it management

Der Motor für Innovation
Mai/Juni 2023

INKLUSIVE 48 SEITEN
it security

MONTE CARLO-ANALYSEN

Innovation durch Simulation

MODERNE DATA WAREHOUSES

Preis, Leistung & Funktionen

THOUGHT LEADERSHIP

AB SEITE 14
PAESSLER
THE MONITORING EXPERTS

AB SEITE 18
BLACKLINE

SAP-TRANSFORMATION

Aufräumen, ordnen und ausmisten

Patric Dahse, Natuvion GmbH

www.it-daily.net

SNP TRANSFORMATION WORLD

EXPLORE NEW HORIZONS!

Seien Sie Teil einer der größten SAP-Partner-Veranstaltungen in Europa. Ein Muss für Unternehmen, die Daten neu denken und ihr Potential maximal nutzen wollen.

Unsere Experten, Partner und Kunden freuen sich auf zwei Tage intensiven Wissens- und Best-Practice-Austausch mit Ihnen. Sie präsentieren zukunftsweisende Lösungen, erfolgreiche Transformationsprojekte und die Möglichkeiten, die moderne Systeme und innovative Datennutzung Ihrem Unternehmen bieten.

JETZT ANMELDEN

14.-15. Juni 2023
SNP dome Heidelberg

EXPLORE NEW HORIZONS

UNSERE SPONSOREN

IBM
FUJITSU
all for one Group
accenture
Scheer
TCS TATA CONSULTANCY SERVICES
pwc
T Systems
delaware
smartShift TECHNOLOGIES
exa AG

IT-ARCHITEKTURMANAGEMENT IM WANDEL

LIEBE LESERINNEN UND LESER,

das IT-Architekturmanagement hat in den letzten Jahren bedeutende Veränderungen durchgemacht. Mit der rasanten Entwicklung neuer Technologien wie etwa dem Cloud Computing, Microservices, DevOps, und innovativer Geschäftsmodelle müssen Unternehmen ihre IT-Systeme anpassen, um wettbewerbsfähig zu bleiben. Die IT-Architektur spielt hierbei eine entscheidende Rolle. Die durch Pandemie und Krieg beschleunigte Dynamik und die veränderte Rolle der Fachbereiche, haben dazu beigetragen.

Heute geht es um viel mehr als nur um Technologie. IT-Architekturmanagement ist ein integrierter Teil des Geschäftsstrategieprozesses und muss die Anforderungen aller Bereiche eines Unternehmens berücksichtigen, einschließlich Geschäftsentwicklung, Finanzen, Kundenerfahrung und Datensicherheit.

Eine weitere Herausforderung ist die Verwaltung der immens steigenden Daten. IT-Architekten müssen sicherstellen, dass die Datensicherheit und -integrität gewahrt bleiben. Darüber hinaus müssen die Daten effektiv genutzt werden, um bessere Geschäftsergebnisse zu erzielen. Außerdem ist die IT-Sicherheit generell ist zu einem zentralen Thema für die IT in den Unternehmen geworden und das muss natürlich auch in Architekturkonzepten seinen Niederschlag finden.

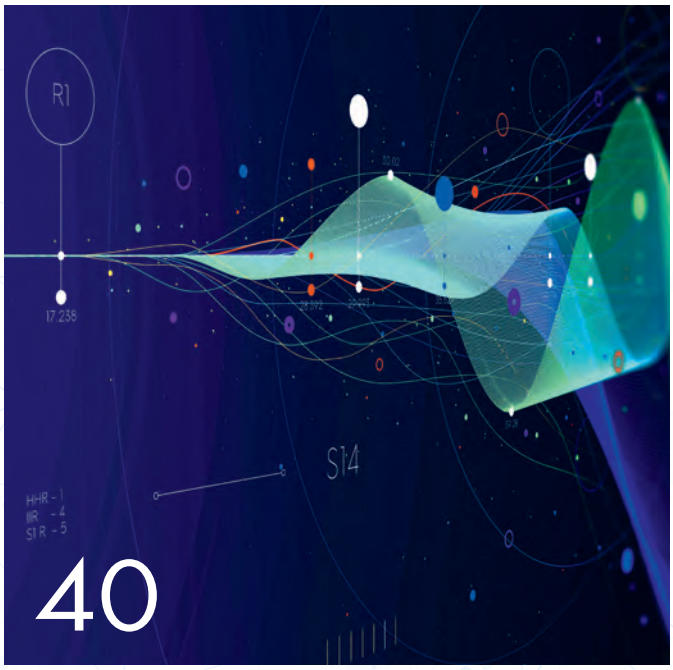
Fazit: es geht nicht mehr nur um die Organisation von Systemen, sondern um die Fähigkeit, Geschäftsanforderungen in die IT-Systeme einzubetten und sie flexibel genug zu gestalten, um sich an Veränderungen anzupassen. Unternehmen, die ihre IT-Architektur erfolgreich verwalten, werden in der Lage sein, sich schnell an Veränderungen anzupassen und erfolgreich am Markt zu bestehen.

Herzlichst

Ulrich Parthier | Publisher it management & it security

INHALT

Farblich hervorgehobene Artikel sind von der Redaktion als besonders lesenswert empfohlen



Inklusive 48 Seiten it security

GUT ZU WISSEN

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

No-Code Low-Code

WIE UNTERNEHMEN DAS BESTE AUS IHRER PLATTFORM HERAUSHOLEN

Low-Code- und No-Code-Plattformen erfreuen sich zunehmender Beliebtheit, da sie es Unternehmen ermöglichen, Software einfacher und effizienter zu erstellen und zu pflegen. Wie bei jeder Technologie gibt es auch hier Best Practices, mit denen Unternehmen das Beste aus ihrer Low-Code- oder No-Code-Plattform herausholen können.

#1 Klein anfangen

Bei der Implementierung von No-Code-Tools ist es am besten, klein anzufangen und die Komplexität schrittweise zu erhöhen. Auf diese Weise erhalten Unternehmen ein besseres Verständnis für die Möglichkeiten der No-Code-Plattform und können sicherstellen, dass sie ihr Potenzial voll ausschöpfen.

#2 Möglichkeiten und Grenzen verstehen

No-Code-Plattformen haben Grenzen und es ist wichtig zu verstehen, wo diese Grenzen liegen, bevor man sie implementiert. So können Unternehmen fundierte Entscheidungen über die Nutzung der Plattform treffen und sicherstellen, dass sie nicht etwas von ihr erwarten, was sie gar nicht kann.

#3 Zusammenarbeit mit der IT-Abteilung

No-Code-Plattformen sind für die Verwendung durch technisch nicht versierte Benutzer konzipiert, aber die Zusammenarbeit mit der IT-Abteilung ist dennoch unerlässlich. IT-Teams können wertvolle Einblicke in die Fähigkeiten und Grenzen der Plattform geben und bei Sicherheit, Compliance und Integration helfen.

#4 In Schulungen investieren

No-Code-Plattformen sind einfach zu bedienen, aber es ist dennoch wichtig, in eine Benutzerschulung zu investieren. So stellen Unternehmen sicher, dass die Mitarbeiter die Plattform effektiv und effizient nutzen.

#5 Den Entwicklungsprozess planen

Bei der Verwendung einer Low-Code- oder No-Code-Plattform ist es wichtig, den Entwicklungsprozess zu planen. Dazu gehören die Definition der Anforderungen, die Erstellung eines Entwurfs und das Testen der Software. So kann das Projekt besser gesteuert und sichergestellt werden, dass die Software den Unternehmensanforderungen entspricht.

#6 Vorgefertigte Komponenten nutzen

Low-Code- und No-Code-Plattformen werden mit vorgefertigten Komponenten geliefert, die Unternehmen zur einfacheren Erstellung und Wartung von Software verwenden können. Nutzen Unternehmen diese vorgefertigten Komponenten, können sie Software schneller und effizienter erstellen und warten.

#7 Vorgefertigte Vorlagen verwenden

Viele No-Code-Plattformen verfügen über vorgefertigte Vorlagen, mit denen sich Software einfacher erstellen und pflegen lässt. Die Verwendung dieser Vorlagen spart Zeit und Mühen und stellt gleichzeitig sicher, dass die Software den Best Practices und Branchenstandards entspricht.

#8 Analysen und Berichte nutzen

No-Code-Plattformen werden häufig mit Analyse- und Berichtsfunktionen geliefert, die Unternehmen helfen, datengestützte Entscheidungen zu treffen. Sie erhalten Einblicke in die Nutzung der Software, erkennen Verbesserungsmöglichkeiten und können den Erfolg ihrer Implementierung messen.

https://baserow.io

HYBRIDE ARBEITSWELT

ÜBERLEBEN ODER GEDEIHEN?

Die neue Studie der Unisys Corporation „From Surviving to Thriving in Hybrid Work" (Vom Überleben zum Gedeihen in der hybriden Arbeitswelt), die in Zusammenarbeit mit dem Forschungsunternehmen HFS Research durchgeführt wurde, liefert einen Fahrplan für Arbeitgeber, um die Produktivität und das Engagement ihrer Mitarbeiter zu steigern.

Der Bericht zeigt: Zugang zu erstklassiger Technologie wird weiterhin ein entscheidender Faktor für das Mitarbeiterengagement und ihre Leistung sein. 62 Prozent der befragten Mitarbeiter gaben an, dass der Zugang zu Technologie ein sehr motivierender Faktor für ihre Arbeitsleistung ist. Der Bericht zeigt jedoch auch, dass die Art und Weise, wie Unternehmen Technologielösungen einführen und kontinuierlich unterstützen, für Mitarbeiter eine Herausforderung darstellt

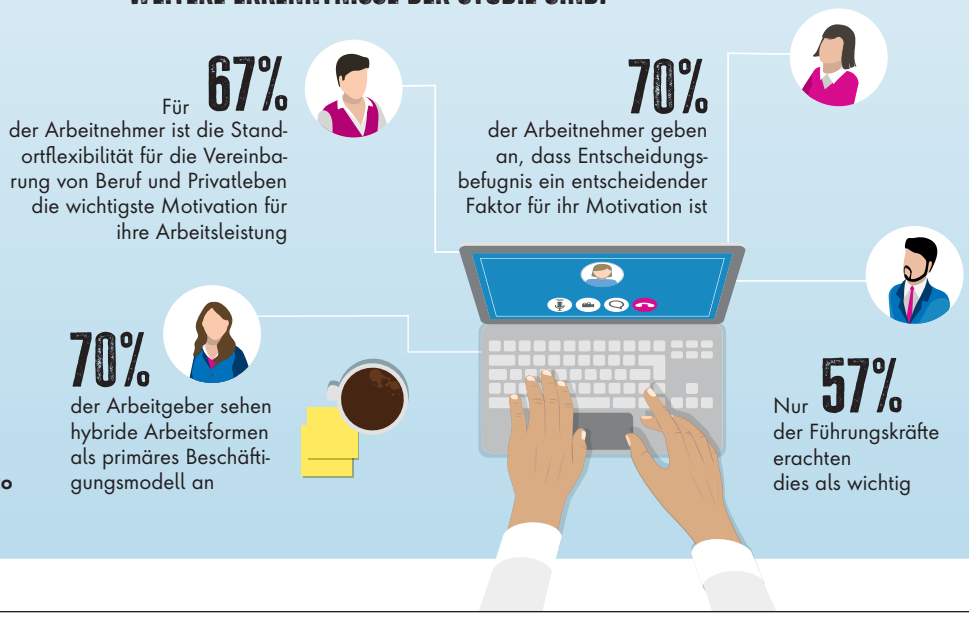
Der neue Standard

„Hybride Arbeit wird sich durchsetzen", denn ein hybrides Arbeitsmodell ist zum Standard geworden. Unternehmen müssen jedoch nicht nur hybride Arbeitsformen einführen, sondern sie auch optimieren, um Talente zu gewinnen und zu halten, neue Teammitglieder zu schulen und einzubinden, neue Führungskräfte zu gewinnen und das Engagement und die Produktivität zu maximieren.

www.unisys.com

GUT ZU WISSEN Die komplette Studie können Sie sich hier herunterladen: **https://bit.ly/41GdJzo**

WEITERE ERKENNTNISSE DER STUDIE SIND:



IT-OPTIMIERUNG

VERMEIDBARE AUSGABEN

Im IT-Portfolio ist Geld versteckt, das ungenutzt bleibt: Jedes Jahr verlieren die meisten internationalen Unternehmen mindestens 10 bis 20 Prozent ihres IT-Budgets durch vermeidbare Ausgaben. Rund ein Viertel der Firmen räumt ein, dass der Anteil des verschwendeten Budgets sogar noch höher ist. Vor allem technische Schulden und redundante Applikationen gelten als Kostentreiber. Die Mehrheit plant zwar die Einführung von Methoden zur Optimierung der IT-Landschaft. Doch 40 Prozent haben aktuell noch nicht eines der gängigen Verfahren implementiert – und besonders selten solche zur Applikationsrationalisierung. Die mögliche Kostenreduktion ist dabei nur einer der Vorteile, den Firmen außer Acht lassen. Denn auch die als unzureichend bewertete Zusammenarbeit von IT und Business verbessert sich deutlich, je mehr Maßnahmen zur Optimierung eingesetzt werden. Der aktuelle LeanIX IT Cost Optimization Survey macht klar: Unternehmen haben es selbst in der Hand, in ihrer IT neue Spielräume für die Zukunft zu schaffen.

www.leanix.net

WELCHE DER FOLGENDEN VERFAHREN ZUR IT-OPTIMIERUNG WERDEN IN IHREM UNTERNEHMEN EINGESETZT?

44%
Aktives Cloud-Management

29%
Regelmäßiges Technology-Risk/ Obsoleszenz-Management

20%
Aktives SaaS-Management

15%
Regelmäßige Applikationsrationalisierung

ANZAHL DER IMPLEMENTIERTEN VERFAHREN ZUR IT-OPTIMIERUNG

28%
eines der aufgeführten Verfahren implementiert

33%
noch keine der aufgeführten Verfahren implementiert

32%
zwei oder mehr ausgeführte Verfahren implementiert

8%
nichts implementiert oder geplant

Sicherheitsrisiko Mensch

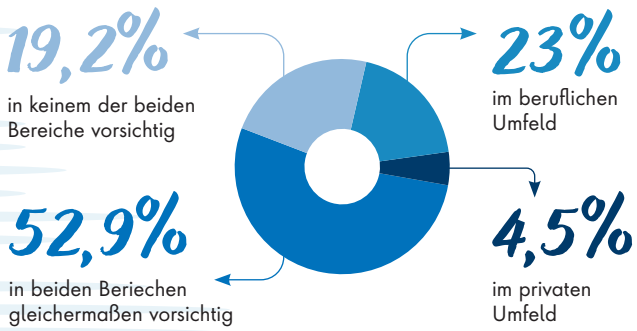
MEHR SICHERHEITSBEWUSSTSEIN IN ALLEN ARBEITSGRUPPEN NÖTIG

25 Prozent der deutschen Angestellten geben an, am Arbeitsplatz weniger vorsichtig zu sein als im privaten Umfeld. Das zeigt die aktuelle Studie „Cybersicherheit in Zahlen" von G DATA CyberDefense AG, Statista und brand eins. Ein ernüchterndes Ergebnis, denn Cyberkriminellen genügt nur ein Klick auf den falschen Link, um das Unternehmensnetzwerk zu kapern und finanzielle Schäden anzurichten. Hinzu kommt, dass Kriminelle mit Betrugsmaschen wie Spear-Phishing oder CEO-Fraud immer raffinierter werden, um Menschen dazu zu verleiten, vertrauliche Firmendaten preiszugeben. Daher gilt: Auch wenn Unternehmen aufgrund des steigenden Bedrohungspotenzials zunehmend in die technische IT-Sicherheit investieren, kommt es am Ende auf den Faktor Mensch an. Ein ganzheitliches IT-Sicherheitskonzept ist erst gewährleistet, wenn die gesamte Belegschaft ein integraler Teil davon ist.

Der Trend zieht sich durch alle Altersgruppen

Die Studie zeigt außerdem: Die Tendenz am Arbeitsplatz unvorsichtig zu sein, zieht sich durch alle Altersgruppen. In der Altersspanne von 16 bis 70 Jahren geht jeder vierte deutsche Arbeitnehmer am Arbeitsplatz Risiken bei der IT-Sicherheit ein. Ein

SIND SIE IM PRIVATEN ODER IM BERUFLICHEN UMFELD VORSICHTIGER IN BEZUG AUF IT-SICHERHEIT?



Ergebnis, das verdeutlicht, wie wichtig es ist, jeden einzelnen Mitarbeitenden – egal aus welcher Abteilung und in welchem Alter – für Cybergefahren zu sensibilisieren. Firmen müssen anfangen, das Thema Security Awareness ganz oben auf die Agenda zu setzen. Nur so kann bei den Angestellten ein Bewusstsein für die Wichtigkeit von IT-Sicherheit am Arbeitsplatz geschaffen werden.

www.gdata.de

SAP-Transformationen enden nie

AUFRÄUMEN, ORDNEN UND AUSMISTEN

Unternehmen, die SAP im Einsatz haben, sind kontinuierlich gefordert. Anpassungen an neue Funktionen und Prozesse aber auch der Umzug in die Cloud sind zwei der wichtigsten Aspekte, die Unternehmen intensiv beschäftigen und wofür sie Lösungen finden müssen. Wie kann ein SAP-Dienstleister hier helfen? Patric Dahse, Geschäftsführer von Natuvion, im Gespräch mit it management-Herausgeber Ulrich Parthier.

Ulrich Parthier: *Daten sind die unverzichtbare Basis für innovative, digitale Geschäftsmodelle und mit das wichtigste Kapital für Unternehmen. Deshalb steht bei Transformationsprozessen eine Bereinigung an, das sogenannte Housekeeping. Was zählen Sie im Einzelnen dazu?*

Patric Dahse: Housekeeping ist nichts anderes als Aufräumen, Ordnen und Ausmisten – oftmals mit riesigen Datenmengen. Im Tagesgeschäft erleben wir drei Typen von Unternehmen. Der erste Typ behauptet, dass ihre Datenqualität gut sei und die Aussage ist auch nicht allzu weit weg von der Wahrheit. Dann gibt es Unternehmen, die ebenfalls behaupten, dass die Qualität ihrer Daten super ist, nur dass das leider nicht stimmt. Und dann gibt es Typ 3: Unternehmen, die genau wissen, dass sie ein Datenqualitätsproblem haben. Sie nutzen die Transformation dazu, um aufzuräumen. In allen Fällen stellt sich die Frage: Ist es sinnvoll, sämtliche Daten auf eine neue Plattform zu transformieren? Viele Altdaten sind Ballast und können gelöscht oder archiviert werden.

Bei Kunden, die so viele Altlasten haben, dass ein „Aufräumen" unverhältnismäßig viel Aufwand darstellt, macht eine Selektive Datentransformation, ein sogenannter Smart Brownfield-Ansatz am meisten Sinn. Der Kunde befüllt sein neues System nur mit den aktuellen und bereinigten Daten, die er braucht, und lässt den Rest im Altsystem. Besteht nur eine geringe Datenhistorie, weil es sich um ein junges System handelt oder gibt es nur wenig Inkonsistenzen, macht wahrscheinlich ein Brownfield Approach Sinn. Das ist der

> UNSERE MISSION IST ES, ALLE SCHWIERIGKEITEN UND HINDERNISSE BEIM UMZUG AUF DIE WUNSCHPLATTFORM DER KUNDEN ZU ÜBERWINDEN.
>
> **Patric Dahse, Geschäftsführer, Natuvion GmbH, www.natuvion.com**

Grund, warum viele Kunden erstmal ein Housekeeping-Projekt mit Roadmap Workshop vorneweg machen, um zu entscheiden, wie es weiter geht.

Ulrich Parthier: *SAP hat das Ende des ECC-Supports auf Ende 2027 verschoben, weil Bestandskunden beim Wechsel in die Cloud gezögert haben und SAP bis zum ursprünglich geplanten Ende 2025 nicht alle Bestandskunden umstellen konnte. Was raten Sie den Kunden hinsichtlich des Zeitpunktes für den Umstieg und welche Zeitspanne sollten sie für die Transformation einplanen?*

Patric Dahse: Unsere Erfahrung zeigt, dass der Umzug auf SAP S/4HANA im Schnitt ein bis zwei Jahre in Anspruch nimmt. Das kann bei komplexen Transformationsanforderungen auch länger dauern aber auch viel kürzer, bei optimalen Voraussetzungen. In den meisten Fällen – und das bestätigt unsere Transformationsstudie 2023 eindrucksvoll – wird die Transformation unterschätzt.

Ulrich Parthier: *Welchen Ansatz sollten Unternehmen wählen, Brownfield- oder Greenfield-Ansatz?*

Patric Dahse: Alle Methoden haben je nach Projektausprägung ihre Berechtigung. Laut unserer aktuellen Studie wird ausschließlich Brownfield zu 32 Prozent genutzt, Greenfield zu 27 Prozent und Selective Data Transition (SDT) zu 20 Prozent. SDT in Kombination mit einer der anderen Methoden kommt zu 21 Prozent zum Einsatz. Bei unseren Kunden ist häufig die Kombination aus SDT und einer der anderen Methoden – wie dem Smart Brownfield – die beste Wahl. SDT ist vor allem beliebt, wo das Downtime-Fenster sehr klein ist. Denn SDT ermöglicht eine Zero-Downtime-Transformation. Laut unserer Studie wird das auch immer wichtiger. 19 Prozent der Befragten müssen jedwede Downtime vermeiden und 30 Prozent haben höchstens ein paar wenige Stunden, ohne dass sie spürbare Auswirkungen auf ihren Geschäftsbetrieb hinnehmen müssen.

Ulrich Parthier: *In ihrer aktuellen Transformationsstudie 2023 benennen Sie als größte Herausforderung die Tatsache, dass den Unternehmen Zeit & Ressourcen für die Digitale Transformation fehlen. Was empfehlen Sie ihnen?*

Patric Dahse: Fehlendes Knowhow, mangelnde Datenqualität und Ressourcen gehören laut den Studienergebnissen zu den größten Herausforderungen. In DACH bestätigen 35 Prozent eine Ressourcenknappheit, 34 Prozent das fehlende Knowhow und 29 Prozent Probleme mit der Datenqualität. Die Kunst dabei ist es, diese Situation in geordnete Bahnen zu lenken, um eine Transformation erfolgreich durchzuführen. Unsere Empfehlung ist im ersten Schritt eine fundierte Analyse und ein Housekeeping-Projekt, um die Qualität der Daten und Prozesse intensiv zu prüfen und zu steigern. Über eine Selektive Datentransformation beziehungsweise Smart Brownfield können unsere Kunden viele der Housekeeping-Anforderungen aber kombinieren und in einem Schritt vereinen. Meine zweite Empfehlung: Planen Sie nicht zu knapp. Viele Unternehmen unterschätzen die Transformation. 40 Prozent derjenigen Befragten, die eine Transformation durchlaufen haben, wollen beim nächsten Mal viel früher mit der Migration anfangen. 46 Prozent wollen beim nächsten Mal mehr Ressourcen einplanen.

PLUS

Transformation Roadbook
bit.ly/3nxsDZW

Ulrich Parthier: *Aktuell sind alle SAP-Dienstleister für die kommenden Jahre gut gebucht. Sie selbst sind in den vergangenen 2,5 Jahren enorm gewachsen von 100 auf aktuell 300 Mitarbeiter. Eine der Herausforderungen des Fachkräftemangels bei Migrationsprojekten sind gerade die fehlenden SAP-Experten. Was tun?*

Patric Dahse: Ja, wir sind stark gewachsen und tun das auch weiterhin. Dieses Wachstum zeigt, wie groß der Bedarf hinsichtlich professioneller Unterstützung bei der technischen Transformation ist, insbesondere bei SAP. Und der Wettbewerb um diese Spezialisten ist hart. Wenn man heute derart viele Experten an Bord holt, dann darf man nicht einfach nur einen Job anbieten, sondern muss äußerst attraktive, gelegentlich auch kreative Arbeitsumgebungen schaffen. Bis dato gelingt uns das sehr gut.

Ulrich Parthier: *Natuvion beschreibt sich selbst als digitales Umzugsunternehmen. Wie würden Sie selbst Ihre Mission beschreiben?*

Patric Dahse: Moderne digitale Plattformen werden in der Cloud betrieben. Unternehmen mieten dort notwendige Funktionalitäten als Service. Die wertvollen Assets und IP liegen damit ausschließlich in den Daten. Daten in hoher Qualität, frei von Inkonsistenzen und rechtskonform sind nicht nur die DNA und Geschäftsgrundlage des Unternehmens, sie sind vor allem das alles entscheidende Differenzierungsmerkmal. Unsere Mission ist es, alle Schwierigkeiten und Hindernisse beim Umzug auf die Wunschplattform der Kunden zu überwinden. Der Kunde wird in die Lage versetzt, seine Daten in bestmöglicher Qualität ein-, aus- oder umzuziehen, wo immer er hinwill. Das ermöglicht unseren Kunden einen entscheidenden Wettbewerbsvorteil: Sie sind jederzeit und problemlos in der Lage, die modernsten Plattformen am Markt nutzen zu können.

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

#eIDAS23:

BUSINESS & PROZESSE SICHER UND EINFACH DIGITALISIEREN

Digitale Prozesse lassen sich nicht mehr aus unserem Leben wegdenken und sind der Schlüssel für effiziente Unternehmen und eine funktionierende Verwaltung. Deswegen ist es essenziell, dass sie nicht nur schnell und einfach, sondern auch sicher und vertraulich eingesetzt werden können.

Um dabei auch vom europäischen Binnenmarkt zu profitieren, müssen insbesondere Unternehmen und Arbeitnehmende ortsunabhängig und über Ländergrenzen hinweg agieren können. Genau das regelt die eIDAS-Verordnung: Unternehmen können mit elektronischen Identifizierungsmitteln und Vertrauensdiensten digitale Dokumente wie Angebote, Bestellungen und Verträge rechtssicher, effizient und transparent innerhalb der EU austauschen und so Geschäfte abwickeln. Für Wirtschaft und öffentliche Verwaltung bieten sich große Chancen und neue Entwicklungsmöglichkeiten.

Wie die Digitalisierung von papierbasierten Transaktionen, betrieblichen Abläufen und Geschäftsprozessen erfolgreich umgesetzt werden kann, besprechen wir auf dem eIDAS Summit des Bitkom. Deutschlands führende Konferenz rund um Digital Trust & Identity bringt am 10. Mai 2023 Fachleute aus Politik, Wirtschaft und Technologie zu einem digitalen, branchenübergreifenden und interaktiven Austausch zusammen.

Auf dem #eidas23 erleben Sie ein vielfältiges Programm aus interaktiven Workshops, aufschlussreichen politischen Keynotes, Best-Practice-Beispielen und konkreten Handlungsempfehlungen aus der ganzen EU. Entdecken Sie Technologietrends, diskutieren Sie über die eIDAS-Verordnung und erweitern Sie Ihr Netzwerk.

https://eidas-summit.de/de

#doc23

DIE EIGENE ZUKUNFTSFÄHIGKEIT SICHERN

Digitale Geschäftsprozesse sind das Fundament der digitalen Transformation. Dadurch können Daten effizient genutzt werden, um das eigene Unternehmen besser zu machen und von wichtigen Zukunftstechnologien wie Künstlicher Intelligenz zu profitieren. Vor allem aber gilt: Ohne digitale Geschäfts- und Verwaltungsprozesse sind Unternehmen nicht mehr zukunftsträchtig. Sie ermöglichen, dass Performance, Automatisierung und Transparenz in Unternehmen steigen, die Kunden- und Mitarbeiterzufriedenheit zunimmt und das Angebot an neuen Produkten und Dienstleistungen erweitert werden kann.

Für Unternehmen heißt es 2023 also dringend: Let's get digital! Aber wie können Prozesse, die noch auf Papier stattfinden, digitalisiert und damit effizienter werden? Wie geht digitales Workflowmanagement? Und wie kann am besten auf Wissen und Ressourcen innerhalb der Firma zurückgegriffen werden?

Das zeigen wir Ihnen auf der Digital Office Conference 2023 – am 11. Mai dreht sich alles rund um „Business Transformation". Erfahren Sie von den wichtigsten Experten, Anwendern und Anbietern der Branche, welche Prozesse und Tools es braucht, um Ihr Unternehmen in digitale Fahrwasser zu bringen und wie Sie Herausforderungen auf dem Weg bewältigen können. Auf der #doc23 können Sie spannende Panel-Diskussionen und interessante Keynotes verfolgen, Fragen stellen und sich mit anderen Teilnehmenden im Online-Format austauschen. Außerdem präsentieren wir exklusiv die Ergebnisse der Sondererhebung zum Digital Office Index 2023 – die Leitstudie zeigt, wie digital Geschäftsprozesse in deutschen Unternehmen heute schon sind.

www.office-conference.com/de

SUBJECT:

MONITORING & ERP-TRANSFORMATION

Herzlich willkommen zu unserem Thought Leadership-Block. Die Frage lautet: was haben die beiden Themen in der Headline miteinander zu tun? Wenn ihre Antwort spontan lautete: nichts, dann liegen sie quasi halb richtig. Es sind zwar zwei separate Themen, das Bindeglied aber lautet SAP.

SAP ist immerhin eine Kernapplikation, verfügt in vielen Bereichen aber nur über rudimentäre Tools. Ein Beispiel gefällig? SAP bietet mit Application Operations als Teil des SAP Solution Manager eigene Werkzeuge zum Monitoring von SAP-Umgebungen. Das war die Chance für Drittanbieter und so ist ein Ökosystem entstanden, das seinesgleichen sucht.

Um die maximale Verfügbarkeit und Performance einer SAP-Umgebung sicherzustellen, müssen neben den SAP-Systemen auch die IT-Infrastruktur und das Netzwerk in ein übergreifendes Monitoring-Konzept integriert werden. Nachfolgend beschreiben wir wie das gehen kann, nämlich, dass das Tool neben Hardware, Betriebssystem, Datenbanken und Applikationen auch Netzwerk-Performance, Cloud-Umgebungen und vieles mehr überwachen können muss. Das geht über das reine Monitoring mit den üblichen Alarmierungs- und Benachrichtigungsmechanismen inklusive Daten und Monitoring-Ergebnisse via Reports und Dashboards weit hinaus.

Nun zum Thema SAP S/4HANA-Projekte. Solche Transformationen stehe für viele Unternehmensbereiche an, trotzdem werden diese Transformationen entgegen besseren Wissens lediglich als IT-Projekte betrachtet und geplant. Das hat zur Folge, dass bei einer Transformation Entscheidungen über die Prozessgestaltung und funktionsübergreifende Gesichtspunkte auf der Strecke bleiben.

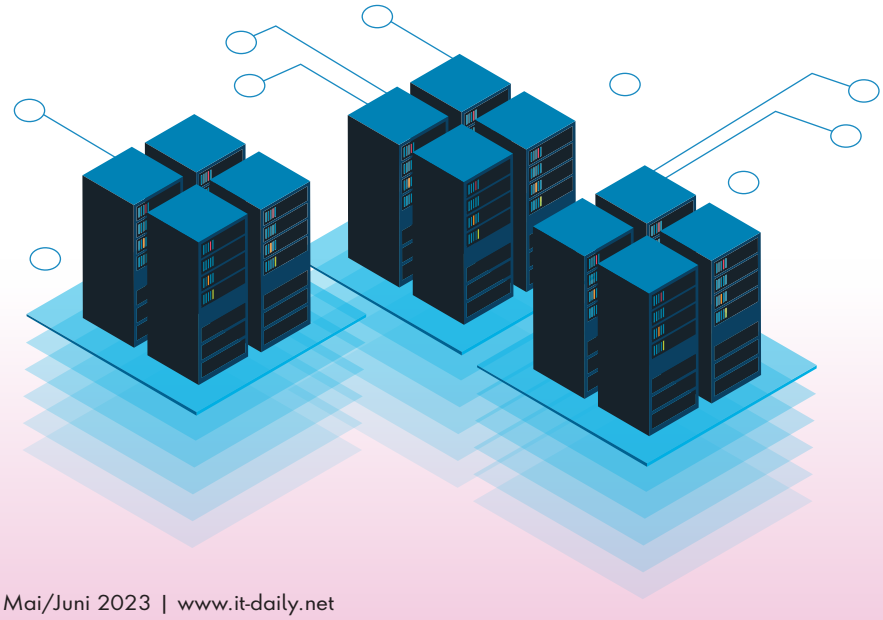
Unternehmen müssen die Transformation als unternehmensweite Chance sehen, um veraltete Technologie zu ersetzen und gleichzeitig Integration, Prozessstandardisierung, Automation und Verbesserungen der gesamten Geschäftsabläufe zu unterstützen.

Monitoring

... IM UND AUS DEM EDGE-RECHENZENTRUM

Die großen Rechenzentren oder die Public Cloud sind in der Regel weit entfernt von den Orten, an denen Daten generiert werden, ganz egal, ob das lokale IT-Infrastrukturen, Produktionsumgebungen oder auch Krankenhäuser sind. Große Datenmengen zur Speicherung und Auswertung in die Cloud zu bringen, kann aufwändig, zeitintensiv und letztlich teuer werden. Auf dem Weg in die Cloud müssen Daten die Grenze zwischen dem Netzwerk, in dem sie erzeugt werden und der Cloud passieren. Im aktuellen Sprachgebrauch wird diese Grenze als Edge bezeichnet. Um zeitkritische Daten möglichst schnell verarbeiten zu können, werden an dieser Grenze Rechenzentren eingerichtet, sogenannte Edge-Rechenzentren oder Edge Datacenter. Dabei handelt es sich meist um relativ kleine Rechenzentren, die sich in unmittelbarer geographischer Nähe zur datenerzeugenden Umgebung befinden. Ganz kleine Rechenzentren werden als Mikro-Rechenzentren bezeichnet: modulare Systeme, normalerweise in einem 19"-Racks, die auch als Bauteile eines Edge-Rechenzentrums dienen können.

Edge-Rechenzentren haben besondere Stärken bei der Verarbeitung zeitkritischer Daten. Als weitere Aufgabe können hier Daten vorverarbeitet werden, die zur Speicherung und Analyse an Cloud-Plattformen geschickt werden sollen. Die Vorverarbeitung senkt die zu verschickende Datenmenge und verringert so die Last auf die involvierten Systeme. Auch die Verarbeitung sensibler Daten, die das Unternehmen aus Sicherheitsgründen nicht verlassen sollen, kann von Edge-Rechenzentren übernommen werden. Egal, welche Aufgaben das Edge-Rechenzentrum übernimmt, Monitoring spielt in vielerlei Hinsicht eine entscheidende Rolle. Das gilt sowohl für das Monitoring der Edge-Rechenzentren selbst als auch für die Möglichkeit, vom Edge-Rechenzentrum aus unterschiedlichste Bereiche in ein zentrales Monitoring zu integrieren und so den Vorteil der Nähe für ein möglichst echtzeitnahes Monitoring zu nutzen. All das schafft eine ganze Reihe von Fragen, auf die ich im folgenden Artikel Antworten liefern möchte: Was muss eine Monitoring-Lösung leisten können, um das Edge-Rechenzentrum zu überwachen? Welche Monitoring-Aufgaben sind für den Einsatz von der Edge aus prädestiniert? Gibt es Monitoring-Tools, die alle Anforderungen erfüllen und was müssen die können?



Das Edge-Rechenzentrum monitoren

Egal, welche Rolle das Edge-Rechenzentrum für die Unternehmens-IT spielt, es ist in der Regel von elementarer Bedeutung und jede Beeinträchtigung oder Störung kann schwere Schäden und hohe Folgekosten verursachen. Von daher ist es wichtig, das Edge-Rechenzentrum auf allen Ebenen kontinuierlich in Hinblick auf Performance und Verfügbarkeit zu überwachen. Die eingesetzte Monitoring-Lösung muss all diese Ebenen und Komponenten überwachen können:

➤ Hardware

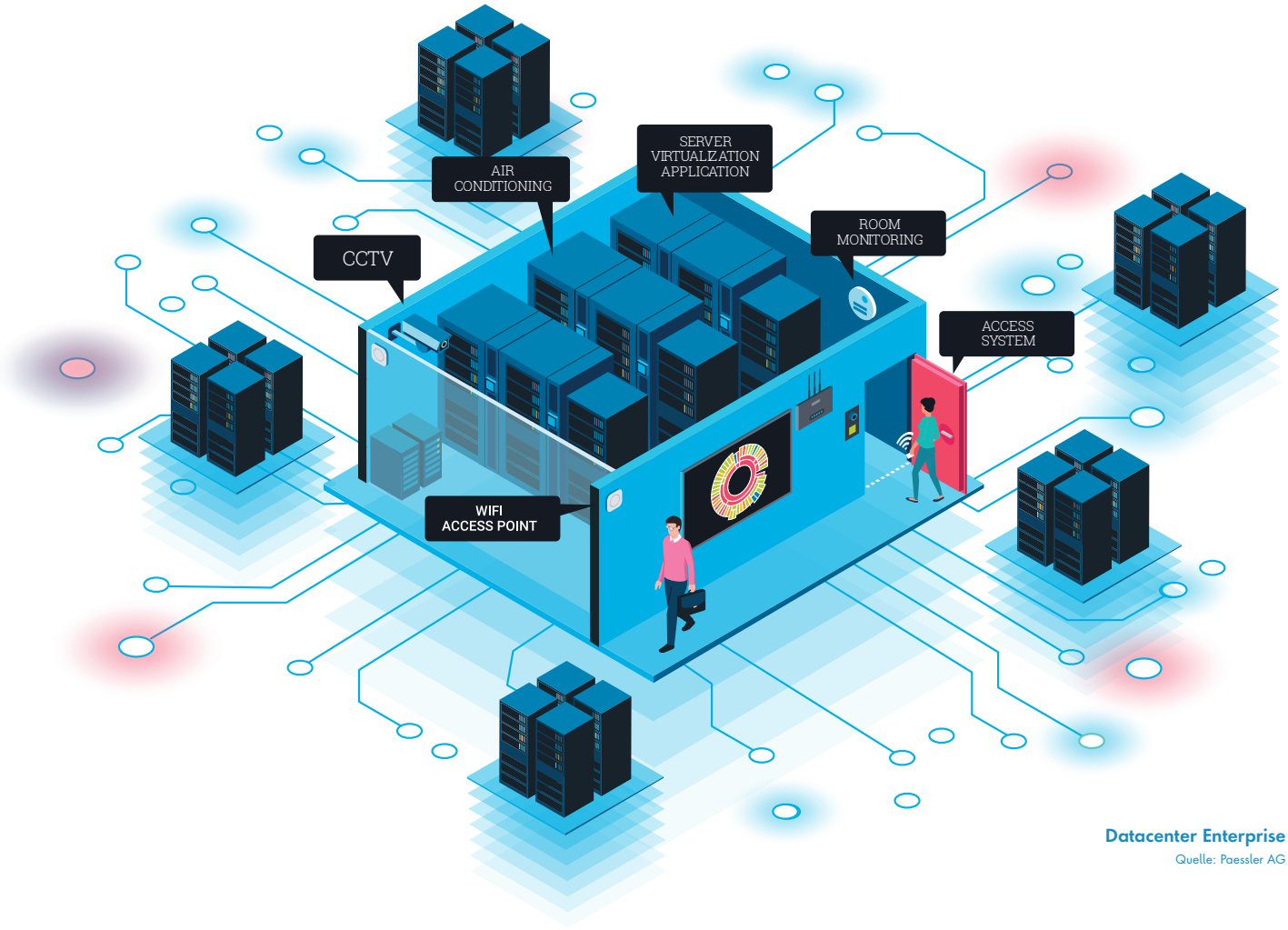
Server, Festplatten, Switche – ein Edge-Rechenzentrum ist kleiner als ein großes, zentrales Rechenzentrum, setzt sich aber aus den gleichen Komponenten zusammen.

➤ IT-Infrastruktur

Server, Datenbanken, Applikationen, Storage-Systeme: Alles was für eine umfassende Datenverarbeitung benötigt wird, findet sich im Edge-Rechenzentrum. Und nachdem das Edge-Rechenzentrum in erster Linie zur möglichst schnellen Verarbeitung zeitkritischer Daten dient, sind maximale Performance und Verfügbarkeit aller Komponenten enorm wichtig und müssen kontinuierlich überwacht werden.

➤ Netzwerk-Performance

Unter dem Aspekt der Geschwindigkeit liegt ein besonderes Augenmerk auf dem Netzwerk. Der Datenverkehr muss ständig überwacht werden, um bei Beeinträchtigungen umgehend eingreifen zu können.



Datacenter Enterprise
Quelle: Paessler AG

Nur so kann die maximale Geschwindigkeit beim Transport und der Verarbeitung der Daten gewährleistet werden.

➤ Gebäudetechnik

Wie in jedem Rechenzentrum spielen auch in einem Edge-Rechenzentrum physikalische Aspekte wie Stromversorgung, Temperatur, Rauchentwicklung oder Feuchtigkeit eine wesentliche Rolle für den reibungslosen Betrieb. Im Idealfall kann die eingesetzte Monitoring-Lösung auch die Ergebnisse der Umgebungs-Sensorik ebenso wie die Überwachung der USVs oder der Klimaanlage in das zentrale Monitoring einbeziehen.

➤ Sicherheit

Das Edge-Rechenzentrum liegt exponiert an der Grenze zwischen IT, Produktionsanlagen, IoT-Umgebungen und dem Internet. Dazu kommt, dass hier vorwiegend zeit- und auch unternehmenskritische Daten verarbeitet werden. Das macht es zu einem idealen Ziel für jede Art von Angriff und das wiederum erfordert, dass alle Sicherheitssysteme, sowohl auf IT-Ebene (Firewalls, Backup-Systeme, Intrusion-Detection-Systeme...) als auch physikalische Sicherheitssysteme (Türschließsysteme, Sicherheitskameras, Alarmanlagen...) ständig verfügbar und integer sind.

Deckt eine Monitoring-Lösung alle hier aufgeführten Bereiche ab, erfüllt sie zumindest schon mal die Anforderungen für das Monitoring des Edge-Rechenzentrums. Oft sind unterschiedliche Teams oder Abteilungen für den Betrieb des Rechenzentrums und die Verarbeitung der Daten zuständig, die dann unterschiedliche Monitoring-Tools einsetzen. Allerdings gibt es auch Lösungen, die beides können: Das Edge-Rechenzentrum überwachen und die Datenverarbeitung, sprich die Generierung, den Transport, die Verarbeitung und die Speicherung der Daten. Was letzteres im Detail bedeutet, behandeln wir im nächsten Kapitel.

Aus dem Edge-Rechenzentrum monitoren

Immer mehr Monitoring-Tools werden als Service aus der Cloud angeboten. Das ermöglicht eine enorme Rechenleistung bei der Verarbeitung und Analyse der ermittelten Monitoring-Daten, speziell wenn es um das Monitoring von Cloud-basierten Diensten und Applikationen geht. So werden tiefgehende Ursachenanalysen oder KI-basierte Vorhersagen möglich. Geht es allerdings um das Alarmieren im Störfall vor Ort, dann ist Schnelligkeit alles – und dann stellt die Entfernung der Cloud ein unüberwindbares Hindernis dar. Dazu braucht es eine Monitoring-Lösung vor Ort oder im Edge-Rechenzentrum. Um die Vielzahl der möglichen Szenarien abzudecken, für die das Edge-Rechenzentrum zum Einsatz kommt, muss die Monitoring-Lösung eini-

ges an unterschiedlichen Methoden und Protokollen unterstützen.

Industrie-Monitoring aus der Edge

Die Digitalisierung der Produktion hat zu massiven Veränderungen im Industrieumfeld geführt. Maschinen und Anlagen erzeugen gigantische Mengen an Daten und schicken diese zur Analyse in die Cloud. Das Edge-Rechenzentrum dient dabei als Tor oder Gateway zur Cloud ebenso wie zur lokalen IT. Hier werden Daten konsolidiert, vorverarbeitet und übersetzt – schließlich sprechen Produktionsanlagen andere Sprachen als die IT. Das Edge-Rechenzentrum verbindet Maschinen mit dem Internet und der Cloud ebenso wie mit der lokalen IT. Und dank seiner Nähe dient es als Basis für das Überwachen sowohl der Produktionsumgebung als auch der IT. Kurze Wege ermöglichen schnelle Reaktionszeiten, Störungen können umgehend erkannt, gemeldet und behoben werden.

Dabei haben sich die Voraussetzungen mit der Digitalisierung grundlegend geändert: Früher war jede Maschine, jede Anlage isoliert und ein Alarm erfolgte noch als rotes Blinklicht oder Sirene, woraufhin der zuständige Techniker am MMI das Problem analysierte und Maßnahmen zur Lösung einleitete. Heute sind Produktionsanlagen vernetzt, alte Maschinen werden über Retrofitting eingebunden, die Kommunikation läuft über IT-Netzwerke. Die meisten Prozesse sind bereichsübergreifend und Störungen müssen erst lokalisiert werden, bevor sie behoben werden können. Gerade in der Industrie aber können Ausfälle schnell enorme Kosten verursachen. Da ist es essenziell, sofort zu wissen, ob die Ursache der Störung innerhalb der Produktionsanlage, bei der Steuerung oder beim Datentransport liegt.

Das geht nur mit einem übergreifenden Monitoring, das sowohl IT als auch OT integrieren und so Zusammenhänge aufdecken und Ursachen für Störungen identifizieren kann – möglichst in Echtzeit. Und es muss im Edge-Rechenzentrum implementiert sein, nicht in der Cloud. Hier kann die Monitoring-Lösung davon profitieren, dass das Edge-Rechenzentrum auch als Übersetzer zwischen OT und IT dient – zahlreiche Hersteller bieten Gateways, die diese Aufgabe an der Edge übernehmen. Daten zu Zustand und Performance der Produktionsumgebung können so schnell und einfach in das zentrale Monitoring integriert werden. Zusätzlich sollte die Monitoring-Lösung aber auch die wichtigsten Protokolle und Methoden aus dem Produktionsumfeld beherrschen wie beispielsweise Modbus, MQTT oder OPC UA. Das erleichtert die Kommunikation mit den Gateways und ermöglicht in Einzelfällen den direkten, noch schnelleren Zugriff auf Produktionssysteme. Neben dem Entdecken und Alarmieren in quasi Echtzeit kann eine geeignete Lösung auch weitere Aufgaben im Edge-Rechenzentrum übernehmen und den Transport der Daten für tiefergehende Analysen in der Cloud überwachen oder Cloud-Dienste in das zentrale Monitoring einbeziehen.

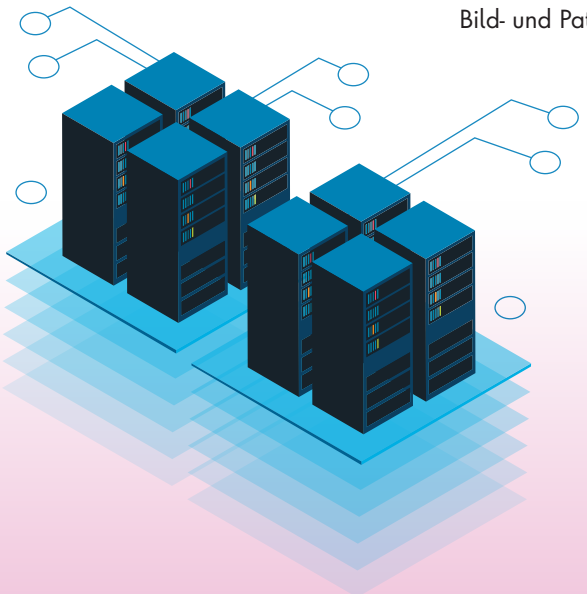
DAS EDGE-RECHENZENTRUM VERBINDET MASCHINEN MIT DEM INTERNET UND DER CLOUD EBENSO WIE MIT DER LOKALEN IT.

Thomas Timmermann,
Senior Market Expert, Paessler AG,
www.paessler.com

Krankenhaus-Monitoring aus der Egde

Digitalisierung ist auch im Gesundheitswesen eines der großen Themen der letzten Jahre. Digitalisierung im Krankenhaus bedeutet eine enorme Steigerung der Effizienz, was in Zeiten von Personal- und Geldknappheit immer wichtiger wird. Allerdings stellt die Digitalisierung auch neue Anforderungen an die Zuverlässigkeit der Systeme: Probleme bei Datentransport und -verarbeitung können ganze Abteilungen lahmlegen. Monitoring ist hier unerlässlich und im hochsensiblen Krankenhaus-Umfeld spielt Geschwindigkeit eine elementare Rolle. Das Edge-Rechenzentrum bietet den idealen Standort für eine Monitoring-Lösung im Krankenhaus. Die muss allerdings in der Lage sein, neben der IT-Infrastruktur auch die medizinischen Systeme und Geräte einzubeziehen. Dazu sollte die Lösung sich mit den im Krankenhaus üblichen Kommunikationsservern integrieren lassen und im Idealfall auch DICOM und HL7 unterstützen, die im medizinischen Umfeld wichtigsten Methoden zum Verwalten von Bild- und Patientendaten.

Thomas Timmermann



HALTET DEN DATENDIEB!

WER IHRE DATEN WILL. WAS ER DAMIT TREIBT. WIE SIE SICH SCHÜTZEN.

Digitale Privatsphäre hat nichts damit zu tun, dass wir etwas zu verstecken hätten. Die meisten Menschen schmuggeln keine Drogen, planen keinen Anschlag oder hacken keine Accounts. Beim Schutz der digitalen Privatsphäre geht es um viel mehr: um unsere Persönlichkeit, unsere intimsten Geheimnisse, Wünsche, Sorgen, die niemand kenn – außer Google und Co.

Längst geht es nicht mehr um Beiträge, die wir freiwillig liken, teilen oder posten. Die Internetriesen wie Meta, Apple oder Amazon registrieren jeden Klick, jede Bewegung, jede Verweildauer. Sie speichern alles ab, erstellen Persönlichkeitsprofile und machen uns nackt. Diesen digitalen Zwilling verkaufen sie teuer unterm Ladentisch, entwickeln mit unseren Schwächen neue Produkte, täuschen und lenken uns, ohne dass wir es merken.

In „Haltet den Datendieb!" spricht der zertifizierte Datenschutzexperte Achim Barth aus, was die Tech-Giganten lieber verschweigen. In dramatischer Klarheit benennt er, wo die Bedrohungen lauern, welche Technologien im Hintergrund wirken und was passiert, wenn wir es den Räubern weiterhin so einfach machen wie bisher. Das Sachbuch hilft jedem, weniger digitalen Schatten zu werfen, ohne auf WhatsApp, Instagram oder Sprachassistenten zu verzichten.

Haltet den Datendieb!
Wer Ihre Daten will.
Was er damit treibt.
Wie Sie sich schützen.;
Achim Barth, GABAL Verlag; 03-2023

Zentrale Schaltstelle

DIE HERAUSFORDERUNGEN EINER ERP-TRANSFORMATION

Eine Unternehmensressourcenplanung (ERP) ist für viele Unternehmen nicht nur eine Software, sondern die zentrale Schaltstelle. Hier wird das Business organisiert und wertvolle Daten für die Zukunftsplanung generiert. Wichtige Prozesse wie Lieferketten, Lagerhaltung, Betrieb, Handel, Finanzen, Berichterstattung, Fertigung und Personalwesen gehören zu den Kernaufgaben eines ERP. Gleichzeitig dient es der abteilungsübergreifenden Transparenz und ermöglicht die Koordination und Analyse von Prozessverbesserungen. Der schiere Umfang an Daten und Prozessen macht ein ERP jedoch oft zu einer komplexen Maschinerie. Deshalb ist es vielfach schwierig, sie zu transformieren – beispielsweise zu SAP S/4HANA. Eine solche Transformation betrifft alle und trotzdem werden gelegentlich diese Transformationen entgegen besseren Wissens lediglich als IT-Projekte betrachtet und geplant. Das hat zur Folge, dass bei einer Transformation Entscheidungen über die Prozessgestaltung und funktionsübergreifende Gesichtspunkte auf der Strecke bleiben. Das Resultat: Die Ergebnisse bleiben hinter den Erwartungen zurück, Zeitpläne werden nicht eingehalten und Unternehmen sind mit unnötigen geschäftlichen und finanziellen Risiken konfrontiert.

