist sie nun in der Lage, verschiedenste Fähigkeiten miteinander zu kombinieren: von der Erstellung von Texten über das Verständnis natürlicher Sprache bis hin zur Generierung von Bildern oder Softwarecode.

Auch im ERP-Kontext eröffnen sich dadurch neue Einsatzszenarien. Bereits in naher Zukunft werden die KI-Fortschritte die Interaktionsmöglichkeiten zwischen Mensch und Maschine stark verändern, beispielsweise in Form einer Zusammenarbeit per Sprachsteuerung. Dies wird es Anwendern ermöglichen, etwa während einer Autofahrt mit einer ERP-Lösung wie mit einem Kollegen zu interagieren, der sie durch die erforderlichen Abläufe führt. Auf diese Weise werden sich Aufgaben wie Auftragserstellung, Materialkommissionierung oder die Verarbeitung von Serviceanfragen auch ohne Maus und Monitor mit optimaler Effizienz bearbeiten lassen.

KI liebt Struktur

Damit ein solches Szenario jedoch Realität werden kann, sind auf Prozessebene die richtigen Voraussetzungen zu schaffen, um einer künstlichen Intelligenz die Bedienung des ERP-Systems zu ermöglichen. Für einen menschlichen Anwender ist die traditionell datenzentrierte Arbeitsweise kein Problem: Sie finden sich nach etwas Einarbeitung in der Fülle an Datenfeldern und Schaltflächen zurecht, wissen, in welcher Reihenfolge Prozessschritte – auch bei Sonderfällen – bearbeitet werden sollten. Eine KI hingegen ist in einem solchen Kontext überfordert. Sie benötigt klare, strukturierte Abläufe und vordefinierte Prozesspfade, an denen sie sich orientieren kann.

Eine dedizierte Prozesssicht ist hierfür entscheidend, welche die hinter den Abläufen stehende Logik beschreibt und für die KI nutzbar macht. So ist dann beispielsweise ein LLM in der Lage, den Anwender effizient und korrekt durch die erforderlichen Abläufe zu führen. Aus diesem Grund müssen sich die Unternehmen einen umfassenden Überblick über die Einzelschritte ihrer zentralen Prozesse verschaffen, um diese auf klar definierte Art und Weise im ERP-System zu verankern – und damit den Weg zu ebnen für die KI-Anwendungen der Zukunft.

Vorarbeit frühzeitig angehen

Gemessen an der Schlagzahl, mit der sich KI-Innovationen derzeit vollziehen, wird es nur noch eine Frage der Zeit sein, bis eine solche interaktive „Zusammenarbeit" zwischen Mensch und Maschine im täglichen Arbeitsalltag Einzug hält. Es empfiehlt sich daher, möglichst zeitnah damit zu beginnen, die eigene Prozesswelt zu analysieren und zu dokumentieren – eine Aufgabe, die je nach Unternehmen durchaus Zeit erfordern wird. Wer hier frühzeitig beginnt, verschafft sich eine ideale Ausgangslage, um die Vorteile der kommenden KI-Innovationen auch möglichst frühzeitig für sich zu nutzen.

Ralf Bachthaler

MITHILFE DER LLM IST ES DER TECHNOLOGIE ERSTMALS MÖGLICH, AUFGABENSTELLUNGEN NICHT LÄNGER NUR IN EINEM ENG UMRISSENEN KONTEXT ZU BEARBEITEN.

Ralf Bachthaler,
Vorstand, Asseco Solutions AG,
www.applus-erp.de

Gefangen in der Microsoft-Cloud?

EIN BEFREIUNGS-TIPP

NICHT SELTEN LAUFEN DIE ONLINE-PLÄNE, DIE GENUTZT WERDEN, AM BEDARF DES UNTERNEHMENS VORBEI.

Markus Seirer,
Microsoft-zertifizierter Lizenzberater,
VENDOSOFT GmbH,
www.vendosoft.de

Im August 2023 war es noch ein Gerücht. Im Oktober wurde es Gewissheit und erhitzte die CIO-Gemüter: Microsoft nahm eine Gesetzesänderung zum Vorwand, um mit Wirkung zum November letzten Jahres TEAMS aus den E- und F-Plänen von Office beziehungsweise M365 zu entfernen. Jahrelang wurden die User auf die Kollaborationsplattform konditioniert, nun fliegen den Unternehmen buchstäblich die Kosten um die Ohren. Wer TEAMS in den genannten Plänen weiter nutzen will, zahlt ab sofort etwa 30 Euro mehr pro Lizenz. Kein Wunder, dass sich bei der VENDOSOFT GmbH die Anfragen mehren, wie man dieser Kostenfalle entgehen kann. Nachgefragt wird hier, weil das Unternehmen nicht nur CSP-Anbieter, sondern auf jede Form der Microsoft-Lizenzierung spezialisiert ist: Neu, gebraucht, hybrid, Cloud-only.

Die Nöte der IT-Verantwortlichen

Markus Seirer versteht die Nöte seiner Kunden. „Von den ursprünglichen Vorteilen der M365 Cloud ist ja nicht viel übrig", sagt der Lizenzberater. Um bis zu 25 Prozent sind die wichtigsten Dienste seit Anfang 2022 teurer geworden. Je flexibler ein Abo, desto höher mittlerweile die Gebühren. Lizenzrechtliche Anpassungen zu Ungunsten der User ärgern den Consultant. „Wir raten deshalb schon lange von einer vollständigen Migration in die Cloud ab. Weil das nicht notwendig ist. Viel zu teuer und für die Zukunft unberechenbar!"

Ein Anlagenbauer, der auf diese Weise viel Geld sparen konnte, ist die KIESELMANN GmbH. Acht Gesellschaften fertigen am Produktionsstandort Baden-Württemberg Prozessarmaturen und Edelstahlanlagen für den Export in die ganze Welt. Für 350 PC-Arbeitsplätze sollte bestehende Software ergänzt werden. Der Teamleiter für Systeme und Security IT machte den Vorschlag, unternehmensweit auf gebrauchte Software zu gehen. Damit war er bei VENDOSOFT genau richtig und lernte deren kostenfokussierte Beratung kennen.

Das Sparpotenzial von Software

Nach einem Testkauf mit gebrauchten Office-Paketen stand fest: Lizenzen von VENDOSOFT sind nicht nur günstig, sondern Microsoft-konform und Audit-sicher! Innerhalb kürzester Zeit wurden daher alle Computerarbeitsplätze mit Gebrauchtsoftware ausgestattet: MS Office, Project und Vision, Windows, SQL und Exchange Server (die gebraucht besonders hohe Einsparungen bringen!). Innerhalb der letzten drei Jahre sparte das Unternehmen 245.000 Euro (!) verglichen mit einem Neukauf oder M365 – bei einem Einkaufsvolumen von 70.000 Euro.

Angesichts solcher Preisvergleiche ist die Microsoft Cloud bei KIESELMANN kein Thema. „Die Features eines neuen Office-Pakets sind dem Kunden zu Recht nicht mehrere hundert Euro im Jahr wert", erklärt Markus Seirer. So geht es vielen, die einmal mit dem Anbieter ins Gespräch kommen. „Mit Lizenzen vom Zweitmarkt reduzieren wir die IT-Kosten unserer Kunden drastisch."

Warum die Cloud oft too much ist

Optimalerweise erfolgt so eine Beratung, bevor migriert wurde. Doch auch, wenn ein Unternehmen bereits weite Teile seiner Microsoft-Lizenzen über die Cloud bezieht, muss das nicht in Stein gemeißelt bleiben. „Zu uns kommen IT-Verantwortliche, die das Gefühl haben, ihre Abo-Gebühren steigen ins Unermessliche. Dann schauen wir uns die Lizenzierung an", erklärt der Microsoft-Profi. Nicht selten laufen die Online-Pläne, die genutzt werden, am Bedarf des Unternehmens vorbei. Nach der eingängigen Formel: „Cloud wo nötig, gebraucht wo möglich" empfehlen Markus Seirer und seine Kollegen dann hybride Infrastrukturen – das reduziert die IT-Kosten. Oft um 60 Prozent und mehr.

Angelika Mühleck | Fachjournalistin

Drei Irrtümer der Cloud-Migration

KMUs AUFGEPASST!

Ab in die Cloud – aber wie, wann und womit? Eine belastbare Strategie für die Migration fehlt in vielen Unternehmen. Manche wechseln unfreiwillig, da Software-Hersteller gewohnte Anwendungen nur noch als Cloud-Lösung anbieten. Auch Innovationsstaus, veraltete Hard- und Software oder der IT-Fachkräftemangel können zum Umdenken unter Zeit- und Kostendruck zwingen. Nicht alle Wünsche an die neue Lösung gehen dabei in Erfüllung, denn drei große Irrtümer bei der Cloud-Migration verleiten zu vorschnellen Entscheidungen.

IRRTUM 1:

Alles einfacher mit der Cloud?

Die Cloud kennen alle aus dem privaten Umfeld: Fotos, Kontakte, Termine und Dokumente sind an ein einem Ort abgelegt, darauf greifen Smartphone, Tablet, Fernseher und sogar der Kühlschrank zu. „Wenn ich mit dem Unternehmen in die Cloud will, muss mir bewusst sein: Hier gibt es nicht diese eine Wolke, mit der alles läuft", erklärt Christian Kaspar vom Technologie- und Managed Service-Provider Konica Minolta. „Im Geschäftsumfeld kommen schnell vier bis fünf Anbieter für verschiedene Anforderungen zusammen. Eine unserer wichtigsten Aufgaben besteht darin, diese Instrumente zu orchestrieren und Schnittstellen für ein harmonisches Zusammenspiel zu finden." Selten sind Unternehmen zu hundert Prozent in der Cloud, so Kaspar. „Sinnvoll sind oft Hybrid-Lösungen, bei denen bestimmte Anwendungen lokal laufen."

IRRTUM 2:

Alles billiger mit der Cloud?

Cloud-Lösungen können zwar dazu beitragen, Kosten zu senken. „Viel entscheidender ist aber die Flexibilität in punkto Mobile Working, Skalierbarkeit und schnelle Reaktion auf neue Marktverhältnisse. Weitere gute Gründe sind die erhöhte Sicherheit sowie der Ausgleich von fehlendem Know-how durch externe Unterstützung", verrät Oliver Jeutner, ebenfalls Cloud-Experte bei Konica Minolta. In bestimmten Fällen können nach der Migration auch höhere Kosten anfallen als vorher. „Manche zahlen unbewusst mehrfach Lizenzen für ähnliche Dienste. Andere schließen Verträge mit ungünstigen Abrechnungsmodellen ab und sind von den Kosten überrascht." Selbst optimal auf das Unternehmen abgestimmte Cloud-Anwendungen bleiben ein Kostenfaktor – der sich aber durch Effizienz, Resilienz und optimierte Prozesse auszahlt.

MEHR WERT

Hier geht's zum Whitepaper:

it daily.net

IRRTUM 3:

Alles schneller mit der Cloud?

Der erhoffte Turbo-Effekt durch die Cloud-Migration bleibt oftmals aus. „Wenn ich Bilder oder große Dokumente in die Cloud hochlade, muss ich, je nach Bandbreite, eben eine oder zwei Sekunden länger warten", gibt Christian Kaspar zu bedenken. Der Flaschenhals ist jetzt die Internetanbindung im Büro oder Homeoffice. „Im Hintergrund kann aber vieles schneller laufen. Zum Beispiel Cloud-zu-Cloud-Prozesse wie Backups oder Datenbankabfragen. Das merke ich als Anwender aber nicht." Auch das Anzeigen eines Echtzeit-Reports kann einige Sekunden dauern – aber an anderer Stelle die Arbeit von mehreren Stunden ersparen.

Mit individueller Cloud-Strategie mehr erreichen

Was ist also die beste Strategie für die Cloud-Migration? „Das hängt ganz vom Unternehmen ab", so Jeutner. Die Experten von Konica Minolta bieten KMUs deshalb Cloud Readiness Workshops an. „Die gemeinsamen Analysen führen zu handfesten Resultaten: Technologie-Empfehlungen auf Basis der aktuellen Situation, der strategischen Ziele, der aktuellen und zukünftigen Marktlage, der Wirtschaftlichkeit und der IT-Sicherheit." Davon lässt sich ein individueller, klarer Fahrplan für die Migration ableiten – bei dessen Umsetzung die Consultants mit Rat und Tat unterstützen.

www.konicaminolta.de/cloudreadiness

KONICA MINOLTA

Kostenfalle Cloud

DIE VORTEILE EINER UMFASSENDEN IT-MANAGEMENT-LÖSUNG

30 Prozent des Cloud-Budgets werden durch ungenutzte Cloud-Ressourcen verschwendet – ein vermeidbares Problem, das aber sorgfältiges Management erfordert. Wir sprachen mit Peter Stanjeck, Managing Director der USU GmbH, über effiziente Strategien zur Cloud Cost Optimierung.

it management: *Cloud Computing und daraus entstehende Kosten stehen auf der CIO-Agenda derzeit ganz weit oben. Wie bewerten Sie das Thema?*

Peter Stanjeck: Das Management der Cloud und die Kontrolle der Cloud-Kosten zählen momentan zu den größten Herausforderungen in der IT-Welt, direkt nach dem Hype um generative AI. Wie so oft liegen jedoch Chancen und Risiken nah beieinander. Die Attraktivität der Cloud basiert auf ihrer Flexibilität und Skalierbarkeit - es ist möglich, Server in Sekundenschnelle hoch- oder runterzufahren und Ressourcen nach Bedarf zu nutzen. Daher werden bereits in zwei Jahren etwa die Hälfte aller Unternehmen ein Multi-Cloud-Modell nutzen. Aber viele Unternehmen unterschätzen derzeit noch die Kostenimplikationen. Mit der Auslagerung von Anwendungen und Servern an Hyperscaler wie Google, Microsoft und Amazon steigen die Kosten rasant an. Damit sind aktuell 80 Prozent der Unternehmen konfrontiert, denn es fehlt der Überblick, welche Kosten wo entstehen, wie sie zugeordnet und wie sie optimiert werden können

it management: *Können Sie die Problematik der explodierenden Cloud-Kosten näher erläutern?*

Peter Stanjeck: Extrem hohe Cloud-Kosten sind leider ein reales Szenario, zumal die großen Hyperscaler in den letzten Monaten kräftig an der Kostenschraube gedreht haben. Dazu kommt die ständig weiterentwickelte, kaum überschaubare Vielfalt des Service-Angebots von Cloud-Anbietern. Allein AWS hat über 350 verschiedene Server-Services im Angebot. Es ist wichtig, über neue Angebote, Preismodelle und Kostenunterschiede informiert zu bleiben, um fundierte Entscheidungen zu treffen. Aber der Mangel an Transparenz und Kontrolle ist in der Praxis ein Problem. Auf der Kostenseite fallen vor allem ungenutzte Ressourcen wie untätige Server, Datenbanken ohne Verbindung oder nicht zugewiesener Speicherplatz ins Gewicht. Laut einer Studie von Gartner sind etwa 30 Prozent der Cloud-Infrastruktur tatsächlich ungenutzte Ressourcen. Das ist ein enormes Sparpotenzial, das derzeit unangetastet bleibt. Eine aktuelle Studie von Couchbase kommt zu ähnlichen Ergebnissen: Unternehmen ab etwa 1.000 Mitarbeitenden geben pro Jahr durchschnittlich über 6 Millionen Dollar zu viel aus. Nicht nur ungenutzte, auch überdimensionierte Cloud-Ressourcen sind ein Kostenfresser. Viele Rechner sind für Peak-Zeiten dimensioniert, aber ein Großteil der Zeit langweilen sie sich.

it management: *Was gehört zu einem effektiven Cloud-Management dazu?*

Peter Stanjeck: Zunächst die Verrechnung von Cloud-Kosten. Häufig gibt es Sammelrechnungen mit kryptischen Bezeichnungen zu Servern, Datenbanken oder Netzwerk-Ressourcen, die monatlich von der Firmen-Kreditkarte abgebucht werden. Das ist eine Blackbox und ohne weiteres nicht zuordbar. Hierfür ist ein ausgefeiltes Cloud-Tagging unerläss-

lich. In Verbindung mit einem definierten integrierten Servicemodell lassen sich Kosten detailliert den Services zuordnen. Dies ermöglicht außerdem aktives Showback oder Chargeback – und damit eine Kostentransparenz, die auch psychologisch wertvoll ist, denn sie schärft auch in den Fachbereichen das Bewusstsein für die Kostentreiber und dafür, Ausgaben zu optimieren.

Und noch ein zweites Thema ist wichtig: Unkontrollierte Cloud-Ressourcen sind auch ein Governance-Thema. Wenn man nicht weiß, wo sich die Daten genau befinden und wer Zugriff darauf hat, ist das ein hohes Sicherheitsrisiko. Hier sind klare Richtlinien für die Cloud-Nutzung und ein aktives User-Management gefragt.

it management: *Welche Strategien und konkreten Lösungsmöglichkeiten empfehlen Sie?*

Peter Stanjeck: Aus unserer Sicht ist der Erfolgsschlüssel ein ganzheitlicher Ansatz, der strategische Planung, regelmäßige Überwachung, effektive Governance und die interdisziplinäre Zusammenarbeit in einem FinOps-Team umfasst.

Auf der operativen Seite ist eine der Maßnahmen, die sofortige Einsparungen verspricht, die Identifizierung und Deaktivierung ungenutzter Konten. Hier unterstützen Monitoring- und Alarmierungssysteme. Diese überwachen die Kapazitätsparameter der Cloud Services über die komplette hybride Infrastruktur und melden auf Basis definierter Schwellwerte automatisiert, wenn Cloud-Systeme „betriebsbereit, aber untätig" sind.

Für die Software-Nutzung kommen entsprechende aktive Software Asset Management-Tools zum Einsatz. Weist ein Anwendungsabonnement keine Nutzung auf, wird es dem zugewiesenen Mitarbeiter entzogen und entweder jemandem zugewiesen, der es benötigt, oder deaktiviert. Wir haben im Rahmen der jüngsten Kundenprojekte alleine für Microsoft Office 365 Kosteneinsparungen zwischen 7 und 22 Prozent für ungenutzte Konten realisiert. Das sind bei großen Unternehmen bis zu siebenstellige Beträge pro Jahr.

Ein weiterer Hebel zur Kostenoptimierung ist das Maßschneidern von Cloud-Abonnements.

Viele Anwender haben ein MS 365 E3-Abonnement, nutzen jedoch nur Exchange für die E-Mails. Hierfür reicht die weitaus günstigere E1-Lizenz aus. Und nur ein kleiner Teil der Belegschaft benötigt normalerweise eine E5-Lizenz mit erweiterten Sicherheitsfunktionen. In die gleiche Richtung geht auch die Konsolidierung von redundanten Anwendungen, die den gleichen Zweck erfüllen.

it management: *Wie können die vergleichsweise hohen Betriebssystem- und Datenbankkosten in der Cloud reduziert werden?*

Peter Stanjeck: In der Tat – hier lohnt der Blick auf installierte Software mit „Bring Your Own License" (BYOL) -Rechten. Beispielsweise können Kunden mit Oracle BYOL ihre vorhandenen On-Premises-Lizenzen mit 100prozentiger Workload-Garantie und Lizenzmobilität auch in der Cloud einsetzen. Im Falle von SQL-Datenbanken lassen sich auf diese Weise zum Beispiel jedes Jahr 37 Prozent der Lizenzkosten einsparen.

it management: *Worauf sollten Unternehmen bei der Auswahl einer Cloud-Kostenmanagementlösung achten?*

Peter Stanjeck: Die Komplexität des Themas erfordert eine interdisziplinäre Herangehensweise, welche die kaufmännische und technische Welt verknüpft. Ein effektives Cloud Management benötigt das Zusammenspiel mehrerer Disziplinen wie etwa Service Request, Monitoring, Lizenzmanagement oder Compliance. Ein Anbieter sollte über langjährige Erfahrung im IT-Controlling und ein integriertes Lösungspaket verfügen.

EINE GUTE LÖSUNG UNTERSTÜTZT DIE BUDGETPLANUNG, DIE ÜBERPRÜFUNG UND ANPASSUNG VON VERTRÄGEN, DAS DURCHSETZEN VON GOVERNANCE-REGELN UND BIETET MANAGED SERVICES AN.

Peter Stanjeck,
Managing Director, USU GmbH,
www.usu.com

Eine gute Lösung unterstützt auch die Budgetplanung, die Überprüfung und Anpassung von Verträgen, das Durchsetzen von Governance-Regeln und bietet Managed Services an, um den Kunden bei der Nutzung von Einsparpotenzialen zu unterstützen. Ein transparenter 360-Grad-Blick auf die komplette hybride IT-Infrastruktur bildet die Basis für eine genaue Kostenallokation auf Kostenstellen, Projekte und Services. Damit verwalten Unternehmen ihre Ausgaben effizient und ziehen den vollen Nutzen aus der Cloud-Technologie.

it management: *Herr Stanjeck, wir danken für das Gespräch.*

THANK YOU

IT Service Management

DIE WARTUNGSPLANUNG INTEGRIEREN

Für einen reibungslosen Betrieb muss so gut wie jedes Unternehmen und jede Organisation regelmäßig ihr Equipment warten. Die Bandbreite reicht von ganzen Gebäuden und Anlagen über Werkzeuge und Geräte bis hin zu IT-Systemen. Ein digitaler Helfer kann da ziemlich hilfreich sein. Das dachten sich auch die Entwickler von KIX Service Software. Für ihre Open Source ITSM-Software KIX haben sie nun das Add-on Maintenance Plan veröffentlicht. Für den Einsatz einer professionellen und ins Servicemanagement integrierten Wartungsplanung gibt es einige gute Gründe.

#1 Weniger Fehler und Ausfallzeiten

Technische Probleme lassen sich nie restlos ausschließen. Durch regelmäßige Wartungen können Servicemitarbeiter Fehler aber frühzeitig erkennen und beheben, bevor es womöglich zu einem kompletten Ausfall kommt. Vor allem eine automatisierte und durchdachte Wartungsplanung reduziert die Stillstände spürbar.

#2 Längere Lebensdauer

Ein gut geölter Wagen bringt seinen Fahrer über tausende Kilometer sicher ans Ziel. Und diese Weisheit lässt sich auch auf andere Bereiche übertragen. Technische Geräte und Anlagen haben nachweislich einen längeren Lebenszyklus, wenn sie regelmäßig gewartet werden. Und das optimiert schließlich den Einsatz und trägt zur Wirtschaftlichkeit von Unternehmen bei.

#3 Weniger Nachkauf, weniger Kosten

Reparaturen, Ersatzteile und neue Anschaffungen können ziemlich schnell die Kosten in die Höhe treiben. Im schlimmsten Fall müssen ganze Systeme, Maschinen oder Anlagen ersetzt werden. Besonders ärgerlich, wenn es um teure Sonderanfertigungen geht. Eine professionelle Wartungsplanung kann dies verhindern und zu erheblichen Kosteneinsparungen führen.

#4 Zufriedene Kunden

Stillstände tun nicht nur Unternehmen weh, sondern können sich auch auf längere Sicht negativ auf Kundenbeziehungen auswirken. Instandhaltungen und Wartungen gehören zu den essentiellen Serviceaufgaben, die die gesamte Qualität der Produkte, Abläufe und Dienstleistungen beeinflussen. Sollte es zu eigentlich vermeidbaren Problemen kommen, gerät die Kundenzufriedenheit in Gefahr.

#5 Die Vorgaben erfüllen

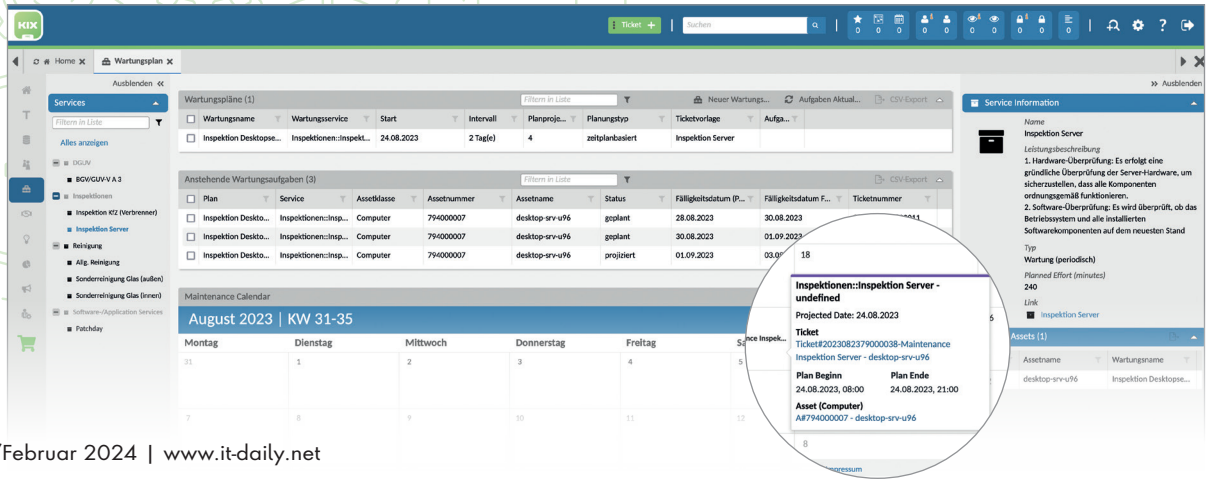
Alle Einrichtungen müssen ihr Equipment regelmäßig prüfen und warten. Mal ist es nur die jährliche Prüfung sogenannter elektrischer Betriebsmittel, die die Deutsche Gesetzliche Unfallversicherung vorgibt (DGUV V3). Mal geht es aber auch darum, verschiedene Standards wie eine ISO 27001-Zertifizierung oder DIN 31051 zu erreichen. In jedem Fall kommt kein Unternehmen und keine Organisation an ihren Wartungsaufgaben vorbei.

Digitale Wartungsplanung

Tools wie das KIX-Add-on Maintenance Plan sind für Serviceteams eine große Unterstützung, weil sie das Ticket-, Asset- und Wartungsmanagement in einer Lösung kombinieren. Die Mitarbeiter haben damit alle Wartungsaufträge in einer Kalenderdarstellung im Blick und können auf die dazugehörige Ticket-Kommunikation zugreifen. Sämtliche Arbeitsschritte, festgestellte Mängel und etwaige Zusatzaufträge werden im System dokumentiert, sodass sich auch andere Kollegen zu einem späteren Zeitpunkt schnell einarbeiten können. Durch individuelle Konfigurationsmöglichkeiten gibt es beim Einsatz quasi keine Beschränkungen – sei es in der Verwaltung oder auch im mobilen Field Service bei weitläufigen Anlagen.

Wartungsarbeiten sind nervig und zeitraubend, ohne sie geht es aber nicht. Zeitgemäße Mittel wie eine digitale Wartungsplanung schaffen aber Abhilfe. Mit ihnen wird die Arbeit ein deutliches Stück angenehmer.

www.kixdesk.com



ITSM 2024

WAS SIND DIE TOP 4-TRENDS?

Welche ITSM-Trends und Entwicklungen erwarten uns 2024? Und wie werden sie Ihre Arbeitsweise beeinflussen? Renske van der Heide, Head of Strategy and Innovation bei TOPdesk, teilt ihre Erkenntnisse.

#1 ITSM-Trend: KI-Applikationen haben inzwischen echte Auswirkungen

Künstliche Intelligenz wird zunehmend zum Standard in ITSM-Lösungen. Von automatischer Ticketweiterleitung bis zur Nutzung von ChatGPT für Textfelder in Incidentkarten – IT-Fachleute erwarten, dass Softwareanbieter KI integrieren. Die Entwicklung von KI-Anwendungen geht weg von netten Spielereien hin zu echter Hilfe, indem sie Meldern und Bearbeitern effektiv Antworten liefern, im Gegensatz zu früheren Chatbot-Erfahrungen.

Obwohl die Vorteile derzeit begrenzt sind, könnte KI langfristig eine enorme Hilfe für IT-Abteilungen sein. Die automatisierte Bearbeitung repetitiver Verwaltungsaufgaben wie Ticket-Registrierung und -Bearbeitung könnte in Zukunft durch künstliche Intelligenz unterstützt werden, was den Arbeitsablauf verbessern würde.

#2 ITSM-Trend: Erhöhte Anforderungen an die Benutzerfreundlichkeit

IT-Teams stehen vor wachsenden Erwartungen an die Benutzerfreundlichkeit ihrer Software. Privat genutzte Apps setzen jedes Jahr neue Maßstäbe für nahtlose Nutzererfahrungen, und diese Erwartung überträgt sich auf Unternehmenssoftware. Fehlt es an diesem Erlebnis, neigen Kollegen dazu, nach einfacheren Alternativen zu suchen, was die sorgfältig ausgewählten Tools der Organisation gefährdet.

Zusätzlich gewinnt Barrierefreiheit an Bedeutung, angetrieben von der Vielfalt in der Belegschaft. Organisationen setzen vermehrt auf barrierefreie Software, damit sie auch von Menschen genutzt werden kann, die beispielsweise farbenblind sind oder Lese-Schwierigkeiten haben, unterstützt durch Richtlinien wie die WCAG 2.1.

#3 ITSM-Trend: Fokus auf dem Mehrwert

Moderne IT-Abteilungen streben nicht nur danach, IT-Infrastrukturen zu warten, sondern primär Mehrwert für ihre Nutzer zu generieren. Diese Fokussierung hat zwei Hauptursachen.

Zum einen hat ITIL 4 das Konzept des „Mehrwertes" im ITSM populär gemacht, indem es von prozessorientierten Ansätzen zu einer starken Betonung der Wertschöpfung für die Nutzer überging. Dies bedeutet, herauszufinden, was für sie wirklich wichtig ist und dies gezielt umzusetzen.

Der andere Grund liegt in der steigenden Erwartung, den Wert der IT-Abteilung nachweisbar zu machen, insbesondere angesichts wirtschaftlicher Herausforderungen wie Inflation und dem Druck, die Effizienz zu steigern. Ein solcher Nachweis stärkt Ihre Argumente bei anstehenden Budgetgesprächen erheblich.

#4 ITSM-Trend: Service-Flux - klein anfangen, iterieren und pragmatisch sein

Die Herangehensweise von IT-Abteilungen an Projekte verändert sich: weg von großen, starren Implementierungen hin zu einem iterativen Ansatz, den wir bei TOPdesk als „Service Flux" bezeichnen. Dieses Konzept betont fortlaufende Veränderungen, beginnend mit geringem Aufwand und hoher Wirkung, anstatt perfekte Ergebnisse beim ersten Mal zu erzielen.

Ein Beispiel hierfür ist der „Knowledge Centered Service" (KCS). Statt einer umfassenden Wissensdatenbank von Anfang an, startet man klein und lässt das Wissen stetig wachsen, indem man allen Mitarbeitern ermöglicht, kontinuierlich Einträge zu erstellen und zu verbessern. Diese schrittweise Vorgehensweise im Alltag erweist sich als effizienter als ein großes Projekt.

www.topdesk.com

IT Service Management 2024

DIE ACHT WICHTIGSTEN TRENDS

Mit der fortschreitenden Digitalisierung und dem anhaltenden Homeoffice-Trend verändern sich die Anforderungen an das IT-Service-Management. Gleichzeitig stehen die Unternehmen unter wachsendem Druck durch globale Herausforderungen wie Lieferkettenprobleme, Inflation und Rezession. Um die Produktivität ihrer IT-Abteilungen zu erhöhen, benötigen sie Lösungen, mit denen sich Prozesse optimieren lassen. In welche Richtung werden sich IT-Service- und Asset-Management-Lösungen und Unified-Endpoint- und Digital-Workspace-Management entwickeln?

Generative KI optimiert den Helpdesk

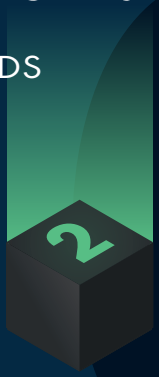
Künstliche Intelligenz (KI) ist seit gut einem Jahr der Trend schlechthin. Im Helpdesk bietet KI als Technologie durch die Verknüpfung verschiedener Fähigkeiten enormes Potenzial. Liegen zu einer Anfrage bereits Antworten aus früheren Tickets vor, kann der Serviceagent diese für die Bearbeitung über die Knowledge Base der IT-Abteilung nutzen. Auf diese Weise lässt sich mit KI bereits ein großer Teil der Serviceanfragen automatisiert beantworten.

Bei der Ticket-Bearbeitung im Self-Service hilft KI auf diese Weise, die Zahl der einfachen Tickets zu reduzieren und die Effizienz ihrer Bearbeitung zu steigern. Der Nutzer landet mit seinem Problem nicht beim First-Level-Support. Über das Self-Service-Portal erhält er sofort eine Lösung. Das steigert die Zufriedenheit der Nutzer und die Mitarbeiterbindung: Ein Helpdesk-Mitarbeiter, der ständig mit Standardanfragen zu tun hat, wird sich unter Umständen auf absehbare Zeit einen neuen, interessanteren Job suchen. Werden die einfachen Aufgaben dagegen automatisiert erledigt, müssen die Serviceagenten nur noch die komplexeren, anspruchsvolleren Anfragen bearbeiten.

Immer häufiger werden Knowledge-Base-Artikel von Generativer KI verfasst, was die technikaffinen Serviceagenten entlastet. Eine KI kann die Texte so schreiben, dass auch weniger technisch versierte Anwender sie verstehen. Wichtig ist allerdings, dass KI-generierte Artikel anschließend von einem Fachexperten gründlich geprüft und gegebenenfalls angepasst werden.

BEI DER TICKET-BEARBEITUNG IM SELF-SERVICE HILFT KI, DIE ZAHL DER EINFACHEN TICKETS ZU REDUZIEREN UND DIE EFFIZIENZ ZU STEIGERN.

Horst Droege,
Chief Product Architect, Matrix42 GmbH,
www.matrix42.com



Conversational AI: Chatbots werden schlauer

Durch den Einsatz von Conversational AI verändert sich die Suche nach Wissen grundlegend. Die Eingabe eines Begriffs in eine Suchmaschine ist bald überholt. Künftig werden die Anwender mit Chatbots interagieren, die ihnen eine optimale Antwort liefern und Suchmaschinen auf absehbare Zeit obsolet machen.

Auch im Helpdesk wird Conversational AI künftig verstärkt eingesetzt – indem sie dem Endanwender eine Antwort auf seine Fragen liefert. User können ihre Probleme genauso schildern, wie sie es einem Menschen gegenüber tun würden. Der Chatbot liefert dann sofort eine Lösung oder stellt weitere Fragen, um das Problem einzugrenzen und an einen Serviceagenten weiterzuleiten. Das optimiert und beschleunigt die Bearbeitung von IT-Problemen und sorgt für eine bessere Nutzererfahrung.

Verbesserung der Digital Employee Experience

Um Mitarbeiter bei der IT-Nutzung zu unterstützen, werden Unternehmen künftig verstärkt auf eine bessere Digital Employee Experience (DEX) achten. Eine effektive Möglichkeit bietet die Auswertung der Telemetriedaten der verwendeten Endge-

ANHAND VON TELEMETRIEDATEN LASSEN SICH POTENZIELLE PROBLEME PROAKTIV ERKENNEN UND GEGENMASSNAHMEN ERGREIFEN, OHNE DASS DIE NUTZER DAS PROBLEM ÜBERHAUPT WAHRNEHMEN.

Klaus Ziegerhofer, Product Manager Enterprise Service Management, Matrix42 GmbH, www.matrix42.com

räte. Anhand dieser Daten lassen sich potenzielle Probleme proaktiv erkennen und Zusammenhänge aufzeigen, die außerhalb der jeweiligen Anwendung liegen. Ist beispielsweise in einer bestimmten Nutzergruppe die Prozessorlast besonders hoch, liefern die Telemetriedaten entsprechende Gründe dafür – etwa, dass die jeweiligen Mitarbeiter eine bestimmte Software nutzen oder dass Systemeinstellungen verändert wurden. Die IT-Abteilung kann dann entsprechende Gegenmaßnahmen ergreifen, ohne dass die Nutzer das Problem überhaupt wahrgenommen haben.

Integration des Helpdesks ins Collaboration-Tool

Eine weitere Entwicklung, die die Matrix42-Experten im IT-Service-Management sehen, ist die Integration des Helpdesks in Collaboration-Tools wie MS Teams oder Slack. Das bislang übliche Verfahren, ein Ticket via E-Mail oder über ein Helpdesk-Portal zu eröffnen, hat auf absehbare Zeit ausgedient.

Desktop as a Service vermeidet Oversizing

Auch die Nutzung virtueller Desktops wird weiter zunehmen. Alle benötigten Anwendungen werden im eigenen Rechenzentrum gehostet. Künftig werden die Desktops zudem immer häufiger komplett auf dem Server oder in der Cloud liegen. Das bietet sich beispielsweise bei temporären Beschäftigungsverhältnissen oder wechselnden Projekten an. Zeitarbeiter nutzen ihre eigene Hardware und erhalten für die Dauer ihrer Beschäftigung einen Zugang zur Cloud. Der Vorteil: Dem Kunden entstehen keinerlei Infrastrukturkosten, er zahlt nur die Mietgebühr für die Dauer der Nutzung und vermeidet Oversizing.

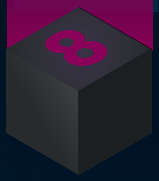
Für die Verwaltung von Prozessen, Berechtigungen und Kosten ist der Cloud-Kunde allerdings nach wie vor verantwortlich. Unterstützung dabei bieten IT-Servicemanagement-Systeme, mit denen sich Berechtigungen und Verantwortlichkeiten einzelner Mitarbeiter klar regeln lassen.

Cloud Computing setzt sich auch in Deutschland durch

Mittlerweile hat sich die Cloud auch in Deutschland weitgehend etabliert. Ein Grund dafür sind vor allem die verbesserten Angebote. Hinzu kommt, dass immer mehr Unternehmen positive Erfahrungen mit der Cloud gesammelt haben, unter anderem, weil manche Anwendungen nur in der Cloud verfügbar sind. Und schließlich sind die rechtlichen und regulatorischen Rahmenbedingungen nicht mehr so komplex wie früher.

Digitale Transformation bleibt beherrschendes Thema

Auch wenn die meisten Unternehmen schon seit Jahren daran arbeiten, bleibt der Trend zur Digitalisierung nach wie vor ungebrochen. Die Gründe, weshalb die digitale Transformation vielerorts noch nicht abgeschlossen ist, liegen häufig in knappen Ressourcen im IT-Bereich, Compliance-Herausforderungen, aber auch im Widerstand der Mitarbeiter. Gerade in Großunternehmen sind auch viele Entscheidungsträger an der Freigabe und Umsetzung beteiligt. Das verlangsamt den Prozess.



Nachhaltigkeit gewinnt weiter an Bedeutung

Kunden fragen immer häufiger nach umweltverträglichen Produkten und Dienstleistungen. Dabei geht es nicht nur um energieeffiziente Hardware sowie deren nachhaltige Beschaffung und Entsorgung. Auch Softwarelösungen können durch eine energieeffiziente Programmierung erhebliche Ressourcen einsparen. Dieser Weg ist für viele Hersteller noch zu gehen, denn vor allem KI-gestützte Systeme beanspruchen noch relativ viel Rechenleistung.

Fazit

Künstliche Intelligenz, die Verbesserung der Digital Employee Experience und Desktop as a Service: Neue Technologien und Nutzungsmodelle verändern das IT-Service-Management. Während der anhaltende Trend zum Cloud Computing das Leben für die IT-Verantwortlichen einfacher macht, sind Themen wie die digitale Transformation und nachhaltige Konzepte noch vielerorts eine Herausforderung.

Horst Droege, Klaus Ziegerhofer

IT-Organisation 2025

IT UND BUSINESS VERSCHMELZEN ZUNEHMEND

Die Studie „IT-Organisation 2025: Product & Data Driven" von kobaltblau untersucht die mögliche Verschmelzung von Business und IT, getrieben durch Produkt- und Kundenorientierung sowie Data Analytics für die Entscheidungsfindung. Sie beleuchtet die aktuellen Herausforderungen und Trends der Transformation von IT-Organisationen. Mit einer verstärkten Ausrichtung auf Produkte gehen auch Change-Prozesse für alle Beteiligten einher.

Die Studie zeigt anhand einer branchenübergreifenden Befragung von Top-Entscheidern aus über 100 Unternehmen, wie sich die Zusammenarbeit zwischen Business und IT in den kommenden Jahren entwickeln könnte und welche Faktoren dabei eine entscheidende Rolle spielen. Mehr als die Hälfte der Befragten (56 %) zählt das Zusammenarbeitsmodell zwischen Business und IT als eines ihrer zentralen Handlungsfelder auf. Zwar steht es in der Rangfolge hinter den Handlungsfeldern Cybersecurity (70 %) und Modernisierung der IT (61 %). Eine optimierte Organisation zwischen Geschäfts- und IT-Tätigkeiten kann jedoch auf sie einzahlen. Das gewählte Zusammenarbeitsmodell birgt durchaus Relevanz für viele andere Handlungsfelder der IT.

Der präferierte Grad an Symbiose

Die Studie arbeitet fünf verschiedene Modelle zwischen Business und IT heraus, die einen unterschiedlichen Verschmelzungsgrad aufweisen. Am weitesten gehen die Modelle der Plattform IT mit 75 Prozent Verschmelzung sowie Integrierte IT mit 100-prozentiger Integration von Business und IT. Bei der Plattform IT realisieren immer mehr Unternehmen bereits eine teilweise Zusammenführung von IT und Business. Dabei zerfällt die IT-Organisation in zwei Teile: Im ersten verschmelzen IT und Business zu gemeinsamen, vollintegrierten End-to-End-Produktteams, während der andere Teil als eigenständige IT-Einheit (Foundational IT) bestehen bleibt und zusammen mit externen Dienstleistern die geeignete Infrastruktur als flexible (Cloud-)Plattform betreibt. Von großer Bedeutung sind klare Rollen und Verantwortlichkeiten sowie die Ausrichtung auf Produkte und Services. Zwar haben erst vier Prozent der Befragten sie realisiert, aber die Mehrheit (57 %) sieht die Plattform IT als präferiertes Modell für die Zukunft. Mit Blick auf den Transformationsprozess hebt mehr als die Hälfte (55 %) den unterschiedlichen Reifegrad von IT und Business als Herausforderung hervor. So gilt es nicht nur, das Zusammenarbeitsmodell selbst zu entwickeln, sondern die unterschiedliche Ausgangslage einzelner Bereiche und Teams zu berücksichtigen.

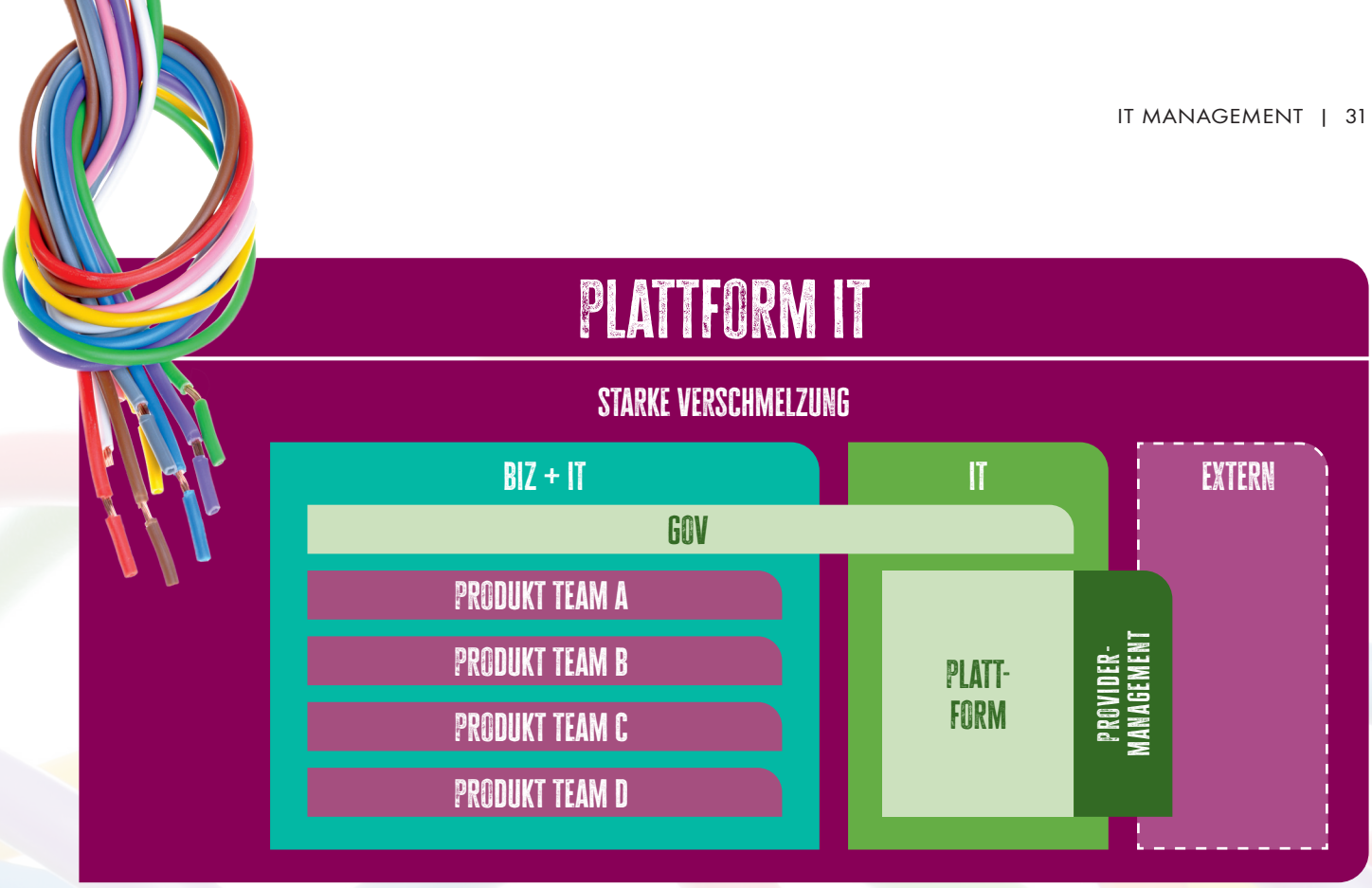
Produktorientierung in Business und IT

Die Studie zeigt zudem, dass Produktorientierung in Business und IT für Unternehmen zunehmend an Bedeutung gewinnt. 68 Prozent der Befragten sehen Produktteams, die aus einem stabilen Kernteam bestehen und bedarfsorientiert durch virtuell zugeordnete Mitarbeitende ergänzt werden, als ideal an. Diese Teams werden in „Communities of Practice" eingebettet, um Standards und Vorgehensweisen einzuhalten und den Wissenstransfer zu gewährleisten. Für die Funktionen Business Prozess Management (47 %), Application Design (47 %) und Governance (51 %) zeigt sich ebenfalls eine verstärkte Tendenz zu integrierter Verantwortung. Während Application Design und Governance auch von der Hälfte der Unternehmen in der IT-Verantwortung gesehen werden, liegt das Business Prozess Management traditionell eher in der Business-Verantwortung.

Bei den Funktionen Demand Management (59 %) und Projekt Portfolio Management (76 %) sieht die Mehrheit eine integrierte Verantwortung von Business und IT. Deshalb wird sich voraussichtlich die Rolle des Demand Managers verändern. In der Vergangenheit war dieser oft Vermittler zwischen Business und IT. In Zukunft könnte er eine aktivere Rolle bei der Gestaltung und Umsetzung von produktfernen oder produktübergreifenden IT-Projekten übernehmen. Klare pro-

DIE VERSCHMELZUNG VON BUSINESS UND IT IST ERFOLGSKRITISCH UND DIE IT-ORGANISATIONEN MÜSSEN SICH AKTIV MIT DIESEM THEMA AUSEINANDERSETZEN.

Thomas Heinevetter, Geschäftsführer, kobaltblau management consultants GmbH, www.kobaltblau.de



duktbezogene Anforderungen hingegen adressieren der Product Owner oder andere Teamrollen direkt im Produktteam. 42 Prozent geben an, dass die Rolle des Demand Managers in Zukunft sogar vollständig durch den Product Owner ersetzt wird.