Fakt ist, dass die Umstellung und Transformation eines ERP-Systems nicht nur eine IT-Initiative sein darf. Stattdessen sollten Unternehmen die Transformation als unternehmensweite Chance sehen, um veraltete Technologie zu ersetzen und gleichzeitig Integration, Prozessstandardisierung, Automation und Verbesserungen der gesamten Geschäftsabläufe zu unterstützen.

Vier Herausforderungen einer ERP-Transformation

1. **Implementierung:** Eine ERP-Transformation braucht Zeit und jeder Schritt erfordert kritisches Fachwissen und Kontrolle.
2. **Datenintegration:** Die Übertragung von Daten aus bestehenden Systemen ist lebenswichtig und birgt viel Raum für Fehler.
3. **Planung:** Unvorhergesehene Verzögerungen können zu erheblichen Engpässen führen und die Kosten schnell in die Höhe treiben.
4. **Budget:** Es ist nicht ungewöhnlich, dass ERP-Projekte die Budgets überschreiten, da unvorhergesehene Ausgaben entstehen.

Je besser ein Transformationsprojekt durch eine effiziente Planung, Personalausstattung und potenzielle Vorabinvestitionen gesteuert wird, desto wahrscheinlicher ist ein erfolgreiches Ergebnis. Diese Tatsache wird durch erfahrene Beratungsunternehmen bestätigt, beispielsweise Deloitte, wonach die „Projektvorbereitung ein entscheidender Faktor" für den Erfolg einer Transformation ist.

Doch wie lässt sich eine erfolgreiche Transformation sicherstellen? Der CFO und sein Team sind die besten Anlaufstellen, wenn es darum geht, Einblicke und Fachwissen für ERP-Transformationsinitiativen zu erhalten. Laut einer Studie betrachten drei Viertel der CFOs die Automatisierung von ressourcenintensiven und manuellen Aufgaben sowie die Cloud-Technologie als die wichtigsten Elemente eines modernen Finanzsystems. Darüber hinaus sind mehr als die Hälfte der Umfrageteilnehmer der Meinung, dass die Automatisierung von Arbeitsabläufen (68 Prozent) und prädiktive Analysen (54 Prozent) das größte Potenzial haben, um die meisten wertschöpfenden Anwendungsfälle zu ermöglichen.

55%-75%

aller ERP-Projekte verfehlen ihre Ziele.

-Gartner

Warum eine werteorientierte ERP-Transformation sinnvoll ist

Die Boston Consulting Group ist der Meinung, dass eine ERP-Transformation - wie jede andere größere Geschäftsinitiative - von Anfang an eine Werteperspektive erfordert. Mit einem wertebasierten Ansatz können sich Unternehmen ganzheitlich auf die ERP-Transformation konzentrieren und im Anschluss die Früchte ernten, einschließlich einer weniger komplexen und flexibleren ERP-Landschaft.

Dank eines werteorientierten Ansatzes lassen sich ERP-Transformationen zudem schrittweise und in Form nacheinander folgender kleinerer Initiativen durchführen. Diese kleineren, in sich abgeschlossenen Transformationsphasen ermöglichen es, kontinuierlich Werte zu schaffen und mit jedem Prozessschritt einen Return on Investment zu erzielen.

Laut einer Studie von Harvard Business Review gaben 90 Prozent der Befragten an, dass die Menge der Daten, die ihr Finanzteam sammelt und nutzt, in den letzten Jahren zugenommen hat. 88 Prozent der Befragten sagten, dass eine datengesteuerte Kultur im Finanzwesen für die zukünftige Leistung entscheidend sein wird. Von führenden Positionen in den Finanzabteilungen wird außerdem erwartet, dass sie die digitale Transformation vorantreiben und die ERP-Umgebung aufrüsten. Doch eine ERP-Transformation ohne Werteansatz und eine vorherige Korrektur der Prozesse, etwa im Finance und Accounting, birgt das Risiko eines Fehlschlags.

Häufigste Transformationsprobleme

Eines der meisten Probleme einer ERP-Transformation wird dadurch hervorgerufen, dass die Finanzprofis bei der Planung nicht mit am Tisch sitzen. Damit fehlt der wichtigste Faktor, das Buy-in der Profiteure einer Transformation. Dies wiederum hat maßgeblich Einfluss auf das Change Management. Das sehen auch namhafte Analysten so. In ihren Prognosen gehen sie davon aus, dass etwa 55 bis 75 Prozent aller ERP-Initiativen ihre Ziele nicht erreichen. Die richtigen Entscheidungen können nur dann getroffen werden, wenn die Endnutzer und damit auch die Finanzprofis an den Diskussionen und Planungen einer Transformation beteiligt sind.

Ein weiteres Problem besteht in veralteten Prozessen, insbesondere wenn diese nach der Transformation weiterhin bestehen. Dabei bietet ein ERP-Upgrade die

47%

der ERP-Implementierungen werden aufgrund von Datenproblemen verzögert.

-Panorama Consulting Group

beste Möglichkeit, Prozesse neu zu definieren und optimieren. Die Neugestaltung der Prozesse mit einer möglichst hohen Automation führt zu einer optimalen Effizienz. Das mutmaßlich schwerwiegendste Problem bei Transformationen tritt dann auf, wenn sie zu Betriebsunterbrechungen oder Risiken für die Daten führt. Derartige Komplikationen gilt es unter allen Umständen zu vermeiden, was wiederum nur mit einer guten Planung und der Einbeziehung der ERP-Fachleute geht.

Warum Transformation und Automation Hand in Hand gehen müssen

Fest steht, dass eine ERP-Transformation bereits im Vorfeld gut vorbereitet werden kann. Besonders wichtig ist dabei die höchstmögliche Automatisierung von Standardprozessen. Das Financial Close Management, die Automatisierung der Debitorenbuchhaltung und das Intercompany Financial Management von BlackLine ergänzen und erweitern ERP-Systeme beispielsweise, indem sie manuelle Prozesse eliminieren, die normalerweise außerhalb des ERP-Systems in Tabellenkalkulationen durchgeführt werden.

Je nachdem welche Systeme und Prozesse durch die Transformation optimiert werden, gibt es unterschiedliche Ansätze. Eine Möglichkeit besteht darin, das Altsystem während der Vorbereitungsphase mit maximaler Automation zu optimieren, um die Transformationsteams massiv zu entlasten. Damit wird sichergestellt, dass die existierende Grundlage, bestmöglich für die Transformation vorbereitet ist. Eine weitere Option ist die Prozessoptimierung und Automatisierung während der Transformation selbst. Die besten Möglichkeiten bietet die Kombination beider Ansätze. Sie sorgt für eine weitreichende Wertschöpfung – insbesondere im Finance und Accounting. Denn durch die Integration, Orchestrierung und Automatisierung von End-to-End-Buchhaltungsprozessen werden schneller vollständige und genaue Ergebnisse erzielt. Diese Continuous-Accounting-Lösungen können schnell und mit minimaler IT-Unterstützung implementiert werden und erlauben den Unternehmen mehr Kontrolle, reduzieren die Risiken und sorgen dafür, den Nutzen einer umfassenden ERP-Umstellung bereits zu einem sehr frühen Zeitpunkt zu erzielen.

Ralph Weiss

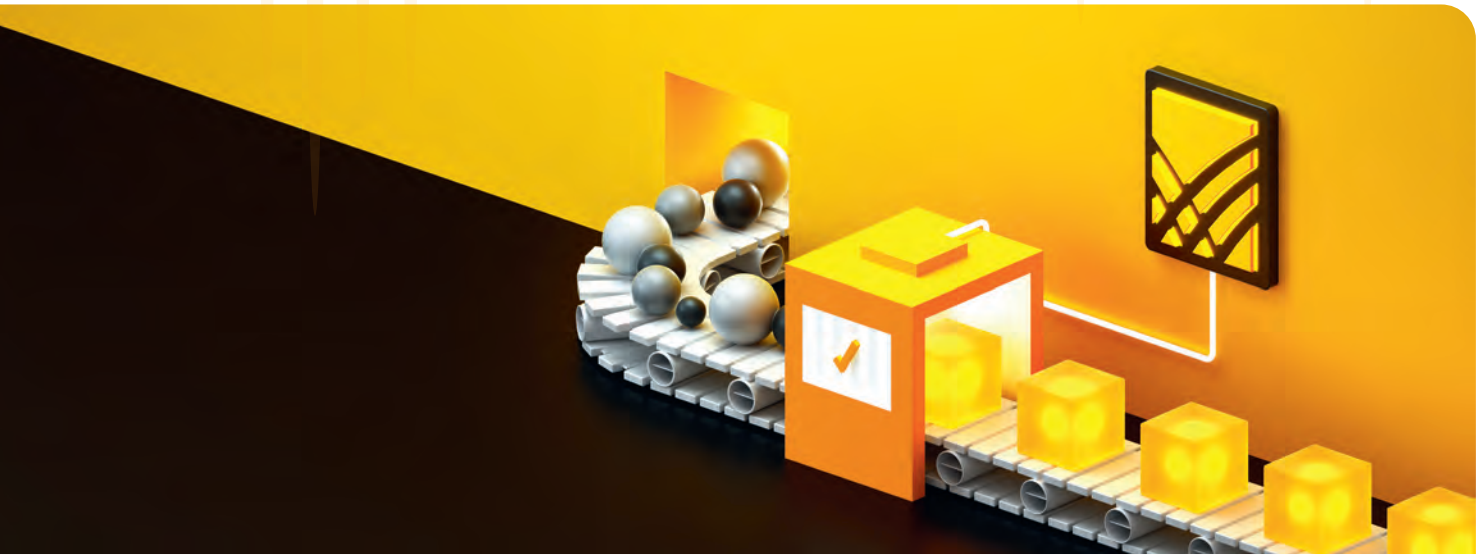
EINES DER MEISTEN PROBLEME EINER ERP-TRANSFORMATION WIRD DADURCH HERVORGERUFEN, DASS DIE FINANZPROFIS BEI DER PLANUNG NICHT MIT AM TISCH SITZEN.

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

20%-30%

der Kosten für die Transformation können durch einen wertebasierten Ansatz gesenkt werden.

-BCG



#mbufJK23

AUS DER PRAXIS. FÜR DIE PRAXIS.

Der Jahreskongress des Microsoft Business User Forums hat den turbulenten vergangenen Jahren getrotzt und seinen Status als Veranstaltungshighlight gefestigt. Mit seinem Schwerpunkt auf dem direkten Austausch zwischen IT-Professionals und mit den Kongress-Partnern hat das Event ein einzigartiges Flair und ist mit den anonymen Großevents nicht zu vergleichen. CIOs und IT-Verantwortliche aus mittelständischen Unternehmen, bei denen Microsoft-Lösungen eine wichtige Rolle spielen, tauschen sich dort seit Jahren über ihre Strategien und Projekte oder die Relevanz neuer Produkte und IT-Trends aus.

2023 findet der mbuf Jahreskongress vom 19. bis 21. Juni 2023 in den Hauptsälen und den umgebenden Freiflächen des darmstadtium in Darmstadt, statt. Der bewährte Mix aus Fachvorträgen, Networking und der integrierten Partner-Messe soll auch in diesem Jahr die Veranstaltung prägen.

Der Montag beginnt am späten Nachmittag und steht unter dem Motto „Ankommen und Netzwerken". Am Dienstag dreht sich alles um „Erfahrungstransfer mit abschließender Community-Party": Die Besucher bekommen in drei parallelen Vortrags-Tracks spannende Projekte unter dem Kongressmotto vorgestellt und können abends in lockerer Atmosphäre den Tag ausklingen lassen.

Mit der Neuplanung kommt am Mittwochvormittag schließlich ein spannendes Element hinzu: thematisch geclusterte Workshops – gemeinschaftlich gehostet von Partnern und MVPs. Eine tolle Gelegenheit, sich unter realen Bedingungen einen persönlichen Eindruck von deren Expertise zu verschaffen.

Der Jahreskongress endet zur Mittagszeit, sodass die reichhaltigen Erkenntnisse entspannt auf der Heimreise verdaut werden können.

https://2023.mbuf.de/

Unified Communications as a Service

DER SCHLÜSSEL FÜR MEHR ROI IN DER UNTERNEHMENSKOMMUNIKATION

Kommunikation innerhalb und zwischen Unternehmen befindet sich seit jeher im Wandel, sowohl durch technologischen Fortschritt als auch oft durch zusätzliche Trends und Faktoren, wie aktuell die zunehmende Akzeptanz und Nutzung von Remote- und Hybrid-Arbeitsmodellen. Dementsprechend lohnt es sich für Unternehmen, regelmäßig einen Blick auf die eigene Kommunikations- und Kollaborationsinfrastruktur zu werfen – und deren Kosten.

Die oben genannten Arbeitsmodelle funktionieren beispielsweise nur dann, wenn Mitarbeiter die Möglichkeit haben, flexibel multimodal zu kommunizieren, also über verschiedene Standorte und Geräte hinweg. Die Liste der dafür notwendigen Kanäle ist lang: Telefon, Videokonferenzen, E-Mails und Messengers sind lediglich die Basics, die in fast jedem Unternehmen zu finden sind. In vielen Branchen oder Funktionen sind zudem noch spezialisierte Tools notwendig, beispielsweise zur visuellen Kollaboration im Produktdesign.

Die Kosten falscher Kommunikationsinfrastrukturen

Damit stehen Unternehmen vor einer Herausforderung, denn dieser Mix an Kommunikationskanälen muss eingekauft, bereitgestellt, orchestriert, verwaltet, gewartet und abgesichert werden. All dies ist mit direkten oder indirekten Kosten verbunden und Unternehmen, die versuchen, soviel wie möglich davon intern abzudecken, binden wertvolle Kapazitäten ihrer IT-Teams, zusätzlich zu den Kosten für Server-Räume, Hardware und Energie. Gerade die Höhe der Erstinvestition ist bei diesem Ansatz signifikant. Noch kostspieliger wird es, wenn im Sinne der Ausfallsicherheit zusätzliche, redundante Systeme und Komponenten integriert werden.

Zudem muss sichergestellt werden, dass die aufgebaute Infrastruktur bei Bedarf entsprechend skalieren kann – zu Zeiten der Erstanschaffung ist jedoch selten klar, zu welchem Grad. Um auf der sicheren Seite zu sein, werden deshalb Kapazitäten geschaffen, die vielleicht nie oder nicht durchgehend abgerufen werden und sich dementsprechend nicht amortisieren können.

Vor diesem Hintergrund liegt es nahe, externe Dienstleister für diese Aufgaben zu beauftragen. Wenn Unternehmen für die einzelnen Kommunikations- und Kollaborationslösungen jedoch unterschiedliche Anbieter oder Dienstleister beauftragen, summieren sich die Kosten für Anschaffung und Nutzungsgebühren schnell. Zudem steigt die Komplexität rasant an, denn die einzelnen Lösungen sollten auch kompatibel sein. Die Aufgabe der Orchestrierung und Verwaltung der einzelnen Komponenten liegt dann ebenfalls wieder beim Unternehmen selbst und bindet Ressourcen, die an anderer Stelle Mehrwert schaffen könnten.

Die Lösung: UCaaS

Die Situation scheint verfahren, aber es gibt eine Lösung: UCaaS (Unified Communications as a Service) ist ein cloudbasiertes Bereitstellungsmodell, mit dem verschiedene Kommunikations- und Kollaborationslösungen auf einer einzelnen Plattform konsolidiert werden, sodass Nutzer mit einem einzigen Klick zwischen den verschiedenen Kanälen wechseln können. Üblicherweise umfassen UCaaS-Angebote bereits Cloud-Telefonie, Videokonferenzen und Messaging, aber über offene APIs können weitere Funktionen, auch solche von Drittanbietern, integriert und vom UCaaS-Anbieter orchestriert werden. Mit UCaaS können Unternehmen dementsprechend alle oder fast alle ihrer Kommunikationskanäle kostengünstig und ausfallsicher aus einer Hand beziehen. Ein hoher Grad an Skalierbarkeit und Flexibilität ist ebenfalls gegeben, da Kapazitäten einfach nach Bedarf zugebucht oder zurückgefahren werden können.

Michaela Mars-Matzke

MIT UCAAS KÖNNEN UNTERNEHMEN ALLE ODER FAST ALLE IHRER KOMMUNIKATIONS-KANÄLE KOSTENGÜNSTIG UND AUSFALLSICHER AUS EINER HAND BEZIEHEN.

Michaela Mars-Matzke,
Regional Vice President Strategic Channel Partners EMEA, RingCentral,
www.ringcentral.com

Die neue Snom M500 Serie

Unabhängig von Ihren geschäftlichen Anforderungen, Snom bietet Ihnen passgenaue Kommunikationslösungen. Und das seit über 25 Jahren.

snom

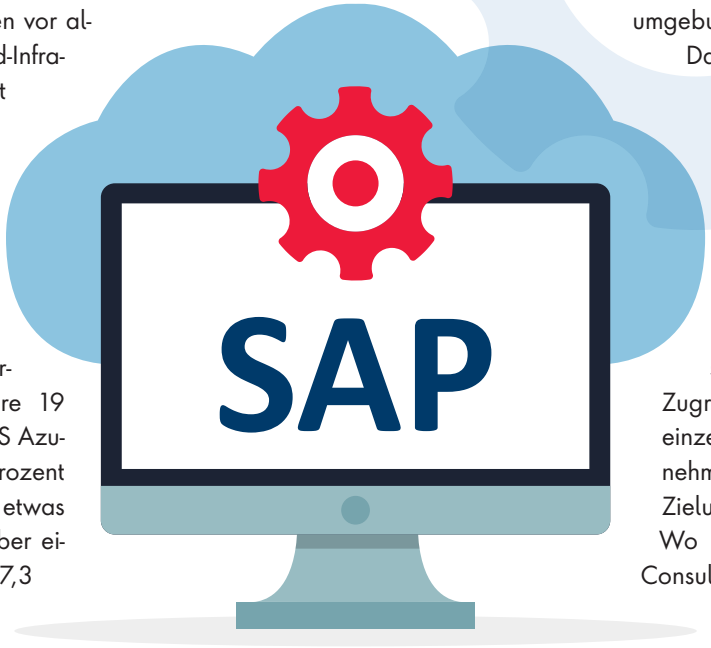
SAP-Cloud-Integration

DATEN NUTZEN UND PROZESSE AUTOMATISIEREN AUF NO-CODE-BASIS

Die Studie „SAP im Mittelstand" von Theobald Software zeigt die enorme und stark wachsende Relevanz von Cloud-Lösungen im SAP-Kontext.

Für fast 39 Prozent der befragten Unternehmen stellt die Migration der SAP-Systeme in die Cloud eine große Herausforderung dar. Sollen SAP-Daten in der Cloud gespeichert und verarbeitet werden, vertrauen die Unternehmen vor allem auf Amazons Public-Cloud-Infrastruktur S3: Mit rund 59 Prozent aktueller und 27 Prozent geplanter Nutzung hat sich das US-amerikanische Unternehmen den ersten Platz gesichert. Diesen teilt es sich mit der Cloud-Infrastruktur von SAP. Sie wird von ebenso vielen Unternehmen verwendet, doch lediglich weitere 19 Prozent haben dies geplant. MS Azure liegt derzeit mit knapp 50 Prozent aktueller Nutzung zwar noch etwas zurück, kann sich aber bald über einen hohen Zuwachs freuen: 37,3 Prozent planen den Einsatz. Microsoft hat also gute Chancen, zur derzeitigen Nr. 1 Amazon aufzuschließen und sie sogar zu überholen. Bei der Anbindung der SAP-Umgebung an Cloud-Plattformen zeigt sich ein ähnliches Bild: Amazon führt, SAP-eigene Cloud-Lösungen sind ebenfalls sehr stark und Microsoft – hier aber vor allem Power BI deutlich vor Azure – folgt dicht dahinter.

Zur Verarbeitung und Speicherung von SAP-Daten werden also Data Lakes und Data Warehouses aktuell oder zukünftig gleichermaßen intensiv genutzt. Eine wichtige Anforderung der Fachanwender ist die zentrale Datenhaltung (Single Point of Truth), die durch die Installation von Data Lakes und Data Warehouses erfüllt wird. Daraus entsteht ein erhöhter Bedarf, die Daten auch in der Cloud verfügbar zu machen.



Sales, Controlling, HR und andere

Immer mehr Unternehmen wollen ihre SAP-Daten möglichst vollständig, performant und schnell in andere Cloud-Zielumgebungen übertragen, um sie dort mit anderen Daten zusammenzuführen, zum Beispiel für monatliche Auswertungen und Prognosen in den Bereichen Sales, Controlling oder HR. Das soll ohne Programmieraufwand und Eingriff in die SAP GUI geschehen. Gleiches gilt zunehmend auch für SAP-Prozesse: Sie in diversen Cloud-Anwendungen abzubilden und mit anderen Lösungen zu verknüpfen, ist die Basis, damit der angestrebte Automatisierungssprung gelingt.

SAP-Datenintegration

Zunächst zur SAP-Datenintegration. Gemeint ist damit die automatische Übertragung von Daten aus dem SAP-System (On-Premises oder Cloud) in andere Zielumgebungen per Schnittstelle. Die Daten werden beispielsweise in unterschiedlichen Formaten direkt in einer Datenbank zur Verfügung gestellt. Die SAP-Schnittstelle soll diese Schritte im Hintergrund ausführen, ohne dass der Nutzer es im Alltag bemerkt. So ermöglicht sie den schnellen und sicheren Zugriff auf SAP-Daten, damit die einzelnen Abteilungen des Unternehmens diese in ihren gewohnten Zielumgebungen nutzen können. Wo klassische Entwicklungs- und Consultingprojekte Wochen, Monate und manchmal Jahre beanspruchen, verkürzt der No-Code-Ansatz einer unabhängigen Schnittstelle die Implementierung auf wenige Tage.

Ein bisher wenig erschlossenes Anwendungsspektrum

Durch die Datenintegration können Unternehmen jederzeit die aktuellen Daten für Analysen extrahieren und in zahlreiche gewünschte Zielumgebungen integrieren. Das können Vermessungs- und Beschaffungsdaten sein, die für Reporting-Zwecke in der Google Cloud bereitgestellt werden. Oder es handelt sich um

Rohdaten, die zuverlässig in den Amazon S3 Data Lake übertragen werden, um anschließend für eine bessere Preis- und Verfügbarkeitsplanung agil die Kundennachfrage zu prognostizieren.

Das gesamte Anwendungsspektrum der über eine unabhängige Schnittstelle integrierten SAP-Daten ist groß: Verwaltung in einer performanteren Datenbank (Cloud und „klassisch"), Anreicherung mit Informationen aus anderen Systemen oder Visualisierung aller unternehmenskritischen Daten, etwa der Soll-Ist-Vergleich über ein BI-Tool für den Vertrieb oder die Produktion.

SAP-Prozessintegration

Inzwischen geht es nicht mehr nur um SAP-Daten. Mit einem Cloud-Konnektor wie yunIO von Theobald Software können Unternehmen ihre SAP-Prozesse über ihre vertrauten Cloud-Anwendungen direkt im Webbrowser gestalten, automatisieren und integrieren. Die No-Code-Lösungen verbinden SAP und web- oder cloudbasierte Anwendungen und sorgen dafür, dass auch komplexe Prozessabläufe Systemgrenzen überwinden. Anwender können Prozesse individuell nach Bedarf gestalten und zu jeder Zeit über eine zentrale Plattform orts- und geräteunabhängig auf Daten zugreifen, auch ohne SAP-Wissen.

MIT EINEM CLOUD-KONNEKTOR KÖNNEN UNTERNEHMEN IHRE SAP-PROZESSE ÜBER IHRE VERTRAUTEN CLOUD-ANWENDUNGEN DIREKT IM WEBBROWSER GESTALTEN, AUTOMATISIEREN UND INTEGRIEREN.

Christoph Schuler, General Manager US, Theobald Software, www.theobald-software.com

SIE WOLLEN IHRE SAP-DATEN UND -PROZESSE IN DIE CLOUD BRINGEN?

Ein großer Vorteil liegt im Master Data Management, bei dem SAP die zentrale Rolle spielt. Auf die Kunden- oder Materialstammdaten müssen sich Unternehmen verlassen können. Oft sind in die Datenpflege mehrere Personen involviert und weitere verantwortlich für die Prüfung und Freigabe von Änderungen. Für das Data Management existieren jedoch deutlich nutzerfreundlichere, kollaborativere Umgebungen als SAP, etwa SharePoint. Das Übertragen der dort hinterlegten und freigegebenen Daten in SAP kann mit einem Konnektor per Knopfdruck automatisch geschehen. Dies beschleunigt den Prozess und minimiert Fehler bei der manuellen Eingabe.

Starke Vereinfachungen

Ein weiteres Beispiel ist das Anlegen eines Business Partners: Über Tools wie PowerApps oder Nintex kann ein Eingabeformular frei gestaltet werden, in das der Anwender den Namen des Partners, Adress- und Bankdaten sowie weitere Informationen einträgt. Im Vergleich zur Erfassung in SAP mittels mehrerer Eingabemasken wird der Prozess stark vereinfacht und benutzerfreundlicher gestaltet – SAP-Kenntnisse sind dabei nicht mehr erforderlich.

In Kombination mit der Microsoft Power Platform lassen sich außerdem zahlreiche Prozesse automatisieren und integrieren, die heute noch langsam und fehleranfällig ablaufen. Beispiele sind der automatische Übertrag von Rechnungsdaten aus einer SharePoint-Tabelle nach SAP, ein Urlaubsantrag mit mehrstufiger Genehmigung oder ein außerhalb von SAP ausgefülltes und automatisch weitergegebenes BANF-Formular.

Fazit

Die Studie „SAP im Mittelstand" von Theobald Software zeigt, dass sich die SAP-Cloud-Integration in vollem Gange befindet und für einen erheblichen Teil der Unternehmen eine Herausforderung darstellt. Der Markt sortiert sich derzeit noch, wobei sich bereits einige dominante Anbieter etabliert haben. SAP muss heute nicht mehr die verschlossene Auster sein, mit schwer zu extrahierenden Daten, komplizierter Anbindung an externe Lösungen und unflexiblen Prozessen. Schnittstellen und Konnektoren erlauben die vollständige No-Code-Integration von SAP in die Cloud-Umgebung der Unternehmen, auch bei hohem und stetig steigendem Datenvolumen oder zunehmender Prozesskomplexität.

Christoph Schuler

PLUS

Die Ergebnisse der Studie sind jetzt kostenlos erhältlich:
https://theobald-software.com/studie/

SAP Sales Cloud V2

ERSTE EINBLICKE IN DIE NEUE VERSION

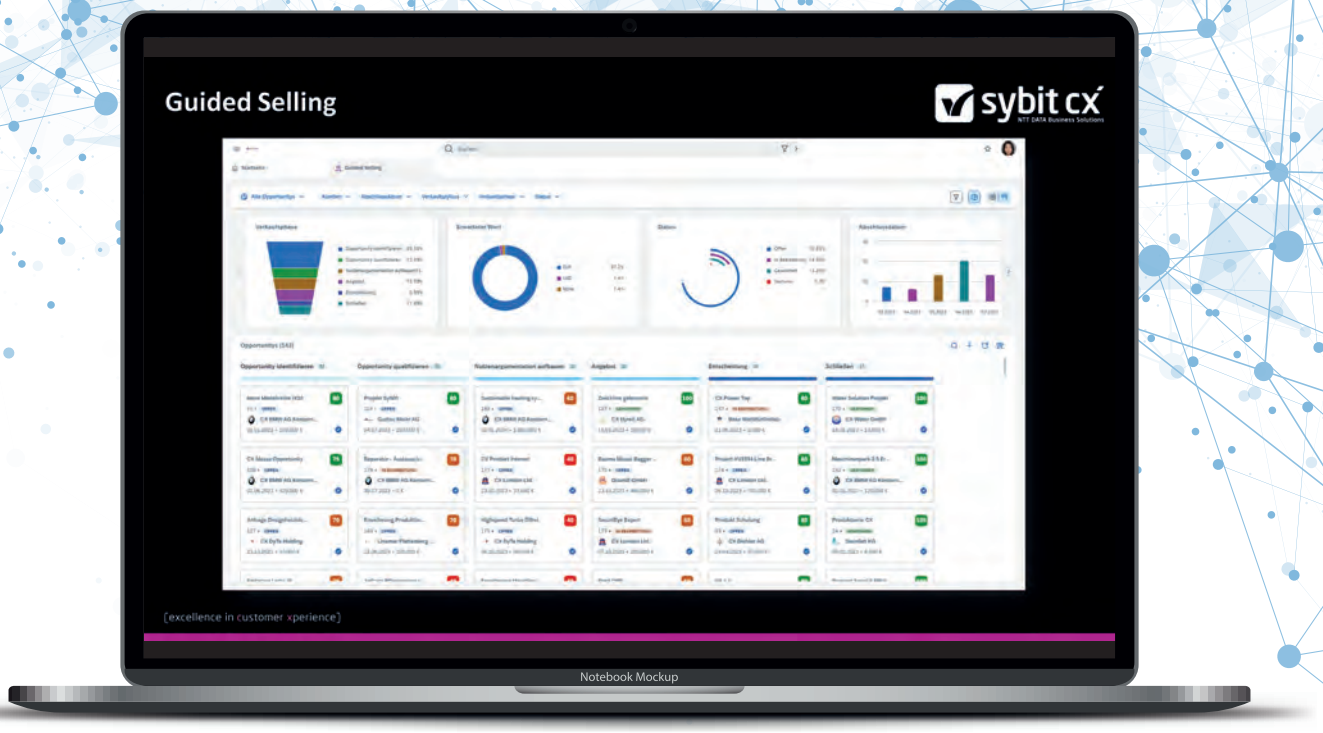
Es ist die neue Vertriebs-Lösung der SAP: Die Sales Cloud V2. Sie verspricht vor allem eines: intelligente, automatisierte und anwenderfreundlichere Prozesse. Wie viel Erleichterung verschafft die neue Lösung den Vertriebs-Teams? Und was sind die Unterschiede zur Vorgängerversion?

Die Strategie von SAP-Chef Christian Klein ist deutlich. Investitionen sollen künftig vor allem in das zukunftsträchtige Cloud-Geschäft fließen. Mit der SAP Service Cloud V2 stellte das Software-Unternehmen bereits im August 2022 eine Nachfolgeversion der bisherigen Cloud-Lösung vor. Nun findet sich im Lösungsportfolio der SAP eine weitere Neuerung: die SAP Sales Cloud V2. Klar ist: Die Änderung der Hauptversionsnummer bringt signifikante Änderungen mit sich. Intelligente Insights, moderne UX, ein natives mobiles Erlebnis: Die SAP will Vertriebsteams mit der neuen Lösung ein Paket zur Seite stellen, das es ermöglicht „in der komplexen Vertriebsumgebung von heute mehr Geschäfte schneller abzuschließen". An sich keine revolutionäre Idee – entscheidend sind die neuen Funktionalitäten und Verbesserungen.

Um es vorwegzunehmen: Am Lead to Order- Kernprozess hat sich nichts geändert. Der Sales Funnel bleibt „klassisch" aufgebaut und dient dem Innendienst, Außendienst und der Sales-Leitung als Kooperations-Plattform, um Absatzchancen zu erhöhen und die Kundenbindung zu steigern. Aber: In den Bereichen User Experience und Technologie hat die SAP mit der V2 neue, spannende Maßstäbe gesetzt.

Moderne UX

Es gibt eine Sache, die haben Sales-Mitarbeiter nicht: Sehr viel Zeit. Warten, bis das CRM-System lädt? Immer dran denken, auf Speichern zu klicken? Sich durch Tabs navigieren? Bitte nicht. Die SAP Sales Cloud V2 verspricht eine intuitive und benutzerfreundliche Oberfläche. Ein erster Praxis-Test zeigt: Es genügen tatsächlich wenige und intuitive Klicks, um ans Ziel zu gelangen. Komplexe Abfragen werden dank Elastic Search-Funktionen der nächsten Generation schneller, flexibler und intelligent ausgeführt. Über das Global Search-Feld auf der Startseite etwa lassen sich direkt Angebote, Kunden, Aufgaben, Ansprechpartner oder Opportunities finden. Wer nur schnell eine Telefon-Nummer ändern will, kann dies unkompliziert und schnell über ein Side Panel. Detaillierte Informationen etwa zu einem Kunden sind übersichtlich auf einen Blick aufbereitet: Welche Leads sind offen? Wer ist im Kunden-Team? Wer sind die Ansprechpartner? Die CTI-Integration macht es möglich, den jeweiligen Ansprechpartner mit einem Klick anzuru-



fen. Zudem zeigt der erste Praxis-Test: Die System-Performance der SAP Sales Cloud V2 ist beeindruckend schnell und die User profitieren in der Remote-Arbeit vom „Mobile first"-Ansatz für iOs und Android und der In-App-Integration mit Microsoft Teams.

Guided Selling

Die Funktion vereint mehrere Prozesse wie die Erstellung von Opportunities, die Qualifizierung von Deals und vieles mehr in einem optimierten Arbeitsbereich. Es soll den Vertriebs-Teams helfen, die richtigen Verkaufschancen zu identifizieren, den Verkaufszyklus in verschiedenen Phasen zu durchlaufen und schließlich den Geschäftsabschluss zu erzielen. Was viele vielleicht schon von Projektmanagement-Tools kennen, gibt es nun auch im Rahmen des Guided Selling: Auf einem Kanban-Bord werden alle Verkaufschancen nach Phasen visualisiert und nach Prioritäten geordnet. Per einfachem Drag-and Drop lassen sich die Opportunities in die unterschiedlichen Phasen bis zum Abschluss verschieben.

Basierend auf einem zentral definierten „Playbook" schlägt das System automatisch Aktionen vor, um die Opportunities weiter zu qualifizieren und diese zum Ziel zu führen. Strukturiert zum Vertriebserfolg – das scheint das klare Prinzip zu sein. Die SAP hat den Arbeitsbereich auf jeden Fall mit wichtigen Erkenntnissen, Einsichten und intelligenten Empfehlungen optimiert.

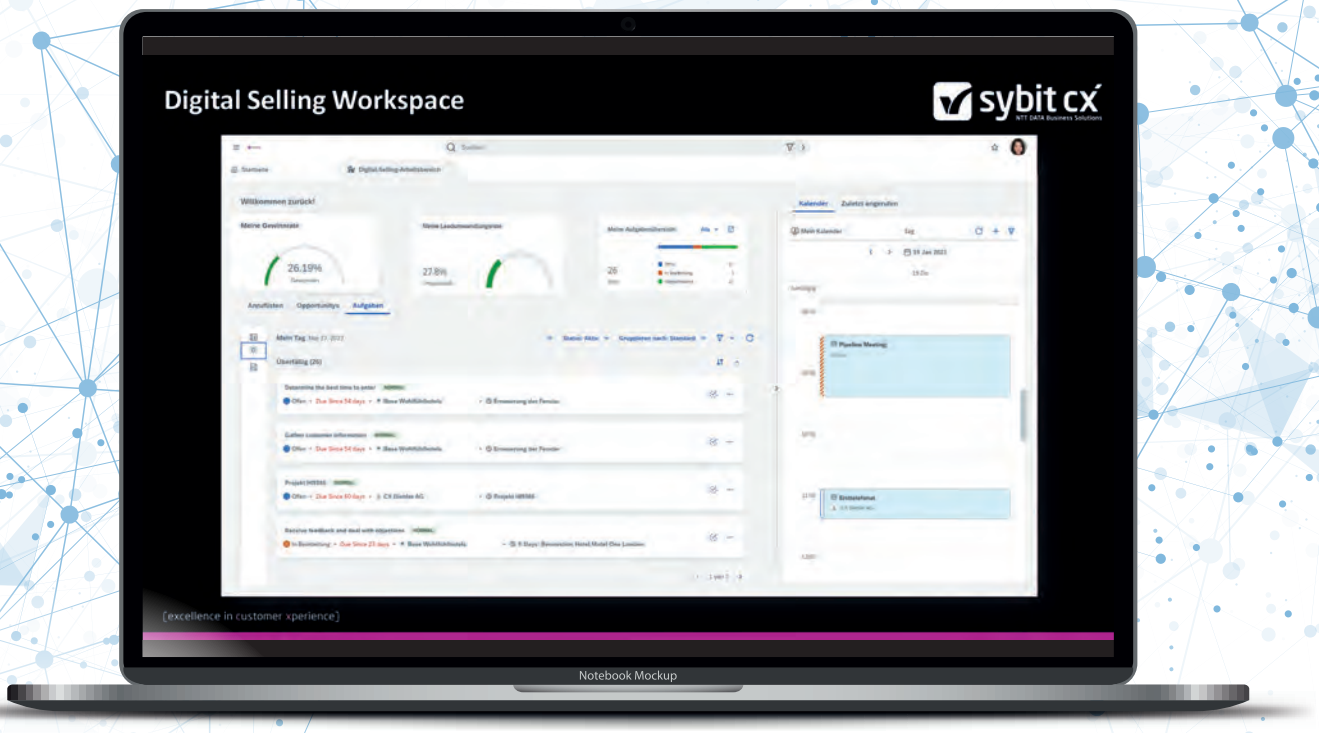
IN DER NEUEN SALES CLOUD STECKT VIEL POTENZIAL – FÜR BESTIMMTE ANFORDERUNGEN WIRD DIE VORHERIGE LÖSUNG ABER IMMER NOCH DIE RICHTIGE VERSION SEIN.

Martin Schneider, SAP Senior Consultant C/4 HANA, Sybit GmbH, www.sybit.de

Pipeline Manager und Forecast Tracker

Vor allem für die Vertriebsleitung eine entscheidende Übersicht, um das Sales-Team besser zu steuern und beispielsweise mittels Forecasts auch innerhalb der Organisation Richtung Controlling oder Geschäftsführung schnell auskunftsfähig zu sein. Wie steht es beispielsweise um die Pipeline in Q2 oder im Gesamtjahr 2023? Antworten finden sich in diesem Bereich kompakt dargestellt, um auch Risikogeschäfte schnell zu identifizieren. Der Pipeline Manager soll auf einen Blick Aufschluss darüber geben, wie sich die Opportunities in der Pipeline entwickeln. Opportunities sind in Form von farblichen Blasen visualisiert und es ist auf einen Blick erkennbar, welcher Wert und welche Qualifizierungsstufe dahinterstecken. Zugeordnete Vertriebsmitarbeiter können direkt angesprochen werden. Was-wäre-wenn-Analysen ermöglichen genaue Prognosen, die sich im Verlauf mit der Live-Pipeline gleichen lassen.

Der Forecast-Tracker vergleicht unter anderem die eingereichten Prognosedaten mit den Verkaufszielen und den aggregierten Opportunity-Beträgen für den ausgewählten Geschäftszeitraum. Zur Lösung gehört mit dem Sales Assistant



auch eine Art Sprachassistent, der als Teil der mobilen App verfügbar ist.

Digital Selling Workspace

Es ist ein neuer Arbeitsbereich, den die SAP hier eingeführt hat. Er kann am Morgen den Einstieg in den Sales-Tag erleichtern und zeigt beispielsweise direkt die aktuelle Gewinnrate an. Eine Kalenderansicht schafft Überblick über die anstehenden Termine und eine Anruferliste dient dem schnellen Abarbeiten von möglichen Telefonaktionen. Der Tab Opportunity bietet für den aktuellen Tag eine Übersicht an Aktivitäten, die der Vertriebsmitarbeiter heute tun könnte, um die Opportunity weiter voranzubringen. Anstehende oder überfällige Aufgaben werden direkt angezeigt. Mit einem Klick können sie aber auch abgeschlossen werden.

AI und Relationship Intelligence

Die neue Kundenansicht in der SAP Sales Cloud V2 verspricht einen noch besseren Überblick über alle relevanten Informationen zum Kunden, den Beziehungs-Score und alle Interaktionen. Mit der Relationship Intelligence sind Vertriebsteams in der Lage, ganz einfach herauszufinden, wer wie und mit wem im jeweiligen Unternehmen vernetzt ist. So können verborgenen Beziehungen aufgedeckt und die Geschäftsentwicklung durch eine verbesserte Kundenbetreuung beschleunigt werden.

Diese AI-basierte Funktion erlaubt es also, ein intelligentes Netzwerk aufzubauen und die CRM-Anwendung zu optimieren, indem tiefere Einblicke in das Engagement von externen Kunden generiert werden. Dieses Netzwerk wird durch eine Verbindung zum Office 365-E-Mail-Server mit allen bekannten Beziehungen zusammen mit einer Messung der Beziehungsstärke (Hugrank) erreicht.

Skalierbarkeit

Als Cloud-basierte Lösung ist SAP Sales Cloud V2 hochgradig skalierbar und eignet sich daher für Organisationen jeder Größe - vom Kleinbetrieb bis zum Großunternehmen.

Fazit: Viele Benefits, keine Ablösung

Die SAP hat hier umgesetzt, was sich viele Anwender schon lange wünschen und setzt vor allem auf zwei Attribute: userfreundlich und automatisiert. Die SAP Sales Cloud V2 ist eine moderne Plattform mit besserer Performance und höherer Verfügbarkeit, da sie in der Public Cloud eines Hyperscalers betrieben wird. Die SAP selbst spricht sogar von „Zero Downtime". Es gibt zahlreiche Erweiterungsmöglichkeiten, bedingt durch die Microservice-Technologie. Integrierbare und integrierte Produkte aus dem SAP-Kosmos wie Standardschnittstellen zu S/4 HANA oder die embedded Sales Analytics Cloud ermöglichen durchgängige end-to-end Prozesse. Aber auch Sales Cloud V1-User kennen bereits diesen Vorteil. Zumal der Funktionsumfang der V2 – Stand März 2023 – noch nicht gleichwertig zur V1 ist.

In der neuen Sales Cloud steckt also viel Potenzial – für bestimmte Anforderungen wird die vorherige Lösung aber immer noch die richtige Version sein. Zumal die SAP Sales Cloud V1 weiterhin verbessert und gewartet wird, es keine Pläne für einen End of Support der V1-Version gibt und alle neuen Features aus der SAP Sales Cloud V2 als Add-on auch den V1-Kunden zur Verfügung stehen.

Aber: Unternehmen, die strategisch denken und ihre Customer Journey dynamisch verbessern möchten, sollten sich die SAP Sales Cloud V2 genauer ansehen.

Martin Schneider

Explore new Horizons

DATEN SICHER MIGRIEREN UND IHREN WERT NEU DENKEN

Laut DSAG-Investitionsreport arbeitete 2022 mehr als jeder dritte SAP-Kunde mit S/4HANA. Die Mehrheit der Unternehmen, knapp 69 Prozent, die den Wechsel nach SAP S/4HANA oder SAP S/4HANA Cloud planen, wollen dies im Laufe dieses Jahres tun, weitere 23 Prozent in den nächsten zwei bis drei Jahren und nur sechs Prozent später, so Research Services by Foundry. Die Uhr tickt, nicht nur weil SAP Wartung und Support für die SAP ERP-Vorgängerversion einstellen wird. Welt und Märkte entwickeln sich weiter rasant und Unternehmen müssen ihre IT- und Geschäftsprozesse nicht nur anpassen, sondern neu denken und modernisieren. Sie müssen innovative Umgebungen schaffen, in denen Daten produktive Quelle und Basis für eine nachhaltige Wertschöpfung sind. Verschiebungen in globalen Netzwerken und Lieferketten, verändertes Verbraucherverhalten und Themen wie KI und ESG müssen abgebildet, umgesetzt und schnell angepasst werden können. Mit dem Umzug nach SAP S/4HANA schaffen sich Unternehmen die Grundlage für die digitale Transformation, die alle weiteren Entwicklungen ermöglichen wird.

Die meisten Unternehmen wollen die digitale Transformation mit SAP S/4HANA meistern. Zurecht, denn die Lösung ist technologisch und funktional führend. Es gibt Faktoren, die den Projekterfolg bestimmen und beachtet werden sollten. Für den erfolgreichen Wechsel ist eine umfassende Analyse des Ist-Zustandes der Systeme und die gründliche Planung unumgänglich. Zudem sichern Unternehmen das Gelingen mit einem standardisierten Verfahren und einem industrialisierten Migrationsansatz. S/4HANA ebnet den Weg in die digitale Zukunft. Versäumen Unternehmen es im Vorfeld, die strategischen Rahmenbedingungen zu analysieren und eine daraus abgeleitete Roadmap zu definieren, führt das zu einer unnötigen Komplexität und der Gefahr, Ziele zu verfehlen.

Unternehmen, die wettbewerbsfähig bleiben möchten, können sich extreme Langzeitprojekte nicht leisten. Sie müssen ihre definierten Ziele zeitnah erreichen. Möglich wird dies durch die „Industrialisierung" von Transformationsprojekten und komplexen S/4HANA-Einführungen. Mithilfe automatisierter, szenarienbasierter Transformationssoftware sowie einem softwaregestützten Projektmonitoring über alle Projektphasen hinweg, kann dies erfolgreich realisiert werden. SNP hat dafür die Transformationssoftware CrystalBridge und ein selektives Datenmigrationsverfahren entwickelt, SNP BLUEFIELD. Sie bieten Kunden maximale Transparenz, höchste Flexibilität und jederzeit Kontrolle über ihr Projekt.

Transformation braucht Flexibilität

Unternehmen gehen mit unterschiedlichen Voraussetzungen und Anforderungen in ein Transformationsprojekt. Mit dem Wechsel nach S/4 und in die Cloud wollen sie Geschäftsprozesse schnell digitalisieren und Innovationspotentiale voll ausschöpfen. Sie wollen Investitionen aus der Vergangenheit sichern und gleichzeitig notwendige Innovationen einführen. Das ermöglicht ein selektiver Datenmigrationsansatz mit einer flexiblen Umstrukturierung von Stammdaten, Organisationsmodellen und Geschäftsprozessen. Damit wählen Unternehmen nur die historischen Daten aus, die in den künftigen Systemen benötigt werden. Übrige Daten werden im Archiv konserviert, wo sie weiterhin verfügbar bleiben. Kurz gesagt können Unternehmen mit einer flexiblen und selektiven Methodik schneller, sicherer und kostengünstiger auf SAP S/4HANA umsteigen und das volle Potenzial der neuen Technologie nutzen.

www.snpgroup.com

EXPLORE NEW HORIZONS – TRANSFORMATION WORLD 2023

Alle Fragen rund um Ihr Transformationsprojekt, das Potenzial Ihrer Daten und wie Sie es maximal ausschöpfen, beantworten unsere Experten und Partner auf der Transformation World 2023 in Heidelberg.

Jetzt anmelden und Ihre kostenlose Teilnahme sichern!

SAP ist keine Insel

ÜBERGREIFENDES MONITORING-KONZEPT GESUCHT

Um die maximale Verfügbarkeit und Performance einer SAP-Umgebung sicherzustellen, müssen neben den SAP-Systemen auch die IT-Infrastruktur und das Netzwerk in ein übergreifendes Monitoring-Konzept integriert werden. Das erfordert Tools, die in der Lage sind, einen solchen Überblick mit einer Lösung abzubilden. Was aber müssen diese Tools im Detail können?

Eingeschränkte Bordmittel

SAP bietet mit Application Operations als Teil des SAP Solution Manager eigene Werkzeuge zum Monitoring von SAP-Umgebungen. Allerdings gilt die Lösung gemeinhin nicht als die intuitivste Software. Das Einrichten von Alarmen und Benachrichtigungen, das Erstellen von Dashboards oder das Überwachen von Datenbanken: Viele Monitoring-Aufgaben gestalten sich mit dem SAP Solution Manager umständlich, erfordern den Einsatz von Agenten oder mehreren Tools. In der Praxis zeigt sich aber immer wieder, dass komplexe und aufwändig zu bedienende Monitoring-Tools dazu führen, dass das Monitoring vernachlässigt wird. Beeinträchtigungen werden dann nicht mehr zeitnah erkannt und können zu ernsten Problemen bis hin zu Totalausfällen führen.

Darüber hinaus arbeitet der SAP Solution Manager systemimmanent: Nur wenn die SAP-Systeme laufen, läuft auch der Solution Manager. Bei einem Totalausfall gibt's auch keinen Alarm mehr, Performance-Einbrüche beeinträchtigen auch den Solution Manager. Die wesentliche Einschränkung beim Solution Manager liegt allerdings in seiner Reduzierung auf das Monitoring der SAP-Systeme. Probleme bei Hardware, Storage-Systemen oder Netzwerk, die sich negativ auf die Performance der SAP-Systeme auswirken, werden vom Solution Manager nicht erkannt. Das Überwachen bereichsübergreifender Prozesse oder gar über die SAP-Umgebung hinausgehende Root-Cause-Analysen sind nicht möglich. Dafür braucht es Tools, die sowohl IT- als auch SAP-Umgebungen überwachen können.

IT-Monitoring plus SAP

Die Grundlage einer solchen kombinierten IT- und SAP-Monitoring-Lösung liefert ein möglichst breit aufgestelltes Monitoring-Tool. Das bedeutet, dass das Tool neben Hardware, Betriebssystem, Datenbanken und Applikationen auch Netzwerk-Performance, Cloud-Umgebungen und vieles mehr überwachen können muss. Natürlich muss es über das reine Monitoring hinaus die üblichen Alarmierungs- und Benachrichtigungsmechanismen unterstützen und Daten und Monitoring-Ergebnisse über Reports und Dashboards zielgerichtet publizieren können. Um als Basis für ein vertieftes SAP-Monitoring zu dienen, muss die Software entsprechend erweiterbar sein und Schnittstellen liefern, die das Einbinden von Skripten zum Monitoring von SAP-Systemen erlauben. Im Idealfall stellt das Monitoring-Tool Vorlagen bereit, die das Erstellen und Einbinden solcher Skripte vereinfachen.

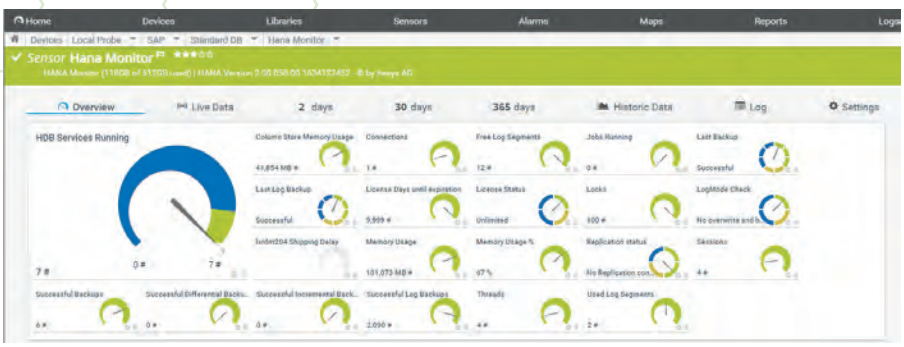
SAP richtig überwachen

Die Anforderungen an ein umfassendes SAP-Monitoring lassen sich im Wesentlichen in vier essenzielle Bereiche und eine Reihe von Extras gliedern:

#1 SAP-Basismonitoring: Basis eines erfolgreichen SAP-Monitoring ist das Sicherstellen der SAP-Grundfunktionen. Das umfasst die Überwachung von Verbuchungsabbrüchen, Sperreinträgen, System-Dumps, Auslastung der SAP Workprozesse, SAP-Jobs

#2 Datenbanken: Egal ob SAP HANA, MSSQL, Sybase, DB2 oder Oracle, reibungslos arbeitende Datenbanken sind essenziell für den Betrieb einer funktionierenden SAP-Umgebung. Daher sind die Statusinformationen für die Sicherheit und Performance hier essenziell.