Data-Driven verändert das Entscheidungsverhalten

Hier zeigt sich die starke Tendenz zu Veränderung und Wegfall sowie Aufwertung von bekannten Rollen. Zudem sehen die Teilnehmenden neue Rollen am Horizont aufziehen, die für eine integrierte Business- und IT-Organisation von großer Bedeutung sein werden. Etwa 75 Prozent der Befragten sehen den Bedarf an neuen Rollen, die die Verantwortung für businessgetriebene Daten Use Cases sowie den Aufbau von Daten-Ökosystemen übernehmen. Je größer die Unternehmen sind, desto eher gelten Daten-Ökosysteme aufgrund der exponentiell steigenden Datenkomplexität als Priorität.

Welchen Einfluss Data-Driven auf den Businesserfolg haben kann, zeigt die Zustimmung von 70 Prozent zu folgender Aussage: „Data-Driven verändert das Entscheidungsverhalten, weg von persönlichen Erfahrungen hin zu datenbasierten Entscheidungen". Bei der Frage, wie man sich Data-Driven organisiert, gibt es keine eindeutigen Tendenzen. Die Hälfte der Befragten stimmt zu, eine eigene Data-Einheit und zentrale Bereitstellung von Daten umsetzen zu wollen. Größere Unternehmen sehen dies aufgrund der Menge und Komplexität wiederum als nicht zentralisierbar. Die Regelung der Verantwortlichkeiten ist dabei ein wichtiger Schritt auf dem Weg zu einer Data-Driven Organisation.

Evolutionärer Transformationsprozess

Natürlich gibt es keines dieser Organisationsszenarien in Reinkultur. Auch weiterhin wird es zahlreiche unternehmensindividuelle Organisationsmodelle geben. Es ist aber deutlich, dass sich rund 80 Prozent der Befragten aktuell mit der Transformation zu einer Product-Driven (PDO) oder Data-Driven Organisation (DDO) beschäftigen. Zudem verändern sich etablierte Rollen und erfordern zusätzliche Skills der Mitarbeitenden. Etwas mehr als ein Jahr nach der Veröffentlichung von ChatGPT erleben wir aktuell, dass die hochdynamische Entwicklung von generativen KI-Anwendungen zunehmend mit neuen Aufgaben wie Prompt Engineering einhergeht.

Vor allem aber ist der Schritt in die Umsetzung von PDO- und DDO-Strategien für viele Unternehmen noch die größte Hürde. Erst 18 Prozent haben ein Konzept zur PDO erfolgreich eingeführt, bei DDO sind es sogar nur fünf Prozent. Personelle Ressourcen (66 %), der bereits erwähnte Unterschied im Reifegrad von IT und Business sowie unklare Visionen und Ziele der Transformation (51 %) bremsen die Vorhaben. Hinzu kommt, dass sich bislang nur jede zweite Führungskraft für den anstehenden Change bereit fühlt. Sie verstehen zwar die Notwendigkeit (44 %), nur jeder Fünfte sieht bei den Führungskräften die erforderliche Kompetenz, Veränderungen zu begleiten und zu managen. Vielleicht auch deshalb favorisieren 75 Prozent der Befragten einen iterativen und evolutionären Ansatz. Sie wollen lieber mit Pilotprojekten in einzelnen Bereichen starten, anstatt einen schwer zu stemmenden „Big Bang" zu realisieren.

Klar ist: Die Verschmelzung von Business und IT ist erfolgskritisch und die IT-Organisationen müssen sich aktiv mit diesem Thema auseinandersetzen. Die Transformation ist unausweichlich. Es stellt sich nicht die Frage nach dem Ob, sondern nur nach dem Wie!

Thomas Heinevetter

DIGITALE TECHNOLOGIE IM GLOBALEN WANDEL

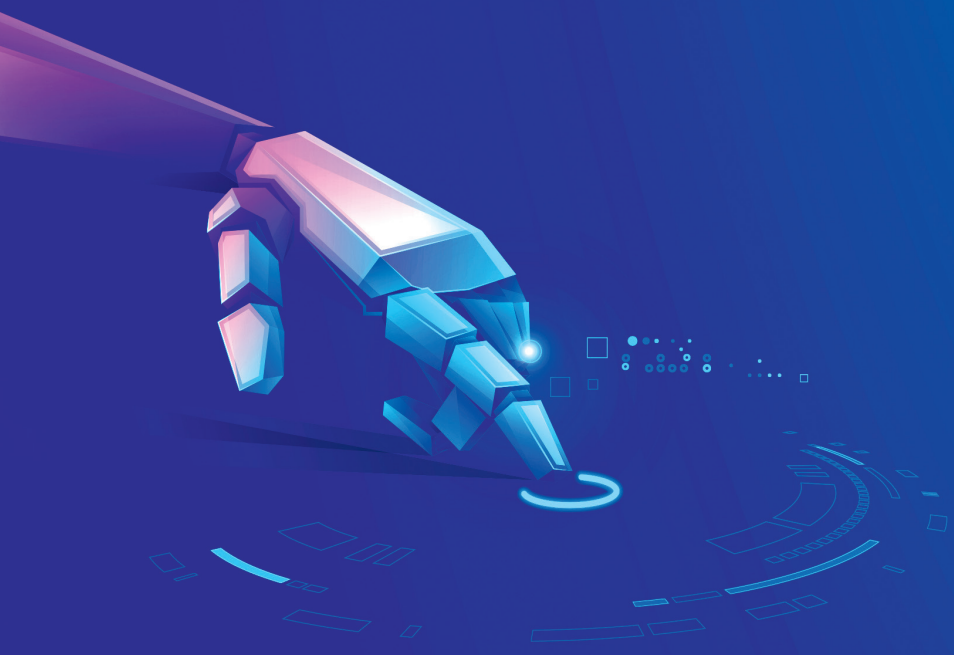
CHANCEN EINER SICH SCHNELL VERÄNDERNDEN WELT NUTZEN

Unsere Welt durchlebt eine dramatische Phase des Wandels. Wir alle stehen vor erheblichen Herausforderungen in Bezug auf Umwelt und Gesellschaft. Vom Klimawandel über den Verlust biologischer Vielfalt bis hin zu Ressourcenknappheit – die natürliche Umwelt und die von uns geschaffene Welt sind durch unseren Lebensstil und die Art und Weise bedroht, wie die Menschheit expandiert und sich weiterentwickelt. Deshalb müssen wir Veränderungen herbeiführen.

In diesem eBook greifen wir einige der wichtigsten Herausforderungen auf, vor denen die Weltbevölkerung steht. Welche Rolle spielen Unternehmen in diesem Zusammenhang? Wie kann der intelligente Einsatz von Technologie uns alle auf dem Weg in eine positivere Zukunft unterstützen?

INHALT:

1. Die zunehmende Bedrohung durch Cyberangriffe und -kriege
2. Neue Technologien und Softwaresysteme
3. Der Einzug der Generation Z in den Arbeitsmarkt
4. Die Klimakrise
5. Zunehmende Globalisierung
6. Digitale Verantwortung und die Einbeziehung von Mitarbeitern



Das **eBook** umfasst 33 Seiten und steht zum kostenlosen Download bereit.
www.it-daily.net/download

UC-Tools für Digital Workplaces

UNIFIED-COMMUNICATIONS-LÖSUNGEN SPIELEN EINE TRAGENDE ROLLE FÜR DEN „ARBEITSPLATZ DER ZUKUNFT"

Vier Prozent mehr Produktivität bescheinigen Wirtschaftsvertreter Arbeitnehmern in einem hybriden Arbeitsumfeld und begründen dies mit einer verbesserten Mitarbeiterzufriedenheit und dem geringeren Zeitaufwand für das Pendeln. Der Produktivitätszuwachs könnte der europäischen Wirtschaft zusätzliche 113 Milliarden Euro im Vergleich zu Arbeitsmodellen vor der Pandemie einbringen. Genutzt wird dieses Potenzial laut einer Studie von Ricoh Europe jedoch nicht.

So hat nur rund die Hälfte der Unternehmen überhaupt hybride Arbeitsmodelle eingeführt. Darüber hinaus sprechen sich 52 Prozent der Führungskräfte für eine vollständige Rückkehr der Mitarbeiter ins Büro aus, obwohl 78 Prozent der Arbeitnehmer eine Form des hybriden Arbeitens der reinen Heim- oder Büroarbeit vorziehen. Arbeitgeber, die den potenziellen Produktivitätszuwachs durch Hybrid Work ignorieren, riskieren dadurch das Einbremsen zukünftigen Wachstums und schwächen ihre Wettbewerbsfähigkeit.

Die Basis für den Digital Workplace

Umsetzung hybrider Arbeitsplatz-Konzepte aus mobilem, halbmobilem und bürobasiertem Arbeiten scheitert oft an den richtigen Tools und Technologien, die eine effiziente Kommunikation zwischen Kollegen im Büro und zu Hause ermöglichen. Zwar arbeiten viele Mitarbeiter mit Notebook und Docking-Station. Allerdings ist ihr Präsenzstatus im Homeoffice nicht ersichtlich, wodurch eine Zusammenarbeit im Team erschwert wird. Zudem steht im Büro oftmals noch ein Festnetztelefon, das nicht selten aufs private Handy umgeleitet wird – keine Dauerlösung.

Für die professionelle Ausstattung der Mitarbeiter im Homeoffice und den Erhalt des Teamgefüges können Unified-Communications-Lösungen eine tragende Rolle spielen. Es geht darum, die richtigen Technologien einzusetzen, um den vielbeschriebenen „Arbeitsplatz der Zukunft" Wirklichkeit werden zu lassen. Folgende Tools stehen dabei im Vordergrund:

#1 Softphone

Tischtelefon ade. Das Softphone ist ein softwarebasiertes Telefon, das über den Computer genutzt wird. Mitarbeiter sind damit immer unter ihrer Festnetz-Durchwahl erreichbar, und dem Geschäftspartner wird mit der One-Number-Funktion ausschließlich die Büronummer angezeigt – egal, ob ein Mitarbeiter im Homeoffice, Hotel oder unterwegs ist.

#2 Hotline-Management

Erreichbarkeit ist im Kundenservice entscheidend. Mit einem intelligenten Call-Routing werden Anrufe auf ein Team verteilt. Optimal ist es, wenn das Hotline-Management-System und die Telefonie Hand in Hand gehen und in einem Client integriert sind. Dies ist zum Beispiel bei der UC-Lösung XPhone Connect der Fall. Mitarbeiter können so von überall aus in der Hotline mitarbeiten.

#3 AnyDevice

Telefonieren mit dem privaten Festnetztelefon, aber unter der geschäftlichen Nummer – das funktioniert. UC-Lösungen wie XPhone bieten hierfür die Funktion „AnyDevice": Jedes Telefon – ob Mobil oder Festnetz – kann mit dem UC-Client gesteuert werden, alle CTI-Funktionen wie Weiterleiten oder Makeln inklusive. Das Gespräch wird über ein Callback aufgebaut, sodass die privaten und geschäftlichen Telefonkosten sauber getrennt sind.

#4 Mobile App

Je flexibler der Arbeitsplatz, desto flexibler müssen Kommunikations-Tools sein. Volle Flexibilität bieten mobile Apps. Mit dem Softphone in der App telefonieren Mitarbeiter weltweit im WLAN oder Mobilfunknetz so, als wären sie im Büro: inklusive Firmen-Durchwahl, integrierten Kontakten und Präsenzstatus der Kollegen.

Judith Beck | www.c4b.com

Digitalisierungs-Booster

KEINE DIGITALISIERUNG OHNE UNIFIED COMMUNICATIONS

Marktforscher und Analysten verschiedenster Institute sind sich einig: der weltweite Markt für Unified Communication and Collaboration (UCC) wird weiter wachsen. Dafür sind im Wesentlichen drei Faktoren verantwortlich: Homeoffice ist gekommen, um zu bleiben. Außerdem ist es mittlerweile eine betriebswirtschaftliche Notwendigkeit, Kommunikationsprozesse innerhalb eines Unternehmens und zwischen Unternehmen bruchfreier und damit effizienter zu gestalten. Und drittens muss diese gesamte Kommunikation gegen Cyberangriffe abgeschirmt werden. Dass UCC-Lösungen auch aus der Cloud bezogen werden können, beflügelt das Wachstum zusätzlich.

Für das Jahr 2023 erwartete IDC gemäß seines Worldwide Quarterly Unified Communications and Collaboration Trackers einen Umsatz von 64,7 Milliarden US-Dollar für dieses Marktsegment. Das entspricht einem prognostizierten jährlichen Wachstum von 8,6 Prozent gegenüber dem Vorjahr.

Noch besser sieht das Wachstum beim Cloud-basierten Bereitstellungsmodell Communications-Platform-as-a-Service (CPaaS) aus: hier rechnet IDC für 2023 mit einer Steigerung der weltweiten Umsätze von 12,4 Prozent gegenüber dem Vorjahr auf insgesamt 15,6 Milliarden US-Dollar. Die Marktforscher von Fortune Business Insights erwarten, dass der Markt für Unified-Communications-as-a-Service bis zum Jahr 2030 auf 85,77 Milliarden Dollar anwachsen wird, was einer kontinuierlichen Steigerung von gut 15 Prozent pro Jahr entspräche. Diese Zahlen zeigen sehr eindrücklich, welche Dynamik im weltweiten Markt für UCC steckt.

Digitalisierung treibt UC-Wachstum

Wenn man nach den Ursachen für diese guten Wachstumsprognosen fragt, wird ganz schnell der Überbegriff Digitalisierung fallen. Denn letztendlich sind alle Phänomene, die das Wachstum des UCC-Markts antreiben, darauf zurückzu-

führen. Der schnelle Wechsel ins Homeoffice im Rahmen der Covid-Ausgangsbeschränkungen war für Beschäftigte in informationsverarbeitenden Unternehmen nur möglich, weil die grundlegenden Voraussetzungen, wie digitale Arbeitsplätze, Remote-Zugänge, Cloud-Software oder ausreichend schnelle Internetverbindungen schon vorhanden waren.

Hybride Arbeitswelten werden Standard

Da Homeoffice vor der Pandemie aber bei den meisten Unternehmen keine Priorität hatte, waren die unterschiedlichen Technologien nicht orchestriert. Vielfach musste zu Beginn der Lockdowns hektisch improvisiert werden, meist zu Lasten der Sicherheit oder der Nutzerfreundlichkeit. Mittlerweile hat sich das zum Teil geändert. Echte Digital Workplaces, die alle Arbeitswerkzeuge aus der Cloud bereitstellen, sind zahlreich eingeführt worden, Kommunikationstools wurden der zentralen Verwaltung unterworfen und IT-Sicherheitsvorkehrungen entsprechend erweitert. Doch auch hier ist noch Luft nach oben.

Auch im Jahre vier nach den ersten Covid-Lockdowns wird das Rad nicht mehr auf Vor-Pandemie-Zustände zurückgedreht werden: 2022 arbeitete rund ein Viertel aller Beschäftigten in Deutschland ganz oder ab und zu im Homeoffice, wie das Statistische Bundesamt (Destatis) mitteilt. Demnach nutzten 2022 8,4 Millionen das Homeoffice gelegentlich, wie die Rheinische Post vermeldete. 2,3 Millionen Menschen gingen ihrer Arbeit ausschließlich aus dem Homeoffice nach. Damit hat sich die Anzahl der Angestellten in Deutschland, die komplett aus dem Homeoffice arbeiten, zwischen den Jahren 2019 und 2022 nahezu vervierfacht.

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

Mit UCC Prozesse optimieren

Eine ideale UCC-Lösung vereint Kommunikationskanäle wie den Dokumentenaustausch, Voicemail und SMS auf einer einheitlichen Plattform und stellt dabei einen rechts- und manipulationssicheren, DSGVO-konformen Dokumentenaustausch in IP-Umgebungen sicher. Darüber hinaus lässt sie sich an Dokumenten-Management- und BPM-Systeme anbinden. Dokumente und Voicemail-Nachrichten können von allen Devices aus abgerufen und weiterverarbeitet werden. Selbst den Herausforderungen weltweit tätiger Unternehmen sind zeitgemäße UCC-Lösungen gewachsen, wenn sie den international gültigen ITU-Standard erfüllen.

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

Nahtlose Sicherheit

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

Keine Digitalisierung ohne UCC

Interessant werden UCC-Lösungen auch dadurch, dass sie sich heute über die Cloud beziehen lassen. Gerade in Zeiten fehlender IT-Fachkräfte ist es nicht nur wirtschaftlich oft sinnvoller, auf Cloud-Lösungen zurückzugreifen, sondern manchmal unvermeidbar. Denkbar ist dies beispielsweise im Bereich der Telefonie. Wird etwa die OfficeMaster Suite über Azure Marketplace bezogen, lassen sich ausgewählte Rufnummern von der Telefonanlage entkoppeln, über den Provider auf die Plattform leiten und gezielt verteilen. Der Anwender behält die Hoheit über die Anwendung, betreibt diese aber in der Cloud. Das Thema Sicherheit steht auch hier an erster Stelle: Der Austausch der Dokumente findet in einer abgesicherten Umgebung statt, die Übertragung bleibt über den gesamten Kommunikationsweg verschlüsselt. Auch die Daten selbst sind in Deutschland hinterlegt, der SIP-Trunk ist ebenfalls hier angeschlossen.

Unternehmen sollten im Rahmen ihrer Digitalisierungs-Initiativen Unified Communication and Collaboration gleich mitdenken, um Home Office technisch einwandfrei zu integrieren, Datenaustauschprozesse effizienter zu gestalten und die Sicherheit der Kommunikation zu erhöhen.

www.ferrari-electronic.de

MEHR WERT

Next Generation Document Exchange:

it-daily.net

Kleiner Schritt, große Wirkung

OFFICE 4.0 DANK SAP-SCHNITTSTELLEN

Unternehmen mit einer SAP-Umgebung haben ein großes Potenzial, administrative Prozesse in ihrem Arbeitsalltag zu optimieren. Dabei spielt ihnen der aktuelle Trend des Office 4.0 in die Hände, der unter anderem die Digitalisierung und die stärkere Vernetzung von Prozessen fördert. Einen ersten niedrigschwelligen Einstieg Richtung Office 4.0 können für Unternehmen mit SAP-Umgebung Schnittstellen sein. Sie ermöglichen eine einfache Vernetzung beispielsweise mit Office-Anwendungen und vereinfachen so administrative Arbeitsabläufe von Wissensarbeitenden.

Optimierungspotenzial

Wer administrative Aufgaben besser miteinander vernetzen möchte, muss nicht gleich in Großprojekte investieren. Eine einfache Lösung, moderne Tools zur Implementierung von Office 4.0 mit einer vorhandenen Infrastruktur zu nutzen, sind Schnittstellen. Sie dienen als Bindeglied zwischen Flexibilität und Leistungsfähigkeit der modernen Cloud-Lösungen und der Datentiefe von SAP. Nutzen Unternehmen solche Schnittstellen, haben sie die Möglichkeit, Echtzeitdaten in Office-Anwendungen wie Microsoft Teams zu migrieren und ihren Mitarbeitenden den Weg für optimierte Arbeitsabläufe und eine gesteigerte Zusammenarbeit zu ebnen. Mitarbeitende erhalten Zugriff auf aktuelle und genaue Informationen direkt in ihrer vertrauten Softwareumgebung. Indem die verschiedenen Anwendungen miteinander kommunizieren, können Daten schnell und sicher ausgetauscht werden, was wiederum zu einer reibungsloseren und effektiveren Geschäftstätigkeit führt und sogar Fehlerquoten bei der Datenübertragung minimiert.

> DIE VERBINDUNG VON OFFICE- UND CLOUD-ANWENDUNGEN MIT SAP-SYSTEMEN ERMÖGLICHT UNTERNEHMEN, PROZESSE ZU VEREINFACHEN UND SO KREATIVER ZU ARBEITEN.
>
> **Christian Tauchmann, Software Consultant, Theobald Software GmbH, www.theobald-software.com**

Vermeintlich (für Mitarbeitende) lästige Arbeiten werden durch die Bereitstellung einer vernetzten Office-Umgebung mit Schnittstellen und SAP einfacher. Ein Beispiel ist die automatisierte Erstellung von Reports aus SAP-Daten in Excel: Statt mühsamer manueller Datenkopien und -formatierungen ermöglicht die Integration von SAP-Daten eine automatisierte Berichterstellung. Das spart nicht nur Zeit, sondern minimiert auch das Risiko menschlicher Fehler. Im besten Falle ist die Schnittstelle nicht nur in der Lage, die einzelnen Softwarelösungen miteinander zu verbinden, sondern bietet darüber hinaus einen Mehrwert, beispielsweise durch Automatisierungsoptionen. Die Erstellung des besagten Reports kann dadurch automatisiert werden. Das ist effizient und ermöglicht es den Mitarbeitenden, sich auf anspruchsvollere und kreativere Aufgaben zu konzentrieren. Insgesamt ist erkennbar, dass schon ein kleiner Schritt in Richtung Office 4.0 für alle einen erheblichen Mehrwert bietet.

Bye Bye Screenshot

Ein interessanter Anwendungsfall für Office 4.0 mithilfe von SAP-Schnittstellen ist beispielsweise die Verknüpfung von SAP mit MS Teams. Teams, mit rund 270 Millionen Nutzern (Stand: 2022) der Branchenprimus unter den Kollaborationstools, ist für viele Anwender so wichtig wie das E-Mail-Postfach. Viele Kollegen und Fachabteilungen nutzen das Tool auch abteilungsübergreifend für den effizienten Austausch von Informationen. Nehmen wir einmal den Beschaffungs- und Einkaufsprozess: Ein reibungsloses Zusammenspiel zwischen Einkauf, Disposition und Verwaltung beim Umgang mit Materialstammdaten vereinfacht hier Vorgänge enorm. Es ist kein Geheimnis, dass es wichtig ist, ein Unternehmen optimal mit Material zu versorgen. Herausfordernd ist allerdings, wie zeitaufwendig das Zusammenspiel der drei Fachabteilungen mit SAP bislang ist. Zunächst muss eine Verbindung zwischen Materialstammsatz und dem zuständigen Einkäufer oder Disponenten hergestellt und verwaltet werden.

Sowohl Einkäufer und Disponenten müssen sich, wenn keine Schnittstelle genutzt wird, in SAP anmelden, die richtige Transaktion finden und manuell die Materialstammdaten abfragen, um so entsprechende Zuordnungen zu prüfen oder zu ändern. Nicht nur, dass dieser Prozess umständlich klingt, er erfordert tatsächlich spezifische Kenntnisse in SAP, um die einzelnen Schritte durchzuführen. Und, um am Ende die Daten via Kommunikationstools, wie Teams, mit Kolleginnen und Kollegen zu teilen, mussten diese entweder als Screenshot oder per Copy & Paste in die Konversation eingefügt werden.

Mit einer passenden Schnittstelle wird die Materialstammdatenpflege in SAP deutlich einfacher und vor allem zugänglicher. Dank Integrationen, wie beispielsweise von PowerApps Formularen, über die SAP-Daten übergeben werden, können alle die Einkäufergruppe und die zugehörigen Materialstammdaten aus SAP direkt und komfortabel in einer Teams Konversation anzeigen und aktualisieren. Sich in SAP einzuloggen oder eine Transaktion zu suchen wird überflüssig. Mitarbeitende haben so Zugriff auf Echtzeitdaten, ohne eine Konversation oder den Workflow zu verlassen.

Schnittstellen so individuell wie jedes Unternehmen

Doch wie starten Unternehmen bestmöglich in die Umsetzung einer Vernetzung ihres Büros? Zunächst müssen Unternehmen wissen, welche Prioritäten sie in der Vernetzung setzen wollen, und sich fragen, wie die Implementierung einer Schnittstellenlösung bestmöglich auf ihre Unternehmensziele einzahlt. Es gilt, sorgfältig zu planen, um sicherzustellen, dass die Integration die gewünschten Effekte erzielt und sich nahtlos in die Arbeitsabläufe integriert und so von Mitarbeitenden akzeptiert und letztendlich die passende Lösung ausgewählt wird. Sowohl die umfassende Planung als auch die transparente Kommunikation sind letztendlich Schlüsselkomponenten für einen erfolgreichen Implementierungsprozess. Im besten Falle suchen sich Unternehmen hierfür einen erfahrenen Partner, der sie bei der Herausforderung unterstützt, gegebenenfalls eine Schnittstellenlösung angepasst an die individuellen Herausforderungen bereitstellt und zudem Schulungen für die Mitarbeitenden bietet. Idealerweise steht eine Robotic Process Automation (RPA) Technologie zur Verfügung, um wiederkehrende, regelbasierte SAP-Transaktionen zu automatisieren, Daten in Drittsysteme zu übertragen und dann zu verarbeiten.

SAP mit Office verknüpfen – einfacher als gedacht

Die Ansprüche von Mitarbeitenden an ihre IT-Infrastruktur und an das Zusammenspiel der einzelnen Softwarekomponenten für ihre individuellen, produktiven Workflows wächst. Flexibilität und Effizienz sind nicht nur Schlagworte, die allein den Arbeitsort betreffen. SAP-Schnittstellen bieten für Unternehmen einen niedrigschwelligen Einstieg in die Umsetzung einer Office 4.0 Strategie. Die Verbindung von Office- und Cloud-Anwendungen mit SAP-Systemen ermöglicht Unternehmen, Prozesse zu vereinfachen, die Zusammenarbeit der Mitarbeitenden zu optimieren und letztlich so kreativer und intelligenter zu arbeiten.

Christian Tauchmann

Effektives SAP-Management

DATENGETRIEBENE PROZESSE FÜR SICHERHEIT UND LIZENZEN

Die IT-Sicherheit stellt heutzutage ein unverzichtbares Thema dar und ist wichtiger denn je. Angesichts der zunehmenden Komplexität der Bedrohungslage und der steigenden Anzahl von Cyber-Angriffen können die Folgen, wie Strafzahlungen und Reputationsverlust, existenzbedrohlich für Unternehmen sein. Die Sicherheit der Unternehmensdaten, die in SAP-Systemen gespeichert sind und als besonders wertvoll angesehen werden, wird häufig nicht ausreichend berücksichtigt. Die Zusammenarbeit zwischen dem Chief Information Security Officer (CISO) und den Fachbereichen ist entscheidend, um diese Herausforderung in einer unternehmensweiten IT-Sicherheitsstrategie anzugehen.

Die SAP-Welt befindet sich im Wandel durch S/4HANA Transformation, Fiori, Cloud und die Business Technologie Plattform, was zu einer stärkeren Vernetzung und zunehmender Komplexität innerhalb der IT-Landschaft führt. Jedoch fehlen oft Prozesse, Richtlinien, Ressourcen und Experten, um diesen Herausforderungen gerecht zu werden.

Eine strukturierte, datenbasierte Herangehensweise, unterstützt durch Frameworks wie NIST2.0 und vorgefertigte Inhalte wie Secure Operations Map, kann helfen. Tools wie SAP Solution Manager und SAP Enterprise Threat Detection allein lösen das Problem nicht, da es in erster Linie ein prozessuales Thema ist. Eine Experteneinschätzung und Priorisierung sowie Fokussierung auf bestimmte Kernthemen sind entscheidend, da die Zukunft datengetrieben ist.

Effektive und sichere Berechtigungen

Die Sicherheit eines SAP-Systems ist erst vollständig gewährleistet, wenn auch die SAP-Berechtigungen wirksam und bedarfsgerecht eingestellt sind. Denn jedes SAP-Anwendungsunternehmen muss sein SAP-Berechtigungskonzept an den internen und externen Compliance-Anforderungen ausrichten. Zusätzlich steuern SAP-Berechtigungen auch die Geschäftsprozesse im SAP-System. Sie definieren, welche Anwender auf welche Funktionen und Daten im SAP-System zugreifen dürfen. Die richtige Konfiguration der SAP-Berechtigungen ist dadurch essenziell, um sicherzustellen, dass Anwender nur auf die für ihre Geschäftsaufgaben relevante Funktionen und Daten zugreifen können. Nur dann können die Geschäftsprozesse im SAP-System effektiv und sicher gesteuert werden.

Die Verwaltung von SAP-Berechtigungen erfordert allerdings ein hohes Maß an technischem Verständnis für SAP-Systeme und spezifische Expertise. Diese Komplexität erfordert häufig das Hinzuziehen von Experten und Einsetzen von Tools. Doch wie kann man die hochkomplexen SAP-Berechtigungen effizient und sicher gestalten?

Transparenz ist das Stichwort. Bevor man bedarfsgerechte Zugriffsberechtigungen für sämtliche Geschäftsprozesse und Anwender definieren kann, sollte man verstehen, wie die Geschäftsprozesse ablaufen und was die Anwender im System genau tun. Ein datengetriebener Ansatz bietet hier volle Transparenz und entlastet insbesondere die IT und Fachbereiche bei der mühseligen Definition von Berechtigungsanforderungen und auch bei der Umsetzung dieser. Durch Analyseverfahren, die alle Aktivitäten im System aufzeichnen und bewerten, können die Berechtigungen effizient und sicher nach dem Minimalprinzip konzipiert werden.

Datengetriebener Ansatz

Die Einführung neuer Technologien wie SAP S/4HANA erhöht die Komplexität im Berechtigungsmanagement zusätzlich. Bestehende Berechtigungskonzepte müssen überarbeitet und angepasst werden. Der datengetriebene Ansatz ist nicht nur bei herkömmlichen S/4HANA Trans-

formationsprojekten, sondern auch bei S/4HANA Cloud Private (RISE with SAP) oder Public (GROW with SAP) Projekten von Bedeutung, da er eine nahtlose Überführung und/oder Neugestaltung der SAP-Berechtigungen ermöglicht. Eine sorgfältige Berechtigungsprüfung von SAP ECC-Landschaften im Hinblick auf die Umstellung auf SAP S/4HANA Private und Public Cloud ist unerlässlich.

Die laufenden und anstehenden Transformationsprojekte machen das Thema SAP-Berechtigungen relevanter denn je. Auch das finanzielle Risiko steigt, denn ab S/4HANA bestimmen die vergebenen Berechtigungen auch die notwendigen Lizenzen für SAP. Somit ist eine Kopplung von SAP-Lizenzen an Berechtigungen ein notwendiger und empfohlener Schritt, um eine korrekte Umwandlung und Ermittlung der Lizenzbedarfe in SAP S/4HANA On-Premises und S/4HANA Cloud sicherzustellen. Durch die Kombination von Berechtigungs- und Lizenzmanagement in Verbindung mit einem datengetriebenen Ansatz können unnötige Lizenzinvestitionen vor und während einer S/4HANA Transformation vermieden werden. Dies schafft mehr Sicherheit und ein gutes Gefühl bei der Umstellung auf SAP S/4HANA.

Aus diesem Grund erfordert die Autorisierung gemäß den S/4-Regelungen im Einklang mit den neuen Lizenzbestimmungen für S/4HANA eine präzise Zuweisung der Lizenzen zu den damit verbundenen Berechtigungen. Dies ist notwendig, um finanzielle Risiken zu vermeiden und die Einhaltung der Vorschriften sicherzustellen.

SAP-Lizenzmanagement

Mit der Einführung des S/4HANA-Lizenzmodells hat das SAP-Lizenzmanagement eine neue Dimension erreicht. Es berücksichtigt nun nicht nur die tatsächliche Nutzung, sondern auch die Vergabe von Berechtigungen. Unternehmen haben nun die Möglichkeit, durch ein ganzheitliches Berechtigungsmanagement in Verbindung mit den S/4HANA-Lizenzbestimmungen Kosten zu sparen und teure Professional Use Lizenzen zu vermeiden.

Es ist von entscheidender Bedeutung, dass Unternehmen nicht nur über fachliche Kenntnisse im Bereich Berechtigungskonzept, Lizenz- und Vertragserfahrungen verfügen, sondern auch sicherstellen, dass dieses Wissen innerhalb der Organisation zusammengeführt und implemen-

tiert wird. Eine transparente Darstellung von Rollen und Benutzermanagement sowie die Überwachung der Benutzernutzung in der SAP-Umgebung sind unerlässlich, um Compliance sicherzustellen und gleichzeitig Kosteneinsparungspotenziale zu realisieren.

Da sich die Anforderungen und Aufgabenprofile in den Abteilungen im Laufe der Zeit verändern, müssen auch die damit verbundenen Berechtigungen sowie die Reallokationen der Lizenzen kontinuierlich angepasst und überprüft werden. Idealerweise sollte eine Rollenänderung einen automatisierten Prozess durchlaufen, der anhand der Rollenänderung und Rollenrezertifizierung die erforderlichen Lizenzen zuweist und gleichzeitig die lizenzrechtliche und wirtschaftliche Implikation ausweist.

Es ist daher ratsam, sich frühzeitig mit den technischen und organisatorischen Anforderungen einer S/4HANA-Transformation auseinanderzusetzen und dabei auch die damit einhergehenden Lizenzbedarfe zu berücksichtigen, um diese in ein wirtschaftliches und flexibles Vertragsmodell zu überführen. Nur so kann angemessen auf die kontinuierlichen technischen Anpassungen während und nach der Transformation reagiert werden.

Die Automatisierung und kontinuierliche Verwaltung des Berechtigungskonzepts sind entscheidend, um sicherzustellen, dass das Rollenkonzept und die Lizenznutzung optimal und kosteneffizient umgesetzt werden. Ohne entsprechende Automatisierung und Verwaltung besteht die Gefahr von Unstimmigkeiten und Inkonsistenzen im Berechtigungskonzept, was zu unnötigen Lizenzkosten, Security- und Compliance-Risiken führen kann.

Um diesen Herausforderungen im Zusammenhang mit SAP-Lizenzen zu begegnen, bietet AIM eine umfassende und datengetriebene Lösung für ein effektives SAP-Lizenzmanagement und daraus resultierend die richtigen Unternehmensentscheidungen.

Authorization and Identity Management

Unser Authorization and Identity Management (AIM)-Service und Vorgehen ermöglichen es Unternehmen, die erforderlichen Daten und die Transparenz zu erhalten, um Security- und Compliance-Maßnahmen abzuleiten. Dies bildet die Grundlage für die Optimierung des S/4HANA-Berechtigungskonzeptes und

die Reduzierung der Lizenzinvestitionen im Zuge der Umwandlung von Altlizenzen in S/4HANA Produkte sowie im operativen Betrieb. Ein gut konzipiertes Berechtigungs- und Lizenzkonzept spielt daher eine entscheidende Rolle, um den vollen Nutzen aus SAP RISE und GROW zu ziehen und ermöglicht eine sichere, effiziente und ressourcenoptimierte Nutzung, während gleichzeitig eine reibungslose Integration neuer Technologien wie S/4HANA gewährleistet wird.

Intelligente Automatisierung spielt dabei eine wichtige Rolle als Effizienztreiber. Nach einer erfolgreichen Bereinigung und Optimierung des SAP-Systems im Hinblick auf Security, Berechtigungen und Lizenzen ist das Interesse groß, die Investition nachhaltig zu schützen. Dabei stellt die Nicht-Einhaltung definierter Prozesse im täglichen operativen Betrieb die größte Gefahr für die Erhaltung der Qualität dar. Durch eine intelligente Automatisierung der aufgestellten Prozesse und der tiefen Integration in die bestehende Systemlandschaft kann dem entgegengewirkt werden.

Servicequalität verbessern

Wie das in der Praxis aussehen kann, zeigt sich am Beispiel IT-Helpdesk. Der IT-Helpdesk ist in vielen Unternehmen die erste Anlaufstelle für Mitarbeiter, um IT-Probleme diagnostizieren und lösen zu lassen. Insbesondere für Berechtigungsprobleme im SAP-Umfeld sind dafür oftmals aufwändige, manuelle Prüfungen von Experten notwendig, die in der Regel bereits stark ausgelastet sind, was die Bearbeitung- und Lösungszeiten negativ beeinträchtigen kann.

KI-gestützte Assistenten wie Chatbots bieten hier einen vielversprechenden Ansatz, um die Servicequalität nachhaltig zu verbessern. Integriert man einen solchen Chatbot in die Kommunikationskanäle des Unternehmens und verbindet ihn mit zentralen IT-Systemen wie SAP, können viele manuelle Prüfschritte automatisiert werden. Der Benutzer wird über das Chat-Interface eindeutig identifiziert,

DURCH DIE KOMBINATION VON BERECHTIGUNGS- UND LIZENZMANAGEMENT IN VERBINDUNG MIT EINEM DATENGETRIEBENEN ANSATZ KÖNNEN UNNÖTIGE LIZENZINVESTITIONEN VOR UND WÄHREND EINER S/4HANA TRANSFORMATION VERMIEDEN WERDEN.

Dmitrij Spolwind,
Consulting, Lighthouse Germany,
www.kpmg.com

sodass der Chatbot eine individuelle Problemdiagnose erstellen kann. Das Berechtigungsproblem wird dabei in Echtzeit direkt im SAP-System analysiert und mit Hilfe fachlicher Analysetools ein qualifizierter Lösungsvorschlag erstellt. Dabei können Risikoanalysen oder Auswirkungen auf die SAP-Lizenz des Benutzers in Echtzeit bewertet und berücksichtigt werden.

Alle Schritte erfolgen dabei komplett automatisiert, sodass der Chatbot der IT am Ende des Prozesses ein vollständiges Ticket mit Problemdiagnose und Lösungsvorschlag zur Bearbeitung bereitstellt. Die Bearbeitungszeit kann dadurch um bis zu 90% reduziert werden.

Vorteile nutzen

Die Integration neuer Technologien wie Generative Pre-trained Transformer (GPT) birgt enorme Potenziale. Die Interaktion zwischen Anwender und Maschine wird immer natürlicher, flexibler und vielfältiger, was zu einer Reduzierung der Akzeptanzhürden führt. Generative AI bietet insbesondere im Bereich der funktionalen Erweiterung von Lösungen erhebliche Möglichkeiten. Beispielsweise können Anfragen von Anwendern in natürlicher Sprache direkt in technische Befehle übersetzt werden. Dies ist besonders im SAP-Kontext von großem Vorteil, um nahtlos zwischen natürlicher und SAP-Sprache zu „übersetzen". Durch eigens trainierte Sprachmodelle können die positiven Effekte noch verstärkt werden, da somit unternehmensinternes Wissen und Sprache in den Assistenten eingearbeitet werden können.

Fazit

Es lässt sich festhalten, dass die Themen Security, Berechtigungen, Lizenzen sowie KI-gestützte Assistenten im SAP-Umfeld von hoher Bedeutung sind und eine datengetriebene Herangehensweise sowie intelligente Automatisierung dabei helfen können, die Komplexität zu bewältigen und die Sicherheit zu gewährleisten. Eine präzise Zuweisung der Lizenzen zu den Berechtigungen ist notwendig, um finanzielle Risiken zu minimieren und die Einhaltung der Vorschriften sicherzustellen. In diesem Zusammenhang bietet AIM eine umfassende und datengetriebene Lösung für ein effektives SAP-Lizenzmanagement und die Optimierung des S/4HANA-Berechtigungskonzepts, um Unternehmen bei der Bewältigung dieser Herausforderungen zu unterstützen und eine nachhaltige Investitionssicherheit zu gewährleisten.

Dmitrij Spolwind

Nachjustierung erforderlich

SAP ERKENNT DIE SCHLÜSSELROLLE VON KI UND OPTIMIERT SEIN PORTFOLIO

SAP arbeitet daran, das eigene Portfolio für Künstliche Intelligenz (KI) zu öffnen. Die Roadmap beinhaltet dabei die schrittweise Integration von KI-Funktionen, um den sich wandelnden Geschäftsanforderungen gerecht zu werden. Doch in Bezug auf die Bereitstellung einer KI-Plattform bleibt der Software-Hersteller offen. Anstatt eine eigene Plattform zu entwickeln, setzt SAP auf Partnerschaften mit führenden Unternehmen wie OpenAI (ChatGPT), Aleph Alpha, Microsoft, IBM Google Cloud und Anthropic sowie Cohere. Dieses Vorgehen passt zur SAP-Strategie der vergangenen Jahre. Das Ökosystem spielt bei SAP eine zentrale Rolle. Partner gewinnen an Bedeutung und umso wichtiger ist es, die Vielfalt des Umfelds im Blick zu haben. Dazu hat die DSAG einen Partnerbeirat ins Leben gerufen. Dieser soll sich mit Partner-relevanten Themen im SAP-Ökosystem beschäftigen.

SAP setzt bei KI auf Partner

Die SAP-KI-Strategie bedeutet, dass die fortschrittlichen Algorithmen und KI-Modelle von Partnern bereitgestellt werden, während SAP weiter Anbieter der unternehmensspezifischen Geschäftsdaten ist. Diese Herangehensweise ermöglicht es dem Softwarehaus, die Innovationsgeschwindigkeit zu erhöhen, gleichzeitig von den Entwicklungen und Erfahrungen der Partner zu profitieren und Kunden nicht auf einen Partner festzulegen. Das SAP-eigene „Foundational Model", das auf Basis der Systemnutzung von circa 20.000 SAP-Kunden entwickelt werden soll, wurde als strategischer Ausblick zwar schon kommuniziert, eine konkrete inhaltliche Ausgestaltung ist aber noch nicht erkennbar.

Grundsätzlich ist diese Ausrichtung aus DSAG-Sicht verständlich und unterstützenswert. Allerdings sind noch Fragen offen. So kündigte SAP-Chef Christian Klein in der Bilanzpressekonferenz im Juli 2023 an, dass Innovationen wie KI nur noch für die Cloud- Versionen von S/4HANA (Private und Public Cloud Edition) verfügbar sein werden. Ferner schränkte er die Verfügbarkeit auf RISE-with-SAP- und GROW-with-SAP-Verträge ein. Dabei hieß es, dass Lösungen wie KI in einem neuen RISE-with-SAP-Premium-Package verfügbar sein werden. Für dieses Package sollen zusätzliche Kosten von bis zu 30 Prozent anfallen. Wichtig ist dabei zu wissen, dass dieses Premium-Package freiwillig und optional ist und nicht automatisch alle RISE-Verträge teurer werden.

Offen bleibt aber, was genau das Paket enthält – und was KI in Form von konkreten Anwendungen bedeutet. Positiv zu bewerten ist jedoch, dass SAP sich technologisch an der Realität ausrichtet – denn in den Unternehmensarchitekturen halten große Sprachmodelle (LLM) nicht nur „SAP-only" Einzug. Zwar ist zunächst nur OpenAI verfügbar, danach sollen weitere Modelle wie Llama oder Claude von Anthropic folgen.

Generative KI soll Portfolio erweitern

Nach eigenen Angaben bietet SAP bereits über 130 Anwendungsszenarien für KI. Bisher handelt es sich bei den hier angebotenen Services und Funktionen jedoch nicht um generative KI. Diese soll erst hinzukommen, zum Beispiel für Stellenbeschreibungen, Fragen für Vorstellungsgespräche, Produktbeschreibungen und Abfragen für Analysen. Dafür kommen KI-Verfahren und -Technologien wie trainierte neuronale Netzwerke oder Deep Learning zum Einsatz, um Texte, Bilder, Audio- und Videoinhalte, 3D-Modelle oder auch Programm-Code zu erzeugen.

Neu in diesem Reigen ist der KI-Assistent SAP Joule, der den Geschäftskontext verstehen und direkt in das Cloud-Portfolio für geschäftskritische Prozesse integriert werden soll. Aus DSAG-Sicht handelt es sich hierbei primär um ein Tool, das in den Kinderschuhen steckt und mit konkreten Szenarien ausgestattet werden muss. Die Konkretisierung wird entscheiden, ob die Kunden das Produkt annehmen. Aus technologischer Sicht ist zu klären, auf welcher Plattform der KI-Assistent implementiert werden soll, wie die Integration aussehen wird und welches Harmonized Data Model genutzt werden soll, das Stand heute noch nicht existiert.

Die DSAG steht mit SAP im konstruktiv-kritischen Austausch, um KI in ihren mehr als 3.800 Mitgliedsunternehmen zu etablieren. Damit das gelingt, sind jedoch seitens des Software-Herstellers noch Stellschrauben zu drehen:

#1 Bereitstellung aller KI-Innovationen für alle S/4HANA-Kunden

Mit der Bekanntgabe der ursprünglichen Wartungsverlängerung bis 2040 hatte SAP zugesichert, Innovationen für S/4HANA konsequent und langfristig bereitzustellen und Kunden damit Stabilität versprochen. Alle KI-Innovationen für die S/4HANA Private Cloud sind somit für S/4HANA On-Premises mit identischem Leistungsumfang zur Verfügung zu stellen. Das ist notwendig, um die Verfügbarkeit von Technologien wie Machine-Learning (ML) und KI in S/4HANA-Systemen ebenso grundsätzlich sicherzustellen, wie die aus den zahlreichen neuen KI-Funktionen wie ChatGPT oder OpenAI resultierenden Funktions- und Integrationsszenarien.

#2 Einheitliche und standardisierte Rahmenbedingungen

Bei der Integration von LLM in SAP-Business-Prozesse muss SAP ein zentrales Monitoring der Integration und der abgewickelten Transaktionen ermöglichen. Zudem müssen die Transaktionen wie die mit Hilfe des LLM getroffenen Entscheidungen in unternehmenskritischen Prozessen nachvollziehbar sein. Sobald es sich um für die Rechnungslegung relevante Prozesse handelt, sind die Anforderungen der (IT-)Prüfungsstandards ebenso wie branchenspezifische Prüfungs- und Auditierungsstandards zu beachten. Zudem braucht es eine klare Regelung von Rollen, Verantwortlichkeiten und ein vollautomatisiertes internes Kontrollsystem (IKS) inklusive einfacher, transparenter Kontrollen und der Bewertung von Risiken.

#3 Angemessene Preismodelle

Es braucht angemessene und transparente Lizenz- und Nutzungsbedingungen. Für die von SAP bekanntgegebenen Partnerschaften wird ein kommerzielles Angebot „aus einer Hand" benötigt. Die kaufmännische Orchestrierung der KI-Funktionen aus diesen Partnerschaften darf nicht zu Lasten der Anwendungsunternehmen gehen, sodass diese mit den Anbietern selbst verhandeln müssen. SAP-Kunden sollten alle benötigten Komponenten für die Integration von KI-Algorithmen der Partner komplett über SAP beziehen und auf Basis prozess- oder transaktionsbasierter Metriken erhalten. SAP sollte wenigstens für den Mittelstand als Vertragspartner auftreten, damit dieser keine weiteren Verträge mit anderen Anbietern eingehen muss.

SAP SOLLTE ALLE KI-INNOVATIONEN FÜR DIE S/4HANA PRIVATE CLOUD AUCH FÜR S/4HANA ON-PREMISES BEREITSTELLEN.

Jens Hungershausen, DSAG-Vorstandsvorsitzender, DSAG e.V., www.dsag.de

#4 Klarheit zur indirekten Nutzung

Aus DSAG-Sicht braucht es einheitliche Regelungen zur Integration von KI-Modellen in SAP-Applikationen. Insofern derzeit Informationen zwischen SAP-Software und einem Drittsystem ausgetauscht werden, verstößt dies gegen die Bedingungen einer herkömmlichen Benutzerlizenz. Das darf künftig nicht der Fall sein, wenn ein LLM-Modell als Nicht-Named-User auf die SAP-Software zugreift und gegebenenfalls auch Aktionen in ihr ausführt. SAP muss das einheitlich für alle SAP-Produkte in den Lizenzvereinbarungen sicherstellen.

Jens Hungershausen

SAP Datasphere

DAS CLOUD DATA WAREHOUSE DER ZUKUNFT?

Im März 2022 hat SAP die Weiterentwicklung der bisherigen SAP Data Warehouse Cloud verkündet und bietet damit eine eigene Business Data Fabric Lösung an.

Der Wechsel zu SAP Datasphere eröffnet Unternehmen neue Perspektiven, indem es die effektive Verknüpfung von Daten aus verschiedenen Quellen ermöglicht. Dies fördert die Zusammenarbeit zwischen Teams, steigert die Transparenz und Lesbarkeit von Daten, und ermöglicht eine nahtlose Integration von externen Daten sowie Partner-Applikationen. Auf diese Weise wird die Grundlage für datengetriebene Entscheidungsprozesse geschaffen.

Bestehende SAP-Kunden mit gewachsenen BW 7.x Applikationen müssen sich daher überlegen, wie sie mit dem Supportende bis 2027 mit ihrer Applikation weiter umgehen. Wollen sie auf ein BW/4HANA migrieren oder mit SAP Datasphere die genannten Möglichkeiten der Cloud nutzen.

Im nachfolgenden Abschnitt werden die Funktionen und Vorteile der SAP Datasphere beleuchtet und unsere Einschätzung über die Zukunftsaussichten der SAP Datasphere als mögliche wegweisende Data Fabric Lösung diskutiert.

Funktionsübersicht der SAP Datasphere

SAP Datasphere bietet eine Vielzahl an Funktionen beginnend von der Anbindung unterschiedlichster Quellsysteme (Source), dem Management von Daten (Data Driven and Business Driven), einfache Integration von Partnerlösungen (SAP Open Data Ecosystem) und Bereitstellung der Daten für Endanwender und

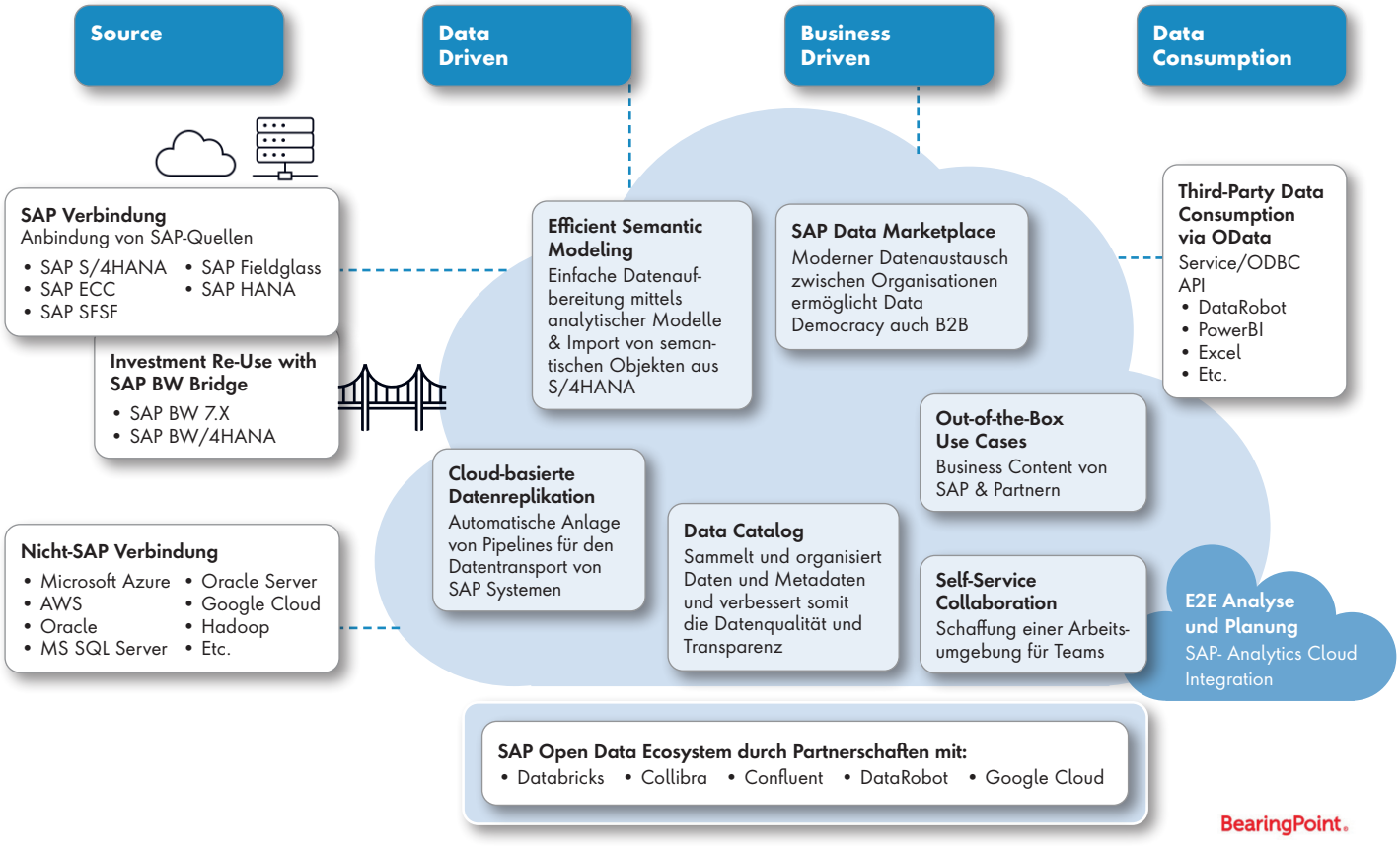


Bild 1: Übersicht SAP Datasphere (Quelle: BearingPoint, basierend auf SAP-Material)

Systemschnittstellen (Data Consumption) für die weitere Verwendung.

ANBINDUNGSMÖGLICHKEITEN

SAP Datasphere bietet eine breite Palette an Anbindungsmöglichkeiten, mit denen Benutzerinnen und Benutzer auf eine Vielzahl unterschiedlicher SAP- & nicht SAP-Datenquellen zugreifen können unter anderem SAP S/4HANA, BW/4HANA und etablierte Cloud Datenspeicher bei AWS, Azure oder Google BigQuery. Dadurch entfallen Hürden bei der technischen Datenintegration und der Grundstein für die Data Fabric Architektur ist gelegt.

BUSINESS DATA FABRIC

Die Data Management Funktionen der Business Data Fabric teilen sich in „Data Driven" und „Business Driven" auf. Hier deutet sich die enge Verzahnung zwischen IT und den Fachabteilungen an und damit das Arbeiten in Cross-funktionalen Teams, welches die Barrieren zwischen IT und Fachbereich weiter aufbrechen sollen.

• Data Catalog

In Unternehmen wird der Wert von Daten oft nicht voll ausgeschöpft, da ihre Auffindbarkeit und Lesbarkeit begrenzt sind. Ein Data Catalog löst dieses Problem, indem es die Suche nach benötigten Daten erleichtert, die Klassifizierung und Organisation von Data Assets ermöglicht und Begrifflichkeiten im Unternehmen allgemeingültig und -verständlich festlegt.

• SAP Data Marketplace

SAP Datasphere stellt einen Data Marketplace bereit, um externe Branchendaten leichter zugänglich zu machen. Mit über 3.000 Datenprodukten aus verschiedenen Industriebereichen und öffentlichen Datenquellen strebt SAP die Schaffung eines kontinuierlich wachsenden B2B-Netzwerks für den Datenaustausch an.

SAP HAT MIT DATASPHERE KEIN NACHFOLGEPRODUKT FÜR SAP BW GESCHAFFEN, SONDERN GEHT KOMPLETT NEUE WEGE.

Marius Wagner, Business Consultant, BearingPoint, www.bearingpoint.com

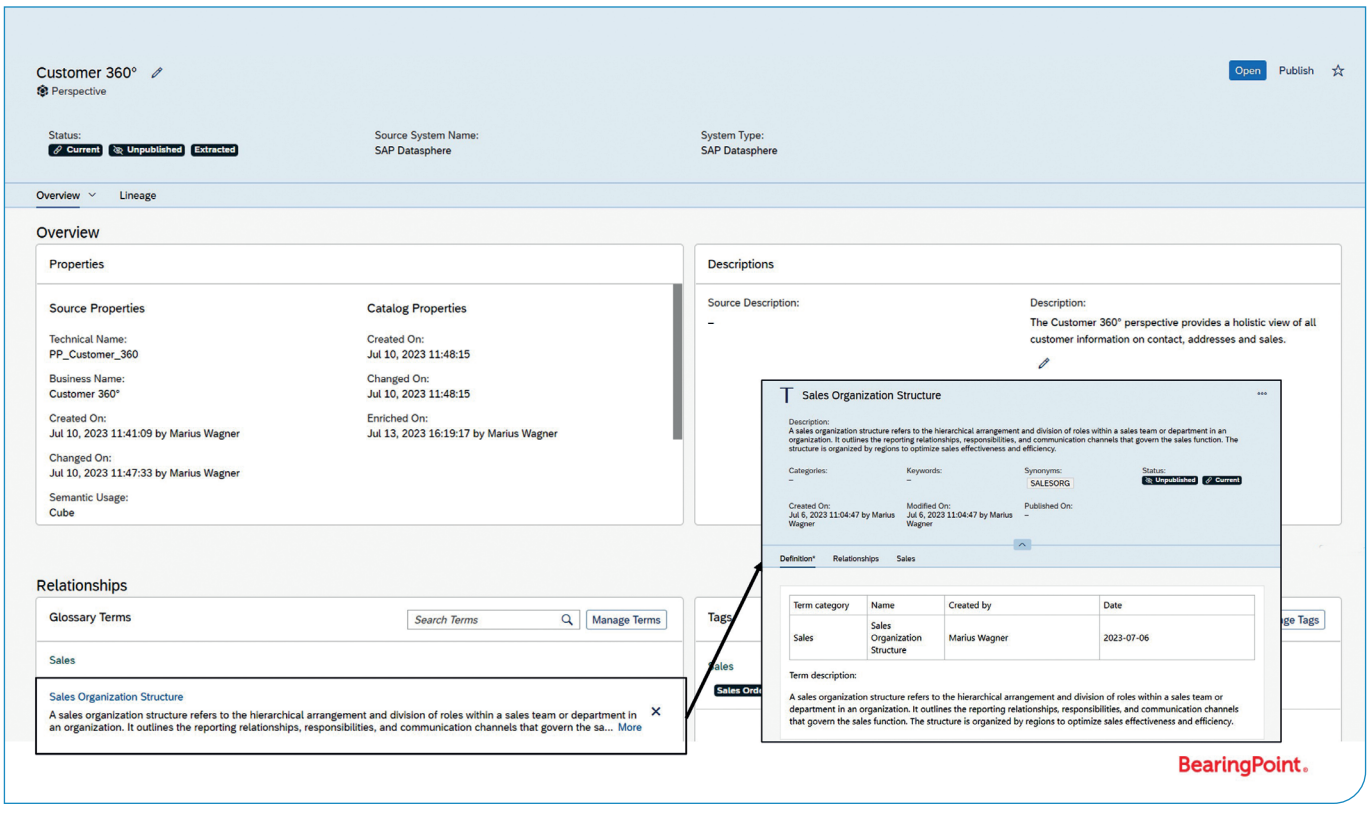


Bild 2: Illustration zu Business und Data Builder (Quelle: BearingPoint, basierend auf SAP-Material)

• **Efficient Semantic Modeling**
Die Gestaltung und Strukturierung von Daten erfolgt innerhalb von SAP Datasphere mithilfe des Data- und Business Builders. Dabei übernimmt der Data Builder die technischen Modellierungsaufgaben, während der Business Builder in der Lage ist, Daten auf einer semantischen Ebene zu modellieren.

SAP-Kunden profitieren zusätzlich von der Funktion „Entitäten importieren" um Metadaten zu umfangreichen semantischen Objekten automatisch aus SAP S/4HANA zu importieren.

• **Self-Service Collaboration**
Spaces ermöglichen die Schaffung einer organisatorischen Arbeitsumgebung für Projekte, Teams oder ganze Abteilungen. So können „cross-funktionale" Teams Daten selbstständig sammeln, organisieren und mit anderen Abteilungen austauschen, um so den Wert Ihrer Daten zu maximieren.

• **Cloud-basierte Datenreplikation**
SAP Datasphere erleichtert die nahtlose und effiziente Integration von Daten aus SAP S/4HANA durch Replication Flows. Damit können Daten und Strukturen aus CDS Views mühelos übertragen werden und stehen anschließend für weitere Verarbeitungsschritte zur Verfügung.

• **Investment Re-Use & Extension mit SAP BW Bridge**
SAP BW Bridge bietet Unternehmen, welche SAP BW 7.x nutzen, einen unkomplizierten Weg in die Cloud. Mit BW Bridge

MIT DATASPHERE GEHT SAP DEN NÄCHSTEN KONSEQUENTEN SCHRITT IN DIE CLOUD UND STÄRKT DAMIT AUCH SEINE BUSINESS TECHNOLOGY PLATFORM (SAP BTP).

Stefan Zizelmann, Senior Manager, BearingPoint, www.bearingpoint.com

ist es möglich eine Vielzahl an SAP BW Objekten in die neue SAP Datasphere Umgebung zu überführen. Die bisherigen SAP BW-Funktionen bleiben weitestgehend erhalten, und es eröffnen sich neue Möglichkeiten und Vorteile durch die Nutzung der Cloud-Plattform.

• **Out-of-the-Box Use Cases**
SAP bietet vorgefertigte Standardlösungen für verschiedene Geschäftsszenarien, Branchen und Geschäftsbereichen an. Dazu gehören komplett dokumentierte Datenmodelle, Objekte, KPIs, Kennzahlen und Schnittstellen.

• **Open Data Ecosystem**
Im Rahmen der Einführung von Datasphere hat SAP strategische Partnerschaften mit führenden Unternehmen im Bereich Data Analytics wie Confluent, Collibra, Databricks, Google Cloud und DataRobot angekündigt. Diese Kooperation ermöglicht eine nahtlose Integration von Partner-Applikationen und erweitern den Funktionsumfang nochmals.

DATA CONSUMPTION

Durch integrierte Anwendungen und APIs lassen sich die Daten einfach für Analysen und weitere Verwendungszwecke nutzen.

• **E2E Analyse und Planung**
Die reibungslose Integration und der bidirektionale Datenaustausch zwischen SAP Analytics Cloud und Datasphere vereinfachen die Erstellung von Storyboards, Berichten, Analysen und vor allem Planungsanwendungen erheblich.

• **Third-Party Data Consumption**
Durch ODATA Services und ODBC APIs haben Entwicklerinnen und Entwickler die Möglichkeit Daten in andere Anwendungen zu exportieren oder mit maßgeschneiderten Lösungen zu verbinden. Dies erweitert die Flexibilität und Nutzbarkeit der Daten.

SAP Datasphere – eine Zukunftssichere Investition?
SAP Datasphere bringt viele Benefits und Features gegenüber den bisherigen SAP BW Lösungen mit sich. Dadurch steht die Frage im Raum, ob SAP Datasphere das Potenzial hat, das etablierte SAP BW 7.x abzulösen. Aus unserer Sicht ergeben sich folgende Vorteile für SAP Datasphere:

#1 Zentrale Datenplattform: SAP Datasphere bildet eine zentrale und zukunftsorientierte Datenplattform für SAP- und Non SAP Daten. Mit Funktionen wie Konnektivität, Data Catalog und dem SAP Data Marketplace legt sie die Grundlage für eine fortschrittliche Data-Fabric-Architektur. Die Plattform ermöglicht eine nahtlose Integration verschiedener Datenquellen und schafft eine umfassende Datenlandschaft. S4/HANA Kunden profitieren zudem von der Möglichkeit des Imports von kompletten Entitäten.

#2 Erweiterte Konnektivität: SAP Datasphere ermöglicht die Nutzung von Partner-Applikationen wie Confluent, Collibra, Databricks, Google Cloud und DataRobot und bildet damit die Grundlage für eine Data-Fabric-Archi-

SAP DATASPHERE

- Zentrale Datenplattform für SAP- und Non-SAP-Daten
- Erweiterte Konnektivität zum Aufbau eines Partner-Ökosystems (z. B. Collibra)
- Hoher Integrationsgrad mit SAP Analytics Cloud
- Vereinfacht die Zusammenarbeit und den Datenaustausch für den abteilungsübergreifenden Austausch erheblich
- Wiederverwendung bestehender Investitionen mit BW-Bridge
- Verbesserte Datenzugänglichkeit für Geschäftsbereiche
- SAP Data Marketplace als B2B-Plattform für vereinfachten Datenaustausch
- Datasphere ist eine zukunftssichere Investition

BW/4HANA

- Bewährte Lösung mit Mainstream-Wartung bis 2040
- Bestehende BW-Kunden haben wenig Änderungsaufwand bei der Migration / Umstellung auf BW/4HANA
- Verwendung von SAP Analytics Cloud als einheitliches Frontend für bestehende Analytics- und Planung-Anwendung
- BW/4HANA ist in der Cloud und On-Premise verfügbar
- Umfangreichere Funktionen als in BW Bridge und weniger Datenspeicherung durch virtuelle Datenmodellierung

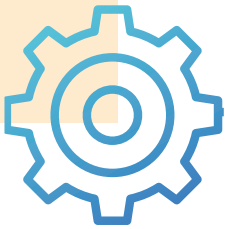


Bild 3: Vorteile von SAP Datasphere und BW/4HANA (Quelle: BearingPoint, basierend auf SAP-Material)

tektur. Dadurch entfallen viele der bisherigen Herausforderungen bei der Anbindung von Non SAP Anwendungen.

#3 Integrierte SAP Analytics Cloud: Sowohl SAP Datasphere als auch SAP Analytics Cloud basieren beide auf der SAP Business Technology Platform (BTP) und sind somit eng miteinander verzahnt. Anwenderinnen und Anwender können dadurch zwischen Berichten, Analysen, Planungen und den dahinterliegendem semantischen Datenmodell springen.

#4 Kollaboration: Teams können flexibel in der Cloud zusammenarbeiten, Daten über Spaces hinweg teilen und gemeinsam Erkenntnisse gewinnen. SAP Datasphere fördert eine reibungslose und abteilungsübergreifende Zusammenarbeit und erleichtert den Austausch von Informationen und Erkenntnissen.

#5 Wiederverwendung bestehender Investitionen: Die BW Bridge ermöglicht die Migration von Objekten aus bestehenden SAP BW Anwendungen in Datasphere, wodurch Unternehmen ihre bestehenden SAP BW-Investitionen sichern können und gleichzeitig von den Vorteilen der Cloud-Plattform profitieren.

#6 Verbesserter Datenzugang und Transparenz für Fachbereiche: Der Data Catalog verbessert die Datenzugänglichkeit für Fachbereiche, indem Datenobjekte, Begriffe und KPIs klassifiziert, organisiert und verständlich beschrieben werden. Dies erleichtert die Zusammenarbeit zwischen Fachbereichen und IT-Abteilungen.

#7 SAP Data Marketplace: SAP Datasphere bietet einen Data Marketplace, der eine stetig wachsende B2B-Plattform für den Datenaustausch bietet. Unternehmen können externe Branchendaten nutzen und von einem breiten Spektrum an Datenquellen profitieren.

#8 Zukunftssichere Investition: Die Datasphere Roadmap zeigt geplante Verbesserungen und unterstreicht SAPs ehrgeizige Pläne für die Zukunft. Im Gegensatz dazu gab es seit 2021 kaum mehr Updates für SAP BW Anwendungen, und der Mainstream Support für BW 7.5 wird im Jahr 2027 auslaufen. Ein Wechsel zu SAP Datasphere bietet Unternehmen die Gewissheit, dass ihre Investitionen langfristig geschützt werden.

Trotzdem bleibt ein etabliertes SAP BW/4HANA eine bewährte Lösung für Unternehmen, besonders wenn eine Vielzahl der operativen Systeme ebenfalls von SAP kommen wie etwa S/4HANA.

Als Basis für die Entscheidung, welche der beiden Lösungen für Unternehmen besser geeignet ist, haben wir die Vorteile beider Lösungen in Bild 3 zusammengestellt.

Ein Wechsel zu SAP Datasphere hängt von den individuellen Geschäftsanforderungen, dem Umfang der Datenintegration, der Komplexität der Analysen und anderen spezifischen Anforderungen des Unternehmens ab. Es kann auch sinnvoll sein, beide Lösungen zu kombinieren, um die Vorteile beider Welten zu nutzen.

Stefan Zizelmann, Marius Wagner

Transformationsstudie 2023

MANGELNDE DATENHYGIENE GEFÄHRDET TRANSFORMATIONSERFOLGE

Dass die Datenpflege im Businessalltag allerdings oft zu kurz kommt, ist kein Geheimnis. Im vergangenen Jahr gaben bei einer IHK-Umfrage 41 Prozent der Unternehmen an, dass ihre tägliche Arbeit unter mangelnder Datenqualität leidet. Wie weitreichend die Folgen einer mangelhaften Datenhygiene sind, bestätigen die Ergebnisse der Studie von Natuvion und NTT Data Business Solutions.

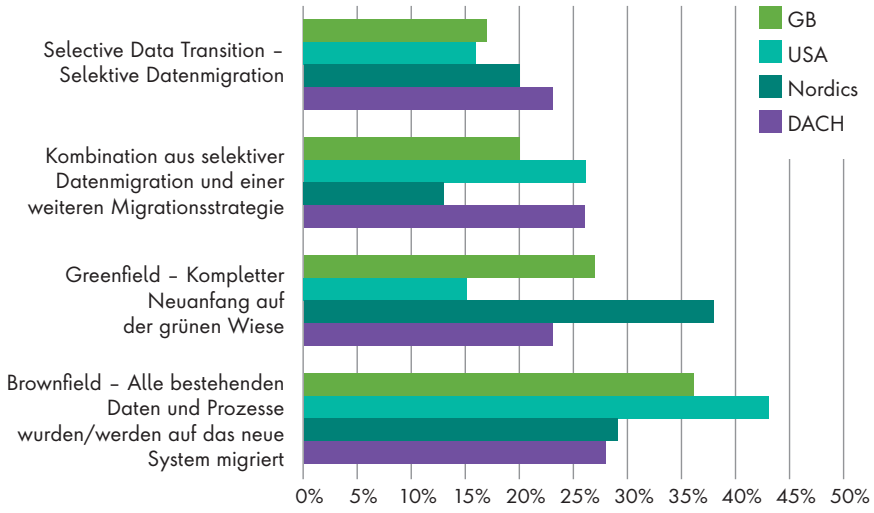
Schwerpunkt der Untersuchung war die digitale Transformation großer Systeme und die damit verbundenen Herausforderungen, Chancen und Mehrwerte. Ein wichtiger Aspekt der Befragung war die Bereitschaft zu Housekeeping-Projekten, also die gezielte Datenpflege vor oder während einer Transformation. Um es gleich vorwegzunehmen: Die Komplexität einer digitalen Transformation macht die Mobilisierung vieler Ressourcen und Kompetenzen sowie die Durchführung teils unangenehmer Aufgaben erforderlich. Die Qualität der zu migrierenden Daten ist dabei ein elementarer Schlüsselfaktor.

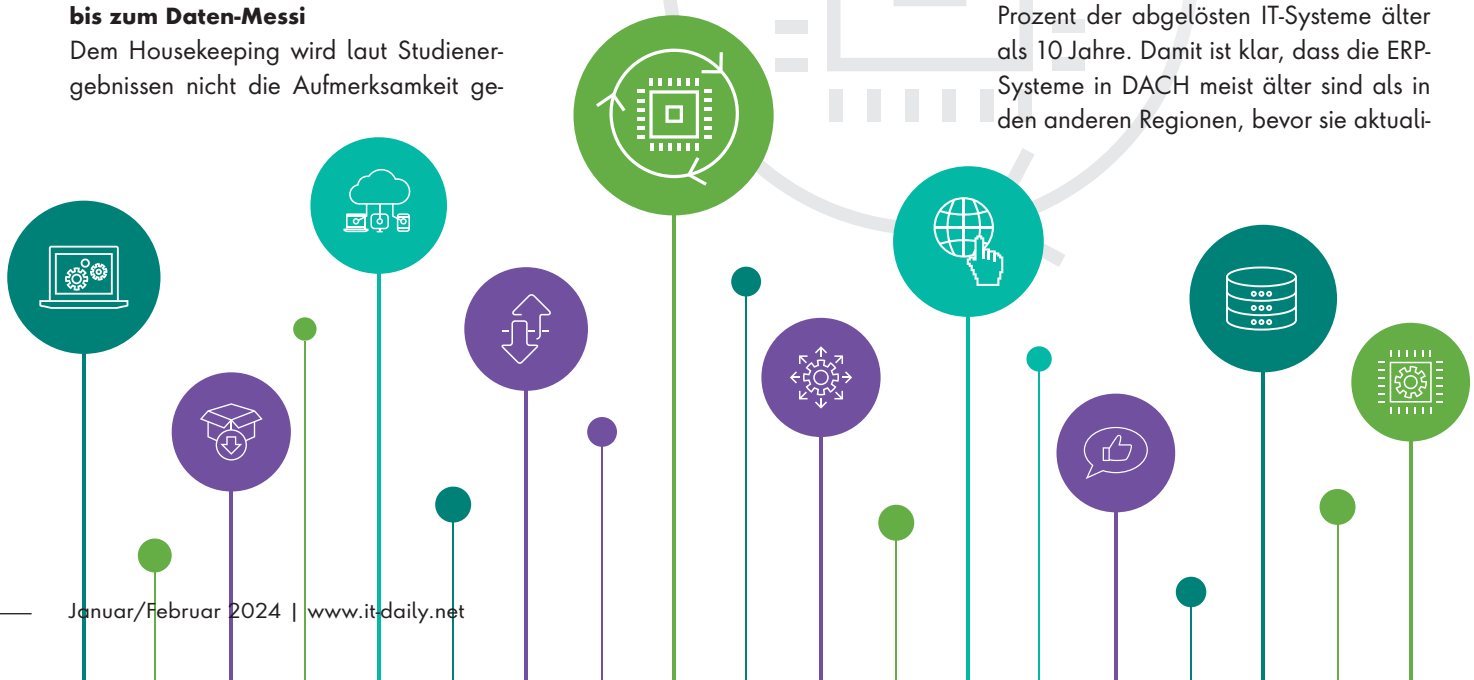
Von der Tabularasa-Fraktion bis zum Daten-Messi

Dem Housekeeping wird laut Studienergebnissen nicht die Aufmerksamkeit geschenkt, die es gebraucht hätte. Zwar nannten die Unternehmen auf die Frage nach den Erfolgsfaktoren der Transformation die „Prüfung der Datenqualität" und die „Bestandserfassung". Doch diese Antworten kommen einem Lippenbekenntnis gleich. Warum? Weil 35 Prozent der deutschen Unternehmen angaben, während des Transformationsprozesses von der schlechten Qualität ihrer Daten überrascht worden zu sein.

Fakt ist, dass der Löwenanteil der Systeme, die im Rahmen einer digitalen Transformation durch moderne Cloudlösungen ersetzt werden, aus internationaler Sicht zwischen 6 und 10 Jahren alt sind. In der DACH-Region sind zwar 16 Prozent der Systeme nicht älter als 5 Jahre, jedoch 26 Prozent der abgelösten IT-Systeme älter als 10 Jahre. Damit ist klar, dass die ERP-Systeme in DACH meist älter sind als in den anderen Regionen, bevor sie aktuali-

BEVORZUGTE MIGRATIONSSTRATEGIE





siert werden. Das alles hat Einfluss auf die Datenqualität, denn deren Relevanz für die Zukunftsfähigkeit eines Unternehmens hat sich erst in den letzten Jahren als kritisch entpuppt. Deshalb sind weder Transformationsprojekte, bei denen Daten rigide gelöscht werden noch solche bei denen auch noch die ältesten Daten mitumgezogen werden, erfolgreich.

Das Zauberwort: „Selective Data Transition“

Umso wichtiger ist es, vor der Migration ein solides Housekeeping durchzuführen. Es sollte hinterfragt werden, welche Daten archiviert, umgezogen oder gelöscht werden können. Dabei gilt die Devise, nur das Nötigste zu migrieren. Das hat in der Regel zur Folge, dass Unternehmen weder auf der grünen Wiese einen kompletten Neuanfang starten (Greenfield) noch alle bestehenden Daten und Prozesse einfach auf das neue System migrieren. Am zielführendsten ist deswegen meist der Selective-Data-Transition-Ansatz (SDT). Und es gibt noch mehr, was für diesen Approach spricht: das kleine Umstellungsfenster (Near Zero Downtime). In der Studie gaben 57 Prozent der deutschen Unternehmen an, für eine Datenmigration nur wenige Stunden zu haben - 74 Prozent haben maximal einen Tag. Für diese Organisationen ist SDT der interessanteste Transformationsweg. Denn die selektive Datenmigration ist der einzige Weg, das Umstellungsfenster und damit die „Downtime“ so klein wie möglich zu halten, weil diese Methode den Parallelbetrieb der alten und neuen Systeme mit nahezu allen Daten ermöglicht. Zum Umstellungszeitpunkt wird nur das Delta der veränderten Daten übertragen und das alte System deaktiviert. Das verringert die Downtime drastisch!

Für welche Vorgehensweise auch immer sich ein Unternehmen entscheidet - wenn es vorher nicht seine Daten ausmistet und für die Zukunft eine konsequente Datenpflege etabliert, wird die nächste Herausforderung nicht lange auf sich warten lassen.

Philipp von der Brüggen
www.natuvion.com

Das **eBook** umfasst 44 Seiten und steht zum kostenlosen Download bereit
www.it-daily.net/download

STORAGE

INNOVATIONEN NONSTOP

Gartner hat 2023 einen neuen Magic Quadranten für Primärspeicher veröffentlicht. Anwender von Primärspeicherlösungen setzen demnach auf verbrauchsbasierte Infrastruktur-Services für hybride, multidomäne und unternehmenskritische Anwendungen sowie auf die Anpassung der Kosten an Geschäftsanforderungen.

Der Hauptzweck eines Primärspeicherprodukts ist die Unterstützung von Workloads mit strukturierten Daten, die auf Antwortzeiten und IO/s angewiesen sind.

In unserem aktuellen eBook finden sie Beiträge zu Themen wie Hybrid-Storage, Storage Hochverfügbarkeit, Date Warehouses und 22-TByte-HDDs.

Integrierter Ansatz für die digitale Transformation

VOM WANDEL DER UNTERNEHMENS-DIGITALISIERUNGSPROJEKTE

Das Thema Digitalisierung ist für Unternehmen keinesfalls neu, aber immer noch eine große Herausforderung. Eine Ursache hierfür ist: Die Digitalisierung ist weiterhin ein Change-Treiber in Wirtschaft und Gesellschaft. Hinzu kommt: Während die Personal- und Organisationsentwicklung in etablierten Unternehmen meist linear verläuft, bewirkt oder erfordert der technologische Wandel oft disruptive Brüche. Auch deshalb werden, wenn es um das Thema digitale Transformation geht, so häufig Start-ups gegründet.

Ziel in der DACH-Region: Kostensenkung

Interessant in diesem Kontext ist, wie unterschiedlich in der DACH-Region und in den USA die Motive, digitale Transformationsprojekte zu starten, sind. Studien (wie die NTT DATA Transformationsstudie 2023) zeigen: In der DACH-Region ist Kostensenkung oft das zentrale Ziel. In den USA hingegen liegt der Fokus viel stärker auf den Themen Organisation, Kundenservice und neue Geschäftsmodelle. Deshalb wird auch der Erfolg der Transformationsprojekte in der DACH-Region viel kritischer als in den USA gesehen, denn das Ziel Kostensenkung wird in den Projekten häufig nicht erreicht; im Gegenteil oft werden die Digitalisierungsprojekte zu Kostenruinen.

Der Projektfokus liegt oft auf der technischen Innovation

Eine zentrale Ursache ist hierbei, dass bei vielen Digitalisierungsprojekten der Fokus auf dem Bereitstellen neuer Technologien liegt. Die Projekte werden also eher als Innovations- denn als Transformationsprojekte gesehen, bei denen zunächst einmal die oberste Führung verstehen muss, welche technologischen Möglichkeiten es aktuell und in naher Zukunft überhaupt gibt, wie diese in unternehmerischen Wert übersetzt werden können und welche Voraussetzungen hierfür organisatorisch, personell und kulturell nötig sind.

Fakt ist: Weil in vielen Digitalisierungsprojekten, die (vorgeblich) auf eine Transformation der Organisation abzielen, der Fokus primär auf der technischen Innovation liegt, werden in ihnen häufig die mit Einführung der neuen Technologien verbundenen strukturellen und kulturellen Aspekte vernachlässigt. Deshalb sind die Veränderungen oft nicht nachhaltig und die Entwicklungsziele sowie betriebswirtschaftlichen Ziele werden nicht erreicht.

Um dies zu vermeiden, bedarf es eines integrierten digitalen Transformationsansatzes, der auch die Organisations- und Kulturentwicklung sowie Digitalkompetenz umfasst. Existiert ein solcher Ansatz

nicht, kämpft das Unternehmen beim Planen und Realisieren des Projekts immer wieder mit folgenden Problemen:

- Den Top-Entscheidern fällt es aufgrund der rasanten Entwicklung der Informations- und Kommunikationstechnik schwer, sich für einen Lösungsweg zu entscheiden.
- Die IT-Budgets werden immer höher, ohne dass die Performance und/oder Wertschöpfung entsprechend steigt.
- Die technische Infrastruktur gleicht zunehmend einem Flickenteppich von digitalen Lösungen, ohne eine erkennbare digitale Gesamtarchitektur.
- Einzelne Geschäftseinheiten preschen unkoordiniert beim Einführen innovativer digitaler Lösungen vor, ohne dass zuvor aus den Unternehmenszielen abgeleitete Standards definiert wurden.
- Die Organisation und Mitglieder fühlen sich von der Transformation zunehmend überfordert, auch weil ein Kompass fehlt, der ihnen eine Orientierung gibt. Entsprechend groß sind die Widerstände.
- Der digitale Reifegrad der Organisation bleibt trotz aller Anstrengungen hinter dem Wettbewerb zurück.
- Das Management hat Probleme, das Gesamtprojekt und die Unternehmensentwicklung zu steuern.

Strukturelle und kulturelle Änderungen

Ein zentrales Element der digitalen Transformation ist die Veränderung der Unternehmenskultur hin zu mehr Kollaboration, Performance-Orientierung und Transparenz. Im Unternehmen sollte eine End-to-End-Prozessorganisation etabliert werden, die sicherstellt, dass alle in einen Geschäftsprozess involvierten Personen und Bereiche bestmöglich zusammenarbeiten.

Letztlich zielen integrierte digitale Transformationsprojekte darauf ab, in den Unternehmen ein Zusammenarbeitsmo-

EINEN INTEGRIERTEN DIGITALEN TRANSFORMATIONSANSATZ ENTWICKELN

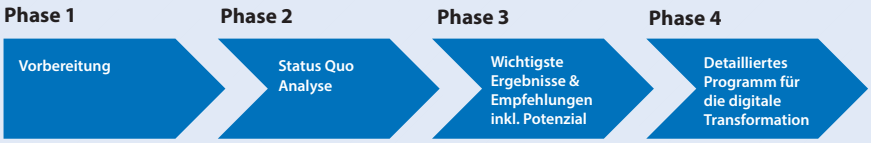
Beim Entwickeln eines integrierten digitalen Transformationsansatzes gilt es, vier sich teils überlappende Phasen oder Ebenen zu unterscheiden.

Verständnisebene: Digitalisierung ist ein fortlaufender Prozess. Deshalb existiert in den meisten Unternehmen bereits ein riesiger Fundus an IT-Lösungen. Zudem ist die Erwartungshaltung bezüglich der Digitalisierung oft verschieden: Während sich manche mehr Speed wünschen, befürchten andere eine Überforderung der Organisation. Das heißt, auf der Agenda steht auch die Frage nach der Veränderungsfähigkeit und -geschwindigkeit. Ein gemeinsames Verständnis über die Ausgangslage zu schaffen, ist eine Voraussetzung für das Entwickeln einer integrierten Digitalisierungsstrategie.

In dieser Phase gilt es unter anderem den digitalen Reifegrad der Organisation zu bestimmen. Dazu gehört

- das Entwerfen eines Zielbilds,
- ein Ermitteln des Reifegrads im Vergleich zu den Wettbewerbern,
- ein Abgleich der aktuellen Unternehmenskultur, organisatorischen Aufstellung sowie Qualifikation der Mitarbeiter mit dem Zielbild und
- das Entwickeln einer ersten Roadmap für den digitalen Transformationsprozess.

Bild 1: Möglicher Ablauf eines digitalen Reifegradchecks



Ein Reifegradcheck besteht normalerweise aus einem 4- bis 6-wöchigen Stream, in dem das digitale Effizienzpotenzial des Unternehmens einschließlich eines groben Realisierungsplans mit seinem Potenzial (Hauptthemen: Strategie, Organisation, Struktur, Architektur, Technologie, Beschaffung) bewertet wird.

Das setzt wiederum eine Bestandsaufnahme der vorhandenen Systeme, Technologien und Systembrüche und das Erzielen eines Commitments im Management bezüglich der Ausgangssituation sowie (Entwicklungs-)Ziele voraus.

Designebene: Hier geht es darum, ein Konzept zu erstellen, das die Strategie, Struktur und Prozesse sowie die Kultur und Fähigkeiten der Organisation zusammenbringt. Es gilt eine integrierte Digitalisierungsstrategie zu entwickeln, die umsetzbar ist, auch weil sie dem Reifegrad der Organisation und ihren Ressourcen entspricht.

Ein zentrales Element der digitalen Transformation ist die Veränderung der Unternehmenskultur hin zu mehr Kollaboration, Performance-Orientierung und Transparenz. Das setzt ein Wertemanagement voraus, das die in der Organisation angestrebten Werte definiert und operationalisiert sowie für

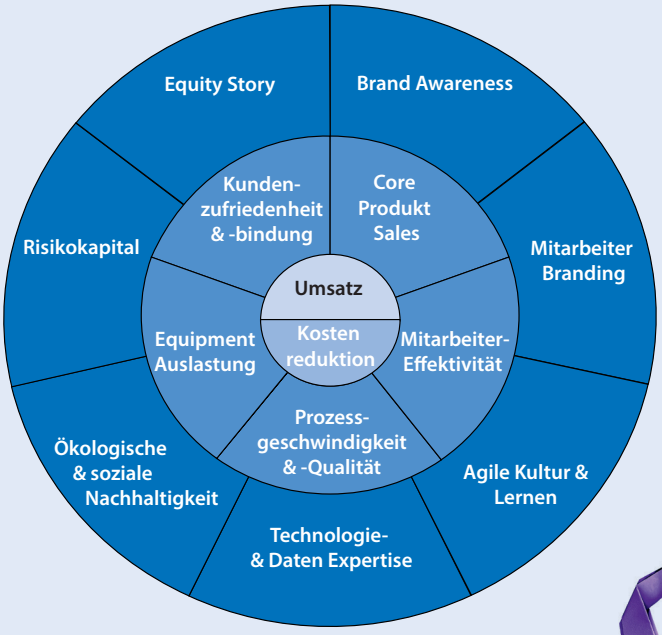


Bild 2: Beispiel eines möglichen Werteradars

die Mitarbeiter transparent macht - zum Beispiel mit einem Werteradar (siehe Bild 2).

In dieser Phase gilt es, das technisch und kulturell Mögliche sowie die Unternehmensziele zu kalibrieren; außerdem eine Transformationsarchitektur zu entwerfen, die eine Balance zwischen den Zielen, dem Reifegrad der Organisation und dem technisch Machbaren gewährleistet. Am Ende dieser Phase steht ein erster Plan, wie die integrierte digitale Transformation angegangen werden soll. Dieser muss im Umsetzungsprozess permanent überprüft und angepasst werden.

Umsetzungsebene: Bei der Umsetzung geht es unter anderem darum, den Transformationsprozess professionell zu begleiten und sicherzustellen, dass alle Beteiligten gut getaktet zusammenarbeiten. Ein Programm-Management, das die Technologie, Business-Ziele und Personalentwicklung ausbalanciert und alle relevanten Stakeholder top-down involviert, ist hierbei der Schlüssel zum Erfolg.

Auf Basis des Programmdesigns ergeben sich unter anderem folgende Umsetzungsschritte:

- PMO-Struktur zur Steuerung aufbauen,
- Qualifizierung des oberen Managements,
- Kommunikations-Roll-Out (Ziele, Vorgehen, Verantwortlichkeiten),
- Projektidentifikation, -integration und -priorisierung,
- Qualifizierung der Projektleiter,
- fortlaufende Reviews und Anpassungen sowie Change-Kommunikation.

Dabei gilt es stets die vier in Bild 3 dargestellten Ebenen der integrierten Umsetzungssteuerung zu beachten, da diese interagieren.

Dies ist auch nötig, weil das primäre Ziel der integrierten digitalen Transformation nicht lokale und funktionale Verbesserung ist. Vielmehr soll im Unternehmen eine End-to-End-Prozessorganisation etabliert werden, die sicherstellt, dass alle in einen Geschäftsprozess involvierten Personen und Bereiche bestmöglich zusammenarbeiten.

Verankerung: Integrierte digitale Transformationsprojekte zielen darauf ab, in den Unternehmen ein Zusammenarbeitsmodell zu etablieren, das gewährleistet, dass die angestrebte Art, wie in der Organisation an der Digitalen Transformation gearbeitet wird, zum neuen Standard wird. Deshalb ist es wichtig, die neuen Rollen und Verantwortlichkeiten einzuüben. Das erfordert einen prozessbegleitenden Support der Inhaber der verschiedenen Rollen – fachlich und persönlich.

Bei einem so strukturierten Vorgehen werden die unternehmerischen Problemstellungen, die mit der digitalen Transformation verbunden sind, nachhaltig gelöst. Zudem werden die Mitarbeiter dazu befähigt, den Transformationsprozess eigenständig voranzutreiben. Deshalb sichert es langfristig den Markterfolg.

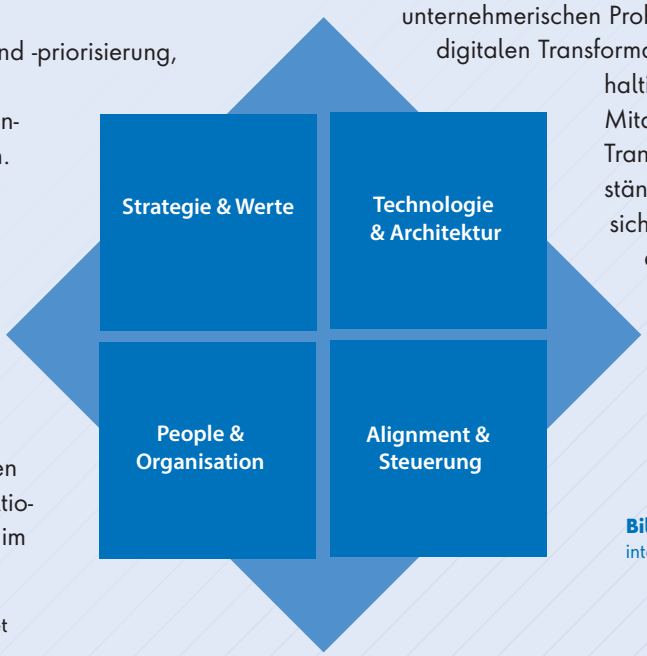


Bild 3: Die vier Ebenen einer integrierten Umsetzungssteuerung

dell zu etablieren, das gewährleistet, dass die angestrebte Art, wie in der Organisation an der Digitalen Transformation gearbeitet wird, zum neuen Standard wird. Wichtig ist deshalb auch, die neuen Rollen und Verantwortlichkeiten einzuüben.

Ganzheitliche und nachhaltige Unternehmensentwicklung

Bei digitalen Transformationsprojekten entsteht die gewünschte Nachhaltigkeit durch die organische Verbindung der technologischen Innovation mit einer zielorientierten Organisations- und Personalentwicklung. Von zentraler Bedeutung ist hierbei die Management- und Führungskräfteentwicklung, da das Top-Management der Prozesstreiber sein muss.

Bei den Innovationsprojekten der Vergangenheit lag die Verantwortung für das Realisieren der Projekte meist beim Leiter der IT-Abteilung. Sein Team implementierte die Technik und schulte die Mitarbeiter. Die Projektverantwortung trugen also die Personen, die das größte IT-Know-how hatten. Ähnlich verhielt es sich bei den Innovationsprojekten, die auf das Optimieren einzelner Prozesse abzielten. Bei ihnen gab das Top-Management zwar oft das Projekt und die erforderlichen Mittel frei, die Verantwortung für die Umsetzung lag aber meist bei dem IT-Leiter oder CIO, also dem Leiter der Abteilung mit dem größten IT-Know-how, und den Leitern der betroffenen Fachabteilungen, weil sie den sogenannten „Need" vor Ort am besten kannten.

Dadurch standen beim Projektmanagement solche Fragen im Vordergrund wie:

- „Was ist die IT-technisch beste Lösung?"

BEIM ENTWICKELN EINES INTEGRIERTEN DIGITALEN TRANSFORMATIONSANSATZES GILT ES, VIER SICH TEILS ÜBERLAPPENDE PHASEN ODER EBENEN ZU UNTERSCHEIDEN.

Paul Schwefer,
Associate Expert, Kraus & Partner,
www.kraus-und-partner.de

- „Welche Lösung bietet uns als Fachabteilung den größten Nutzen?"

Eine eher untergeordnete Rolle spielten hingegen Fragen wie:

- „Welche Lösung wäre aufgrund der Strategie und Entwicklungsziele des Unternehmens sinnvoll?"
- „Wie kompatibel sind die angedachten Lösungen mit der (angestrebten) IT-Architektur im Unternehmen?"

Aufgabe des Top-Management

Eine solche Verlagerung der Projektverantwortung auf die Fachebene ist auch heute noch möglich und zuweilen sogar sinnvoll – unter anderem, weil die Unternehmen heute viel mehr Erfahrung mit dem Implementieren digitaler Problemlösungen haben. Deshalb hat sich auch der Charakter vieler Projekte im Digitalbereich geändert: Aus früheren Innovationsprojekten wurden Routineprojekte und aus Akzeptanzprojekten Innovationsprojekte.

Anders sieht dies jedoch bei den Wandel- oder Transformationsprojekten aus, die darauf abzielen, dass Unternehmen sich strategisch neu in ihren Märkten positionieren und teilweise neu erfinden. Für das Planen und Realisieren solcher Projekte ist neben einem strategischen auch ein unternehmerisches Denken nötig.

Es erfordert zudem eine Vision:

- Wie entwickelt sich voraussichtlich unser Markt?
- Welche Chancen und Risiken ergeben sich hieraus für unser Unternehmen?
- Welche neuen Problemlösungen sind künftig aufgrund der technologischen Entwicklung möglich?
- Welche Produkte und Leistungen werden künftig von unseren Zielkunden nachgefragt?

Deshalb muss die Verantwortung für diese Projekte auf der Top-Ebene der Unternehmen angesiedelt sein und bleiben, selbst wenn die Verantwortung für das Realisieren gewisser Teilprojekte an Fachabteilungen delegiert wird.

Höhere Digitalkompetenz erforderlich

Zudem müssen die Verantwortlichen auf der Top-Ebene eine höhere Digitalkompetenz als früher haben. Diese ist nötig, damit sie einschätzen können,

- welche Problemlösungen aufgrund der technologischen Entwicklung künftig möglich sind und
- welche Relevanz diese für die Strategieentwicklung und das Geschäftsmodell des Unternehmens haben.

Denn nur, wenn das Top-Management über diese Beurteilungskompetenz verfügt, kann es das Gesamtprojekt so aufsetzen, dass dieses dem Bedarf der Organisation und den künftigen Marktanforderungen entspricht. Zudem kann es nur dann im Projektverlauf beurteilen, inwieweit die Entwicklung des Unternehmens dieses dem Ziel, langfristig einer der Top-Player im Markt zu sein, auch wirklich näherbringt.

Paul Schwefer

KI in Finanzabteilungen

IST KÜNSTLICHE INTELLIGENZ DER NÄCHSTE GROSSE RENNER?

Die aktuelle, jährliche Studie von BlackLine bestätigt, dass die deutschen Unternehmen auch in den Finanzabteilungen an den Möglichkeiten der Künstlichen Intelligenz (KI) durchaus interessiert sind.