#3 SAP-Cloud: Werden SAP-Cloud-Dienste genutzt, müssen diese in das zentrale SAP-Monitoring einbezogen werden.



Monitoring einer SAP Hana-Instanz mit Scansor und PRTG

#4 Sicherheit des SAP-Systems: In der Regel werden alle wichtigen Unternehmensdaten in SAP zusammengeführt. Die Sicherheit der SAP-Systeme hat daher allererste Priorität. Das Überwachen der Anzahl Nutzer oder Nutzer mit bestimmten resp. kritischen Berechtigungen, der Status von SAP-Zertifikaten und vielen weiteren sicherheitskritischen Parametern erhöht die generelle Sicherheit der SAP-Systeme.

#5 Extras: Ein umfassendes und breit angesetztes SAP-Monitoring kann über die reine Betriebssicherung hinaus Informationen liefern, die den täglichen Betrieb erleichtern, für zusätzliche Transparenz sorgen und so die allgemeine Zuverlässigkeit verbessern. Dazu gehören beispielsweise das Monitoring des Application Log (SLG1), der einzelnen Server-Instanzen oder SAP iDocs.

Neben dem Funktionsumfang kommt es in erster Linie auf Bedienbarkeit und Übersichtlichkeit an. Nur wenn die Lösung einfach einzurichten und zu bedienen ist, nur wenn Alarme in Echtzeit zielgerichtet verschickt werden und nur wenn die Monitoring-Ergebnisse auf übersichtlichen Dashboards und über individuelle Berichte an die jeweils Verantwortlichen ausgeliefert werden, nur dann wird das Monitoring im täglichen Betrieb genutzt und kann liefern, was so dringend benötigt wird: einen ständigen Überblick über Performance und Verfügbarkeit der SAP-Systeme und die Sicherheit, dass im Falle von Störungen die Zuständigen umgehend informiert oder alarmiert werden.

Kooperation gefordert

SAP-Umgebungen sind genau wie IT-Infrastrukturen eine hochkomplexe Angelegenheit und erfordern für einen reibungslosen Betrieb Spezialisten. Solange das Monitoring der SAP-Umgebungen ausschließlich bei den SAP-Spezialisten liegt, wird es auch ein ausschließliches SAP-Monitoring bleiben. ITOps, die Spezialisten für den Betrieb der Nicht-SAP-IT, sind normalerweise keine SAP-Spezialisten, sprich sie wissen nicht, was in einer SAP-Umgebung wie überwacht werden muss. Hier ist Zusammenarbeit gefragt. Die erfordert allerdings als Basis Tools, die von beiden Teams nutzbar sind. Nachdem SAP-Tools für gewöhnlich die IT-Umgebung ignorieren, sind hier IT-Tools gesucht, die auch „SAP können". SAP stellt aber ein derartig komplexes Spezialgebiet dar, dass ein breit aufgestelltes IT-Monitoring-Tool mit einer vollwertige SAP-Monitoring-Lösung viel zu sehr in die Tiefe gehen würde. Außerdem erfordert die Entwicklung einer solchen SAP-Lösung das Knowhow echter SAP-Experten. Kooperation ist hier also nicht nur im Unternehmen zwischen SAP-Spezialisten und ITOps gefordert, sondern auch zwischen SAP-Experten und den Herstellern von IT-Monitoring-Lösungen. Nur so kann eine klassische IT-Monitoring-Lösung mit tiefgehenden SAP-Monitoring-Funktionen erweitert werden und IT- und SAP-Umgebungen in einem zentralen Tool zusammengeführt werden. Denn auch wenn es manchmal so aussieht: SAP ist keine Insel, sondern an vielen Stellen eng mit der IT verbunden.

Der Schweizer SAP-Dienstleister itesys und das deutsche Monitoring-Unternehmen Paessler sind eine solche Kooperation eingegangen. Basierend auf der langjährigen Erfahrung als SAP-Dienstleister hat itesys Scansor entwickelt, eine SAP-Erweiterung für Paessler PRTG, die IT-Monitoring-Lösung der Paessler AG. Dank der nahtlosen Integration von Scansor in PRTG lassen sich SAP- und IT-Umgebungen mit einem Tool überwachen. Daten aus Infrastruktur, Netzwerk und SAP-Systemen werden in Kontext gesetzt und ermöglichen die Ursachenanalyse bei bereichsübergreifenden Störungen.

Thomas Timmermann | www.paessler.de

360-Grad-Monitoring

MIT EINER LÖSUNG ALLES IM BLICK

In der digitalen Welt ist die IT-Infrastruktur einer Organisation von entscheidender Bedeutung für ihre Leistungs- und Wettbewerbsfähigkeit. Diese wird jedoch mit der fortschreitenden Entwicklung von Technologien wie Cloud Computing, künstlicher Intelligenz, Container- und Microservices, dem Internet of Things (IoT) und anderen digitalen Werkzeugen zunehmend komplexer. Das kann sowohl positive als auch negative Auswirkungen auf ein Unternehmen haben. Auf der einen Seite bieten große IT-Umgebungen Skalierbarkeit, Effizienz, Innovation und Wettbewerbsfähigkeit, die entscheidend für den Erfolg sind. Auf der anderen Seite können sie aber auch Risiken und Herausforderungen mit sich bringen, denn je komplexer die IT-Infrastruktur wird, desto größer wird die Gefahr von schwerwiegenden IT-Ausfällen. Gerade die Unterbrechung kritischer Geschäftsprozesse kann in Organisationen zu rechtlichen Konsequenzen, schwindendem Kundenvertrauen und erheblichen Kosten führen.

Komplexe IT-Infrastruktur erschwert Überwachung

Der Ausbau der IT- Infrastruktur erfordert in der Regel erhebliche Investitionen in Sicherheit, Redundanz – aber auch in das Personal. Nur so kann sichergestellt werden, dass die eigenen Mitarbeiter über die erforderlichen Kenntnisse und Fähigkeiten verfügen, um mit der sich ständig verändernden Technologieumgebung Schritt zu halten. Denn für Organisationen wird es immer schwieriger, neue IT-Spezialisten zu finden, die über das erforderliche Fachwissen verfügen, um die eigenen Systeme effektiv betreiben und warten zu können.

Mit der zunehmenden Komplexität der IT-Infrastruktur wird aber auch das IT-Monitoring immer wichtiger, denn dadurch wird der administrative Aufwand im IT-Betrieb deutlich entlastet. Für IT-Administratoren ist Monitoring inzwischen ein unverzichtbares Instrument für den reibungslosen Betrieb von IT-Systemen. Mit der technischen Unterstützung werden im Arbeitsalltag potenzielle Probleme frühzeitig erkannt und ein IT-Mitarbeiter kann proaktiv auf diese reagieren, bevor es im Produktiv-Betrieb zu größeren Störungen kommt. So werden Ausfallzeiten reduziert und die Verfügbarkeit von Systemen und Anwendungen verbessert.

DAMIT UNTERNEHMEN SCHNELL AUF IT-AUSFÄLLE REAGIEREN UND SYSTEME WIEDERHERSTELLEN KÖNNEN, IST EIN 360-GRAD-MONITORING WICHTIGER DENN JE.

Frank Laschet,
Global Produkt Marketing Manager,
USU Software AG, www.usu.com

Historisch gewachsene IT-Infrastrukturen

Gerade in Unternehmen, in denen eine Vielzahl von Anwendungen und Systemen eingesetzt werden, ist es wichtig, schnell auf Ausfälle oder Leistungsprobleme zu reagieren, um Geschäftsprozesse nicht zu beeinträchtigen

Deswegen nutzen viele IT-Abteilungen schon seit langem IT-Monitoring-Lösungen. Häufig vertraut man hierbei noch immer auf mehrere, nicht integrierte Monitoring-Insellösungen, die über die Jahre mit der IT-Infrastruktur gewachsen sind. In der Praxis werden so oftmals verschiedene Tools eingesetzt. Nicht selten finden sich bei großen, international agierenden Organisationen bis zu 20 solcher isolierten Überwachungssysteme, gerne auch über den gesamten Erdball verteilt. Diese sind meist –analog zur Ausweitung der IT-Infrastruktur – historisch gewachsen.

Ursachenfindung im Störungsfall erschwert

Der im Ernstfall so wichtige systemübergreifende 360-Grad-Blick ist bei diesem Überwachungsansatz nicht gegeben. Die Folgen können gravierend sein, denn die Ursachenfindung gestaltet sich in der Regel schwierig und ist sehr zeitraubend. Die Störungsbehebung verzögert sich im Ernstfall, da die einzelnen Systemadministratoren zunächst ihre eigenen Ansichten überprüfen. Außerdem lässt sich der Schweregrad einer Störung und die Auswirkung auf die Kunden und auf das eigene Business isoliert betrachtet meist nicht richtig einschätzen.

Um solche Situationen zu vermeiden, ist ein effektives IT-Monitoring für die Aufrechterhaltung der Geschäftskontinuität und die Bereitstellung von hochwertigen IT-Services heutzutage unerlässlich. Damit Unternehmen schnell auf IT-Ausfälle reagieren und Systeme wiederherstellen können, ist ein 360-Grad-Monitoring wichtiger denn je.

Hierbei handelt es sich um ein ganzheitlicher Lösungsansatz, mit dem über Jahre gewachsene heterogene Monitoring-Insellösungen durch ein übergeordnetes, einheitliches und umfassendes Monitoring zusammengeführt werden. Infolgedessen liefert ein 360-Grad-Monitoring eine einzigartige Möglichkeit, die IT-Umgebung mit nur einer einzigen Lösung vollständig im Blick zu haben. Bei einem Problem in der IT-Infrastruktur werden vom Monitoring-Tool Zusammenhänge automatisch erkannt, abgebildet, bewertet und gezielt ein Sammelticket für den zuständigen Fachbereich erstellt. Damit lassen sich nicht nur die Aufwände und die Anzahl der Tickets innerhalb eines Unternehmens reduzieren, Bearbeitungszeiten verkürzen und Kosten senken, sondern auch die Risiken von Systemausfällen und Compliance-Verletzungen werden minimiert.

Was eine ideale Lösung leisten sollte

Eine gute Lösung führt über Jahre gewachsene heterogene Monitoring-Insellösungen durch ein übergeordnetes, einheitliches und umfassendes Monitoring zusammen, bietet die volle Informationstransparenz und liefert den Systemadministratoren und den IT-Verantwortlichen in Echtzeit alle Daten, um physikalische und virtuelle Ressourcen sowie die Integration von Cloud-Applikationen und Cloud-Services unterschiedlichster Anbieter in die eigene IT-Infrastruktur erfolgreich planen und steuern zu können. Zusätzliche Alarmierungsfunktionen ermöglicht den operativen Teams, Service-Ownern und dem Management eine schnelle Reaktion von überall und sorgen im Störungsfall für eine schnelle Fehlerbehebung.

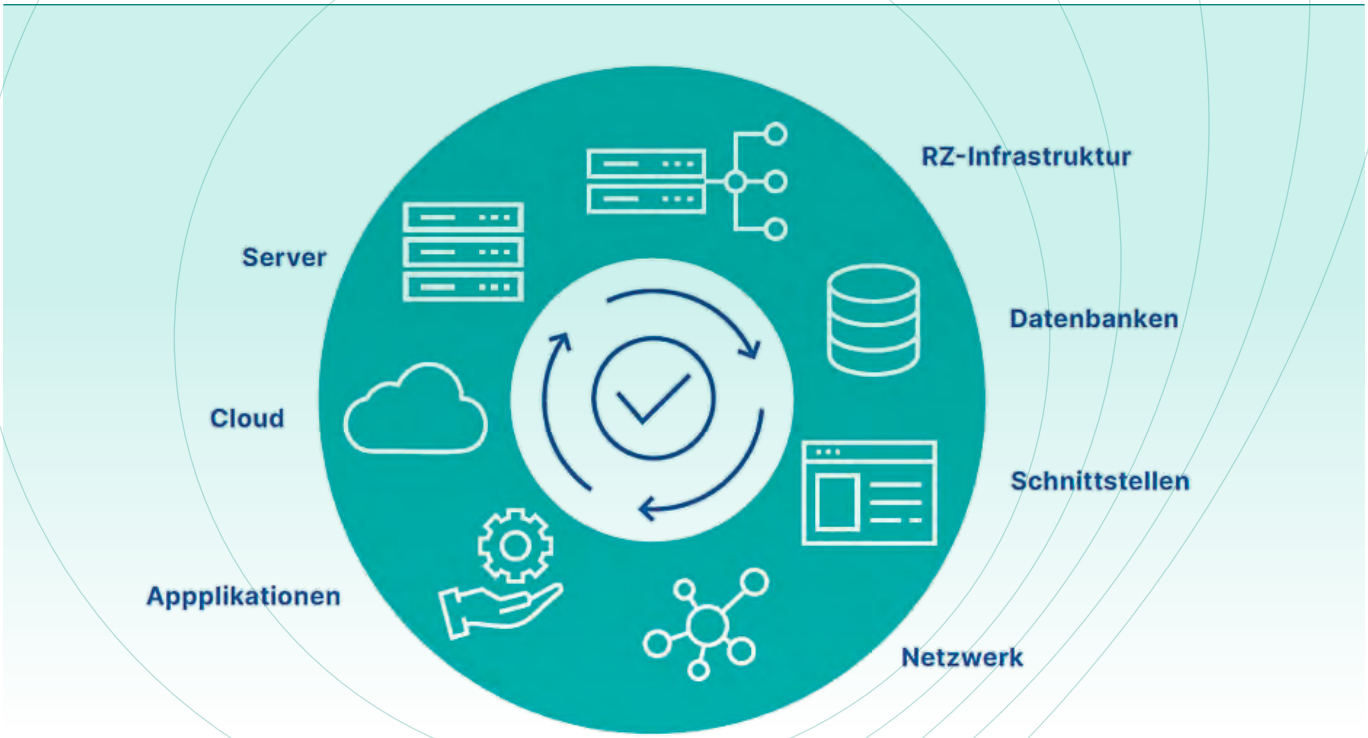
Voraussetzung für ein effizient funktionierendes 360-Grad-Monitoring ist die Integrationsfähigkeit des Systems. Ein weiterer zentraler Aspekt ist die flexible Skalierbarkeit – gerade angesichts moderner dynamischer IT-Infrastrukturen mittels Cloud Computing. Ein entsprechendes System muss in der Lage sein, kurzfristig und automatisiert zum Beispiel 30 neue Webserver zu überwachen.

Fazit

Moderne IT-Infrastrukturen umfassen oft eine Vielzahl von Systemen und Anwendungen, die miteinander verbunden sind. Daher ist es entscheidend, dass Unternehmen ein effektives IT-Monitoring-System implementieren, um sicherzustellen, dass alle Komponenten der Infrastruktur gut zusammenarbeiten. 360-Grad-Monitoring bietet an dieser Stelle einen ganzheitlichen Lösungsansatz, mit dem über Jahre gewachsene heterogene Monitoring-Insellösungen durch ein übergeordnetes, einheitliches und umfassendes Monitoring zusammengeführt werden. Diese einzigartige Möglichkeit ermöglicht Unternehmen die eigene IT-Umgebung vollständig im Blick zu haben. So lassen sich nicht nur die Betriebs- und Systembetreuungskosten senken, sondern vor allem auch das Risiko von Systemausfällen und Compliance-Verletzungen minimieren.

Frank Laschet

360-GRAD-ÜBERWACHUNG ALLER SYSTEME MIT EINER EINZIGEN IT-MONITORING-LÖSUNG



ITSM der Zukunft

UNTERNEHMENSWEITE PROZESSOPTIMIERUNG

Da IT-Umgebungen immer komplexer werden und ihre geschäftskritische Bedeutung wächst, gewinnt auch ein leistungsstarkes IT-Service-Management (ITSM) stetig an Bedeutung. Hinzu kommt der Wunsch nach mehr Agilität im gesamten Unternehmen, was den Einsatz neuer IT-Lösungen zur Prozessoptimierung in weiteren Abteilungen erfordert. Cloud- und SaaS-Provider wie Atlassian stellen sich diesen Herausforderungen: Sie bieten Tools, die sowohl die konventionellen ITSM-Prozesse unterstützen als auch die notwendige Flexibilität für den Einsatz in weiteren Unternehmensbereichen bieten. Die Integration und Anpassung an die Geschäftsprozesse erfolgt in der Regel durch externe ITSM-Experten – in enger Zusammenarbeit mit den IT-Teams der Unternehmen.

Die digitale Transformation schreitet in deutschen Unternehmen stetig voran und ITSM-Software wird immer wichtiger für die effiziente Prozessgestaltung. Dabei fällt auf: Herkömmliche ITSM-Lösungen können die neue IT-Welt häufig nur begrenzt abbilden und schwierig in bestehende Infrastrukturen anderer Geschäftsbereiche integriert werden. Denn die meisten ITSM-Tools sind – wie ihr Name verrät – stark auf konventionelle IT-Frameworks wie ITIL zugeschnitten, um die klassischen Aufgaben von IT-Teams zu unterstützen. Doch dadurch fehlt den Tools oft die nötige Flexibilität, um sie auch in anderen Geschäftsbereichen zur Durchführung digitaler Prozesse einzusetzen. Um Entwickler-, IT-, Ops- und Business-Teams wie HR oder Finance besser zusammenzubringen, werden jetzt alte Silos aufgebrochen und ganzheitlich überdacht. Ein gutes Beispiel dafür ist die Weiterentwicklung von ITIL und die unternehmensweite Adaption von digitalen Prozessen aus der IT.

ITIL 4: ITSM-Framework weiter gedacht

ITIL soll Unternehmen helfen, sich an die laufende Transformation und Skalierung anzupassen. Allerdings weist das konventionelle ITIL einige Schwächen auf: Gemeint ist die Überregulierung von IT-Services, die IT-Prozesse verlangsamt und somit agiles Arbeiten erschwert. Die neueste Version der ITIL-Standards – ITIL 4 – berücksichtigt diese Kritikpunkte und sorgt für einen Quantensprung des Ansatzes. Flexible Zusammenarbeit, Einfachheit und Feedback, kombiniert mit geschäftlichem und Kundennutzen, stehen hier im Mittelpunkt. Statuten, die in vielen Geschäftsbereichen wichtig sind und durchaus ähnlich organisiert sein können. Für die optimale Umsetzung braucht es jedoch das richtige Tool, das genug Flexibilität bietet und die Prozesse umfassend unterstützt. Christopher Mohr, CSO des ITSM-Specialized Atlassian Solution Partner Jodocus, setzt sich täglich mit diesen Ansprüchen auseinander: „Entwickelt für IT-Teams bieten unsere Tools, inbesondere Jira Service Management, die Unterstützung für nahezu alle ITSM-Prozesse. Darüber hinaus können wir die Tools für

spezifische Anwendungsfälle und Nutzen konfigurieren, sodass sie sogar unternehmensweit kollaborativ einsetzbar sind."

Jira Service Management als All-in-one-Lösung?

Jira Service Management (JSM) von Atlassian ist für eine breite Palette an ITSM-Prozessen – angelehnt an ITIL – zertifiziert. So deckt das Tool einige der wichtigsten ITSM-Prozesse out-of-the-box ab. Dazu zählen unter anderem das

- Incident-Management,
- Problem-Management,
- Change-Management,
- Service-Request-Management

und weitere.

Dabei arbeitet JSM nahtlos mit anderen Atlassian-Tools wie Jira Software, Confluence und Bitbucket zusammen und bietet Unternehmen die Möglichkeit, ihre gesamten Entwicklungs- und Support-Zyklen zentriert zu verwalten. Genauso können nahezu alle IT-gestützten Prozesse in „nicht-IT-Teams" mit den Tools realisiert werden, etwa die Finanzbuchhaltung, Bewerbungsverfahren, Sales Services und weitere.

Zahlreiche IT-gestützte Prozesse optimieren

„Durch Anpassungsoptionen, wie benutzerdefinierte Felder, Workflow-Regeln und automatisierte Aktionen, kann JSM zur Optimierung von Workflows und Prozessen auch außerhalb von IT-Teams eingesetzt werden. Eben überall dort, wo Prozesse durch IT unterstützt werden", fasst Christopher Mohr zusammen. Dieses unternehmensweite Weiterdenken von ITSM-Prozessen wird im Atlassian-Umfeld "Enterprise-Service-Management" (ESM) genannt. Dabei stehen ITSM und ESM nicht in Konkurrenz zueinander, sondern ergänzen sich optimal. Einige Anwendungsbereiche von JSM außerhalb der IT-Teams – also im ESM – sind zum Beispiel:

- **Human Ressources:**
Verwaltung von HR-Tickets, Lohnabrechnung, Mitarbeiterdaten und Onboarding

- **Rechtsabteilung:**
Verarbeitung von Verträgen, Anfragen zu Rechtsstreitigkeiten und Datenschutzanfragen

- **Finanzabteilung:**
Administration von Rechnungsstellung, Zahlungsanfragen, Budgetmanagement und Buchhaltungsprozessen

- **Kundensupport:**
Verwaltung von Serviceanfragen, Beschwerden, Rücksendungen und Rückerstattungen

- **Sales:**
Organisation von Verkäufen, Kundendaten, Kampagnen und Akquise-Aktionen

Die Vielseitigkeit von JSM spiegelt sich neben den zahlreichen Einsatzgebieten entsprechend auch in den Funktionen des Tools wider. So ermöglicht die Plattform automatisierte Workflows zur Ticket-Verwaltung, Analysen, integrierte Wissensdatenbanken und die Echtzeit-Kommunikation. Vor allem letztere, kombiniert mit einer zuverlässigen Verfügbarkeit, ist in unternehmenskritischen Fällen von großer Bedeutung, etwa bei Major Incidents.

MIT DEN ATLASSIAN TOOLS, BESONDERS MIT JSM, KÖNNEN WIR NAHEZU ALLE GESCHÄFTSPROZESSE DIGITAL ABBILDEN UND OPTIMIEREN.

Christopher Mohr, CSO, Jodocus GmbH, https://jodocus.io

Cloud-basiertes ITSM

Sobald ein Major Incident ausgerufen wird, muss es schnell gehen – und vor allem müssen Prozesse funktionieren. Cloud-basierte ITSM-Tools können hier die Rettung sein: Sie sind skalierbar, bieten SLAs mit einer hohen Verfügbarkeit und sind ortsunabhängig bedienbar. So können Incident-Management-Teams innerhalb kürzester Zeit von überall auf das System zugreifen und zusammen schnellstmöglich eine Lösung entwickeln. Jan Szczepanski, CMO von Jodocus, fasst zusammen: „Cloud-basierte ITSM-Tools ermöglichen eine schnelle, flexible und effektive Incident-Response und unterstützen maßgeblich dabei, verheerende Auswirkungen zu minimieren."

Integration von ITSM-Tools im gesamten Unternehmen

Ob bei Major Incidents oder im täglichen Arbeitszyklus: Unternehmen brauchen heutzutage Tools, um sämtliche IT-gestützte Prozesse einheitlich zu managen – im besten Fall mit einem bereichsübergreifenden Service Management Tool. Auf diese Weise werden gleiche und serviceübergreifende Workflows mit IT-Tools vereinheitlicht, digitalisiert und weitestmöglich automatisiert. Jira Service Management bietet eine Plattform, die zahlreiche ITSM-Prozesse out-of-the-box unterstützt und flexible Anpassungsoptionen für weitere Business-Service-Prozesse bietet. Für den Support und die damit verbundene optimale Nutzung der Software, hat der Anbieter ein Partnerprogramm eingeführt. Die Solution Partner wie Jodocus sind ausgewiesene Produktexperten und unterstützen Unternehmen unter anderem bei der Produktkonfiguration, Anpassung von Lösungen und der Implementierung der Tools sowie beim Lizenzmanagement. „Unsere Erfahrung hat uns gezeigt, dass fast alle Service-Prozesse in JSM realisierbar sind. Das treibt uns an, weiter mit dieser Lösung zu arbeiten, sie gemeinsam mit unseren Kunden immer wieder zu challengen und zu bestätigen", schließt Christopher Mohr ab.

Vincent Effertz

Quelle: TOPdesk

Automatisierung

OPTIMIEREN SIE IHREN SERVICEDESK IN 5 EINFACHEN SCHRITTEN

Abläufe zu automatisieren, ist heute ein wichtiger Trend für IT-Abteilungen. Dadurch lassen sich richtig eingesetzt, Anfragen beim IT-Servicedesk um mehr als 40 Prozent reduzieren. Leerlaufzeiten für Mitarbeiter und Kunden (Melder) können verringert werden. Ein guter Start zur Automatisierung sind diese 5 IT-Aufgaben.

#1 Incidents mit KI registrieren

Für jede IT-Abteilung ist es wichtig, Incidents korrekt zu registrieren, zu priorisieren und zuzuordnen. Das kostet sehr viel Zeit. Zum Glück kann die Künstliche Intelligenz (KI) dabei assistieren. Indem die KI Wissen aus der Datenbank Ihrer IT-Abteilung zieht, kann sie den Registrierungsprozess vereinfachen und Vorschläge für geeignete Kategorisierungen oder anwendbare SLAs machen. Bearbeiter begehen weniger Fehler und haben mehr Zeit für Ihre Melder. Außerdem können neue IT-Mitarbeiter so schneller eingearbeitet werden.

#2 Aufgaben einfach zuordnen

Zusätzlich zur Incidentregistrierung wird durch die KI auch die Zuordnung von Aufgaben viel einfacher. Auf der Grundlage früherer Incidents schätzt die KI ein, wie lange die Lösung eines bestimmten Incidents dauern wird. So kann die KI Aufgaben gemäß dem Wissensstand der Bearbeiter und deren Verfügbarkeit zuordnen. Sollte ein Bearbeiter merken, dass er für eine Stunde nichts zu tun hat, schlägt die KI beispielsweise eine Aufgabe vor, die voraussichtlich eine Stunde dauern würde.

#3 Einfache Anfragen mit Chatbots lösen

„Wie wähle ich mich in das WiFi der Organisation ein, wie füge ich ein geteiltes Postfach hinzu oder wie verbinde ich meinen Laptop mit einem Drucker?" Fragen wie diese dürften Ihrer IT-Abteilung sehr bekannt vorkommen. Wäre es nicht toll, wenn die Melder selbstständig Antworten zu diesen Fragen finden könnten?

Mit einem Self Service Portal oder einem Chatbot können Sie genau das. Ein Chatbot kann die Fragen der Melder mithilfe von Spracherkennung und dem Fachwissen Ihrer IT-Abteilung verstehen und ihnen die entsprechenden Antworten liefern. Das Beste daran? Chatbots sind nicht an Ihre üblichen Bürozeiten gebunden, was in Anbetracht der steigenden Serviceerwartungen wichtig ist.

#4 Bearbeitung wiederkehrender Aufgaben automatisieren

Bearbeiter wissen, dass wiederkehrende Aufgaben zu den Schattenseiten Ihres Berufs gehören. Sie benötigen viel Zeit und Aufwand. Außerdem verursachen sie Kosten. Betrachten wir das Zurücksetzen von Passwörtern als Beispiel: Forrester schätzt die durchschnittlichen Kosten für das Zurücksetzen eines Passworts auf 70 Dollar. Automatisierung ist die Lösung für leidige Aufgaben wie das Zurücksetzen von Passwörtern. Wiederkehrende Aufgaben zu automatisieren kann die beim Servicedesk eingereichten Incidents um mehr als 40 Prozent verringern.

#5 Onboarding und Offboarding vereinfachen

Beginnt ein neuer Mitarbeiter, sorgt die IT-Abteilung dafür, dass alle benötigte Hardware, Software und die erforderlichen Berechtigungen zur reibungslosen Arbeit vorhanden sind. Ebenso liegt es an ihr, Zugriffsrechte zu entfernen und herauszufinden, welche Assets von einem Mitarbeiter, der das Unternehmen verlässt, genutzt wurden, und wo diese sich jetzt befinden. Diese Prozesse können Sie durch Automatisierung stark vereinfachen. Neue Mitarbeiter erhalten direkt Zugriff auf alle benötigten Systeme, um am ersten Arbeitstag loszulegen. Nach dem gleichen Prinzip kann ein automatisierter Offboarding-Prozess schnell und einfach Konten und Zugriffsrechte einschränken.

An dem On- und Offboarding von Mitarbeitern sind aber auch die HR-, Facility- und andere Serviceabteilungen beteiligt. Mithilfe von automatisierten Workflows wissen alle Abteilungen was wann zu tun ist.

www.topdesk.de

Erfahren Sie mehr über Service Excellence

iStock | demaerre

Work-Experience

DEN DIGITALEN ARBEITSPLATZ OPTIMIEREN

MitarbeiterInnen gewinnt und hält man mit guter Work-Experience. Um sich von der Konkurrenz abzuheben, reicht es aber nicht aus, die neuesten Tools zu implementieren. Erst wenn Unternehmen die richtige Balance zwischen Technologie und Organisationsstruktur finden, können sie die Work-Experience signifikant verbessern.

Das bestätigt auch eine neue Studie von Harvard Business Review Analytic Services, die die größten Herausforderungen für gute digitale Work-Experience in den Bereichen Design, Überfrachtung, Integration und Leadership sieht.

In der Vergangenheit designten IT-Abteilungen umständliche Tools, ohne genau zu verstehen, was Teams erledigen müssen und wie sie diese Aufgaben angehen. Um dies zu vermeiden, nutzen Unternehmen mittlerweile Ansätze wie Design Thinking und agile Problemlösungen. Damit stellen sie sicher, dass digitale Tools relevant, nützlich und einfach zu bedienen sind. Bei der Entwicklung der Tools sollte deshalb sowohl Input von NutzerInnen als auch von ExpertInnen einbezogen werden, um die Experience beim Einsatz zu optimieren.

Überfrachtung entsteht, wenn Mitarbeitende Lösungen und Services verschiedenster Anbieter einsetzen müssen, die alle unterschiedliche Interfaces haben und nicht kompatibel sind. Intranets und Wissensmanagementsysteme helfen den Teams dabei, sich zurechtzufinden und benötigte Informationen zu finden.

MitarbeiterInnen sind der Schlüssel zur Wertschöpfung eines Unternehmens. Darum sollten Unternehmen ihr Augenmerk auf die Work-Experience legen, um die besten Talente zu gewinnen und auch zu halten. Das gelingt mit Software, die die Leute lieben.

Gabriel Frasconi | www.freshworks.com

freshworks

Datenkompetenz
Daten erfolgreich Nutzen

Prof. Dr. Michael Lang (Hrsg.), Carl Hanser Verlag GmbH & Co.KG; 06/2023

DATENKOMPETENZ

DATEN ERFOLGREICH NUTZEN

Durch den digitalen Wandel entstehen immer mehr Daten, die für die Geschäftstätigkeit genutzt werden können. Für Unternehmen ergeben sich damit enorme Chancen und Risiken zugleich. Somit ist es für den zukünftigen Erfolg von Unternehmen entscheidend, wie gut es ihnen gelingt, relevante Daten zu sammeln, diese systematisch auszuwerten, daraus wertvolle Erkenntnisse abzuleiten und diese für die Geschäftstätigkeit zu nutzen.

Die zentrale Grundlage dafür ist, dass die Mitarbeitenden des Unternehmens die erforderlichen Kompetenzen für eine erfolgreiche Nutzung von Daten besitzen.

M&A in der Digitalbranche

DIE KRISE ALS „NEW NORMAL"

Covid19 und Post-Pandemic-Restart, der Krieg in der Ukraine, Energie- und Klimakrise, dazu Lieferkettenprobleme, Zinsanstieg, Inflation – Krisen sind das „New Normal" und Unternehmer müssen sich fast täglich neuen Herausforderungen stellen. Finanzinvestoren sondieren ihre Targets deutlich genauer als noch zu den Boom-Zeiten in den letzten drei Jahren. Doch was genau bedeutet das für Verkäufer? Wurde die Chance verpasst, in den M&A-Markt einzusteigen?

Der globale M&A-Markt reagiert empfindlich auf Krisen und Konjunkturschwankungen. Das haben die letzten Jahre deutlich gezeigt. Sicher ist derzeit nur, dass nichts sicher ist. Krisen seien das New Normal, doch könnten durchaus Lehren aus der jüngsten Vergangenheit gezogen werden, meint Ralf Heib, Geschäftsführer matchIT. „Große Deals wurden während der Corona-Hochphase sehr häufig und auch schnell gestoppt", erklärt der erfahrene M&A-Berater. „Transaktionen im KMU-Bereich, also im sogenannten Small- und MidCap-Markt, verhalten sich hingegen deutlich resilienter gegenüber der Krise." Es dürfe nicht vergessen werden, dass dem eine lange Phase des Wachstums und der Stabilität voraus ging. Zuletzt hatte es eine ungewöhnlich hohe Nachfrage nach IT-Unternehmen gegeben. Der Verkäufermarkt dominierte das M&A-Geschehen. Aktuell findet das Käufer/Verkäufer-Verhältnis zu einer stärkeren Balance zurück. Die Analyse von Ralf Heib: „Wir kommen aus einem etwas überhitzten Verkäufermarkt, jetzt beginnen sich die Marktbedingungen etwas zu verschieben: Käufer sondieren ihre Targets wieder genauer und bemessen sie an den eigenen Geschäftsmodellen."

Digitalisierung weiterhin starker Nachfragetreiber

Legt man den M&A-Fokus auf die Digitalbranche, so sorgt dort weiterhin der Megatrend der Digitalisierung für durchaus stabile Nachfrageverhältnisse. Immer wieder neue Treiber pushen den Markt, trotz oder gerade wegen der anhaltenden Krisenstimmung. So löste der Ukraine Krieg zuletzt eine starke M&A-Nachfrage für den Bereich Cyber-Security aus. Und auch Resilienz-Themen wie Nachhaltigkeit/ Sustainability oder Green IT sorgen aktuell für sehr viel Dynamik am Digitalmarkt.

Zudem ist auch der Fachkräftemangel gerade in der IT-Branche ein zusätzlicher

VORGEHENSMODELL ZUM UNTERNEHMENSVERKAUF

Strategie- und Such-Phase

- Verkaufsstrategie
- Update Story und Business Plan
- Teaser
- Exposé
- Long List
- Auswahl und Kontaktierung geeigneter Kaufinteressenten
- Matching (Shortlist)

Verhandlungsphase

- Non-Disclosure-Agreement (NDA)
- Management-Präsentation
- Indikatives Angebot
- Letter of Intent
- Datenraum
- Due Dilligence
- Vertragsverhandlung
- Vertragsabschluss

Integrationsphase

- Integrationsstrategie
- Integrations-Masterplan
- Change & Culture Management
- Integrations-Tracking & Controlling

Treiber für das M&A-Geschäft. „Das M&A-Geschehen im IT-Sektor zeigt sich nach wie vor vital und generiert gerade bei Small- und MidCap-Unternehmen weiterhin einen hohen Deal Flow", so die Erfahrung des match.IT-Geschäftsführers Ralf Heib. „Potentielle Verkäufer sollten allerdings im Hinterkopf behalten, dass die Käufer vorsichtiger geworden sind und Multiples noch genauer bewerten. Sie müssen sich deshalb gezielt auf den Verkaufsprozess vorbereiten – am besten mit einer genau auf die Käufergruppe abgestimmten Verkaufsstrategie." Die Story ist also ausschlaggebend. Sie sollte möglichst gute Argumente zur Zukunftsfähigkeit eines Unternehmens enthalten. „Aus Sicht des Eigentümers müssen potentielle Käufer sein Unternehmen wahrnehmen können, sie müssen die Vision dahinter verstehen. Im Kern geht es darum, welcher unmittelbare Nutzen aus dem Kauf generiert werden kann."

Wer eine gute Story verkaufen will, muss jedoch genau wissen, an wen sich diese richtet. Nach Ralf Heib positionieren sich derzeit mindestens fünf verschiedene Investorentypen am M&A-Markt. Mit 75-80 Prozent sind die strategischen Investoren (aus der eigenen Branche) die dominanteste Käufergruppe für mittelständische IT-Unternehmen. Dies können sowohl nationale als auch internationale Investoren sein. Aber zunehmend suchen auch Finanzinvestoren wie Private Equity-Gesellschaften oder Family Offices verstärkt nach Investitionen im IT-Sektor. Und auch Non-IT-Investoren, also IT-Anwendungsunternehmen aus unterschiedlichen Branchen haben mittlerweile vermehrt Interesse am Kauf von IT-Unternehmen. Und letztendlich kommen auch Personen des Managements als mögliche Käufer in Nachfolgesituationen in Frage.

Dreistufiges Vorgehensmodell für M&A-Projekte im IT-Sektor

Laut den Experten von match.IT lässt sich der Unternehmensverkauf in drei Phasen unterteilen: Die Strategie- und Suchphase, die Verhandlungsphase und die Integrationsphase.

> WER HEUTE SEIN IT-UNTERNEHMEN ERFOLGREICH VERKAUFEN WILL, BENÖTIGT EINE KLARE, ZUKUNFTSFÄHIGE VISION, GEPAART MIT EINEM REALISTISCHEN, NACHVOLLZIEHBAREN BUSINESS-PLAN.
>
> **Ralf Heib, Geschäftsführer, match.IT GmbH, www.match-it.biz**

Die erste Phase umfasst die Verkaufsstrategie. Hier wird die Story für den Marktangang entworfen und der Business-Plan abgestimmt. Die Verhandlungsphase beinhaltet zunächst das Durchführen von Management-Präsentationen gegenüber den Investoren, welche intensiv vor- und nachbereitet werden müssen. Zu einem definierten Meilenstein werden diese Investorenkandidaten dann aufgefordert, erste indikativen Angebote abzugeben. Anschließend wählt der Verkäufer das Angebot aus, das seiner Meinung nach am besten ist, und beginnt in der Regel auf der Grundlage eines Vorvertrags (Letter of Intent) einen exklusiven Verhandlungsprozess mit dem ausgewählten Unternehmen. Bereits mit der Verhandlungsphase beginnt der fließende Übergang zur Integrationsphase. In dieser dritten Phase geht es dann um die Integration des verkauften Unternehmens in die bestehende Unternehmenslandschaft des Käufers.

Die Auswahl des finalen Bieters ist also ein mehrstufiger Prozess. Den anonymen Teaser erhalten am Anfang vielleicht 25-50 Bieter. Herausgefiltert werden dann diejenigen, die sich am ehesten für ein Gespräch eignen. Indikative Angebote geben dann etwa noch drei bis fünf Bieter ab. Erst wenn ein Bieter übriggeblieben ist, wird diesem die gesamte Datenlage in einem virtuellen Datenraum offenbart, sodass man entsprechend einer Due Diligence in ganz konkrete Vertragsverhandlung gehen kann. „Länger als sechs bis neun Monate sollte ein solcher Verkaufsprozess nicht andauern, sonst wird auch das Management zu lange von der operativen Arbeit abgehalten", rät Ralf Heib.

Der ganze Transaktionsprozess kann auch mit Blick auf den Unternehmenswert als Value Chain bezeichnet werden. In der Strategie- und Suchphase sowie in der Verhandlungsphase geht es um die Wertermittlung des Unternehmens, ab der Integrationsphase steht dann die Werterhaltung und -realisierung im Vordergrund.

Erfolgsfaktoren für den Verkauf in Krisenzeiten

Wer heute sein IT-Unternehmen erfolgreich verkaufen will, benötigt eine klare, zukunftsfähige Vision, gepaart mit einem realistischen, nachvollziehbaren Business-Plan. Eine M&A-Transaktion hat darüber hinaus immer sehr viel mit konkreten Zahlen zu tun: Verkäufer müssen ihre eigenen Zahlen beherrschen und verstehen, wie sie die Profitabilität ihres Unternehmens gegenüber den Käufern transparent machen. Dazu gehören auch saubere Bilanzen und GuV-Rechnungen. „Wir erleben häufig die Situation, dass gerade kleinere Unternehmen sehr steueroptimierend agieren und dann natürlich keine beeindruckende Profitabilität in den Büchern vorweisen können", erklärt Ralf Heib. „Hier bedarf es dann guter Argumente gegenüber dem Käufer, am besten mithilfe des Steuerberaters."

Gerade für kleinere Unternehmen ist es wichtig, den potentiellen Käufern eine überlebensfähige Organisation aufzuzeigen. „Verkauft wird am Ende die Zukunft eines Unternehmens, nicht die Vergangenheit", bringt es Ralf Heib auf den Punkt.

Ralf M. Haaßengier

Monte Carlo-Analysen in der IT

INNOVATION DURCH SIMULATION – EINE KURZE EINLEITUNG

In der Business-Welt gibt es viele Möglichkeiten, die Zukunft vorauszusagen. Die bekannteste davon ist neben der Glaskugel das Hopecasting. Auf der Basis der aktuellen Zahlen und des Wachstums errechnet man die wichtigsten Kennzahlen für das nächste Geschäftsjahr. Etwas zielgerichteter geht es bei Prognose (eher mittelfristig) und Forecasting (eher kurzfristig) zu. Dies wird meist in der operativen Unternehmensplanung und -steuerung eingesetzt. Budgets für Umsätze, Kosten, Gewinne und Liquidität werden so ständig angepasst.

Bei Monte Carlo denkt man erst einmal unwillkürlich an das Thema Glücksspiel. Zahlreiche Erfindungen und Innovationen sind durch Zufall oder Glück entstanden. Andere hingegen durch Systematik. Die bekannteste Simulationsmethode ist die Monte Carlo-Simulation (auch als Szenarioanalyse bekannt). Die Simulation bietet die unglaubliche Möglichkeit „If-Then-Else"-Szenarien durchzuspielen und die Wirklichkeit zu testen.

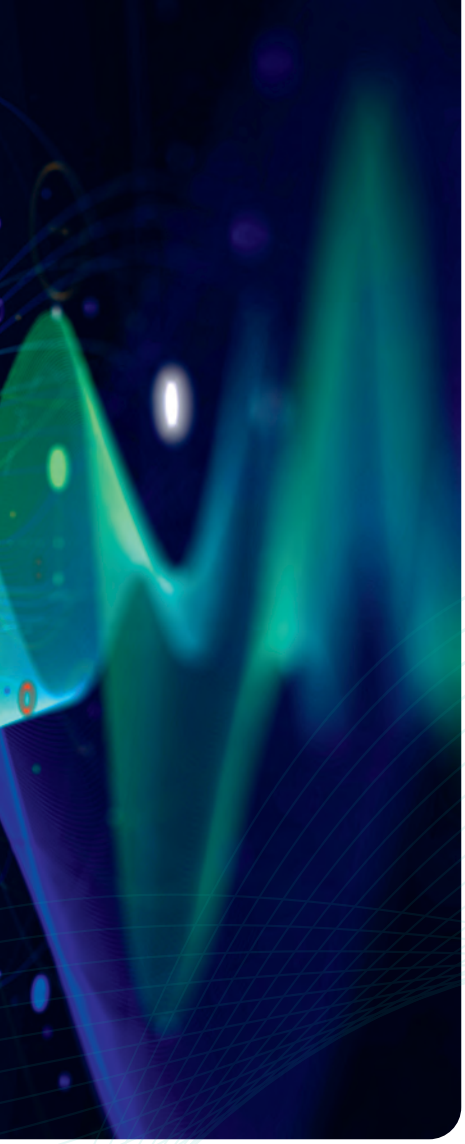
Unternehmen werden oft mit Problemen konfrontiert, bei denen es schwierig ist, eine genaue Vorhersage zu treffen, weil es viele variable Faktoren gibt oder die Anwender nicht wissen, wie verschiedene Komponenten sich untereinander beeinflussen. Die Idee einer Monte Carlo-Simulation besteht nun darin, unterschiedliche Szenarien oder Variablenkonfigurationen auszuprobieren und zu verstehen, wie sich die Ausgabe ihres Modells verändert.

Predictive-Szenarien

Und wo liegt der Unterschied zu Predictive-Szenarien? Predictive Analytics (PA) verwendet Daten, um zukünftige Ereignisse vorherzusagen. Im Allgemeinen werden historische Daten verwendet, um ein mathematisches Modell zu erstellen, das wichtige Trends berechnet. Dieses prädiktive Modell (voraussagendes Model) wird dann auf aktuelle Daten angewendet, um vorherzusagen, was als Nächstes passieren wird, oder um Aktionen vorzuschlagen, mit denen optimale Ergebnisse erreicht werden können. PA wird in den letzten Jahren zunehmend im Controlling für Planung & Simulation eingesetzt, vor allem in den Bereichen von Big Data und Machine Learning. Mehr Informationen dazu bietet der Blog von Rainer Pollmann auf der Website prt.de

Verwendung von Monte-Carlo-Methoden

Zu Beginn des Artikels haben wir die Unterschiede von Hopecasting, Forecasting, Predictive-Verfahren und Monte-Carlo Analysen beschrieben. Für die verschiedensten Einsatzgebiete gibt es zahlreiche Tools. Unabhängig davon, welches Tool Sie verwenden, umfasst das Monte-Carlo-Verfahren drei grundlegende Schritte, die IBM auf seiner Website gut beschrieben hat (ibm.co/3IW1Ehs).



Richten Sie das Vorhersagemodell ein, indem Sie sowohl die abhängige Variable, die vorhergesagt werden soll, als auch die unabhängigen Variablen (auch als Eingabe-, Risiko- oder Vorhersagevariablen bezeichnet) angeben, die die Vorhersage steuern werden.

Geben Sie Wahrscheinlichkeitsverteilungen der unabhängigen Variablen an. Verwenden Sie historische Daten und/oder das subjektive Urteil des Analysten, um einen Bereich von wahrscheinlichen Werten zu definieren und jedem eine Wahrscheinlichkeitsgewichtung zuzuweisen.

Führen Sie wiederholt Simulationen durch und erzeugen Sie dabei zufällige Werte für die unabhängigen Variablen. Tun Sie dies so lange, bis Sie genügend Ergebnisse gesammelt haben, um eine repräsentative Stichprobe aus der nahezu unendlichen Anzahl möglicher Kombinationen zu bilden.

Sie können so viele Monte-Carlo-Simulationen ausführen, wie Sie möchten, indem Sie die zugrunde liegenden Parameter ändern, die Sie für die Datensimulation verwenden. Sie werden jedoch auch den Variationsbereich innerhalb einer Stichprobe berechnen wollen, indem Sie die Varianz und die Standardabweichung berechnen, die allgemein verwendete Maße für die Streuung sind. Die Varianz einer gegebenen Variablen ist der Erwartungswert der quadrierten Differenz zwischen der Variablen und ihrem Erwartungswert. Die Standardabweichung ist die Quadratwurzel der Varianz. In der Regel werden kleinere Varianzen als besser angesehen.

ANWENDUNGSGEBIETE

Wo findet sie in der IT Anwendung?

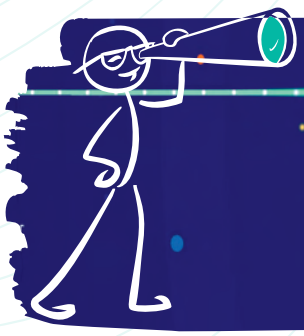
Beispiel 1:
Alteryx. Diese Analytics Automation Platform bietet eine End-to-End-Automatisierung von Analysen, Machine Learning und Data Science-Prozessen und beschleunigt so die digitale Transformation. Dort gibt es ein Tool zur „Simulation der Stichprobennahme". Es nimmt parametrisch Datenstichproben von einer Verteilung, von Eingabedaten oder als Kombination, die am besten für eine Verteilung passt. Die Daten können auch „gezeichnet" werden, wenn Sie sich bei den Parametern einer Verteilung nicht sicher sind und Daten fehlen. Dieses Tool verwendet R als Programmiersprache. R gibt es seit 1992. Es handelt sich um eine freie Programmiersprache, die vornehmlich für statistische Berechnungen und Grafiken entwickelt wurde. Die Syntax orientiert sich an der Programmiersprache S, mit der R weitgehend kompatibel ist, und die Semantik an Scheme.

Beispiel 2:
Regelwerk von UiPath, einer Plattform für die Robotic Process Automation, kurz RPA. Dort kommt quasi eine abgespeckte Variante zur Geltung: Regel: If-Then-Else: bit.ly/41QFpCk

Die Zukunft der Simulationen

Soweit so gut. Echtzeitdaten, Predictive Maintenance und Analytics, Monte Carlo-Simulationen, noch stellt sich die Frage nicht, aber schön zu wissen wäre: kommt danach noch etwas? Die Antwort: sicher! Dazu muss man einen Blick in die Zukunft werfen. Mit genau dieser Thematik beschäftigen sich Zukunftsforscher wie die von 2b Ahead. Und das Fazit ihres Think Tanks lautet: KI und Quantencomputer werden die Ära der Echtzeitdaten überholen, quasi in Lichtgeschwindigkeit und ein neues Zeitalter einläuten, nämlich das der Predictive Economy. In der werden uns Waren geliefert, bevor wir erkennen, dass wir sie benötigen. Spannende Zeiten stehen uns bevor, auch wenn es noch ein paar (wenige) Jahre dauert.

Ulrich Parthier | www.it-daily.net



MEHRWERT

Monte Carlo Analysen in der IT:

- Google-Suche: **bit.ly/3Jef4Hg**
- YouTube: **bit.ly/3F2gu5c**
- Podcast: **apple.co/3L0fQJk**

Videos

- Wahrscheinlichkeit und Monte Carlo-Simulation: **bit.ly/3SOiaF7**
- Monte Carlo-Simulation mit Excel: **bit.ly/3ILiPlO**
- Monte-Carlo-Simulation von Tests: **bit.ly/3KY9sC2**

Planspiele

WARUM ÜBERHAUPT SIMULATIONEN?

Die Errechnung von Erwartungswerten ist oft fehlerbehaftet. In der IT werden Planungen und Forecasting deshalb oft als Hopecasting bezeichnet. Grundlage sind meist Excel-Tabellen. Doch wozu gibt es Software? Durch die Monte-Carlo-Simulation erhält man durch eine große Anzahl an Zufallsexperimenten belastbare Ergebnisse der Quantifizierung. Dadurch können empirische Quantile (etwa der Schaden übersteigt in 95 Prozent der Zufallsexperimente den Wert x nicht) ermittelt werden.

Hierbei ist oft gewünscht, verschiedene Verteilungsfunktionen anwenden zu können. Die am häufigsten nachgefragten Verteilfunktionen sind:

- Binomialverteilung
- Poisson-Verteilung
- Dreiecksverteilung
- PERT-Verteilung
- Gleichverteilung
- Weibull-Verteilung

Moderne Softwaresysteme besitzen eine vollintegrierte Monte-Carlo-Simulation, die unter anderem in Aktivitäten per Button oder in Reports genutzt werden kann. Werfen wir einen Blick auf die Vorteile am Beispiel des Anwendungsfalles GRC (Governance, Risk & Compliance) und was so eine Lösung können sollte.