Spätestens seit dem öffentlichen Zugang zu ChatGPT ist die Künstliche Intelligenz einer der am heißesten und durchaus kontrovers diskutierten Trends. Über was sich die meisten Unternehmen aber einig sind ist, dass in der neuen Technologie eine große, vermutlich heute noch nicht vollständig erfassbare, Chance liegt. Das bestätigt auch die neueste Studie von BlackLine. Bei der Befragung war aus weltweiter Sicht die Meinung deutlich, dass moderne Unternehmen neue Technologien wie KI einsetzen müssen, um ihre Finanzabläufe zu rationalisieren. Die überwiegende Mehrheit der Befragten gab an, dass generative KI (78 Prozent) und neue Arten von KI (76 Prozent) von entscheidender Bedeutung sind, um die Resilienz von Unternehmen angesichts künftiger Instabilität und Disruption zu verbessern.

Auf Länder heruntergebrochen zeigt sich jedoch, dass es bei den Studienergebnissen markante Unterschiede zwischen den Regionen gibt. In Deutschland messen lediglich 57 Prozent der generativen KI diese Bedeutung zu, in Frankreich 69 Prozent, in UK 72 Prozent. Eine Art Vorreiter scheint nach Aussagen der Studienteilnehmer die USA mit sage und schreibe 90 Prozent zu sein, wenn es darum geht mit KI die Resilienz der Unternehmen zu härten. Ähnliche Werte und Gewichtungen zwischen den Regionen gelten auch für die Einschätzungen bezüglich neuer Arten von KI.

Damit ist klar, dass die Begeisterungsfähigkeit der Manager und Finanzprofis hinsichtlich der KI aus weltweiter Sicht nicht darüber hinwegtäuschen darf, dass es in den einzelnen Industriestaaten deutliche Unterschiede in den Einschätzungen gibt. Tatsachen, dass die meisten KI-Innovationen in den USA entwickelt werden und damit einen anderen Stellenwert einnehmen oder dass in diversen europäischen Ländern die Diskussion über die KI auch über deren Nachteile und Gefahren geführt wird, tragen zu unterschiedlichen Stimmungsbildern maßgeblich bei. Ein Fazit: Ja, KI wird von allen Befragten als eine Zukunftstechnologie gesehen, allerdings mit einer weiten Spanne zwischen Hype und nüchterner Betrachtung.

KI in Finance und Accounting?

Inwieweit eine KI in Finanzabteilungen und im Controlling nützlich sein kann, hängt von den Anwendungsbereichen und vor allem vom Vertrauen in die neue Technologie ab. Insbesondere das Vertrauen ist entscheidend, da komplexen Abläufe im Hintergrund von nur wenigen Spezialisten überhaupt komplett verstanden werden. Es ist eben eine KI und nicht nur eine Automation. In diesem Zusammenhang geben zusätzliche, in der Studie beleuchtete Aspekte etwas mehr Aufschluss, insbesondere wenn es darum geht, die neue Technologie perspektivisch im Finance und Accounting (F&A) einzusetzen. Auf die Frage was die größten Herausforderungen bei der Einführung von KI für die F&A-Branche sind, sehen 34 Prozent weltweit „im Vertrauen in die Ergebnisse von KI" ein potenzielles Problem. Die Deutschen sind hier etwas zuversichtlicher, was auf den ersten Blick verwunderlich wirkt, hätte man doch das große Vertrauen den USA zugeschrieben, die deutlich mehr an die verbesserte Unternehmensresilienz durch KI glauben. In Deutschland haben lediglich 28 Prozent, aufgeteilt auf 25 Prozent der C-Suite und 31 der F&A-Spezialisten, ein Problem mit dem Vertrauen in die KI. Diesen Resultaten könnten konkrete Erfahrungen von Unternehmen mit der KI zugrunde liegen, die ein größeres Vertrauen in die Ergebnisse zufolge haben. Dies könnte auch erklären, weshalb 37 Prozent der deutschen Unternehmen neben diversen weiteren Vorteilen der KI hauptsächlich davon ausgehen, dass KI und Automation repetitive Aufgaben sowie Fehler reduzieren und damit zu einer höheren Qualität im F&A beitragen.

Die Befragten bestätigen zudem Hürden für den effektiven Einsatz von KI im F&A. Die am häufigsten genannten sind das Training von KI-Modellen (36 Prozent), um komplexe Finanzdaten richtig zu verstehen und zu interpretieren, sowie die Sicherstellung eines robusten Governance-Rahmens (32 Prozent), um den potenziellen Missbrauch von KI zu verhindern. Sowohl das Training von KI-Modellen als auch ein robuster Governance-Rahmen sind Aspekte, die zumindest heute nicht in den Händen und im Einflussbereich der C-Level-Manager oder der F&A-Profis liegen. Ergo ist es verständlich, dass die beiden wichtigen Aspekte zu einer gewissen Sorge beitragen – übrigens in den USA mit den höchsten Werten von 41 und 37 Prozent.

ÜBER DIE STUDIE

Die Studie wurde im August 2023 vom unabhängigen Marktforschungsinstitut Censuswide in Deutschland, England, Frankreich, Australien, Singapore, Kanada und den USA durchgeführt. Befragt wurden 1.339 C-Level-Verantwortliche sowie F&A Spezialisten in Unternehmen.

Angst vor Neuem ist nicht neu

Wie bei vielen Innovationen in der Vergangenheit, führt auch der allgegenwärtige Hype und die kontroversen Diskussionen zu KI gelegentlich zu Verunsicherung. Diese bezieht sich allerdings nicht nur auf die Technologie, deren Leistungsfähigkeit und auf das Vertrauen der durch KI erzeugten Zahlen, Daten und Fakten. In erster Linie geht es um Persönliches. Nicht wenige der in der Studie befragten C-Level-Manager und Finanzprofis glauben, dass durch die Einführung der KI potenziell Arbeitsplätze verloren gehen: Weltweit befürchten dies 36 Prozent der Befragten, in Deutschland sind es mit 32 Prozent nur etwas weniger. Am zuversichtlichsten sind die Befragten in England mit knapp 28 Prozent.

Es scheint, als würde mehr oder weniger ein Drittel der Befragten KI als eine Art disruptive dunkle Macht in der Finanzabteilung einordnen, die alles selbstständig erledigt und damit viele bisherigen Funktionen im F&A obsolet machen. Die zuvor genannte Hoffnung, dass die KI und Automation repetitive Aufgaben sowie Fehler reduzieren und damit zu einer höheren Qualität im F&A beitragen, unterstreicht die Sorge derer, die um Jobs bangen. Allerdings wurde hier noch nicht berücksichtigt, dass allein durch die Finanzautomation oder Modelle wie das Continuous Accounting ein Großteil der manuellen Prozesse schon heute entfällt, dafür aber neue und deutlich hochwertigere Aufgaben auf die Finanzprofis zukommen – beispielsweise die Szenarienerstellung und die Beratung des Managements.

Fazit: KI ist bereits Realität

Laut der neuen Studie von BlackLine überwiegen die positiven Erwartungen gegenüber der Bedenken. Auch wenn der Umgang mit KI in den Kinderschuhen steckt und noch lange nicht vollständig ausgereift ist, zeigt das Stimmungsbild, dass nicht nur das Ableiten möglicher Vorteile, sondern sogar der Einsatz im F&A bereits begonnen hat. Die Existenz der KI im F&A bestätigt beispielsweise BlackLine mit seinem neuen KI-unterstützen Intercompany Accounting. Das sogenannte ‚Intercompany Predictive Guidance' wurde entwickelt, um Transaktionsfehler zu verhindern, bevor sie auftreten, und um den Zeit- und Ressourcenaufwand über den gesamten Transaktionslebenszyklus zu minimieren – maßgeblich durch die Unterstützung von KI.

Trotz vieler offener Fragen ist KI auch im F&A schon heute Realität. Jetzt geht es darum, die Bedenken auszuräumen und die Vorteile daraus zu ziehen.

Ralph Weiss | www.blackline.com

Quelle: BlackLine 2023

TDM: Vielschichtiges Testdatenmanagement-Framework

SYNTHETISCHE UND REFERENTIELL KORREKTE TESTDATEN ERSTELLEN

– TEIL 1 VON 5 –

Die ist der erste Artikel einer fünfteiligen Serie, die sich tiefgreifend mit einem entscheidenden Aspekt in der IT-Welt auseinandersetzt: dem Testdatenmanagement. In der sich rasant entwickelnden IT-Landschaft ist die Qualitätssicherung von Softwareprodukten von entscheidender Bedeutung und das richtige Handling von Testdaten spielt dabei eine Schlüsselrolle. Es werden verschiedene Aspekte des Testdatenmanagements beleuchtet um Einblicke in bewährte Praktiken, Herausforderungen und Chancen innovativer Lösungen zu erhalten. Wir beleuchten die Rolle realistischer Testdaten in der Qualitätssicherung und die effiziente Durchführung von Performance-Tests. Erfahren Sie, wie diese Aspekte nicht nur die Effektivität von Softwaretests steigern, sondern auch zu robusteren und zuverlässigeren IT-Lösungen führen als entscheidenden Beitrag zum Erfolg in der digitalen Ära.

Das Testdatenmanagement (kurz „TDM") bezieht sich auf den Prozess der Verwaltung und Bereitstellung von Daten, die in Softwaretests verwendet werden. Testdaten sind entscheidend für die Durchführung da sie sicherstellen, dass Anwendungen unter verschiedenen Bedingungen getestet werden können, um ihre Leistungsfähigkeit, Zuverlässigkeit und Sicherheit zu überprüfen. Das TDM umfasst verschiedene Aufgaben:

#1 Bereitstellung von Testdaten: Sicherstellen, dass geeignete Testdaten für verschiedene Testfälle verfügbar sind. Dies beinhaltet oft die Erstellung von realistischen Datensätzen, um verschiedene Szenarien abzudecken.

#2 Anonymisierung und Maskierung:
Schutz sensibler Daten, um sicherzustellen, dass sensible Informationen während der Tests nicht gefährdet werden. Dies ist besonders wichtig, wenn echte Produktionsdaten für Tests verwendet werden.

#3 Bildung von Teilmengen:
Auswahl und Bereitstellung von Teilmengen der Daten, die für bestimmte Tests benötigt werden. Dies hilft, den Ressourcenbedarf zu optimieren und die Test-Effizienz zu steigern.

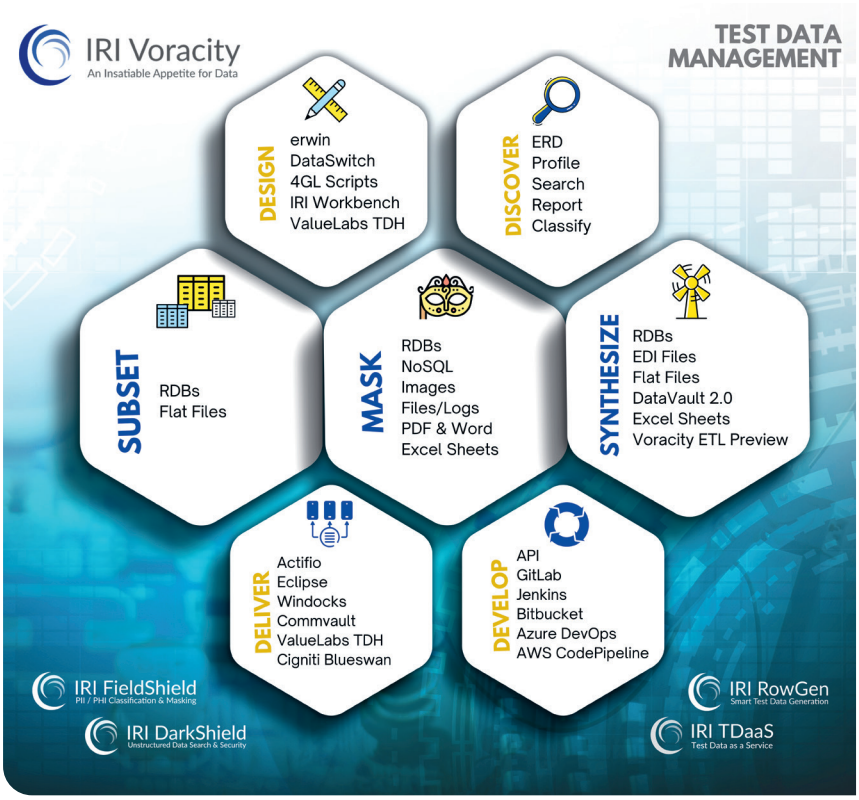
#4 Datenkonsistenz:
Sicherstellen, dass die Testdaten konsistent und zuverlässig sind, um reproduzierbare Testergebnisse zu gewährleisten.

#5 Integration in CI/CD-Pipelines:
Einbinden von Testdatenmanagementprozessen in die Continuous Integration und Continuous Delivery (kurz „CI/CD")-Pipelines, um automatisierte Tests zu ermöglichen.

#6 Synthetische Daten:
Generierung von künstlichen, aber realistischen Daten, um verschiedene Testbedingungen abzudecken, insbesondere wenn echte Daten nicht verwendet werden können oder dürfen.

Ein effektives TDM trägt dazu bei die Qualität von Softwareprodukten zu verbessern, indem es sicherstellt, dass Tests unter realistischen Bedingungen durchgeführt werden können. Das TDM hilft auch, potenzielle Probleme frühzeitig im Entwicklungszyklus zu erkennen und die Effizienz von Testprozessen zu steigern.

Die Artikelserie hebt die Testdatenverwaltungsfunktionen von IRI Voracity in verschiedenen Kontexten hervor. IRI Voracity ist eine End-to-End Datenmanagementplattform, Sie vereint Datenerkennung, -integration, -migration und -verwaltung in einem Metadaten-Framework. Die Verwendung einer einzigen Konsole ermöglicht eine effizientere Bedienung und führt zugleich zu Kosteneinsparungen in vernetzten IT-Umgebungen.



ÜBER 4 JAHRZEHNTE ERFOLG MIT BIG DATA

„IRI, The CoSort Company" ist ein US-amerikanisches Familienunternehmen, das im Jahr 1978 gegründet wurde.

Die Entwicklung des Kundenstamms und des Software-Stacks basierte auf einem leistungsfähigen Dienstprogramm namens „CoSort", das für die Verarbeitung großer Datenmengen konzipiert wurde und auch heute weltweit im Einsatz ist.

Ausblick
Es wird die Automatisierung von Testentwürfen aufgezeigt, die nicht nur die Testausführung, sondern den gesamten Testprozess umfasst. Die Herausforderung liegt in der Automatisierung aller Testprozesse, da ein Engpass in einem Teil den gesamten Prozess beeinträchtigen kann. Testdaten gelten als Engpass, historisch durch lange Lieferzeiten, insbesondere bei sensiblen Daten. IRI Voracity bietet automatisierte Funktionen für Datenentdeckung, Maskierung und Teilmengenbildung, sowie synthetische Datengenerierung. Diese Funktionen können in CI/CD-Pipelines integriert werden und bieten umfassende Möglichkeiten zur Anpassung von Testdaten.

Die Serie schließt mit der Betonung der Bedeutung von Testdaten in der Generie-

rung synthetischer Daten. Die synthetischen Daten sind realistisch, aber nicht echt und bewahren statistische Integrität. Eine präzise Anpassung der generierten Testdaten ist möglich, einschließlich der Integration in CI/CD-Pipelines.

Fazit

IRI Voracity ist eine umfassende Lösung für die Automatisierung von Testprozessen und die Generierung von realistischen, maßgeschneiderten Testdaten. Es stehen vier Methoden zur Erzeugung sicherer und intelligenter Testdaten zur Verfügung, die für verschiedene Datenquellen wie Datenbanken, Flat-Files, semistrukturierte Dateien, formatierte Berichte und sogar unstrukturierte Dateien (Dark Data) geeignet sind:

#1 Maskierung von Produktionsdaten:
Schützt sensible Informationen in Produktionsdaten durch das Ersetzen von Datenfeldern mit anonymisierten oder pseudonymisierten Werten.

#2 RDBMS-Tabellen-Subsetting und Spaltenmaskierung:
Ermöglicht die Erstellung von Teilmengen von Produktionsdatenbanktabellen und die gleichzeitige Anwendung von Spaltenmaskierung für Datenschutz.

#3 Synthese strukturierter Daten (Zufallsgenerierung/-auswahl):
Generiert realistische Testdaten durch die zufällige Erstellung oder Auswahl von strukturierten Daten.

#4 Beliebige Kombination der vorher drei gelisteten Funktionen:
Erlaubt die flexible Kombination aller genannten Methoden, um maßgeschneiderte Testdaten zu erstellen.

Die integrierten Assistenten für Tabellenersetzung und die Generierung von Testdaten erleichtern die Entwicklung von Datenbanken und Enterprise Data Warehouses (EDW) sowie die Erstellung virtueller Testdaten für DevOps. Dabei werden Kopien von Produktions-Tabellenauszügen erstellt, die maskiert und referenziell korrekt sind. Die Testdaten sind strukturell und referenziell korrekt, können für verschiedene Datenbanken und Formate synthetisch generiert oder aus Set-Dateien ausgewählt werden. Es werden über 100 Datentypen unterstützt, und die Realitätsnähe wird durch benutzerdefinierte/zusammengesetzte Datenwerte, Wertebereiche, Verteilungen sowie die Verwendung von Set-Dateien und bedingter Auswahl verbessert. Die Testdaten können in verschiedenen Umgebungen ausgeführt werden, einschließlich IRI Voracity, Value Labs TDH, Befehlszeile oder Windocks.

IRI VORACITY IST EINE UMFASSENDE LÖSUNG FÜR DIE AUTOMATISIERUNG VON TESTPROZESSEN UND DIE GENERIERUNG VON REALISTISCHEN, MASSGESCHNEIDERTEN TESTDATEN.

Amadeus Thomas, Geschäftsführer, JET-Software, www.jet-software.com

Die Testdatenbereitstellung bietet vielfältige Vorteile, darunter die Schaffung von Testdatenbanken mit referenzieller Integrität, Simulation von Datei-, Bild- und Berichtslayouts, Einhaltung von Datenschutzgesetzen, Durchführung von Belastungstests und Benchmarking. Zudem ermöglicht sie die Entwicklung und Durchführung von ETL-Tests (Extract, Transform and Load) für Enterprise Data Warehouses sowie die Erstellung umfangreicher virtueller Szenarien.

Amadeus Thomas

KI FÜR CONTENT CREATION

TEXTE BILDER, AUDIO UND VIDEO ERSTELLEN MIT ChatGPT & CO.

Mit KI-Tools wie ChatGPT und Co. ist Content Creation um ein Vielfaches einfacher geworden – zumindest wenn man weiß, wie diese Tools effektiv eingesetzt werden können.

Alexander Loth erläutert detailliert, wie Sie mit KI-Tools arbeiten können, so dass diese Ihnen dabei helfen, schnell guten Content zu erstellen. Dabei kommt es darauf an zu wissen, wie Sie mit Prompts arbeiten, die den KI-Tools möglichst genau vorgeben, was sie tun sollen, damit sie gute und möglichst hilfreiche Ergebnisse liefern.

ChatGPT kann nicht nur beim Erstellen von Texten helfen, sondern in den gesamten Workflow des Schreibens integriert werden und auch beim Strukturieren, bei Überschriften und vielem mehr helfen. So können Sie sich auch dabei helfen lassen, eine Pressemitteilung in einen Blogpost und davon ausgehend weiter in einen Social-Media-Beitrag umzuschreiben.

KI-Tools können auch hervorragend in den Content-Marketing-Prozess und in eine bestehende Content-Marketing-Strategie integriert werden.

Außerdem zeigt Loth anhand verschiedener Beispiele, welche Ergebnisse Sie von verschiedenen KI-Bildgeneratoren wie DALL-E, Midjourney, Adobe Firefly und Stable Diffusion erwarten können. Des Weiteren erläutert er hilfreiche Tools zum Erstellen von Audio und Video.

Sie finden zahlreiche praxisnahe Anwendungen und reale Fallstudien sowie vor allem konkrete Tools, Beispiele und Strategien, die Sie sofort anwenden können.

Das Buch richtet sich an alle Content-Ersteller: von freiberuflichen Kreativen über Marketingexperten und PR-Agenturen bis hin zu Unternehmern, die KI-Tools effektiv für die Content-Erstellung nutzen wollen.

KI für Content Creation – Texte Bilder, Audio und Video erstellen mit ChatGPT & Co.; Alexander Loth, mitp Verlags GmbH & Co.KG, 02-2024

Data Automation

EINFACH, SCHNELL UND SICHER ZUR DATA-ANALYTICS-LÖSUNG

Die Fähigkeit, Daten zu sammeln, zu analysieren und daraus wertvolle Einsichten zu gewinnen, ist nicht mehr nur ein Wettbewerbsvorteil – sie ist heute längst zu einer Notwendigkeit geworden. Grundlage hierfür sind leistungsstarke Data-Analytics-Lösungen.

Die SaaS-Applikation von biGENIUS automatisiert den gesamten Life-Cycle von Data-Analytics-Lösungen – von Analyse, Design und Implementierung bis Dokumentation, Monitoring und Wartung. Dies ermöglicht nicht nur eine kosteneffiziente Umsetzung, sondern auch eine flexible Anpassung und Skalierung der Lösungen, beispielsweise durch Hinzufügen neuer Datenquellen oder Modellierungen als Reaktion auf veränderte Geschäftsanforderungen. Mit biGENIUS-X ist zudem die Aktualität und Zuverlässigkeit der Daten gewährleistet, wodurch Risiken wie etwa fehlerhafte Prognosen minimiert werden. Kurz zusammengefasst können Unternehmen ihre Daten effizienter nutzen und so fundierte Entscheidungen treffen.

Um zu verstehen, wie biGENIUS-X in der Praxis funktioniert und welche Vorteile die Applikation bietet, werfen wir einen Blick auf die wichtigsten Funktionalitäten.

Getrennte Verarbeitung von Metadaten und Datenpipeline: höhere Systemstabilität

Mit der Lösung werden die Metadaten separat von der Datenpipeline verarbeitet. Man stelle sich vor, ein Team führt eine wichtige Datenmigration durch, während ein anderes gleichzeitig die Metadaten – quasi das „Inhaltsverzeichnis" dieser Daten – in biGENIUS-X aktualisiert. Dank der Applikation kann das zweite Team die Metadaten ohne Unterbrechungen oder Beeinflussungen der laufenden Datenmigration anpassen. Dies ermöglicht eine schnellere Iteration und Entwicklung, eine bessere Kontrolle über Live-Datenprozesse und eine höhere Systemstabilität.

Bereitstellung spezialisierter Wizards: effiziente Datenmodellierung

Das Tool unterstützt Datenteams auch bei der Datenmodellierung, einem essentiellen Prozess, bei dem Datenstrukturen und deren Beziehungen in einem systematischen Modell erfasst werden. Dies mit dem Ziel, Daten konsistent, logisch und effizient speichern und verarbeiten zu können. Mithilfe der spezialisierten Wizards können selbst komplexe Datenmodelle mühelos erstellt, überprüft und modifiziert werden. Das User Interface präsentiert sich dabei in einem übersichtlichen Design und ist intuitiv bedienbar. Manueller Code wird dank der Wizards massiv reduziert, wodurch sich Data Engineers auf ihre Kernaufgaben und die Lösung spezieller Modellierungsherausforderungen konzentrieren können.

Sofortige Speicherung und Versionierung mit Git: höhere Transparenz

Eine weitere Stärke liegt in der Integration von Git, einem bewährten Versionsverwaltungssystem. Dank sofortigem Speichern sind die Entwicklungen nicht nur vor Verlust geschützt, sondern jede Änderung und Anpassung wird auch präzise dokumentiert. Dies ermöglicht eine detaillierte Nachverfolgung des gesamten Projektverlaufs. In Kombination mit den fortschrittlichen Analysefunktionen von biGENIUS-X können Datenteams nicht nur Fehlerquellen schnell identifizieren und beheben, sondern auch wertvolle Einblicke in den Entwicklungsprozess und die Effizienz ihrer Dateninfrastruktur gewinnen.

Multi-User-Funktionalität: effizientere Kollaboration

Dank der Multi-User-Funktionalität können verschiedene Nutzer zeitgleich an denselben Feature Branches arbeiten und dabei die Änderungen an der Codebase nachverfolgen. So wird sichergestellt, dass keine Konflikte entstehen und Änderungen transparent und nachvollziehbar bleiben. Dies fördert nicht nur die Effizienz und Produktivität, sondern auch die Kollaboration innerhalb von Teams.

Repositories für Code und Artefakte: optimierte CI/CD-Pipeline

Änderungen und Verbesserungen an Data-Analytics-Lösungen müssen heute schnell und zuverlässig ausgerollt werden können. Auch hier leistet biGENIUS-X einen Beitrag, indem es Datenteams dabei unterstützt, ihre CI/CD-Pipeline (Continuous Integration/Continuous Deployment) zu optimieren. So werden Metadaten und generierte Artefakte in Repositories gespeichert. Änderungen und Verbesserungen können auf diese Weise effizient und einfach implementiert werden.

Orchestrierung: effizientes Load Management

Orchestrierung in der Datenverarbeitung sorgt dafür, dass verschiedene Datenlade-prozesse koordiniert ablaufen – vergleichbar mit einem Orchester, das durch einen Dirigenten geleitet wird. Auch dies gewährleistet die Applikation, denn sie sorgt dafür, dass Daten in der richtigen Reihenfolge und zum richtigen Zeitpunkt geladen und verarbeitet werden. Diese Automatisierung reduziert einerseits das Risiko von Konflikten und Fehlern und andererseits den Bedarf an manuellen Eingriffen.

> IM DATENGETRIEBENEN BUSINESS VON HEUTE HAT SICH DIE FÄHIGKEIT, RELEVANTE DATEN ZU ERFASSEN UND NUTZBAR ZU MACHEN, VOM LUXUS ZUR NOTWENDIGKEIT GEWANDELT.
>
> **Gerald Klump, CEO, biGENIUS, www.bigenius-x.com**

Visualisierungen von Data Lineage und Data Flow: bessere Entscheidungsgrundlage

Zu guter Letzt überzeugt die Lösung auch mit Visualisierungen von Data Lineage und Data Flow, die die Herkunft und den Weg von Daten durch Systeme und Prozesse abbilden. Sie dienen als Karte zur Navigation im „Datenlabyrinth". Mit biGENIUS-X können Datenteams solche Darstellungen rasch erstellen und einsehen, wodurch sie Abhängigkeiten erkennen, Bottlenecks lokalisieren und die Datenintegrität sicherstellen können. Dadurch sind sie auch in der Lage, fundiertere und zielgerichtete Entscheidungen auf Basis ihrer Datenlandschaft zu treffen.

INTEGRATION, AKTUALITÄT UND SICHERHEIT

Als Cloud-Lösung punktet biGENIUS-X ergänzend dazu mit folgenden Vorteilen:

- Einfache Implementierung und Skalierbarkeit: Eine langwierige Installation fällt weg, genauso wie Wartungsarbeiten. Das Tool lässt sich als Cloud-Anwendung nahtlos in bestehende Systeme integrieren und gemäss den Anforderungen des Unternehmens skalieren.
- Immer auf dem neuesten Stand: Mit der Lösung profitieren Datenteams immer automatisch von den neuesten Funktionen, Updates und Bug Fixes.
- Hosting der Extraklasse mit Azure: Dank der Partnerschaft von biGENIUS und Microsoft kommt die hohe Sicherheit und Performance von Azure voll zum Tragen.

FAZIT

Im datengetriebenen Business von heute hat sich die Fähigkeit, relevante Daten zu erfassen und nutzbar zu machen, vom Luxus zur Notwendigkeit gewandelt. Die Dynamik und Komplexität heutiger Geschäftsanforderungen erfordern leistungsstarke und kosteneffiziente Data-Analytics-Lösungen. Mit biGENIUS-X können diese einfach, schnell und sicher umgesetzt werden.

Von einer verbesserten Systemstabilität und vereinfachten Datenmodellierung mit intuitivem User Interface über ein effizientes Load Management und eine erhöhte Transparenz bis hin zur effizienten Kollaboration bietet die Applikation alles, was Datenteams benötigen, um – im wörtlichen und übertragenen Sinn – die Hoheit über ihre Daten zu behalten. Gepaart mit den Vorteilen einer Cloud-Lösung, wird die Lösung zu einer unverzichtbaren Applikation für jedes datenorientierte Unternehmen.

Gerald Klump

Potenziale freisetzen

DIE MACHT DER IT-UNTERNEHMENSARCHITEKTUR

Der erste Schritt auf dem Weg zu einer erfolgreichen Digitalisierung ist das Überdenken der eigenen Unternehmensarchitektur. Zur Förderung von Innovation und Effizienz im Unternehmen ist dies nicht nur notwendig, sondern auch eine ideale Chance, um die eigenen IT-Infrastrukturen effizienter zu gestalten und dadurch neue Ressourcen für strategische Unternehmensinitiativen freisetzen zu können. Gelingen kann dieser Neuanfang im Rahmen eines mehrstufigen Wertschöpfungsprozesses, durch den Unternehmen auf Basis einer soliden Ist-Analyse eine zukunftsorientierte Zielarchitektur entwickeln können. Am Ende dieses Prozesses steht das Modell einer „Enterprise Architecture as a Service", mit der eine kontinuierliche digitale Transformation möglich wird.

Das Enterprise Architecture Framework

Als Digitalisierungsberatung für nachhaltige Innovation haben wir für unsere Kunden einen detaillierten Prozess entwickelt, der sich auf vier zentrale Ebenen der Unternehmensarchitektur – Unternehmensstrategie, Lösungsarchitektur, Betriebsarchitektur und Datenmodelle – stützt, die den Systemaufbau eines Unternehmens bestimmen. Dieses Enterprise Architecture Framework, das wir hier vorstellen, startet mit der Unternehmensstrategie: Sie dient als notwendiges Fundament, um die ambitionierten Ziele eines Unternehmens fokussiert zu erreichen. In dieser Phase werden Visionen entworfen, Kompetenzen und strategische Pfade geklärt und definiert. Auch die Entwicklung von User Stories zur Erreichung der Unternehmensziele unterstützt den Prozess auf dieser ersten Ebene.

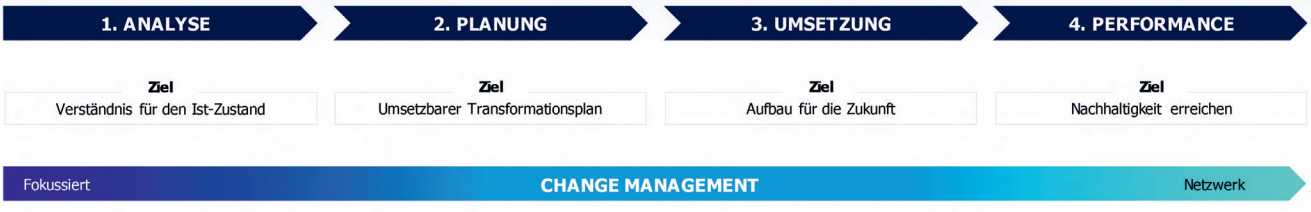
Auf der zweiten Ebene, der Lösungsarchitektur, liegt der Fokus auf der Entwicklung kundenorientierter und interner Systeme, die zur Erfüllung der zuvor festgelegten strategischen Ziele eingesetzt werden. Die für den Einsatz vorgesehenen Technologien und Systeme müssen direkt zur Umsetzung der entwickelten Unternehmensvision beitragen. Die Betriebsarchitektur betrachten wir in unserem Framework als dritte Ebene, in der das Zusammenspiel der Systeme im Mittelpunkt steht. Daten- und Content-Flows müssen in diesem Schritt genau analysiert und optimiert werden, um reibungslose und effiziente Systeminteraktionen zu gewährleisten. Schließlich gibt es als vierte zentrale Ebene noch die Datenmodelle, durch die eine solide und zuverlässige Datenbasis geschaffen wird, auf denen die verschiedenen Systeme operativ tätig werden.

Von der Analyse zur Performance

Unser Framework bildet einen ganzheitlichen Ansatz ab, bei dem IT-Architektur als Voraussetzung für Unternehmensstrategie betrachtet wird. Eine synchrone Abstimmung zwischen Unternehmensstrategie und IT-Architektur ist aus unserer Sicht daher entscheidend für den unternehmerischen Erfolg. Die IT-Unternehmensarchitektur wird hierbei aus einer High-Level-Perspektive betrachtet und der Fokus liegt auf den wesentlichen funktionalen Bausteinen, die notwendig sind, um eine robuste Verbindung zwischen den Geschäftsanforderungen und den IT-Kapazitäten sicherzustellen. Für die Lösungsarchitektur ist eine Hersteller-unabhängige Perspektive zentral: Unternehmen sollten Systemlösungen unabhängig vom Hersteller auswählen, um höchstmögliche Flexibilität und Anpassungsfähigkeit zu erreichen. Die Systemarchitektur ist die detaillierteste Ansicht mit dem Fokus auf herstellerspezifischen sowie eigenentwickelten Systemen, um die Architektur in allen Einzelheiten darzustellen.

VORGEHENSWEISE | VON DER ANALYSE ZUR PERFORMANCE

VIER SCHRITTE BEGLEITEN DIE TRANSFORMATION DER UNTERNEHMENS- UND IT-ARCHITEKTUR



Quelle: OMMAX

Der Transformationsprozess der Unternehmens- und IT-Architektur gestaltet sich im Rahmen dieses Frameworks als ein sorgfältig choreographierter Change-Management-Prozess, der vier Stufen von der Analyse über die Planung und Umsetzung bis hin zur Performance durchläuft.

Die Analysephase ist dabei sehr wichtig, da hier ein tiefgreifendes Verständnis für den aktuellen Ist-Zustand des Unternehmens geschaffen wird. Dabei darf nichts dem Zufall überlassen werden: Jede Nuance des bestehenden Systems wird genau unter die Lupe genommen. In der Planungsphase wird darauf hingearbeitet, einen pragmatischen und umsetzbaren Transformationsplan zu erstellen. Die entwickelten Strategien müssen entsprechenden Ressourcen zugeordnet werden, um die Transformation wirksam vorantreiben zu können. Die Umsetzungsphase ist gekennzeichnet durch die aktive Entwicklung und immer wieder auch notwendigen Anpassungen sowie die Implementierung neuer Systeme und Strategien. In dieser Phase wird die Transformation real und greifbar, der Aufbau für die Zukunft des Unternehmens wird hier ganz konkret sichtbar. In der abschließenden Performance-Phase müssen Unternehmen unbedingt die Wirksamkeit ihrer implementierten Änderungen bewerten, da hier das Ziel ist, eine wirkliche Nachhaltigkeit der Transformation zu erreichen.

Wie man eine IT-Architektur-Transformation zum Erfolg führt

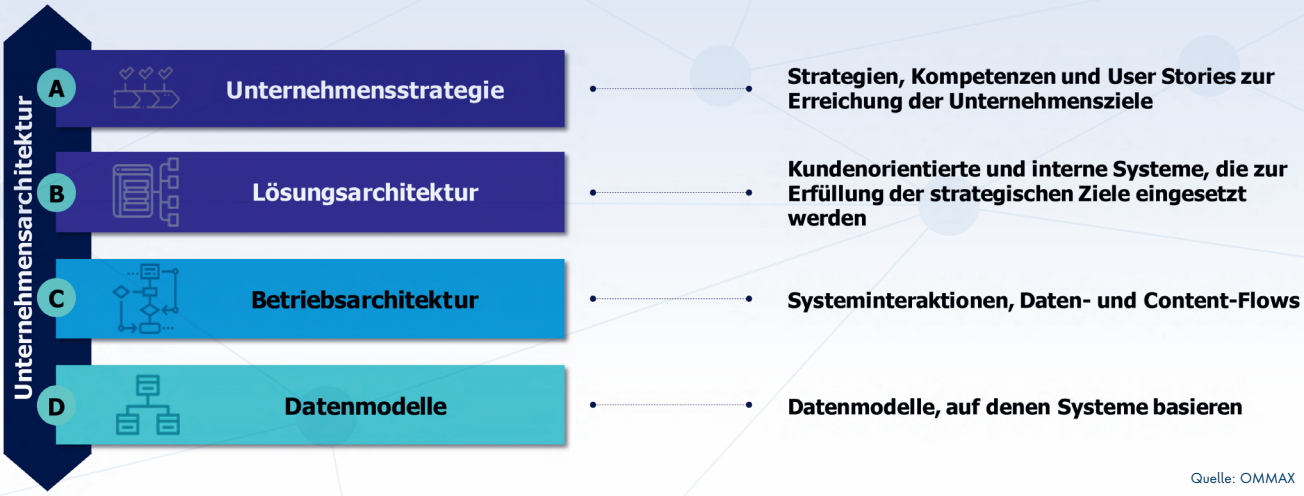
Es gibt einige Kernelemente, die das Fundament jedes erfolgreichen Transformationsprozesses bilden und die in jeder Phase berücksichtigt werden sollten: Menschen, Prozesse, Ergebnisse und Unternehmenspolitik sind die tragenden Säulen, die für das Gelingen einer Transformation entscheidend sind. Dabei beginnt ein erfolgreicher Change-Prozess bei den Menschen, den wahren Treiber jeder Transformation. Ihre Fähigkeiten, Kenntnisse und das Engagement bilden das Rückgrat jeder erfolgreichen Initiative. Ihre Motivation und Hingabe sind deshalb essenziell, und jede Phase der Transformation sollte darauf ausgerichtet sein, Ergebnisse zu liefern, die das Team nicht nur motivieren, sondern auch in seiner Entwicklung und seinem Wachstum unterstützen. Da erfolgreiche Initiativen nur von erfolgreichen Teams getragen werden können, müssen sich die Ergebnisse auch auf die Menschen in der Initiative konzentrieren.

Gleichzeitig sind effiziente Prozesse ein weiteres zentrales Element des Transformationsprozesses. Sie müssen flüssig und reibungslos konzipiert sein, damit sie wirklich nachhaltigen Fortschritt und kontinuierliche Verbesserung fördern. Nur so lässt sich die Agilität und Fähigkeit des Unternehmens unterstützen, sich proaktiv an neue Herausforderungen und Chancen anzupassen und dadurch zukunftsfähig zu bleiben. Denn das Ergebnis jeder Phase ermöglicht die Durchführung der Initiative oder hat direkte Auswirkungen auf die Gesamtstrategie.

Zudem muss das Zusammenwirken von Menschen und Prozessen anhand der dadurch erzielten Ergebnisse immer wieder sorgfältig analysiert und bewertet werden. Denn das gesamte Projekt wird immer an den Ergebnissen gemessen, und

OMMAX ENTERPRISE ARCHITECTURE FRAMEWORK

DAS OMMAX ENTERPRISE ARCHITECTURE FRAMEWORK ERSTRECKT SICH ÜBER DIE VIER WICHTIGSTEN EBENEN, DIE DEN SYSTEMAUFBAU EINES UNTERNEHMENS BESTIMMEN – UNTERNEHMENSSTRATEGIE, LÖSUNGSARCHITEKTUR, BETRIEBSARCHITEKTUR UND DATENMODELLE



Quelle: OMMAX

jede Phase muss deshalb auch einen klaren und messbaren Wert für die Beteiligten innerhalb des Projekts haben. Erst wenn die aus dieser Symbiose entstehenden Strategien und Taktiken wirksam sind, entsteht nämlich eine Grundlage, mit der sich auch zukünftige Innovationen und Verbesserungen im Unternehmen aktivieren lassen.

Schließlich spielen unternehmenspolitische Aspekte eine wichtige Rolle, da sie die Rahmenbedingungen und den Kontext bestimmen, in dem die Transformation stattfindet. Alles ist miteinander verbunden. Deshalb muss auch in jeder Phase der potenzielle Einfluss auf die Unternehmenspolitik innerhalb und außerhalb des eigenen Bereichs berücksichtigt werden. Dies ist eine Voraussetzung, damit Unternehmen gute strategische Entscheidungen treffen können, die den Erfolg ihrer Veränderungsinitiativen unterstützen und fördern. In ihrer Gesamtheit bilden diese Elemente ein kohärentes und integriertes Ökosystem, das die Transformation der IT-Architektur vorantreibt und in der jedes Element für die Schaffung eines harmonischen und erfolgreichen Transformationsprozesses unerlässlich ist.

MEHR WERT

Vortrag: Potenziale freisetzen

Die Unternehmensarchitektur auf die nächste Stufe bringen

Die praktische Umsetzung unseres OMMAX Frameworks zur Transformation der IT-Architektur definiert sich in unserem „Enterprise Architecture as a Service" (EAaaS)-Modell. EAaaS beantwortet die wesentlichen Fragen, die sich Unternehmen stellen sollten, die ihre IT-Architektur, und damit ihre Unternehmensarchitektur auf die nächste digitale Stufe bringen und die Umsetzung ihrer IT-Transformationen beschleunigen sollen. Diese sind zum Beispiel:

- #1 Wie sieht die aktuelle IT-Landschaft aus?
- #2 Was muss beachtet werden, wenn eines meiner IT-Systeme aufgerüstet werden soll?
- #3 Wie hoch ist der Aufwand für die Integration eines neuen IT-Systems in meine aktuelle IT-Landschaft?
- #4 Welche APIs sind derzeit verfügbar und welche Informationen liefern sie?

Solche Fragen, die im Rahmen des EAaaS-Modells analysiert werden, führen dazu, dass Unternehmen ihre Ausgangsposition präzise bestimmen können. Im Ergebnis erhalten sie auf diese Weise:

- einen einfachen Überblick über ihre aktuelle IT-Landschaft
- eine Skizzierung möglicher Ad-hoc-Szenarien für ihre IT-Architektur und möglicher „Was-wäre-wenn-Analy-

sen" während der Projektdurchführung
- eine transparente und aktuelle Übersicht über ihre IT-Architektur
- eine Integrationsunterstützung für Upgrades in ihrer IT-Landschaft
- die Befähigung der DevOps-Organisation

Unternehmen müssen sich dabei aber im Vorfeld auch über die Herausforderungen klar werden, die immer mit dem Transformationsprozess verbunden sind. Ein wichtiger Aspekt ist dabei der Kostenfaktor, denn jedes IT-Projekt muss zunächst in eine umfassende Analyse des aktuellen Ist-Zustands der Architektur investieren – die Grundlage für den Erfolg der Transformationsinitiative. Das Fehlen eines „Single Point oft Truth" kann zu Schwierigkeiten führen, wenn etwa Anwendungslandschaften über mehrere PowerPoints, Excel und Applikations-Repositories verteilt sind. Ebenfalls können Abhängigkeiten im Transformationsprojekt Schwierigkeiten heraufbeschwören, wenn das Wissen über die IT-Architektur etwa sehr stark von einzelnen Personen abhängig ist. Unternehmen müssen auch den Zeit-Faktor im Auge behalten, denn fast alle Integrationen und Aktualisierungen der IT-Architektur sind in der Regel zeitintensiv und sehr komplex.

Mit EAaaS digitale Change-Projekte erfolgreich meistern

EAaaS bietet hier einen klaren und präzisen Weg, damit Unternehmen die gewünschten Ziele ihres Transformationsprojekt bei der Aktualisierung ihrer IT-Architektur auch erreichen. Und das sind:

- Ein wertorientiertes Management ihrer Unternehmensarchitektur
- Eine frühzeitige Architekturanalyse bei ihren IT-Projekten
- Eine vollumfängliche Unterstützung der IT-Organisation
- Ein nachhaltiges Wissensmanagement
- Die schnelle und sorgfältige Unterstützung bei Integrationen von Anwendungen

In der Praxis hat OMMAX die erfolgreiche Implementierung dieses Frameworks bereits für unterschiedlichsten Business Cases evaluiert. Von der technischen Optimierung von Webseiten über die Integration von Self-Service-Plattformen bis hin zur Entwicklung ausgeklügelter Reporting-Suites für digitales Performance-Management – mit der strategischen und durchdachten Anwendung des EAaaS-Frameworks lassen sich selbst herausfordernde Digitalisierungsprojekte zu einem nachhaltigen Erfolg führen und unterstützt Unternehmen dabei, sich zukunftsfähig aufzustellen und selbst in dynamischsten Marktsituationen handlungsfähig zu bleiben.

Ina Roth

DER ERSTE SCHRITT AUF DEM WEG ZU EINER ERFOLGREICHEN DIGITALISIERUNG IST DAS ÜBERDENKEN DER EIGENEN UNTERNEHMENSARCHITEKTUR.

Ina Roth,
Director of Tech Delivery, OMMAX,
www.ommax-digital.com/de/

ENTERPRISE ARCHITECTURE AS A SERVICE

WIE SIE IHRE IT-ARCHITEKTUR AUF DIE NÄCHSTE STUFE BRINGEN

Herausforderungen

- **Kosten -** jedes IT-Projekt muss in eine umfassende Analyse des aktuellen Ist-Zustands der Architektur investieren
- **Single Point of Truth fehlt -** Anwendungslandschaften sind über mehrere PowerPoints, Excel und Anwendungs-Repositories verteilt
- **Abhängigkeit -** das Wissen über die IT-Architektur ist stark von einzelnen Personen abhängig
- **Zeit -** Integrationen und Aktualisierungen der IT-Architektur sind zeitintensiv und komplex

Gewünschte Ergebnisse

1. **Wertorientiertes** Management der Unternehmensarchitektur
2. **Frühzeitige Architekturanalyse** bei IT-Projekten
3. **Unterstützung** der IT-Organisation
4. **Nachhaltiges** Wissensmanagement
5. **Schnelle und sorgfältige** Unterstützung bei Integrationen von Anwendungen

Quelle: OMMAX

it management

AUSGABE 3-4/2024
ERSCHEINT
AM 1. MÄRZ 2024

UNSERE THEMEN

30 Jahre it management
Nachhaltigkeit
Industrial Transformation

it security

AUSGABE 3-4/2024
ERSCHEINT
AM 1. MÄRZ 2024

UNSERE THEMEN

Industrial IT Security
Ransomware
Identity Access Management

WIR WOLLEN IHR FEEDBACK

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

INSERENTENVERZEICHNIS

it management

it verlag GmbH	U2, U4
USU Software AG	7
Deutsche Messe AG	9
Konica Minolta Business Solutions Deutschland GmbH (Advertorial)	23
TOPdesk Deutschland GmbH (Advertorial)	27
DSAG e.V.	55
E3/B4B Media	U3

it security

it verlag GmbH	U2, U3
Deutsche Messe AG	17
genua GmbH	U4

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: Ralf Bachthaler, Judith Beck, Lars Becker, Philipp von der Brüggen, Horst Droege,Thomas Heinevetter, Jens Hungershausen, Gerald Klump, Carina Mitzschke, Angelika Mühleck, Silvia Parthier, Ulrich Parthier, Guido Piech, Bernd Rischer, Ina Roth, Paul Schwefer, Peter Stanjeck, Guido Simon, Dmitrij Spolwind, Christian Tauchmann, Amadeus Thomas, Marius Wagner, Ralph Weiss, Klaus Ziegerhofer, Stefan Zizelmann

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
und BTP Summit 2024
28. und 29. Februar 2024
Heidelberg
e3mag.com/de/steampunk-summit
Abap auf der SAP Business Technology Platform, BTP, wird nach Meinung der SAP-Community die bestimmende ERP-Strategie. Der Summit 2024 präsentiert Steampunk, Embedded Abap und BTP als aktuelle SAP-Basis und S/4-Hana-Nachfolger.
Wird gesponsert von:
snap consulting
Security Bridge™
Eine Veranstaltung vom E3-Magazin:
e3mag.com

Fokustag
IAM
+

WE SECURE IT

17. bis 19. April

Digitalevent

#WesecureIT2024

it-daily.net

Mehr erfahren

Eine Veranstaltung von itsecurity & it-daily.net

it security

Detect. Protect. Respond.
Januar/Februar 2024

EFFIZIENTE CYBERSICHERHEIT

Expertise, Mensch, Services & Technologie

Stefan Fritz, Sophos

SICHERER EINSATZ VON KI

Von wegen Drahtseilakt!