- Die Simulation soll integraler Bestandteil der Lösung sein.
- Die Auswahl von Verteilungsfunktionen sowie die quantitativen Bewertungen sollen für Anwender durch entsprechende Hilfestellungen intuitiv ermöglicht werden.
- Anwender sollen gezielt erforderliche Risikoinformationen für die Monte-Carlo-Simulation abfragen können.
- Die Analysemöglichkeiten der Gesamtrisikosituation des Unternehmens soll verbessert werden.
- Es sollen belastbare, entscheidungsrelevante Informationen zur Gesamtrisikosituation des Unternehmens für das Management verfügbar werden.
- Der gesamte Risikomanagement-Prozess inklusive der Monte-Carlo-Simulation soll abgebildet werden.
- Quantitative Risikoanalysen können ohne Zwischenschritte für Benutzer oder Datenexporte durchgeführt werden.
- Die Monte-Carlo-Simulation ist auf allen Unternehmensebenen nutzbar.

Die Monte-Carlo-Simulation

Fakt ist, dass für viele Unternehmen eine rein qualitative Bewertung nicht mehr zeitgemäß ist. Der Trend bewegt sich zunehmend in Richtung quantitativer Bewertung und das meist in Vorbereitung für die Anwendung von Simulationsverfahren. Was sind die Vorteile:

- Durch Quantifizierung und Simulation werden Risiken und Maßnahmen in der „Sprache der Unternehmensleitung" kommunizierbar – in monetären Werten.
- Durch Simulationen erhält man belastbarere Ergebnisse als bei der Be-

trachtung des Erwartungswerts, da Ergebnisse nicht als ein absoluter Wert, sondern als Quantile dargestellt werden.

- Durch moderne CPUs und Parallelisierbarkeit, können auch Simulationen in einer hohen Anzahl an Zufallsexperimenten mit vertretbarer Rechenzeit durchgeführt werden.
- Die Ergebnisse der Simulation erlauben es, verschiedene Optionen, Handlungsmöglichkeiten und mögliche Konsequenzen im Rahmen einer Entscheidungsfindung zu beachten.
- Durch zusätzliche Auswertungs- und Visualisierungsmöglichkeiten (etwa Histogramme und Boxplots) können Zusammenhänge und Auswirkungen für das Management nachvollziehbar visualisiert werden.
- Ansätze wie gewichtete Spearman-Korrelationen bieten die Möglichkeit zu einer Rangordnung der signifikantesten Risiken zu gelangen.
- Szenarioanalysen wie Risk Stressing ermöglichen Worst-Case-Szenarien in Bezug auf einzelne Risiken zu untersuchen.
- Maßnahmenoptimierung ermöglicht eine Kosten-Nutzen-Rechnung anhand des Risikoappetits des Unternehmens.

Herausforderungen

Wo liegen die Fallstricke? Oft fehlt es an Basiswissen im Bereich Quantifizierung/Monte-Carlo-Simulation sowohl bei Risikoverantwortlichen in der 1st Line of Defense (LoD) als auch bei Risikokoordinatoren in der 2nd LoD. Die Hürden bei der flächendeckenden Quantifizierung von Risiken erschweren zudem die Arbeit von Risikomanagern. Eine qualitative Einordnung von Risiken (zum Beispiel durch eine Matrix) fällt Risikoverantwortlichen leichter als eine Quantifizierung (etwa mittels 3-Punkt-Bewertung). Oftmals herrscht auch mangelndes Bewusstsein für die konkrete Bedeutung/Auswirkung von Verteilungen und Eintrittswahrscheinlichkeiten.

Qualifizierte Risiken können zwar einzeln betrachtet, aber nicht summiert werden (beispielsweise über Organisationseinheiten, Regionen oder Risikokategorien). Der Fokus liegt daher überwiegend auf der Betrachtung von Einzelrisiken. Es fehlt somit eine aussagekräftige Darstellung des Risikoportfolios und der Gesamtrisikosituation für die Entscheidungsträger im Unternehmen (Management/Geschäftsführung/Vorstand/Aufsichtsrat). Sie führen darüber hinaus zu Anlass-Entscheidungen zu einzelnen Risiken, anstatt Entscheidungen über Maßnahmenbudgets in der Gesamtsicht zu treffen.

Die Darstellung von Einzelrisiken für den Vorstand/Aufsichtsrat aus dem Risikomanagementprozess heraus bringen in der Regel wenig neue Erkenntnisse, da sie den Empfängern meist bereits über andere Wege kommuniziert wurden.

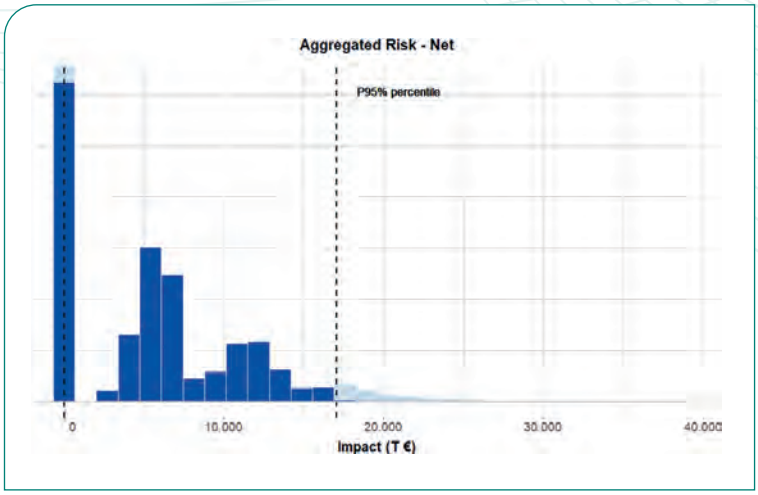
Die Ergebnisse der Monte-Carlo-Simulations-gestützten Risikoanalyse sind für Vorstände häufig nicht verständlich und erkenntnisgebend, weil sie keinen direkten, belastbaren Bezug zu deren Kern-Steuerungsinstrumenten haben (Geschäftszahlen).

Die Nutzung der Monte Carlo Simulation bleibt wenigen Experten vorbehalten (meist zentralen Konzern-Risikomanagern). Es bestehen Berührungsängste mit dem Thema Simulation als „Blackbox" und es fehlt an Know-how/Experten-Wissen über die Bedeutung der Monte-Carlo-Simulations-Ergebnisse. Die Ergebnisse von Simulationen werden in den meisten Fällen nur auf Konzernebene berichtet und nicht auf unterschiedlichen Ebenen (etwa den Abteilungen) genutzt.

Durch die Quantifizierung von Risiken kann Risikomanagement einen Beitrag zu Planung, Budget und Jahresabschluss liefern. Allerdings ist dies aufgrund der Entkopplung des Risikomanagements häufig nicht der Fall (Stichwort: Silofunktion). Risiken (wie etwa das Eintreten einer Pandemie!) werden von Vorständen häufig als unrealistisch abgetan, weil die Eintrittswahrscheinlichkeit entsprechend gering ist. Vorsorge für solche Fälle zu leisten ist häufig schwer argumentierbar. Dem Risikomanagement fehlen Instrumente und Wissen, wie Ergebnisse der Risikosimulationen für das Management aufbereitet und verständlich kommuniziert werden müssen.

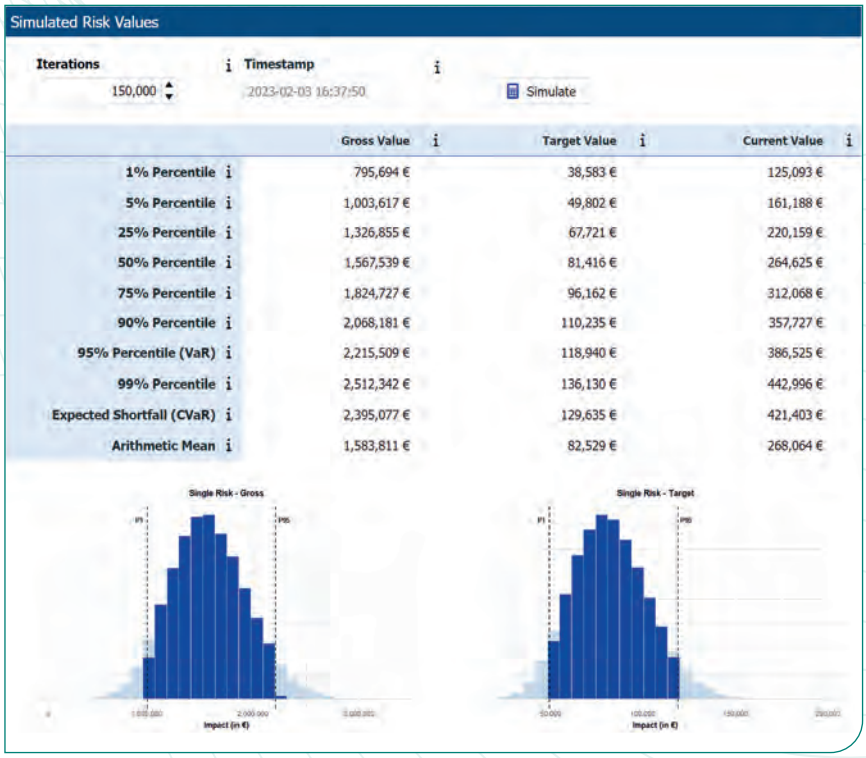
Auswertungsmöglichkeiten

Durch die Monte-Carlo-Simulation erhält man zusätzliche Auswertungsmöglichkeiten. Es können beispielsweise VaR (Value at Risk) und Expected Shortfalls (Conditional Value at Risk) errechnet werden. Durch die Ergebnisse der Zufallsexperimente erhält man die Möglichkeit zahlreicher Darstellungsformen (wie Boxplots, Histogramme, Dichteplots), welche einen neuen Einblick ins Risikomanagement ermöglichen.



Für die technische Umsetzung für das Simulieren verwenden Programme wie BIC die Programmiersprache R, die als eine der Standardsprachen für statistische Problemstellungen gilt.

Anwendungsfall 1:
Einzelrisikosimulation
Das Ziel ist die Bestimmung von Stichprobenquantilen (Überschreitungswahrscheinlichkeit) bei einem einzelnen Risiko. Dazu wird die Eintrittswahrscheinlichkeit des Risikos mit der Poisson- oder Binomialverteilung bestimmt, je nachdem, ob ein mehrfaches Eintreten möglich ist. Tritt das Risiko ein, wird der Schaden mit einer wählbaren Verteilung ermittelt (standardmäßig wird die PERT-Verteilung verwendet). Dieses Beispiel zeigt, dass in 95 Prozent aller simulierten Fälle (bei vollständig umgesetzten Risikomaßnahmen) der Schaden 118,940 Euro nicht übersteigt.



VOR ALLEM DER EINSATZ EINER MEHRPERIODEN-SIMULATION IN VERBINDUNG MIT RISK LINKING BIETET DEN UNTERNEHMEN EINEN ERHEBLICHEN MEHRWERT, DER DIE KURZ- UND MITTELFRISTIGE PLANUNG DEUTLICH ERLEICHTERT UND ZU VALIDEREN ERGEBNISSEN FÜHRT ALS HERKÖMMLICHE METHODEN.

Marcin Fijalkowski,
Product Consultant/ R Developer/
Data Scientist, GBTEC Software AG,
www.gbtec.com

Zur Entscheidungsunterstützung bei der Planung und Freigabe wird eine Simulation der Maßnahme durchgeführt. Dabei wird das Risiko ohne Behandlung durch eine Maßnahme mit dem durch die Maßnahme geminderten Risiko verglichen und so die Wirkung der Maßnahme aufgezeigt. Es ist auch möglich, die Wirksamkeit einer Maßnahme während des Prozesses der Maßnahmenumsetzung zu simulieren.

Anwendungsfall 2:
Simulation des Risikoportfolios
Das Ziel ist die Bestimmung der Gesamtrisikoposition einer Organisation oder eines Teilbereichs durch die Zusammenfassung (Aggregation) von Einzelrisiken. Hinter der Aggregation steckt eine Monte-Carlo-Simulation mit konfigurierbaren Iterationen, die konfigurierte Verteilungsfunktionen auf eine quantitative Bewertung anwendet und ein Aggregationsergebnis liefert. Die grafische Verteilung des zu erwartenden Schadens kann mittels einfacher Charts visualisiert werden.

Anwendungsfall 3:
Korrelation
Das Ziel ist die Ermittlung eines Spearman-Korrelationskoeffizenten für Einzelrisiken und die Bestimmung einer Maßzahl (-1 bis 1) für den Grad des Zusammenhanges eines Risikos zum Aggregationsergebnis. Damit können die Einzelrisken ermittelt werden, welche den höchsten Anteil der Gesamtrisikoposition verursachen. Je höher die Maßzahl desto stärker ist der Einfluss des Einzelrisikos auf den Gesamtschaden. Per Grafik können dann die Einzelrisiken mit Priorisierung dargestellt werden

Anwendungsfall 4:
Risikotragfähigkeit
Das Ziel ist es, einen Vorschlag zu ermitteln, welche Maßnahmen umgesetzt werden sollten, um die vorgegebene Risikotragfähigkeit (etwa das 95 Prozent-Quantil der Gesamtschadensverteilung darf Euro x nicht überschreiten) bei möglichst geringen Kosten der Maßnahmen zu erfüllen. Die Simulation liefert ein Aggregationsergebnis, das nur die eingesetzten Maßnahmen berück-

sichtigt und zeigt, welche Maßnahmen umgesetzt werden sollten.

Anwendungsfall 5:
Maßnahmenoptimierung nach Budget
Das Ziel ist die Ermittlung eines Vorschlages, welche Maßnahmen unter Berücksichtigung des vorhandenen Budgets umgesetzt werden sollen. Als Bedingung werden die maximalen Kosten des Maßnahmenmanagements angegeben. Die Simulation liefert ein Aggregationsergebnis, welches nur die genutzten Maßnahmen berücksichtigt und zeigt auch hier, welche Maßnahmen umgesetzt werden sollten.

Anwendungsfall 6:
Mehrperioden-Simulation
Mit Hilfe dieser Simulation ist es möglich, ein Portfolio von Risiken mit einem kurz- und mittelfristigen Zeithorizont zu simulieren und zu aggregieren. Die Funktionalität ermöglicht sowohl die Risiko- als auch die Maßnahmenplanung und die Verfolgung der anfänglichen und wiederkehrenden Maßnahmenkosten.

Anwendungsfall 7:
Risikoverknüpfung / Verkettung
Es gibt kein Unternehmen, in dem die Risiken völlig unabhängig sind. Daher ist es notwendig, Risiken miteinander zu verknüpfen. Der Benutzer kann ein umfangreiches Netz von Abhängigkeiten zwischen Risiken erstellen und diese speichern. Bei der Aggregation von Einzelrisiken werden diese Beziehungen zwischen den Risiken berücksichtigt. Auf diese Weise kann das gesamte Risikoprofil eines Unternehmens modelliert werden.

Anwendungsfall 8:
Risk Stressing
Das Ziel ist es, die Auswirkung einzelner Risiken in Extremfällen auf die Gesamtrisikoposition zu ermitteln. Dafür können einzelne Risiken ausgewählt werden. Gestresst kann Eintritt (Risiko tritt immer ein) und Schaden (zum Beispiel >75 Prozent) werden. Zum Vergleich wird auch das reguläre Netto-Ergebnis dargestellt.

Zusammenfassung
Simulation ist der Weg, Risikomanagement praxisorientiert umzusetzen. Sie stellt den effektivsten Weg dar, dem Management ökonomische Implikationen von Risiken transparent zu machen. Simulation sorgt somit für deutlich fundiertere Entscheidungen und eine zielgenauere Planung von Maßnahmenbudgets.

Durch die Modellierung von Interdependenzen zwischen den Risiken kann die Simulation die betriebswirtschaftliche Realität für das Management deutlich besser abbilden.Mit Hilfe der Mehrperiodensimulation kann dies auch für die kurz- und mittelfristige Planung abgebildet werden.

Marcin Fijalkowski | www.gbtec.com

Für die Zukunft lernen

WIE MAN MIT DATEN VERGANGENES VERSTEHEN, IN DER GEGENWART STEUERN UND ÜBER DIE ZUKUNFT LERNEN KANN

In unserer schnelllebigen, globalisierten Welt besitzen selbst kleine Veränderungen im Gleichgewicht großes Hebelpotenzial auf die Steuerungsgrößen eines jeden Unternehmens. Entscheider stehen vor der großen Herausforderung, belastbare Einschätzungen über zukünftige Entwicklungen unter hoher Unsicherheit zu tätigen. Ist es da noch zeitgemäß, sich bei der Informationsbeschaffung vorrangig auf das menschliche Bauchgefühl zu verlassen?

Wie oft haben Sie sich über unbefriedigend ungenaue und doch ressourcenaufwendig generierte Bottom-up-Planzahlen geärgert, die – sobald die Hochrechnung erstmal abgeschlossen ist – schon wieder veraltet sind? Wenn Sie faktenbasierte Prognosen erhalten wollen, um auf einer objektiven Entscheidungsgrundlage die Weichen bestmöglich für die Zukunft Ihres Unternehmens zu stellen und Ressourcen dort einzusetzen, wo sie am ehesten gebraucht werden – dann können Predictive Analytics die richtige Antwort sein. Wir sind überzeugt: Mensch und Maschine ZUSAMMEN sind smarter – in diesem Artikel erklären die Experten von Deloitte, was das bedeuten kann.

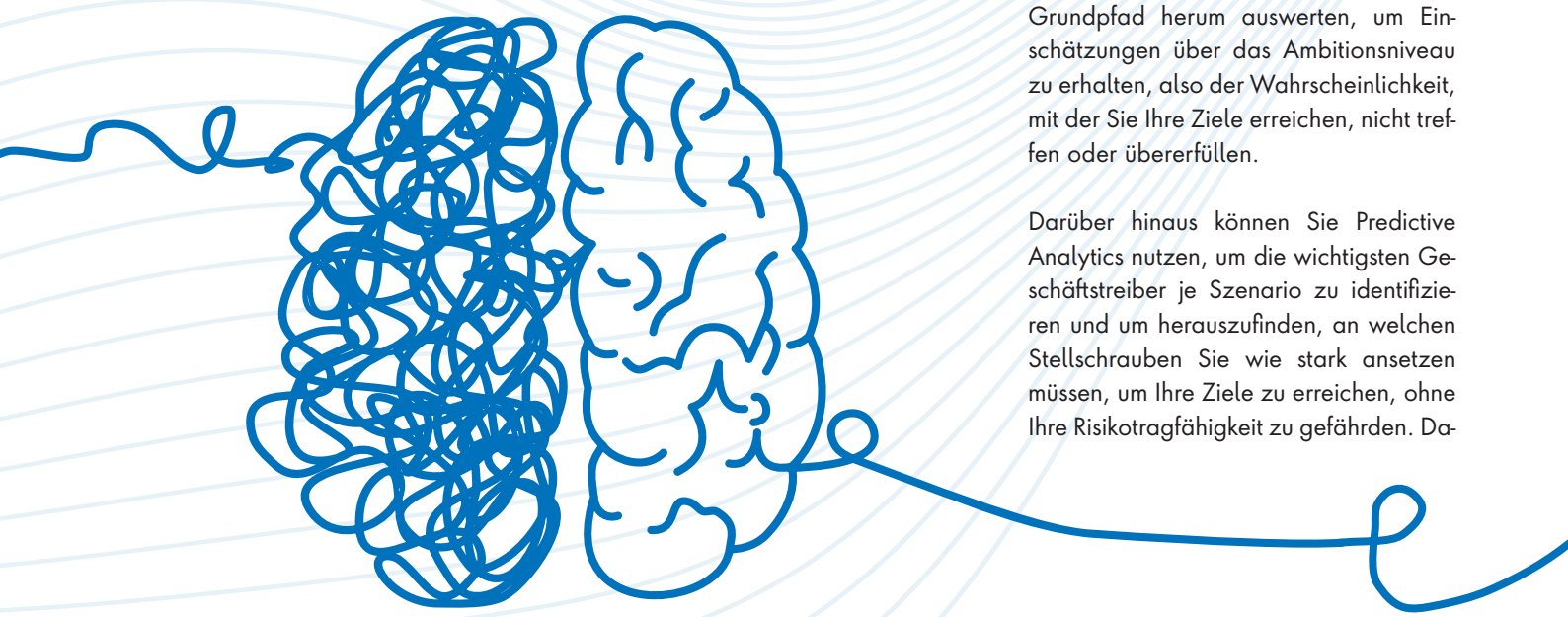
Fortschrittliche Prognosemethoden

Predictive Analytics ist eine algorithmengestützte analytische Verfahrensweise, in der man sich interne und externe Daten und deren Wechselwirkungen zunutze macht, um Erkenntnisse über zukünftige Entwicklungen zu gewinnen. Die Methode eignet sich dort, wo zukünftige Ausprägungen einer Zielgröße durch volatile Umweltbedingungen beeinflusst sind und findet dadurch häufig Anwendung in Planungsprozessen bei der Prognose wichtiger Unternehmenskennzahlen.

Ganz konkret können das der Cash-Flow, Umsatz, EBIT, die Absatzmenge einer Produktgruppe bis hin zur Abbildung der gesamten Gewinn- und Verlust- oder Kapitalflussrechnung sein. Im Vergleich zu traditionellen Planungsmethoden kann unter Einsatz von Predictive Analytics die Prognosegeschwindigkeit von mehreren Wochen auf ein paar Stunden reduziert werden. In vergangenen Projekten verbesserte sich die Vorhersagegüte signifikant bei deutlich reduziertem Ressourceneinsatz.

In jedem Planungsprozess gibt es gleich mehrere Ansatzpunkte, an denen Ihnen die Anwendung fortschrittlicher Prognosemethoden Mehrwert liefern kann. Im Fokus der Ausgangsanalyse steht die Gewinnung eines Verständnisses darüber, welche Faktoren zur aktuellen Situation geführt haben und was passieren würde, wenn man diesen Pfad weiter beschreitet. Ganz im Sinne einer Bandbreitenplanung können Sie Schwankungsbreiten, sogenannte Konfidenzbänder, um diesen Grundpfad herum auswerten, um Einschätzungen über das Ambitionsniveau zu erhalten, also der Wahrscheinlichkeit, mit der Sie Ihre Ziele erreichen, nicht treffen oder übererfüllen.

Darüber hinaus können Sie Predictive Analytics nutzen, um die wichtigsten Geschäftstreiber je Szenario zu identifizieren und um herauszufinden, an welchen Stellschrauben Sie wie stark ansetzen müssen, um Ihre Ziele zu erreichen, ohne Ihre Risikotragfähigkeit zu gefährden. Da-



bei agieren interne und externe Einflussgrößen – sogenannte Treiber – als Frühwarnindikatoren, die eine rechtzeitige Erkennung von Chancen und Risiken ermöglichen und – sobald gezielt in die Unternehmensplanung einbezogen – insgesamt eine deutlich größere Sicherheit in der Unternehmensentscheidung und -steuerung bieten.

Als Treiber eignen sich je nach Prognoseobjekt verschiedenste Mikro- und Makroinformationen, beispielsweise demographische Informationen, Steuerquoten, Produktionsindices, mit denen wir ein erstes Outside-in Modell erstellen. Um die Prognoseergebnisse weiter zu verbessern, reichern Sie diese Modelle idealerweise um unternehmensspezifische Faktoren, beispielsweise Einsatzgütermengen, Vertriebszahlen und Marktfaktoren an.

Natürlich können auch externe, qualitätsgesicherte Algorithmen in bestehende Systemarchitekturen eingebettet werden und unternehmensspezifische Daten über dynamische Schnittstellen in das Modell einfließen. Vorprogrammierte Algorithmen filtern und analysieren mittels Techniken aus dem Bereich Machine Learning (Artificial Intelligence) die für das jeweilige Geschäftsumfeld relevanten Treiber in Echtzeit heraus und geben Klarheit darüber, welche Inputgrößen relevante Wirkungsmechanismen in der Wertschöpfungskette auslösen.

> ENTSCHEIDER STEHEN VOR DER GROSSEN HERAUSFORDERUNG, BELASTBARE EINSCHÄTZUNGEN ÜBER ZUKÜNFTIGE ENTWICKLUNGEN UNTER HOHER UNSICHERHEIT ZU TÄTIGEN.
>
> **René Scheffler, Partner Deloitte, www.deloitte.de**

Einsatzgebiete

Viele Unternehmen nutzen bereits Predictive Analytics für Controlling- und integrierte GRC-Ansätze und erzielen dadurch deutlich höhere Planungs- und Budgetsicherheit sowie enorme Zeit- und Kosteneinsparungen. Sie schaffen Vertrauen mit transparenter und objektiver Datenanalyse und stärken so das Managements nach innen wie nach außen. Proof of Concepts sind hier hilfreich. Die Einsatzgebiete reichen von globalen Rollouts bis hin über die Vorhersage klassischer finanzieller Kenngrößen wie Umsatz und EBIT und weit darüber hinaus. Analytische Methoden zur Verringerung des Betrugsrisikos bei der Aufdeckung von Anomalien in Lagerbeständen können mit Predictive Analytics festgestellt werden, Qualität der Ressourcenplanung im öffentlichen Sektor kann verbessert werden oder Einschaltquoten für Mediensender oder Besucherzahlen einer Restaurant-Kette prognostiziert werden können.

Unternehmen erkennen so zunehmend den Mehrwert von Predictive Analytics zur Verbesserung der Planung und Risikoprognosen. Vorbehalte gegenüber neuen Technologien schwinden und Anforderungsprofile verändern sich, sodass auch in traditionellen Bereichen vermehrt Kenntnisse von Mathematik, Statistik und Ökonometrie erforderlich werden, um mit der Zeit Schritt zu halten.

Entdecken Sie die Mehrwerte von Advanced Analytics in Ihrem Umfeld und klären Sie, welche Use Cases vielversprechend sind. Ein schlanker Projektsprint zu ausgewählten Prognoseobjekten, um das Potenzial von Predictive Analytics zu erkunden, ist weniger aufwendig, als Sie es sich womöglich vorstellen können, und Resultate liegen bereits nach kurzer Zeit vor.

Bei dem Projektteam empfiehlt sich ein interdisziplinäres Team an Data Scientists, Finanz- und Branchenexperten, das so eine vollständige und erfolgreiche Integration von Predictive Analytics-Lösungen über alle Hierarchien des Geschäftsmodells hinweg ermöglicht. Von Vorteil ist eine externe Beratung, um die richtigen Ansätze, die Konzeption eines passgenauen Target Operating Models bis hin zur digitalen Transformation zu finden. Lassen Sie uns in Schritt zwei einen tieferen Blick in den Bereich Analytics werfen.

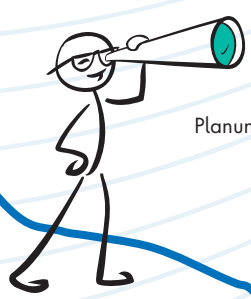
Risk Analytics Assurance

Beim Thema Risk Analytics Assurance geht es darum, die Steuerung der Risiken durch eine Wirkungsanalyse zu untersuchen und aufzuzeigen, wie hoch der Einfluss der jeweiligen Risiken auf das Gesamtportfolio ist. Dadurch können gezielte Maßnahmen für die einflussreichsten Risiken ermittelt werden.

Denn eine zentrale Herausforderung unternehmerischer Entscheidungen ist das Abwägen von Erträgen und Risiken. Welches zusätzliche Risiko entsteht durch eine neue Investition? Und reichen die finanziellen Mittel, um dieses Risiko abzudecken? Risikomanagement ist mittlerweile weitaus mehr als die Erfüllung von regulatorischen Anforderungen. Vielmehr muss die Unternehmenssteuerung in der Lage sein, Risikoinformationen, die die Unsicherheit des Geschäftsumfeldes abbilden, in unternehmerische Entscheidungen mit einzubeziehen. Hierbei kann Risk Analytics Assurance einen wertvollen Beitrag leisten.

Unser Umfeld ist stetig im Wandel – aktuell aber ganz besonders stark, nicht nur durch Globalisierung und Digitalisierung. Sich rasant verändernde Rahmenbedingungen und eine zunehmende Wettbewerbsintensität erschweren die Erreichung der gesetzten Strategie und der damit verbundenen Ziele. Ein vorausschauender Umgang mit Risiken gewinnt immer mehr an Bedeutung. Über Risk Analytics können Risiken in die Unternehmenssteuerung miteinbezogen werden. Dies ermöglicht unter anderem, Investitionen unter Risikotragfähigkeitsaspekten zu bewerten und bereits vor der Entscheidungsfindung die daraus resultierende Auswirkung auf das zukünftige Risikoportfolio zu kennen.

Risk Analytics generiert dabei, durch Data Analytics gestützt, tiefergehende Analysen. Die dabei genutzten Methoden können zum einen die einzelnen Phasen des Risikomanagementprozesses bei der Informationsgewinnung unterstützen. Zum anderen können die generierten Steuerungsinformationen über den direkten Risikomanagementprozess hinaus, etwa bei Investitionsentscheidungen oder in deren Planung, Einzug finden. Diese beiden Optionen – innerhalb und außerhalb des Ri-



PLUS

Planung im digitalen Zeitalter
bit.ly/3ZIAxxi

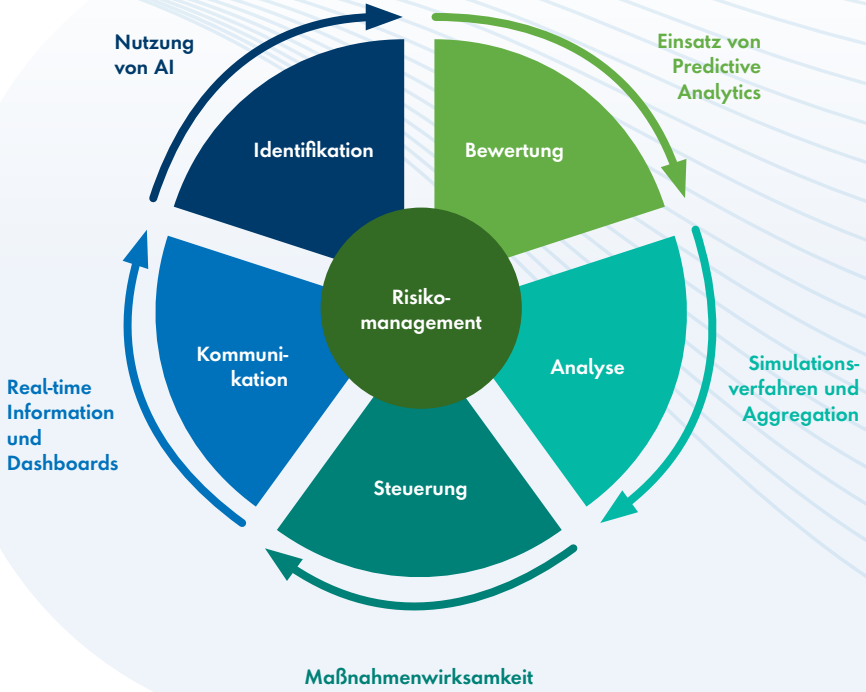
Predictive Analytics & Forecast Assurance
bit.ly/42Kdkx1

sikomanagementprozesses – werden im Folgenden näher beschrieben.

Risk Analytics Assurance unterstützt Sie innerhalb der einzelnen Phasen des Risikomanagementprozesses, beispielsweise:

Artifical Intelligence kann bei der Identifikation von Risiken dienen. Mögliche Anwendungsgebiete sind hier etwa das automatisierte Durchsuchen von Nachrichten oder Social-Media Posts.

Der Einsatz von Predictive Analytics unterstützt hingegen die Bewertung von Risiken. Dabei ermöglichen historische Daten sowie die Zuhilfenahme externer Daten die Vorhersage über Veränderungen von Planungsrisiken wie etwa Stahlpreise, Währungsschwankungen.



Innerhalb der Analysephase erfolgt die Bestimmung des Gesamtrisikos sowie der Risikotragfähigkeit. Risk Analytics unterstützt dabei durch den Aufbau und die Überprüfung von Modellen zur Ermittlung der kumulierten Wirkung verschiedener Risiken.

Schließlich ermöglicht Risk Analytics Assurance die Steuerung der Risiken durch eine Wirkungsanalyse, die aufzeigt, wie hoch der Einfluss der jeweiligen Risiken auf das Gesamtportfolio ist. Dadurch können gezielte Maßnahmen für die einflussreichsten Risiken ermittelt werden.

Letztlich unterstützen Echtzeit-Informationen die Kommunikation der Risiken. Interaktive Dash-boards sorgen dabei für eine empfängerorientierte, dynamische Visualisierung.

Unterstützung von Unternehmensentscheidungen

Risk Analytics dient jedoch nicht nur zur Bewertung und Steuerung der Unsicherheit innerhalb des direkten Risikomanagementprozesses. Es ermöglicht ebenfalls die Berücksichtigung der Unsicherheit in Unternehmensplanung und -entscheidungen. Denkbar ist dabei eine Spanne von einfachen Szenario- und Aggregationsmethoden bis hin zu fortgeschrittenen ökonometrischen Modellen, die Planungspositionen in Bandbreiten betrachten oder prognostizieren.

Der nächste Schritt: Von Analytics zu Monte-Carlo

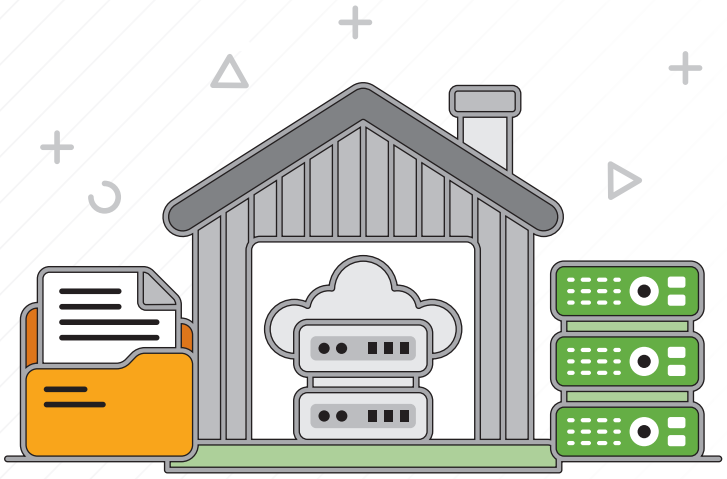
So gelingt es zum Beispiel durch den Einsatz einer Monte-Carlo-Simulation Risiken und Chancen als Konfidenzintervall zu sehen. Dies repräsentiert, zugeordnet zu Planungspositionen, ebenfalls das Risiko- und Chancenvolumen – und damit die Unsicherheit – innerhalb einer Planungsposition und erhöht die Prognosegenauigkeit. Auch die Zuhilfenahme von Risiko-Ertrags-Betrachtungen auf Investitions- oder Bereichsebene kann Unternehmensentscheidungen risikobasiert stützen.

Die beschriebenen Risk-Analytics-Assurance-Lösungen erzeugen Risikoinformationen, die der Unternehmenssteuerung und Verbesserung der Prozesseffizienz dienen. Dies ermöglicht es, Unsicherheiten in unternehmerischen Entscheidungen zu berücksichtigen und bereits vor der Entscheidung Veränderungen des Risikoumfangs einzuschätzen. Dabei generiert Risk Analytics u. a. einen positiven wirtschaftlichen Beitrag durch die Erhöhung von Transparenz, die Senkung von Kapitalkosten und den Aufbau resilienter Strategien.

René Scheffler

ANFORDERUNGEN AN MODERNE DATA WAREHOUSES

PREIS, LEISTUNG UND DIFFERENZIERTE FUNKTIONEN



Ein aktueller Report von Fivetran beschäftigt sich intensiv mit den Eckdaten führender DWHs. Das Unternehmen unterstützt Anwender Daten aus Hunderten von SaaS- und On-Premises-Datenquellen in Cloud-Destinationen zu zentralisieren, zu transformieren und für Analysen zu nutzen. Über die Ergebnisse des Reports sprach Ulrich Parthier, Publisher it management mit Data-Management-Experte George Fraser, CEO bei Fivetran.

Ulrich Parthier: *Worin genau sehen Sie Ihre Mission?*

George Fraser: Fivetran bietet Data Pipelines, die Daten aus Apps, Datenbanken und File Stores in die Data Warehouses von Kunden synchronisieren. Was wir in diesem Zusammenhang am häufigsten gefragt werden: „Welches Data Warehouse ist für uns das richtige?"

Um diese Frage besser beantworten zu können, haben wir uns mit Brooklyn Data Co. zusammengetan, um die Geschwindigkeit und die Kosten von fünf der beliebtesten Data Warehouses zu vergleichen: Amazon Redshift, Snowflake, Google BigQuery, Databricks und Azure Synapse.

Ulrich Parthier: *Wie sind die Test durchgeführt worden?*

George Fraser: Bei Benchmarks geht es darum, eine Auswahl zu treffen: Um welche Art Daten geht es? Um wie viele Daten handelt es sich? Welche Art von Abfragen werden durchgeführt? Es kommt sehr stark darauf an, auf welcher Basis diese Entscheidungen getroffen werden: Wenn sich die Form der Daten oder die Struktur der Abfragen ändert, kann das schnellste Warehouse im Nu zum langsamsten werden. Wir haben versucht, diese Auswahl so zu gestalten, dass durch sie ein typischer Fivetran-Nutzer abgebildet wird.

Ulrich Parthier: *Wie definieren sie einen typischen Nutzer?*

George Fraser: Ein typischer Nutzer würde beispielsweise Daten aus Salesforce, JIRA, Marketo, Adwords und seine Oracle-Produktionsdatenbank in seinem Data Warehouse synchronisieren. Diese Datenquellen sind nicht sehr groß: Eine übliche Quelle enthält normalerweise einige zehn bis hundert Gigabyte. Allerdings sind sie vergleichsweise komplex: Sie enthalten hunderte normalisierte Tabellen, und unsere Kunden fassen diese Daten mithilfe komplexer SQL-Abfragen zusammen.

Ulrich Parthier: *Welche Abfragen wurden durchgeführt?*

George Fraser: Wir haben von Mai bis Oktober 2022 insgesamt 99 TPC-DS-Abfragen durchgeführt. Diese Abfragen sind komplex: Sie umfassen viele Join-Operationen, Aggregationen und Unterabfragen. Wir haben jede Abfrage nur einmal durchgeführt, um zu verhindern, dass das Warehouse vorhergehende Ergebnisse zwischenspeichert. Die Abfragen wurden sequenziell, eine nach der anderen, ausgeführt, was sich von einem typischen realen Anwendungsfall unterscheidet, bei dem viele Benutzer-Abfragen gleichzeitig ausgeführt werden.

Ulrich Parthier: *Vergleiche sind immer schwierig, da nicht alle Produkte über identische Funktionen, Preisgebilde oder Releasestände verfügen.*

PLUS

Den kompletten Data Warehouse-Report können sie kostenlos hier abrufen:
bit.ly/3Jq5Bwp

George Fraser: Richtig, Kostenvergleiche zwischen verschiedenen Systemen sind in der Tat schwierig, da jedes System unterschiedliche Funktionen bietet, mit denen sich die Kosten senken lassen. Folgende Vorteile werden beispielsweise in diesen Zahlen nicht widergespiegelt:

- Databricks Spot-Instance-Preise
- Automatische Skalierung von Snowflake-Multiclustern
- BigQuery On-Demand-Preise

Diese und andere plattformspezifische Funktionen können zur Kostensenkung bei vielen Aufgaben eingesetzt werden. Man muss also das jeweilige Einsatzgebiet prüfen.

Ulrich Parthier: *Wie wurden die Warehouses optimiert?*

George Fraser: Die betrachteten Data Warehouses bieten erweiterte Funktionen wie Sortierschlüssel, Clustering-Schlüssel und Datenpartitionierung. Wir haben für die Zwecke dieses Benchmark-Tests keine dieser Funktionen verwendet. Wir haben Spaltenkompressionscodierung bei Redshift und Spaltenspeicherindizierung bei Synapse angewendet. Snowflake, Databricks und BigQuery wenden die Kompression automatisch an.

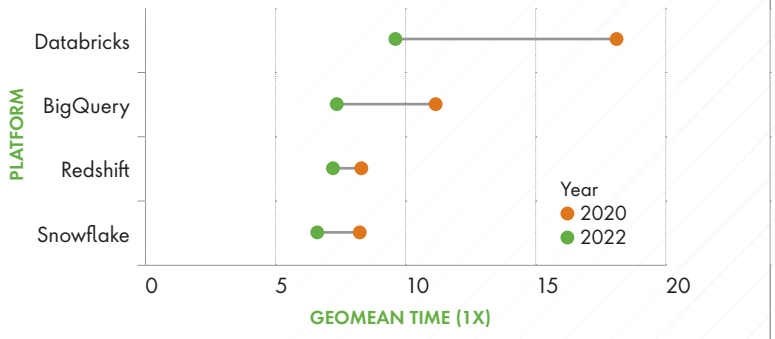
Ulrich Parthier: *Und wie sah die Performance aus?*

DIE LEISTUNG ALLER SYSTEME HAT SICH IN DEN LETZTEN ZWEI JAHREN VERBESSERT.

George Fraser, CEO Fivetrain
www.fivetran.com

George Fraser: Alle Warehouses wiesen eine hervorragende Ausführungsgeschwindigkeit auf und eignen sich für interaktive Ad-hoc-Abfragen. Eine kleine Einschränkung gibt es: Die Leistung von Redshift ist sehr anfällig für Cache-Fehler im gemeinsamen Abfragekompilierungs-Cache. Dies hat zu einer gewissen Zufälligkeit in unseren Ergebnissen geführt und bewirkt, dass Redshift nicht die gleichen Kompromisse zwischen Kosten und Leistung aufwies wie andere Systeme. Zur Berechnung der Gesamtkosten haben wir die Laufzeit mit den Kosten der Konfiguration pro Sekunde multipliziert.

Ulrich Parthier: *Wie stark hat sich die Leistung verbessert?*



Im Vergleich zu demselben Benchmark-Test 2020 hat sich die Leistung aller Systeme verbessert, die größte Steigerung hat Databricks erzielt. (Quelle: Fivetran)

George Fraser: Wir haben 2020 denselben Benchmark-Test durchgeführt. Die Leistung aller Systeme hat sich in den letzten zwei Jahren verbessert. Databricks hat dabei die größten Verbesserungen erzielt, was nicht überraschend ist, da sie ihre SQL-Ausführungs-Engine komplett umgeschrieben haben.

Ulrich Parthier: *Wie lautet ihr Fazit?*

George Fraser: Alle getesteten Warehouses punkten mit hervorragender Leistung und fairen Preisen. Dass sie sich sehr ähnlich sind, überrascht nicht: Die grundlegenden Techniken zum Aufbau eines schnellen spaltenorientierten Data Warehouse sind spätestens seit der Veröffentlichung der C-Store-Studie 2005 hinreichend bekannt. Solche Data Warehouses nutzen zweifelsohne die Standardtaktiken zur Steigerung der Performance: spaltenorientierte Speicherung, kostenbasierte Abfrageoptimierung, Ausführungs-Pipelines und Just-in-time-Kompilierung. Benchmark-Tests, die extreme Geschwindigkeitsunterschiede von Data Warehouses als Ergebnis präsentieren, sind mit Vorsicht zu betrachten.

Die wichtigsten Unterschiede zwischen Warehouses bestehen in den durch ihre Designansätze bedingten Qualitätsunterschieden: Einige Warehouses sind auf Optimierungsmöglichkeiten ausgelegt, andere auf Benutzerfreundlichkeit. Bei der Bewertung von Data Warehouses sollten Unternehmen mehrere Systeme berücksichtigen und jenes auswählen, das die für sie erforderliche Ausgewogenheit mitbringt.

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

TEIL 1 VON 4

End-to-End Datenmanagement

MODERNER ANSATZ: ORGANISCH GEWACHSEN UND VOLLSTÄNDIG INTEGRIERT

Daten bilden die Grundlage für Entscheidungen, Prozesse und Analysen.Veraltete, nicht vollständige, oder sogar falsche Daten beeinflussen den Erfolg des Unternehmens negativ. Es kann zu fehlerhaften Entscheidungen, verlangsamten oder ineffizienten Prozessen, dem Verlust von Vertrauen und schließlich zu enormen Konkurrenznachteilen kommen. Umso wichtiger ist damit das Datenmanagement beziehungsweise eine effektive Datenverwaltung und die sichere Datennutzung für den signifikanten Einfluss auf das Unternehmen. Dies sind nur einige Gründe, warum korrekte und aktuelle IT-Daten so wichtig sind:

#1 **Entscheidungsfindung:** Daten bilden die Basis für fundierte Entscheidungen und ermöglichen Trends, Muster und Verhaltensweisen zu identifizieren.

#2 **Prozessoptimierung:** Durch die Analyse von Daten können interne Prozesse optimiert und automatisiert werden, das spart Zeit und verringert den Einsatz von Ressourcen.

#3 **Kundenerfahrung:** Gesammelte Daten können genutzt werden, um dem Kunden personalisierte Erfahrungen zu bieten, indem man erst individuelle Bedürfnisse erkennt und daraufhin berücksichtigt.

#4 **Compliance:** Es gibt viele nationale und internationale rechtliche Anforderungen, die bei einer Missachtung zu hohen Risiken und verbundene Geldstrafen führen können.

Natürlich gibt es noch andere Gründe, doch schon diese vier gelisteten Gründe beeinflussen den eigenen Vorteil gegenüber dem Wettbewerb enorm. Ein effektives Datenmanagement, also die Verwaltung von Daten, schafft einen Wettbewerbsvorteil, indem man interne Prozesse optimiert und so schneller und bessere Entscheidungen als die Konkurrenz treffen kann.

IRI VORACITY IST EINE ORGANISCH GEWACHSENE UND VOLLSTÄNDIG INTEGRIERTE SUITE FÜR DEN KOMPLETTEN DATENLEBENSZYKLUS, UM DEN MAXIMALEN WERT AUS DATEN ZU ERZIELEN.

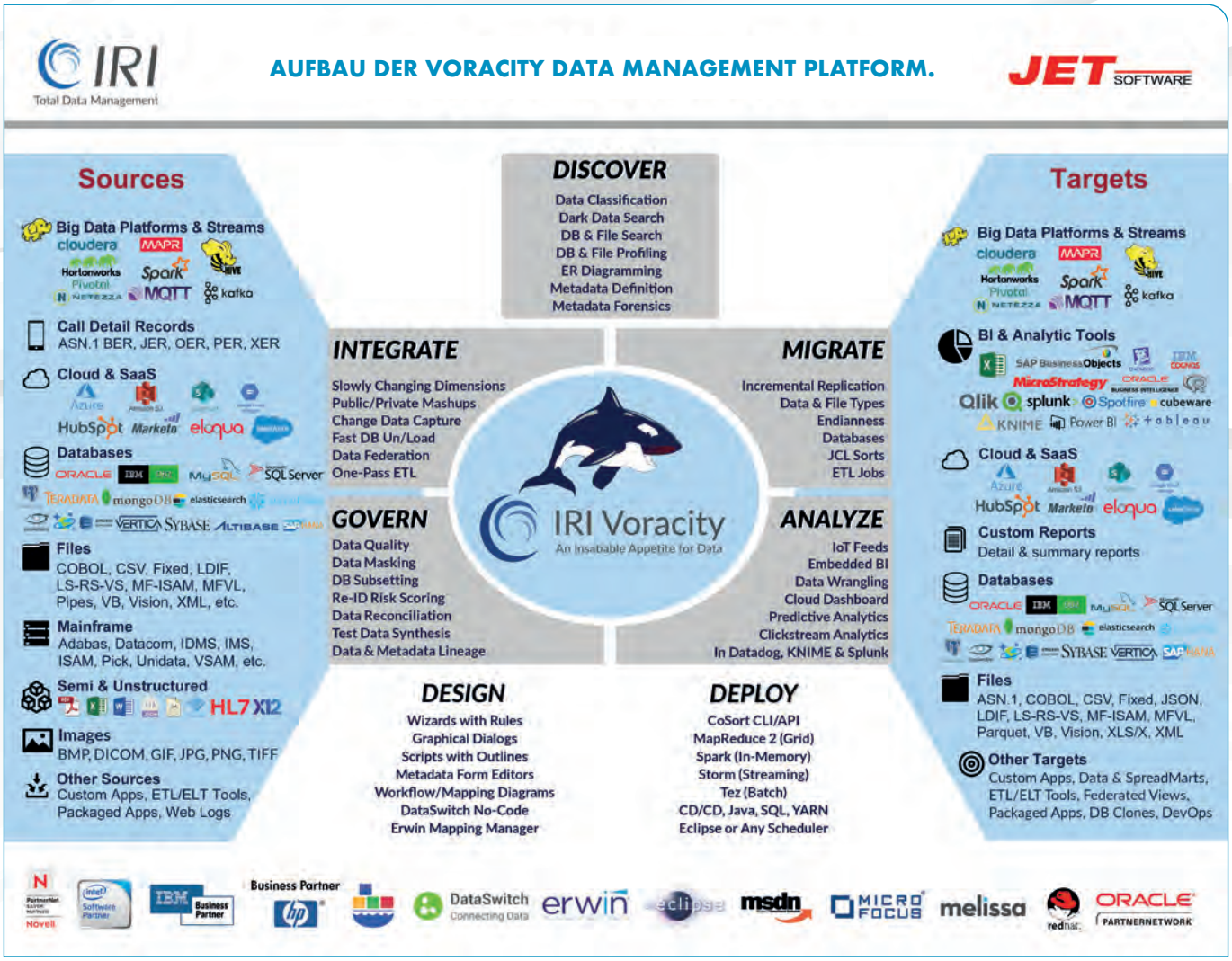
Amadeus Thomas, Geschäftsführer, Jet-Software GmbH, www.jet-software.com

Daten sind dynamisch

Datenverwaltung ist kein statischer Zustand, sondern ein dynamischer Prozess. Dieser Prozess verläuft von der Überwachung, Organisation, Speicherung, Wartung bis hin zum Schutz der Daten. Er umfasst alle Phasen des Datenlebenszyklus, von der Datenerfassung und Datenübertragung bis zur Archivierung oder Löschung. Ziel der Datenverwaltung ist es, sicherzustellen, dass Daten effektiv genutzt werden können, wann und wo sie benötigt werden und dass ihre Integrität, Sicherheit und Verfügbarkeit gewahrt bleiben. Damit ist ein End-to-End Datenmanagement zu erzielen, um den verschiedenen Prozessen in dieser mehrschichtigen Umgebung gerecht zu werden.

Aufgrund der in den 60er Jahren entstandenen und noch heute aktiven Mainframe-Systeme (Großrechner) und der aktuellen Trends wie das Internet der Dinge (IoT), der Industrie 4.0 oder die Digitalisierung im öffentlichen Sektor und im Gesundheitssystem ist die Komplexität der Daten groß. Daher unterteilt sich die Struktur der Daten in fünf grundlegende Arten:

#1 **Strukturierte Daten:** Hier sind die Daten in einem definierten und organisierten Format gespeichert, sie besitzen eine logische Struktur und Beziehung untereinander wie etwa in Tabellen, Datenbanken, bei einem EDI-Austausch, CSV- und XML-Dateien.



#2 Unstrukturierte Daten, auch Dark Data: Hier liegen die Daten noch im Rohformat vor und müssen für eine effektive Verarbeitung erst in ein strukturiertes Format umgewandelt werden, dies ist bspw. bei Texten in Office-Dokumenten oder in E-Mails, Bildern, Audios, Videos und Sensordaten der Fall.

#3 Semi-strukturierte Daten: Hier liegen die Daten in einer Kombination aus strukturierten und unstrukturierten vor, dies ist zum Beispiel bei HTML-Dateien und XML-Dokumenten der Fall.

#4 Binäre Daten: Diese im Binärformat gespeicherten Daten können nur vom Computersystem gelesen werden, wie bspw. ausführbare Dateien.

#5 Metadaten: Beschreiben nähere Informationen über die Eigenschaft, Struktur und Bedeutung anderer Daten, wie den Datentyp, den Dateinamen, die Größe und das Erstellungsdatum.

Überall im Unternehmen in verschiedensten Quellen finden sich diese legacy und modernen, statischen oder Streaming-Daten in unzähligen Datenbanken und Formaten, egal ob lokal auf dem eigenen System oder verschoben in der Cloud. Um nun eine unternehmenskritische Datenverarbeitung zu gewährleisten, benötigt man in der Regel verschiedene Tools von unterschiedlichen Herstellern um das Datenmanagement auch komplett abzudecken. Das ist auf der einen Seite sehr kostspielig und auf der anderen Seite sehr aufwendig zu bedienen, zu betreiben und zu warten.

That's new

Der neue Ansatz für ein umfassendes End-to-End Datenmanagement ist die Plattform „IRI Voracity", eine organisch gewachsene und vollständig integrierte Suite für den kompletten Datenlebenszyklus um den maximalen Wert aus den Daten zu erzielen.

IRI Voracity kombiniert die Datenerkennung, die Datenintegration und Datenmigration, mit anschließender Verwaltung und Analytik in nur einem verwalteten

Metadaten-Framework. Die Verwendung von nur einer Konsole erleichtert nicht nur die Bedienung wesentlich, sondern spart auch enorme Kosten bei der Anschaffung und bei der künftigen Wartung.

Der Hersteller hat über 40 Jahre Erfahrung mit Big Data Management, von gezielter Datenmanipulation bis zur umfänglichen Datenbewegung. Durch diese langjährige Historie mit den fortlaufenden Entwicklungen nah an kundenspezifischen Bedürfnissen aus über 4 Jahrzehnten, konnten stetig neue Datentypen und Bereiche unterstützt werden. Mittlerweile werden über 150 verschiedene semi/un/strukturierte Datenquellen unterstützt, egal in welchem Daten-Silo sie sich befinden.

AUSBLICK

In den kommenden Ausgaben wird die Plattform näher durchleuchtet. Es wird auf die Bereiche der Datenmodernisierung beziehungsweise der Datenmigration, der Verbesserung der Datenqualität eingegangen, sowie Beispiele für die gezielte Sicherheit von sensiblen Daten auch in Verbindung mit synthetisch generierten Testdaten (TDM) aufgezeigt. Es bleibt spannend!

Fazit

IRI Voracity ist eine leistungsstarke Plattform für umfassendes Datenmanagement, die schnell, benutzerfreundlich, vielseitig und wertorientiert ist. Das Ziel hierbei ist ein schnelles, kostengünstiges und ergonomisches Datenlebenszyklus-Management. Es findet eine Kombination von der Datenerkennung, über die Datenintegration und Datenmigration, bis hin zum Data Governance und der anschließenden Analytik statt – alles vereint in einer einzigen Konsole, die auf Eclipse basiert.

Amadeus Thomas

IDP: ohne KI geht nichts

WO LIEGEN DIE UNTERSCHIEDE ZWISCHEN OCR UND IDP?

IDP steht für Intelligent Document Processing (IDP), also der intelligenten Dokumentenverarbeitung, und in diesem Marktsegment ist viel Bewegung. OCR (Optical Character Recognition) kann nur Dokumente scannen und sie in eine maschinenlesbare Form umwandeln. Aber sie „versteht" Daten nicht so wie es die intelligente Dokumentenverarbeitung tut.

OCR kann uns zum Beispiel sagen, dass bestimmte Pixel die Zahlen 1 9 8 0 ergeben - aber es versteht nicht, dass es sich dabei um eine Jahreszahl und einen Teil eines Geburtsdatums handelt. IDP hingegen kann das. Menschen kennen die Bedeutung hinter bestimmten Wörtern und verstehen sie somit. Ähnlich verhält es sich nun mit der intelligenten Dokumentenverarbeitung (IDP): es versteht Wörter und Dokumente.

Das Schweizer Unternehmen Acodis hat sich aufgemacht dem Thema einen neuen Schub zu geben und in der Folge in einem Series A Funding sechs Millionen Schweizer Franken eingesammelt. Nachfolgend die sechs Hauptunterschiede von IDP zu OCR:

- #1 Hohe Geschwindigkeit bei der Verarbeitung von Daten
- #2 Einfache Einrichtung und Aktivierung
- #3 Vollständige Automatisierung der Dokumentenverarbeitung
- #4 Versteht die Daten kontextbezogen
- #5 Selbstlernendes System
- #6 Lässt sich nahtlos in bestehende Systeme integrieren

OCR oder IDP - Eine Übersicht

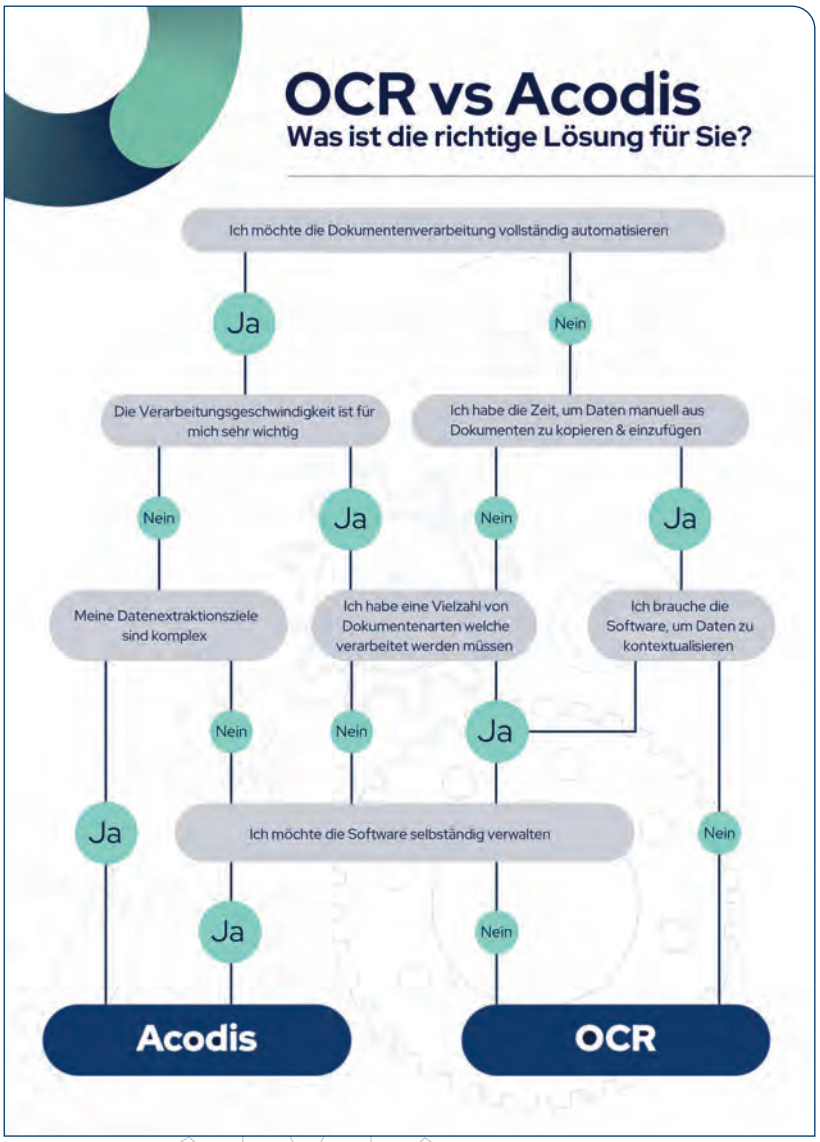
Acodis hat ein Verfahren entwickelt, das durch maschinelles Lernen jedes Dokument wie ein Mensch lesen und verstehen kann. Sobald Dokumente in maschinenlesbare Daten umgewandelt sind, können Unternehmen bisher verborgene Daten problemlos durchsuchen, analysieren und verarbeiten, um daraus neue Erkenntnisse zu gewinnen.

OCR und die Acodis-KI des IDP unterscheiden sich in zahlreichen Aspekten.

Von Zeit zu Zeit kann es schwierig sein, sich für einen Softwaretyp zu entscheiden – vor allem, wenn man ständig mit Fach-

FUNKTIONEN	OCR (Optical Character Recognition)	ACODIS (Powered by IDP)
Hohe Geschwindigkeit bei der Datenverarbeitung	✓	✓
Einfach einzurichten und zu initiieren	✗	✓
Automatisierung der Dokumentenverarbeitung	✗	✓
Kontextualisiert Daten	✗	✓
Selbstlernendes System	✗	✓
Leichte Integration in bestehende Systeme	✗	✓

ausdrücken konfrontiert und die Unterschiede nicht sichtbar werden. Die Lösung: Ein Flussdiagramm, das Anwendern bei der Wahl zwischen Standard-OCR und auf maschinellem Lernen basierender Software hilft.



Performance & Automatisierung
Datenverarbeitung mit hoher Geschwindigkeit spart nicht nur Zeit und Geld, sondern hilft auch den Mitarbeitern, sich auf andere, wichtige Geschäftsziele zu konzentrieren. Die Möglichkeit, Daten innerhalb von Sekunden statt Stunden zu extrahieren und zu klassifizieren, ist schon eine kleine Revolution, denn Geschwindigkeit ist ein Aspekt, der für Unternehmen große Relevanz hat. Immer gewünscht, aber oft nicht erreicht wird der Aspekt „keep it simple". Auch komplexe Systeme sollten so einfach wie möglich in der Benutzeroberfläche und -führung sein.

Ein vollautomatisches Datenverarbeitungssystem steht zwar nicht auf der Wunschliste jedes Unternehmens, kann aber für die Effizienz des Unternehmens von entscheidender Bedeutung sein. Bei OCR fehlt dieses Element in der Regel, so dass die Benutzer ständig Vorlagen bereitstellen und überwachen müssen. Mit der IDP hingegen kann die Datenextraktion vollständig automatisieren werden.

Kontextuelles Verständnis der Daten
OCR ist zwar in der Lage, einfache Texte, Zahlen und Symbole zu verarbeiten, verfügt aber nicht über ein so ausgeprägtes kontextbezogenes Wissen wie Acodis. Der Einsatz von OCR-Software erweist sich als eher unpraktisch, wenn Unternehmen sie zeitnah benötigen, um Daten, wie etwa von einer Versicherungspolice, in den richtigen Kontext zu bringen und umzuwandeln.

Selbstlernend & integrationsfähig
Es gibt einen ständig wiederkehrenden Faktor, wenn es um die Implementierung von Datenautomatisierung geht: die Fähigkeit, selbständig zu lernen und damit wirtschaftlich zu sein. Während dies bei der Standard-OCR nicht der Fall ist, ist Acodis-KI in der Lage, zu lernen und sich weiterzuentwickeln, ohne dass eine ständige Unterstützung erforderlich ist.

Im Vergleich zu OCR bietet das IDP die Möglichkeit, sich ohne große Probleme oder Komplexität in Unternehmen zu integrieren. Diese Funktion ist sowohl Zeit als auch Geld sparend. Die einfache Integration entlastet die Unternehmen, die tech-

DIE VORTEILE IM ÜBERBLICK

Für die Anwender
No-Code-Plattform
Intuitive und einfache Benutzeroberfläche
Klicken und Ablegen
Bis zu 50 Prozent höhere Effizienz

Für die IT-Abteilung
Nahtlose API-Integration in bestehende Anwendungen
Cloud agnostisch
Nur begrenzte IT-Ressourcen erforderlich
In drei Tagen einsatzbereit

CHECKLISTE

WIE LASSEN SICH IDP-ANBIETER VERGLEICHEN?

Wenn Sie sich nach einer Software zur Datenextraktion umsehen, sollten Sie die folgenden Faktoren berücksichtigen:

#1 Komplexität der Dokumente: Bedenken Sie, wie viele Dokumente in Ihrem Unternehmen verarbeitet werden und wie viele davon komplex sind.

#2 Standarddokumente gibt es nicht, das Layout ändert sich ständig. Stellen Sie sicher, dass Ihr System nicht auf Vorlagen basiert, da Vorlagen bei jeder Änderung neu erstellt werden müssen.

#3 Können Sie mit wenigen Klicks Ihr eigenes Modell erstellen, um die höchste Genauigkeit bei der Datenextraktion zu erreichen? Und bietet Ihr System auch vortrainierte Modelle für die gängigsten Dokumente an, um schnelle Ergebnisse zu erzielen?

#4 Kann Ihr System benutzerdefinierte und vortrainierte Modelle problemlos kombinieren, um genauste Ergebnisse zu erzielen?

https://www.acodis.io/

nischen Kenntnisse müssen somit nicht auf dem Stand eines Codingexperten sein.

Kategorisierung – Extraktion – Analyse

Wie funktioniert nun IDP genau und wo liegen die Vorteile? Der Hersteller, hier Acodis, verspricht, dass jedes Dokument, egal ob PDF, PNG, JPG, aus verschiedenen Quellen wie etwa SharePoint, API, eMail, erfasst und automatisch verarbeitet werden kann. In der Kategorisierung können die Anwender die Dokumente bestimmten Workflows zuordnen. In der Trennphase erfolgt die Extraktion der Daten aus Texten, Bildern, Tabellen, Diagrammen. In der Analysephase schließlich werden die Daten analysiert, validiert und als strukturierte Daten für den späteren Gebrauch abgelegt. Der Output kann in verschiedenen Formaten (XML, JSON, CSV) und den unterschiedlichsten Anwendungen (CRM, DMS, RPA, PLM) erfolgen.

Die vortrainierten Modelle sind getestet und ermöglichen so sofort mit der Extraktion von Daten aus Dokumenten zu starten. Möglich sind eigene KI-Modelle, um die größtmögliche Genauigkeit aus den Daten herauszuholen. Die Unternehmen bestimmen selbst, wie und wo ihre Daten extrahiert werden sollen. Die Benutzer können zudem die Performance verbessern, indem sie markierte Ausnahmen überprüfen und bearbeiten, um die selbstlernende Plattform zu verbessern. Programmierkenntnisse sind dabei nicht erforderlich. Die Anwender erhalten automatisch Hinweise, falls Dokumentenkategorien und Datenpunkte überprüft werden müssen.

Und schließlich können die Anwender konkrete Parameter für Ihre KI-Modelle definieren, um zusätzlich sicherzustellen, dass Ihre Datenpunkte mit höchster Genauigkeit extrahiert werden.

Nachfolgend ein paar Beispiel für den Funktionsumfang:

Intelligente Erkennung von Datenfeldtypen

Bei der Erstellung eines Datenextraktionsschemas muss nicht mehr jeder Datenfeldtyp manuell festgelegt werden. Acodis schlägt automatisch den richtigen Typ vor, basierend auf den Dateneigenschaften, die es im Dokument erkennt (Datum, Zahl, Text).

Automatisierte Tabellenerkennung

Das Programm erkennt Tabellen automatisch, extrahiert die darin enthaltenen Informationen, ohne die bestehende Reihenfolge zu verändern. So erhält man die Daten schnell, einfach und ganz ohne abzutippen.

Handschrifterkennung

Die Mitarbeiter verbringen weniger Zeit damit, handschriftliche Informationen zu „entschlüsseln". Die Software erkennt handschriftlichen Text genau und verarbeitet die getippten oder handschriftlichen Dokumente automatisch.

Und der Mensch?

Der wird natürlich nicht überflüssig. Die Zugriffsrechte der Mitarbeiter und die operative Kontrolle über ihre Workflows mit benutzerdefinierten Benutzerrollen müssen angepasst werden, das kann keine KI erledigen. Es müssen benutzerdefinierte Benutzerrollen zugeordnet und unterschiedliche Zugriffs- und Betriebsberechtigungen vergeben werden.

Schon allein aus Compliance- und Auditgründen müssen zudem detaillierte Aufzeichnungen der beteiligten Benutzer und der in jeder Phase Ihres Dokumentenverarbeitungs-Workflows durchgeführten Aktionen protokolliert werden. Und last but not least müssen die Unternehmen benutzerdefinierte Parameter festlegen, um sicherzustellen, dass die Datenpunkte genau nach Ihren Wünschen extrahiert werden.

Ulrich Parthier | www.it-daily.net

Anbieter von IDP-Plattformen

Parashift	https://parashift.io/
Ephesoft	https://ephesoft.com/de/
Acodis	https://www.acodis.io/
Inserve	https://www.inserve.de/
Appian	https://appian.com/de
Klippa	https://www.klippa.com/de/startseite/

Praxisprobleme?

WIE ÜBERFÜHRE ICH MACHINE-LEARNING-MODELLE PROFESSIONELL IN DIE PRODUKTIVE PHASE?

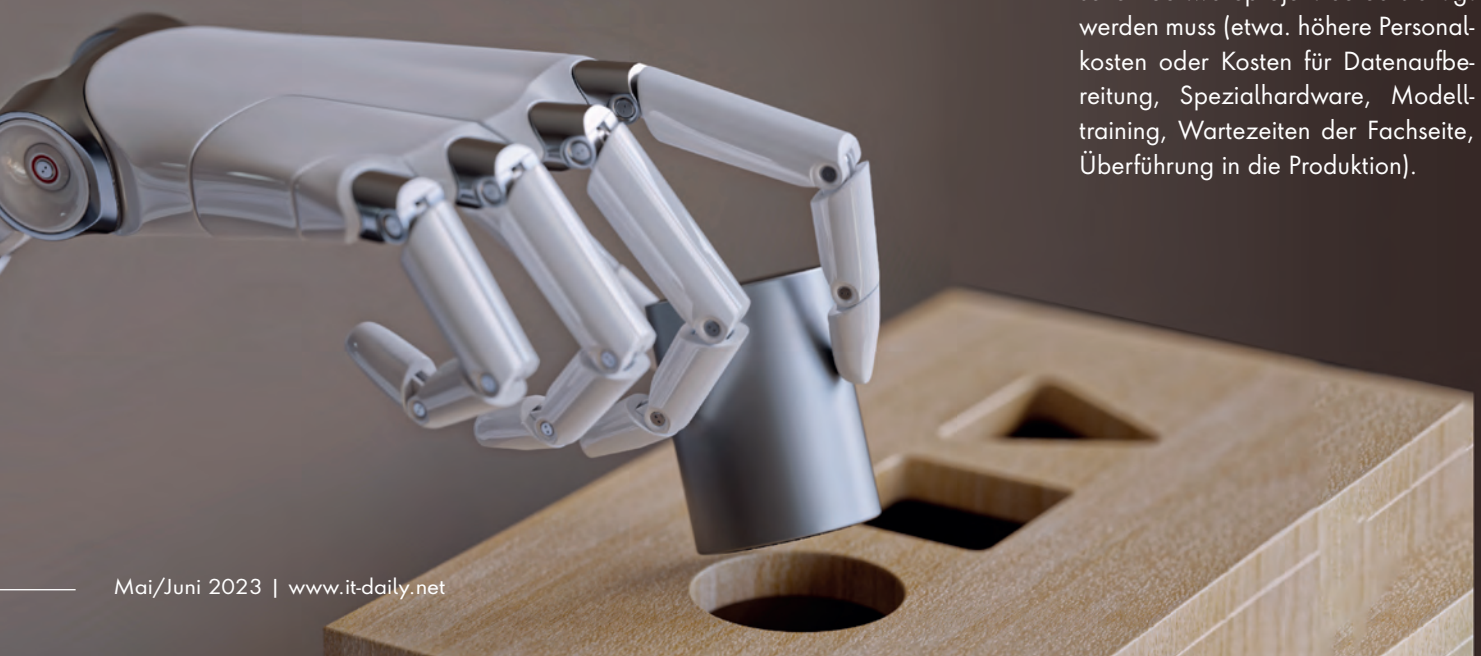
„Ich habe drei Wochen gebraucht, um das Machine-Learning-Modell zu entwickeln. Inzwischen ist ein Jahr vergangen und es ist immer noch nicht in Produktion." Dies oder ähnliche Aussagen kommen immer wieder in Projekten vor. Diese Klage eines anonymen KI-Entwicklers beschreibt das Dilemma, in dem viele Unternehmen stecken, die ML-Projekte verfolgen und eigentlich die Vorteile von Künstlicher Intelligenz und Machine Learning (KI / ML) in größerem Umfang nutzen möchten.

Auch die Mitglieder des Cross-Business-Architecture Lab (CBA Lab) sehen bei der Übernahme der als Prototypen entwickelten ML-Lösungen in die Produktion noch einige unbewältigte Hürden. Bei ML ist man noch weit entfernt von einem reifen und etablierten DevOps-Ansatz, der bei Entwicklung und Produktion von Nicht-KI/ML-Projekten inzwischen zum Mainstream geworden ist. DevOps beschreibt die Verzahnung des Entwicklungsprozesses mit dem IT-Betrieb. Deshalb befasste sich der KI/ML-Workstream des CBA Lab genau mit diesem Übergang zwischen Entwicklung und Produktion.

Qualität und Automatisierungsgrad
Ziel war es einen Ansatz zu entwickeln, der den Anforderungen in ML-Projekten an Qualität und Automatisierungsgrad entsprechen kann. Der Workstream hat sich deshalb intensiv mit dem sogenannten MLOps- Ansatz auseinandergesetzt. MLOps steht für eine auf Machine Learning ausgerichtete Vorgehensweise, die die Tugenden des Development-and-Operations-Modells (DevOps) nutzt.

Der Workstream führt einige der Aufgaben aus, die der ML-Einsatz mit sich bringt:

- Der Betrieb von ML-Systemen ist aufwändiger als bei klassischer Software, weil Training, Deployment und das Monitoring sowie die regelmäßige Anpassung (Retraining) der ML-Modelle mehr Aufwand bringen. Auch die Versionierung ist anspruchsvoll, weil bei ML die zugehörigen Modelle, Trainings, Validierungs- und Testdaten mit versioniert werden müssen, um die Nachvollziehbarkeit zu gewährleisten.
- Datenschutz ist in Bezug auf ML oft nicht klar. Dürfen zum Beispiel Bilder von Personen für das Training von ML-Modellen genutzt werden? Wenn Entscheidungen von einer ML getroffen werden, zum Beispiel bezüglich eines Kredites, ist nicht klar geregelt, wie detailliert die Entscheidung gegenüber den Betroffenen nachvollziehbar gemacht werden muss.
- Erfahrene Data Science- und ML-Engineering-Spezialisten sind am Arbeitsmarkt eine rare Ressource. Sie werden aber für kompetente Entwicklungsteams gebraucht – genauso wie Expertise im Bereich Software-Engineering und Betrieb. Den eingesetzten Teams fehlt es außerdem an Kompetenzdiversität. Das kann dazu führen, dass Pilotprojekte in kleinem Rahmen funktionieren, dann aber technisch und organisatorisch nicht skalieren (cross-funktionale Teams können hier eine Lösung darstellen).
- Die Kosten werden häufig unterschätzt, weil mehr Aufwand als in einem klassischen Softwareprojekt berücksichtigt werden muss (etwa. höhere Personalkosten oder Kosten für Datenaufbereitung, Spezialhardware, Modelltraining, Wartezeiten der Fachseite, Überführung in die Produktion).



- Fehlende Nachvollziehbarkeit der Entscheidungen.
- Unbekannte Abhängigkeiten der Daten, die für das Trainieren der Modelle verwendet werden.
- Fehlende oder nicht verlässliche Daten.

Von DevOps zu MLOps

Einige dieser Gestaltungsaufgaben können adressiert werden, indem man ML-Anwendungen einem erweiterten DevOps-Ansatz unterwirft, dem sogenannten MLOps. Es erweitert die bekannten DevOps-Prinzipien, um die Entwicklung und den Betrieb von ML-basierten Anteilen der Lösungen spezifisch und optimal zu unterstützen. Das Hinzufügen neuer Datensätze, aber auch die schleichende Degradation der Modellperformanz benötigt ein kontinuierliches Training (CT), um diese stabil zu halten oder gar zu verbessern.

Da ein ML-Modell meistens nur eine kleine, aber sehr kritische Komponente eines Software-Systems darstellt, muss ihre Interaktion mit anderen Komponenten ständig überprüft werden. Das bedeutet die Überprüfung neuer Modelle durch besondere Testverfahren wie Daten- und Modellvalidierung.

Das MLOps-Prinzip funktioniert allerdings nur dann, wenn die Organisation auch über die nötigen Fähigkeiten verfügt, die der Workstream in einem Capability Framework zusammenfasst.

Es besteht aus folgenden sechs Bausteinen:

1. Mensch & Kompetenz: Der Mensch und die benötigten Fertigkeiten sind Grundvoraussetzung für ein erfolgreiches MLOps. Es braucht nicht nur den Data Scientist oder den ML Engineer, sondern eine Vielzahl unterschiedlichster Fähigkeiten. Diese müssen rekrutiert, ausgebildet und an die Organisation gebunden werden.

DAS MLOPS-PRINZIP FUNKTIONIERT NUR DANN, WENN DIE ORGANISATION AUCH ÜBER DIE NÖTIGEN FÄHIGKEITEN VERFÜGT, DIE DER WORKSTREAM IN EINEM CAPABILITY FRAMEWORK ZUSAMMENFASST.

Dr. Jürgen Klein,
Digital Technology Portfolio Manager,
Carl Zeiss AG, www.zeiss.de

2. Kultur: Die Organisation muss sich auf die neuen Technologien auch kulturell vorbereiten. Es braucht bei den einzelnen Teilnehmenden einer MLOps-Initiative, aber auch in der gesamten Organisation, eine Bereitschaft, sich auf ML-unterstützte Prozesse einzulassen und diese ständig weiterzuentwickeln. Eine Grundvoraussetzung dafür ist die Unterstützung des Topmanagements. Die Organisation kann sich erst dann zur Einführung von MLOps verpflichten, wenn das Topmanagement klare Support-Signale sendet.

3. Prozesse: Änderungen, die mit der Adaption von ML einhergehen, beeinflussen immer die Prozesse einer Organisation. Die Prozesse werden aufgrund des systematischen Einbezugs von Datenströmen geändert.

4. Daten: Daten sind der Treibstoff für eine ML- Organisation. Ohne qualitativ hochwertige und korrekte Daten gibt es kein ML. Unternehmen haben häufig Probleme mit der Qualität historischer Daten. Deshalb müssen grundlegende Fähigkeiten wie Datenaufbereitung, Datenverarbeitung und Datenqualitätssicherung verbessert werden, um die Bereitschaft für ML zu erhöhen.

5. Technologie und Infrastruktur: ML basiert auf einem komplexen Technologie-Stack und benötigt eine hoch performante Infrastruktur, die in einem sehr dynamischen Umfeld funktionieren muss. Die stetige technologische Innovation und Pflege sind Grundvoraussetzung für ML. Dafür müssen die notwendigen Ressourcen sowohl finanziell als auch personell bereitgestellt werden.

6. Risiko, Compliance & Ethik: Der Einsatz von Systemen, die potenziell selbstständig Entscheidungen treffen, birgt Gefahren. So können unausgewogene Daten zu tendenziösen Resultaten und unethischen Entscheidungen führen, die im schlimmsten Fall Menschen gefährden und die ganze Organisation bedrohen können.

Für die Beherrschung der Risiken und die Sicherstellung der Compliance ergeben sich damit völlig neue Fragestellungen.

Dr. Jürgen Klein

ÜBER DAS CROSS-BUSINESS-ARCHITECTURE LAB

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

Produkt-IT

WEITREICHENDE KONSEQUENZEN FÜR UNTERNEHMEN, IT UND ENTERPRISE ARCHITECTURE

Produkt-IT ist ein heißes Eisen. Wie definiert man sie, welche Fähigkeiten werden gebraucht und welche Wechselwirkungen haben Produkt- IT und kommerzielle IT? Wie wird „the new kid on the block" ins Gesamtunternehmen integriert und was müssen die Stakeholder dabei beachten?

Das Das Cross-Business-Architecture Lab (CBA Lab) definiert Produkt-IT als Ressourcenpool für alle Technologien und Funktionen, die für Entwicklung und Betrieb digitaler Kundenprojekte notwendig sind. Die im Anwenderverband zum Thema Produkt-IT eingerichtete Arbeitsgruppe geht davon aus, dass für die Herstellung digitaler Kundenprodukte – von Apps über digitale Services bis hin zu Predictive Maintenance – kommerzielle IT und Produkt-IT eng miteinander arbeiten müssen, da kaum ein Unternehmen auf der grünen Wiese mit digitalen Produkten beginnen dürfte.

Veränderung der Business-Modelle

Auf der strategischen Business-Ebene bedeuten digitale Kundenprodukte und Produkt-IT eine Veränderung der Business-Modelle hin zu Data Driven Business Models, die nicht nur auf Daten als Key Ressourcen zugreifen, sondern sie weitergeben und verkaufen.

So werden Daten zur Kernaktivität, mit einem hohen Wertschöpfungsanteil. Dieser Change wiederum benötigt neue organisatorische Fähigkeiten wie agile Arbeitsorganisation sowie erweiterte und neue technische Capabilities.

DAS ENTWICKELN, VERKAUFEN UND BETREIBEN VON DIGITALEN KUNDENPRODUKTEN ALS SERVICE STELLT FÜR VIELE UNTERNEHMEN EIN NEUES GESCHÄFTSMODELL DAR.

Christian Schwaiger, Leiter des Workstreams und Head of Enterprise Architecture, KUKA AG, https://cba-lab.de

Drei Fragen bestimmen das Handeln

Natürlich gibt es eine prinzipielle Handlungsempfehlung zur Umsetzung einer Produkt-IT. Man systematisiert die Fragen nach dem anvisierten Ziel, nach den dafür nötigen Voraussetzungen und nach dem Umsetzungsprozess:

#1 Was möchte ich tun?

Entwicklung eines gemeinsamen Verständnisses von Produkt-IT und digitalen Kundenprodukten.

- Abfrage der Stakeholder-Erwartungen

#2 Was benötige ich dafür?

Identifikation benötigter Capabilities – technisch und fachlich im eigenen Unternehmen.

- Fit- / Gap-Analyse – wie vollständig ist die Abdeckung von Capabilities, Skills und Reifegraden im eigenen Unternehmen und den verschiedenen Abteilungen?
- Wie können identifizierte Gaps geschlossen und vorhandene Capabilities optimiert werden?

#3 Wie setze ich es um?

Ein Idea-to-EOL-Prozess für digitale Kundenprodukte muss etabliert werden (EOL=End of Lifecycle). Dies bildet die Grundlage für die Ablauforganisation und die daraus abzuleitende Aufbauorganisation.

- Neben der Zuteilung der Aufgaben, Kompetenzen und Verantwortungen empfiehlt sich ein flankierendes Change-Management für das Gesamtunternehmen, nicht zuletzt, um die agilen Arbeitsweisen zu lernen und zu verinnerlichen.

Welche Anforderungen welche Capabilities bedingen

Die Enterprise Architecture muss sich deshalb verstärkt mit den zusätzlichen An-

forderungen und den sich daraus ergebenden Capabilities auseinandersetzen. Als Anforderungen hat der Workstream zum Beispiel folgende formuliert:

- Compliance in Zielmärkten und branchenspezifische Anforderungen,
- gesetzliche Anforderungen
- Data Ownership – Anbieter, Kunde, beide? Abhängig vom Entstehungsort.
- Abrechnungs- und Lizenzierungsmodelle für digitale Kundenprodukte sowie deren Kombinationen mit klassischen Produkten, Ermittlung von ROI, Marktanalyse und Preisfindung, Verbrauchsmessung und Monetarisierung
- neue Geschäftsmodelle (Freemium, „Razor and Blades Model")
- Digital Product Delivery und Entitlement bei On-Premises-Installationen
- Positive Value Generation – Cost to Revenue bei der Einführung digitaler Kundenprodukte
- Vertriebsmodell und Incentivierung: Cost of Sales im Kontext von Margen,
- Skills über alle Ebenen im Bereich digitale Kundenprodukte
- Customer Success Management – Retention und Loyalty in der Subscription Economy.

Um die sich daraus ergebenden Capabilities zu identifizieren, hat die Arbeitsgruppe einige Capability-Maps der teilnehmenden Unternehmen nach fachlichen und technischen Capabilities analysiert.

Viele der für eine Produkt-IT nötigen Capabilities müssen die Unternehmen ausbauen oder noch entwickeln. Dazu gehören zum Beispiel: Retention and Loyalty Management, Product Licence Management, Operate Digital Products and Services oder Data Management.

IT in der Zwitterfunktion

Die kommerzielle IT muss ihre Kompetenzen erweitern. Das bedeutet, sie muss ihre Außensicht schärfen, um Kundenanforderungen verstehen und erfüllen zu können. Kommerzielle und Produkt-IT müssen sich ergänzen. Sie müssen miteinander klären, wer jeweils welche Aufgaben für Entwicklung und Betrieb digitaler Kundenprodukte übernimmt. Dabei gilt es, drei grundsätzliche Fragen zu beantworten:

#1 Welche Anforderungen werden an die kommerzielle IT in Zusammenhang mit digitalen Kundenprodukten gestellt?

#2 In welchen Bereichen soll die kommerzielle IT an digitalen Kundenprodukten mitwirken?

#3 Welche Erwartungen hegen die Fachabteilungen im Unternehmen?

Christian Schwaiger

#HUB.BERLIN23

EXPLORE THE FUTURE – CHANGE THE GAME!

Zwei Tage lang dreht sich auf der hub.berlin alles um Tech-Innovationen, die unsere Zukunft gestalten. Globale CEOs, politische Entscheidungsträger, Startup-Gründer und Branchenexperten diskutieren gemeinsam die Themen, die unsere Zeit bestimmen. Profitieren Sie von den Einblicken bedeutender Branchenexperten wie Dr. Daniela Gerd tom Markotten, Digitalvorständin der Deutschen Bahn, Timotheus Höttges, CEO der Deutschen Telekom AG, Dirk Hoke, CEO der Volocopter GmbH und Jörg Gerbig, COO und Gründer von Lieferando.

Das Veranstaltungskonzept sieht 4 Cluster vor. Die hub.conference vermittelt inspirierende Inhalte mit Experten-Workshops, Keynotes und Diskussionsrunden. Hier erhalten Sie die neuesten Einblicke in die Branche und zu den wichtigsten Technologiethemen.

Ein breites, kreatives Angebot zum Networking, wie Networking Lounges, Pub Crawls, die Club Night, Executive Dinner oder die Möglichkeit auf Einzelgespräche mit Referenten, bietet die hub.experience. Netzwerken wird bei der hub.berlin großgeschrieben.

Einzigartig ist zudem die interaktive Ausstellungsfläche der hub.exhibition, sowie das Digital Arts Lab, in welchen die digitalen Technologien zur Realität werden.

Der Bereich hub.career leitet den nächsten Schritt der Karriere ein, dank einer effektiven Jobbörse und Employer Sessions auf einer extra Bühne.

Erleben Sie die einzigartige Atmosphäre vor Ort, vernetzen Sie sich mit Branchenexperten und entdecken Sie neue Karrieremöglichkeiten. Sichern Sie sich jetzt Ihr Ticket für den 28. und 29. Juni auf Europas Business-Tech-Festival.

www.bitkom-live.de/de/hub-berlin

Storage-Hochverfügbarkeit

JA BITTE!

Hochverfügbare Speichersysteme (High-Availability, HA) stehen für hohe Investitionen, vor allem aus der Sicht von KMUs. Die höhere Investition als ein Stand-Alone-Speichersystem beziehungsweise ein SAN ist einfach der Tatsache geschuldet, dass in einer HA-Umgebung alle Komponenten mindestens doppelt vorhanden sein müssen. Zusätzlich bedarf es einer zuverlässigen Applikation, die dafür sorgt, dass die Daten auf allen beteiligten Komponenten synchron gehalten werden.

Deshalb hat sich Speicherhersteller N-Tec mit DataCore zusammengetan. Ergebnis war die, mittlerweile in fünfter Generation, rapidCore-Serie: eine DataCore SANsymphony-zertifizierte, synchron gespiegelte Speichereinheiten, die je nach Anforderung in den verschiedensten Kapazitäts- und Leistungsklassen vertrieben werden.

Nachfrage nach hochverfügbaren Speichersystemen

Tatsächlich steigt die Nachfrage nach hoch- und höher verfügbaren Speicherlösungen in den letzten Jahren ständig an. Auch in kleinen Unternehmen werden Speicher und Server konsolidiert und virtualisiert.

Die Technologie dahinter verspricht zwar einerseits mehr Komfort – Tatsache ist aber auch, dass genau dieser Komfort andererseits mehr Komplexität und Abhängigkeit von einer zentralen Komponente bedeutet. „Wir liefern das Fundament für diese zentrale IT-Infrastruktur und das muss schlichtweg zuverlässig funktionieren und verfügbar sein.“, sagt Sven Meyerhofer, Geschäftsführer der N-Tec GmbH.

Meyerhofer weiter: „Wenn wir von Hochverfügbarkeit sprechen, dann stehen – mindestens zwei – synchron gespiegelte Speicherknoten dahinter. Im Idealfall mit transparentem Failover und Failback. „Das heißt, die Dienste können sowohl im Wartungs- wie im Fehlerfall manuell, aber auch automatisch auf die verbliebene Seite geschwenkt werden. User und Applikationen merken davon nichts – eine korrekte Konfiguration vorausgesetzt. Downtime von Systemen wird damit zur absoluten Ausnahme. Und die Konfiguration des Systems muss danach nicht zwangsweise mühselig manuell wieder hergestellt werden, das kann man getrost unseren Systemen überlassen.“

Die wichtigsten Faktoren

Wir werden immer wieder bei Problemen mit Fremdsystemen um Unterstützung gebeten. Häufig stellen wir fest, dass bereits bei der Vorplanung und später in der Umsetzung Fehler gemacht wurden. Software und Hardware werden immer leistungsfähiger und müssen umso mehr aufeinander abgestimmt sein.

Einer der wichtigsten Punkte für ein performanten Systems sind möglichst geringe Latenzen. Bei falscher Planung können sie sich rasch aufsummieren und letztendlich mindestens zu schlechter Performance oder gar Fehlern bei Applikationen führen.

Unterschiede bei Lösungen

Der große Vorteil von Software-defined Storage ist, dass die Software im besten Fall auf jeder, zumindest aber auf einer zertifizierten und freigegebenen Hardware-Plattform betrieben werden kann.

Daraus ergeben sich größtmögliche Flexibilität und Skalierbarkeit. Risiken birgt der Ansatz bei der Vielzahl an möglichen Hardware-Konfigurationen.

Große globale IT- und Storage-Hersteller mit ihren integrierten Lösungen werben unter anderem damit, dass hier alle Komponenten, Hard- und Software perfekt aufeinander abgestimmt sind. Großer Nachteil: man ist und bleibt an diesen Hersteller über Jahre gebunden – Stichwort: Vendor Lock. Erweiterungen können dann nur vom Hersteller bezogen werden, zu meistens überzogenen Preisen. Der Kunde hat ja schließlich keine Wahl.

Diesen vermeintlichen Vorteil greifen wir eben mit unserer Lösung auf. Das heißt, wir haben Hardware-Plattform und Software aufeinander abgestimmt und zertifiziert. Jedoch mit dem großen Unterschied, dass N-Tec-Lösungen auf Standard-Hardware setzen, zu den marktüblichen Preisen. Bei späteren Erweiterungen erlebt der Kunde keine preislichen Überraschungen Der Kunde erhält alle Vorteile aus beiden Welten.

Hochverfügbarkeit integrieren

Die Gretchenfrage ist, wie kann ich Hochverfügbarkeit in die bestehende IT-Infrastruktur integrieren, ohne den Betrieb zu beeinträchtigen? Das ist natürlich von der Infrastruktur des Kunden abhängig. Ziel ist immer eine Datenmigration mit möglich wenig oder bestenfalls komplett ohne Downtime.

HOCHVERFÜGBARE SPEICHERSYSTEME STEHEN FÜR HOHE INVESTITIONEN, VOR ALLEM AUS DER SICHT VON KMUS. EINE ALTERNATIVE IST STANDARD-HARDWARE IN KOMBINATION MIT SOFTWARE-DEFINED STORAGE.

Sven Meyerhofer, Geschäftsführer, N-Tec GmbH, www.n-tec.eu

Falls der Kunde etwa eine VMware VSphere Umgebung betreibt, kann die Integration per Storagemotion, ohne jegliche Downtime, per Mouse mit wenigen Klicks erfolgen. Wir analysieren und diskutieren ab dem ersten Gespräch, die aktuelle und künftige Infrastruktur des Kunden.

Trends und Entwicklungen

Aktuell sehen wir einen Trend in Richtung hybrider Infrastruktur. Unternehmen teilen ihre Infrastruktur auf und halten einen Teil in eigenen Räumen und den Rest in externen Rechenzentren.

Durch die Tatsache, dass die Rapidcore-Lösung sowohl synchrone Replikation (Mirror) als auch asynchrone Replikation anbietet – können die Daten auch entsprechend georedundant gehalten werden.

Karl Fröhlich | www.speicherguide.de

WHITEPAPER DOWNLOAD

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

MIGRATION AUF WINDOWS 11

SO KLAPPT DER UMSTIEG FÜR UNTERNEHMEN

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

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

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

Hybrid-Storage

DIE RICHTIGE SPEICHERSTRATEGIE FÜR BIG DATA?

Die Wahl der richtigen Speicherstrategie für das Handling großer Datenmengen stellt viele Unternehmen vor eine Herausforderung. Als optimale Wahl hat sich Hybrid-Storage etabliert, ein Ansatz, der generell viele Vorteile bietet. Was sollte man dennoch beachten?

In der Zeit, bevor es die Cloud gab, standen bereits verschiedene Speichertechnologien zur Verfügung, die je nach Anwendungsszenarien zum Einsatz kamen. Der Speicher konnte sehr schnell sein wie etwa fest installierte RAM-Disks vor allem für Arbeitsspeicher, leicht transportabel als Wechselmedien wie Floppy-Disks, zuverlässig wie Festplattenlaufwerke (HDD) als Rechen- und Speicherkomponenten oder kostengünstig wie Bandspeicher für große Datenmengen. Gleichgeblieben ist bis heute, dass Unternehmen die Wahl treffen mussten zwischen schnellem Datenzugriff, verbunden mit höheren Kosten, oder großen Speicherressourcen, die zwar kostengünstiger, aber auch langsamer sind.

Mit der Cloud hat sich die Speicherfrage komplett verändert. Bandspeicher wurde abgelöst durch Objektspeicher wie Amazon S3. Im Kleinen hat sich zuvor auch eine technische Revolution vollzogen. So haben Flash-basierte USB-Sticks zunächst die altgedienten Disketten verschiedener Formate abgelöst. Flash-Speicher wurde mit der Zeit insgesamt immer günstiger, was zuletzt den Einzug von SSD-Arrays in Rechenzentren einläutete.

Insgesamt ist die Storage-Landschaft heute vielfältiger, es gibt Technologien, die leistungsfähiger und dennoch energieeffizienter sind. Eines hat sich aber nicht geändert gegenüber den vergangenen Jahrzehnten: Sehr schneller Speicher ist immer noch sehr teuer. Unternehmen müssen immer noch die Wahl treffen – oder einen Kompromiss finden – zwischen Geschwindigkeit und Kosten.

HYBRIDE SPEICHERUNG BEDEUTET, DASS VERSCHIEDENE SPEICHERTYPEN IN EINER EINZIGEN LÖSUNG INTEGRIERT SIND, UM DAS BESTE AUS BEIDEN STORAGE-WELTEN ZU VEREINEN.

Stefan Käser,
Solutions Architect, DoubleCloud GmbH,
https://double.cloud/

Das Beste aus zwei Welten: Hybrid-Storage

An dieser Stelle kommt Hybrid-Storage, also die hybride Speicherung ins Spiel. Hybride Speicherung bedeutet, dass verschiedene Speichertypen in einer einzigen Lösung integriert sind, um das Beste aus beiden Storage-Welten zu vereinen. Im kleinen Rahmen steht „hybrid" für Laufwerke, die eine herkömmliche HDD mit einer schnellen SSD im selben Gehäuse kombinieren. Der integrierte Controller verschiebt die Daten zwischen den verschiedenen Teilen der Hardware auf der Grundlage von Regeln wie der Häufigkeit der Zugriffe oder der Zeit seit dem letzten Zugriff. Benutzer können das Hybridlaufwerk einfach als einen gemeinsamen Speicher nutzen.

Auf einer größeren Ebene ist Hybrid-Storage eher an die Hybrid-Cloud angelehnt, wie bei DoubleCloud. Als Anbieter eines modernen Data-Stacks für End-to-End-Analytik kombiniert das junge Berliner Unternehmen kostengünstigen, aber langsameren S3-Objektspeicher mit schnellem, aber teurem lokalem GP2-Speicher. Dies ermöglich die stetige Dateneingabe, ohne ältere Daten nach S3 verschieben oder die Anwendung anpassen zu müssen, um etwa andere Zugriffsmuster zu unterstützen.

Speicherwahl: Verschiedene Aspekte zu berücksichtigen

Wie in Zeiten vor der Cloud sind bei der heute möglichen Wahl zwischen Objektspeicher in der Cloud, einer lokalen Speicherumgebung oder Hybrid-Storage verschiedene Aspekte zu berücksichtigen. So ist ein Objektspeicher sehr günstig und prinzipiell unbegrenzt verfügbar. Objektspeicher sind aber teuer, wenn viele kleine I/O-Operationen stattfinden. Ein Vorteil ist jedoch bei der internen Replikation gegeben. Lokaler Speicher ist hingegen generell kostenintensiv und die Replikation erhöht den Bedarf an Speicherressourcen linear.

Hybrid-Storage – als vielerorts etablierter Mittelweg – bietet Kosteneinsparungen, ist aber trotzdem für die meisten Szenarien schnell. Die nötigen Datenbewegungen, um bei zeitkritischen Workloads schnelles Datenhandling zu ermöglichen, erfolgen völlig unbemerkt im Hintergrund. Dieser Ansatz bietet die Möglichkeit, große, ältere Datensätze auf S3 vorzuhalten, und kleine aktuelle Daten-

sätze lokal zu speichern. Der lokal bereitstehende Cache sorgt für die Extraportion an Geschwindigkeit bei häufigen I/O-Operationen. Hybrid-Storage ist somit im Vorteil vor dem Hintergrund, dass 95 Prozent der Anfragen auf schnelle Daten gerichtet sind. Ein weiterer Pluspunkt ist das automatische Unloading, wenn der Speicherplatz knapp wird.

Cloud-Datenzugriff auf dem Prüfstand

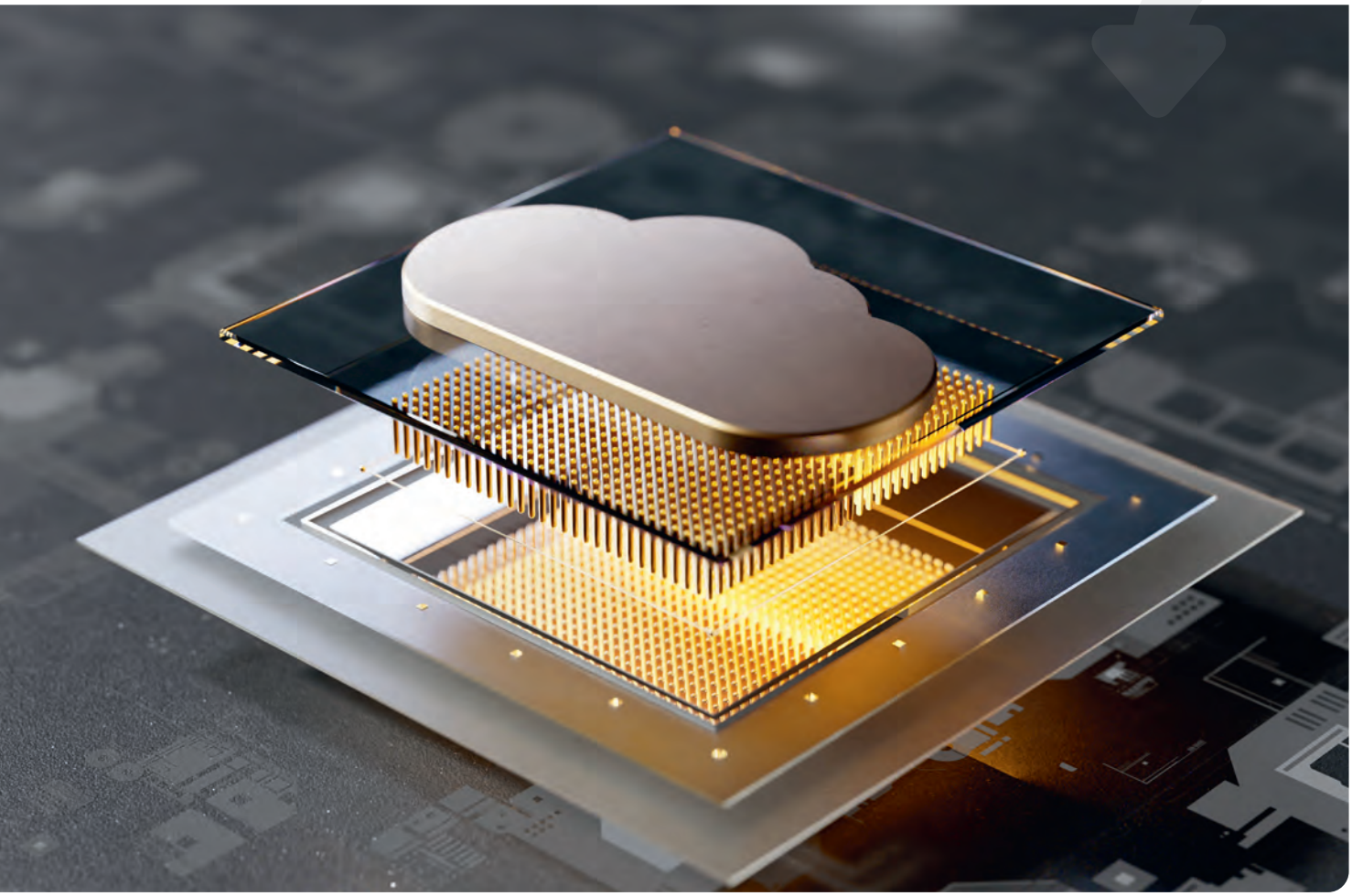
Versuche, die DoubleCloud in der Praxis umgesetzt hat, zeigen, dass beim Datenzugriff auf S3 „kalte" Abfragen deutlich mehr Zeit in Anspruch nehmen. Dies ist der Nachteil bei der Verwendung von Objektspeicher anstelle von lokalem Speicher. Wenn Benutzer jedoch dieselbe Abfrage zweimal ausführen, nutzt das im Test herangezogene Datenbank-Managementsystem ClickHouse die interne Zwischenspeicherung, um die nachfolgenden Abfragen zu beschleunigen. Die Abfragen sind dann in der Regel „nur" 1,5- bis 3-mal langsamer. Bei kaltem Cache kann sich die Abfragezeit sogar um den Faktor zehn erhöhen. Wie dieses Ergebnis zu werten ist, hängt natürlich von der Arbeitslast ab. Werden ständig alte Daten abgefragt, dann ist ein Faktor von drei oder mehr als kritisch einzustufen. In anderen Fällen kann sich mit S3 die Zugriffszeit etwas verkürzen, da es bei Abfragen auf alte Daten mitunter nicht zu Konflikten mit den Caches des File-Systems kommt.