SECURITY@ WORK

Content Disarm and Reconstruction

SICHERE AUTHENTIFIZIERUNG

Im Visier der Cyberkriminellen

www.it-daily.net

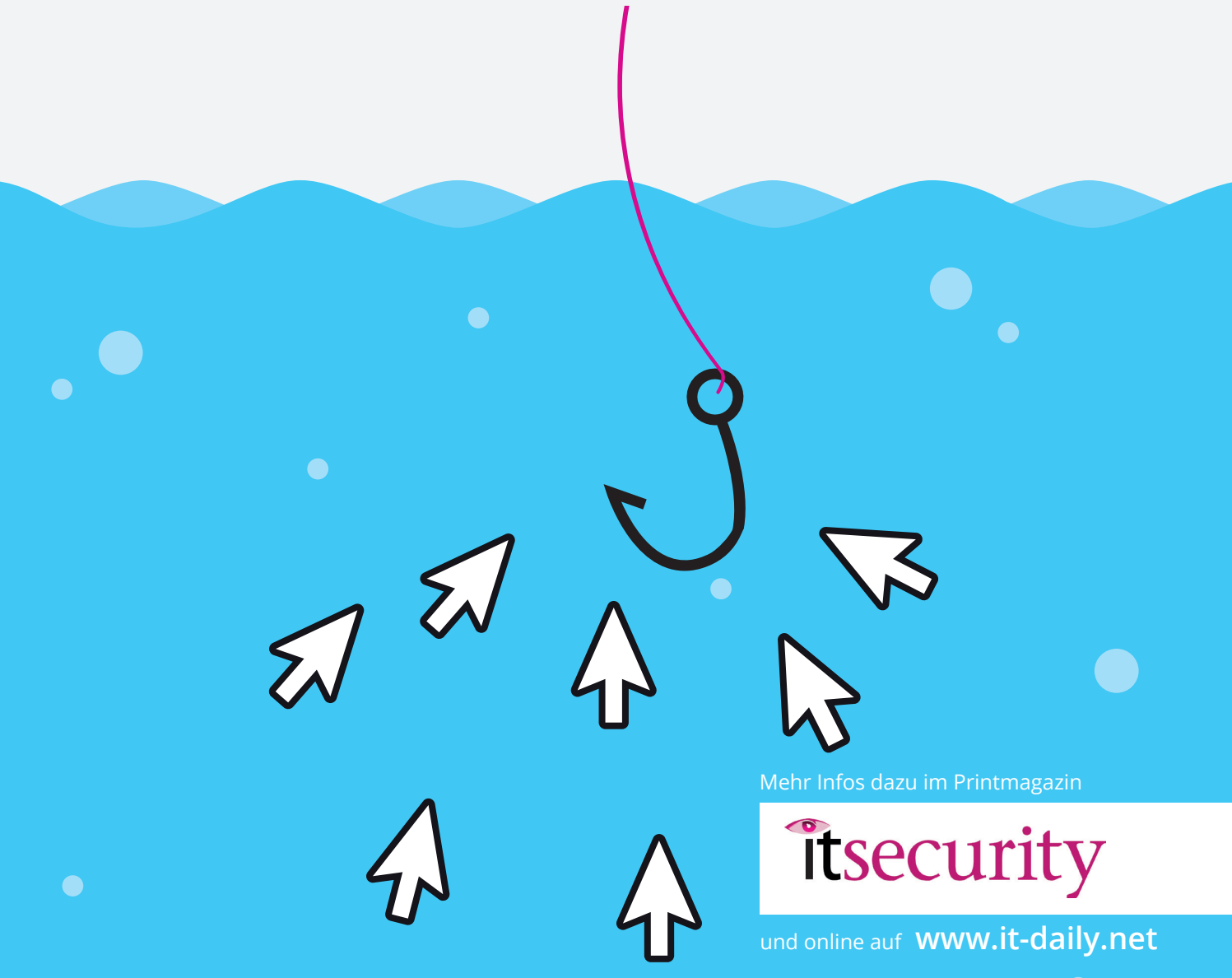
Phi·shing

/'fɪʃɪŋ/

Substantiv, Neutrum [das]

englisch phishing, zu: fishing = das Fischen;
die ph-Schreibung als häufig gebrauchte Verfremdung im Hackerjargon für f wohl nach englisch-amerikanisch phreaking = das Hacken (zu: freak, Freak).

Beschaffung persönlicher Daten anderer Personen (Passwort, Kreditkartennummer o. Ä.) mit gefälschten E-Mails oder Websites.



Inhalt

COVERSTORY

4 **Effiziente Cybersicherheit**
Ökosysteme aus Menschen, Expertise, Services und Technologie

IT SECURITY

6 **Ein Blick in die Glaskugel**
2024 steht im Zeichen von Sicherheit und Automatisierung

8 **Ausblick auf 2024**
KI verschärft die Bedrohungslage

12 **Im Visier der Cyberkriminellen**
Effektive Abwehr durch sichere Authentifizierung

14 **Passwort knacken? – Kein Problem!**
ChatGPT und Automatisierung erleichtern Passwort-Cracking-Angriffe

18 **Von wegen Drahtseilakt!**
So gelingt Unternehmen der sichere Einsatz von KI-Lösungen

20 **KI basiertes IAM**
Eine Revolution der Identitätsverwaltung kommt auf uns zu

22 **Konvergente Identitätssicherung**
Ein neuer Begriff bahnt sich seinen Weg

25 **Mit Macht ins Cyberrisiko**
Sicherheitsrisiko Führungsetage

26 **Security@Work**
Content Disarm and Reconstruction

31 **Zero Trust**
Ganzheitlicher Ansatz für umfassende Sicherheit

32 **Cybersecurity auf Applikationsebene**
Der blinde Fleck in der IT-Sicherheitsstrategie

36 **API-Sicherheit neu definiert**
Mehr Schutz für komplexere Infrastrukturen

40 **Fein-granulare Autorisierung**
Warum der Hype?

44 **Kritischer Blick gefragt**
Die Wahrheit hinter den Werbeversprechen von VPN-Anbietern

22

18

Effiziente Cybersicherheit

ÖKOSYSTEM AUS MENSCHEN, EXPERTISE, SERVICES UND TECHNOLOGIE

Cybersicherheit ist und bleibt eines der wichtigsten Themen für Unternehmen. Wie die Unternehmen die heutigen Lösungen, Angebote und Services nutzen, welche Rolle die IT-Dienstleister und Managed Service Provider dabei spielen und wie die Aussichten für 2024 sind, bespricht IT-Security Chefredakteur Ulrich Parthier mit Stefan Fritz, Director Channel Sales für EMEA Central bei Sophos.

Ulrich Parthier: *Die Cybersicherheit wird zunehmend aus den Unternehmen in die Hände von spezialisierten Dienstleistern gegeben. Ist CSaaS für alle Unternehmen eine Option?*

Stefan Fritz: Cybersecurity as a Service (CSaaS) ist eine hervorragende Möglichkeit, für jedes Unternehmen eine noch bessere Sicherheit vor Angreifern aus dem Internet zu etablieren. In der sich ständig wandelnden Landschaft der Cyberbedrohungen ist es von entscheidender Bedeutung, dass Unternehmen schnell und effizient reagieren können. Neben der technischen Sicherheit, die mit vernetzten Sicherheitslösungen und dem Einsatz von KI sichergestellt werden kann, bietet CSaaS die erforderliche Agilität, um den vielfältigen Bedrohungen entgegenzuwirken. Diese extern bezogene Leistung kann nicht nur einen großen Teil der sicherheitsrelevanten Aspekte in Unternehmen übernehmen und den Schutz der IT-Infrastruktur verbessern, sondern durch die menschliche Komponente und Expertise den Schutz auf ein noch höheres Niveau heben.

Ulrich Parthier: *Wie weit ist CSaaS Ihrer Meinung nach bereits verbreitet?*

Stefan Fritz: Aus unserer Sicht ist CSaaS nicht nur ein Trend, sondern vielmehr das, was Unternehmen seit langem gesucht haben und jetzt endlich erhalten. CsaaS hat bereits heute eine große Akzeptanz sowohl bei Unternehmen als auch bei Managed Service Providern erreicht. Wir haben dazu erst kürzlich Unternehmen in Deutschland über die Nutzung von CSaaS befragt. Die Ergebnisse bestätigen, dass CSaaS heute und in Zukunft eine der besten Methoden ist, Unternehmen zu schützen. Laut unserer Umfrageergebnisse nutzen bereits 46 Prozent der Befragten die Security-Services, 35 Prozent befindet sich in der Implementierung und weitere 13 Prozent planen den Einsatz in den nächsten 12 Monaten. Ich denke, deutlicher kann die Nachfrage nach CSaaS kaum bestätigt werden.

Ulrich Parthier: *Das sind beeindruckende Umfrageergebnisse. Welche Faktoren hindern Unternehmen daran, sich für die Implementierung von CSaaS zu entscheiden?*

Stefan Fritz: Hierzu gibt es keine einfache Antwort. An erster Stelle steht meiner Meinung nach die Beratung der Unternehmen. Dem Channel ist bewusst, dass gute Geschäfte im Bereich Cybersecurity nicht mehr nur mit einer rein technologiefokussierten Strategie realisierbar sind. Die Vermittlung von Know-how und individuelle Gespräche mit den Kunden sind ebenso ein absolutes Muss, wie das Anbieten von Security-Services. Entsprechend hat sich die Qualität der Kundenberatung und das Portfolio der Partner in den letzten Jahren enorm gewandelt und verbessert – eine Entwicklung, die auch wir als Hersteller forcieren.

Zweitens geht es um Vertrauen. Ein Managed Service Provider, der eine der wichtigsten Aufgaben eines Unternehmens mit seinen Services übernehmen soll, muss beim Kunden ein hohes Vertrauen genießen. Zu hoch ist die Gefahrenlage, um sich bei der Security auf ein vages Spiel einzulassen.

Der dritte Grund ist der Fachkräftemangel. Das klingt paradox, denn gerade dieser sollte Unternehmen dazu veranlassen, die Aufgaben, die sie selbst intern nicht zufriedenstellend lösen können, an externe Spezialisten zu übergeben. Allerdings ist bei vielen Unternehmen die Personallage derart angespannt, dass oftmals schlicht nicht die Zeit dafür zur Verfügung steht, sich um externe Security-Services und Angebote zu kümmern.

Ulrich Parthier: *Was sind die Hauptkriterien, die bei Kunden zu Security-Services führen?*

Stefan Fritz: Für uns steht und fällt die gesamte Argumentations- und Entscheidungskette mit unseren Partnern. Sie sind das entscheidende Bindeglied zwischen uns als Entwickler und Anbieter von Security-Lösungen und den Kunden – sowohl was klassische Security als auch die Services angeht. Das bedeutet natürlich, dass wir unsere Partner entsprechend schulen und betreuen, damit

diese wiederum CSaaS bei ihren Kunden an der richtigen Stelle und zum richtigen Zeitpunkt platzieren und verargumentieren können. Zudem haben die Kunden sehr spezifische Anforderungen an die IT- und Security-Dienstleister. Beispielsweise legten in unserer Umfrage 30 Prozent der befragten IT-Verantwortlichen großen Wert auf die Branchenkompetenz des Serviceproviders. Zudem war bei 29 Prozent die Skalierbarkeit der Dienste, sowohl technisch als auch kommerziell, sehr wichtig.

Ulrich Parthier: *Sie sprachen den Fachkräftemangel an. Dieser betrifft nicht nur Ihre Endkunden, sondern auch Ihre Partner und Sie selbst?*

Stefan Fritz: Das ist richtig, viele Unternehmen klagen über den Fachkräftemangel. Vielleicht sollte man neue Wege gehen und lernen, wie man dem Mangel entgegentreten und die Situation verbessern kann. Die Kluft zwischen Mangel und Angebot könnte kleiner sein, wenn wir bei den Bewerbungen von Sicherheitsexperten aufgeschlossener sind und die Vielfalt der potenziellen Bewerber gutheißen. Menschen mit einer Leidenschaft für die Security, die jedoch in ihrer Vergangenheit teils ganz andere Ausbildungen durchlaufen haben, sind enorm wichtig. Wir müssen offener denken, denn sie haben ein Potenzial Lücken zu erkennen, die reine Software-Ingenieure oder Datenschutzexperten vielleicht nicht bemerken. Unternehmen, die dies berücksichtigen, haben oftmals weniger zu klagen als solche, die zwar ein gutes Jobangebot haben, beim Lebenslauf jedoch eingleisig entscheiden.

Ulrich Parthier: *Der Jahresbeginn ist auch immer die Zeit, um über die Zukunft zu sprechen. Was erwarten Sie sich vom Jahr 2024?*

Stefan Fritz: Ich glaube, dass sich eindeutige Trends für 2024 abzeichnen. Einer davon ist, dass die Lieferketten zunehmend im Fokus der Cyberkriminellen stehen. 2023 erfolgten immer mehr Attacken nicht über das anvisierte Unternehmen direkt, sondern über einen Geschäftspartner. Noch überschaubar ist der Einsatz von Künstlicher Intelligenz bei den Angreifern. Im Moment wird diese Technologie hauptsächlich im Social Engineering eingesetzt, um Phishing-Attacken zu perfektionieren. Der große Einsatz von KI ist, meiner Meinung nach, bei Cyberattacken noch nicht passiert. Ein weiterer Aspekt für 2024 ist die Tatsache, dass immer mehr vernetzte Geräte mit niedriger Sicherheitsqualität zum Einsatz kommen. Während beispielsweise bei der Sicherheit von Smartphones große Fortschritte erzielt wurden, kommen solche Vorsichtmaßnahmen beim Internet der Dinge, den betrieblichen Sicherheitstools und einem Großteil der Unternehmenssoftware, leider immer noch viel zu kurz.

Zusammengefasst wird uns allen die Arbeit, um die Cybersicherheit an noch mehr Stellen zu verbessern und die Cyberresilienz von Unternehmen zu stärken, nicht ausgehen. Ein positiver Aspekt zum Schluss: Während der letzten Jahre haben die Cybersicherheitsanbieter gewaltige Schritte nach vorne gemacht und wir haben den Einsatz, die Mittel, das Wissen und die Finanzen, die Cyberkriminelle aufwenden müssen, enorm erhöht. Immer mehr können diesem Druck nicht standhalten und geben auf.

Ulrich Parthier: *Herzlichen Dank für das Gespräch Herr Fritz.*

Ein Blick in die Glaskugel

2024 STEHT IM ZEICHEN VON SICHERHEIT, AUTOMATISIERUNG UND KONSOLIDIERUNG

Immer weniger Hackerangriffe, State-of-the-Art-Technologie in der gesamten Infrastruktur und ein saftiges Budget: So sieht die Zukunft der IT wohl nur in den Träumen der Verantwortlichen aus. Die bittere Realität stellt sich ziemlich gegenteilig dar und der ständige Wandel macht die Situation auch nicht einfacher. Eine aktuelle Studie von Omdia, einem unabhängigen Beratungsunternehmen, und dem Plattformanbieter NinjaOne zeigt, was für Unternehmen in 2024 und darüber hinaus im Fokus steht und wie IT-Teams sich für die nächsten Jahre rüsten.

Erst Prioritäten setzen, dann Budgets verplanen

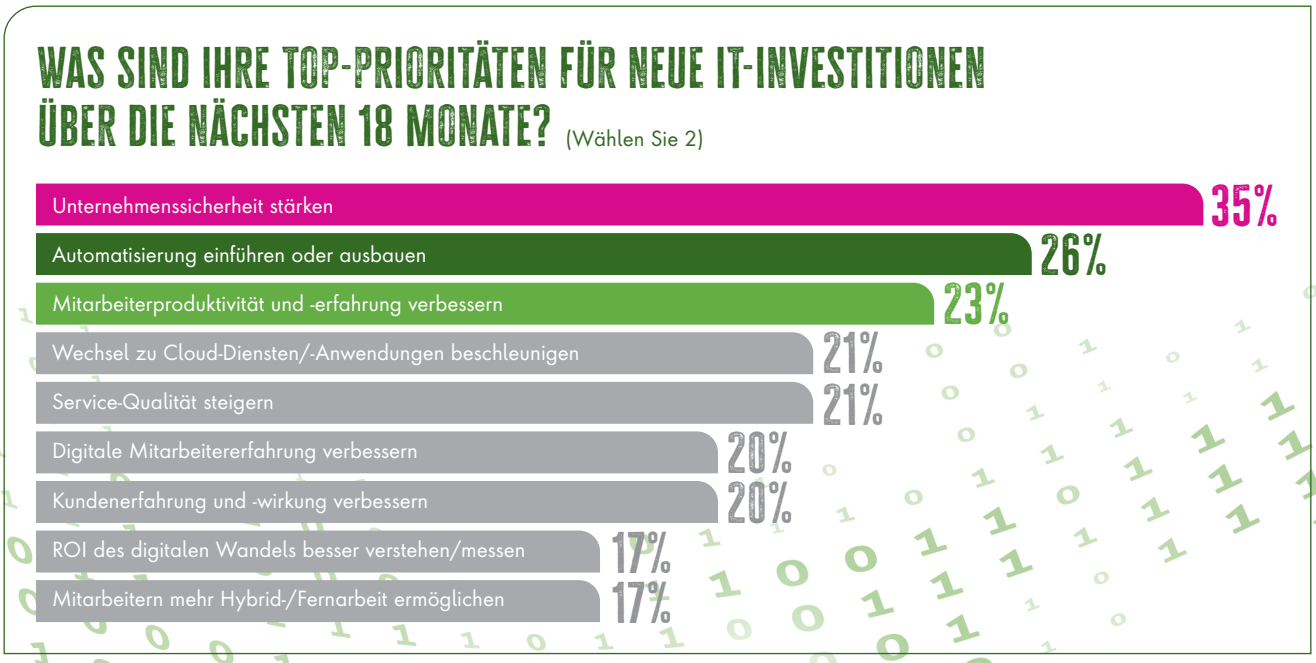
Die Automatisierung hat sich für Unternehmen aller Größen, Branchen und Regionen zu einer der wichtigsten Prioritäten entwickelt. Und auch das Thema Sicherheit steht für die meisten Betriebe ganz oben auf der Agenda für 2024, dicht gefolgt von der Produktivität der Endbenutzer und der damit verbundenen Umgestaltung von Arbeitsplätzen. Dabei fällt sofort auf, dass all diese Schwerpunktthemen eng miteinander verwoben sind: Ohne Automatisierung lässt sich heute kaum noch ein Unternehmen zuverlässig absichern, dafür sind die Infrastrukturen und Prozesse inzwischen zu komplex. Muss beispielsweise jedes Softwareupdate an jedem einzelnen Endgerät manuell eingespielt werden, bietet das aufgrund der enorm langen Bearbeitungszeit nicht nur ein willkommenes Einfallstor für Cyberattacken, sondern beeinträchtigt auch die Produktivität der Teams enorm. Ihnen käme wiederum automatisiertes Patch Management zugute, um ihre wertvolle Arbeitszeit in anspruchsvollere Aufgaben investieren zu können. Im Umkehrschluss erfordert die Umstellung auf moderne Arbeitsplätze für produktive Remote-Teams auch die entsprechenden Sicherheitskonzepte sowie automatische Workflows, die orts- und zeitunabhängiges Arbeiten überhaupt erst ermöglichen.

Mit Blick auf diese drei wichtigsten Prioritäten ergeben sich die Investitionspläne für das kommende Jahr quasi von selbst: 35 Prozent der befragten Unternehmen werden Budget in die Stärkung ihrer Security-Maßnahmen stecken, 26 Prozent investieren in Automatisierung und 23 Prozent in die Produktivität und ein attraktives Arbeitsumfeld für ihre Mitarbeitenden. Im internationalen Vergleich fällt allerdings bei deutschen Unternehmen eine Besonderheit auf: 24 Prozent der IT-Verantwortlichen hierzulande ist es besonders wichtig, den ROI ihrer Digitalisierungsprojekte zu messen. Sie möchten noch besser verstehen, in welchem Maße sich die Investitionen in die digitale Transformation tatsächlich auszahlen. Dieses Ergebnis unterstreicht den massiven Druck auf die IT als Profit Center. Es zeigt deutlich, wie wichtig hier der Blick auf die Ausgaben ist – auch wenn die Bedrohungen durch Cyberkriminalität und die Notwendigkeit zur Modernisierung kaum noch zu leugnen sind.

Neben der Sicherheit, Automatisierung und Produktivität steht der Mittelstand im Jahr 2024 zusätzlich vor der Herausforderung, auch die Verbesserung der allgemeinen Servicequalität, die Customer Experience und die Umstellung auf die Cloud nicht aus den Augen zu verlieren. All diese Bereiche können im Wettbewerb erfolgsentscheidend sein und erfordern ebenfalls Investitionen. Hier gilt es also besonders, die vorhandenen Budgets geschickt an den richtigen Stellen zu platzieren, um alle kritischen Themen abzudecken und sich gut für die Zukunft aufzustellen.

Investitionen nicht ohne Controlling

Bei der Bewertung des Erfolgs von Technologieinvestitionen im IT-Management ist es für Unternehmen wichtig, die Ergebnisse nachzuhalten und den ROI zu messen. Nur so gelingt es, die ohnehin



knappen Budgets auch in Zukunft sinnvoll und zielgerichtet einzusetzen und damit Schritt für Schritt die eigenen IT-Strukturen zu optimieren. Daher hat die Befragung auch einen Blick darauf geworfen, wie IT-Verantwortliche den Erfolg ihrer Investitionen messen. Effizienzgewinne im IT-Team (62 Prozent), Zufriedenheit der User (57 Prozent) und eine höhere Sicherheit (53 Prozent) sind die drei wichtigsten Indikatoren über alle befragten Betriebe hinweg.

Allerdings zeigen sich durchaus Unterschiede in den einzelnen Branchen: Nur 44 Prozent der Banken, Finanzdienstleister und Versicherungen setzen auf Userzufriedenheit als Messgröße. Dagegen messen 48 Prozent der Befragten in dieser Branche eher das Kundenengagement als Kennzahl. Im Kontrast dazu stehen bei Behörden (71 Prozent), im Gesundheitswesen (68 Prozent) und in der Fertigungsindustrie (67 Prozent) die Nutzer und ihre Bedürfnisse im Fokus.

Mit 51 Prozent sind es vor allem Unternehmen aus dem Gesundheitswesen, die ihre Erfolge daran messen, wie sehr sie die Kosten für ihre Tools senken können. Im verarbeitenden Gewerbe hingegen führt die Verbesserung der Sicherheitslage als Indikator mit 62 Prozent, während die Medien- und Unterhaltungsbranche mit 76 Prozent die Effizienzsteigerung des IT-Teams am häufigsten als Erfolgskriterium nutzt.

Konsolidierung is Key

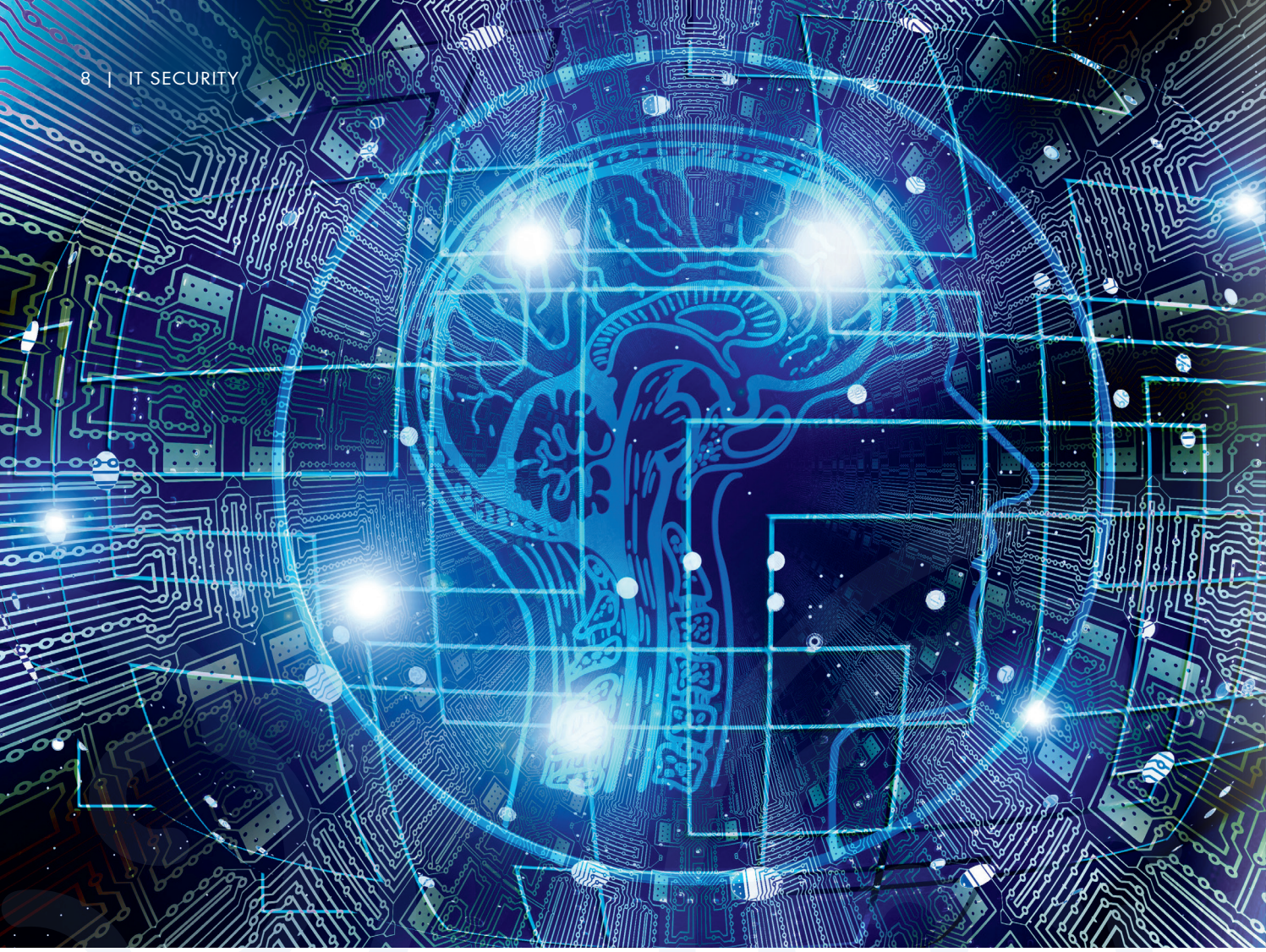
Bei all den Herausforderungen, der Dynamik im Wettbewerb und den sich daraus ergebenden notwendigen Investitionsfeldern fällt es schwer, den Überblick zu behalten und die begrenzten Ressourcen sinnvoll einzusetzen. Doch es gibt einen Lösungsweg, der Erfolg verspricht: Konsolidierung. Denn insbesondere größere Unternehmen sind auf eine Vielzahl komplexer digitaler Technologien angewiesen. So geben beispielsweise 28 Prozent der Unternehmen mit 5.000 oder mehr Mitarbeitenden an, dass sie derzeit mehr als sieben Backup- und Recovery-Lösungen einsetzen. Und auch in kleinen und mittelständischen Betrieben kommt es nicht selten vor, dass man vor lauter Tools nicht mehr weiß, wo einem der Kopf steht. Diese ausufernde Technologielandschaft führt zu einer komplexen Infrastruktur, überhöhten Kosten und negativen Erfahrungen der User.

Angesichts des wirtschaftlichen Drucks beginnen viele Unternehmen deshalb damit, aufzuräumen und sich von komplexen Strukturen zu befreien. 45 Prozent der befragten Firmen planen, Budget für neue Lösungen zur Effizienzsteigerung einzusetzen, und 36 Prozent wollen ihre vorhandenen Systeme reduzieren und konsolidieren. Dieser Abbau von IT-Altlasten durch Technologieintegration und -verschlankung spart nicht nur Kosten, sondern verbessert den Betrieb und wirkt sich positiv auf die Geschäftsergebnisse aus. Erfreulicherweise stehen Personalabbau mit 13 Prozent und Einstellungsstopp mit 17 Prozent ganz unten auf der Liste der geplanten Maßnahmen.

Fazit

2024 wird von der Troika aus Sicherheit, Automatisierung und Konsolidierung bestimmt werden. Unternehmen müssen es schaffen, ihre Infrastruktur effizient, robust und schlank aufzustellen, um den Herausforderungen von morgen gewachsen zu sein. Der Abschied von IT-Altlasten und die Investition in effizienzsteigernde Tools sind wichtige Schritte in die richtige Richtung.

André Schindler | www.ninjaone.de



Ausblick auf 2024

KI VERSCHÄRFT DIE BEDROHUNGSLAGE

KI hat zwar das Potenzial viele Sicherheitslösungen zu verbessern, doch auch Cyberkriminelle machen sich die Technologie mehr und mehr zunutze. Ein Ausblick darauf, wie KI das Security-Business in den kommenden Monaten verändern wird.

ChatGPT hat vielen Unternehmen die Augen geöffnet, wozu moderne KI-Tools inzwischen fähig sind. Sie beantworten Fragen, fassen Meetings zusammen, verbessern Präsentationen, analysieren Kennzahlen und optimieren Quellcode, und das viel schneller als Menschen es je könnten. Wurde 2023 noch viel experimentiert, werden mehr und mehr Unternehmen die KI-Nutzung in den kommenden Monaten zielgerichtet und koordiniert angehen, um ihren Mitarbeitern den Arbeitsalltag zu erleichtern. Damit dürften die Nutzerzahlen weiterhin schnell wachsen und die Dienste zunehmend für Cyberkriminelle attraktiv werden – schließlich können sie über ein einziges kompromittiertes KI-Angebot eine Vielzahl von Opfern erreichen.

Ein möglicher Angriffsvektor ist das sogenannte Data Poisoning, bei dem versucht wird, die Algorithmen zu manipulieren, damit sie weniger genau arbeiten oder sogar falsche Ergebnisse liefern. Wirklich neu ist das nicht: Schon seit Jahren versuchen Cyberkriminelle auf diese Weise, Spam-Filter zu unterlaufen, und 2016 machte der Austausch mit Twitter-Nutzern einen lernenden Chatbot von Microsoft binnen weniger Stunden zum Rassisten. Mit den vielen neuen KI- oder KI-basierten Tools und dem einfachen Zugang zu Rechenleistung in der Cloud wird die Zahl solcher Manipulationen jedoch zunehmen, um beispielsweise Falschinformationen zu

Quelle: Gerd Altmann | Pixabay

verbreiten oder die Erkennungsmechanismen von Sicherheitslösungen zu schwächen.

Vergiftete Trainingsdaten

Grundsätzlich basiert Data Poisoning auf dem Verfälschen von Trainingsdaten. Dabei werden bereits zugewiesene Labels für Datensätze ausgetauscht oder die Datensätze selbst verändert und mit „Approved"-Labels versehen, damit die KI falsche Klassifizierungen vornimmt und False Positives oder False Negatives produziert. Je nach der Menge der Manipulationen kann das komplette KI-Modell kompromittiert sein, sodass es insgesamt ungenauer arbeitet (Availability Attacks), oder nur ein Teil – dann arbeitet es größtenteils korrekt und hat nur in einzelnen Bereichen Schwächen (Targeted Attacks und Subpopulation Attacks). Durch gezielte Manipulationen können Cyberkriminelle aber auch eine Art von Hintertür einbauen, damit das KI-Modell später im Produktiveinsatz bei einigen Inputs einen ganz bestimmten Output liefert (Backdoor Attacks).

Wollen Cyberkriminelle die KI in bestimmten Bereichen schwächen oder spezifische Outputs hervorrufen, müssen sie das Modell und die Trainingsparameter genau kennen. Geht es nur darum, die Genauigkeit der KI insgesamt zu verringern, kommen sie ohne dieses Wissen aus.

Unabhängig davon ist es meist schwer, ein Data Poisoning zu entdecken, solange die KI keine groben Auffälligkeiten zeigt. Zudem ist es extrem aufwendig, das KI-Modell zu reparieren, da Unternehmen alle Trainingsdatensätze analysieren und in der Lage sein müssen, die manipulierten Datensätze aufzuspüren und zu entfernen. Das anschließende Neutraining des Modells erfordert viel Rechenleistung und verursacht hohe Kosten, weshalb das beste Mittel gegen Data Poisoning ein zuverlässiger Schutz der Trainingsdaten ist. Bewährt hat sich Zero Trust, das unberechtigte Zugriffe und damit Manipulationen verhindert. Mit statistischen Methoden lassen sich darüber hinaus Anomalien in den Daten aufspüren, und während des Trainings helfen Tools wie Azure Monitor und Amazon SageMaker, die Leistung der Modelle zu überwachen und unerwartete Schwankungen in der Genauigkeit zu erkennen.

Zunehmende Regulierung

Nicht immer rühren Ungenauigkeiten in KI-Modellen allerdings von einer Manipulation durch Cyberkriminelle her. Manchmal sind die Trainingsdaten bereits von vornherein vorurteilsbehaftet, weil sie älteren Ursprungs sind oder von Menschen erstellt wurden. Die KI-Modelle trainieren sich diese Vorurteile an, was zu diskriminierenden oder unfairen Ausgaben und Entscheidungen führt. Im Security-Bereich könnte eine Sicherheitslösung dann beispielsweise den legitimen Zugriff auf ein System verweigern, weil der betreffende Anwender oder das betreffende System in der Vergangenheit in einen Sicherheitsvorfall involviert war.

Verhindern lässt sich das durch die Auswahl von geeigneten Trainingsdaten und transparente KI-Modelle, deren Entscheidungen nachvollzogen und erklärt werden können. Solche Best Practices wollen Organisationen wie die UNESCO und Unternehmen wie Microsoft und IBM durch Frameworks für ethische KI vorantreiben. Darüber hinaus arbeiten die EU und die USA an Gesetzen, die Leitplanken für die Entwicklung und den Einsatz von KI abstecken sollen. Das dürfte zunächst zu einer uneinheitlichen Regulierungslandschaft und einem hohen Compliance-Aufwand für Unternehmen führen, das wilde Herumexperimentieren ohne Grenzen und Regeln – das manche KI-Experten schon mit dem Wilden Westen verglichen haben – jedoch unterbinden.

NICHT NUR FÜR NORMALE BÜROANGESTELLTE SIND KI-TOOLS NÜTZLICHE HELFER, SONDERN LEIDER AUCH FÜR CYBERKRIMINELLE.

Fabian Glöser,
Team Leader Sales Engineering,
Forcepoint, www.forcepoint.com

Bösartige KI-Tools

Nicht nur für normale Büroangestellte sind KI-Tools nützliche Helfer, sondern leider auch für Cyberkriminelle. Sie nutzen die Tools unter anderem, um täuschend echte Phishing-Mails in den verschiedensten Sprachen zu formulieren, Deepfakes für Betrugsmaschen wie den Enkeltrick zu erstellen oder Malware-Code kontinuierlich zu verändern, bis Sicherheitslösungen ihn nicht mehr als schadhaft erkennen. Auch eine völlig neue Malware können sie ohne Programmierkenntnisse in kurzer Zeit entwickeln – ganz einfach per Textanweisung. Inzwischen verhindern ChatGPT und Co. dies zwar durch Filter, die sich selbst mit geschickten Fragestellungen nur schwer austricksen lassen. Doch Cyberkriminelle haben längst eigene Chatbots wie WormGPT, FraudGPT und DarkBERT entwickelt, die auf derartige Aufgaben spezialisiert sind.

In den kommenden Monaten dürfte die Zahl von bösartigen KI-Tools deutlich zulegen, da mehr und mehr unzensierte Open Source LLMs zur Verfügung stehen (Large Language Models). Diese frei verfügbaren Modelle lassen sich dank effizienten Finetuning-Methoden wie LoRA (Low-Rank Adaption), bei denen nur ein kleiner Teil der Parameter und Gewichtungen angepasst wird, mit vergleichsweise geringem Aufwand für bestimmte Aufgaben trainieren. Notfalls reichen dafür die Rechenressourcen eines modernen Gaming-PCs aus, auch wenn das Training dann ein wenig länger dauert. Anschließend könnte die Nutzung des Modells anderen Cyberkriminellen gegen Gebühren angeboten werden – es wäre die nächste Stufe des Geschäftsmodells Cybercrime-as-a-Service.

Positive Effekte

Ebenso wie Cyberkriminelle sind allerdings auch Security-Unternehmen in der Lage, Open Source LLMs zur Verbesserung ihrer Produkte anzupassen, ohne ein LLM von Grund auf neu entwickeln zu müssen – das können ohnehin nur die ganz großen Tech-Unternehmen oder finanziell gut ausgestattete Start-ups leisten. Hier zeigt sich jedenfalls, dass der Wettlauf zwischen Cyberkriminellen und Security-Spezialisten unverändert weitergeht und vielversprechende Technologien von beiden Seiten genutzt werden. Im Security-Business hat KI in den vergangenen Jahren bereits zu erheblichen Verbesserungen beigetragen und wird das auch weiterhin tun, weil Algorithmen schlicht viel besser und schneller auffällige Verhaltensweisen erkennen und Risikoabschätzungen vornehmen können als Menschen. Darüber hinaus könnten beispielsweise ChatGPT-ähnliche Fähigkeiten künftig helfen, den Umgang mit Security-Tools zu erleichtern.

Fabian Glöser

KI-SPRACHASSISTENTEN MIT PYTHON ENTWICKELN

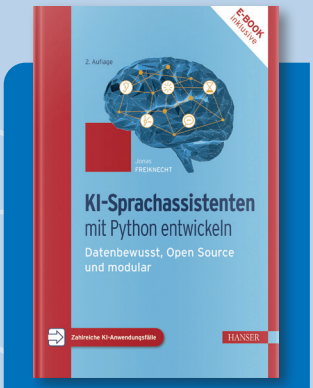
DATENBEWUSST, OPEN SOURCE UND MODULAR

Sprachassistenten werden vermehrt in Bereichen wie Kundenkommunikation, Smart Home oder Automotive eingesetzt. Dieses Buch zeigt Ihnen, wie Sie in Python Schritt für Schritt einen eigenen Sprachassistenten komplett selbst entwickeln.

Sie lernen, wie Sprachanalyse, -synthese und das Erkennen einer Benutzerintention funktionieren und wie Sie diese praktisch umsetzen. Und Sie kommen mit vielen Themen aus der professionellen Python-Entwicklung in Berührung, mit Logging, dem dynamischen Installieren von Paketen, dem „Einfrieren" einer Anwendung oder der Überführung in einen Installer.

Ein weiteres wichtiges Thema ist der Datenschutz. Wenn Sie einen eigenen Assistenten programmiert haben, wissen Sie genau, welche Daten Sie rausgeben und welche auf Ihrem Gerät verarbeitet werden. Schreiben Sie Intents, denen selbst sensible Daten anvertraut werden können. Das schafft auch Vertrauen beim Anwender.

Darüber hinaus kann Ihr selbstprogrammierter Assistent ein paar Dinge mehr als die Marktführer. So können Sie ihm zum Beispiel erlauben, nur auf Ihre Stimme zu reagieren und andere Personen zu ignorieren oder das Alter und Geschlecht an der Stimme zu erkennen.



KI-Sprachassistenten mit Python entwickeln
– Datenbewusst, Open Source und modular; Jonas Freiknecht; Carl Hanser Verlag GmbH & Co.KG, 05/2024

ZWEISCHNEIDIGES SCHWERT

CYBERSICHERHEIT IN ZEITEN VON KI

Für die „Story of the Year" haben die Kaspersky-Experten die Auswirkungen von Künstlicher Intelligenz (KI) auf die Cybersicherheitslandschaft analysiert. Im Fokus steht ihr Einsatz durch Cyberkriminelle, aber auch wie man sie im Bereich Cybersicherheit einsetzen kann. Die Analyse ist Teil des Kaspersky Security Bulletin, einer jährlichen Reihe von Vorhersagen und analytischen Reports im Bereich der Cybersicherheit.

Egal, ob Bildbearbeitung oder das Schreiben von Essays – Künstliche Intelligenz hat sich rasend schnell im vergangenen Jahr 2023 entwickelt und verbreitet. Allerdings ist auch die Hälfte (47 Prozent) der Bundesbürger in Deutschland über den Einzug von KI ins alltägliche Leben besorgt. Eng verknüpft mit KI-gestützten Large Language Models (LLMs) ist die Frage nach Cybersicherheit und Datenschutz.

#1 Komplexere Schwachstellen:
Textbefehlen folgende LLMs werden zunehmend in Verbraucherprodukte integriert. Hierdurch werden neue komplexe Schwachstellen an der Schnittstelle von (probabilistischer) generativer KI und traditionellen (deterministischen) Technologie entstehen. Infolgedessen wird die Angriffsfläche größer. Entwickler müssen daher neue Sicherheitsmaßnahmen schaffen, indem sie beispielsweise Nutzer-Zustimmungen zu von LLM-Agenten eingeleiteten Aktionen fordern.

#2 Umfassender KI-Assistent für Cybersicherheitsexperten:
Red-Team-Mitglieder und Sicherheitsexperten setzen das Potenzial generativer KI zunehmend für innovative Cybersicherheitstools ein. Dies könnte zur Entwicklung von Assistenten führen, die LLM oder Machine Learning (ML) einsetzen, um Red-Team-Aufgaben zu automatisieren.

#3 Neurale Netzwerke zur Bildgenerierung für Scams:
In diesem Jahr könnten Betrüger ihre Taktiken ausweiten, indem sie neurale Netzwerke und KI-Tools nutzen, um überzeugendere Betrugsinhalte zu erstellen.

#4 KI wird die Cybersicherheitswelt nicht grundlegend verändern:
Trotz des KI-Trends erwarten die Kaspersky-Experten keine grundlegende Veränderung der Bedrohungslandschaft in naher Zukunft. Genauso wie Cyberkriminelle werden auch IT-Sicherheitsverantwortliche dieselben oder fortschrittlichere generative KI-Tools einsetzen, um die Sicherheit von Software und Netzwerken zu verbessern.

#5 Mehr Initiativen und Regularien:
Synthetische (künstlich erzeugte) Inhalte werden gekennzeichnet werden müssen, so dass weitere Regulierungen und Investitionen in Erkennungstechnologien notwendig sind. Entwickler und Wissenschaftler werden Methoden entwickeln, um synthetische Medien durch Wasserzeichen leichter identifizierbar und rückverfolgbar zu machen.

www.kaspersky.de

Im Visier der Cyberkriminellen

EFFEKTIVE ABWEHR DURCH SICHERE AUTHENTIFIZIERUNG

Phishing-E-Mails sind nach wie vor eine häufig eingesetzte Angriffstaktik in der komplexen Welt der Cyberkriminalität. Der aktuelle Mimecast Global Threat Intelligence Report unterstreicht diese Entwicklung für das dritte Quartal 2023 nachdrücklich: Im zurückliegenden Jahr wurden zwei Drittel aller Unternehmen Opfer von Ransomware-Angriffen, während nahezu jede Firma (97 Prozent) E-Mail-basierten Phishing-Angriffen ausgesetzt war. Das Ausmaß ist alarmierend und stellt lediglich die Spitze des Eisbergs dar. Besonders besorgniserregend ist die Tatsache, dass die Bereiche IT, Finance und Personalwesen am stärksten betroffen sind. Die Analyse von mehr als einer Milliarde E-Mails pro Tag verdeutlicht, dass Sicherheitsteams weltweit weiterhin mit einem Anstieg schwerwiegender Angriffe rechnen müssen, bei denen E-Mails als Einfallstor dienen.

Damit sich Unternehmen unabhängig von ihrer Größe wirksam schützen können, sind robuste Authentifizierungsmaßnahmen ratsam. Insbesondere die Integration von Biometrie oder Risk Based Authentication (RBA) tragen dazu bei, potenzielle Gefahren zu minimieren und die Cyberresilienz signifikant zu stärken. Angesichts kontinuierlicher Bedrohungen ist proaktives Handeln unerlässlich, um die digitale Integrität zu bewahren und sensible Daten vor den zunehmend raffinierten Methoden der Cyberkriminellen zu schützen.

DIE RBA HAT SICH ALS EFFEKTIVES INSTRUMENT ETABLIERT, UM DIE SICHERHEIT VON ANMELDEPROZESSEN IN UNTERNEHMEN ZU OPTIMIEREN.

Stephan Schweizer, CEO, Nevis Security AG, www.nevis.net

Biometrische Authentifizierung

Die biometrische Authentifizierung ist eine verlässliche Methode, um zweifelsfrei die Identität einer Person zu überprüfen. Der Ansatz setzt auf eindeutige biologische oder verhaltensbezogene Merkmale zur Identifikation. Im Verlauf des Authentifizierungsprozesses werden die bereitgestellten Daten mit validierten Benutzerinformationen in einer sicheren Datenbank abgeglichen, um deren Echtheit festzustellen.

Ein anschauliches Beispiel hierfür ist der Abgleich von Fingerprints, bei dem der Fingerabdruck erfasst und in numerische Daten umgewandelt wird. Dies wird dann mit den Informationen in der Datenbank verglichen, um die Identität zu verifizieren.

Es existieren diverse Arten von biometrischen Identifikatoren, darunter Gesichtsmuster, Augen- oder Fingerabdrücke, Stimmenschallwellen und die Bewegungen der Finger auf Eingabegeräten. Diese Daten gewährleisten eine äußerst präzise Identitätsverifizierung.

Die Integration biometrischer Daten in die Zwei-Faktor- (2FA) oder Multi-Faktor-Authentifizierung (MFA) bietet eine zusätzliche Sicherheitsebene. Diese Methode erfordert neben Benutzernamen und Passwort einen zweiten Faktor wie beispielsweise einen Einmalcode oder einen Fingerabdruck zur Anmeldung. Angesichts der zunehmenden Nutzung von Online-Diensten und mobilen Geräten ist dies besonders relevant. Die Einbindung eindeutiger Identifikationsmerkmale in den Verifizierungsprozess ist eine äußerst wirkungsvolle Methode, um persönliche Daten zu schützen und höchste Sicherheit zu gewährleisten.

Risk Based Authentifizierung

Risk Based Authentifizierung (RBA) ist ebenfalls eine moderne Methode zur Sicherung des Zugriffs auf Systeme, Anwendungen und Benutzerdaten. Sie basiert auf der Bewertung von Risikofaktoren. Im Gegensatz zu herkömmlichen Methoden beschränkt sich die RBA nicht nur auf Benutzernamen, Passwörter oder Token, sondern integriert eine Viel-

zahl von Kontextinformationen zur Authentifizierung. Hierbei werden zum Beispiel der geografische Standort, die genutzten Geräte, das Verhaltensmuster und die Anmeldehistorie berücksichtigt. Diese Daten werden mittels Unternehmenssicherheitsprotokollen abgeglichen, um einen Risikowert zu bestimmen.

Die RBA justiert das Verfahren entsprechend der Risikobewertung. Bei geringem Risiko könnte eine einfache Authentifikation ausreichen, während bei erhöhtem Risiko zusätzliche Methoden wie das biometrische Verfahren erforderlich sind. Die Anwendung von 2FA in Kombination mit RBA steigert die Sicherheit zudem.

Vorwiegend wird die RBA in Branchen eingesetzt, die mit sensiblen personenbezogenen Daten arbeiten, wie das Finanzwesen, E-Commerce-Unternehmen und Regierungsbehörden. Insbesondere im Finanzsektor, etwa bei Banken und Finanzinstituten, bietet das Authentifizierungsverfahren Schutz vor unbefugtem Zugriff auf Kundendaten und Transaktionen. Im E-Commerce ermöglicht sie die Erkennung von verdächtigen Transaktionen, wodurch zusätzliche Authentifizierungsschritte aktiviert werden können, um Betrugsversuche zu verhindern. In Regierungsinstitutionen wird RBA eingesetzt, um den Zugriff auf sensible Daten zu beschränken und zu gewährleisten, dass nur befugte Personen darauf zugreifen können.

Stärkung der Anmeldesicherheit für Unternehmen

Die RBA hat sich als effektives Instrument etabliert, um die Sicherheit von Anmeldeprozessen in Unternehmen zu optimieren. Hierbei werden Risiken identifiziert und proaktiv Maßnahmen zur Risikoreduzierung umgesetzt. Eine kontinuierliche Risikobewertung ermöglicht es, potenziellen Missbrauch zu erkennen und zu unterbinden, noch bevor Schaden entsteht. Dies trägt dazu bei, Betrugsfälle zu minimieren.