Da die Kosten für S3-Objektspeicher etwa fünfmal niedriger liegen als für EBS (Elastic Block Store), bietet eine Hybrid-Storage-Lösung eine kosteneffiziente Option. Benutzer können hybriden Speicher auf Tabellenebene einrichten und unterschiedliche TTL-Richtlinien (Time to Live) für verschiedene Tabellen konfigurieren, je nach Anwendungsszenario. Sie müssen zudem ihre Anwendungen nicht anpassen, sondern ändern einfach die Einstellungen in den Clustern.

Hybrid-Storage: Kein Allheilmittel, aber kosteneffizient

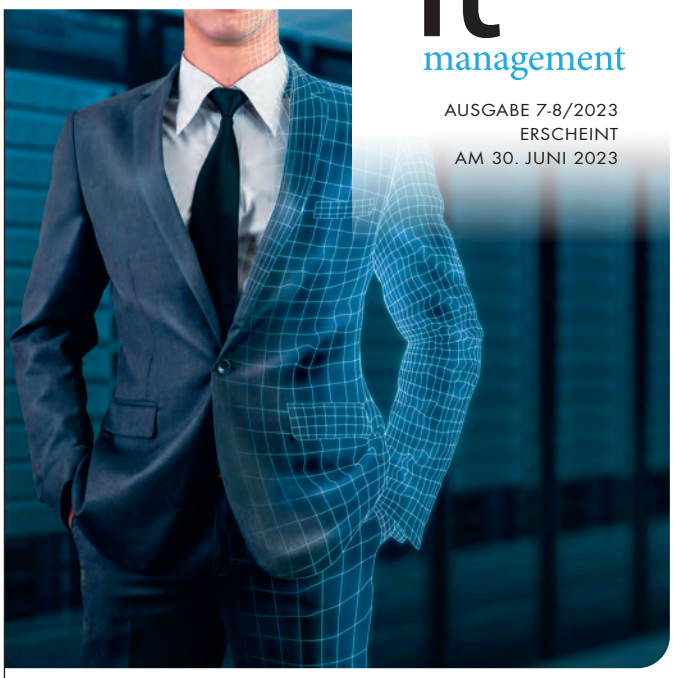
Für Unternehmen, die permanent einen großen Teil ihres Datenbestands abrufen müssen, ist Hybrid-Storage aufgrund des verlangsamten Datenzugriffs vielleicht nicht die richtige Lösung. In der gängigen Praxis nutzen Unternehmen jedoch aktive Daten während 99 Prozent, und die restlichen Daten nur ein Prozent der Zeit. Wenn der etwas langsamere Zugriff für zeitlich ein Prozent des Datenzugriffs verschmerzbar ist, kann Hybrid-Storage mit einer überzeugenden Kosteneinsparung punkten.

Stefan Käser



it management

AUSGABE 7-8/2023
ERSCHEINT
AM 30. JUNI 2023



UNSERE THEMEN

Digitale Transformation
Lizenzmanagement
Bank, Controlling, Finance

it security

AUSGABE 7-8/2023
ERSCHEINT
AM 30. JUNI 2023

UNSERE THEMEN

Cybercrime: Detect & Respond
Security Awareness
Verschlüsselungstechnologien

WIR WOLLEN IHR FEEDBACK

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

INSERENTENVERZEICHNIS

IMPRESSUM

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

Chefredaktion: Silvia Parthier (-26)

Redaktion: Carina Mitzschke (nur per Mail erreichbar)

Redaktionsassistenz und Sonderdrucke: Eva Neff (-15)

Autoren: Vincent Effertz, Marcin Fijalkowski, Gabriel Frasconi, Karl Fröhlich, Ralf M. Haaßengier, Andreas Käser, Dr. Jürgen Klein, Frank Laschet, Michaela Mars-Matzke, Carina Mitzschke, Silvia Parthier, Ulrich Parthier, René Scheffler, Martin Schneider, Christoph Schuler, Christian Schwaiger, Amadeus Thomas, Thomas Timmermann, Ralph Weiss

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.

Das E-3 Magazin

SUMMIT DER SAP-COMMUNITY

COMPETENCE CENTER

Salzburg, 1. und 2. Juni 2023

April 2023:

Das Magazin zum Competence Center Summit 2023

In dieser Ausgabe befindet sich das E-3 Extra zum Summit mit dem Beitrag zur SAP-Keynote von Uwe Grigoleit sowie weiteren Wissensbeiträgen der Aussteller und Sponsoren über Automatisierung, SolMan und ALM, Monitoring, Lizenzmanagement und natürlich Steampunk als zweite Keynote auf dem Summit in Salzburg.

Conversion, ALM, Lizenzen und Steampunk,

die SAP-Basis-Funktionen und damit das CCC, Customer Competence Center, und CCoE, Customer Center of Expertise, sind sowohl für die Private (On-prem) als auch für die Public Cloud die Garantie für nachhaltigen Erfolg. Wir greifen die Tradition des erfolgreichen CCC-Forums auf und präsentieren den Competence Center Summit 2023.

Auf dem Weg nach Hana und S/4 entstehen viele Fragen hinsichtlich Betriebsmodell, Architektur, Lizenzen und natürlich Basissupport. Viele dieser Fragen werden am 1. und 2. Juni in Salzburg auf dem Summit 2023 beantwortet.

Der Summit liefert die On-prem- und Cloud-Antworten zu SolMan und ALM sowie Maintenance, Monitoring, System- Updates, Applikationsbetreuung, Programmdokumentation, DevOps und API, Change Management, ITSM und 1st/2nd Support, Sourcing-Strategien, Automatisierung und Modifikationen, DB-Management und Berechtigungsmanagement etc.

Jetzt anmelden: Die Teilnahmegebühr zum Summit exkl. USt. beträgt 590,– Euro.

Alle Infos unter e-3.de/summit-cc

E-3 Summit **COMPETENCE CENTER** wird gesponsert von:

DATA MIGRATION INTERNATIONAL · itesys · new relic

e-3.de/summit-cc/

1 connect Mobilfunk- und 5G-Netztest, Heft 01/2023: „sehr gut“ (894 Punkte) für O_2; insgesamt wurden vergeben: 2x „sehr gut“ (915 und 894 Punkte) und 1x „überragend“ (952 Punkte). 5G ist für geeignete Endgeräte an immer mehr Standorten verfügbar. Weitere Informationen unter: o2.de/netz

2 Mobilfunk-Studie 2022 durchgeführt vom Marktforschungsinstitut SWI Finance für Handelsblatt, Veröffentlichung Handelsblatt am 28.9.2022: „sehr gut“ (87,4 Punkte) für O_2 Business; insgesamt wurden vergeben: 2x „sehr gut“ (87,4 und 85,3 Punkte) und 4x „gut“.

it security

Detect. Protect. Respond.
Mai/Juni 2023

Aagon
Unified Endpoint Management
ab Seite 8

CYBER-RESILIENZ & MDR-SERVICES

Hand in Hand für mehr Sicherheit

Sven Janssen, Sophos Technology GmbH

www.it-daily.net

IT WELT.at is IT

IT NEWS

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

itwelt.at

IT TERMINE

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

itwelt.at/events

IT UNTERNEHMEN

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

itwelt.at/top-1001

IT JOBS

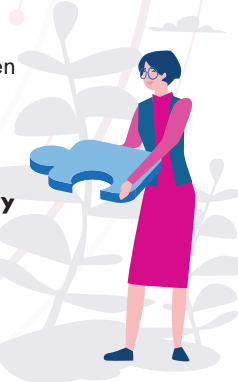
Hier sind laufend aktuelle IT Job-Angebote zu finden. In Zusammenarbeit mit der Standard.at/Karriere, dem Jobportal der Tageszeitung Der Standard, findet man auf dieser Plattform permanent hunderte offene Stellen aus dem Bereich IT und Telekom. Eine aktive Jobsuche nach Tätigkeitsfeld und Ort ist natürlich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

itwelt.at/jobs

Inhalt

COVERSTORY

IT SECURITY



Cyber-Resilienz und MDR-Services

HAND IN HAND FÜR MEHR SICHERHEIT

Cybersicherheit ist ein Thema, das uns gefühlt schon immer begleitet und das von Jahr zu Jahr wichtiger, aber auch komplexer wird. Durch die sich ständig verschärfende Bedrohungslage und das mittlerweile hoch professionelle Verhalten der Cyberkriminellen sind Unternehmen zu Sicherheitsstrategien angehalten, die auf einem weit höheren Level stattfinden als noch vor wenigen Jahren. Cyber-Resilienz ist ein wichtiges Stichwort und dazu gehört zusätzlich zur Software- und KI-gesteuerten Sicherheit auch eine menschliche Komponente in Form von Security-Services. Über die Managed Detection and Response (MDR)-Services sprechen Sven Janssen, Director Channel Sales DACH bei Sophos und Ulrich Parthier, Herausgeber it security.

Ulrich Parthier: *Wie kann man den heutigen Status der Cyberbedrohung kurz beschreiben und wie das Verhalten der Unternehmen?*

Sven Janssen: Die Landschaft der Cyberbedrohungen ist heute unglaublich vielfältig, wobei die Angriffstaktik über Ransomware nach wie vor und voraussichtlich auch in Zukunft den gefährlichsten Part einnimmt. Es ist nicht nur so, dass die Summen für die Lösegeldforderungen stetig steigen und dass die Akteure dahinter ihre Angriffe auf technisch höchstem Niveau durchführen. Die Cyberkriminellen haben zusätzlich zur Verschlüsselung der Daten den Datendiebstahl für sich entdeckt. Das hat zwei Gründe. Erstens sind viele Unternehmen mit ihrer Sicherheitsstrategie gegen Verschlüsselung heute besser gerüstet und verfügen über sichere Backups, was sie vor Lösegeldforderungen schützt. Der Datendiebstahl und der angedrohte Verkauf im Darknet ist jedoch für viele Unternehmen ein Grund, sich den Erpressern zu ergeben und zu bezahlen.

Auf der anderen Seite haben wir die Unternehmen, die sich deutlich bewusst sind, wie gefährlich das Internet ist. Allerdings hat eine unserer Studien ergeben, dass die Security immer noch nicht genügend in den Chefetagen angekommen ist, obwohl sie durchaus businesskritisch ist. Die große Mehrheit der befragten Manager (rund 81 Prozent) gab an, ein hohes bis sehr hohes Bewusstsein für IT-Sicherheit zu haben. Je größer die Unternehmen jedoch sind, desto weniger sieht sich die Führungsebene tatsächlich in der Verantwortung. Vor dem Hintergrund der aktuellen und neuen Regeln der Geschäftsführerhaftung ist das im Grunde fahrlässig.

Ulrich Parthier: *Cyber-Resilienz ist derzeit eines der Top-Themen. Was genau verstehen Sie darunter und wie setzt Sophos diesen Ansatz um?*

Sven Janssen: Zum einen ist Cyber-Resilienz die nächste höhere Stufe über

> WIR VERSTEHEN UNTER CYBER-RESILIENZ AUCH, UNTERNEHMEN MIT UNSEREN MANAGED DETECTION AND RESPONSE (MDR)-SERVICES AUS IHRER NOT ZU HELFEN. DENN NUR WENIGE UNTERNEHMEN HABEN DAZU DIE RESSOURCEN.
>
> **Sven Janssen, Senior Director Channel Sales, Sophos Technology GmbH, www.sophos.com**

der klassischen Security. Dabei geht es vor allem darum, eine noch höhere Erkennungssicherheit zu erreichen und auch die gezielten und trickreichen Angriffe abzuwehren. Die heute sehr guten technischen Lösungen aus vernetzten Security-Ökosystemen in Verbindung mit künstlicher Intelligenz werden daher mit menschlicher Expertise ergänzt. Denn Fakt ist, dass die technische Security zwar enorm viele Angriffe erkennen und abwehren kann. Für die letzten paar Prozent zur maximal möglichen Sicherheit benötigt man aber hoch spezialisierte Experten, die kontinuierlich die IT-Umgebung der Kunden beobachten und dabei die trickreichen Angriffe der besonders versierten Cyberkriminellen erkennen.

Zweitens verstehen wir unter Cyber-Resilienz auch, Unternehmen mit unseren Managed Detection and Response (MDR)-Services aus ihrer Not zu helfen. Denn nur wenige Unternehmen haben die Ressourcen, einen ganzen Stab an Security-Experten an Bord zu holen – ganz abgesehen davon, dass solche Experten schwer zu finden sind.

? **Ulrich Parthier:** *Und diese Experten sitzen bei Sophos und werden im Fall der Fälle selbstständig aktiv?*

Sven Janssen: Bei MDR-Services lagern Unternehmen den Sicherheitsbetrieb an externe Experten wie beispielsweise Sophos aus. Zu den Serviceleistungen gehören Analysen durch ein Expertenteam, Bedrohungssuche (Threat Hunting), Überwachung in Echtzeit sowie die Reaktion auf Vorfälle, kombiniert mit Technologien zum Erfassen und Analysieren von Bedrohungsdaten. Die Security Services werden je nach Vereinbarung mit dem Kunden auch selbstständig aktiv. Im Modus „Benachrichtigung" werden Kunden bei einer erkannten Bedrohung informiert und bekommen Detailinformationen, um eigene Teams bei der Priorisierung der potenziellen Gefahr zu unterstützen und die entsprechende Reaktion auszulösen. Im Modus „Zusammenarbeit" interagieren die Sophos-Experten mit den Ansprechpartnern, um auf erkannte Bedrohungen zu reagieren. In der dritten Variante kümmert sich das Sophos MDR-Team im Modus „Autorisierung" um alle erforderlichen Maßnahmen zur Eindämmung und Beseitigung von Bedrohungen inklusive der Information über die ergriffenen Maßnahmen. Diese Variante könnte man als Äquivalent für das individuelle Security Operations Center als umfassend gemanagter Service im Kampf gegen Cyberangriffe bezeichnen.

? **Ulrich Parthier:** *Ersetzen die MDR-Services ein klassisches SOC?*

Sven Janssen: Klassische Security Operations Center fand man in der Vergangenheit aufgrund der Komplexität und der hohen Kosten fast ausschließlich bei großen Unternehmen. MDR hat mit seinem Service-Konzept einen noch größeren Umfang und ist auch für KMUs in Reichweite. MDR-Services ersetzen also nicht nur das SOC, für viele Unternehmen macht es dieses Level an Sicherheit überhaupt erst möglich. Zudem greift ein MDR-Angebot nicht nur auf interne Datenquellen zu, sondern das Threat Hunting profitiert von einem riesigen Data Lake, der mit Daten aller Sophos-Kunden gefüttert wird. Das bietet ein riesiges Potenzial für effektive Bedrohungssuche.

? **Ulrich Parthier:** *Sie sprechen mit Reichweite die Kosten für MDR-Services an. Ist MDR wirklich günstiger und im Gegensatz zu einem SOC wirtschaftlich realisierbar?*

Sven Janssen: Unternehmen, die ihr eigenes SOC implementieren möchten, erkennen schnell, wie schwierig sich der Aufbau und vor allem der Betrieb gestaltet. Selbst in kleinen und mittelständischen Unternehmen würden mindestens vier Cybersecurity-Analysten benötigt, um ein SOC rund um die Uhr, jeden Tag im Jahr zu besetzen. Größere Unternehmen benötigen noch mehr teure Fachkräfte, die, wie gesagt, nur sehr schwer zu finden sind. Darüber hinaus braucht es Teamleiter und IT-Engineers zur Anpassung und Wartung von Tools. Zu diesen Personalkosten kommen weitere Kosten für Tools hinzu. Als Service entfällt ein großer Teil der genannten Personal- und Betriebskosten und ein Anbieter wie Sophos beziehungsweise die Partner können dies nicht nur aus wirtschaftlicher Sicht zu besseren Konditionen anbieten, sondern gleichzeitig mit einer weltweit vernetzten und damit wesentlich höheren Expertise.

? **Ulrich Parthier:** *Wie würden Sie in einem Elevator-Pitch die Vorteile von MDR-Services für Unternehmen beschreiben?*

Sven Janssen: Zusammengefasst gibt es fünf Gründe, weshalb Unternehmen zusätzlich zu einem technologie- und softwarebasierten Security-Ökosystem auch auf MDR-Services mit menschlicher Expertise setzen sollten: Die Härtung der Cyber-Abwehr, die Entlastung der verfügbaren IT-Ressourcen, das Hinzufügen von echter Expertise anstatt Headcount, die Optimierung des Return on Investments in die Cybersecurity und vor allem die Konzentration aller verfügbaren Ressourcen auf das Kerngeschäft.

! **Ulrich Parthier:** *Herr Janssen, herzlichen Dank für das Gespräch.*

Ein Schritt nach vorn für die Cybersicherheit?

GESETZE ZUR CYBER-RESILIENZ UND GESCHÄFTSFÜHRERHAFTUNG

Gesetze sind dafür da, Dinge klar zu regeln und im Idealfall sogar zu verbessern. Dazu gehören zu Recht Regeln zur Cybersicherheit, denn die Bedrohungslage wird seit Jahren zunehmend prekär und es entstehen große wirtschaftliche Schäden, sowohl für einzelne Unternehmen als auch aus volkswirtschaftlicher Perspektive. Zu den neuesten Gesetzen zählen das EU-weite Cyber-Resilienz-Gesetz sowie die Geschäftsführerhaftung bei Cyberangriffen.

Compliance-Anforderungen

Eine funktionierende und sichere IT ist für jedes Unternehmen von elementarer Bedeutung. Bei Cyberangriffen oder Verstößen gegen IT-sicherheitsrechtliche Vorschriften drohen dem Vorstand, der Geschäftsführung und/oder den Aufsichtsratsmitgliedern rechtliche Konsequenzen. Die Geschäftsleitung oder Aufsichtsratsmitglieder können zivilrechtlich auf Schadensersatz haften, wenn sie ihre Pflichten zur Sicherstellung der Digital Compliance vorsätzlich oder fahrlässig verletzen. Darüber hinaus können die Mitglieder der Geschäftsleitung und des Aufsichtsrats auch strafrechtlich belangt werden. Ein solcher Fall wäre denkbar, wenn aufgrund vorsätzlichen oder fahrlässigen Verhaltens durch einen Cybervorfall Geschäftsgeheimnisse oder Know-how des Unternehmens gegenüber unbefugten Dritten offenbart werden oder ein Angriff dazu führt, dass das Unternehmen seinen Geschäftsbetrieb vollständig einstellen muss und dadurch in die Insolvenz schlittert.

BEI IHREM RISIKOMANAGEMENT DÜRFEN DIE VERANTWORTLICHEN NICHT ALLEIN AUF TECHNISCHE MASSNAHMEN SETZEN, SONDERN MÜSSEN MENSCHLICHE EXPERTISE EINBINDEN.

Michael Veit, Security-Experte, Sophos Technology GmbH, www.sophos.com

Dem Unternehmen selbst können ebenfalls erhebliche Geldbußen drohen. Das Gesetz vom das Bundesamt für Sicherheit in der Informationstechnik (BSIG), das vor allem die Betreiber „Kritischer Infrastrukturen", die Anbieter „Digitaler Dienste" und „Unternehmen im besonderen öffentlichen Interesse" betrifft, sieht Geldbußen in Höhe von bis zu 20 Millionen Euro vor. Nach der kürzlich verabschiedeten Richtlinie NIS 2.0 wird sich dieser Rahmen künftig weiter verschärfen. Die Richtlinie sieht Sanktionen in Höhe von zwei Prozent des weltweiten Jahresumsatzes vor. Noch drastischer können sich Verstöße gegen die datenschutzrechtlichen Vorschriften auswirken. Hier drohen Geldbußen von bis zu 20 Millionen Euro oder vier Prozent des weltweiten Jahresumsatzes. Die neue EU Cybersecurity-Richtlinie NIS2 ist längst überfällig und wird dringend benötigt. Die Harmonisierung für die Einhaltung der Vorschriften in den einzelnen Mitgliedstaaten in Verbindung mit klar definierten Meldepflichten und Einhaltungsvorschriften sowie die Aktualisierung im Hinblick auf moderne Bedrohungen, sollten die Sicherheit und Stabilität der EU bezüglich disruptiver Angriffe erheblich verbessern. Die erweiterte Liste der Branchen ist zu begrüßen, lässt aber immer noch die Tür für nicht regulierte Unternehmen offen, die durch Angriffe auf die Lieferkette ein Risiko darstellen können.

EU Cyber-Resilienz-Gesetz

2022 hat die Europäische Union zudem einen Gesetzentwurf mit dem Titel „Cyber Resilience Law" vorgelegt. Darin wird ein horizontaler europäischer Ansatz zur Cybersicherheit befürwortet, der insbesondere Hardware- und Softwarehersteller betrifft, da diese die größte Verantwortung bei der Entwicklung (sicherer) technologischer Mittel tragen. Die Europäische Union hat große Ambitionen in Bezug auf dieses Cybersicherheitsgesetz. Sie glaubt zum Beispiel, dass sie durch klare Regeln für Technologiehersteller die Zahl der Cyberangriffe und damit die Gesamtkosten der Cyberkriminalität um 290 Milliarden Euro pro Jahr senken kann. Es steht die Frage im Raum: Wie realistisch sind diese Ambitionen?

Die Aufgabe besteht darin, die wichtigsten Engpässe im Bereich der Cybersicherheit zu ermitteln. Dabei sind jedoch strukturelle Herausforderungen zu meistern. Die erste ist das allgemeine Sicherheitsniveau der Technologie. Jedem vierten auf dem Markt befindlichen IKT-Produkt (Informations- und Kommunikationstechnologie) wird ein „niedriges" oder „sehr niedriges" Sicherheitsniveau attestiert. Einige Hersteller nehmen Abstriche bei der Sicherheit in Kauf, um ihre Produkte schneller auf den Markt zu bringen. Wenn das anfänglich niedrige Sicherheitsniveau später durch Updates korrigiert wird, geschieht dies meist, wenn eine Schwachstelle bereits entdeckt wurde. Das zweite strukturelle Problem ist der Mangel an Wissen über den verantwortungsvollen Umgang mit IKT-Produkten. In Europa geben sieben von zehn Nutzern zu, dass sie nicht ausreichend über die Risiken von Cyberangriffen informiert sind. Darüber hinaus betrachten die Endnutzer beim Kauf von Produkten die Sicherheit nicht als Hauptkriterium, weil sie zu oft annehmen, dass sie mit dem Design einhergeht.

Risikomanagement – Technik ist nicht genug

Bei ihrem Risikomanagement dürfen die Verantwortlichen – sprich Geschäftsleitung und Hersteller – nicht allein auf technische Maßnahmen setzen, sondern müssen menschliche Expertise einbinden. Denn viele Angriffe, bei denen sich die Hacker durch gestohlene Informationen Zugriff auf die Daten und Systemen ihrer Opfer verschaffen, verlaufen still und heimlich. Die Unternehmen stehen vor der Herausforderung, diese Angriffe bereits in der Entstehungsphase zu stoppen, noch bevor ein Schaden entstehen kann. Hierzu sind spezialisierte Bedrohungsexperten notwendig, die auf dem Arbeitsmarkt nur schwer zu finden sind und oft teuer eingekauft werden müssen. Die Folge: Zunehmend mehr Unternehmen entscheiden sich für Security-Services zusätzlich zu den technischen Security-Maßnahmen. Dazu zählen vornehmlich die MDR-Services (Managed Detection and Response), welche die eigene IT-Abteilung bei der Aufdeckung und Bekämpfung von Cyberangriffen unterstützt. Das ist nicht nur ein Trend. Denn laut Analysten von Gartner werden bis 2025 rund 50 Prozent aller Betriebe einen MDR-Service nutzen.

Um nachzuvollziehen, welche Vorteile ein MDR-Service bietet und was sich hinter der wachsenden Nachfrage verbirgt, ist es wichtig zu verstehen, was ein MDR-Service eigentlich ist – und was nicht. Managed Detection and Response (MDR) ist ein 24/7 Fully-Managed Service durch ein Team von Sicherheitsexperten, das darauf spezialisiert ist, Cyberangriffe zu erkennen und zu bekämpfen, die Technologielösungen allein nicht verhindern können. Die tägliche Cybersecurity-Verwaltung, wie die Bereitstellung von Sicherheitstechnologien, die Aktualisierung von Richtlinien oder die Installation von Updates, sind dagegen nicht Teil des MDR-Services. Managed Service Provider (MSPs) bieten entsprechende IT Security Management Services für Unternehmen und Einrichtungen, die Unterstützung in diesem Bereich benötigen.

Dass die Marktexperten von Gartner mit ihren Prognosen Recht haben, zeigt das große Interesse an Sophos MDR: Weltweit vertrauen bereits über 15.000 Unternehmen und Einrichtungen diesen Services. Und genau dieses Bewusstsein für das heutige und künftige Risiko im Cyberraum und das Engagement, die bestmögliche Security einzusetzen, wird Unternehmen und Hersteller gleich doppelt schützen: vor Cyberattacken auf das eigene Unternehmen und davor, mit den neuen Gesetzen zu Cyber-Resilienz und Geschäftsführerhaftung in Konflikt zu geraten.

Michael Veit

CHEFSACHE IT-SECURITY?

46,3 %
sagen, dass die IT-Security seit mindestens zwei Jahren auf einer höheren Hierarchie angesiedelt ist

bei **39,8 %**
der deutschen Unternehmen kümmert sich hauptsächlich die IT-Abteilung um die IT-Security

16,4 %
der deutschen Unternehmen sehen IT-Security als Chefsache an

bei **33,8 %**
der deutschen Unternehmen kümmert sich hauptsächlich ein Dienstleister um die IT-Security

(Quelle: Sophos)

Konsolidierung des Unified Endpoint Managements

DAS ZIEL HEISST: EINE EINHEITLICHE LÖSUNG!

Noch keine UEM-Lösung im Einsatz, Silolösungen oder Lösungen unterschiedlicher Hersteller in verschiedenen Werken und Tochtergesellschaften – das ist vielerorts noch business as usual. Über Lösungsansätze und Chancen sprach Ulrich Parthier, Herausgeber it management, mit Sebastian Weber, Head of Product Management bei Aagon.

Ulrich Parthier: *Picken wir uns exemplarisch einmal die Unternehmen heraus, die auf der grünen Wiese beginnen, also noch kein UEM im Einsatz haben. Wie gehen Sie hier vor? Gibt es ein Vorgehensmodell?*

Sebastian Weber: Mittels Inventarisierung verschaffen wir uns zunächst einmal einen Überblick über die Client- und Serverlandschaft: Wie viele Arbeitsplätze gibt es, auf wieviel Standorte sind sie verteilt, welches Wachstum weist die IT-Landschaft auf? Ab etwa 50 Devices kann man damit rechnen, dass ein effizientes Reagieren auf Incidents nicht mehr zu bewältigen ist. Zusätzlich zur Arbeitserleichterung – Stichwort Turnschuh-Administration – geht es also heute in gleichen Teilen um Security.

Maßnahmen zur Vorsorge und Abwehr von Bedrohungen zu treffen, ist für kleine und mittelständische Unternehmen inzwischen obligatorisch, jedoch aufgrund des notwendigen Umfangs sehr personalintensiv oder nicht leistbar. Diese Maßnahmen lassen sich sehr gut mit einer UEM-Lösung wie der ACMP Suite umsetzen. Bei der Inventarisierung werden alle Clients in der Zentralkomponente erfasst, bei Aagon ist dies mit ACMP Core möglich. Anschließend kann es umstandslos mit den automatischen Updates und Patches losgehen; weitere Ausbaustufen wie OS Deployment, Lizenzverwaltung, Schwachstellenmanagement und ähnliches lassen sich schnell anschließen und erhöhen die Sicherheit der Infrastruktur.

Ulrich Parthier: *Unified Endpoint Management, warum ist es so wichtig, eine solche Lösung im Einsatz zu haben?*

Sebastian Weber: Kleine und mittelständische Unternehmen beschäftigen aus Kosten- und Kapazitätsgründen in der Regel nicht jeweils eigene Teams für Security, UEM oder Patching. Sie müssen alle Bereiche von Client Management und Security mit dünner Personaldecke bewältigen und suchen deshalb nach den besten Arbeitserleichterungen. Diese bieten ihnen UEM-Lösungen, denn damit können IT-Abteilungen alle Endgeräte im Netzwerk über eine zentrale Konsole verwalten und auf aktuellem Stand halten. Der wesentliche Punkt ist dabei, dass dies automatisiert stattfindet.

Die Automatisierung entlastet IT-Abteilungen nicht nur von aufwändigen manuellen Wartungsaufgaben, sie ermöglicht auch das Erreichen eines deutlich höheren Sicherheitsniveaus im Unternehmen. Denn neben Inventarisierung, Asset-, Update- und Patch Management gehört heute eben auch das Schwachstellen (Vulnerability)-Management zu den festen Modulen einer UEM-Lösung. In Anbetracht von Zero-Day-Exploits und ähnlichen Attacken ist es schlichtweg nicht mehr möglich, bei neuen Schwachstellen manuell angemessen gegenzusteuern. Erst Automatisierung garantiert bestmöglichen Schutz, weil dadurch ein jederzeitiger, aktueller Überblick über die Client-Landschaft gegeben ist.

Ulrich Parthier: *Wenn die Anforderungsphase abgeschlossen ist, also beispielsweise welche Geräte sollen unterstützt werden, welche Funktionen benötigen sie, welche Sicherheitsanforderungen müssen erfüllt werden, wie sieht es mit Integrationen, Skalierbarkeit und Support aus, dann stellt sich die Frage: welches ist das richtige Tool? Es gibt eine Vielzahl von UEM-Lösungen auf dem Markt. Helfen hier Checklisten weiter?*

Sebastian Weber: Aus unserer Marktbeobachtung heraus scheuen es Unternehmen, für verschiedene Einsatzzwecke jeweils spezielle Tools verschiedener Hersteller einzusetzen. Dagegen sprechen Kostengründe sowie auch die Handhabbarkeit. Bei Aagon setzen wir deshalb auf einen integrierten Ansatz. Dabei stehen alle Funktionalitäten im Zusammenhang mit Endpoint Management und IT-Security innerhalb einer Konsole bereit und werden darin verknüpft: Softwareverteilung, OS Deployment, Patch- und Schwachstellenmanagement und weitere. Der User kann sie je nach Bedarf lizenzieren und damit aktivieren.

Ulrich Parthier: *Automatisierung zum gebündelten Abarbeiten von Sicherheitsmaßnahmen läuft seit einiger Zeit unter dem Schlagwort Security Orchestration, Automation and Response, kurz SOAR. Können Unternehmen mit einer UEM-Lösung also SOAR umsetzen?*

Sebastian Weber: Beim SOAR-Konzept geht es um nichts anderes als um eine Sammlung von Funktionen, die darauf abzielen, durch Standardisierung und Priorisierung automatisiert und damit effizient auf erkannte Bedrohungen zu reagieren. Die drei grundlegenden SOAR-Bausteine für Sicherheits-Teams sind: Case- und Workflow-Management, Aufgabenautomatisierung sowie eine zentrale Methode, um Bedrohungsinformationen (die so genannte Threat Intelligence) aufzurufen, zu durchsuchen und zu teilen.

Jedes KMU, das seine Endpoints bereits über eine UEM-Plattform administriert, hat also im Prinzip schon alle Zutaten beisammen, die es zur Umsetzung von SOAR benötigt. Über eine einheitliche Konsole lässt sich SOAR daher im Mittelstand unkompliziert anwenden. Das funktioniert wie erläutert über die Verknüpfung der einzelnen Module: Aus dem Schwachstellenmanagement lässt sich mit wenigen Klicks ein Prozess erstellen, der bestimmt, dass ein Patch zur Fehlerbehebung eingespielt wird.

Ulrich Parthier: *Als Gründe, warum noch kein UEM im Einsatz ist, werden oft die Kosten und das fehlende Know-how von Mitarbeitern genannt. Sind diese Gründe nur vorgeschoben, und wie kann man sie gegebenenfalls entkräften?*

Sebastian Weber: Sobald die Fachkräfte in der IT-Administration erkannt haben, wie viel Zeit sie durch Einsatz einer UEM-Lösung sparen können, muss man eigentlich niemanden mehr groß überzeugen. Ihnen bleibt dadurch wesentlich mehr Freiraum für strategische Aufgaben, die sich nicht rein manuell erledigen lassen. Und mit dem schnellen ROI einer UEM-Lösung rennt man auch im Management offene Türen ein. Natürlich spielt die einfache Bedienung einer Konsole eine wesentliche Rolle bei der Akzeptanz – ganz unbenommen davon, dass in IT-Abteilungen technisches Know-how ja ohnehin selbstverständlich sein dürfte.

Ulrich Parthier: *Nun wird die IT ja immer komplexer, Stichwort On-Premises, Cloud, Managed Services. Was raten Sie hier den Unternehmen?*

Sebastian Weber: Wir haben es mit einer Komplexitätszunahme in zweierlei Hinsicht zu tun: Nicht nur die Security-Herausforderungen, auch übliche bekannte IT-Herausforderungen nehmen zu, weil die meisten Unternehmen heute in hybriden Umgebungen arbei-

ten, das heißt, sie sind sowohl On-Premises als auch in der Cloud unterwegs.

In hybriden Umgebungen kommen zu den herkömmlichen Clients noch einmal viele weitere Assets hinzu, die gleichwertig geschützt werden müssen: Ladesäulen, Zutrittskontrollen, IoT-Devices, Temperatursensoren in der OT. Sie alle stellen Angriffsflächen dar; gleichzeitig werden die Attacken immer raffinierter und intelligenter. Dies zusammengenommen spricht gerade für UEM, denn Unternehmen stehen vor der Aufgabe, cloud-basierte und inhouse installierte Security-Lösungen unter ein Dach zu bringen und zentral zu managen. Genau hier kann UEM umfassend unterstützen.

Ulrich Parthier: *Als Ersatz für eine vollintegrierte Lösung müssen oft Teillösungen herhalten, die bereits tief im Betriebssystem integriert sind – wie Microsoft Defender und BitLocker. Das kostet nichts und wiegt die Unternehmen in Sicherheit. Ist das eine gefährliche Strategie?*

Sebastian Weber: Ganz im Gegenteil! Microsoft hat in den letzten Jahren große Anstrengungen unternommen, seine Security-Lösungen Defender und Bitlocker zu verbessern, und dies nicht ohne Erfolg: Inzwischen sind die Redmonder Leader im Gartner Magic Quadrant for Endpoint Protection Platforms. Dass die Grundfunktionen bereits tief im Betriebssystem verankert sind, bedeutet zudem keine hohen zusätzlichen Kosten. Da die Anwenderoberfläche des Defenders, als auch BitLockers, in der Vergangenheit nicht gerade mit Benutzerfreundlichkeit geglänzt hat, hat Aagon die Module ACMP Defender Management und ACMP BitLocker Management entwickelt. Sie versetzen Administrations-Abteilungen in die Lage, die Microsoft Lösungen in nur einer Oberfläche auf allen Clients und Servern zu verwalten.

DIE AUTOMATISIERUNG ENTLASTET IT-ABTEILUNGEN NICHT NUR VON AUFWÄNDIGEN MANUELLEN WARTUNGSAUFGABEN, SIE ERMÖGLICHT AUCH DAS ERREICHEN EINES DEUTLICH HÖHEREN SICHERHEITSNIVEAUS IM UNTERNEHMEN.

Sebastian Weber,
Head of Product Management, Aagon,
www.aagon.com

Ulrich Parthier: *Funktionen und Integrationen bei UEM-Plattformen sind essentiell. Es ist ja extrem komplex, geht es doch um Gerätemanagement, Anwendungsmanagement, Datenmanagement, Identitätsmanagement und natürlich um Integrationsmöglichkeiten. Wie sehen Sie bei Aagon das Szenario?*

Sebastian Weber: Aufgrund unserer langjährigen Erfahrung im UEM-Bereich verknüpfen wir die verschiedenen Funktionalitäten wie bereits beschrieben miteinander. Aufbauend auf dem notwendigen Fundament der Inventardaten und der daraus gewonnenen Erkenntnisse entsteht die Möglichkeit des integrierten und automatisierten Security-Managements.

Ulrich Parthier: *Abschließend die Frage, wie es mit dem Reporting, der Compliance und den Auditing-Funktionen aussieht. Sind die in der Lösung bereits enthalten?*

Sebastian Weber: Eine Reporting-Funktion in unserer UEM-Konsole liefert zeitlich automatisch einstellbare Statusinformationen. In einem frei konfigurierbaren Dashboard kann die IT-Administration zusammenstellen, was im SOAR-Kontext angezeigt werden soll: Daten aus der CVE-Datenbank (Wo befinden sich die meisten betroffenen Rechner?), aktueller Patch-Stand, Auswertung des Defender (gibt es gerade besonders viele Ereignisse, auf die er reagiert hat?) etc. Auf diese Weise können auch mittelständische Unternehmen mit kleinerem IT-Budget ein zeitgemäßes SOAR-Konzept zur Sicherung ihres Netzwerkbetriebs aufsetzen.

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

THANK YOU

Unternehmen leben länger mit

IT-Security Schutzmaßnahmen

SCAN ME

Mehr Infos dazu im Printmagazin

itsecurity

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

Eine Frage der Sicherheit

IST DIE CLOUD MITTLERWEILE UNVERZICHTBAR?

In einer zunehmend auf ortsungebundener Produktivität fokussierten Welt wächst der Einsatz von cloudbasierten Infrastrukturen von Jahr zu Jahr. Doch Datenhoheit, Latenz, Infrastruktursicherheit und Menge der öffentlichen, hybriden oder privaten Cloud-Infrastrukturen werfen Fragen auf, die einer Antwort bedürfen – auch im Hinblick auf die Risiken.

Obwohl Unternehmen in den letzten zehn Jahren schrittweise Cloud-Migrationen geplant hatten, ist der Einsatz outgesourcter Hosting-Plattformen durch die mittlerweile in hybriden Arbeitsmodellen verankerte Fernarbeit zu einem besonders heiß diskutierten Thema geworden. Die Cloud ist ein Synonym für die On-Demand-Bereitstellung einer virtuellen Umgebung, die einen Pool von Ressourcen wie Computing, Speicher, Anwendungen, Datenbanken und Netzwerk über Pay-as-you-go-Preismodelle umfasst. Mit SaaS, IaaS, PaaS, SECaaS oder SASE passen sich dabei die Angebote der Cloud-Anbieter an die technischen und betrieblichen Entwicklungen der Firmen an. So bietet heute die Cloud eine erhöhte Flexibilität und ortsungebundene Produktivität sowie – je nach Strategie – eine attraktive Reduzierung der Betriebskosten. Doch nicht nur. Mittlerweile setzen Unternehmen auf Cloud-Umgebungen, um ihre Wettbewerbsfähigkeit zu steigern, besonders bei rezessiven Wirtschaftstrends. Diese Meinung teilen ebenfalls bekannte Analysten. Laut dem jüngsten Report von Research & Markets soll die Größe des globalen Marktes für Cloud-Computing-Plattformen bis 2027 mit 17,9 Prozent jährlicher Wachstumsrate (CAGR) von 545,8 auf 1.240,9 Milliarden US-Dollar steigen. Dabei soll laut Gartner allein der Umsatz öffentlicher Cloud-Infrastrukturen bereits 2023 auf 591,8 Milliarden US-Dollar wachsen, ergo knapp 21 Prozent mehr als 2022.

UM DIE VORTEILE DER CLOUD-ANWENDUNGEN UND -DIENSTE ZU NUTZEN, MUSS DER BESTE KOMPROMISS ZWISCHEN DEN ZUGANGSMÖGLICHKEITEN UND DER AUFRECHTERHALTUNG DER KONTROLLE ZUM SCHUTZ DER KRITISCHEN DATEN GEFUNDEN WERDEN.

Uwe Gries,
Country Manager DACH, Stormshield,
www.stormshield.com

Der unaufhaltsame Aufstieg der Cloud

Der Einsatz von Cloud-Diensten ist zwar besonders stark in der Hard- und Softwareindustrie, im Bankenumfeld, im Einzelhandel und im E-Commerce, aber alle Wirtschaftssparten profitieren mittlerweile davon. 2023 ist es schwer vorstellbar, ohne cloudbasierte Dienste auszukommen, besonders in Unternehmen, die sich von sesshaften Arbeitsweisen zugunsten hybrider Arbeitsplatz-/Homeoffice-Lösungen abwenden. Obwohl die Verwendung eines VPNs das Arbeiten von zu Hause aus und einen mobilen Zugriff auf Unternehmensressourcen ermöglicht, bedarf die VPN-Nutzung eines zusätzlichen Aufwands seitens des Benutzers. In der Zwischenzeit sind Cloud-Plattformen – egal ob es sich um CRMs oder SaaS-Büroumgebungen handelt – direkt von jedem Ort aus und mit jedem Gerät verfügbar. SaaS-Anwendungen können insbesondere von überall aus bereitgestellt, konfiguriert und genutzt werden und sind für Administratoren genauso bequem wie für Benutzer. Besonders in KMUs müssen keine infrastrukturellen Fragen geklärt werden, also etwa die Installation von Software (Server und Clients) oder die Bereitstellung von Remote-Zugriffen. Für mittlere und große Unternehmen ist der Wechsel jedoch nicht so einfach. Der Umstieg von einer On-Premises- auf eine Cloud-Lösung ist mit Kosten verbunden, die geplant werden müssen. Die Migration von inhouse produzierten und verarbeiteten Daten, die Schulung der Anwender, die Sicherung der Plattform und des Zugriffs: Ein Projekt dieser Größenordnung kann sich auf die Mitarbeiterproduktivität und insgesamt auf die Sicherheit des Unternehmens auswirken. Eine Kompromisslösung, die sowohl On-Premises- als auch Cloud-Infrastrukturelemente umfasst (also eine „hybride Cloud“) wird deshalb oft bevorzugt.

Trotz der vielen Vorteile der Cloud sind Firmen, die eine Migration anstreben, dazu gezwungen, ihre Arbeitspraktiken

anzupassen. Der Einsatz von cloudbasierten Diensten ist weit entfernt vom Marketing-Bild, das ein paar Klicks zur perfekten Infrastruktur suggeriert: Was kostet die Adoption? Welche Anforderungen und welchen Datenumfang umfasst sie? Und vor allem: Welche Sicherheitsregeln gelten? Die Beantwortung dieser Fragen erfordert eine starke Kommunikation unter den Produktions-, Logistik-, Marketings-, Vertriebs-, IT- und Sicherheitsteams. Angesichts der Dominanz von Big Tech auf dem Hosting-Markt und der Einführung des „Cloud Acts" in den Vereinigten Staaten bleibt die Sicherheitsfrage für diese Daten in Cloud-Umgebungen ein Anliegen für Unternehmen, insbesondere für europäische Organisationen.

Die Cybersicherheitsfrage

Cybersicherheits- und Datenhoheitsfragen bringen immer wieder die Tatsache zutage, dass die Sicherheit der Daten in der Cloud ein großes Anliegen für Organisationen bleibt. In zahlreichen Studien beklagen Firmen die fehlende Kontrolle über die Subunternehmerkette des Hosting-Anbieters. Auch Probleme mit den Zugriffskontrollen, mangelnde Cloud-Sicherheitsfähigkeiten und -expertise oder Herausforderungen im Bereich Datenschutz und -sicherheit gemäß der Rechtslage, besonders im Umfeld europäischer KRITIS, werden kritisiert. Denn die „Herausgabe" von Daten ist immer ein risikoreiches Unterfangen. Statista geht noch detaillierter auf die wichtigsten Cloud-Sicherheitsbedenken ein: Datenverlust und -lecks (69 %) sowie Datenschutz/Vertraulichkeit (66 %), gefolgt von versehentlicher Offenlegung von Zugangsdaten (44 %).

Obwohl diese Befürchtungen bekannt sind und laut IBM 45 Prozent der Sicherheitsvorfälle in der Cloud stattfinden, bewertet nur eine von fünf Organisationen ihre gesamte Cloud-Sicherheitslage in Echtzeit. Darüber hinaus sind CISOs oft der Meinung, dass die Absicherung von in der Cloud gespeicherten Daten eine Aufgabe ist, die spezialisierte Werkzeuge erfordert, die über die vom Cloud-Betreiber angebotenen hinausgehen. Um diese Herausforderungen zu bewältigen, werden vertrauenswürdige, cloudbasierte Sicherheitsprodukte von europäischen Cybersecurity-Herstellern und „Managed Security Service Providers" (MSSPs) angeboten. Mit Akronymen wie SECaaS („Security as a Service"), SASE („Secure Access Service Edge") und FWaaS („Firewall as a Service") stellen sie Unternehmen Werkzeuge zur Verfügung, die eine umfassende Sicherheitsstrategie ungeachtet der gewählten Cloud-Art (öffentlich, hybrid oder privat) ermöglichen. Zudem führen sie eine vertiefte Analyse der Netzströme durch, um die Kommunikation ins Internet zu sichern und zu kontrollieren, ohne die Leistung und die Nutzer-Erfahrung zu beeinträchtigen.

Die Entwicklungen und Ereignisse in der Gesellschaft scheinen somit eine klare Antwort auf die Frage zu geben, ob die Nutzung der Cloud mittlerweile unverzichtbar ist. Es gibt jedoch immer noch Fragen hinsichtlich Leistung, Kosten, lokaler Gesetzgebung und – am wichtigsten – Datensicherheit, die in jeder Diskussion von Unternehmen und Organisationen zu diesem Thema von zentraler Bedeutung sind. Um die Vorteile der Cloud-Anwendungen und -Dienste zu nutzen, muss der beste Kompromiss zwischen den Zugangsmöglichkeiten und der Aufrechterhaltung der Kontrolle zum Schutz der kritischen Daten gefunden werden. Parallel dazu ist die Cloud auch mit einer größeren Konnektivität und einer höheren Abhängigkeit von den Netzzugängen verbunden, wodurch die Probleme hinsichtlich Sicherheit und Verfügbarkeit noch größer werden.

Folglich: Cloud ja, aber nicht ohne Cybersicherheit.

Uwe Gries

ZUKUNFT ODER REALITÄT?

DOKUMENTENBASIERTE ANWENDUNGEN IN DER CLOUD

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

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

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

Die Ergebnisse der Umfrage wurden in einem Ergebnisbericht zusammengefasst.

WHITEPAPER DOWNLOAD

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

Die Produktion von JOYSONQUIN ist hoch präzise – die security-Lösung von macmon ebenso.

Erfolgreiche Zertifizierung

MACMON SECURE UNTERSTÜTZT AUTOMOBILZULIEFERER JOYSONQUIN

JOYSONQUIN Automotive Systems ist einer der drei führenden globalen Anbieter für hochwertige Innenraumausstattung. Durch die erfolgreiche Implementierung des macmon Network Bundle konnte das Unternehmen die Zertifizierungsanforderungen seiner Kunden, zu denen Mercedes-Benz, BMW, Volvo und VW zählen, in Rekordzeit erfüllen.

Der Verband der Automobilindustrie (VDA) hat mit TISAX einen Standard für Informations- und Cybersicherheit geschaffen. Ziel ist eine sichere Verarbeitung und ein vertrauensvoller Austausch von Informationen zwischen Zulieferern und Automobilherstellern. Mit TISAX wird für Zulieferer eine Zertifizierung für Informationssicherheit im Unternehmen geschaffen, die sich speziell an die Bedürfnisse der Branche richtet. Um diese zu erlangen, müssen Unternehmen die Anforderungen erfüllen, die im VDA-ISA- Prüfungskatalog festgelegt sind. Dieser besteht aus drei Modulen: **1.** Informationssicherheit, **2.** Datenschutz und **3.** Prototypenschutz.

Ziel des Moduls „Informationssicherheit" ist, dass die IT-Sicherheit in einem Unternehmen geplant, überwacht, geprüft und laufend verbessert wird. Dies setzt im Wesentlichen drei Dinge voraus: Standardisierte Prozesse, automatisierte Workflows und revisionssichere Reports. Hier greift macmon Network Access Control als IT-Security-Lösung ein.

Schnell zur umfassenden Netzwerk-Übersicht und -Kontrolle

Das Asset Management im Sinne der TISAX-Anforderungen beschäftigt sich zum einen mit Informationswerten (Daten/Informationen) und zum anderen mit Informationsträgern (IT/OT-Systeme jeglicher Art). Dabei ist es elementar, ein zentrales Verzeichnis über alle vorhandenen Assets sowie die zuständigen Personen zu führen. Durch den Einsatz von macmon NAC besteht bei JOYSONQUIN eine vollständige Transparenz über alle mit dem Netzwerk verbundenen Geräte. Gerätetypen können nach diversen Kriterien, wie dem Standort, dem Netzwerkzugang, dem Geräte-typ, dem Informationsgehalt und vielen anderen Eigenschaften gruppiert, und im Netzwerk verwaltet werden. macmon NAC erstellt damit ein Verzeichnis sämtlicher mit dem Netzwerk verbundenen Assets und liefert zudem ergänzende Informationen, wie den Lebenszyklus oder den aktuellen Standort der Geräte.

Sicherheitsrichtlinien geprüft und realisiert

macmon NAC unterstützt die Durchsetzung von Sicherheitsrichtlinien für mobile Endgeräte indem zum einen die Überprüfung der umgesetzten Sicherheitsmaßnahmen, wie Virenschutz, Windows Firewall oder installierte Patches geprüft werden, und zum anderen direkte Maßnahmen eingeleitet werden können. Mobile Endgeräte, die längere Zeit nicht im JOYSONQUIN Unternehmensnetzwerk angemeldet waren, werden in einem separaten Quarantänenetz überprüft, und falls nötig aktualisiert oder rekonfiguriert, um erst nach bestandener Sicherheitsprüfung wieder Zugriff zum Unternehmensnetzwerk zu erhalten. Die Integrität dieser Endgeräte wird durch Sicherheitsmaßnahmen aus den Bereichen des Fingerprinting, des WMI und SNMP, sowie des Footprinting individuell verifiziert.

Adriano Vasile, Teamleiter IT-Infrastruktur: „Versucht sich ein nicht-autorisiertes Gerät im Netzwerk anzumelden wird das Gerät sofort geblockt und somit der Zugriff auf das Netzwerk automatisch unterbunden. Soll der Zugriff eines neuen Gerätes erlaubt werden, können wir das direkt in der macmon-Konsole konfigurieren und mit einem Klick innerhalb von wenigen Sekunden am entfernten Switch-Port das richtige Netzwerk (VLAN) aktivieren und somit den Zugriff gewähren. Dieser Prozess ist sehr komfortabel und spart wichtige Zeit und Nerven bei der IT- Administration."

www.macmon.eu

macmon intelligent einfach

Effektives Privileged Access Management

DIE ANTWORT AUF CYBER-ANGRIFFE LAUTET PAM

Cyber Security ist ein Thema, das gerade wieder an Aktualität gewinnt. Vor Kurzem erst hat eine globale Welle von Cyberangriffen viele Unternehmen in Deutschland getroffen – laut dem Bundesamt für Sicherheit in der Informationstechnik (BSI) wurde auch mit Erpressungssoftware gearbeitet und das Ausmaß der Schäden ist noch nicht bekannt. Solche und andere Bedrohungen können Sicherheits- und Risikomanagementverantwortliche zwar nicht vorhersagen, aber sie können aus der Vergangenheit lernen und sich mit effektiver Software schützen.

DIE 360° PRIVILEGE PLATFORM UMFASST AUSSERDEM ENDPOINT PEDM, DSM FÜR DEVOPS & SECRETS MANAGEMENT, EIN KOMPLETTES ZERTIFIKATS-LEBENSZYKLUSMANAGEMENT, CLOUD IAM UND MULTI-CLOUD-LÖSUNGEN.