Ein herausragendes Merkmal von RBA ist ihre Benutzerfreundlichkeit, die den Anmeldeprozess nicht nur vereinfacht, sondern auch komfortabler gestaltet. Dies führt nicht nur zu einer positiven Nutzererfahrung, sondern trägt gleichzeitig zur Kosteneffizienz bei, da aufwendige Sicherheitsmaßnahmen zurückgefahren werden. Die intelligente Risikobewertung ermöglicht es, Sicherheitsvorkehrungen gezielt auf potenzielle Bedrohungen auszurichten, anstatt breit angelegte und möglicherweise hinderliche Sicherheitsprotokolle anzuwenden.

Ein weiterer wichtiger Vorteil von RBA ist, dass sich damit die Einhaltung von Compliance-Vorschriften gewährleisten lässt. Durch die Begrenzung des Zugangs zu geschützten Ressourcen ausschließlich auf autorisierte Benutzer werden die regulatorischen Anforderungen erfüllt und das Unternehmen vor möglichen Sanktionen geschützt. Dies macht RBA zu einer umfassenden Lösung, die die Sicherheitsstandards erhöht, die Benutzerfreundlichkeit optimiert und gleichzeitig dazu beiträgt, Compliance-Anforderungen effektiv zu erfüllen.

Stephan Schweizer

Passwort knacken? – Kein Problem!

ChatGPT UND AUTOMATISIERUNG ERLEICHTERN PASSWORT-CRACKING-ANGRIFFE

Sicherheitslücken machen Unternehmen kontinuierlich das Leben schwer. Der Einsatz von Quantencomputertechnologien wird diese Problematik noch verstärken. Vor diesem Hintergrund hat Specops Software eine Untersuchung durchgeführt, die zeigt wie lange Cyberkriminelle benötigen, um Passwörter mithilfe moderner Hardware und Brute Force zu knacken. Das Ergebnis: Nicht ansatzweise lang genug. Die Analyse erfolgte mittels der Breached Password Protection Liste, die mehr als vier Milliarden(!) kompromittierte Passwörter umfasst und jüngst aktualisiert wurde.

Cyberkriminelle - immer einen Schritt voraus

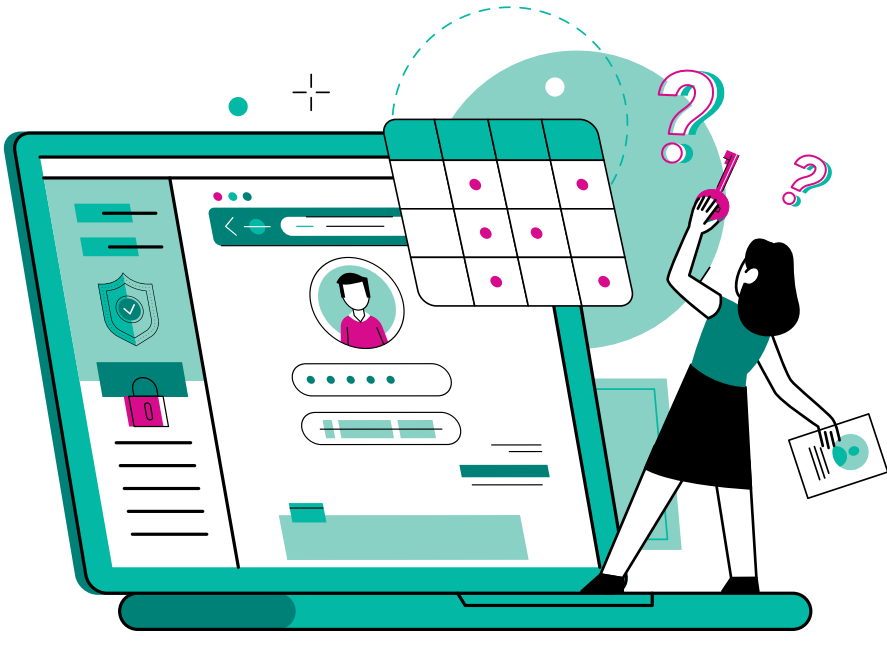
Gängige Hash-Algorithmen, wie MD5 und SHA256 sind für eine schnelle Verarbeitung ausgelegt und eignen sich besonders für häufig verwendete Anwendungen. Die Erstellung eines bcrypt-Hashes hingegen braucht seine Zeit – genau wie das Erraten des Passwortes.

Im Vergleich zu MD5 und SHA256 bietet der bcrypt-Hash-Algorithmus eine sichere Speicherung des Kennworts sowie die notwendige Zeit für Sicherheitsteams, verdächtige Aktivitäten zu erkennen. Eine Kompromittierung kann dadurch trotzdem nicht verhindern werden. Selbst wenn Unternehmen in der Lage wären, den sichersten Hash-Algorithmus zu verwenden, um alle Benutzerpasswörter zu schützen, stellt die Wiederverwendung von Kennwörtern eine Bedrohung dar. Die einzige Lösung: Passwortsicherheit verbessern und regelmäßig auf kompromittierte Kennwörter scannen.

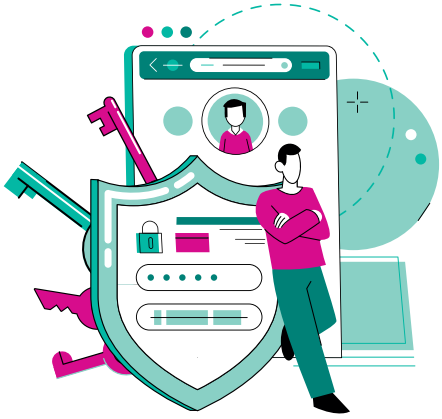
Lange Passwörter helfen

Je länger ein Passwort ist, desto mehr Zeit oder Rechenpower benötigen Angreifer, um dessen Hash-Wert zu entschlüsseln. Doch lange Passwörter treffen selten auf Begeisterung bei den Endnutzern, da diese oftmals mehrere Kennwörter mit unterschiedlichsten Richtlinien verwalten und merken müssen. Längenbasierte Ablaufdaten und die Verwendung von Passphrasen können Benutzern dabei helfen, längere Passwörter zu verwenden.

Doch Vorsicht ist geboten: Auch lange Kennwörter werden zu einer Gefahr, wenn sie auf kompromittierten Kennwortlisten auftauchen. Deshalb sollte die Sperrung von bereits kompromittierten Passwörtern oberste Priorität beim Schutz vor passwortbasierten Angriffen und in jedem Cybersecurity-Prozess haben. Passwortfilter von Drittanbietern, wie Specops Password Policy, helfen dabei kompromittierte Kennwörter im Active Directory aufzuspüren und zu sperren.



Für eine erste Analyse der Situation lohnt sich auch ein Audit der Umgebung mit Hilfe eines Tools wie



SO LANGE DAUERT ES BIS EIN MD5-GEHASHTES PASSWORT GEKNACKT WIRD

Zeichenanzahl	Nur Zahlen	Nur Kleinbuchstaben	Groß-/Kleinbuchstaben	Zahlen, Groß-/Kleinbuchstaben	Zahlen, Groß-/Kleinbuchstaben, Sonderzeichen
8	Sofort	Sofort	2 Minuten	5 Minuten	3 Stunden
9	Sofort	9 Sekunden	2 Stunden	5 Stunden	12 Tage
10	Sofort	4 Minuten	2 Tage	14 Tage	3 Jahre
11	Sofort	2 Stunden	132 Tage	3 Jahre	279 Jahre
12	Sofort	2 Tage	19 Jahre	159 Jahre	26,5 Tsd. Jahre
13	Sofort	6 Wochen	995 Jahre	10 Tsd. Jahre	3 Mio. Jahre
14	3 Minunten	3 Jahre	51 Tsd. Jahre	608 Tsd. Jahre	239 Mio. Jahre
15	26 Minunten	82 Jahre	2 Mio. Jahre	37 Mio. Jahre	22,7 Mio. Jahre
16	5 Stunden	2136 Jahre	140 Mio. Jahre	3 Mrd. Jahre	3 Bio. Jahre
17	43 Stunden	56 Tsd. Jahre	8 Mrd. Jahre	145 Mrd. Jahre	205 Bio. Jahre
18	18 Tage	2 Mio. Jahre	379 Mrd. Jahre	9 Bio. Jahre	20 Brd. Jahre
19	6 Monate	38 Mio. Jahre	20 Bio. Jahre	557 Bio. Jahre	2 Trio. Jahre
20	5 Jahre	977 Mio. Jahre	2 Brd. Jahre	35 Brd. Jahre	176 Trio. Jahre
21	49 Jahre	26 Mrd. Jahre	54 Brd. Jahre	3 Trio. Jahre	17 Trd. Jahre
22	290 Jahre	660 Bio. Jahre	3 Trill. Jahre	133 Trill. Jahre	2 Qrd. Jahre

Bild 1: Zeitdauer bis ein MD5-gehashtes Passwort geknackt wird

des Specops Password Auditors. Dieses Read-Only-Tool analysiert Benutzerpasswörter anhand einer lokalen Datenbank mit über 950 Millionen kompromittierten Passwörtern und gibt dann in einem Report an, wie viele Passwörter kompromittiert oder identisch sind. Passwörter können wirkungsvoll zur IT-Sicherheit und Authentifizierung beitragen, wenn man sicherstellt, dass man sie vor unsicheren Benutzerverhalten schützt und sie geheim bleiben!

Phishing vs. Brute Force-Angriffe

Passwörter werden heute oftmals mit Hilfe sehr gezielter Phishing Attacken gestohlen. Eine andere, schon seit langer Zeit übliche Methode sind die Brute Force-Angriffe. Die Frage ist, wie lange dauert es, ein Passwort mit Hilfe eines Brute Force Angriffes zu knacken?

Das hängt von mehreren Faktoren ab:

#1 Passwortlänge und -komplexität: Je länger und komplexer das Passwort, desto mehr mögliche Kombinationen gibt es. Ein Passwort, das Groß- und Kleinbuchstaben, Zahlen und Sonderzeichen enthält, ist viel schwerer zu knacken als eines, das nur aus Kleinbuchstaben besteht.

#2 Angriffsgeschwindigkeit: Die Geschwindigkeit, mit der ein Angreifer Passwörter ausprobieren kann, hängt von der Hardware und der Software ab, die er verwendet. Spezialisierte Hardware wie GPUs oder sogar dedizierte Hardware für Passwort-Cracking kann die Geschwindigkeit erheblich erhöhen.

#3 Passwort-Richtlinien und -Schutzmaßnahmen: Manche Systeme haben Schutzmaßnahmen gegen Brute-Force-Angriffe, wie etwa die Begrenzung der Anmeldeversuche oder die Verzögerung zwischen den Versuchen.

Hier sind einige grobe Schätzungen, basierend auf verschiedenen Passworttypen und einer angenommenen Angriffsgeschwindigkeit:

- **Einfaches Passwort** (6 Zeichen, nur Kleinbuchstaben): Kann in Sekunden oder Minuten geknackt werden.
- **Mittlerer Komplexität** (8 Zeichen, gemischt mit Zahlen und Buchstaben): Kann Stunden bis Tage dauern.

- **Hohe Komplexität** (12 oder mehr Zeichen, gemischt mit Groß- und Kleinbuchstaben, Zahlen und Sonderzeichen): Kann Jahre bis Jahrzehnte dauern.

Quantencomputing verändert alles

Die große Frage lautet: Wie wird sich diese Zeitspanne durch den Einsatz eines Quantencomputers verändern? Denn es ist nur eine Frage der Zeit, bis es die ersten einsatzfähigen Quantencomputer gibt und dann wird es auch Mietmodelle a la „Hacking as a Service" geben.

SO LANGE DAUERT ES BIS EIN KOMPROMITTIERTES KENNWORT GEKNACKT WIRD

Zeichenanzahl	Nur Zahlen	Nur Kleinbuchstaben	Groß-/Kleinbuchstaben	Zahlen, Groß-/Kleinbuchstaben	Zahlen, Groß-/Kleinbuchstaben, Sonderzeichen
8	Sofort	Sofort	Sofort	Sofort	Sofort
9	Sofort	Sofort	Sofort	Sofort	Sofort
...	...	...	...	...	...
20	Sofort	Sofort	Sofort	Sofort	Sofort
21	Sofort	Sofort	Sofort	Sofort	Sofort
22	Sofort	Sofort	Sofort	Sofort	Sofort

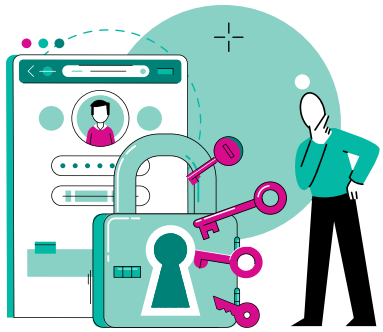


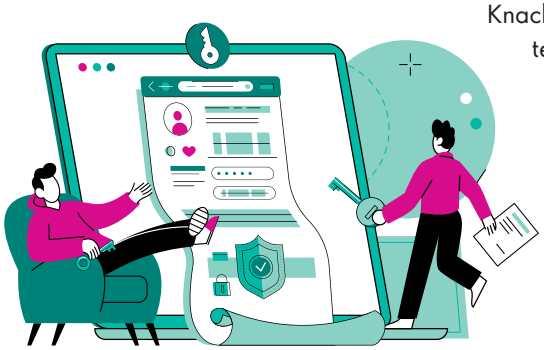
Bild 2: Zeitdauer bis ein kompromittiertes Passwort geknackt wird

Die Einführung von Quantencomputern wird also wahrscheinlich die Zeitspanne für das Knacken von Passwörtern durch Brute-Force-Angriffe dramatisch verkürzen, insbesondere für Verschlüsselungsmethoden, die auf bestimmten mathematischen Problemen basieren, die für klassische Computer schwer zu lösen sind, für Quantencomputer aber eher kein Problem darstellen.

Schlüsselpunkte

Nachfolgend vier Schlüsselpunkte zum Verständnis der Auswirkungen von Quantencomputern auf die Passwortsicherheit:

#1 Quantenüberlegenheit: Quantencomputer nutzen die Prinzipien der Quantenmechanik, um Informationen zu verarbeiten. Dies ermöglicht es ihnen, bestimmte Arten von Berechnungen viel schneller durchzuführen als herkömmliche Computer. Zum Beispiel könnte ein Quantencomputer die Faktorisierung großer Zahlen (ein Schlüsselaspekt der RSA-Verschlüsselung) oder das Finden von diskreten Logarithmen (wichtig für einige Formen der elliptischen Kurvenkryptographie) in einer praktikablen Zeit durchführen, während dies für klassische Computer praktisch unmöglich ist.



#2 Shor's Algorithmus: Dieser Quantenalgorithmus kann genutzt werden, um die Faktorisierung großer Zahlen und das Finden von diskreten Logarithmen effizient durchzuführen. Wenn ein leistungsfähiger Quantencomputer Shor's Algorithmus ausführen könnte, würde dies viele der heute verwendeten Verschlüsselungssysteme kompromittieren.

#3 Auswirkung auf Passwörter: Während Quantencomputer besonders effektiv bei der Kompromittierung von Verschlüsselungsschlüsseln sind, ist ihre Auswirkung auf das direkte Knacken von Passwörtern durch Brute-Force-Angriffe weniger klar. Quantencomputer könnten jedoch die Geschwindigkeit, mit der Passwortkombinationen ausprobiert werden können, erhöhen, insbesondere wenn das Passwort zur Entschlüsselung von Daten verwendet wird, die mit einem jetzt verwundbaren Algorithmus verschlüsselt sind.

#4 Quantensichere Kryptographie: Die gute Nachricht: Als Reaktion auf die Bedrohung durch Quantencomputer wird an der Entwicklung von quantensicheren Kryptographie-Methoden gearbeitet. Diese neuen Algorithmen sind so konzipiert, dass sie auch gegen Angriffe durch Quantencomputer resistent sind.

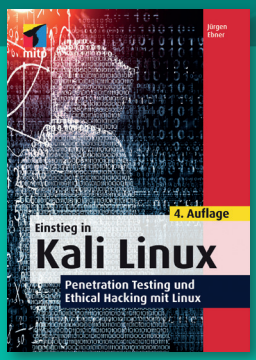
Zusammenfassend lässt sich sagen, dass Quantencomputer das Potenzial haben, die Sicherheit vieler aktueller Verschlüsselungs- und Passwortschutzmethoden zu untergraben. Allerdings sind Quantencomputer, die groß und stabil genug sind, um solche Berechnungen durchzuführen, zum aktuellen Zeitpunkt (Anfang 2024) noch nicht praktisch realisiert.

Natürlich helfen Passwortmanager, aber auch eine Multi-Faktor-Authentifizierung (MFA) leistet ihren Dienst und macht Hackern das Leben schwer. Aber Vorsicht: einen 100prozentigen Schutz bietet keine Lösung.

Ulrich Parthier

EINSTIEG IN KALI LINUX

PENETRATION TESTING UND ETHICAL HACKING MIT LINUX



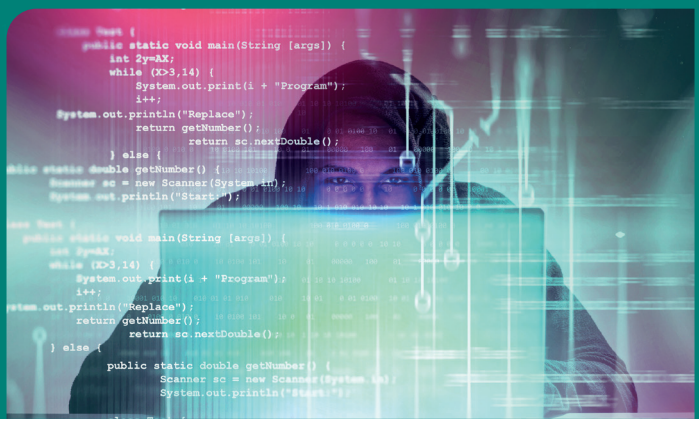
Einstieg in Kali Linux
– Penetration Testing und Ethical Hacking mit Linux; Jürgen Ebner; mitp Verlags GmbH & Co.KG; 12/2023

Die Distribution Kali Linux ist auf Sicherheits- und Penetrationstests spezialisiert. Sie enthält mehrere Hundert Pakete zur Informationssammlung und Schwachstellenanalyse und jede Menge Tools für Angriffe und Exploitation sowie Forensik und Reporting, sodass Penetration Tester aus einem beinahe endlosen Fundus kostenloser Tools schöpfen können. Dieses Buch ermöglicht IT-Sicherheitsexperten und allen, die es werden wollen, einen einfachen Einstieg in Kali Linux. Erfahrung im Umgang mit anderen Linux-Distributionen setzt der Autor dabei nicht voraus.

Im ersten Teil des Buches erfahren Sie, wie Sie Kali Linux installieren und an Ihre Bedürfnisse anpassen. Darüber hinaus gibt Ihnen der Autor grundlegende Linux-Kenntnisse an die Hand, die Sie für das Penetration Testing mit Kali Linux brauchen.

Der zweite Teil erläutert verschiedene Security Assessments sowie die grundlegende Vorgehensweise bei der Durchführung von Penetrationstests. So vorbereitet können Sie im nächsten Schritt gezielt die für Ihren Einsatzzweck passenden Tools für das Penetration Testing auswählen.

Aus der Fülle der bei Kali Linux mitgelieferten Tools stellt der Autor im dritten Teil des Buches die wichtigsten vor und zeigt Schritt für Schritt, wie und wofür sie eingesetzt werden, darunter bekannte Tools wie Nmap, OpenVAS, Metasploit und John the Ripper.



Nach der Lektüre sind Sie bereit, Kali Linux sowie die wichtigsten mitgelieferten Tools für Penetrationstests einzusetzen und IT-Systeme auf Schwachstellen zu prüfen.

Von wegen Drahtseilakt!

SO GELINGT UNTERNEHMEN DER SICHERE EINSATZ VON KI-LÖSUNGEN

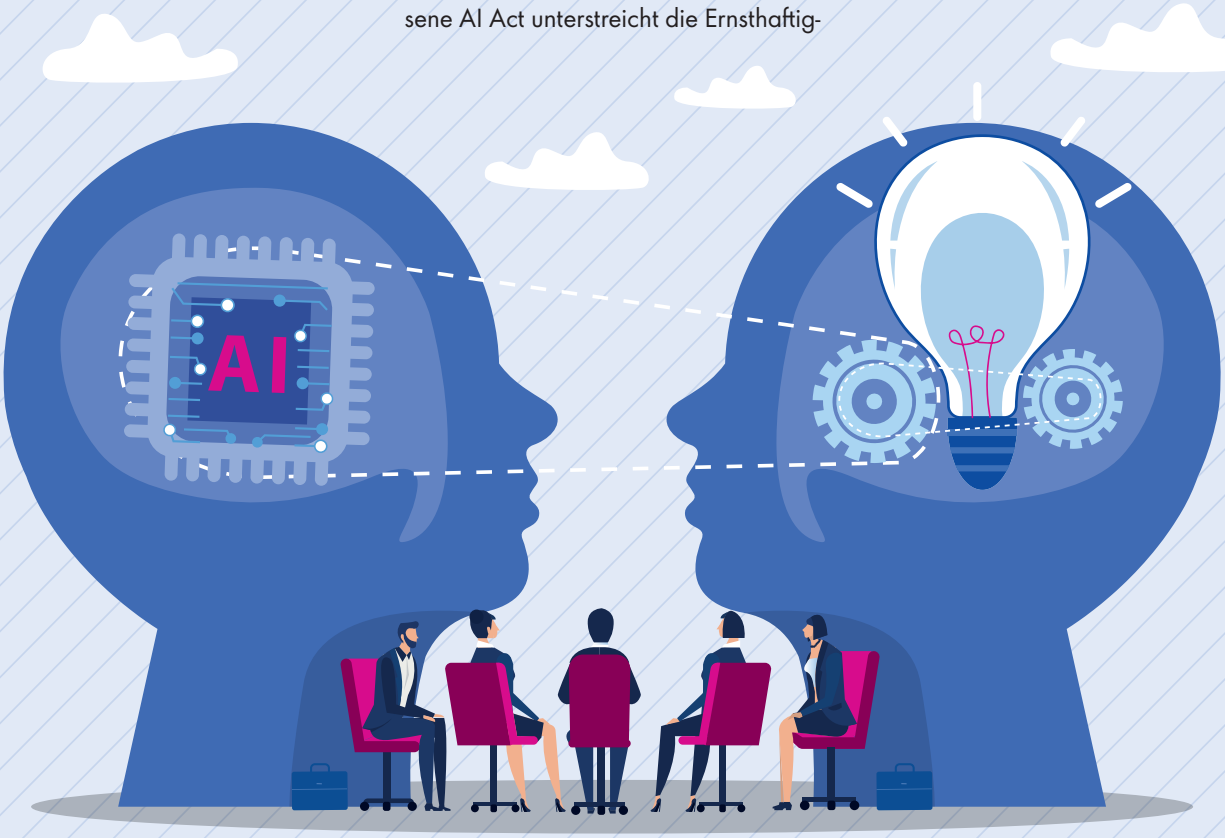
Die Mehrheit der deutschen Unternehmen sind von KI-Lösungen und deren Potenzialen, insbesondere für die wesentliche Wertschöpfung, überzeugt. Der Aussicht auf qualitativ hochwertige Ergebnisse bei gleichzeitig weniger manuellem Ressourcenaufwand steht jedoch die Skepsis der Datensicherheit gegenüber. Welche Maßnahmen können Entscheider treffen?

Noch vor etwa einem Jahr war Künstliche Intelligenz (KI) für viele ein reines Buzz-Word, ein Medienphänomen, das täglich für neue Schlagzeilen sorgte. Schnell stellte sich jedoch ein breites (und tiefgehendes) Interesse für die Potenziale ein, getrieben von öffentlich ausgetragenen Debatten, unternehmensinternen Expertenrunden und großangelegten Studien. Mit Argusaugen wurden die Entwicklungen von Entscheidern der deutschen Wirtschaft analysiert und beobachtet, welche Anwendungsfälle für Unternehmen – von Kleinstunternehmen bis Großkonzern – von besonderem Interesse sind.

Die verschiedenen Stakeholder, neben den Unternehmen beispielsweise die Politik und Ethikräte, konnten sowohl bei der europaweiten Regulatorik von KI-Lösungen Fortschritte erzielen als auch das Verständnis für die vielversprechende Technologie innerhalb der Gesellschaft und insbesondere innerhalb der deutschen Unternehmenslandschaft schärfen. Der im Dezember vom Europaparlament und EU-Staaten beschlossene AI Act unterstreicht die Ernsthaftigkeit des Vorgehens und dürfte sich positiv auf die KI-Entwicklungen innerhalb der EU und das Vertrauen auf Unternehmensseite auswirken.

Keine Zukunft ohne Risiko

Mit Gewissheit lässt sich behaupten: KI-basierte Anwendungen werden zukünftig viele Unternehmensbereiche unweigerlich beeinflussen. So kam eine Studie des Branchenverbands Bitkom zu dem Ergebnis, dass 68 Prozent der deutschen Unternehmen KI als wichtigste Zukunftstechnologie einschätzen. Über zwei Drittel sehen in KI überdies eine Chance für das eigene Unternehmen. Dem entgegen stehen 20 Prozent, für die KI einen prinzipiellen Risikofaktor darstellt.



Die Krux also: Die meisten Unternehmen sind sich inzwischen der Bedeutung der Technologie und ihrer möglichen positiven Auswirkungen auf den Arbeitsalltag bewusst. Allerdings sorgt die an vielen Stellen ungewisse Sachlage in puncto Datensicherheit für Sorgenfalten in den Entscheidergremien. Eine Studie des Instituts für angewandte Arbeitswissenschaft e.V. (ifaa) fand heraus, dass 40 Prozent der befragten Unternehmen Sicherheitsbedenken beim Einsatz von KI haben.

Zwei Gegensätze, die es aus der Welt zu schaffen gilt, wenn die deutsche Unternehmenslandschaft die Potenziale voll ausschöpfen und das Zeitalter der KI erfolgreich bestreiten will.

Welche Schritte können Unternehmerinnen und Unternehmer also gehen, um den sicheren Einsatz von KI-Tools zu gewährleisten?

Wo und wie werden eingespeiste Daten weiterverwendet?

KI-Tools haben gemein, dass sie sich stetig weiterentwickeln. Dafür werden sie trainiert – und zwar mit externen Daten. Daraus ergibt sich die Prämisse, dass die Anbieter dieser KI-Anwendungen Zugriff auf eben jene Daten haben. Nicht alle KI-Anbieter haben jedoch die Sicherheit der Daten, mit denen sie hantieren, im Kern der DNA.

Entscheider, die vor der Wahl ihres KI-Anbieters stehen, sollten diesen Punkt vor allen anderen berücksichtigen und nur solche KI-Unternehmen in die engere Auswahl nehmen, die Grundprinzipien der Datensicherheit verfolgen. Dafür von hohem Stellenwert ist der Betrieb einer eigenen Server-Infrastruktur.

Mit dieser gewährleisten Partner-Unternehmen ständige Datenhoheit, da Informationen nicht an Drittanbieter, wie beispielsweise Cloud-Hosting-Services, weitergegeben werden müssen. Die beste Server-Infrastruktur ist jedoch nur dann von Wert, wenn die Daten bei der Übertragung nicht abgegriffen werden können. Dazu ist ein Datenfluss über End-to-End-Verschlüsselung zwingend notwendig. Diesen sollten sich Unternehmen von ihren Partnern vertraglich festhalten lassen. Im ersten Schritt helfen Zertifizierungen, wie ISO27001 und SOC2, ein grundlegendes Verständnis über die Verarbeitung der Daten zu erlangen. Liegen diese Zertifizierungen vor und sollten dennoch Fragen zur Verarbeitung offen bleiben, können im weiteren Prozess Whitepaper angefordert werden, um die Details verstehen und analysieren zu können.

NDA LOHNEN SICH IMMER DANN, WENN DIE ZUR VERFÜGUNG GESTELLTEN ANGABEN ZU KI-PRODUKTEN UND -SERVICES KEINE VOLLUMFÄNGLICHE BEWERTUNG ERLAUBEN.

Guido Simon, Director of Engineering (IT-Operations & Infrastructure), DeepL, www.deepl.com

Weiterverarbeitung der Daten prüfen

Sind Daten einmal mit Partner-Unternehmen via End-to-End-Verschlüsselung für das Ausführen der gewünschten Dienstleistung geteilt, wird eine Frage oftmals nur unzureichend beantwortet: Was passiert im Anschluss mit meinen Daten? Denn manche KI-Anbieter nutzen die eingespeisten Daten beispielsweise, auch ohne klare Kennzeichnung, weiterführend für das Training ihrer Tools.

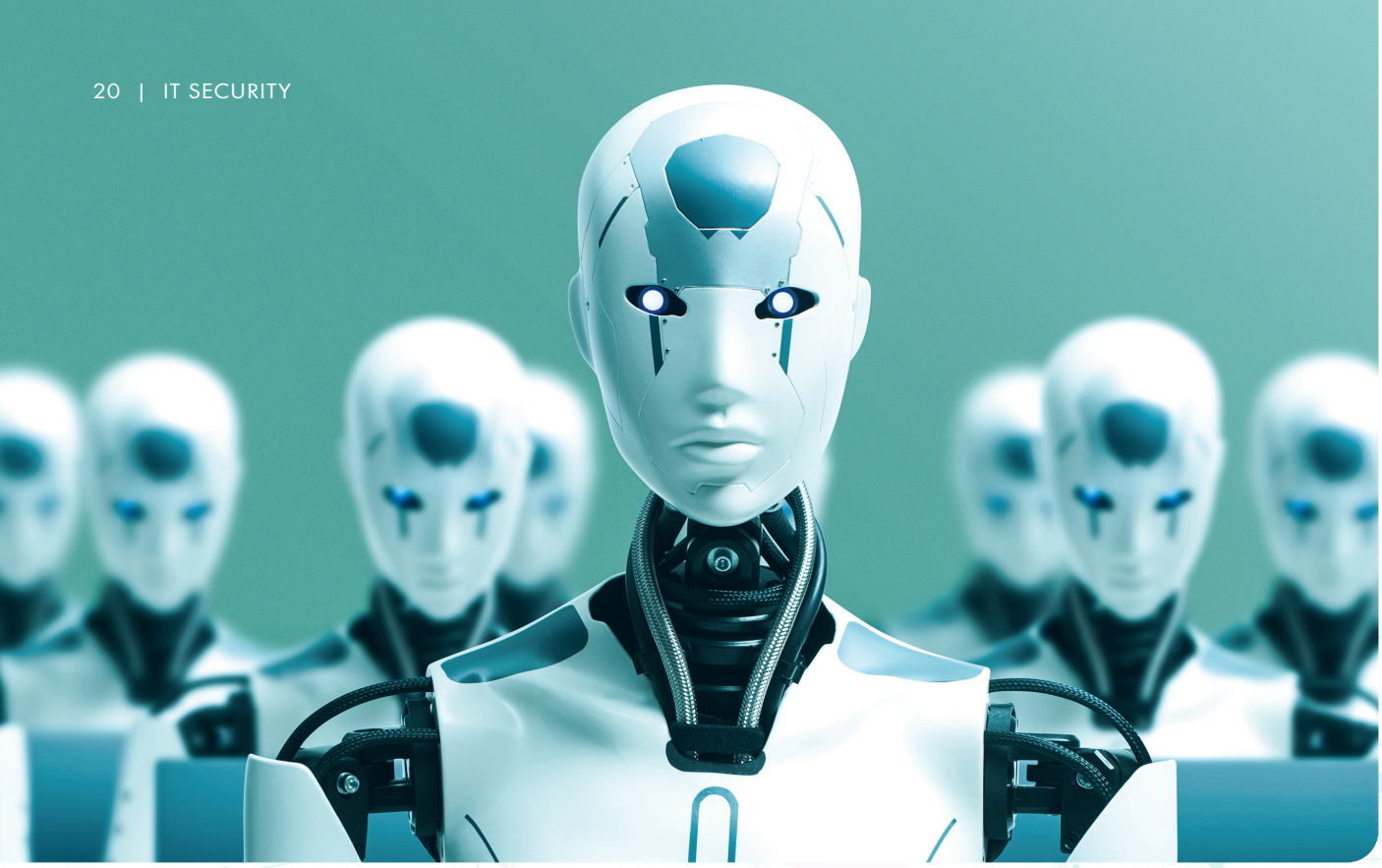
Bei der Auswahl des KI-Anbieters muss deshalb konkret nachgefragt werden, ob und wie die Daten weiterverarbeitet werden. Hier sollte man, je nach Sensibilität der eigenen Daten, auf sofortige und unwiderrufliche Löschung bestehen. Bei DeepL sind wir beispielsweise Eigentümer aller Server und können so ein hohes Maß an Sicherheit eigenständig aufrechterhalten. Zudem löschen wir die Daten unserer Pro-Kunden direkt nach Ausführung der Übersetzung unwiederbringlich.

Datensicherheit in der Zusammenarbeit mit internationalen Partnern

Non-Disclosure-Agreements (NDA), zu Deutsch Geheimhaltungsvereinbarungen, sind im Unternehmenskontext gang und gäbe und ein valides Mittel, um Details in der Zusammenarbeit zwischen Unternehmen festzuhalten. Im Bereich der Datenverarbeitung können sie als weiteres Sicherheitsnetz fungieren, besonders dann, wenn man mit Anbietern aus Nicht-EU-Staaten kooperiert. Denn außerhalb der EU greift die DSGVO nicht und wird – wenn überhaupt – nur auf freiwilliger Basis ganz oder teilweise beachtet. Der durch die DSGVO grundsätzlich gewährleistete hohe Sicherheitsstandard ist für Partner, zum Beispiel in den USA, damit nicht zwingend gegeben.

In einem NDA sollten deutsche Unternehmen deshalb festhalten, ob und wie geteilte Daten gespeichert und genutzt werden dürfen. Auch andere, individuell konzipierte Sicherheitsaspekte können dort festgehalten werden. Viele Unternehmen lassen sich beispielsweise eine dauerhafte Rechenschaftspflicht des Anbieters vertraglich zusichern. NDA lohnen sich also immer dann, wenn die zur Verfügung gestellten Angaben zu KI-Produkten und -Services keine vollumfängliche Bewertung erlauben oder überdies zusätzliche Sicherheitsnetze implementiert werden sollen.

Guido Simon



KI basiertes IAM

EINE REVOLUTION DER IDENTITÄTSVERWALTUNG KOMMT AUF UNS ZU

In der heutigen digitalen Ära, wo Sicherheit und Effizienz an vorderster Front stehen, hat sich das Identity and Access Management (IAM) als unverzichtbares Werkzeug für Unternehmen etabliert. Mit der Integration von künstlicher Intelligenz (KI) in IAM-Systeme erleben wir eine neue Welle der Innovation, die sowohl die Sicherheit erhöht als auch die Benutzererfahrung verbessert. In diesem Artikel werfen wir einen Blick darauf, was ein KI-basiertes IAM leistet und wie es die Landschaft der digitalen Sicherheit verändert.

Was ist KI-basiertes IAM?

KI-basiertes IAM bezieht sich auf die Anwendung von Künstlicher Intelligenz in der Verwaltung von digitalen Identitäten und Zugriffsrechten. Diese Systeme nutzen maschinelles Lernen und andere KI-Technologien, um Sicherheitsprotokolle zu verstärken, Benutzerverhalten zu analysieren und automatisierte Entscheidungen über Zugriffsrechte zu treffen.

Leistungen eines KI-basierten IAM

#1 Verbesserte Sicherheit durch Verhaltensanalyse:
KI-Systeme können kontinuierlich das Verhalten von Nutzern überwachen und analysieren. Ungewöhnliche Aktivitäten, wie der Zugriff zu ungewöhnlichen Zeiten oder von untypischen Standorten, können schnell erkannt und entsprechende Maßnahmen eingeleitet werden.

#2 Automatisierte Zugriffskontrolle:
Durch maschinelles Lernen können KI-basierte IAM-Systeme Muster in Zugriffsanforderungen erkennen und automatisierte Entscheidungen über die Gewährung oder Verweigerung von Zugriffen treffen. Dies reduziert die Notwendigkeit manueller Eingriffe und beschleunigt den Prozess.

#3 Risikobewertung in Echtzeit:
KI-Systeme können Risikobewertungen in Echtzeit durchführen, indem sie aktuelle Anfragen mit historischen Daten vergleichen. Dies ermöglicht eine dynamische Anpassung von Sicherheitsmaßnahmen basierend auf dem aktuellen Risikoniveau.

#4 Benutzerfreundlichkeit und Personalisierung:
KI-basierte IAM-Systeme können die Benutzererfahrung verbessern, indem sie lernfähig sind und sich an die Präferenzen und Verhaltensweisen der Nutzer anpassen. Dies kann beispielsweise durch personalisierte Zugriffsempfeh-

lungen oder vereinfachte Authentifizierungsverfahren erfolgen.

#5 Effizientes Identitätsmanagement:
Mit KI können große Mengen an Identitätsdaten effizient verwaltet und analysiert werden. Dies ist besonders wichtig in großen Organisationen mit Tausenden von Nutzern und komplexen Zugriffsstrukturen.

Workloads
Die Integration von KI und IAM-Systemen ermöglicht die Automatisierung und Optimierung einer Vielzahl von Arbeitsabläufen (Workloads). Diese KI-gesteuerten Funktionen tragen zur Effizienzsteigerung, Sicherheitserhöhung und Verbesserung der Benutzererfahrung bei. Nachfolgend einige Schlüsselbereiche, in denen KI Workloads in einem IAM-System arbeiten können:

- Automatisierte Benutzerverwaltung: KI kann bei der Erstellung, Verwaltung und Löschung von Benutzerkonten helfen. Dies umfasst die Automatisierung von Routineaufgaben wie das Zurücksetzen von Passwörtern, das Aktualisieren von Benutzerprofilen und das Verwalten von Zugriffsrechten.

- Erkennung und Reaktion auf Anomalien: Durch kontinuierliche Überwachung des Benutzerverhaltens kann KI ungewöhnliche Aktivitäten erkennen, die auf Sicherheitsverletzungen oder Insider-Bedrohungen hinweisen könnten. Beispielsweise kann das System Alarm schlagen, wenn ein Benutzer zu ungewöhnlichen Zeiten auf sensible Daten zugreift oder wenn von einem ungewöhnlichen Standort aus auf das System zugegriffen wird.

- Risikobasierte Authentifizierung: KI kann dabei helfen, das Risiko einer jeden Authentifizierungsanfrage zu bewerten, basierend auf Faktoren wie Benutzerstandort, Gerätetyp und früherem Verhalten. Auf dieser Grundlage kann das System entscheiden, ob zusätzliche Sicherheitsmaßnahmen (wie Zwei-Faktor-Authentifizierung) erforderlich sind.

- Zugriffs- und Berechtigungsmanagement: KI kann Muster in den Zugriffsanforderungen und -verhalten der Benutzer erkennen und darauf basierend intelligente Empfehlungen für die Zugriffsrechtevergabe machen. Dies kann dazu beitragen, übermäßige Berechtigungen zu vermeiden und das Prinzip der geringsten Berechtigung (Least Privilege) durchzusetzen.

- Compliance-Überwachung und -Berichterstattung: KI kann kontinuierlich die Einhaltung von Richtlinien und Vorschriften überwachen und automatisierte Berichte erstellen. Dies ist besonders wichtig in regulierten Branchen, wo die Einhaltung spezifischer Compliance-Standards erforderlich ist.

- Selbstlernende Sicherheitsprotokolle: KI-Systeme können aus Interaktionen lernen und ihre Sicherheitsprotokolle entsprechend anpassen. Dies bedeutet, dass das System im Laufe der Zeit effektiver wird, indem es sich an neue Bedrohungen und Veränderungen in der Benutzerumgebung anpasst.

- Vorhersageanalytik: Durch die Analyse historischer Daten kann KI zukünftige Trends vorhersagen und Empfehlungen für präventive Sicherheitsmaßnahmen geben.

- Benutzerfreundliche Interaktionen: KI kann auch in der Benutzeroberfläche des IAM-Systems integriert werden, um eine intuitivere und personalisierte Benutzererfahrung zu bieten, beispielsweise durch Chatbots für die Benutzerunterstützung.

Die Folge ist eine dynamischere, intelligentere und sicherere Verwaltung von Identitäten und Zugriffsrechten, die sowohl die Sicherheitsanforderungen als auch die Benutzerbedürfnisse berücksichtigt.

Herausforderungen und Risiken
Während KI-basierte IAM-Systeme viele Vorteile bieten, gibt es auch Herausforderungen. Datenschutz und ethische Überlegungen sind von großer Bedeutung, insbesondere im Hinblick auf die Verarbeitung persönlicher Daten. Zudem erfordert die Implementierung solcher Systeme eine sorgfältige Planung und fortlaufende Überwachung, um sicherzustellen, dass sie effektiv und sicher funktionieren.

Natürlich wird künstliche Intelligenz auch von den „Bad Guys" genutzt werden, um zum Beispiel Identitäten zu stehlen - Stichwort Deep Fake. Generative KI kann aber auch dazu verwendet werden, Identitäten zu schützen. Das kann zum Beispiel durch das Generieren von gefälschten Datensätzen oder durch das Verschleiern echter Daten geschehen. Das Katz und Maus-Spiel wird auch hier weitergehen.

Zusammenfassung
KI-basiertes IAM wird zu einem mächtigen Werkzeug, das die Art und Weise, wie Unternehmen Identitäten verwalten und Zugriffe steuern, revolutioniert. Durch die Nutzung von KI-Technologien können diese Systeme nicht nur die Sicherheit erhöhen, sondern auch die Benutzererfahrung verbessern und die Effizienz steigern. Trotz der Herausforderungen, die mit ihrer Implementierung verbunden sind, ist das Potenzial von KI im Bereich des IAM enorm und verspricht, ein Schlüsselelement in der Zukunft der digitalen Sicherheit zu sein.

Ulrich Parthier

Konvergente Identitätssicherung

EIN NEUER BEGRIFF BAHNT SICH SEINEN WEG

Identitäts- und Zugriffsmanagement (IAM – Identity and Access Management) spielt eine wesentliche Rolle sowohl in der Sicherheitsstrategie als auch in der Geschäftsanforderung heutiger Unternehmen. Leider zeigen die bestehenden Systeme deutliche Schwächen in beiden Bereichen. Viele Unternehmen sind immer noch mit veralteten Systemen, isolierten Technologielösungen und manuellen, nicht integrierten Prozessen konfrontiert. Diese Systeme und Prozesse waren nie darauf ausgelegt, den heutigen komplexen Anforderungen an die Identitätsverwaltung gerecht zu werden.

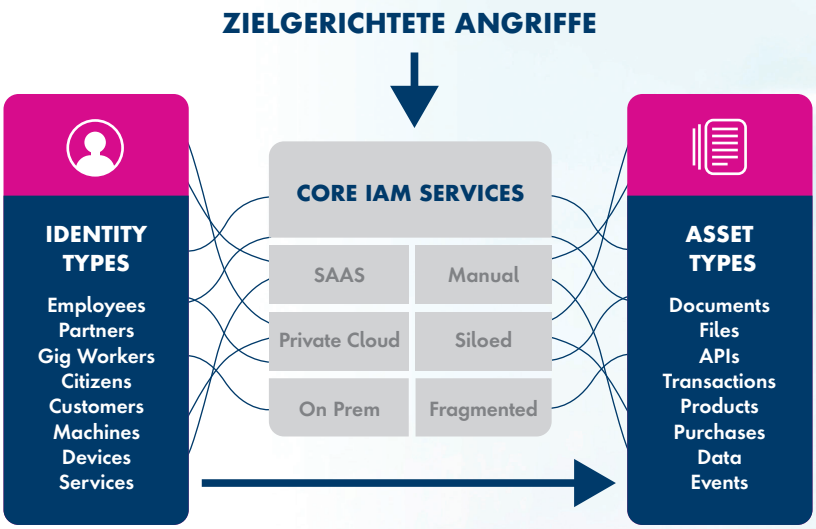
Zudem werden neue Bedrohungsvektoren, die häufig durch generative KI-Technologien unterstützt werden, zunehmend genutzt, um Schwachstellen in diesen fragmentierten Systemen auszunutzen. Dies führt zu alarmierenden Sicherheitsrisiken.

Was aber verbirgt sich hinter dem Begriff „Konvergente Identitätssicherung"? Diese Lösung zielt darauf ab, den gesamten Lebenszyklus der digitalen Identität einer Person sicher zu gestalten, indem sie verschiedene Technologien und Ansätze integriert. Basis ist der Plattformgedanke, der eine starke passwortlose Multi-Faktor-Authentifizierung (MFA) mit kontinuierlicher Risikobewertung und verbesserter Identitätsüberprüfung kombiniert. Dies ermöglicht es Organisationen, die Identität einer Person fortwährend zu überprüfen und sicherzustellen, dass diese Person tatsächlich die ist, die sie vorgibt zu sein. Eine solche Lösung ist die von HYPR (https://www.hypr.com/). Sie umfasst drei Komponenten:

- **HYPR Authenticate:** Diese Komponente ermöglicht eine passwortlose MFA, die auf dem FIDO2-Standard basiert und Phishing-resistent ist. Sie integriert sich nahtlos in bestehende IAM-Umgebungen.
- **HYPR Adapt:** Ein umfassender Identitätsrisikomotor und adaptive Authentifizierung. HYPR Adapt analysiert Risikosignale und Telemetriedaten aus zahlreichen Quellen, einschließlich Benutzerverhalten, mobilen Geräten, Endpunkten und Browser-Signalen.
- **HYPR Affirm:** Eine Lösung für die Überprüfung und Bestätigung von Identitäten, speziell für den Unternehmensbereich entwickelt. Sie verwendet fortschrittliche Technologien wie KI-gestützte Chats, Videoanalyse, Gesichtserkennung und Liveness-Erkennung.

Der Ansatz zielt darauf ab, herkömmliche, manuelle und reaktive Identitätsverifizierungsverfahren zu ersetzen. Durch die Integration von Identitätsüberprüfung und Authentifizierung in einer einheitlichen Plattform sollen Sicherheitslücken geschlossen und Prozesse automatisiert werden. Dies bietet eine dynamische und kontinuierliche Sicherheit für Identität und Authentifizierung.

Eine solche Lösung ist in der heutigen Zeit, in der Identitätsdiebstahl und betrügerische Aktivitäten zunehmen, besonders relevant. Sie ermöglicht es Organisationen, sich gegen solche Bedrohungen zu schützen, indem sie sicherstellt, dass die Identitäten ihrer Benutzer jederzeit verifiziert und geschützt sind.



Der Bedarf an konvergenter Identitätssicherung

Eine umfassende Identity Assurance-Strategie beinhaltet die Betrachtung der Authentifizierung in verschiedenen Reifegraden und den Übergang von isolierten und grobkörnigen Methoden zu einer gesicherten Identität, die kontinuierlich überprüft wird. Das Ziel ist es, die

Fragmentierung und die Vertrauensgrenzen zu reduzieren und die bestehende Authentifizierung mit verifizierten Identitäten auf einer kontinuierlichen Basis zu überlagern.

Diese Strategie umfasst die folgende vier Kernelemente:

1. Passwortlose Multi-Faktor-Authentifizierung (MFA): Sie fußt auf einer FIDO2-basierten, passwortlose MFA-Lösung (HYPR Authenticate). Diese Lösung bietet eine starke Authentifizierung, die gegen Phishing-Attacken resistent ist und sich in bestehende IAM-Systeme integrieren lässt.

2. Risikobewertung in Echtzeit und adaptive Authentifizierung: Das modul HYPR Adapt analysiert Risikosignale aus verschiedenen Quellen, einschließlich Nutzerverhalten und Gerätedaten, um potenzielle Bedrohungen zu erkennen und entsprechende Schutzmaßnahmen einzuleiten, wie zum Beispiel eine verstärkte Authentifizierung oder eine erneute Überprüfung der Identität.

3. Erweiterte Identitätsüberprüfung: Das Modul HYPR Affirm bietet eine Identitätsüberprüfung, die speziell für die Bedürfnisse der Mitarbeiterüberprüfung in Unternehmen entwickelt wurde. Es nutzt Technologien wie KI-gestützte Gespräche, Videoanalyse, Gesichtserkennung und Lebenderkennung, um eine sichere und nahtlose Überprüfung der Mitarbeiteridentität zu ermöglichen.

4. Kontinuierliche Überprüfung: Statt sich auf punktuelle Verifizierungen zu verlassen, erfolgt eine dynamische und fortlaufende Sicherheitsüberprüfung. Dies bedeutet, dass das System bei riskantem Verhalten oder bei Erkennung von verdächtigen Aktivitäten automatische Schritte zur Überprüfung der Identität einleiten kann.

KONTINUIERLICHE RISIKOANALYSE UND -BEHANDLUNG

ROI

Laut einer Forrester Consulting Total Economic Impact (TEI)-Studie, die Kundendaten analysierte zeigte sich, dass Kunden, die HYPR Authenticate einsetzen, einen ROI von 324 Prozent mit einem Gesamtkostenvorteil von 8,1 Millionen US-Dollar und einer Amortisationszeit von weniger als sechs Monaten erzielten. Weitere Positiveffekte waren eine 80prozentige Eliminierung von Passwörtern und damit verbundenen Sicherheitslücken, 95 Prozent weniger Helpdesk-Tickets zum Zurücksetzen von Passwörtern sowie 55 Prozent weniger Zeitaufwand für die Einarbeitung von Mitarbeitern.

Fazit

Durch die Einführung eines konvergenten Identity Assurance-Ansatzes verbessern Unternehmen somit die Identitätssicherheit, beschleunigen die Einführung von Zero-Trust-Prinzipien, verbessern die IAM-Produktivität und verringern ihre Compliance-Anforderungen.

Ulrich Parthier

BETRUGSANTEIL NACH ART DER IDENTIFIZIERUNG

1,5 % Aufenthaltsgenehmigung

11,1 % Führerschein

14,5 % Reisepass

72,8 % Personalausweis

Quelle der Daten: Sumsub

DEEPFAKES

ANSTIEG VON BETRUGSFÄLLEN

Wie Sicherheitsanalysten des Identitätsanbieters Sumsub in ihrem Identitätsbetrugsbericht 2023 feststellten, gab es bei den Betrugstrends einen deutlichen Anstieg bei der Nutzung von Deepfakes. Obwohl auch andere betrügerische Muster wie Mules oder hochentwickelte Fälschungen von IDs weiterhin relevant sind, zeigt sich eine ungefähre zehnfache Wachstumsrate bei der weltweiten Verbreitung von Deepfakes.

MEHR WERT
Identity Fraud Report 2023

Erster Berührungspunkt ist vor allem Desinformation über soziale Medien, wie es zuletzt bei einer philippinischen TV-Moderatorin und ihren Kollegen vorgekommen ist. In einem LinkedIn-Post äußerte die philippinische CNN-Moderatorin Ruth Cabal ihre Besorgnis über die „Gefahren der KI". Zu Beginn des Jahres war sie Ziel eines gefälschten Videos geworden. In einem Deepfake waren das Logo des Unternehmens und eine angebliche Berichterstattung über eine Investitionsplattform zu sehen.

Besonders besorgniserregend ist, dass mittlerweile hochentwickelte Deepfakes dazu genutzt wurden, um nicht nur Prominente, sondern auch Führungskräfte zu imitieren und finanzielle Transaktionen zu autorisieren. Durch künstliche Intelligenz werden Deepfakes von Tag zu Tag realistischer. In einem Selbsttest schaffte es ein Journalist sogar, mittels eines Voicefakes Zugriff auf sein eigenes Konto zu erlangen.

Die Experten von Sumsub führen diesen Anstieg der Deepfake-Betrugsversuche besonders auf die Fortschritte im Bereich der künstlichen Intelligenz in den USA zurück. Angesichts dieser Fortschritte, der einfachen Verfügbarkeit hochwertiger Medieninhalte und der Beliebtheit von Social Media lassen sich die gestiegenen Zahlen der Deepfake Angriffe erklären.

Aufgrund dieser bedenklichen Entwicklung in den USA und Kanada empfiehlt KnowBe4, dass Unternehmen ihre Mitarbeiter in speziellen Security Awareness Trainings schulen. Es gilt, Techniken zur Erkennung und Vermeidung von Deepfakes zu lernen. Dazu zählen Maßnahmen wie die sorgfältige Überprüfung der Identität der anrufenden Person oder der Echtheit der hinterlassenen Voice-Mail.

Organisationen sollten darauf achten, dass die Aufklärung im Bereich Deepfakes über die bloße Erkennung, die schwierig genug ist, hinaus geht. Vielmehr geht es darum, den Teilnehmern zu vermitteln, sich die Zeit zu nehmen, um nach Hinweisen zu suchen, die den Betrug entlarven.

Darüber hinaus muss das Thema Desinformation mit anschaulichen Beispielen nahegebracht werden, um über die Beweggründe und den Ablauf einer Kampagne aufzuklären. Mit Hilfe von Übungen und Workshops lassen sich dann Wege aufzeigen, um Mitarbeiter von der reinen Awareness hin zu einer dauerhaften Verhaltensänderung hinzuleiten.

www.knowbe4.com

Die Verhaltenslücke: Überzeugungen und Verhaltensweisen von Führungskräften

	Was Führungskräfte SAGEN:	Was Führungskräfte TUN:
Sicherheitskultur	**96 %** von Führungskräften erklären, dass sie das Cybersicherheits-Engagement ihres Unternehmens zumindest einigermaßen unterstützen oder es fördern.	**49 % von CXOs haben im letzten Jahr beantragt,** eine oder mehrere Sicherheitsmaßnahmen umgehen zu dürfen.
Schulungen	**78 %** sagen, dass ihre Unternehmen obligatorische Schulungen im Bereich Cybersicherheit anbieten.	**77 % verwenden leicht zu merkende Passwort-Hilfen,** wie z.B. Geburtsdaten oder Spitznamen. Außerdem ist die Wahrscheinlichkeit dreimal höher, dass Führungskräfte ihre Arbeitsgeräte mit unbefugten Nutzern wie Freunden, Familienmitgliedern und externen Freiberuflern teilen.
Phishing	**88 %** der Führungskräfte geben an, dass sie darauf vorbereitet sind, Gefahren wie Malware und Phishing zu erkennen und zu melden.	Von denjenigen, die auf Phishing hereingefallen sind, geben **35 % zu, auf den Link geklickt** zu haben – oder sogar Geld geschickt zu haben.

Quelle: Ivanti

Mit Macht ins Cyberrisiko

SICHERHEITSRISIKO FÜHRUNGSETAGE

Ivanti hat kürzlich den Executive Security Spotlight Report veröffentlicht, der sich auf das Sicherheitsverhalten von Führungskräften, insbesondere der C-Ebene, konzentriert. Obwohl diese Gruppe oft das Ziel von Spear-Phishing- oder Whaling-Angriffen ist, zeigt die Studie, dass Führungskräfte überraschend nachlässig im Umgang mit Cybersicherheit sind. Dies wird besonders problematisch, da sie aufgrund ihrer Führungsaufgaben oft umfangreiche Zugangsrechte besitzen.

Top-Führungskräfte haben häufig ungehinderten Zugang zu firmeninternen Datenquellen und vernetzten Geräten. Gerade sie jedoch sind die Mitarbeitergruppe, die von Bedrohungsakteuren am häufigsten ins Visier genommen wird. Ihre exponierte Position ist ihnen dabei durchaus bewusst: 96 Prozent von ihnen geben an, dass sie den Cybersicherheitsauftrag ihres Unternehmens unterstützen und sich dafür einsetzen.

Aber die Realität sieht anders aus. Nach den Studienergebnissen hatte jeder zweite Top-Entscheider (49 %) im vergangenen Jahr die Umgehung einer oder mehrerer Sicherheitsmaßnahmen durchgesetzt. Dieses Muster zieht sich durch die gesamte Erhebung: Sei es aus Zeitmangel, um spezifische Prozesse zu durchlaufen oder aus einem Gefühl der Sonderstellung heraus: Führungskräfte neigen dazu, sich riskanter zu verhalten als der Rest der Belegschaft.

Unangebrachter Stolz

Die Studie beleuchtet auch die teilweise kritische Zusammenarbeit zwischen Führungskräften und den Security-Teams: Im Gegensatz zum Rest der Belegschaft geben Führungskräfte doppelt so häufig an, dass sie ihre Interaktionen mit der Sicherheitsabteilung als „unangenehm" oder „peinlich" empfunden haben, beispielsweise wenn sie Sicherheitsbedenken geäußert haben. Dies führt dazu, dass Führungskräfte viermal häufiger auf externen, nicht-genehmigten technischen Support zurückgreifen.

Die Ergebnisse unterstreichen die Notwendigkeit, einer vertrauensvollen Zusammenarbeit zwischen Sicherheitsteams und Führungskräften: „Wenn Führungskräfte bereit sind, Sicherheit gegen Benutzerfreundlichkeit einzutauschen, unterschätzen sie, dass sie ein lukratives Ziel für Bedrohungsakteure sind", erläutert Daniel Spicer, CSO bei Ivanti. „In einem digitalen Arbeitsumfeld ist es unmöglich, alle Risiken vermeiden – aber wenigstens die unnötigen Risiken. Die Herausforderung für Sicherheitsverantwortliche besteht darin, die Unterstützung des Unternehmens bei der Erfüllung von Cyberaufgaben einzufordern – insbesondere im Führungsteam. Denn nicht alle Mitglieder der Führungsebene halten Cyberhygiene hoch."

Abhilfe schaffen

Maßnahmen, um die Lücke im Verhalten von Führungskräften zu schließen, umfassen Audits, die Priorisierung von Abhilfemaßnahmen für die häufigsten Risiken, die Durchführung von „spielerischen" Sicherheitstrainings und die Implementierung sogenannter „White Glove"-Sicherheitsprogramme.

www.ivanti.com

MEHR WERT
Executive Security Spotlight Reports

Security@work

CONTENT DISARM AND RECONSTRUCTION (CDR)

Das Ziel von Cybersicherheits-Tools und -Plattformen besteht im Wesentlichen darin, Malware zu beseitigen, bevor sie in das Netzwerk gelangt. Traditionell wurde dies durch Erkennung erreicht, mit Lösungen wie Antivirus-Software und Netzwerk-Sandboxing, die Dateien scannen und verdächtige Dateien markieren.

Einführung in CDR

Content Disarm and Reconstruction (CDR) - auch bekannt als „File Sanitization" oder „Content Sanitization" - ist eine fortschrittliche Technologie, die hervorragende Ergebnisse bei der Abwehr von dateibasierten Angriffen liefert und die erste Zugriffsphase der meisten APTs, Ransomware und Zero-Day-Angriffe effektiv blockiert.

CDR wird zuweilen auch Threat Extraction bezeichnet. In jedem Fall schützt es proaktiv vor bekannten und unbekannten Bedrohungen, die in Dokumenten enthalten sind, indem ausführbare Inhalte entfernt werden.

Die Lösung ist einzigartig, weil sie sich nicht wie die meisten Sicherheitslösungen auf die Erkennung verlässt. Jeder ausführbare Inhalt in einem Dokument wird entfernt, unabhängig davon, ob er als potenzielle Bedrohung für den Benutzer erkannt wird oder nicht. Dadurch bietet CDR eine echte Zero-Day-Prävention und stellt den Anwendern gleichzeitig Dateien schnell zur Verfügung.

Der gesamte Prozess des Auseinandernehmens und Zusammenbauens dauert nur den Bruchteil einer Sekunde und bremst Arbeitsabläufe nicht aus - im Gegensatz beispielsweise zu Sandboxes, die häufig einige Minuten abwarten, bevor sie eine Datei als unbedenklich freigeben. Unternehmen können mit CDR also ihre sicherheitsrelevanten Prozesse beschleunigen und Sandbox-Umgebungen, die Ressourcen binden und Kosten verursachen, entlasten. Nur noch Dateien, die CDR nicht transformieren kann, werden künftig zur Analyse an die Sandbox überstellt.

Manche CDR-Lösungen wandeln die verschiedenen Ausgangsformate, zu denen neben PDFs und Office-Dokumenten in der Regel auch Bilder, HTML-Dateien, Mail-Formate und Archive zählen, lediglich in PDFs um. Das erschwert es jedoch, Daten zu aktualisieren oder zu ergänzen. Besser sind daher Lösungen, bei denen das Endformat dem Aus-

gangsformat entspricht. Wobei es hier sogar Möglichkeiten gibt, das Format zu aktualisieren und einen Wildwuchs mit unzähligen alten Word-, Excel- und PowerPoint-Formaten einzudämmen. Die neu aufgebauten Dateien gleichen optisch dem Original, sodass es keinerlei Einschränkungen bei der User Experience gibt.

Prozessfolge

Der CDR-Prozess, der das Risiko, dass bösartiger Code in ein Netzwerk eindringt, vollständig ausschließt, folgt einem Präventionsverfahren, das immer drei Grundprinzipien folgt:

#1 Jede Datei wird als Bedrohung behandelt

#2 Das Originaldokument ist nicht vertrauenswürdig und wird daher außerhalb des Netzwerks gespeichert.

#3 Es wird eine neue Datei erstellt, die als saubere Replik der Originaldatei dient.

Einige Jahre nach ihrer ursprünglichen Entwicklung wurde diese Technologie als „CDR" – Content Disarm and Reconstruction – bezeichnet.

In den ersten Versionen von CDR wurde das Originaldokument im Wesentlichen „geglättet", das bedeutet, jeder potenzielle aktive Code innerhalb des Dokuments wurde entfernt. Wenn Word- oder Excel-Dateien eintrafen, wurden sie als Bild repliziert, wobei das ursprüngliche Format und die Dateifunktionen verloren gingen. Der gesamte Inhalt der Datei war lesbar, aber die Dokumente konnten nicht bearbeitet, kopiert oder in irgendeiner Weise manipuliert werden.

Die Entwicklung von CDR

Als CDR erstmals auf den Markt kam, sollte es die traditionellen, auf Erkennung basierenden Sicherheitslösungen ersetzen. Obwohl alle diese Lösungen einen Mehrwert bieten, wiesen sie erhebliche Einschränkungen in Bezug auf Sicherheit und/oder Benutzerfreundlichkeit auf. Zu den typischen Einschränkungen gehören die Ineffizienz gegenüber unbekannter Malware, die fehlende Unterstützung verschlüsselter Dokumente und großer Dateien, die Latenzzeit und Skalierbarkeit der Sandbox sowie die Einschränkung von Geschäftsabläufen.

Damit CDR von Unternehmen angenommen werden konnte, musste die Benutzerfreundlichkeit deutlich verbessert werden. Das war leichter gesagt als getan. Die ersten Anbieter, die CDR anboten, setzten weiterhin auf eine geglättete Datei, was zu einer schreibgeschützten Version des Dokuments führte.

Dadurch war das Dokument zwar vollkommen sicher, die Nutzer waren aber frustriert, da die eingebetteten Dateien und die Dateifunktionen verloren gingen.

Diese Einschränkungen führten dazu, dass frühe CDR-Lösungen zum kommerziellen Scheitern verurteilt waren. Zwar gibt es Anwendungen für diese Funktion, und mehrere führende Sicherheitsanbieter bieten diese eingeschränkte Lösung auch heute noch an, doch die meisten Unternehmen benötigen eine robustere Lösung, die die volle Nutzbarkeit der Dokumente, die Verarbeitung in großem Umfang und in Echtzeit ermöglicht.

Blacklisting

Zwar wurde versucht das Paradigma zu durchbrechen, indem man eine fortschrittlichere Methode der CDR entwickelte, man hatte aber immer noch mit dem grundlegenden Problem der Sicherheit im Vergleich zur Benutzerfreundlichkeit zu kämpfen. Um sicherzustellen, dass die Benutzerfreundlichkeit nicht beeinträchtigt wird, wählten diese Sicherheitsanbieter einen Blacklisting-Ansatz. Bei dieser Variante des CDR wurde das gesamte Originaldokument in eine Kopie kopiert, dann wurde die Kopie geöffnet und jedes Element auf bösartigen Code und bekannte Risiken (etwa Makros, aktive Inhalte) gescannt. Schließlich wurden Elemente mit hohem Risiko entfernt, und die Datei wurde an den Empfänger gesendet.

Blacklisting vs. Flattening

Im Gegensatz zum Flattening liefert diese Methode (von den Anbietern manchmal als „Deep-CDR" bezeichnet) den Benutzern eine voll funktionsfähige Kopie, mit Ausnahme aller Makros oder anderer aktiver Inhalte, die entfernt wurden. Dieser Ansatz ermöglichte es den Anbietern, die Benutzerfreundlichkeit zu verbessern - er war relativ schnell, behielt die Dokumententreue bei und konnte eingebettete Dateien scannen.

Allerdings hielt diese Methode nicht die Sicherheitsstandards ein, die die ursprüngliche CDR-Technologie ihren Benutzern versprach. Ähnlich wie herkömmliche Erkennungslösungen und im Gegensatz zu Präventionstechnologien stellt das Blacklisting ein reduziertes Sicherheitsniveau dar, das anfällig für Zero-Day-Angriffe und das Verbleiben

PLUS

Lesen Sie den kompletten Beitrag hier:

verdächtiger Elemente in der neuen Datei ist. Mit anderen Worten: Diese Version von CDR geht Kompromisse bei den CDR-Sicherheitsstandards ein, um eine bessere Leistung zu erzielen.

Paradigmenwechsel

Resec hat hier einen Paradigmenwechsel vollzogen, indem es die ursprüngliche Vision von CDR umsetzte - absolute Sicherheit in Verbindung mit voller Benutzerfreundlichkeit.

Mit dem CDR von Resec wird das Originaldokument in eine digitale Darstellung umgewandelt, die alle Elemente des Originaldokuments enthält. Anschließend wird jedes Element des Originaldokuments überprüft und in kürzester Zeit eine neue, visuell identische Datei erstellt.

Die resultierende Datei sieht aus wie das Original, aber im Gegensatz zu Blacklisting-Techniken wurde sie von Grund auf neu erstellt, wobei nur bekannte und als sicher bestätigte Elemente verwendet wurden. Das Ergebnis ist ein Dokument, das zu 100 Prozent vor bekannten und unbekannten Angriffen geschützt ist.

All dies geschieht unter Beibehaltung des nativen Dateiformats, der vollen Funktionalität und der Verarbeitung auch von großen Umfängen und das in Echtzeit. Damit zielt die Lösung auf globale Unternehmen, die die Sicherheit erhöhen wollen, ohne die Geschäftsprozesse zu beeinträchtigen.

Zero Trust Prevention am Gateway

Resec bietet eine innovative Architektur, die von Anfang an auf solche Anwendungszwecke ausgerichtet ist. Die Zero-Trust-Prevention-Plattform nutzt leistungsstarke Sicherheits-Engines - einschließlich CDR - um einen umfangreichen Schutz vor bekannten und unbekannten dateibasierten Malware-Bedrohungen zu bieten. Alle gängigen Bedrohungsvektoren werden so geschützt, einschließlich E-Mail, Wechseldatenträger, FTP-Übertragungen, Dateiportale, Uploads, Downloads und mehr.

Dateien, die das Gateway erreichen, werden sofort unter Quarantäne gestellt. So bietet man das Beste aus beiden Welten - eine leistungsstarke Erkennung, um bösartige und verbotene Dateien zu blockieren, und eine einzigartige CDR-Prävention, um false negative Meldungen zu vermeiden und Zero-Day-Angriffe zu verhindern. Und das, während der Datenverkehr auch in großen Umfängen und mindestens 90 Prozent schneller als bei herkömmlichen Sandboxen verarbeitet wird.

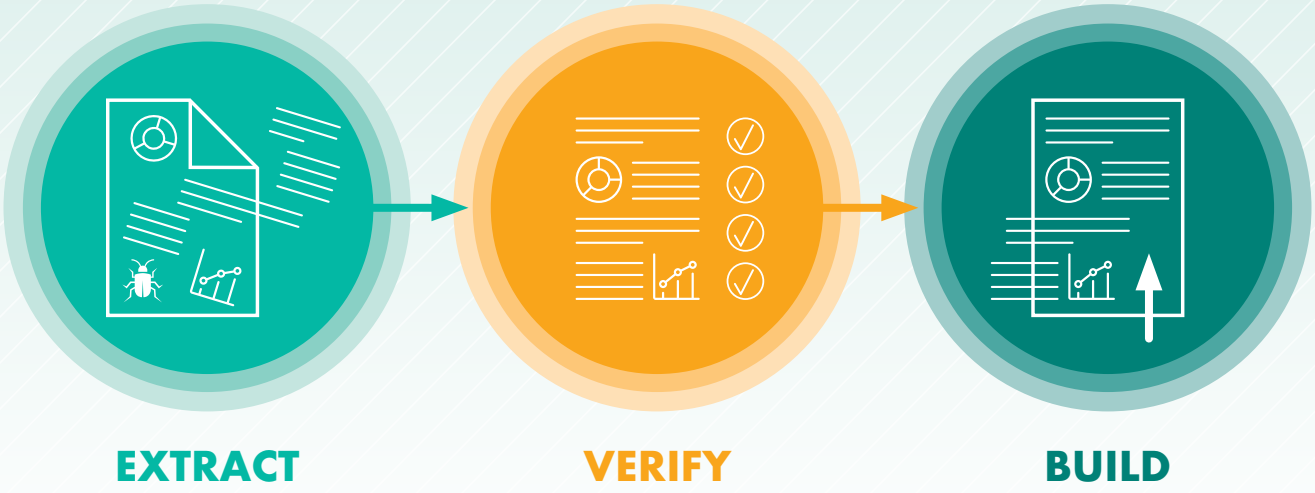
CDR ergänzt andere Sicherheitslösungen

Standardmäßig gehen bei der Transformation von Office-Dokumenten durch CDR alle Makros, die sich in den Ursprungsdateien befinden, verloren. Da einige Unternehmen allerdings Makros benötigten, sollten CDR-Lösungen flexible Optionen bieten, um bestimmte Dateien oder Kommunikationskanäle von der Neuverpackung der Inhalte auszunehmen.

Hier kommen weiterhin die bestehenden Security-Tools zum Zuge, die CDR nicht ablösen will, sondern lediglich ergänzt. Idealerweise greifen alle Lösungen dabei auf einen zentra-

SICHERE DATEIEN IN DREI SCHRITTEN:

CDR LIEST DIE EIGENTLICHEN GESCHÄFTSINFORMATIONEN AUS, PRÜFT SIE AUF EINE GÜLTIGE STRUKTUR UND ERSTELLT DARAUS NEUE, GARANTIERT MALWARE-FREIE DATEIEN



(Quelle: Forcepoint)

len Satz an Richtlinien zu, damit IT-Abteilungen nicht mehrere Sätze parallel pflegen müssen, was aufwendig ist und unweigerlich zu inkonsistenten Regeln führt.

Ähnlich wie der Umgang mit Makros lässt sich dann auch der Umgang mit signierten und verschlüsselten Dateien richtliniengesteuert anpassen. Denn CDR kann zwar signierte Dokumente neu aufbauen und dadurch von möglichen Schadfunktionen bereinigen, doch der Neuaufbau bricht die Signatur. In der Praxis hat es sich bewährt, das bei Dokumenten aus unbekannten Quellen tatsächlich zu tun – aus Sicherheitsgründen. Auf die entfernte Signatur wird der Anwender hingewiesen. Bei klar definierten Prozessen jedoch, die auf signierten Dokumenten basieren, hält sich CDR hingegen zurück und überlässt anderen Security-Tools das Feld.

Verschlüsselte Dateien

Schwieriger ist es bei verschlüsselten Dateien, die CDR nicht einzusehen vermag, so Frank Limberger, Data & Insider Threat Security Specialist bei Forcepoint. Hier könnten IT-Abteilungen etwa die Zustellung via Mail bei vertrauenswürdigen Absendern gestatten – in allen anderen Fällen würde der verschlüsselte Dateianhang entfernt und ein Hinweis den Empfänger darüber informieren. Handelt es sich um verschlüsselte E-Mails, sollte sich die CDR-Lösung als Mail Transfer Agent beim Verschlüsselungsgateway einklinken können, um die dort entschlüsselten Nachrichten neu aufzubauen, bevor sie erneut verschlüsselt und final zugestellt werden.

Überhaupt sollten CDR-Lösungen sehr integrationsfreudig sein. Einerseits um die Arbeitsaufteilung mit anderen Security-Tools wie Firewall oder Sandbox abzustimmen. Andererseits um Zugriff auf alle Wege zu erhalten, auf denen gefährliche Dateien ins Unternehmen gelangen können. E-Mails und Downloads aus dem Internet sind zweifellos die Klassiker, dennoch kann sich Malware auch über Web-Anwendungen, Datei-Uploads, freigegebene Ordner, File-Sharing und Chat-Kommunikation einschleichen.

Ulrich Parthier

Verborgene Bedrohungen

CYBER-ANGRIFFE IM VERSCHLÜSSELTEN DATENVERKEHR

Zscaler veröffentlicht die Ergebnisse des jährlichen ZscalerTM ThreatLabz 2023 State of Encrypted Attacks Report und stellt ein kontinuierliches Wachstum von Bedrohungen fest, die über HTTPS transportiert werden. Im Vergleich zu 2022 stiegen die Angriffe über verschlüsselte Kanäle um 24 Prozent. Im zweiten Jahr in Folge steht die Fertigungsindustrie an der Spitze der am häufigsten angegriffenen Branchen, während Bildungs- und Regierungseinrichtungen den höchsten Anstieg der Angriffe im Vergleich zum Vorjahr zu verzeichnen hatten. Darüber hinaus dominierten schädliche Web-Inhalte und Malware-Payloads gegenüber anderen Arten von verschlüsselten Angriffen und Werbe-Spyware-Seiten. Cross-Site-Scripting machten 78 Prozent aller blockierten Angriffe aus. Der Report analysierte fast 30 Milliarden Bedrohungen von Oktober 2022 bis September 2023 die von der Zscaler Zero Trust Exchange Plattform blockiert wurden. Insgesamt werden 86 Prozent aller Cyber-Bedrohungen einschließlich Malware, Ransomware und Phishing-Angriffe über verschlüsselte Kanäle übertragen.

„Da fast 95 Prozent des Internetverkehrs über HTTPS fließt und 86 Prozent der modernen Bedrohungen über verschlüsselte Kanäle übertragen werden, stellt jeder HTTPS-Verkehr ohne Inline-Inspektion einen toten Winkel dar, den Cyber-Kriminelle für ihre Angriffe auf globale Organisationen ausnutzen", sagt Deepen Desai, Chief Security Officer bei Zscaler. „Um sich gegen verschlüsselte Angriffe zu schützen, sollten Unternehmen Appliances wie VPNs und Firewalls durch eine Zero Trust Network Access (ZTNA)-Lösung ersetzen. Damit können IT-Teams den TLS-Verkehr in großem Umfang inspizieren und gleichzeitig Bedrohungen abwehren und damit den Verlust sensibler Daten verhindern."

ThreatLabz-Empfehlungen im Kampf gegen verschlüsselte Angriffe:

- Einsatz einer Cloud-nativen, Proxy-basierten Architektur, um Bedrohungen im gesamten verschlüsselten Datenverkehr in großem Umfang zu entschlüsseln, zu erkennen und zu verhindern.
- Untersuchung des gesamten Datenverkehrs zu jeder Zeit durch SSL-Inspektion, um Malware-Payloads, Phishing und C2-Aktivitäten zu erkennen, die SSL-/TLS-Kommunikation nutzen.
- Nutzung einer KI-gesteuerten Sandbox, um unbekannte Angriffe unter Quarantäne zu stellen und Patient-Zero-Malware zu stoppen, die möglicherweise über TLS übertragen wird.
- Bewertung der Angriffsfläche des Unternehmens, um das Risiko zu quantifizieren und die exponierte Angriffsfläche zu sichern.
- Verwendung einer Zero Trust-Architektur, um die gesamte Konnektivität ganzheitlich zu sichern.
- Verwendung der User-to-App-Segmentierung mit Hilfe des Prinzips des Least privileged Access-Modells auch für authentifizierte User.

www.zscaler.com

MEHR WERT
Vollständiger Report

Zero Trust

GANZHEITLICHER ANSATZ FÜR UMFASSENDE SICHERHEIT

DIE IDENTITÄT IST UNBESTREITBAR EIN ECKPFEILER DES ZERO-TRUST-MODELLS, ABER SIE IST NUR EIN TEIL EINER KOMPLEXEN STRUKTUR.

Neil Thacker, CISO, EMEA, Netskope, Inc, www.netskope.com

Die Identität ist ein grundlegender Bestandteil eines effektiven Zero-Trust-Ansatzes. Es besteht aber die Gefahr, dass sich Unternehmen so sehr auf dieses eine Element konzentrieren, dass sie vergessen, dass es noch andere gibt. Dies kann zu potenziellen Schwachstellen führen.

Damit Zero Trust erreicht werden kann, muss es mehrere Formen der Verifizierung geben. Wenn man die Komplexität dieses Prozesses zu sehr vereinfacht, besteht die Gefahr, dass ein falscher Eindruck von Sicherheit vermittelt wird. Daher muss immer davon ausgegangen werden, dass jedes System kompromittiert werden kann und wird. Je mehr Maßnahmen zum Schutz ergriffen werden, desto mehr Vertrauen können wir in das System setzen.

Die Identitätsauthentifizierung ist eine der ersten und am häufigsten verwendeten Maßnahmen für Zero Trust und sollte ein zentraler Bestandteil jeder Strategie sein.

Im Folgenden finden Sie sieben weitere Elemente, die Unternehmen integrieren sollten, um eine sichere, robuste Zero-Trust-Infrastruktur zu gewährleisten:

➤ Gerät
Ein vollständig authentifizierter Benutzer auf einem kompromittierten Gerät stellt ein Sicherheitsrisiko dar. Zero Trust sollte zwischen Firmen- und Privatgeräten unterscheiden und den Zustand des Geräts, Patch-Level und Sicherheitskonfigurationen prüfen, bevor der Zugriff gewährt wird.

➤ Standort
Angesichts des zunehmenden hybriden Arbeitens werden Nutzer versuchen, von verschiedenen Standorten aus auf Dokumente zuzugreifen. Daher muss es im Unternehmen ein System geben, das ungewöhnliche Trends erkennen kann, ebenso wenn sich jemand gleichzeitig von zwei unterschiedlichen Standorten aus anmeldet.

➤ App
Mit der Zunahme von Cloud-Diensten sollten Sicherheitsteams bestimmte Apps für die Nutzung im Unternehmen prüfen und genehmigen und bei Bedarf erweiterte Kontrollen und/oder Beschränkungen für nicht genehmigte Anwendungen einführen, um einen möglichen Datenverlust zu verhindern.

➤ Instanz
Unternehmen gestatten ihren Mitarbeitern die Nutzung ihrer persönlichen Cloud-Apps, etwa Microsoft 365. Dies kann jedoch zu einem Problem führen, insbesondere wenn vertrauliche Unternehmensdaten an eine persönliche App freigegeben werden.

➤ Aktivität
Zero Trust erstreckt sich auf die Art und Weise, wie Anwendungen miteinander interagieren und wie sie auf Daten zugreifen. Innerhalb der Sitzung eines einzelnen Benutzers unterliegen die Aktionen, die eine Anwendung im Namen dieses Benutzers durchführt, einer genauen Überprüfung.

➤ Verhalten
Wenn ein Mitarbeiter (oder ein Unternehmen) plötzlich auf große Datenmengen zugreift oder vertrauliche Dateien herunterlädt, sollten Alarmglocken läuten, selbst wenn der Benutzer ursprünglich authentifiziert war.

➤ Daten
Im Mittelpunkt von Zero Trust stehen die Daten – es geht darum, die Integrität und Vertraulichkeit der Daten zu gewährleisten. Daten müssen im Ruhezustand und während der Übertragung verschlüsselt werden und dass Datenzugriffsmuster, unabhängig von der Identität des Benutzers, auf Anomalien überwacht werden.

Die Identität ist unbestreitbar ein Eckpfeiler des Zero-Trust-Modells, aber sie ist nur ein Teil einer komplexen Struktur. Echtes Zero Trust wird nur dann erreicht, wenn ein Unternehmen einen integrierten, ganzheitlichen Ansatz verfolgt, der alle Berührungspunkte, Benutzer und jedes Gerät berücksichtigt. Durch die Einbeziehung aller sieben Elemente in Ihren Zero-Trust-Ansatz können Unternehmen mit weitaus größerem Vertrauen operieren.

Neil Thacker

Cybersecurity auf Applikationsebene

DER BLINDE FLECK IN DER IT-SICHERHEITSSTRATEGIE

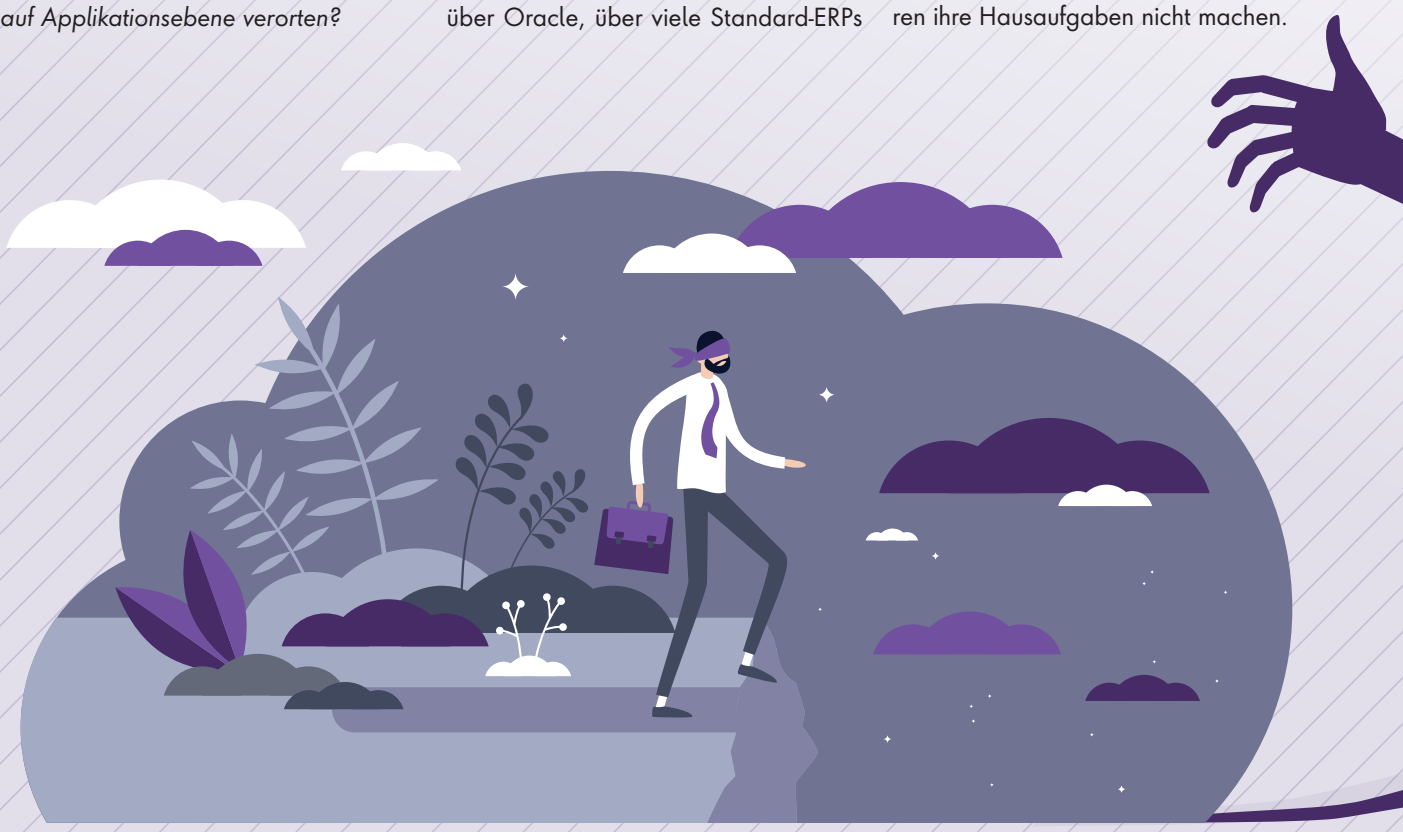
Ralf Kempf, Geschäftsführer von Pathlock Deutschland, Security Researcher und SAP Security Evangelist arbeitet bereits seit 30 Jahren in der SAP-Security-Welt. Er ist Autor vieler Publikationen und Redner auf Security-Konferenzen weltweit. Anlässlich der Thought Leadership Konferenz erklärt er im Gespräch mit Ulrich Parthier, Publisher it security, warum seiner Erfahrung nach Cybersecurity auf Applikationsebene der blinde Fleck in fast jeder Sicherheitsstrategie ist.

Ulrich Parthier: *Herr Kempf können Sie uns erklären, wo genau Sie einen blinden Fleck der Cybersecurity auf Applikationsebene verorten?*

Ralf Kempf: Gerne. In vielen Unternehmen gelten heutzutage Buzzwords wie Zero Trust, Microsegmentierung oder Software Defined Networks als Allheilmittel für die Absicherung von IT-Systemen. Dabei gerät jedoch oft aus dem Blick, dass elementare Grundlagen wie Asset & Application Management, ein IT-Security-Management-System und der Aufbau echter IT-Security-Kompetenz noch gar nicht abgeschlossen – oder schlimmer, noch nicht einmal begonnen wurden. Hier liegt der besagte blinde Fleck.

Wenn wir jetzt über die Applikationsebene reden, dann über SAP-Systeme, über Oracle, über viele Standard-ERPs und andere Geschäftsanwendungen, die eingesetzt werden. Oft hören wir von Unternehmen die erstaunte Frage, wo denn das Problem in der Anwendungssicherheit sei. Es liege doch alles ordentlich beim Outsourcer in der Cloud, inklusive Firewall.

Fragt man andererseits Entscheider oder Anwender, dann fürchten viele nach wie vor Ransomware-Attacken, die typischen Krypto-Trojaner, gestohlene Identitäten oder Schlüssel, sowie nicht gepatchte Systeme. Es geht hier um all die Klassiker, die man auch täglich in der Presse liest, was leider beweist, dass die Unternehmen hier offensichtlich seit Jahren ihre Hausaufgaben nicht machen.



Ulrich Parthier: *Was sind Ihrer Ansicht nach die Ursachen?*

Ralf Kempf: Dafür gibt es zwei Gründe. Zum einen gibt es in der Security-Welt immer wieder neue Begriffe, neue Technologien, die stets mit der trügerischen Hoffnung verbunden sind, damit würde ad hoc alles besser. Aber letztlich, wenn man dies so lange verfolgt wie ich, muss man feststellen, dass jede Umsetzung viel zu lange dauert. Das ist nachvollziehbar, aber gleichzeitig auch der zweite Grund: Es mangelt an Ressourcen, an Wissen und an Budgets.

So sind es noch immer die alten Bekannten unter den Risiken, und nach wie vor liegen die Unternehmen Monate oder Jahre hinter den aktuellen Bedrohungs-Szenarien zurück. Wir reden nach wie vor über Datendiebstahl und Erpressung. Das ist keineswegs neu und nicht nur einigen Kreis- und Gemeindeverwaltungen in Deutschland passiert. Es waren sehr namhafte Unternehmen dabei. Und jetzt hat sich ein neues großes Problem manifestiert, der Super-GAU, als Microsoft kürzlich zugeben musste, dass ein Generalschlüssel für die Azure-Cloud gestohlen wurde.

Ulrich Parthier: *Warum war gerade dies so eklatant?*

Ralf Kempf: Man kann sich das so vorstellen: Die ganze Welt ist ein Gebäude mit Eigentumswohnungen. Nun hat irgendjemand den Generalschlüssel für alle Wohnungen der Welt, kann jede jederzeit betreten und dort anrichten, was er will. Und Sie als Eigentümer werden es nicht einmal merken. Rausgekommen ist dieser Fall übrigens, weil einige öffentliche Stellen merkwürdige Zugriffe in den Logs bemerkt und gemeldet haben. Und dann wurde seitens Microsoft kleinlaut zugegeben, man habe ein Problem. So wird die vermeintlich paranoide Denkweise von uns Sicherheitsexperten durch völlig neue Dimensionen der Worst-Case-Szenarien bestätigt. Bislang gingt es meist um Schäden einzelner Unternehmen, und der GAU war, wenn das Unternehmen aus dem Markt scheidet.

Gerade der Microsoft-Hack zeigt nun aber, dass blindes Vertrauen in die Infrastruktur und das Identity & Account Management der großen Hyperscaler sehr schnell zu viel schwerwiegenderen Sicherheitslücken führen können. Wenn solche Schlüssel in falsche Hände geraten, haben wir alle ein Problem. Nicht auszudenken, wenn jemand damit nicht nur Daten stiehlt, sondern Denial of Service betreibt und alles außer Betrieb nimmt.

MIT KONSEQUENTER METHODIK, DEM RICHTIGEN PRAGMATISMUS UND GUTEN TOOLS KANN MAN THEORETISCH SELBST GROSSE UNTERNEHMEN MIT EIN, ZWEI RESSOURCEN ÜBERWACHEN.

Ralf Kempf,
Geschäftsführer, Pathlock Deutschland,
www.pathlock.com/de

Ulrich Parthier: *Wie kann man diesen neuen Gefahren begegnen?*

Ralf Kempf: Hier lohnt sich ein Blick darauf, wie Unternehmen aufgestellt sind. Zunächst die Gretchenfrage: Gehe ich in die Cloud oder mache ich es On-Premises? Das Mantra lautet oft, die Cloud löse alle Probleme. Und es gibt fraglos sehr gute Szenarien für Cloud-Anwendungen. Aber auch hier kommt es darauf an, dass man es richtig umsetzt, vor allen Dingen mit einer ganzheitlichen Sichtweise auf das IT-System einer Unternehmung.

Hinsichtlich der Applikationsebenen in einer klassischen Unternehmens-IT haben wir einmal die Infrastruktur, darunter das Netzwerk, auch Enterprise Clouds, Datenbanken, Betriebssysteme und Komponenten, auf denen meine Software läuft. Für diese technischen Komponenten gibt es bei vielen Unternehmen schon seit Jahren gute Security Tools, mit denen man Patches, Konfiguration und Logs überwachen kann.

Eine Anwendungsebene höher blicken wir auf die Applikationen, die klassischen Businessanwendungen wie Zahlungsverkehr, ERP-Software, Personalverwaltung. Zuletzt gibt es die Operations-Technology-Anwendungen wie Fließbandsteuerung, Produktionsstraßen, Kraftwerkssteuerungsanlagen. Dieser Bereich funktioniert noch einmal ganz anders, hat aber dennoch Schnittstellen mit der internen IT und mit den Infrastrukturen im Unternehmen.

Ulrich Parthier: *Man muss also eine Unternehmung schon aufgrund der Schnittstellen ganzheitlich betrachten?*

Ralf Kempf: Absolut! Der Aussage, die Bereiche liefen vollständig getrennt, sollte man wenig Glauben schenken. Neulich haben wir ein System von außen gescannt und dem Kunden mitgeteilt, ein Mess- und Regelsystem zu Druck, Temperatur und Füllstand seiner Gasanlagen sei im Internet frei zugänglich und könne von jedermann beliebig eingestellt oder geschlossen werden. Der Kunde wusste nicht einmal von dessen Existenz und letztlich haben wir festgestellt, dass ein Dienstleister ein kleines Gerät in einen Verteilerschrank eingebaut und auf dem falschen Port konfiguriert hatte. Eine Handvoll deplatzierter Technik steuert die ganze Fabrik – da sieht man, wie prekär diese Abhängigkeiten sind.

Betrachtet man nun ein Applikationssystem, sei es Operations Technology oder IT Technology, hat man einen Basis-Bereich, ob Metall oder Virtualisierung, Netzwerkbetriebssystem oder Datenbank. Und darauf läuft dann eine Software wie Windows Office oder Exchange für im Ansatz getrennte Anwendungsbereiche. Genau diese Trennung macht es schwierig, solche Systeme zu verstehen. Besonders wenn wichtige Komponenten nicht mehr im eigenen Haus sind, wo sich ein eigenes Team darum kümmert, sondern in eine Cloud ausgelagert werden. Man verliert den Überblick. Und das macht Unternehmen derzeit leichter angreifbar.

> BLINDES VERTRAUEN IN DIE INFRASTRUKTUR UND DAS IDENTITY & ACCOUNT MANAGEMENT DER GROSSEN HYPERSCALER KANN SEHR SCHNELL ZU SCHWERWIEGENDEREN SICHERHEITSLÜCKEN FÜHREN.
>
> **Ralf Kempf, Geschäftsführer, Pathlock Deutschland, www.pathlock.com**

Bei unseren Umfragen, worauf Unternehmen in puncto Sicherheit gerade fokussieren, war eine häufige Rückmeldung: „Wir arbeiten mit Authentifizierung, haben alles standardisiert, eine einheitliche Identity-Verwaltung und Smartcards eingeführt und uns um segmentierte Berechtigungen gekümmert." Das klingt für sich genommen zielführend. Bis dann der jährliche Wirtschaftsprüfer feststellt, dass es nicht richtig aufgesetzt wurde. Es gab also über 365 Tage ein latentes Risiko und die Erkenntnis ist hart: „Wir wissen gar nicht so richtig, wie unsere Systeme funktionieren. Das wird immer komplizierter, Abhängigkeiten prüfen wir nicht mehr, bei den Patches sind wir schon lange nicht mehr auf dem aktuellen Stand."

Um beim Bild des Hauses zu bleiben, kommt man also ohne ganzheitliche Sicht dahin, ein Konstrukt aufzubauen, bei dem man Schlösser an den Türen verbessert, die Haustür dreifach abgesichert, aber die Fenster offen lässt. Und dies merken wir bei Tests immer wieder an der kurzen Zeit, die es braucht, um in ein System einzudringen. Ein Unternehmen lahmzulegen ist nicht nur technisch immer noch schnell möglich, sondern sogar einfacher, wenn man Social Media wie LinkedIn und Xing nutzt. Früher war es ungleich schwieriger, Informationen über Entscheider und Administratoren zu finden.

Ulrich Parthier: *Wo sehen Sie aktuell die größten Schwachstellen in der Absicherung?*

Ralf Kempf: Zunächst ist die Zuständigkeit oft nicht geregelt oder fragmentiert, und es gibt keine einheitliche Sicht im Unternehmen darauf. Ganz häufig sind etwa die IT klassischer Art und die Produktionssteuerungs-IT so getrennt, dass man sich maximal in der Kantine trifft. Dies sind sehr gefährliche Konstrukte, wenn der eine nicht vom anderen lernt, man voneinander abhängt, dies aber nicht mal weiß.

Dann lohnt ein Blick auf die Zugangssteuerung durch die Einführung modernerer Systeme. Auf der einen Seite wird vieles einfacher, weil man etwa eine Microsoft-ID übergreifend nutzen kann. Andererseits kann man sie dann auch in vielen Systemen missbrauchen. Da ist das Schwachstellen-Management immer noch relativ dünn und auch die Erkennung von Bedrohungen nach wie vor schwach.

Bezeichnend ist, wenn Penetration Tests bei einem Kunden mit SIEM-System aus-

MEHR WERT

Schauen Sie sich hier den Vortrag von Ralf Kempf an:

geführt werden. Dieser müsste eigentlich nach einer Stunde Alarm schlagen. Es ist mir in den letzten zehn Jahren aber nur genau einmal passiert, dass ein Administrator überhaupt etwas gemerkt hat.

? **Ulrich Parthier:** *Wie sollten Unternehmen sich Ihrer Meinung nach aufstellen?*

Ralf Kempf: Es gibt zunächst mal grundsätzliche Prozesse, die relativ einfach umzusetzen sind. Das NIST Framework des National Institute for Security Standards and Technology gibt beispielsweise einen einfachen Zyklus vor, nach dem man arbeiten kann. Es ist tatsächlich weniger relevant, welchen Ansatz man nutzt, man muss es nur tun.