Marcus Scharra,
Mitbegründer und CEO, senhasegura,
www.senhasegura.com

In einem Gartner Bericht aus dem Jahr 2022 „Prepare for New and Unpredictable Cyberthreats" heißt es: „Bis 2026 werden Unternehmen, die mindestens 20 Prozent ihrer Sicherheitsmittel in Resilienz- und flexible Designprogramme investieren, die Gesamtwiederherstellungszeit bei einem großen Angriff halbieren." Das Thema wird also sogar noch wichtiger. Unternehmen sollten sich darauf konzentrieren, Sicherheitsprogramme zu entwickeln, die auf gemeinsamer Risikoverantwortung, Widerstandsfähigkeit und flexibleren Reaktionsmöglichkeiten gegenüber neuen, unvorhersehbaren Bedrohungen der Cybersicherheit beruhen.

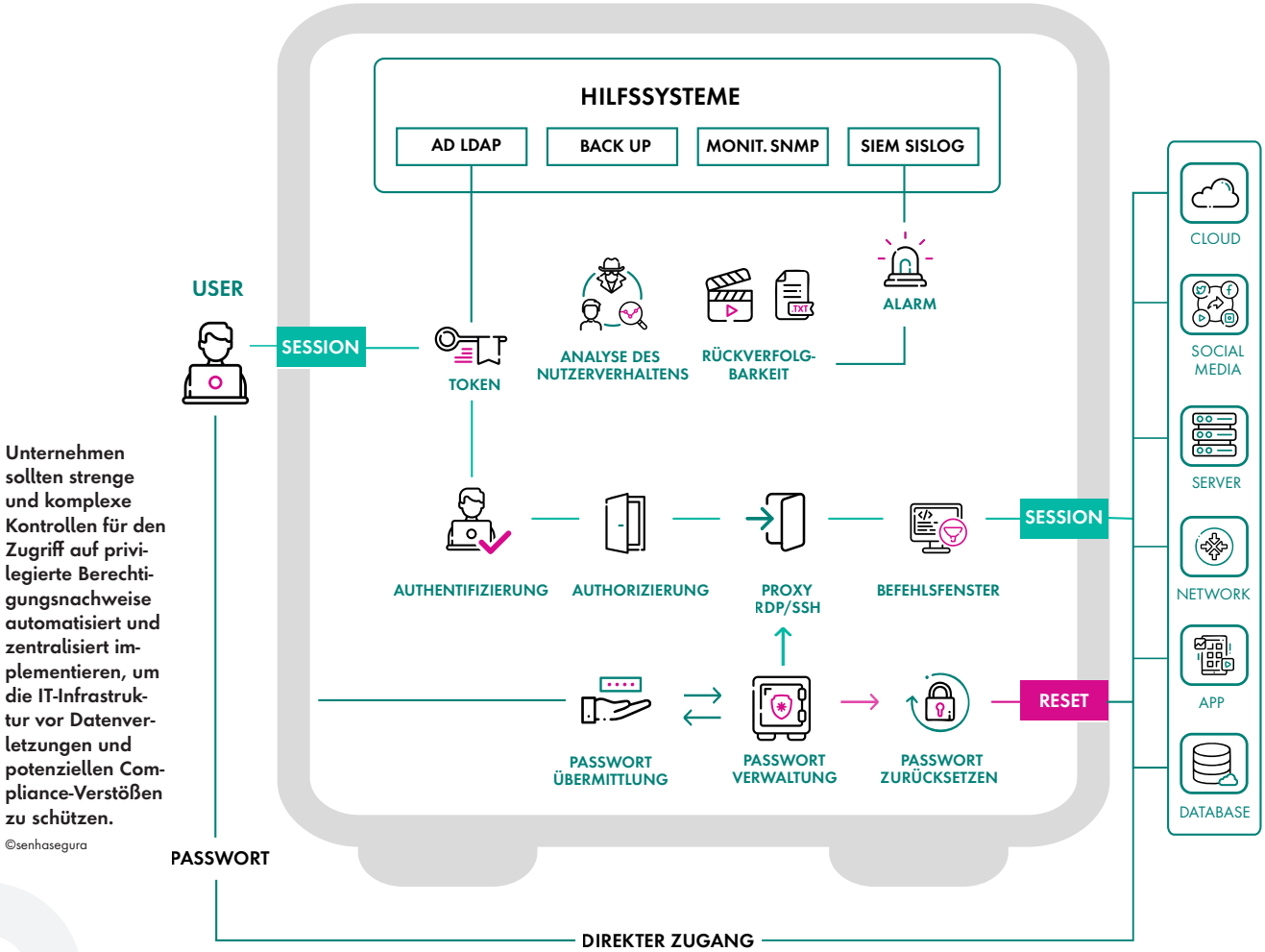
Aus der Vergangenheit lernen

Leider gibt es genügend negative Beispiele: Die Bedrohungslandschaft wird nachweislich immer gefährlicher. Zwischen 2019 und 2020 gab es einen Anstieg der Ransomware-Angriffe um 800 Prozent, wie 2021 der Sicherheitsreport von Deep Instinct herausfand, und für das Folgejahr nochmals einen Anstieg von 125 Prozent. Dabei ist der finanzielle Schaden durch Erpressung genauso schlimm wie der Imageschaden. Aber es gibt Lösungen, um Schwachstellen in IT-Landschaften zu beheben – und damit sind nicht nur Patches, Updates und die Sicherstellung der richtigen Konfigurationseinstellungen gemeint.

Die Zugriffsrechteverwaltung stellt eine wichtige Schwachstelle dar, insbesondere wenn es um privilegierte Benutzerkonten geht. An diesem Punkt setzt die effektive und automatisierte Privileged Access Management Lösung von senhasegura an. Die Software basiert auf der Strategie der Zugriffskontrolle und der Vergabe von privilegierten Berechtigungen an Benutzer, Systeme und Maschinen innerhalb einer kritischen Umgebung oder eines Unternehmensnetzwerks. Privilegierte Benutzerkonten haben Zugriff auf alle Systeme, Anwendungen und Daten und sorgen dafür, dass diese ordnungsgemäß funktionieren.

Zu dieser Nutzergruppe gehören allgemeine IT-Administratoren, Systemmitarbeiter, Netzwerkspezialisten, DevOps-Spezialisten sowie die Geschäftsleitung. Heutzutage werden aber auch oft Automatisierungssysteme, APIs und andere Softwarelösungen dazu gezählt.

Der Ansatz des brasilianischen Unternehmens senhasegura ist eine Full Stack-Lösung mit besonders einfacher und benutzerfreundlicher Handhabung, wofür sie bereits mehrfach ausgezeichnet wurden, zum Beispiel beim jüngsten PAM Leadership Compass von KuppingerCole. Dort sagten die Kunden, sie „bieten die beste Benutzerfreundlichkeit, eine leistungsstärkere PAM-Erfahrung und denken vorausschauend über die Bedürfnisse von Entwicklern und darüber, wie PAM in Infra-



Unternehmen sollten strenge und komplexe Kontrollen für den Zugriff auf privilegierte Berechtigungsnachweise automatisiert und zentralisiert implementieren, um die IT-Infrastruktur vor Datenverletzungen und potenziellen Compliance-Verstößen zu schützen.

©senhasegura

strukturumgebungen passt". Auch die Berater von Frost & Sullivan haben senhasegura 2022 den Frost & Sullivan's Customer Value Leadership Award verliehen.

Mangelndes Zugriffsmanagement als reale Bedrohung

Die PAM-Lösung adressiert den gesamten Lebenszyklus des Privileged Access Managements, und favorisiert eine Zero-Trust-Architektur. Die Full Stack-Lösung setzt auf einfache Handhabung und Zugangskontrolle zu allen Systemen und Programmen, im Gegensatz zu komplexen Lösungen, die oftmals zu einer falschen Wahrnehmung von Sicherheit und Risikominimierung führen – was man bei leider oft erfolgreichen Ransomware-Angriffen sehen kann. Mangelndes Zugriffsmanagement stellt deshalb eine größere Bedrohung für die Datensouveränität eines Unternehmens dar.

Was senhaseguras Ansatz ausmacht, neben der branchenweit niedrigsten TCO, die kürzeste Time to Value und dem höchsten ROI, ist eine 100-prozentige Cyber-Security-Ausrichtung mit PAM. Die 360° Privilege Platform umfasst außerdem Endpoint PEDM (Privileged Elevation and Delegation Management), DSM für DevOps & Secrets Management, ein komplettes Zertifikats-Lebenszyklusmanagement, Cloud IAM und Multi-Cloud-Lösungen. PAM hat sich zu einer umfassenden Risikomanagement-Disziplin entwickelt, da die Digitalisierung die Angriffsfläche vergrößert hat, indem sie die Cloud, mehrere Endpunkte, Heimarbeit und keine sicheren Perimeter umfasst. Deshalb werden vermehrt Funktionen Cloud-basierter Ressourcen und kritische Cloud-basierte Workflows wie DevOps- und CI/CD-Projekte integriert. Denn ohne Beachtung der Cloud kann man heutzutage keine vollständige Sicherheit mehr denken. Viele Produkte und Apps basieren auf riesigen Datenmengen – KI zum Beispiel ist ohne Multicloud-Lösungen nicht umsetzbar. Und diese Daten gilt es zu schützen.

Dennoch bleibt die Nachfrage nach traditionellen PAM-Funktionen (Vaulting, Credential Management, Analysen, Admin-Zugang, Endpoint Privilege Management) robust und der Markt wächst insgesamt.

Markus Scharra

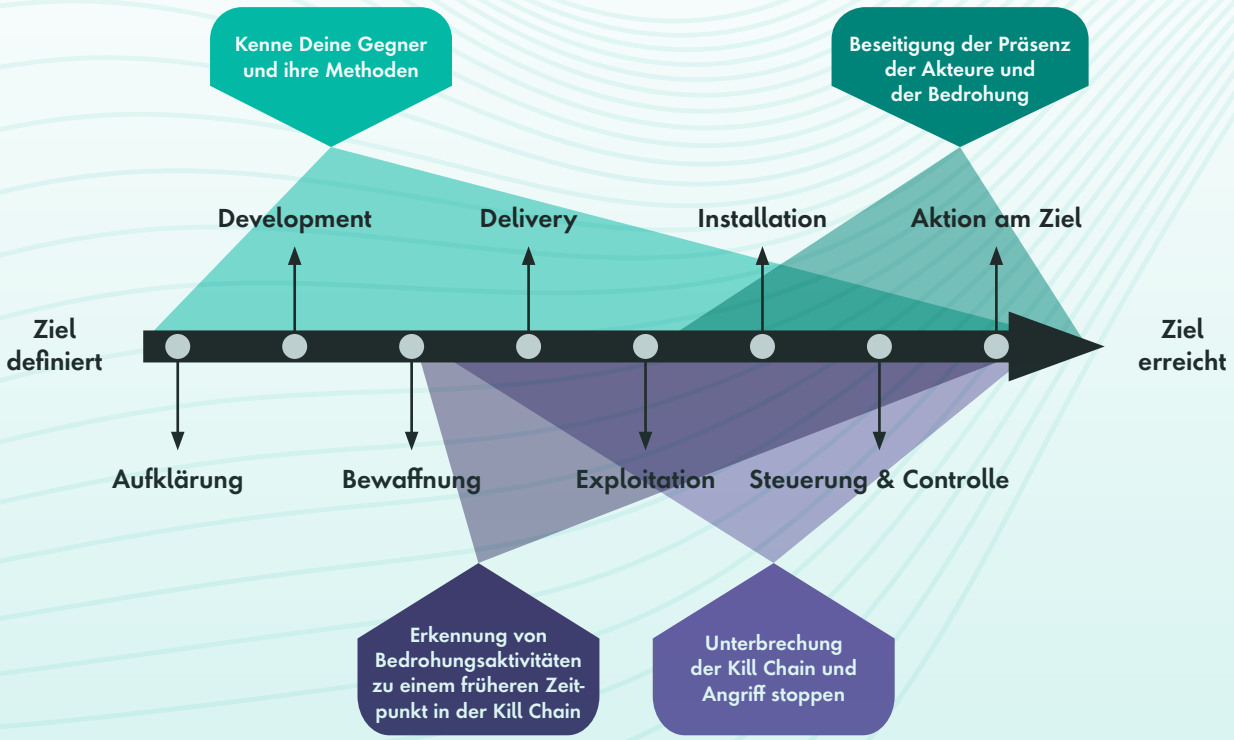
Cybersecurity-Schutz

SCHNELLE ERKENNUNG NEUER GEFAHREN

Wer wünscht sich nicht einen umfassenden IT-Sicherheitsschutz. Hilfe versprechen hier einige neue Plattformen. Eine dieser Plattformen der neuen Generation heißt Anomali. Dabei ersetzt die Lösung keine Technologien, sondern führt mehrere oder im besten Fall alle Sicherheitskontrollen zusammen, um eine horizontale Sicherheit mit XDR zu realisieren.

Es geht also nicht nur um die Erkennung von Anomalien, wie der Name des Unternehmens vermuten lässt. Die Lösung will bisherige Silolösungen in der IT-Security Landschaft zusammenführen und Systeme wie SIEM (Security Information and Event Management), SOAR (Security Orchestration Automation and Responses), und EDR (Endpoint Detection and Response) integrieren. Ziel der Plattform ist es, Exploits und Ransomware zu erkennen und darauf zu reagieren und das quasi in Echtzeit sowie retrospektiv auch bis fünf Jahre rückwirkend. Angriffsflächen und digitale Risiken werden verwaltet - und das alles auf der Grundlage vorher getroffener aussagekräftiger Sicherheitsanalysen.

ZEITSTRAHL & STATUS DER BEDROHUNG



Zu wissen, dass eine neue Bedrohung beobachtet wurde, ist gut. Zu wissen, wo sich eine Bedrohung in der Kill Chain befindet, ist viel nützlicher. Wenn ich weiß, wo sich die Bedrohung im Prozess der Erreichung ihres Ziels befindet, kann ich mich nicht nur dagegen verteidigen, sondern auch die Aktivitäten der Bedrohung verstehen, bevor sie bekannt wird.

Der Plattformgedanke
Die Plattform besteht aus den drei Komponenten ThreatStream, Match und Lens.

- ThreatStream dient der proaktiven Abwehr durch die Operationalisierung der Threat Intelligence auf einer Plattform.
- Match sorgt für die systematische, kontinuierliche Korrelierung aller Threat Intelligence-Informationen mit den Logdaten für die automatische Threat-Erkennung im Netzwerk.
- Drittes Modul im Bunde ist Lens, das dank eines direkten Zugriffs auf Threat Intelligence-Informationen neue und bekannte Bedrohungen sofort identifiziert und sofern es ihr Unternehmen betrifft, Maßnahmen ergreift.

Cyber-Resilienz umsetzen
Unternehmen erwarten von ihren CIOs und CISOs, dass sie für Cyber-Resilienz sorgen. Das bedeutet, sie müssen ihren Ansatz zur Cyber-Resilienz überdenken und zusätzlich von der Verteidigung zur Offensive übergehen.

Die Analyse beginnt damit, ob alle erforderlichen Sicherheitskontrollen (Firewall, SIEM, EDR, usw) vorhanden sind. Als Nächstes kommt die größte und teuerste Security-Herausforderung – die Silos sprechen nicht miteinander und erfordern daher eine komplizierte Orchestrierung. Um eine Cyber-Resilienz zu erreichen, müssen Sie eine „aktion sorientierte Sichtbarkeit" über alle Protokolle und für umfangreiche forensische Rückblicke orchestrieren.

MEHR WERT
Die Anomali Cyber Watch
https://bit.ly/416tKib

GRÖSSTE BEDROHUNGEN FÜR UNTERNEHMEN

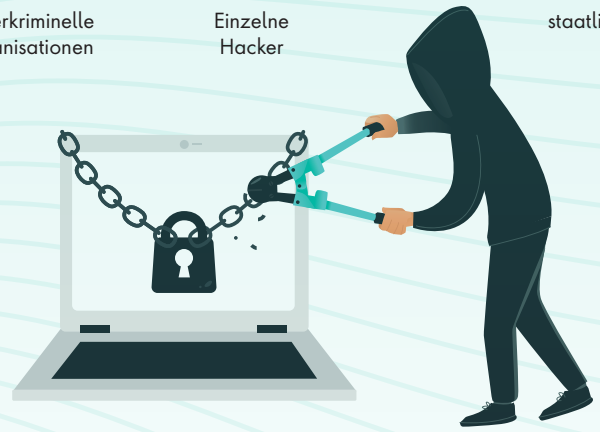
(Quelle: Anomali)

44 % Cyberkriminelle Organisationen

21 % Einzelne Hacker

18 % APTs

15 % staatlich unterstützte Akteure



CYBER-RESILIENZ DES UNTERNEHMENS

(stimme voll und ganz zu)

58 % Mein Unternehmen verfügt über Cyber-Resilienz

53 % Wenn mein Unternehmen Projekte zur digitalen Transformation ausweitet, wird unsere Anfälligkeit für Cyberangriffe und Sicherheitsverstöße zunehmen

50 % Da es in meinem Unternehmen immer häufiger zur Arbeit von zu Hause aus kommt, wird sich unsere Anfälligkeit für Cyberangriffe und Sicherheitsverstöße erhöhen

Der Footprint
Anders ausgedrückt: CIOs und CISOs müssen die „Sichtbarkeit" über alle Sicherheitskontrollen hinweg ausbauen und diesen Big Data Footprint auf das, was „gehandelt" wird, um Angreifer zu stoppen, ausweiten. Gleichzeitig sollte diese massive Orchestrierung mit so viel Automatisierung wie möglich erreicht werden.

In einem weiteren Schritt wird die erreichte Sichtbarkeit verfeinert. Der Ansatz war bisher „irgendeine" Form von Intelligenz zu erreichen, neu ist globale Intelligenz mit Verhaltensanalytik. Dabei hilft ein umfassendes Toolset.

Zusammenfassend lässt sich sagen, dass CIOs und CISOs eine umfassende und erweiterte Sichtbarkeit und nicht nur eine „gewisse" Sichtbarkeit über alle Sicherheits- und Cloud-Protokolle hinweg orchestrieren müssen und das mit der Möglichkeit forensisch bis zu sieben Jahre zurückzugehen. Ein wichtiger Teil der Sichtbarkeit ist ihre Verfeinerung.

Lösungsumsetzung
Wie können Unternehmen nun diese langwierige und kostspielige Herausforderung der orchestrierten Transparenz lösen, um Analysen zu liefern?

Die Big-Data-Analyseplattform von Anomali kann das Problem an einer Stelle lösen und erhebliche Zeit und Kosten einsparen, in dem sie große und gleichzeitig wichtige Arbeitsabläufe automatisiert. Verankert durch eine proprietäre große Datenkompression und einem leistungsfähigen Repository für Actionable Intelligence liefert Anomali differenzierte Business Use Cases, die die oben beschriebene große Herausforderung lösen.

Die Analytik imitiert menschliche kognitive Funktionen wie Lernen und Problemlösung in dieser Sicherheitsautomatisierung. Es ist quasi ein Best-of-Breed aus jahrzehntelanger Sicherheitserfahrungen, aus maschinellem Lernen, Künstlicher Intelligenz und Cloud-Technologie.

Der Nutzen der Plattform
Was kann die Plattform? Es beginnt mit dem Schutz vor Attack Surface Management (ASM), zu deutsch Angriffsflächenmanagement. Darunter wird die kontinuierliche Erkennung, Analyse, Behebung und das Monitoring von Sicherheitslücken und potenziellen Angriffsvektoren verstanden, die die Angriffsfläche eines Unternehmens bilden.

Das und die Digital Risk Protection ermöglicht es Unternehmen, Betrug und Datenverluste zu erkennen und sich davor zu schützen. Basis ist die „Actionable Intelligence". Sie umfasst beides, sowohl als IoCs als auch als IoAs (neuer und differenzierten Ansatz zur Verhaltensanalyse). IoC steht für Indicator of Compromise und deutet auf eine bereits erfolgte Kompromittierung hin.

IoCs können aus dem Betriebssystem, dem Netzwerk, dem Speicher und weiteren Quellen gesammelt werden und haben unterschiedlichste Formen: Indikatoren können ein Dateiname, eine Protokolldatei, ein Registry-Schlüssel, eine IP-Adresse oder ein Hash sein.

IoA hingegen steht für Indicators of Attack und deutet auf einen bevorstehenden oder gerade beginnenden Angriffsversuch hin.

Von dort aus kann die Big Data-Engine alle Sicherheits- und Cloud-Protokolle

Q&A: WAS IST WAS?

EXPOSURE MANAGEMENT

Exposure Management ist eine modernere Art von isolierter Bewertungsmethodik: Die Daten der einzelnen Bewertungstools und -techniken können zusammengeführt und analysiert werden, um die Zusammenhänge zwischen den einzelnen Ergebnissen zu erkennen, sodass Unternehmen nachvollziehen können, wo sie einem Angriff ausgesetzt sein könnten. Da Angreifer häufig von einer Art von Schwachstelle zur nächsten übergehen, müssen Verteidiger in der Lage sein zu verstehen, wie sich alle ihre vorhandenen Daten zu Schwachstellen und Fehlkonfigurationen gegenseitig beeinflussen können. Bisher erfolgten aggregierte, auf wechselseitige Beziehungen ausgelegte Analysen dieser Art manuell in einem externen Datenspeicher. Sicherheitsteams mussten dabei eigene Risikozusammenhänge anlegen und auf ihr individuelles Verständnis der Infrastruktur zurückgreifen. Diese Vorgehensweise führt zu unvollständigen Ansichten der Umgebung – und zu einem sehr umständlichen, komplizierten Prozess, um das Problem in den Griff zu bekommen.

ERWEITERTE THREAT DETECTION & RESPONSE

Ziel ist ein schnellerer Weg zu XDR, um so einen umfassenden Einblick über den Angriffsbereich zu erhalten und die Zeit bis zur präzisen Erkennung (bei ~200 Billionen Bedrohungsereignissen pro Sekunde) durch alle Ihre Sicherheits- und Cloud-Protokolle mit Hilfe des umfangreichen Repositories globaler Actioned Intelligence-Informationen zu verkürzen. So können die Untersuchungen und Reaktionsprozesse schnell ermittelt und die nächsten Schritte des Angreifers antizipiert werden.

THREAT HUNTING

Unter Threat Hunting, Bedrohungssuche, versteht man das proaktive Aufspüren von Cyberbedrohungen, die unerkannt in einem Netzwerk lauern. Es wird auch Cyber Threat Hunting genannt und spürt tief verborgene Bedrohungsakteure in Ihrer Umgebung auf, denen es gelungen ist, die ersten Verteidigungslinien Ihrer Endgeräte-Sicherheitsmaßnahmen zu überwinden. Wichtig ist es, auch auf die Suche nach Angreifer-Fußabdrücken, den sogenannten Footprints, einschließlich retrospektiver Jagd, zu gehen

einlesen und die vorhandenen Daten mit dem weltweit größten Fundus vergleichen und interpretieren, um gegebenenfalls Angreifer zu stoppen. Die Plattform verfügt außerdem über die Möglichkeit eines Natural Language Processing (NLP) Scans, das den Analysten hilft, sich auf das Wesentliche zu konzentrieren, während viele manuelle Aufgaben wegfallen.

Automatisierung ist das Herzstück dieser Arbeit, die Anwender hilft, viele manuelle Arbeitsabläufe zu reduzieren. Die Plattform wird als native Cloud-Architektur, SaaS-Modell und auch als Multi-Cloud-, On-Premises- und Hybrid bereitgestellt.

Ulrich Parthier | www.it-daily.net

SCHUTZ VOR ZERO-DAY-BEDROHUNGEN

Mehr als 100 Millionen globale Sensoren verschaffen Anwendern einen Überblick über neu entdeckte Zero-Day-Bedrohungen. So sind sie gegen unbekannte Bedrohungen innerhalb von Sekunden nach ihrer Entdeckung geschützt.

MONITORING DER SICHERHEITSINVESTITIONEN

Unternehmen können Ihre Sicherheitslage bewerten, indem Sie das Verhalten von Angreifern und Ihre Sicherheitsinvestitionen mit dem MITRE Framework abbilden, um Lücken aufzudecken und Investitionen zu priorisieren.

ERWEITERBARE PLATTFORM

Die Anomali-Plattform integriert sich in den jeweiligen Sicherheits- und IT-Stack, um umfassende Transparenz zu bieten und eine orchestrierte Reaktion über alle Sicherheitsfunktionen hinweg zu bieten.

>> ZUSAMMENFASSUNG

Anomali ist eine Plattform zur Bedrohungsinformation, die Unternehmen dabei unterstützt, sich gegen Cyberangriffe zu schützen.

Jeder spricht von Threat Detection und davon Angriffe zu stoppen, wenige sehen aber das gesamte Bild. Zu einem ist es extrem wichtig zu wissen, wie heutige Threat Actors agieren, welche Kampagne sie planen und Angriffsmethode aktuell anwenden. Nur wenn man seinen Gegner kennt, kann man sich entsprechend verteidigen und die richtigen Maßnahmen einsetzen. Die Threat Intelligence liefert genau diese Informationen.

Parallel dazu ist es ebenso wichtig, die gesamte Cybersicherheit zu betrachten, weg von den Technologie-Silos hin zu einem horizontalen Sicherheitskonzept. Dieser holistische Ansatz erlaubt alle Sicherheitssysteme als eine einzelne Einheit zu sehen, die die Sicherheits-Events im gesamten Kontext betrachtet und deutlich besser identifiziert.
Die ideale Lösung sollte die zwei oben genannten Ansätze zusammenführen, sprich die gesamte relevante Threat Intelligence analysieren, deduplizieren und aufbereiten und diese mit der Sicherheits-Telemetrie der gesamten Infrastruktur korrelieren. Eine Plattform, die einfach zu integrieren ist, die keinen Regelaufbau fordert und vor allem nur die wichtigen Alarmierungen zeigt ohne Informationsüberflutung.

Die retrospektive Analyse von Telemetriedaten bis zu fünf Jahren zurück, erlaubt unter anderem auch die Auswirkung von neuen Schwachstellen innerhalb Sekunden zu analysieren und den „Patient Zero" zu identifizieren.

Schluss mit toten Winkeln

XDR SCHAFFT GANZHEITLICHE SICHT AUF GEFAHRENLAGE

Jüngst hat WatchGuard Technologies seine „Unified Security Platform" um eine XDR-Lösung (eXtended Detection and Response) ergänzt. Zu den Hintergründen und damit einhergehenden Potenzialen bei der Gefahrenabwehr hat Ulrich Parthier, Herausgeber it security, bei Michael Haas, Vice President Central Europe bei WatchGuard Technologies, nachgefragt.

Ulrich Parthier: *Herr Haas, warum verankern Sie XDR im Portfolio?*

Michael Haas: XDR verfolgt das Ziel, mehr und umfassendere Kontrolle gegenüber vielfältig daherkommenden Gefahren zu gewinnen. Dabei wird über ein zentrales Werkzeug die Brücke zwischen unterschiedlichsten IT-Security-Themenbereichen geschlagen – im Fall von WatchGuard zwischen Netzwerksicherheit und Endpoint Protection. Die XDR-Idee ist keinesfalls neu, es zählt in dem Zusammenhang jedoch die Qualität, Breite und Tiefe der Ausprägung. So umfasste das WatchGuard-Angebot beispielsweise schon vorher eine cloudbasierte Korrelations-Engine. Damit ließen sich die per Host Sensor am Endgerät gesammelten Ereignisdaten mit den Informationen der Netzwerk-Appliances abgleichen, um bösartiges Verhalten zu identifizieren. Je nach Schweregrad der Bedrohung konnten so bereits in der Vergangenheit auf Basis des lösungsübergreifenden Informationsaustausches Gegenmaßnahmen eingeleitet werden. Unsere bisherige Lösung nutzte jedoch nur die Endpunkt-Telemetrie aus der Cloud, um schädliche Dateien zu erkennen; Netzwerkereignisse wurden mit einzelnen Dateien und Prozessen am Endpunkt korreliert. Was fehlte, war die Möglichkeit, Bedrohungen im Rahmen eines Vorfalls zusammenhängend und komplett cloudnative zu klassifizieren und den Sicherheitsadministratoren noch umfassendere Reaktionsmaßnahmen anzubieten. Doch genau darauf kommt es angesichts der Komplexität von Angriffsszenarios mehr denn je an. Nachdem wir die verschiedenen IT-Security-Bausteine unseres Portfolios – von Netzwerksicherheit über Endpoint Security, WLAN und Multifaktor-Authentifizierung – inzwischen auf nur einer einzigen Cloud-Plattform zusammengeführt haben, profitieren wir von einem ganz neuen Fundament für unsere XDR-Initiative.

Ulrich Parthier: *Die „Security-Plattformisierung" befeuert also XDR?*

Michael Haas: Absolut. Aus unserer Sicht eröffnet sich so der zielführendste Weg, mit aktuellen Rahmenbedingungen des Marktes – Stichwort Fachkräftemangel – und neuen Bedrohungen überhaupt Schritt halten zu können. Grundsätzlich ist es wichtig, sicherheitsrelevante Ereignisse über alle potenziellen Angriffsflächen hinweg im Blick zu behalten und tote Winkel sukzessive auszumerzen. Und wenn dies alles aus einem Guss erfolgt, zahlt das natürlich maximal auf das Konto der Effizienz ein. Egal ob der Hinweis zu einer Auffälligkeit aus dem Netzwerk oder vom Endpunkt kommt: Die einzelnen Puzzleteile ergeben sofort ein aussagekräftiges Bild. Abwehrmaßnahmen können ebenso unmittelbar, automatisiert und vor allem flächendeckend über alle Schutzschichten Wirkung entfalten. Die „Mean Time to Detect" (MTTD) und die „Mean Time to React" (MTTR) werden auf diese Weise deutlich reduziert, Schaden lässt sich schneller und effektiver abwenden. Insofern adressieren wir mit unserer neuen „ThreatSync"-XDR-Lösung nicht zuletzt eine ganz neue Zielgruppe: die des Incident Responders beziehungsweise SOC-Analysten, dessen Hauptaufgabe genau darin besteht, vielschichtige Angriffe zu identifizieren und zügig passende Gegenmaßnahmen zu ergreifen. Hier geben wir Unternehmen nun ein wirksames Instrument in die Hände, das nicht mal mit zusätzlichen Kosten zu Buche schlägt.

Ulrich Parthier: *Bitte präzisieren Sie dies für uns.*

Michael Haas: XDR via ThreatSync ist sozusagen ein besonderes Goodie im Rahmen unserer „Unified Security Platform"-Architektur und standardmäßig in jeder Firebox Total Security Suite (TSS)-Lizenz sowie den WatchGuard EDR- und EPDR-Produkten enthalten. Je mehr WatchGuard-Produkte ein Unternehmen einsetzt, desto umfangreicher fallen die Möglichkeiten und via ThreatSync erzielbaren Einblicke aus. Dieser umfassende Ansatz wird mit der Integration weiterer Security-Ebenen – also MFA oder den Komponenten zum WLAN-Schutz – künftig noch mehr Schlagkraft erhalten.

? **Ulrich Parthier:** *Dies erhöht aber auch die Anbieterabhängigkeit. Wie reagieren Kunden und Partner darauf?*

Michael Haas: Bei unseren Partnern ist dieser Schritt äußerst gut angekommen, da ihnen ThreatSync natürlich auch gerade im Zuge von Managed-Security-Services-Angeboten voll in die Karten spielt. Und Kunden profitieren gleichermaßen – egal, ob die WatchGuard-Lösungen inhouse oder auf Seiten eines Dienstleisters zum Einsatz kommen. Im Hinblick auf den Aspekt der Anbieterabhängigkeit stellt sich einfach nur die Gretchenfrage: Will ich das oder will ich das nicht? Die Vorteile liegen klar auf der Hand und werden auch im Markt immer stärker wahrgenommen: mehr Entlastung, Produktivität, Kontrolle und Schutz. Und da dieses Konzept nachweislich funktioniert, warum nicht einfach davon profitieren? Moderne, verlässliche IT-Security im Allgemeinen und XDR im Speziellen basieren auf Integration und Zusammenspiel – und am besten und reibungslosesten lässt sich dies auf Basis einer umfassenden cloudbasierten Plattform gewährleisten. Praktikabilität ist entscheidend. Und hier bietet ThreatSync gegenüber anderen XDR-Lösungen wichtige Vorzüge: Die verschiedenen Sicherheitsebenen müssen nicht erst noch sinnvoll miteinander verbunden werden. Zudem sind keine zusätzlichen Lizenzen erforderlich.

? **Ulrich Parthier:** *Aber klassische SIEM- oder SOAR-Modelle kann XDR nicht ersetzen ....*

Michael Haas: Nein, aber das ist auch gar nicht der Anspruch. Es geht vor allem darum, insbesondere kleinen und mittelständischen Unternehmen, die in der Regel über keinerlei Kapazitäten oder separates Budget zur Umsetzung von SIEM oder SOAR verfügen, eine wirkungsvolle Alternative zu bieten. XDR ist in unseren Augen das perfekte Add-on für Managed Service Provider, die genau diesen Kundenkreis bedienen. Das Ziel ist klar formuliert: Angreifern keine Chance geben und Unternehmen ein reibungsloses Arbeiten ermöglichen. Ein bisschen sicher gibt es genauso wenig wie ein bisschen schwanger. Maßgeblich ist der Mitteleinsatz, um diesen Zielzustand zu erreichen. Dafür ist XDR ein nicht zu unterschätzender Weichensteller und nicht zuletzt wichtiger Eckpfeiler für die Umsetzung von Zero-Trust-Strategien. Am Ende zählt im Wettbewerb allein der Aufwand, der aufgebracht werden muss, die nötige Kontrolle und Resilienz zu gewährleisten. Plattformkonzepte sind in dem Zusammenhang kaum zu schlagen.

! **Ulrich Parthier:** *Herr Haas, danke für das Gespräch!*

So funktionieren Pentests

SICHERHEITSLÜCKEN IN IT-SYSTEMEN ERKENNEN

2022 waren 72 Prozent der DACH-Unternehmen von Ransomware-Angriffen betroffen – das zeigt die aktuelle IDC-Studie „Cybersecurity in DACH 2022" im Auftrag von secunet. Ob Phishing-Mail, Malware oder Verschlüsselungen: Die Methoden der Angreifer sind vielfältig. Dabei steigt nicht nur die Anzahl, sondern auch die Raffinesse von Cyberattacken. Immer komplexer werdende IT-Landschaften stellen Unternehmen und ihre entsprechenden Fachabteilungen vor zahlreiche Herausforderungen.

Der Blick in die Praxis zeigt: Administratoren fehlen oftmals Zeit und Geld, um das Kernproblem der IT-Sicherheit zu lösen: Die Verteidiger müssen alle Sicherheitslücken schließen. Einem Angreifer reicht häufig eine einzelne nicht behobene Lücke. Und die kann dann weitreichende Auswirkungen haben. Eine Möglichkeit, Sicherheitslücken aufzudecken, sind Penetrationstests (Pentests).

Gefühlte versus tatsächliche Sicherheit

Im Rahmen eines Pentests werden verwundbare Stellen im Netzwerk bewusst gesucht. Auf diese Weise kann zuverlässig festgestellt werden, wie viele Schwachstellen tatsächlich vorliegen – und wie schnell auf eventuelle Sicherheitslücken reagiert werden sollte. Das Bewusstsein um den Wert eines solchen Tests unterscheidet sich je nach Unternehmen. In vielen Fällen deckt sich die gefühlte Sicherheitslage nicht mit der tatsächlichen Sicherheitslage. Pentester sind Experten darin, genau hinzusehen und Schwachstellen zu finden, die auf den ersten Blick verborgen bleiben. Oft sind es genau die Dinge, die die Auftraggeber vorher selbstbewusst als unproblematisch bezeichnet haben, die einer kritischen Prüfung nicht standhalten. Ein ausgiebiger Pentest kann zudem dazu dienen, im Management Aufmerksamkeit für das Thema IT-Sicherheit zu schaffen und den Status quo zuverlässig darzustellen. Dies ist der notwendige erste Schritt, um Risiken zu reduzieren.

Der Faktor Mensch

Das Internet bleibt einer der größten Risikofaktoren für IT-Systeme. Malware und andere Schadprogramme konnten bereits aufgrund unzureichend sicherer Firewalls ihren Weg in die Systeme finden. Mit zunehmendem Verständnis dieser Bedrohung mussten Angreifer jedoch umdenken und sich neue Ideen einfallen lassen. So sind heutzutage Phishing-Mails, die den Benutzer dazu bringen, Fehler zu machen, ein deutlich attraktiverer Angriffsweg. Ebenso wie der Einsatz von Hardware, beispielsweise bewusst platzierte USB-Sticks, die Viren direkt ins System übertragen.

MEHR WERT

Studie: Angriffserkennung in Unternehmen kritischer Infrastrukturen
https://bit.ly/3AdQpwW

Diese Angriffsmethoden nutzen die Schwachstelle Mensch aus – ein großer Unsicherheitsfaktor, denn dieser verfügt in den meisten Fällen über weitreichende Berechtigungen, die die meisten internen Dokumente und Ressourcen zugänglich machen. Oftmals fehlt auch das Wissen um gängige Sicherheitspraktiken. So kann es vorkommen, dass ein herumliegender USB-Stick benutzt oder Laptops unversperrt offengelassen werden. Auf diese Weise werden verwundbare Stellen im System zugänglich – darunter

auch fehlende Patches, schwache Passwörter, (nachträglich) vernetzte, weniger gehärtete Maschinen oder Sicherheitslücken in der IT und der OT Supply-Chain.

Worauf es beim Pentest ankommt

Bei secunet geht jedem Pentest das sogenannte Scoping voraus, bei dem eine Absprache darüber getroffen wird, welche Systeme untersucht werden sollen. Dabei wird ein offenes Gespräch mit den Unternehmensverantwortlichen geführt, bei dem potenzielle Problemstellen erfragt und so oftmals bereits existente Probleme klar werden. Prüfen können die Pentester dabei im weitesten Sinne alles, was Strom braucht, um zu funktionieren. Dabei spielt es keine Rolle, ob es die IT oder die OT betrifft: Von der klassischen Büro-IT über Webadressen und mobile Apps bis hin zum Social Engineering, bei dem auch die Rolle des Menschen untersucht wird. Auch Zusatzfunktionen von Programmen oder Websites, die den Arbeitsalltag erleichtern sollen, können leicht zu einem Sicherheitsrisiko werden. Gerade bei der zunehmenden Vernetzung zwischen IT- und OT-Systemen spielen Analysen in der Operational IT eine immer wichtigere Rolle. OT-Systeme sind häufig nicht oder nur in sehr aufwändigen Prozessen patchbar, was diese Geräte besonders anfällig gegenüber Angreifern macht.

PENTESTER SIND EXPERTEN DARIN, GENAU HINZUSEHEN UND SCHWACHSTELLEN ZU FINDEN, DIE AUF DEN ERSTEN BLICK VERBORGEN BLEIBEN.

Dirk Reimers,
Bereichsleiter Pentest & Forensik,
secunet Security Networks AG,
www.secunet.com

ADMINISTRATOREN FEHLEN OFTMALS ZEIT UND GELD, UM DAS KERNPROBLEM DER IT-SICHERHEIT ZU LÖSEN: DIE VERTEIDIGER MÜSSEN ALLE SICHERHEITSLÜCKEN SCHLIESSEN, DENN EINEM ANGREIFER REICHT OFT EINE EINZIGE LÜCKE..

Jannik Pewny, Teamleiter
Incident Response & Forensik,
secunet Security Networks AG,
www.secunet.com

Von der Momentaufnahme zur Lösung

Im Zweifelsfall gilt in der IT-Sicherheit das Motto: „Was muss, das darf – was nicht muss, das darf auch nicht." Denn ein Pentest ist immer nur eine Momentaufnahme. Die Systemadministratoren sollten deshalb in die Schwachstellenanalyse einbezogen werden. Auch bei knappem Budget lassen sich so offene Sicherheitslücken und Risiken klar aufzeigen. Doch eine Diagnose ist noch keine Lösung: Systeme bedürfen regelmäßiger Wartung und Schwachstellen sollten gewissenhaft und nachhaltig beseitigt werden. Pentests legen den Grundstein für eine zuverlässige IT-Sicherheit.

Jannik Pewny, Dirk Reimers

Risikominimierung

SAP-TRANSPORTE EFFIZIENT KONTROLLIEREN

In jeder SAP-Umgebung sind Transporte ein wesentlicher Bestandteil, um Änderungen von einem System in ein anderes zu übertragen, neue Funktionen zu implementieren, Updates anzuwenden und Anwendungen von Drittanbietern zu installieren. So elementar diese Auslieferungen sind, bieten sie ungeprüft jedoch Einfallstore für die Einspielung risikobehafteter Objekte. Über SAP-Standards stößt der Versuch, mögliche Bedrohungen zu erkennen, schnell an Grenzen, doch gibt es Möglichkeiten, diese bereits während des Erstellens bzw. Einspielens aufzuspüren und nicht erst im Nachhinein.

Ganze Produkte, Patches, Coding, Datenbank-Inhalte, Rollen, Berechtigungsobjekte: Ein SAP-Transport ist vereinfacht gesagt ein Container zum Austausch zwischen Systemen von eigentlich allem, was man innerhalb eines SAP-Systems findet. Im Normalfall wird der Transport auf einem Entwicklungssystem erstellt, dort freigegeben und exportiert, das heißt, entsprechende Dateien werden im Transportverzeichnis angelegt. Anschließend wird er in die Importqueue zum Beispiel eines Produktivsystems eingehängt und ist bereit zum Import. Sicherheitstechnisch entscheidend ist dabei, dass das Abschließen eines Imports alles Enthaltene, ob Coding oder Datenbankinhalte, automatisch aktiviert – und folglich auch eine möglicherweise enthaltene Sicherheitslücke. Daher müssen zu diesem Zeitpunkt alle Inhalte überprüft und alle Bedrohungen detektiert worden sein.

Die Herausforderungen

Entwickler benötigen weitgehende Berechtigungen, um beispielsweise etwas zu debuggen, Transporte zu befüllen, teilweise auch anzulegen, gegebenenfalls freizugeben, auf jeden Fall Coding zu verändern. Damit einher geht ein hohes Risikopotenzial der Manipulation, sei es per verstecktem SAP_all, Hidden-OK-Codes im Transaktionsaufruf oder modifizierte RFC-Pings. Denn für Kundige gibt es zahlreiche Möglichkeiten, Transporte vom Entwicklungssystem in weitere Systeme zu übertragen. Ein Entwicklungssystem priorisiert im Security Scope kaum und es wird wenig auf Audits oder Auditlogs geachtet. Zudem ist ABAP-Coding üblicherweise eher unübersichtlich mit Reports, die 10.000 Zeilen und mehr beinhalten sowie Funktionsgruppen aus Hunderten Bausteinen.

Eine manuelle Inhaltsprüfung aller auf Schwachstellen ist angesichts der schieren Datenmenge also keine realistische Option.

Wo unterstützt der SAP-Standard?

Zur Risikominimierung bei SAP-Transporten stellt sich damit grundsätzlich die Frage: Was kann der SAP-Standard leisten? In der Entwicklung ist auf jeden Fall das ABAP Test Cockpit (ATC) aktiv einzusetzen und Coding schon bei der Erstellung, aber zumindest im Transportprozess automatisiert zu überprüfen. Allerdings ist ein Problem des ABAP Test Cockpits, dass es nicht sehr tief in die Securityfälle geht, das Code Scanning daher nicht vollständig ist und viele Lücken übrig lässt. So ist es zusätzlich empfehlenswert, ein ChaRM einzurichten, ein Change and Request Management, das hilft, die Transparenz und Prozesskonformität zu erhöhen.

Schließlich kann man, noch vor einem Import, auf den nachfolgenden Systemen wie QS- oder Produktionssystemen die STMS_TCRI pflegen. Hier lässt sich eine Liste sicherheitskritischer Objekte hinterlegen, deren Import automatisch blockiert wird. Das Problem ist, wer erhöhte Berechtigungs-Zugriffsmöglichkeiten hat, könnte diese umgehen und sogar dafür sorgen, dass es nicht einmal auffällt. Hier ist die Tiefe der Scans im Standard schlicht nicht ausreichend.

Erweiterung durch toolgestützte Transportkontrolle und Code Scan

Um aber einen umfassenden Schutzschild zu gewährleisten, sollte man den SAP-Standard gezielt erweitern und ausweiten. Die Kombination mit Lösungen wie von Pathlock macht es effektiv fast unmöglich, alle Sicherheitsschritte zu umgehen. Dies beginnt im Entwicklungssystem durch eine Code-Scanning-Erweiterung des ATC mit über 80 Testfällen. Der ATC erlaubt es auch, einen Scan bereits vor der Freigabe zu machen, wodurch es möglich ist, diese Erweiterung in einem Transport-Scanning automatisch und einfach mit den Standard-Funktionalitäten einzubinden, aber damit eine tiefe Kontrolle auf Security-Schwachstellen zu haben.

Der nächste Schritt ist eine Export-Kontrolle. Mit dieser Möglichkeit wird grundsätzlich jeder Export überwacht, die Objekte innerhalb eines Transports werden auf Kritikalität überprüft und gegebenenfalls wird der gesamte Transport blockiert. Es folgt eine Protokollierung des Security Events, damit das Ganze nachverfolgt werden kann. Äquivalent dazu gibt es die Möglichkeit, jeden Import zu überwachen. Für diese beiden Methoden existieren auch Trusted-Optionen, weil es bei Bedarf möglich sein muss, auch Kritisches wie ein selbstausführendes Programm einzubringen. Als Letztes folgt, zu jeder beliebigen Zeit Ad-hoc-Scans zu machen, um zu prüfen bzw. retrospektiv zu sehen, ob ein Inhalt kritisch ist.

Die Vorteile einer toolgestützten Lösung

SAP-Standardfunktionalitäten für Transportanalysen stoßen schnell an ihre Grenzen. Durch eine Toolerweiterung wird der Aufwand reduziert und Transportkontrollen lassen sich zudem noch automatisieren. Die Integration erfolgt in die von SAP bereitgestellten Standardmechanismen, ohne bereits etablierte Mechanismen zu revidieren.

MEHR WERT

SAP-Transportkontrolle inkl. Live-Hacking-Demonstration:
https://bit.ly/40gGwcG

Erweiterungen wie von Pathlock gehen aber bei den Kontrollanalysen einen entscheidenden Schritt weiter und ermöglichen, dass auf kritische Inhalte geprüft wird, noch bevor sie zur Einspielung in die SAP-Systeme freigegeben werden, und das in Echtzeit bereits während der Implementierung.

Durch die automatische Sperrung fehlerhafter Transporte können Entwicklungsteams so Probleme beheben, bevor die Qualität, Sicherheit oder Compliance des SAP-Systems beeinträchtigt wird, egal, ob es sich um mangelhafte Codierung, fehlerhafte Konfiguration oder absichtliche Manipulation handelt. Das Regelwerk lässt sich dabei individuell erweitern, man kann eigene Pattern anlegen, eigene Suchmuster definieren und damit ganz konkret nach Schwachstellen suchen. Das Ganze ist über Customizing definiert, ohne Programmierkenntnisse möglich und macht damit den erweiterten SAP-Standard zu einer echten Bedrohungserkennung, mit der man kritische Inhalte automatisch blocken und über ein Security Dashboard tracken kann. Und schließlich ein weiterer signifikanter Vorteil: Alle Funde lassen sich in andere Tools exportieren und die Ergebnisse der Transportkontrolle beispielsweise in ein SIEM überführen.

Clemens Güter, Raphael Kelbert
www.pathlock.com/de

Multi-Faktor-Authentifizierung

FÜR ANGREIFER KEIN PROBLEM MEHR

Auf der Suche nach Ratschlägen zur Verbesserung der IT-Sicherheit fällt immer wieder der Begriff MFA. Die Abkürzung steht für Multi-Faktor-Authentifizierung und beschreibt ein Verfahren, bei dem für den Zugriff auf Systeme neben dem üblichen Passwort noch ein zusätzlicher Faktor erforderlich ist. Dadurch gilt MFA als besonders wirksam gegen Phishing- und andere Social-Engineering-Angriffe.

Bei den meisten Implementierungen muss der Benutzer einen zusätzlichen Code eingeben oder einen Login-Versuch über eine App bestätigen. Es ist unbestritten, dass dieser zusätzliche Faktor einen Angriff erschwert. Doch reichen die üblichen Implementierungen von MFA aus, um wirklich resistent gegen Phishing-Attacken und Accountübernahmen zu sein? Die vergangenen Angriffe auf Uber[1] und Cisco[2] zeigen, dass MFA bereits aktiv von Angreifern umgangen wird und MFA-Prozesse zwingend sicherer implementiert werden müssen.

MFA SCHÜTZT NICHT GRUNDSÄTZLICH VOR DER KOMPROMITTIERUNG EINES ACCOUNTS. INSBESONDERE WIRD DER ANGRIFFSVEKTOR DURCH SOCIAL ENGINEERING ÜBERSEHEN.

Timo Sablowski, Senior Security Consultant, carmasec GmbH & Co. KG, www.carmasec.com

Wie überwinden Angreifer den zusätzlichen Schutz durch MFA?

MFA Fatigue

Für Angreifer existieren verschiedene Möglichkeiten, um initial an die Kennwörter von Benutzern zu gelangen. So können diese über vergangene Phishing-Kampagnen, kompromittierte Systeme, gekaufte Zugangsdaten, Credential Stuffing, oder das simple Ausprobieren erlangt werden. Jede dieser Methoden ist auf ihre Art und Weise erfolgreich und beinhaltet eine solide Chance auf Erfolg. Diese steigt mit der Mitarbeiterzahl eines Unternehmens. Damit der Angreifer diese Zugangsdaten aber nicht direkt zur Anmeldung verwenden kann, ist ein zweiter Faktor im Rahmen von MFA üblich.

Das Generieren und Eingeben eines zusätzlichen Einmalpasswortes für jeden Login-Versuch kann für Benutzer schnell lästig werden. Um dem entgegenzuwirken, wurden MFA-Methoden entwickelt, die einen besonders hohen Bequemlichkeitsfaktor aufweisen, wie zum Beispiel die Aufforderung zur Bestätigung über das Smartphone. Hierbei wird der Benutzer nach der Eingabe seines Benutzernamens und Passworts über eine Push-Benachrichtigung aufgefordert, den gerade stattfindenden Login-Vorgang zu bestätigen.

Verwendet der Angreifer ebenfalls die korrekte Kombination von Benutzernamen und Passwort seines Opfers, wird dieses auf dem Smartphone darauf aufmerksam gemacht, dass eine Anmeldung per App bestätigt werden muss. Um den Angriff ins Leere laufen zu lassen, müsste das Opfer diese Nachricht nur ignorieren. Doch was passiert, wenn diese Push-Nachrichten zu Hunderten und über mehrere Tage gesendet werden? Es kann hier zu einer Ermüdung des Benutzers (Fatigue) kommen, sodass dieser schließlich der Aufforderung nachkommt und die Anmeldung bestätigt.

Dieser Angriff ist zwar recht offensichtlich, wird aber häufig nicht erkannt.