Sie alle bedienen sich folgender Methodik: Identifiziere zunächst deine Assets und Technologien. Wo stehen und wie funktionieren sie? Erstelle damit eine realistische Risikoeinschätzung. Dann schütze die Systeme, spiele Patches ein, gehe durch die Handbücher, wirf die Standard-User raus. Etabliere schließlich ein System, das diese Dinge überwacht, und zwar laufend und rund um die Uhr.

Das ist kein Hexenwerk: Mit konsequenter Methodik, dem richtigen Pragmatismus und guten Tools kann man theoretisch selbst große Unternehmen mit ein, zwei Ressourcen überwachen. Allerdings müssen diese exzellent ausgebildet sein und dürfen nicht nebenbei mit Projektarbeiten belastet werden. Und sie müssen ständig hinzulernen wollen und skeptisch hinterfragen.

? **Ulrich Parthier:** *Was sollten Unternehmen also gegen den blinden Fleck tun, was ist Ihre Empfehlung?*

Ralf Kempf: Als Allererstes diesen Pragmatismus mitnehmen: Auf die Unternehmung blicken, ansehen, was wie und wo produziert wird. Anschließend Abhängigkeiten identifizieren, um dann zu hinterfragen, ob es für alle Handlungen definierte Best Practices gibt: für die Konfiguration, den Betrieb, die Überwachung und für ein Notfallfeedback.

Beim Monitoring geht es vor allem darum, die Dinge tatsächlich zu überwachen. Man muss seine Cloud Provider überzeugen, dass sie Logs kostenlos bereitstellen. Die Logs bei Microsoft gab es zum Zeitpunkt des GAUs nur gegen Aufpreis, was natürlich kein Kunde buchte. Sehe ich aber keine Logs, sehe ich auch keinen Angriff. Da kann ich den Schlüssel auch gleich am Marktplatz an die Kirche hängen. Also ist es nur eine Frage gesunden Menschenverstands, warum das schiefgehen muss.

Zyklische Analysen der Schwachstellen sind unverzichtbar. Man muss alle Komponenten in die unternehmensweite Sicherheitsstrategie integrieren. Statt blindem Vertrauen in die Cloud ist man nach wie vor selbst für die Bedrohungs- und Angriffserkennung zuständig und muss die Ressourcen dafür behalten oder beauftragen. Apropos Ressourcen: Denken Sie daran, ausgewiesene Fachleute im Unternehmen zu haben, die das aufbauen, oder vertrauensvolle Partner, mit denen Sie das gemeinsam angehen.

! **Ulrich Parthier:** *Herr Kempf, wir danken für das Gespräch.*

API-Sicherheit neu definiert

MEHR SCHUTZ FÜR KOMPLEXERE INFRASTRUKTUREN

Im Gegensatz zu anderen punktuellen API-Sicherheitslösungen vereinen innovative Plattformen wie beispielsweise die von Cequence Security die Erkennung von APIs, die Inventarisierung, die Einhaltung von Richtlinien und dynamische Tests mit Echtzeit-Erkennung und nativer Prävention zur Abwehr von Betrug, Angriffen auf die Geschäftslogik, Exploits und unbeabsichtigten Datenlecks. Die Unified-API-Protection-Plattform (UAP) genannte Plattform dient der Absicherung von APIs in den heutigen komplexen Infrastrukturen.

Unzureichende API-Sicherheitsmaßnahmen

Warum ist der Einsatz von API-Plattformen überhaupt notwendig? Den API-Business-Logic-Missbrauch, auch definiert als OWASP API10+, eine Erweiterung der OWASP API Top 10, nennt man die Praxis, APIs anzugreifen, um sein bösartiges Endziel zu erreichen. Codierungsfehler wie schwache Authentifizierung, übermäßige Offenlegung von Daten oder die versehentliche Veröffentlichung interner APIs sind bekanntermaßen immer wieder die Hauptursachen für API-Sicherheitsvorfälle. Mit 3,6 Milliarden böswilligen Anfragen, die vom CQ Prime Threat Research Team blockiert wurden, waren diese API10+-Angriffe die zweitgrößte API-Sicherheitsbedrohung, die im ersten Halbjahr 2022 abgewehrt werden konnte. Neuere Zahlen sind aktuell nicht verfügbar, dürften in der Richtung aber eher steil nach oben gehen.

MEHR WERT

Lesen Sie den kompletten Beitrag hier

Understanding the Zero Trust API Security Model

Zahlen, Daten, Fakten

Um das tatsächliche Ausmaß zu erahnen, hier einige Zahlen. Böswillige Anfragen, die auf APIs abzielen, wurden vom CQ Prime Threat Research Team im ersten Halbjahr 2022 wie folgt blockiert:

➤ Über 3 Milliarden Shopping Bots: Shopping Bots zielten auf fehlerhafte APIs mit einem dichten Netz von hochvolumigen und geografisch verteilten Fuzzing-Nutzlasten ab. Diese Angriffe haben oft eine extrem niedrige Erfolgsquote, aber Größenvorteile führen zu einer erhöhten Rendite, wenn das Zielobjekt (etwa Turnschuhe, Luxusgüter, Spielkonsolen) erfolgreich gekauft und dann zu stark überhöhten Preisen weiterverkauft wird.

➤ Über 290 Millionen böswillige Geschenkkarten-Gutscheine: Die Aufzählung von Geschenkkarten basiert auf dem Fuzzing numerischer Muster in APIs, die Zahlungs- und Checkout-Microservices unterstützen. Die Angreifer nutzen billige Cloud-Computing-Ressourcen, die über viele Proxys verteilt sind, um Credential Stuffing-Angriffe auszuführen, die darauf abzielen, kostenlos an Geld zu gelangen. Das Fehlen einer Fehleranalyse bei solchen APIs führt zu einer großen Lücke in der Anwendungssicherheit. Cequence nutzt mehrere Standardfunktionen, um Bedrohungsvektoren und Angriffsnutzlasten im Zusammenhang mit Zahlungsbetrug zu verfolgen.

➤ 37 Millionen Kommentar-Spam-Anfragen: Dieser Satz von Nutzlasten missbraucht APIs, die Workflows für das Kundenbeziehungsmanagement dienen. Spamming und DoS-Aktivitäten in diesen Abläufen führen zu erheblichen Reibungsverlusten bei den Kunden und behindern die Fähigkeit eines Unternehmens, seine Kunden zu bedienen.

Und so gehen Hacker vor!

Das CQ Prime Threat Research Team hat die Vorgehensweisen analysiert und beschreibt die Methodik wie folgt:

Methodischer API-Business-Logik-Missbrauch

Das Team konnte erfolgreich einen Angriff auf eine eCommerce-Plattform entschärfen, der die OWASP API5-Schwachstelle (Broken Function Level Authorization) missbrauchte. Die Angreifer automatisierten den Kauf von Kundenartikeln mit gestohlenen Kreditkarten und PCI-DSS-Daten (Payment Card Industry Data Security Standard). Der Lebenszyklus des API-Missbrauchs-Angriffs sah wie folgt aus:

Scannen der Schwachstellen: Die Angreifer begannen damit, die gesamte Website mit bekannten Tools zum Scannen von Schwachstellen von einer einzigen IP-Adresse aus abzubilden. Dazu

gehörten OWASP API 8-Angriffsverhaltensweisen wie SQL-Injection, Command Injection, Directory Traversal und Fuzzing von sensiblen Daten. Als die grundlegende Aufklärung keinen schnellen Ertrag brachte, ging der Angreifer dazu über, das API-Ökosystem abzubilden.

Angriffssondierungen: Die Angreifer begannen dann, bestehende Angriffskonfigurationen von bekannten Bot-Automatisierungstools wie OpenBullet zu verwenden, um grundlegende Angriffe zum Ausfüllen von Anmeldeformularen und zum Erstellen gefälschter Konten durchzuführen. Während eines Zeitraums von 24 Stunden initiierten die Angreifer mehr als 1,5 Millionen Anfragen von 130.000 IP-Adressen, die alle durch mehr als 1.000 verschiedene Verhaltens-Fingerprints entschärft wurden.

Fortgesetzte Erkundung: Der Angriff wurde, obwohl er entschärft wurde, fortgesetzt. Dabei wurde festgestellt, dass dies eine Täuschung der Angreifer und nicht das eigentliche Ziel war. Bei den folgenden Angriffen kehrte das Erkundungsverhalten zurück, diesmal mit Schwerpunkt auf der Kontoerstellung und den Kassen-APIs.

Entdeckte Schwachstelle: Die Angreifer entdeckten, dass bei der Erstellung eines brandneuen Kontos und vor der E-Mail-Verifizierung die Kassen-APIs (insbesondere die zum Hinzufügen einer Zahlungsmethode) vom Benutzer aufgerufen werden konnten. Dies ist ein Beispiel für eine gebrochene Autorisierung auf Funktionsebene, bei der eine API-Funktion nur von Benutzern verwendet werden soll, die sich sowohl authentifiziert haben als auch autorisiert sind.

Diebstahl: Der Schwerpunkt des Angriffs verlagerte sich auf die Erstellung von Konten und die Angreifer begannen sofort damit, neue (gefälschte) Konten mit gestohlenen Zahlungsinformationen zu füllen, um gezielt Produkte im Einzelhandel zu kaufen. Es war irrelevant, dass ihre Credential Stuffing-Kampagne fehlschlug. Sie überwachten lediglich, welche der neu erstellten Konten erfolgreich auf die Zahlungs-APIs zugreifen konnten, und durchsuchten die gestohlenen Kreditkartendaten iterativ, bis sie eine geeignete für den folgenden Kauf gefunden hatten.

Was ist API-Sicherheit?

API-Sicherheit ist ein entscheidender Aspekt bei der Gewährleistung des Schutzes und der Integrität von Anwendungsprogrammierschnittstellen (APIs) durch die Umsetzung wesentlicher Maßnahmen zur Bekämpfung von Risiken und Schwachstellen, die zu Datenschutzverletzungen, betrügerischen Aktivitäten und Betriebsunterbrechungen führen könnten.

Um eine optimale API-Sicherheit zu erreichen, müssen drei Grundprinzipien beachtet werden: API-Erkennung, Risiko- und Konformitätsanalyse sowie Be-

hebung und Minderung von Bedrohungen. Zu den Schlüsselkonzepten der API-Sicherheit gehören eine sichere API-Verwaltung, Datensicherheit und der Schutz sensibler Informationen.

#1 Der erste Schritt bei der API-Sicherheit umfasst die Identifizierung und Katalogisierung aller APIs, einschließlich verwalteter, nicht verwalteter, Schatten-, Zombie-, Drittanbieter-, interner und externer APIs. Dieser Prozess gewährleistet eine ordnungsgemäße Zugriffsverwaltung, die Einhaltung der OWASP-API-Sicherheitsrichtlinien sowie die allgemeine Netzwerk- und Anwendungssicherheit.

#2 In der zweiten Phase, der API-Sicherheitsrisikoanalyse, liegt der Schwerpunkt auf der Identifizierung von Codierungsfehlern, die Schwachstellen aufdecken können (API-Risiken), und gezielten Angriffen, die diese Schwachstellen ausnutzen oder versuchen könnten, die Geschäftslogik zu manipulieren (API-Bedrohungen). Die Erkennung von Angriffen und Bedrohungen erfordert eine umfassendere Analyse, die menschliche Eingriffe, digitale Tools oder eine Kombination aus beidem beinhalten kann.

#3 Der dritte Aspekt der API-Sicherheit umfasst die Erkennung und Beseitigung von Risiken und die Eindämmung von Bedrohungen, die in der Erkennungsphase festgestellt wurden. Die Risikobeseitigung umfasst die Benachrichtigung des Entwicklungsteams über die erkannten Risiken und die Bestätigung der implementierten Korrekturen durch kontinuierliche Analysen, Tests und Cybersicherheitsmaßnahmen. Native Bedrohungsabwehr erfordert Echtzeit-Reaktionen, ohne sich ausschließlich auf die Signalisierung einer Web Application Firewall (WAF) oder den Einsatz anderer Tools zu verlassen. Die Implementierung von Authentifizierungsprotokollen, die Absicherung von Cloud-basierten Anwendungen und die Einhaltung strenger Anwendungssicherheitsstandards sind unerlässlich, um unbefugten Zugriff zu verhindern und den Schutz sensibler Daten zu gewährleisten.

API-Sicherheit ist entscheidend für den Schutz von APIs vor potenziellen Bedrohungen und Schwachstellen, für die Gewährleistung der Datensicherheit und den Schutz sensibler Informationen. Durch die Befolgung der drei oben genannten grundlegenden Prinzipien können Unternehmen eine sichere Umgebung für ihre APIs, Anwendungen und Netzwerke schaffen.

Ulrich Parthier

TYPEN DER API-SICHERHEIT

Zu den verfügbaren Arten von API-Sicherheitslösungen gehören API-Gateways, Web Application Firewalls (WAF), API-spezifische Sicherheitstools und Unified API Protection. Es ist von entscheidender Bedeutung zu verstehen, wie jedes dieser Tools die API-Sicherheitsanforderungen eines Unternehmens erfüllt. Diese Anforderungen umfassen in der Regel die Erkennung von APIs, die Identifikation von Bedrohungen und Risiken sowie die nachfolgende Schadensbegrenzung und Behebung.

- API-Gateways: Sie sind für die die Zusammenführung und Verwaltung von APIs konzipiert. API-Gateways verfügen über grundlegende Sicherheitsfunktionen wie Ratenbegrenzung und IP-Sperrlisten. Sie sind nicht in der Lage, APIs proaktiv zu erkennen und führen keine Bedrohungserkennung, Risikoanalyse, Abhilfe oder Schadensbegrenzung durch.

- Web Application Firewalls (WAF): WAFs konzentrieren sich auf das Web und führen keine automatische API-Erkennung durch oder decken Codierungsfehler auf. Sie verwenden Signaturen, um bekannte Schwachstellen zu erkennen, die in der OWASP Web Application Top 10 Threats Liste aufgeführt sind.

- API-spezifische Toolsets: Sie konzentrieren sich darauf, die Entwicklung von APIs mit weniger Fehlern zu unterstützen. Diese Tools sind nicht in der Lage, die oben definierten Anforderungen an die API-Sicherheit vollständig zu erfüllen. Die umfassendste Art der API-Sicherheit ist eine einheitliche API-Schutzlösung, die die Erkennung von APIs, von Bedrohungen und Risiken und die anschließende Schadensbegrenzung und -behebung umfasst.

PASSWORT MANAGEMENT

LÖSUNGEN IM ÜBERBLICK

Es gibt verschiedene Passwort-Management-Lösungen, die Benutzern eine sichere und bequeme Verwaltung ihrer Passwörter ermöglichen. Im Folgenden präsentieren wir zehn dieser Lösungen, von denen jede ihre eigenen Stärken hat. Zu jedem Tool stellen wir ein Alleinstellungsmerkmal (USP, Unique Selling Proposition) vor.

LastPass: Ein Passwort-Manager, der Browser-Erweiterungen sowie Apps für alle wichtigen Plattformen bietet. LastPass speichert Passwörter in einem verschlüsselten Tresor und generiert sichere Passwörter.
USP: Notfallzugriffsfunktion

1Password: Bekannt für starke Sicherheit und Benutzerfreundlichkeit. 1Password bietet eine Vielzahl von Funktionen, einschließlich der Möglichkeit, sichere Notizen und Kreditkarteninformationen zu speichern.
USP: Travel Mode

Dashlane: Bietet neben der Passwortverwaltung auch Funktionen zur Identitätsüberwachung, zum sicheren Teilen von Informationen und ist für seine benutzerfreundliche Oberfläche bekannt.
USP: Identitätsüberwachung

Bitwarden: Eine Open-Source-Passwort-Management-Lösung, die großartige Sicherheit zu einem günstigen Preis bietet.
USP: Eigener Server für zusätzliche Kontrolle und Transparenz

Keeper: Bietet eine sichere Passwortverwaltung.
USP: Digitaler Tresor

NordPass: Das Tool bietet eine einfache und sichere Möglichkeit zur Passwortverwaltung und unterstützt auch die Zwei-Faktor-Authentifizierung.
USP: Eingebauten OCR-Scanner

RoboForm: Ein weiterer etablierter Passwort-Manager.
USP: Fortschrittlichen Funktionen für das automatische Ausfüllen von Online-Formularen

KeePass: Eine kostenlose und Open-Source-Option, die etwas mehr technisches Know-how erfordert, aber sehr flexibel und anpassbar ist.
USP: kann ohne Installation direkt von einem USB-Stick ausgeführt werden,

Password Safe/Workforce Passwords: BeyondTrust hat mit Workforce Passwords eine neue Funktionalität in BeyondTrust Password Safe integriert. Das Feature bietet eine professionelle Passwortverwaltung für Mitarbeiter im Unternehmen und gibt Anwendern damit die Möglichkeit, Passwörter für Geschäftsanwendungen auf dem gleichen Kontroll- und Sicherheitsniveau wie bei privilegierten Konten zu verwalten.
USP: Komfortabler Passwortmanager für Privatanwender mit Sicherheits- und Skalierbarkeitsfunktionen für den Unternehmenseinsatz

Ulrich Parthier

Fein-granulare Autorisierung

WARUM DER HYPE?

Fein-granulare Autorisierung ist ein aktuelles Thema im Identity Management, neben „Self-Sovereign Identity" und der EU-Verordnung eIDAS 2.0. Besonders das 2019 von Google präsentierte „Zanzibar"-Konzept für ein globales Autorisierungssystem hat Aufmerksamkeit erregt. Die Idee, nicht nur Identifikation und Authentisierung, sondern auch Autorisierung zu zentralisieren, ist nicht neu, wie der XACML-Standard der OASIS aus den frühen 2000er Jahren zeigt. Dennoch hat sich das Konzept der feingranularen Autorisierung bisher nicht vollständig durchgesetzt.

Altlasten und Beweggründe

Zwar waren die Gründe für den ausbleibenden Erfolg vielfältig - dennoch gilt XACML nicht als „vollkommen gescheitert". Die komplexe Umsetzung in reale Produkte und die mangelnde Agilität der Software-Entwicklung haben die Adaption erschwert. Viele Unternehmen scheuten den Aufwand des Refactorings, um ihre Bestands-Software auf das neue Paradigma umzustellen. Im Jahr 2023 existieren daher immer noch Anwendungen mit interner Benutzerverwaltung, während Microsoft mittlerweile veraltete Technologien wie NTLM aus seinen Produkten entfernt. Die Migration etablierter On-Premises Anwendungen in die Cloud zwingt Unternehmen, alte Strukturen zu überdenken und den Mehrwert moderner Sicherheitsverfahren zu bewerten, wobei die Benutzer- und Rechteverwaltung eine entscheidende Rolle spielt.

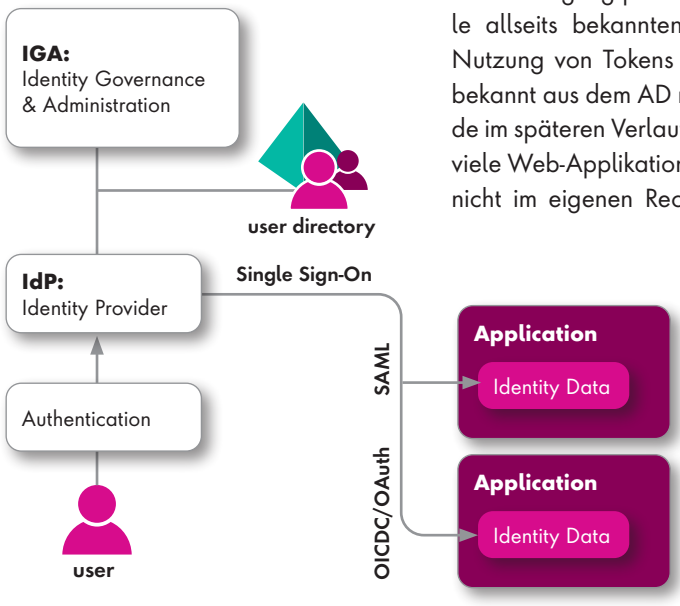


Bild 1: Auslagerung von Benutzerinformationen in einen IdP

Bisherige Entwicklung

In den 2000er Jahren führte der Aufstieg von Web-Anwendungen und der Rückgang der Three-Tier-Applikationsarchitektur zu einem Wildwuchs von Benutzerkonten und Passwörtern in Web-Apps. Unternehmen setzten auf Web-SSO-Systeme, um dem entgegenzuwirken. Allerdings führten unschöne Begleiterscheinungen wie das Scraping von Credentials und die unverschlüsselte Übertragung per HTTP zu mittlerweile allseits bekannten Problemen. Die Nutzung von Tokens statt Credentials, bekannt aus dem AD mit Kerberos, wurde im späteren Verlauf bevorzugt. Doch viele Web-Applikationen befanden sich nicht im eigenen Rechenzentrum oder „line of sight" zum AD-Controller, weshalb Kerberos keine Option war. Das weit unterstützte SAML-Protokoll etablierte sich als Lösung für die Föderation, besonders durch die Adaption von SAML 2.0 im Microsoft Active Directory Federation Server 2.0. Seither erfreute sich SAML 2.0 großer Beliebtheit für Web-Anwendungen, stößt jedoch mit dem Aufkommen mobiler Geräte und Apps an seine Grenzen: Die Verwendung von Cookies und die hohen Ressourcenanforderungen des Protokolls erschwerten die mobile Nutzung.

Ja/Nein Entscheidung

Das SAML-Protokoll ermöglicht zwar die Ersetzung lokaler Anmeldungen durch die Anmeldung an einem eigenen Identity Provider (IdP), wodurch nur Token, nicht jedoch Kennwörter, an die Anwendung übertragen werden. Jedoch fehlt SAML die Möglichkeit, fein abgestufte Berechtigungen jenseits des einfachen „Ja/Nein" zum Zugriff zu verwalten. SAML-basierte Föderationen dienen heutzutage häufig als Gatekeeper, können jedoch komplexe Berechtigungsabfragen nur umständlich abbilden.

Die Herausforderungen von Mobil-Apps wurden durch Protokolle wie OAuth 2.0 und Open ID Connect (OIDC) angegangen, die auch die lästige wiederholte Registrierung bei neuen Diensten entschärfen. Die flexiblere Nutzung über verschiedene Flows ist ein weiterer Vorteil dieser Protokolle.

Identifikation – Authentisierung – Autorisierung?

Die Zentralisierung von Benutzeridentifikation und Authentifizierung durch einen IdP gilt als gelöst, dank passender

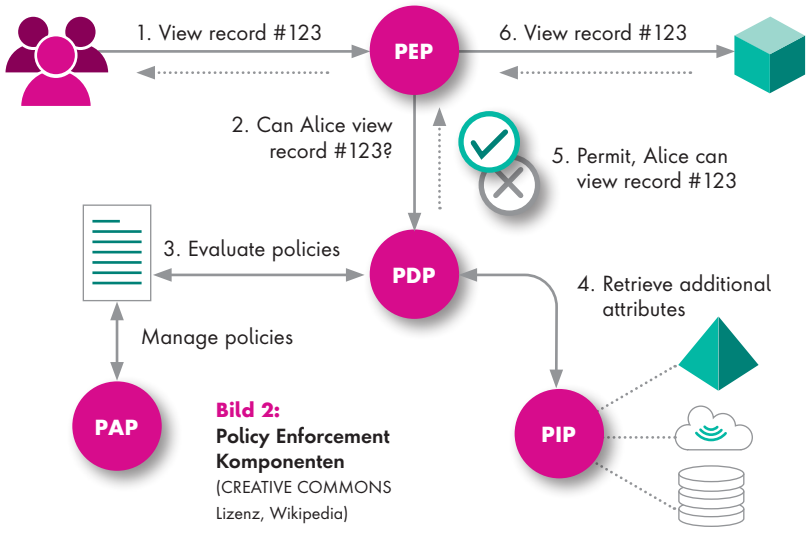


Bild 2: **Policy Enforcement Komponenten** (CREATIVE COMMONS Lizenz, Wikipedia)

Lösungen wie OAuth und SAML – inklusive kommerzieller und kostengünstiger Open-Source-Lösungen am Markt. Für die zentrale Autorisierung stehen neue Technologien zur Verfügung, die nachfolgend behandelt werden. Vom bekannten Role Based Access Control (RBAC) haben sich im Laufe der Zeit Varianten wie Attribute-based (ABAC) und Context-based Access Control (CBAC) entwickelt, wie sie im „Conditional Access" in Microsofts Azure Cloud zum Einsatz kommen. Hierbei sind nicht nur die Rollen, sondern auch Eigenschaften und der aktive Kontext relevant (mehr dazu später).

Um diesen Kontext und die Eigenschaften dynamisch in Zugriffsentscheidungen einzubeziehen, benötigen wir eine angepasste Applikations-Architektur und Infrastruktur. Diese lassen sich am besten herleiten, wenn die Komponenten nach einer bekannten Nomenklatur benannt und deren Eigenschaften beschrieben werden. Hierfür haben sich die folgenden Begriffe etabliert:

PEP – Policy Enforcement Point: Die Komponente, welche eine Zugriffsentscheidung schlussendlich umsetzt. In der Regel ist dies eine Anwendung.

PDP – Policy Decision Point: Fällt anhand von Regeln und Kontext-Informationen Zugriffsentscheidungen für den Enforcement Point

PAP – Policy Administration Point: Zentrale Management-Komponente zur Verwaltung von Policies und Monitoring von Entscheidungen des PDPs

PIP – Policy Information Point: Stellt bei Bedarf einem PDP zusätzliche (Meta-) Daten über Benutzer und Ressourcen zur Verfügung

In klassischen monolithischen Anwendungen sind Benutzerkonten, Passwörter und Berechtigungen lokal in der Anwendung verankert, was zu Redundanzen und ineffizienter Berechtigungsverwaltung führt. Ein moderner Ansatz beginnt mit der Auslagerung der Benutzerverwaltung und der Einführung von Single Sign-On (SSO). Hierdurch wird der gesamte Login-Prozess an einen externen Identity-Provider ausgelagert. Der Anpassungsaufwand hierfür ist meist überschaubar und lässt sich durch externe Module im Webserver oder vorgelagerten Reverse-Proxy verhältnismäßig einfach umsetzen.

In der zweiten Stufe kann die Berechtigungssteuerung derart angepasst werden, dass Zugriffsentscheidungen anhand benutzerbezogener Eigenschaften getroffen werden. Durch SSO liefert der Identity-Provider diese Benutzer-Attribute einheitlich beim Login gleich mit, wodurch die Zugriffssteuerung optimiert werden kann. Die wesentlichen Vorteile sind eine zentralisierte und einheitliche Verwaltung relevanter Benutzereigenschaften sowie eine effiziente Bereitstellung per SSO.

Eine feingranulare Zugriffssteuerung ist trotz SAML und OpenID Connect (OIDC) damit nur eingeschränkt möglich, denn die Fähigkeiten beider Protokolle sind begrenzt:

SSO kann nur begrenzte Benutzerdaten just-in-time übermitteln, da der Platz für SAML/OIDC-Tokens durch das HTTP-Protokoll limitiert ist und in der Praxis wenige kB nicht überschreiten sollte. In realen Umgebungen ist es hingegen üblich, dass ein Benutzer zum Beispiel in vielen Gruppen Mitglied ist.

SSO behandelt nur Identitätsdaten; die Entscheidung über Benutzeraktionen und -berechtigungen liegt weiterhin in der Anwendung. Mit SSO wird nur die Authentisierung ausgelagert, nicht jedoch die Autorisierung, die oft durch Programmlogik innerhalb der Anwendung erfolgt (wie exemplarisch in Listing 1 dargestellt).

LISTING 1

```
def perform_create(self, request, instance):
    group = request.user.group
    if group == "member" or group == "admin":
        instance.save()
    else:
       return HttpResponse("Unauthorized", status=401)
```

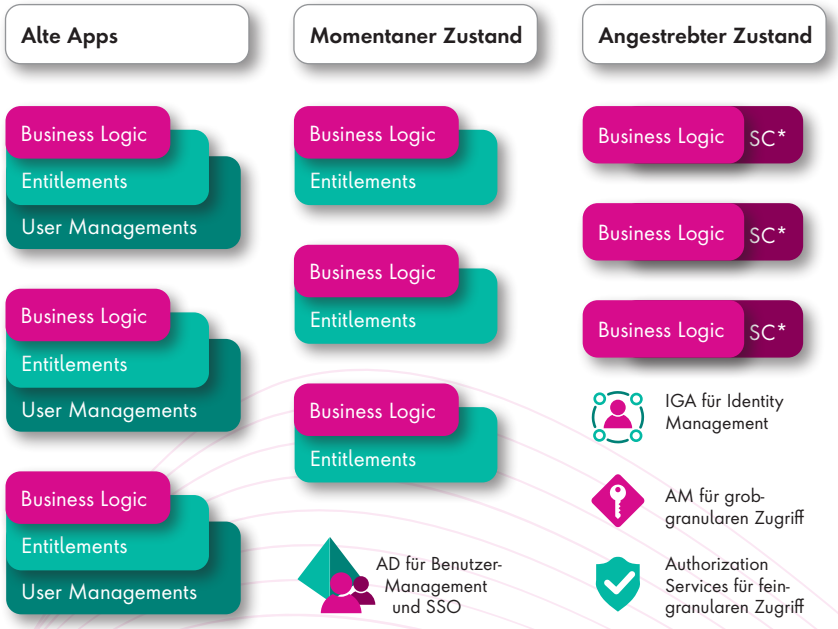


Bild 3: Evolutionsstufen der Auslagerung von Anwendungskomponenten

Softwareentwickler verwenden in realen Projekten oft flexibleren Code für Zugriffsentscheidungen. Die relevante Logik bleibt jedoch im Programmcode verborgen, schwer zu warten und intransparent. Um den Trend zur Auslagerung und Zentralisierung fortzusetzen, sollte demnach nur noch die reine Business-Logik in der Applikation verbleiben, während eine externe und technologisch standardisierte Komponente die Zugriffsentscheidungen aufgrund zentral definierter Policies trifft.

In einem Gesamtschaubild könnte eine mögliche Architektur dann wie rechts abgebildet aussehen.

Eine Herausforderung – viele Lösungsansätze

Bei der Suche nach Umsetzungsoptionen für Zugriffssteuerung kann die Vielzahl neuer Ansätze schnell überwältigend sein. Ein bekannter Vertreter ist der Open Policy Agent (OPA). Dieses Open-Source-Projekt erfreut sich in der Entwickler-Community großer Beliebtheit. OPA nutzt die eigene Beschreibungssprache REGO, um klare Policies für Zugriffsentscheidungen zu formulieren. Damit ist OPA eine Implementierungsoption für den PDP, die sich zudem verhältnismäßig einfach in neue Softwareprojekte einbinden lässt.

Da Softwareentwicklung heute primär für die Cloud in der Cloud stattfindet und Anbieter wie AWS ein umfangreiches Tooling für CI/CD Pipelines und deren Automation anbieten, überrascht es kaum, dass mit CEDAR auch eine Beschreibungssprache von AWS um Aufmerksamkeit buhlt.

Eine Reihe von weiteren Anbietern wie Aserto, Sgnl und Co. nutzen intern den OPA als generische Komponente, um darauf aufbauend umfassendere Dienste und Funktionen anbieten zu können, während andere wie PlainID eigene Implementierungen bevorzugen.

Viele Lösungsansätze – eine abstrakte Lösung

Diese Ansätze verfolgen das Ziel, effiziente, wiederverwendbare und sichere Policies zur Autorisierung zu formulieren und diese zur Laufzeit der Anwendung performant auszuwerten. Im Gegensatz zur Authentisierungsschicht, die sich auf die Identität des Benutzers konzentriert, berücksichtigen Zugriffsentscheidungen in der Regel drei Aspekte:

- ein Subjekt (wer): Der agierende Benutzer, welcher eine Aktion ausführen möchte,
- eine Aktion, zum Beispiel „bearbeiten" oder „löschen",

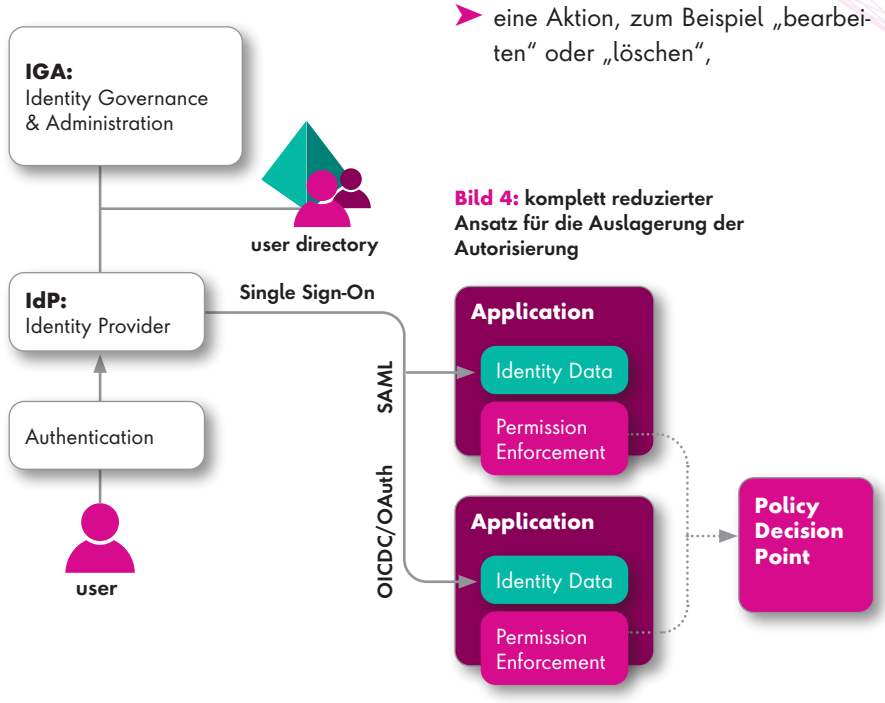


Bild 4: komplett reduzierter Ansatz für die Auslagerung der Autorisierung

- eine Ressource, auf welcher die Aktion ausgeführt werden soll, etwa ein Dokument oder eine Datei

Diese „Triplets" aus SUBJEKT, AKTION und RESOURCE werden in Policies verwendet, um die Anforderungen für gewährte oder verweigerte Zugriffe zu formulieren. Eine Beispiel-Policy könnte besagen, dass „eine Ressource nur gelöscht werden darf, wenn das Subjekt sich per MFA angemeldet hat und entweder Mitglied in der Gruppe „admin" ist ODER Eigentümer der Ressource".

Listing 2 zeigt, wie solch eine Policy am Beispiel von REGO mit dem Open Policy Agent umgesetzt werden könnte:

LISTING 2

```
1  authz.check_permission
2  default allow := false
3  allowed_groups := ["admin", "member"] # required user groups
4  # check if user has required group
5  group_permitted if {
6        user_group := input.group
7        user_group in allowed_groups
8  }
9  resource_owner if {
10       input.resource.owner == input.user
11 }
12 # check if user has MFA enabled
13 mfa_enabled if {
14       input.mfa == true
15 }
16 # allow if: mfa-enabled AND user in permitted group
17 allow if {
18       mfa_enabled == true
19       input.action == "delete"
20       group_permitted == true
21 }
22 # OR allow if: mfa-enabled AND user is resource owner
23 allow if {
24       mfa_enabled == true
25       input.action == "delete"
26       resource_owner == true
27 }
```

Standardmäßig wird Zugriff verweigert (Zeile 2 als Default-Wert). In den folgenden Zeilen werden Teil-Policies geprüft: Ist das Subjekt in bekannter Gruppe (Zeile 4-8), bzw. ist es Ressourceneigentümer (Zeile 9-11) oder per MFA authentifiziert (Zeile 12-15). Das Herzstück der Policy sind die Bedingungen in den darauffolgenden Blöcken (Zeile 16-27), die die Anforderungen kombinieren und nur bei Erfüllung „true" für das Policy-Ergebnis „allow" zurückgeben.

Mit einer solchen Policy kann eine Anwendung alle Autorisierungsentscheidungen an einen externen PDP wie den Open Policy Agent auslagern. Die Anwendung muss nur den Kontext mitliefern: Subjekt, Ressource und Aktion. Die Entscheidung des PDP („allow") wird von der Anwendung ausgewertet und umgesetzt. Das Beispiel zeigt die Grundprinzipien, ohne fortgeschrittene Techniken wie wiederverwendbare Sub-Policies oder externe Datenbankintegration als Policy Information Service (PIP). Dennoch demonstriert es die Stärke des Ansatzes:

- Zugriffsregeln werden in einer universellen Beschreibungssprache formuliert und im zentralen Policy-Register gesammelt.
- Policies können einen gemanagten Review- und Freigabeprozess durchlaufen.
- Die Entscheidungslogik wird an einen PDP delegiert, der Auswertung und Protokollierung vereinheitlicht.
- Feingranulares Zugriffsmanagement kann konsistent über die gesamte Applikationslandschaft realisiert werden, dank einer universellen Beschreibungssprache, und unabhängig von der Programmierumgebung der jeweiligen Anwendung.

Fazit

Das Thema feingranulare Autorisierung ist für alle Unternehmen mit eigenen Projekten in der Softwareentwicklung ein relevanter Agendapunkt für den Austausch zwischen CTO, CIO und der Anwendungsentwicklung. Gerade bei agilen Entwicklungsprojekten und einem dynamischen Umfeld in der IT sollte über eine weitergehende Zentralisierung des Access Management und eine Ergänzung um Authorization Services nachgedacht werden. Für lediglich „konsumierende" IT-Abteilungen mit vornehmlich SaaS-basierten externen Services kann FGA zwar interessant sein, allerdings wird die Anwendung hier eher auf Attribut- und Kontext-bezogene Policy-Erweiterung für einfache „JA/NEIN" Entscheidungen limitiert, da eine direkte Anpassung der Applikationslogik häufig nicht möglich ist.

Sebastian Rohr, Roland Baum
https://www.umbrella.associates/

Kritischer Blick gefragt

DIE WAHRHEIT HINTER DEN WERBEVERSPRECHEN VON VPN-ANBIETERN

Brisante Enthüllungen von Insidern, unter anderem von Edward Snowden, und regelmäßige Datenskandale haben das Bewusstsein für Datenschutz geschärft. Viele Menschen wenden sich an VPNs (Virtual Private Networks) in der Hoffnung, ihre Online-Privatsphäre zu schützen. Doch wie realistisch ist das Versprechen der Anonymität durch VPNs?

Die VPN-Anbieter, die mit „100prozentiger Anonymität" werben, zeigen, dass diese Versprechen oft mehr Marketing als Realität sind. Die meisten VPNs bieten zwar einen gewissen Grad an Privatsphäre, aber echte Anonymität ist schwer zu erreichen.

Technische Grenzen der Anonymität durch VPNs

- **IP-Adresse:** Ein VPN verbirgt zwar Ihre IP-Adresse, aber das ist nur ein Aspekt der Online-Identifikation. Fortgeschrittene Tracking-Methoden nutzen Cookies, Browser-Add-ons, Bildschirmauflösung und Spracheinstellungen im Browser, um Nutzer zu identifizieren.
- **Menschliches Verhalten:** Die meisten Menschen nutzen denselben Browser für verschiedene Online-Aktivitäten, was das Tracking erleichtert. Ohne zusätzliche Maßnahmen wie spezielle Browser-Add-ons bleibt man anfällig für Tracking.
- **Rechtliche Aspekte:** Die Datenschutzbestimmungen vieler VPN-Anbieter offenbaren, dass sie bestimmte Daten speichern und unter Umständen an Behörden weitergeben müssen. Dies steht im Widerspruch zur Idee der Anonymität.

Sinnvolle Einsatzszenarien für VPNs

Trotz der Einschränkungen sind VPNs nützlich für bestimmte Anwendungen:

- Anbindung externer Mitarbeiter an Firmennetzwerke
- Umgehung von Geo-Sperren
- Schutz in öffentlichen WLANs

Fazit

VPNs sind zweifellos wertvolle Instrumente zur Verbesserung von Privatsphäre und Sicherheit im Internet. Dennoch sollten Nutzer sich bewusst sein, dass VPNs keine Allzwecklösung für Online-Anonymität darstellen. Obwohl sie vor bestimmten Überwachsungs- und Tracking-Methoden schützen, können sie nicht sämtliche Formen des Online-Trackings verhindern.

Es ist entscheidend zu erkennen, dass viele VPN-Anbieter Mängel in Transparenz und Ehrlichkeit aufweisen. Einige nutzen die Ängste der Nutzer aus, um Dienstleistungen zu verkaufen, die möglicherweise nicht die vollständige Wahrung der Anonymität einhalten können. Während VPNs die Privatsphäre verbessern können, bieten sie keine absolute Anonymität. Nutzer sollten sich der Grenzen bewusst sein und nicht blind den Werbeversprechen glauben.

Um ein umfassende Datensicherheit beim Surfen im Internet zu gewährleiste4n, sind zusätzliche Maßnahmen und ein kritisches Bewusstsein unerlässlich. Es empfiehlt sich, VPNs als Teil eines breiteren Datenschutzansatzes zu betrachten und nicht als alleinige Lösung für Online-Anonymität.

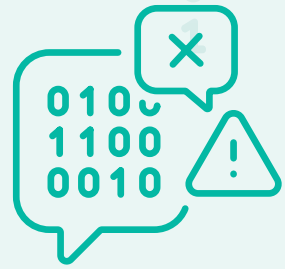
Ulrich Parthier

FUNKTIONSWEISE VON VPNS

Ein VPN (Virtual Private Network) ist ein Dienst, der eine sichere und verschlüsselte Verbindung über ein weniger sicheres Netzwerk, typischerweise das Internet, bereitstellt. Die Funktionsweise eines VPNs lässt sich in mehreren Schritten erklären:

1. **VPN-Client auf dem Gerät**
   Zunächst installieren Sie eine VPN-Software (den VPN-Client) auf Ihrem Gerät (Computer, Smartphone, Tablet). Dieser Client ist verantwortlich für die Herstellung der Verbindung zum VPN-Server.
2. **Herstellung der Verbindung**
   Wenn Sie das VPN aktivieren, stellt der VPN-Client eine Verbindung zu einem VPN-Server her. Dies geschieht in der Regel über das Internet. Der Client authentifiziert sich beim Server, oft mittels Benutzername und Passwort oder anderen Authentifizierungsmethoden.
3. **Verschlüsselung des Datenverkehrs**
   Sobald die Verbindung hergestellt ist, verschlüsselt der VPN-Client alle Daten, die von Ihrem Gerät gesendet werden, bevor sie über das Internet übertragen werden. Diese Verschlüsselung schützt Ihre Daten vor Dritten, die versuchen könnten, Ihre Daten abzufangen und zu lesen.
4. **Datenübertragung über den VPN-Server**
   Die verschlüsselten Daten werden zum VPN-Server gesendet. Dort werden sie entschlüsselt und dann zum ursprünglichen Ziel im Internet weitergeleitet, sei es eine Website, ein Online-Dienst oder ein anderes Netzwerk.
5. **Antwort vom Internet**
   Die Antwort vom Internet (etwa die angeforderte Webseite) wird zuerst an den VPN-Server gesendet. Der Server verschlüsselt die Antwort und sendet sie zurück an Ihren VPN-Client.
6. **Entschlüsselung auf Ihrem Gerät**
   Der VPN-Client auf Ihrem Gerät entschlüsselt die empfangenen Daten und präsentiert sie Ihnen in ihrer ursprünglichen Form. Für Sie als Nutzer scheint es, als ob Sie direkt mit dem Internet verbunden wären, obwohl der gesamte Datenverkehr über den VPN-Server geleitet wird.

ZUSÄTZLICHE FUNKTIONEN



➤ **IP-Adressmaskierung:** Der VPN-Server verbirgt Ihre tatsächliche IP-Adresse und ersetzt sie durch seine eigene. Dies macht es für Websites und Dienste schwierig, Ihren tatsächlichen Standort und Ihre Identität zu ermitteln.

➤ **Umgehung von Geo-Restriktionen:** Da Sie eine IP-Adresse des VPN-Servers verwenden, können Sie auf Inhalte zugreifen, die in Ihrem Land möglicherweise blockiert sind.

➤ **Sicherheit in öffentlichen Netzwerken:** Ein VPN bietet zusätzlichen Schutz in unsicheren Netzwerken, wie etwa öffentlichen WLANs, indem es Ihren Datenverkehr verschlüsselt.

Wichtig zu beachten

➤ **VPN-Protokolle:** Verschiedene VPNs verwenden unterschiedliche Protokolle (wie OpenVPN, WireGuard, IKEv2), die bestimmen, wie Daten verschlüsselt und übertragen werden.

➤ **Vertrauenswürdigkeit des Anbieters:** Da der VPN-Anbieter potenziell Zugriff auf Ihren Datenverkehr hat, ist es wichtig, einen vertrauenswürdigen Anbieter zu wählen.

FAKTEN UND MISSVERSTÄNDNISSE

Fakten über VPNs

- **Verschlüsselung des Datenverkehrs:** VPNs verschlüsseln Ihren Internetverkehr, was bedeutet, dass Dritte wie Ihr Internetanbieter oder Wi-Fi-Betreiber nicht sehen können, was Sie online tun.
- **IP-Adresse verbergen:** Ein VPN verbirgt Ihre tatsächliche IP-Adresse und ersetzt sie durch die IP-Adresse des VPN-Servers. Dies erschwert es, Ihre Online-Aktivitäten direkt zu Ihnen zurückzuverfolgen.
- **Umgehung von Geo-Sperren:** VPNs ermöglichen es Ihnen, Inhalte zu sehen, die in Ihrem Land möglicherweise blockiert sind, indem sie den Anschein erwecken, als ob Sie von einem anderen Standort aus zugreifen.
- **Schutz in öffentlichen Netzwerken:** In öffentlichen WLAN-Netzwerken bieten VPNs Schutz vor Schnüfflern und Hackern.

Missverständnisse im Zusammenhang mit VPNs

- **Vollständige Anonymität:** VPNs verbergen zwar Ihre IP-Adresse, aber sie können nicht alle Formen des Trackings verhindern. Fortgeschrittene Tracking-Methoden wie Fingerabdrücke des Browsers oder Cookies können weiterhin Informationen über Ihre Online-Aktivitäten sammeln.
- **VPN-Anbieter-Protokollierung:** Nicht alle VPN-Anbieter haben eine strikte No-Log-Politik. Einige können Nutzungsdaten speichern, was potenziell Ihre Privatsphäre gefährden könnte.
- **Rechtliche und technische Grenzen:** VPNs unterliegen den Gesetzen des Landes, in dem sie ansässig sind. In einigen Fällen können sie rechtlich verpflichtet sein, Nutzerdaten an Behörden weiterzugeben.
- **Falsches Sicherheitsgefühl:** Die Nutzung eines VPNs allein macht Ihre Online-Aktivitäten nicht immun gegen Sicherheitsrisiken. Phishing-Angriffe, Malware und andere Bedrohungen bleiben bestehen.
- **VPN-Verbindungsabbrüche:** Gelegentlich können VPN-Verbindungen abbrechen. In solchen Fällen könnte Ihr Internetverkehr kurzzeitig ungeschützt sein, es sei denn, das VPN bietet eine Kill-Switch-Funktion.

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)

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

Autoren:
Roland Baum, Fabian Glöser, Ralf Kempf,
Carina Mitzschke, Silvia Parthier,
Ulrich Parthier, Sebastian Rohr, André Schindler,
Stephan Schweizer, Guido Simon, Neil Thacker

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. 31.
Preisliste gültig ab 1. Oktober 2023.

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

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.

Cyberkriminelle überall

da tut Hilfe not

Mehr Infos dazu im Printmagazin

itsecurity

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

Excellence in
Digital Security.

genua.

Schützen Sie Ihre IT- und OT-Netzwerke - Secure by Design -

BSI-zertifizierte IT-Sicherheit für Ihre digitale Souveränität

- Vertrauenswürdige VPNs
- Hochsichere Firewalls
- Intelligente Angriffserkennung
- Sichere Fernwartung
- Robuste Datendioden

Erfahren Sie mehr unter
genua.de

SecurITy made in Germany

Teil der Bundesdruckerei-Gruppe

bdr