Quellen
1 https://www.vice.com/en/article/5d35yd/the-uber-hack-shows-push-notification-2fa-has-a-downside-its-too-annoying
2 https://www.bleepingcomputer.com/news/security/cisco-hacked-by-yanluowang-ransomware-gang-28gb-allegedly-stolen/

Denn wie bei allen Social-Engineering-Methoden reicht ein einziger erfolgreicher Angriff auf einen einzelnen Mitarbeiter aus, damit sich Kriminelle Zugang zum Unternehmensnetzwerk verschaffen können. Um die Erfolgschancen zu erhöhen, werden die Opfer durch weitere Maßnahmen dazu verleitet, ankommenden Aufforderungen zur Authentifizierung über das Smartphone nachzukommen. So geben sich Angreifer als IT-Support aus und nutzen gefälschte Telefonnummern, um ihre Opfer anzurufen. Ebenfalls üblich ist der Versand von SMS mit der Bitte um Entschuldigung für die Unannehmlichkeiten bei der Benutzung von IT-Systemen. Der Benutzer müsse kurz die Anfrage bestätigen, sodass eine normale Arbeit wieder möglich sei.

Eine weniger auffällige, aber ebenso wirksame Variante erfordert Vorarbeit durch Ausspähen der Opfer im Rahmen der Informationsbeschaffung vor dem Angriff. Weiß der Angreifer beispielsweise, wann das potenzielle Opfer mit der Arbeit beginnt oder von der Mittagspause zurückkehrt, kann dieser einen guten Zeitpunkt für einen Angriffsversuch abpassen. Beim Arbeitsbeginn oder bei der Wiederanmeldung an Systemen sind Menschen weniger vorsichtig, weil sie es gewohnt sind, nach einer längeren Phase der Inaktivität zur Eingabe eines zweiten Faktors aufgefordert zu werden. Passt der Angreifer diesen Zeitpunkt ab, ist die Chance, dass das Opfer der Aufforderung nachkommt, deutlich höher.

Adversary in the Middle (AiTM)

Die Gefahr für einen Angreifer bei der Überflutung der Benutzer durch MFA-Anfragen aufzufallen, ist äußerst hoch. Eine weniger auffällige Methode ist die Erstellung von Phishing-Webseiten, die nicht nur Zugangsdaten abgreifen, sondern obendrein als Vermittler zwischen dem Opfer und der eigentlichen Applikation dienen. Man spricht hier vom „Adversary in the Middle" (AiTM).

Mit Hilfe frei zugänglicher Werkzeuge erstellt der Angreifer eine exakte Kopie des Portals, zu dem er sich Zugriff verschaffen will. Nun muss der Angreifer das Opfer auf diese Kopie locken. Hierfür werden die gängige Methoden wie eine Aufforderung per E-Mail, SMS oder ähnliche Wege genutzt.

Mit modernen Texterstellungshelfern wie ChatGPT lässt sich eine gefälschte E-Mail mit der richtigen Wortwahl erstellen, um zum Beispiel Zugänge für eine „Microsoft 365"-Instanz (M365) eines Unternehmens zu erlangen. Diese kann anschließend an die Mitarbeitenden im Unternehmen versendet werden. Die entsprechende Formatierung und eine vertrauenswürdig aussehende Absenderdomain steigern die Chancen auf Erfolg.

```
https://login.microsoft.ganzbestimmtkeinphishing.de/gzfFBSxT

[12:22:05] [imp] [0] [o365] new visitor has arrived: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537
.36 (KHTML, like Gecko) Chrome/111.0.0.0 Safari/537.36 ([redacted])
[12:22:05] [inf] [0] [o365] landing URL: https://login.microsoft.ganzbestimmtkeinphishing.de/gzfFBSxT
[12:27:28] [+++] [0] Password: [jw[redacted]zy]
[12:27:28] [+++] [0] Username: [demo.user@[redacted].com]
[12:27:28] [+++] [0] Username: [demo.user@[redacted].com]
[12:27:41] [+++] [0] Username: [demo.user@[redacted].com]
[12:27:45] [+++] [0] all authorization tokens intercepted!
:
```

Bild1: Speicherung der Zugangsdaten durch den Phishing-Server

id	phishlet	username	password	tokens	remote ip	time
1	o365	demo.user@...	jw...	captured	[redacted]	2023-03-16 12:27

Bild 2: Ein Session-Token konnte erlangt werden

Klickt ein Benutzer auf den mitgelieferten Link, gelangt er auf die Phishing-Webseite. Der Nutzer wird zum Login auf die M365-Dienste aufgefordert. Die Verbindung ist per TLS abgesichert, so dass der Browser keine Warnung anzeigt.

Werden die Zugangsdaten eingegeben, finden folgende Schritte im Hintergrund statt:

Die eingegebenen Zugangsdaten werden auf dem Phishing-Server gespeichert und an das eigentliche Zielsystem weitergeleitet.

Dieses überprüft Benutzername und Kennwort und fordert zur Eingabe des zweiten Faktors auf. Dem Opfer wird die gleiche Abfrage präsentiert. Wird der zweite Faktor eingegeben, wird auch dieser über den Phishing-Server an das Zielsystem übermittelt, woraufhin dort ein Session-Token für den Benutzer erstellt wird. Das Token wird an das Opfer weitergegeben. Mit dem Token kann anschließend der Browser an das Zielsystem weiter- oder die Sitzung durch den Phishing-Server durchgeleitet werden. In beiden Fällen ist der User im Zielsystem eingeloggt. Durch einen für den Benutzer „reibungslosen" Login-Prozess besteht die Möglichkeit, dass das Opfer keinen Unterschied erkennen kann.

Das generierte Session-Token wird dem Angreifer ebenfalls übergeben. Dieser kann das Token im eigenen Browser nutzen, um im Namen des Opfers die Applikation auf dem Zielsystem zu verwenden. In diesem Fall verfügt er nun über eine gültige Sitzung in M365.

Initial Access mit gestohlenem Session-Token

Der Angreifer hat nun initialen Zugriff auf kritische Ressourcen und einen Fuß in der digitalen Tür des Unternehmens. Damit kann er seinen vielfältigen Handlungsspielraum erweitern. So kann er zum Beispiel im E-Mail-Postfach oder in MS Teams nach Nachrichten suchen, die Hinweise auf weitere Zugänge geben. Alle Dokumente, die dem eigentlichen Benutzer zugänglich sind, sind es nun auch für den Angreifer. Dieser kann nun nicht nur Daten stehlen, sondern sie auch modifizieren oder gar zerstören.

Darüber hinaus kann der Angreifer Schadsoftware auf dem SharePoint des Unternehmens ablegen oder Office-Dokumente mit schadhaften Makros versehen. Früher oder später wird eine weitere Person aus dem Unternehmen diese Dokumente oder abgelegten Dateien öffnen und weitere Malware nachladen.

Ebenso öffnet der Zugriff auf das E-Mail-Postfach oder den Teams-Kanal Tür und Tor für Social-Engineering-Methoden. Der Angreifer kann sich als valider Mitarbeitender des Unternehmens ausgeben und diese Vertrauensstellung nutzen, um Kollegen zu manipulieren und sich weitere Berechtigungen im Unternehmensnetzwerk verschaffen.

Ist der Angreifer erst einmal im Unternehmen aktiv, ist eine Erkennung nicht

immer trivial – insbesondere, wenn es sich um eine gezielte Attacke handelt, bei der die Täter möglichst unerkannt bleiben wollen.

Welche Maßnahmen können Unternehmen ergreifen?

In diesem Artikel wurden zwei unterschiedliche Arten zur Überwindung von MFA vorgestellt. Doch wie können sich Unternehmen vor diesen Angriffen schützen und worauf müssen sie achten? Hierzu existieren organisatorische und technische Maßnahmen, die umgesetzt werden sollten.

#1 Reduktion der Angriffsfläche

Zu den organisatorischen Maßnahmen gehört die Prüfung, ob jedes Portal und jeder Dienst überhaupt exponiert sein muss. Es ist wichtig, die Angriffsfläche zu minimieren. Nicht jede (interne) Anwendung muss über das Internet erreichbar sein.

#2 Mitarbeiterschulungen

Ebenso müssen alle Mitarbeitenden regelmäßig in Schulungen über typische Social-Engineering-Angriffe aufgeklärt werden.

#3 Conditial Access

Auch auf der technischen Seite können einige Verbesserungen vorgenommen werden. Conditial Access kann so konfiguriert werden, dass Anmeldungen ausschließlich über vom Unternehmen verwaltete Geräte erfolgen können. Ein Ablauf aktiver Sessions sollte spätestens nach einem Arbeitstag automatisch erfolgen, um Angreifern, die sich noch nicht festgesetzt haben, den erneuten Zugang zu erschweren.

#4 Umstellung auf FIDO2

Die wichtigste Maßnahme ist jedoch die Konfiguration der MFA selbst. Die gängigen Verfahren sind tatsächlich anfällig. Um Login-Verfahren abzusichern, sollte der Umstieg auf eine FIDO2-konforme und passwortlose Authentifizierung erfolgen. Mit kryptographischen Methoden kann dabei sowohl die Identität des Benutzers gegenüber dem System als auch umgekehrt die Identität des Systems gegenüber dem Benutzer eindeutig verifiziert werden. Damit laufen die genannten Angriffsmethoden ins Leere.

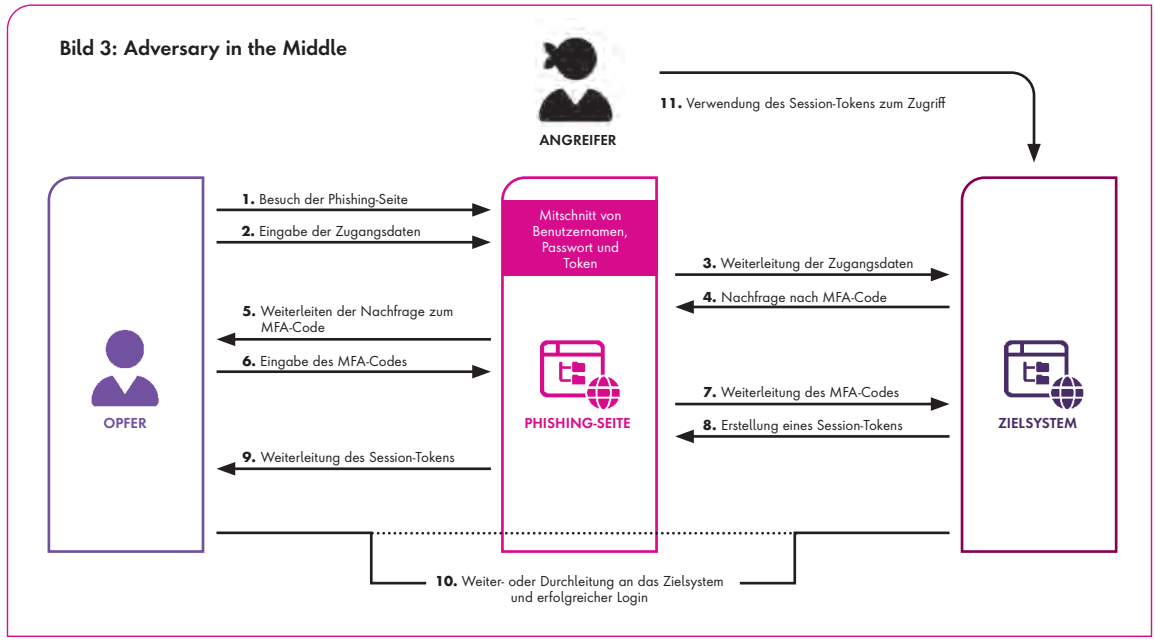
Fazit

MFA bietet einen verbesserten Schutz von Benutzerkonten vor eingekauften Zugangsdaten, Credential Stuffing oder dem Ausprobieren von Kennwörtern. Der Autor widerspricht jedoch der weitverbreiteten Meinung, dass MFA grundsätzlich vor der Kompromittierung eines Accounts schützt. Hierbei wird insbesondere der Angriffsvektor durch Social Engineering übersehen.

Darüber hinaus sollten Unternehmen ihre Angriffsfläche so gering wie möglich halten und sowohl organisatorische als auch technische Maßnahmen zum Schutz umsetzen. Die korrekten technischen Umsetzungen sind hier maßgeblich. Zu diesen zählt insbesondere der Umstieg auf sicherere Verfahren über FIDO2-konforme Implementierungen.

Timo Sablowski

Bild 3: Adversary in the Middle



ENDPUNKTSICHERHEIT FÜR MODERNES ARBEITEN

ERFOLGREICHE IMPLEMENTIERUNG UND GEWÄHRLEISTUNG

Endgerätesicherheit wird allgemein als Schutz Ihrer Geräteflotte vor Cyberangriffen verstanden. Obwohl dies ein wesentlicher Bestandteil ist, gehört zur erfolgreichen Implementierung und Gewährleistung der Endpunktsicherheit in Unternehmen noch mehr. Dabei handelt es sich nämlich um eine Reihe von Funktionen, die Ihre Geräte (sowie Benutzer) vor einer sich ständig weiterentwickelnden Bedrohungslage schützen. In dem Sinne müssen auch Sie handeln und die richtigen Tools für Ihre Geräte auswählen.

Wenn Sie neu im Apple Ökosystem sind oder sich zum ersten Mal mit der Endpunktsicherheit in der modernen Bedrohungslandschaft für Macs oder mobile Geräte befassen, zeigt Jamf Ihnen, wie moderne Verwaltung und Endpunktsicherheit aussehen kann.

Mit diesem White Paper können Sie:

- Unternehmensrisiken verstehen
- Endgerätesicherheit modernisieren
- Basislinien etablieren
- Vor moderner Malware schützen
- Native Apple Sicherheit erweitern
- Mehrschichtigen Ansatz zum Endgeräteschutz einsetzen
- Schwächen von All-in-One-Lösungen erkennen
- Lösungsübergreifende Integrationen verwenden
- Sicherheit und Leistung vereinbaren
- Nutzern helfen, sich selbst zu helfen

WHITEPAPER DOWNLOAD

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

Bildquelle: ©alphaspirit – Stock.adobe.com

Business Continuity Management

MIT BCM RISIKEN ERKENNEN UND RESILIENZ FÜR KRISEN AUFBAUEN

Die Ende 2022 beschlossene NIS2-Direktive muss bis Oktober 2024 in allen EU-Mitgliedsstaaten in nationale Gesetzgebung überführt werden. Ein funktionierendes Business Continuity Management (BCM) ist in jedem Fall ein wichtiger Baustein, um die Vorgaben von NIS2 als betroffenes Unternehmen oder Behörde umzusetzen. Es hilft Ihnen dabei, Risiken von Sicherheitsvorfällen zu erkennen und Maßnahmen zum Erhalt der Geschäftstätigkeit zu definieren. Sie identifizieren Ihre zeitkritischen Kernprozesse oder im behördlichen Umfeld Ihre zeitkritischen Verfahren – und können reaktiv oder vollumfänglich Resilienz für Not- und Krisensituationen aufbauen.

In 6 Schritten vom reaktiven zum vollständigen Standard-BCMS

1. In einem zweistufigen Vorgehen selektieren Sie in einer Voranalyse Ihre Kernprozesse oder -verfahren und bestimmen deren Zeitkritikalität mittels Business Impact Analyse.

2. Im anschließenden Soll-Ist-Vergleich ermitteln Sie bereits Ihren Handlungsbedarf durch divergierende Zeithorizonte zwischen Soll-Vorgaben und Ist-Werten.

3. Mit der folgenden Risikoanalyse bestimmen Sie Ihre Gefährdungen sowie die dadurch entstehenden Risiken und identifizieren erste Maßnahmen zur Risikoreduktion.

4. Für die Kontinuität Ihrer Tätigkeiten oder Verfahren im Not- und Krisenfall erstellen Sie einen Geschäftsfortführungsplan mit Maßnahmen für die Erreichung des Notbetriebes, für die Geschäftsfortführung im Notbetrieb und die Rückführung in den Normalbetrieb.

5. Ergänzt wird die Notfallbewältigung durch das Erstellen eines Notfallvorsorgekonzeptes oder Notfallhandbuchs.

6. Haben Sie alle Schritte durchlaufen, sollten Sie Ihr BCMS dem PDCA-Zyklus folgend konsequent weiterentwickeln und aktualisieren, um eine hohe Resilienz zu erlangen.

Ressourcenschonende Synergien nutzen

Da ein BCM eine Querschnittsfunktion darstellt, ist die initiale Implementierung recht umfangreich. Aber diese Querschnittsfunktion bietet auch großes Potential: Die benötigten Daten sind bereits im Unternehmen vorhanden und müssen nur kommuniziert und miteinander in Verbindung gebracht werden. Wenn Sie bereits ein Information Security Management System (ISMS) implementiert haben, vereinfacht und beschleunigt sich damit der Aufbau eines BCMS erheblich. Beide Managementsysteme basieren größtenteils auf den gleichen Daten. Mit einem geeigneten Software-Tool lassen sich die im Unternehmen vorhandenen Datenbestände des ISM zügig im BCM sichtbar machen, um so Schritt für Schritt ein strukturiertes, effizientes und nachhaltiges BCMS zum Beispiel nach dem BSI 200-4 Standard aufzubauen. Redundanzen und damit der gesamte Zeitaufwand lassen sich damit erheblich reduzieren.

Fazit

Die Vorteile eines BCM liegen auf der Hand: Sie können einer Krise gelassener entgegentreten, wenn der Betrieb auch während eines Notfalls gesichert ist oder schnell wiederaufgenommen werden kann. Beginnen Sie mit einem einfachen reaktiven BCM und suchen Sie sich die für die Bedürfnisse Ihres Unternehmens passenden Hilfsmittel, die Sie dabei unterstützen, den Reifegrad eines vollständigen Standard-BCMS zu erreichen. Betrachten Sie BCM nicht als Projekt mit definiertem Start- und Endzeitpunkt, sondern als dauerhafte Aufgabe, die das Überleben Ihres Unternehmens sichert. Seien Sie vorbereitet. Und fangen Sie am besten schon heute damit an.

www.hiscout.com

Eine Checkliste zur Auswahl eines geeigneten Tools finden Sie hier: **www.hiscout.com/checkliste-notfallmanagement**

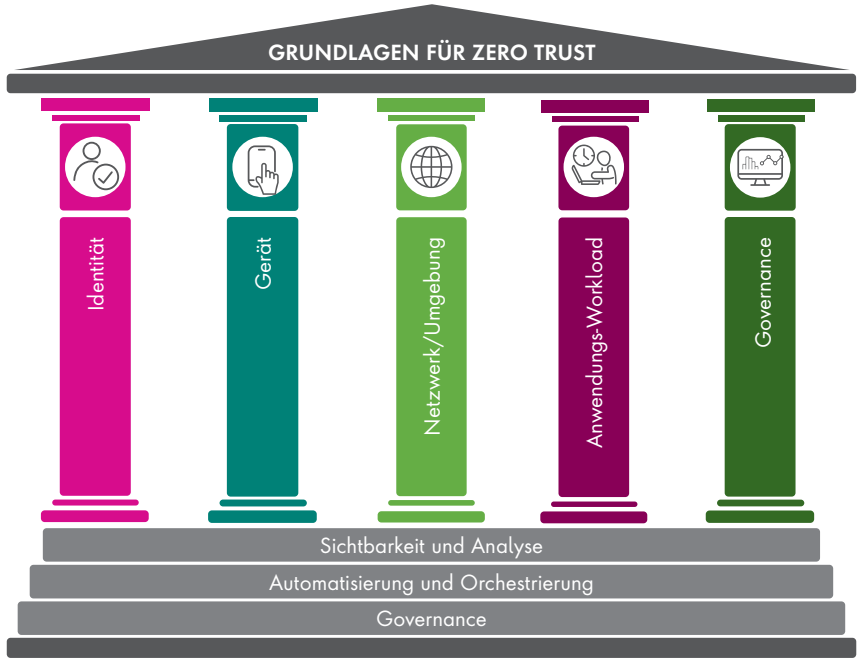


Bild 1: Die fünf Säulen des Reifegradmodells.

Zero Trust-Architektur und -Reifegradmodell

VOM SCHLAGWORT ÜBER DAS MODELL ZUR LÖSUNG

Zero Trust dürfte in den vergangenen Monaten das mit am häufigsten genannte Schlagwort in der IT-Security gewesen sein. Auch wir haben in unserem Printtitel it security und auf it-daily.net zahlreiche Artikel zu dem Thema publiziert. Eng mit dem Thema Zero Trust verwoben sind weitere Begriffe wie ZTNA, VPN, IAM oder auch die Verschlüsselungsthematik.

Zero Trust ist als allererstes kein Produkt, es ist ein Mindset, dessen sollte man sich bewusst sein. Wir sagen es immer wieder: vor allen Tools, die uns helfen sicherer zu werden, stehen Prozesse und natürlich die Frage der Architektur. Eine Zero-Trust-Architektur ist ein Sicherheitsmodell, das darauf abzielt, Cyber-Angriffe durch eine gründliche Überprüfung und Verifizierung von Netzwerkverbindungen und -aktivitäten zu verhindern. Im Wesentlichen vertraut eine Zero-Trust-Architektur keiner Verbindung oder Identität standardmäßig, sondern erfordert eine strenge Authentifizierung und Autorisierung für jeden Zugriff auf Netzwerkressourcen.

Schichtenmodell

Eine Zero-Trust-Architektur besteht immer aus mehreren Schichten, die eine hohe Sicherheit und ein geringes Risiko von Angriffen gewährleisten sollen. Hier sind einige wichtige Merkmale einer Zero-Trust-Architektur:

1. **Micro-Segmentation:** Eine Zero-Trust-Architektur implementiert die strikte Segmentierung von Netzwerken in kleine, unabhängige Abschnitte. Diese Abschnitte sind voneinander isoliert und erfordern eine separate Authentifizierung und Autorisierung, um auf sie zuzugreifen.

2. **Identitäts- und Zugriffsmanagement:** Eine Zero-Trust-Architektur setzt auf eine starke Authentifizierung und Autorisierung von Benutzern, Geräten und Anwendungen. Hierzu gehört eine Identitätsprüfung auf Basis von biometrischen Merkmalen, Zwei-Faktor-Authentifizierung und die Einhaltung von Richtlinien.

3. **Netzwerküberwachung und -analyse:** Eine Zero-Trust-Architektur erfordert eine ständige Überwachung des Netzwerks, um Verhaltensmuster und Anomalien zu erkennen und darauf zu reagieren. Hierbei werden maschinelle Lern- und Analysetechnologien eingesetzt.

4. **Data Protection:** Eine Zero-Trust-Architektur schützt Daten durch Verschlüsselung und Zugriffskontrolle, um sicherzustellen, dass nur autorisierte Benutzer auf Daten zugreifen können.

Insgesamt ist eine Zero-Trust-Architektur also eine sicherheitsorientierte Netz-

werkstruktur, die darauf abzielt, die Angriffsfläche zu minimieren und sensible Daten zu schützen.

Das Zero Trust-Reifegradmodell

In Summe ist Zero Trust nichts anderes als eine Sammlung von Konzepten und Ideen, ergo ein Mindset, das darauf abzielt, die Unsicherheit bei der Durchsetzung präziser Zugriffsentscheidungen mit den geringsten Rechten pro Anfrage in Informationssystemen und -diensten zu minimieren. Es soll den unbefugten Zugriff auf Daten und Dienste verhindern und die Durchsetzung der Zugriffskontrolle so granular wie möglich gestalten. Konzeptionell stellt es eine Verlagerung von einem ortsbezogenen Modell zu einem stärker datenbezogenen Ansatz für feinkörnige, granulare Sicherheitskontrollen zwischen Benutzern, Systemen, Daten und Vermögenswerten dar, die sich im Laufe der Zeit ändern. Dies bietet die nötige Transparenz, um die Entwicklung, Implementierung, Durchsetzung und Weiterentwicklung von Sicherheitsrichtlinien zu unterstützen.

Die Cybersecurity & Infrastructure Security Agency, kurz CISA, hat sich im Zuge des Zero Trust-Hypes näher mit dem Thema beschäftigt und eine von vielen Roadmaps erstellt, auf die sich Behörden beim Übergang zu einer Zero Trust-Architektur beziehen können. Ziel des Reifegradmodells ist es, die Behörden bei der Entwicklung ihrer Zero-Trust-Strategien und Implementierungspläne zu unterstützen und Wege aufzuzeigen, wie verschiedene CISA-Dienste Zero-Trust-Lösungen in den Behörden unterstützen können. Die CISA hat das Zero Trust Maturity Model 2021 ursprünglich entworfen, um die Behörden bei der Einhaltung der Executive Order zu unterstützen. Analog ist so eine Reifegradmodell natürlich auf jedes Unternehmen anwendbar.

Das Reifegradmodell, das fünf Säulen und drei übergreifende Fähigkeiten umfasst, basiert auf den Grundlagen von Zero Trust. Innerhalb jeder Säule bietet das Reifegradmodell Unternehmen wie Behörden spezifische Beispiele für eine traditionelle, fortgeschrittene und optimale Zero-Trust-Architektur. Barracuda hat das in seinem Blog ganz gut beschrieben.

Die fünf verschiedenen Säulen für die Zero-Trust-Implementierung umfassen demnach:

Identität: Ein Attribut oder eine Gruppe von Attributen, die einen Behördenbenutzer oder eine Entität eindeutig beschreibt.

Gerät: Jedes Hardware-Asset, das eine Verbindung zu einem Netzwerk herstellen kann, einschließlich Internet-of-Things-Geräte (IoT), Mobiltelefone, Laptops, Server und andere.

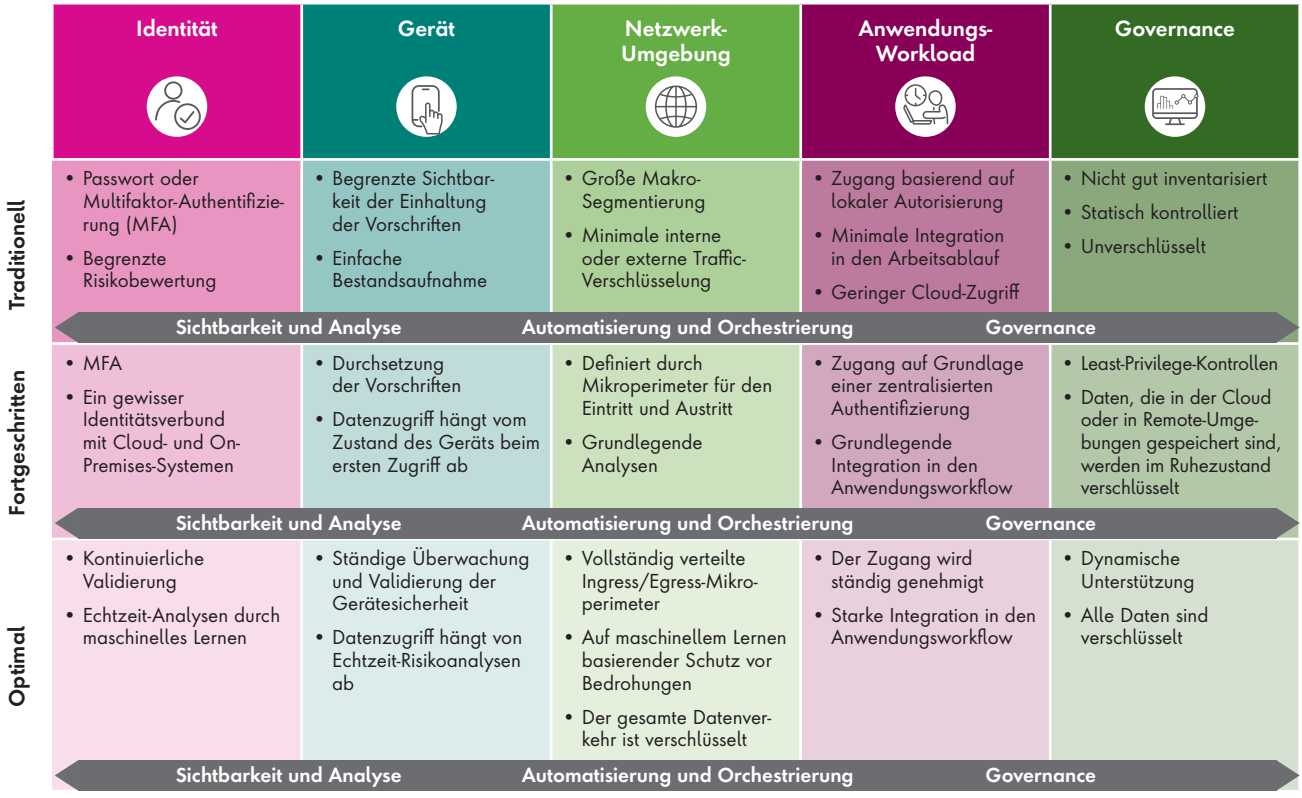


Bild 2: Jede der fünf Säulen hat drei Ausprägungen des Reifegradmodells

MEHR WERT

Zero Trust Maturity Model

Netzwerk: Ein offenes Kommunikationsmedium, einschließlich behördeninterne Netzwerke, Drahtlosnetzwerke und das Internet, das zur Übertragung von Nachrichten verwendet wird.

Anwendungs-Workload: Systeme, Computerprogramme und Dienste, die sowohl lokal als auch in einer Cloud-Umgebung ausgeführt werden.

Daten: Daten sollten auf Geräten, in Anwendungen und in Netzwerken geschützt werden.

Das Maturity-Modell beschreibt einen Verlauf der Implementierung dieser Säulen, was bedeutet, dass die Bereitstellung für jede Säule unabhängig und zu unterschiedlichen Zeiten beginnen kann. Die unternehmensweite Zero-Trust-Bereitstellung kann auf diese Weise erfolgen, bis sie den Punkt erreicht hat, an dem Automatisierung, Transparenz und dynamische Richtlinienerstellung die Integration aller fünf Säulen erfordern.

Drei Reifephasen

Um den Verlauf des Modells zu unterstützen, hat die CISA drei Reifephasen für jede Säule festgelegt:

1. **Traditionell:** Manuelle Konfigurationen und statische Sicherheitsrichtlinien.

2. **Erweitert:** Zentralisierte Transparenz, Identitätskontrolle und Richtliniendurchsetzung auf der Grundlage einer teilweisen säulenübergreifenden Koordination.

3. **Optimal:** Vollautomatische Zuweisung von Attributen zu Assets und Ressourcen, dynamische Richtlinien basierend auf automatischen Auslösern und Abstimmung mit offenen Standards für säulenübergreifende Interoperabilität.

Das Originaldokument (s. QR-Code links oben) geht noch viel detaillierter darauf ein.

Ulrich Parthier – it-daily.net

FRAMEWORK FÜR CYBER RESILIENZ

WARUM ES FÜR UNTERNEHMEN ENTSCHEIDEND IST

eBOOK DOWNLOAD

Das eBook umfasst 21 Seiten und steht zum kostenlosen Download bereit:
www.it-daily.net/download

Cyber Resilienz, das heißt die Fähigkeit, den Geschäftsbetrieb angesichts endloser und sich weiterentwickelnder Cyber-Bedrohungen aufrechtzuerhalten, kann für jedes Unternehmen ein abschreckendes Thema sein. Hinzu kommt die Komplexität der IT-Fußabdrücke von Unternehmen – die heute oft aus einem verteilten Netz aus Cloud-Anwendungen, privaten Servern und Mitarbeitergeräten bestehen. Kritische Daten, die Währung der Geschäftswelt, sind über diesen Fußabdruck verteilt und in Dokumenten, Tabellen, elektronischer Kommunikation und Datenbanken gespeichert. Diese Daten sind die Basis des Geschäfts. Wenn der Zugriff auf Daten unterbrochen wird, wie bei einem Ransomware-Angriff, können die Auswirkungen verheerend sein.

Cyber Resilienz muss aber nicht abschreckend sein.

Anomalien erkennen

END-TO-END-ECHTZEIT-ARCHITEKTUR NUTZEN

Echtzeit-Kommunikationsnetze gewinnen speziell in cyber-physischen Systemen in kritischen Bereichen, wie etwa in modernen Produktionsanlagen oder in intelligenten Energienetzen, immer mehr an Bedeutung. Analog dazu wird der Einsatz von Machine Learning eine zunehmende Rolle spielen, um Anomalien rechtzeitig erkennen zu können.

„Die Erkennung von Anomalien ist ein Beispiel für die erfolgreiche Anwendung von Machine-learning-Methoden. Algorithmen erkennen eigenständig Muster und Gesetzmäßigkeiten in Datensätzen und können daraus Lösungen entwickeln", sagt Peter Dorfinger, Leiter der Forschungsgruppe Intelligent Connectivity der Salzburg Research Forschungsgesellschaft.

Machine Learning trifft Echtzeit-Netzwerke

Salzburg Research hat eine End-to-End-Echtzeit-Architektur zur Erkennung von Anomalien entwickelt. In dieser Architektur werden die Sammlung und Übertragung der erforderlichen Daten, die Analyse dieser Daten in einem maschinellen Lernmodell und die anschließende Reaktion in einer festgelegten Zeit durchgeführt. Während bisherige Ansätze bereits Machine Learning zur Anomalie-Erkennung einsetzen, bringen die Forscher der Salzburg Research Forschungsgesellschaft in ihrem Ansatz auch ihr Know-how im Bereich Echtzeit-Kommunikationsnetze mit hinein.

Zum Einsatz kommen sogenannte „Autoencoder Neuronal Networks" (ANNs), eine besondere Art eines künstlichen neuronalen Netzes. Sie können unstrukturierte Daten verarbeiten. „Der Lernprozess des neuronalen Netzes ist unüberwacht. Das bedeutet, dass keine Kennzeichnung der Eingabedaten erforderlich ist. Dies ist ein großer Vorteil, da diese Vorbearbeitung von Daten in der Regel sehr aufwändig ist", so Dorfinger weiter.

PoC: Neuronales Netz bewirkt Rekonfiguration

Die vorgeschlagene Lösung von Salzburg Research wurde für zwei Use Cases entworfen: Zum einen zur Erkennung von Anomalien in den Netzdaten mit Echtzeit-Rekonfiguration des Echtzeit-Ethernet-Netzes. Und zum anderen zur Erkennung von Anomalien bei Maschinendaten mit Rekonfiguration von Industriemaschinen in Echtzeit. Ein Proof-of-Concept wurde im Labor umgesetzt. Nachdem das ANN eine Anomalie entdeckt hat, wird eine Rekonfiguration der Netzwerkflüsse, wie etwa Abschalten eines Netzwerkpfads, Umschalten auf einen anderen Netzwerkpfad, oder eine Rekonfiguration der Maschinen, beispielsweise mittels neuer Parametereinstellungen, ausgelöst.

In Zukunft sollen Messungen durchgeführt werden, um die vorgeschlagene Architektur im Hinblick auf die tatsächliche Reaktionszeit von der Erkennung von Anomalien bis zur Neukonfiguration des Netzes oder der Maschine zu bewerten. Die Ergebnisse werden dann mit Messungen in bestehenden Anomalieerkennungssystemen verglichen.

Bei der Lösung handelt es sich um einen Architekturvorschlag und nicht um ein fertig verwendbares Produkt. Das Alleinstellungsmerkmal ist die vollständig geschlossene Echtzeit-Schleife (mit Garantien der maximalen Zeitdauer der Reaktion). Dies wird erreicht durch die Kombination von Echtzeitkommunikationsnetz und Feed-Forward NN. Auch passt sich die Architektur dynamisch an das jeweilige Kommunikationsnetz an.

Am Markt verfügbare Produkte wie Genua Congitix fokussieren meist auf klassische LAN-Netze und können somit auch keine Echtzeit-Garantien für die Umsetzung der Reaktion geben.

www.salzburgresearch.at

Neue Abwehr-Strategie

KI VERÄNDERT ALLES, WAS SIE ÜBER E-MAIL-CYBERANGRIFFE WISSEN

BEUNRUHIGENDE FAKTEN

87% der Arbeitnehmer weltweit sind besorgt, dass Hacker generative KI nutzen können, um betrügerische E-Mails zu erstellen, die von echter Kommunikation nicht zu unterscheiden sind.

25% der Mitarbeiter ist in der Vergangenheit auf eine betrügerische E-Mail oder SMS hereingefallen.

65% der Mitarbeiter haben in den letzten sechs Monaten einen Anstieg der Häufigkeit von betrügerischen E-Mails und SMS festgestellt.

87% der Mitarbeiter sind besorgt über die Menge an persönlichen Informationen, die online über sie verfügbar sind und die zum Phishing missbraucht werden könnten.

87% der Unternehmen verhindern die Spam-Filter fälschlicherweise, dass wichtige legitime E-Mails in ihren Posteingang gelangen.

Generative KI verändert Angriffe und macht sie deutlich raffinierter als in der Vergangenheit. Das zeigt der jüngste Fall – der Zusammenbruch der Silicon Valley Bank (SVB) und die daraus resultierende Bankenkrise. Die Angreifer nutzten die Situation sofort, um hochsensible Kommunikation zu fälschen. Dazu fingen sie legitime Mitteilungen ab, in denen die Empfänger angewiesen wurden, ihre Bankdaten für die Gehaltsabrechnung zu aktualisieren. Dieser konkrete Vorfall korrespondiert mit allgemeinen Zahlen: 62 Prozent der Angestellten in Finanzdienstleistungsunternehmen haben in den letzten sechs Monaten eine Zunahme von betrügerischen E-Mails und SMS festgestellt.

Generative KI erfordert daher eine neue Abwehr-Strategie auf Basis von selbstlernender KI. Im Gegensatz zu allen anderen E-Mail-Sicherheitstools ist sie in Darktrace Emails nicht darauf trainiert, wie „Angriffe" aussehen, sondern lernt die normalen Verhaltensmuster in jedem einzelnen Unternehmen kennen. Mit einem tiefgreifenden Verständnis des Unternehmens und der Interaktionen der einzelnen Mitarbeiter mit ihrem Posteingang kann die KI für jede E-Mail bestimmen, ob sie verdächtig oder legitim ist. Insbesondere Mails des CEO werden damit besser geschützt.

ChatGPT als Risiko

Neue Daten von Darktrace zeigen, dass E-Mail-Sicherheitslösungen, einschließlich nativer, cloudbasierter und statischer KI-Tools, im Durchschnitt dreizehn Tage benötigen, bis ein Angriff auf ein Opfer erkannt wird. Dann sind Unternehmen fast zwei Wochen lang ungeschützt, wenn sie sich ausschließlich auf diese Tools verlassen. Social Engineering – insbesondere bösartige Cyber-Kampagnen per E-Mail – ist nach wie vor die Hauptursache für die Anfälligkeit eines Unternehmens für Angriffe. Der weit verbreitete Zugang zu generativen KI-Tools wie ChatGPT sowie die zunehmende Raffinesse der staatlichen Akteure bedeuten, dass E-Mail-Betrügereien überzeugender sind als je zuvor.

https://de.darktrace.com

WORAN ERKENNEN SIE EINEN PHISHING-ANGRIFF?

72% Aufforderung, auf einen Link zu klicken oder einen Anhang zu öffnen

61% unbekannter Absender oder unerwarteter Inhalt

62% schlechte Rechtschreibung und Grammatik

Industrie 4.0

WIR BRAUCHEN INTEGRIERTE SICHERHEIT

Eine präzise Produktion benötigt IT- und OT-Sicherheit, die mit wachsenden Anforderungen flexibel skalieren kann. Eine Herausforderung, der viele Unternehmen gegenüberstehen. Überwachungs- und Steuerungssysteme sind über viele Jahre im Einsatz, ohne kontinuierliche Sicherheitsupdates. Mit der Anbindung an ein IP-Netz stellen diese Maschinen ein Sicherheitsrisiko dar. Hinzu kommen unsichere Verbindungen sowie eine eingeschränkte Sichtbarkeit. Außerdem ersetzen Unternehmen zunehmend proprietäre Kommunikationsprotokolle durch die weltweit verbreiteten und akzeptierten Netzwerkprotokolle Ethernet und TCP/IP. Diese verbesserte Vernetzung bedeutet jedoch, dass Industrieanlagen eine größere Angriffsfläche für Cyberkriminelle bieten.

Zentrales Sicherheits- und Management-System

Der grundlegende Schritt für die Bereitstellung einer sicheren IT-Infrastruktur ist die Implementierung einer umfassenden Sicherheitslösung, wie das Network Bundle von macmon secure. Für den Schutz der Netzwerkzugänge bietet das System die Funktionen Topology, Advanced Security, Network Access Control, VLAN, 802.1X und Guest Service. Es schützt damit Netzwerke vor dem Eindringen unerwünschter Geräte durch eine zentrale Sicherheitsinstanz, ermöglicht deren gezielte Abwehr und gewährleistet eine schnelle und komplette Übersicht aller Geräte für ein transparentes und effizientes Netzwerkmanagement. Bei der Konzipierung und Implementierung einer IT-Security-Strategie müssen Unternehmen dabei immer Wert auf die Balance zwischen einem Maximum an Sicherheit und der Usability für die Mitarbeitenden legen. Ein wichtiger Aspekt bei der Auswahl einer solchen Lösung sollte die Anbindungsmöglichkeit an weitere Sicherheitslösungen sein, um einen Informationsaustausch der Systeme zu gewährleisten.

Ende der doppelten Datenpflege

Eine der gefährlichsten und zugleich unbeliebtesten Aufgaben ist die doppelte Datenpflege. Informationen, die von mehreren Systemen benötigt und verarbeitet werden, müssen konsistent sein, um Fehler und Vorfälle zu vermeiden. Über eine gemeinsame Schnittstelle werden Informationen zielorientiert innerhalb der Anwendungen ausgetauscht. Das reduziert administrative Prozesse, senkt die Fehlerquote durch Automatisierung und erhöht die Netzwerksicherheit.

Ein Beispiel: Die Management Suite von Baramundi unterstützt die IT-Abteilung beim Installieren, Verteilen, Inventarisieren, Schützen oder Sichern von Endgeräten. Mit den modularen Funktionen reduziert sich der Aufwand für bisher manuell erledigte Routineprozesse. Gleichzeitig kann der gesamte Lifecycle aller im Unternehmen eingesetzten Endgeräte betreut werden. Auf der anderen Seite unterstützt die NAC-Lösung bei der Kontrolle und Steuerung des Netzwerkes, inklusive der zugehörigen Infrastruktur. Die Integration beider Produkte ermöglicht den direkten Datenaustausch sowohl zur automatisierten Pflege als auch zur automatisierten Reaktion auf Geräte, die nicht den Sicherheitsanforderungen des Unternehmens entsprechen.

Die Erfassung der gesamten Infrastruktur und aller Endgeräte als Live-Bestandsmanagement zählt zu den Kernkompetenzen von macmon. Darunter fallen beispielsweise die grafische Darstellung der Netzwerk-Topologie mit umfangreichen Analysemöglichkeiten und das Reporting der im Netzwerk ermittelten Messdaten. Durch Technologiepartnerschaften kann die NAC-Lösung als zentrales Sicherheits- und Management-System genutzt werden.

www.macmon.eu

Künstliche Intelligenz & IT Security

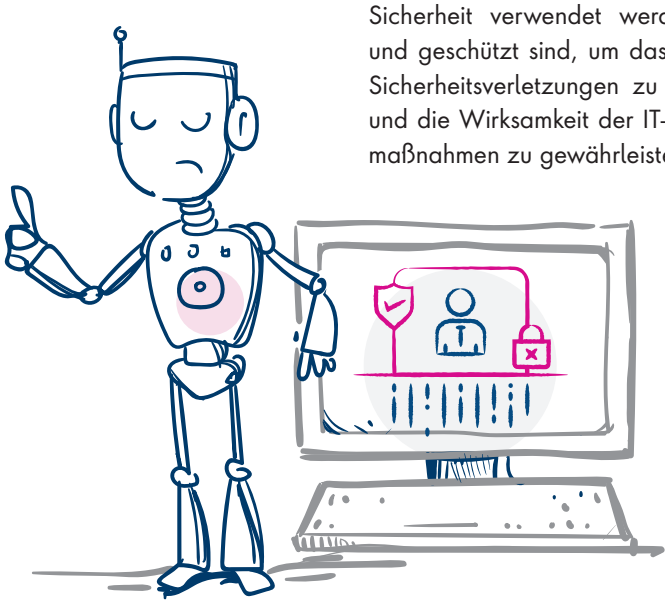
WAS MUSS MAN BEDENKEN?

KI (Künstliche Intelligenz) und IT-Sicherheit sind eng miteinander verbunden, da KI-Systeme selbst potenzielle Angriffsziele sind, aber auch zur Absicherung von IT-Systemen eingesetzt werden können

Nachfolgend beschreiben wir sechs wichtige Aspekte, die man bei der Verwendung von KI in der IT-Sicherheit beachten sollte:

Datensicherheit

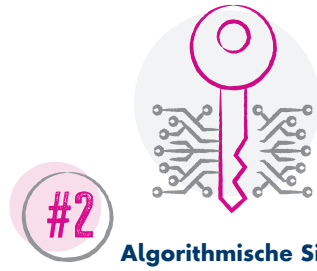
KI-Systeme benötigen große Mengen an Daten, um trainiert zu werden. Es ist wichtig sicherzustellen, dass diese Daten sicher und geschützt sind, um das Risiko von Datenverlust oder -lecks zu minimieren.



Ein Beispiel ist die Verwendung von KI-Systemen zur Erkennung von Malware (Schadsoftware) in Unternehmen. Diese KI-Systeme müssen trainiert werden, um Malware von legitimer Software zu unterscheiden, indem sie große Mengen von Malware-Daten analysieren und Muster identifizieren, die auf eine Bedrohung hinweisen.

Wenn die Malware-Daten kompromittiert werden, könnte dies dazu führen, dass die KI-Systeme falsche Entscheidungen treffen und legitime Software als Malware erkennen oder umgekehrt. Dies würde die Wirksamkeit der IT-Sicherheitsmaßnahmen des Unternehmens beeinträchtigen und die Sicherheit der Systeme und Daten des Unternehmens gefährden.

Daher ist es wichtig, dass Unternehmen sicherstellen, dass die Daten, die für die Verwendung von KI-Systemen in der IT-Sicherheit verwendet werden, sicher und geschützt sind, um das Risiko von Sicherheitsverletzungen zu minimieren und die Wirksamkeit der IT-Sicherheitsmaßnahmen zu gewährleisten.



Algorithmische Sicherheit

Frei nach dem Motto: „Phish me, if you can". Die Algorithmen, die in KI-Systemen verwendet werden, müssen sorgfältig getestet und überwacht werden, um sicherzustellen, dass sie nicht gehackt oder manipuliert werden können. Ein Beispiel für die Bedeutung von algorithmischer Sicherheit wäre die Verwendung von KI-Systemen zur Erkennung von Phishing-Angriffen.

Phishing-Angriffe sind eine häufige Methode, um Informationen von Benutzern zu stehlen, indem sie dazu verleitet werden, auf einen Link zu klicken oder einen Anhang zu öffnen, der schädlichen Code enthält. KI-Systeme können verwendet werden, um Phishing-Angriffe zu erkennen, indem sie Muster in E-Mails und Links analysieren und verdächtige Aktivitäten identifizieren.

Ein praktisches Beispiel für einen Angriff auf KI-Systeme zur Erkennung von Phishing-Angriffen ist eine Adversarial Attack. Hierbei wird der Algorithmus absichtlich manipuliert, um den Angriff zu maskieren und für den Nutzer unerkennbar zu machen. Wenn ein Angreifer den Algorithmus manipulieren kann, um Phishing-E-Mails als legitime E-Mails zu kennzeichnen, würde dies dazu führen, dass Benutzer gefälschte E-Mails als sicher ansehen und dadurch leichter einem Phishing-Angriff zum Opfer fallen.

#3 Vertraulichkeit und Datenschutz

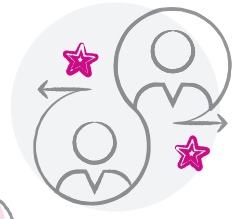
KI-Systeme müssen so konfiguriert werden, dass sie die Vertraulichkeit von Daten und die Privatsphäre der Benutzer schützen. Es ist wichtig sicherzustellen, dass die KI-Systeme nur auf die Daten zugreifen, die sie benötigen, und dass diese Daten nicht von Dritten abgefangen oder gestohlen werden können.

Das bedeutet, dass es möglich sein muss, zu verstehen, wie ein KI-System zu einer Entscheidung gekommen ist, insbesondere wenn diese Entscheidung Auswirkungen auf die Sicherheit hat.

Auch hierzu ein Beispiel: Für die Bedeutung der Transparenz von KI-Systemen in der IT-Sicherheit ist die Verwendung von KI-Systemen zur Erkennung von Anomalien in Netzwerkaktivitäten geeignet. Diese KI-Systeme können verwendet werden, um verdächtige Aktivitäten in Netzwerken zu identifizieren, indem sie Muster in den Daten analysieren und Anomalien erkennen.

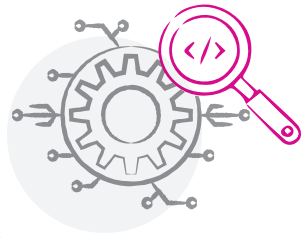
Wenn ein KI-System eine verdächtige Aktivität erkennt, die als mögliche Bedrohung für die IT-Sicherheit eingestuft wird, muss es möglich sein, nachzuvollziehen, wie das KI-System zu dieser Entscheidung gekommen ist. Die Transparenz des KI-Systems ist wichtig, um sicherzustellen, dass die Entscheidung nachvollziehbar ist und dass die erforderlichen Maßnahmen ergriffen werden können, um die Bedrohung zu neutralisieren.

Ohne Transparenz könnte es schwierig sein, das Vertrauen in das KI-System aufrechtzuerhalten und sicherzustellen, dass seine Entscheidungen korrekt sind. Wenn ein KI-System beispielsweise eine verdächtige Aktivität fälschlicherweise als Bedrohung einstuft und unnötige Maßnahmen ergriffen werden, könnte dies die Effizienz des Netzwerks beeinträchtigen und zu unnötigen Kosten führen.



#4 Ethik und Fairness

KI-Systeme sollten außerdem so konzipiert werden, dass sie fair und ethisch sind. Es ist wichtig sicherzustellen, dass die Entscheidungen, die von KI-Systemen getroffen werden, nicht diskriminierend oder voreingenommen sind und dass sie den Datenschutz- und Sicherheitsrichtlinien entsprechen. Dies ist eine der größten Schwachpunkte von KI-Systemen, denn diese Ebene ist in KI-Systemen nicht verankert.



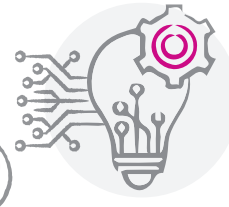
#5 Kontinuierliche Überwachung

KI-Systeme müssen kontinuierlich überwacht werden, um sicherzustellen, dass sie sicher und effektiv funktionieren. Es ist wichtig, dass Fehler oder Anomalien schnell erkannt und behoben werden können, um das Risiko von Sicherheitsverletzungen zu minimieren.

Sie müssen skalierbar sein, um mit der Menge an Daten und Ressourcen umgehen zu können, die für die Sicherheit eines Unternehmens oder einer Organisation erforderlich sind. Das bedeutet, dass ein KI-System so konzipiert sein muss, dass es in der Lage ist, sich an die wachsenden Anforderungen an Skalierbarkeit anzupassen, insbesondere wenn es mit großen Mengen von Daten arbeitet.

Auch hierzu ein Beispiel: Für die Bedeutung der Skalierbarkeit von KI-Systemen in der IT-Sicherheit ist die Verwendung von KI-Systemen zur Erkennung von Angriffen auf Webanwendungen von Vorteil. Da immer mehr Anwendungen online verfügbar sind und die Zahl der Webangriffe ständig zunimmt, ist es wichtig, dass KI-Systeme zur Erkennung von Angriffen auf Webanwendungen in der Lage sind, mit der steigenden Datenmenge und der wachsenden Anzahl von Anwendungen umzugehen. Darüber hinaus muss das System in der Lage sein, die Daten in Echtzeit zu analysieren, um schnell auf Angriffe reagieren zu können.

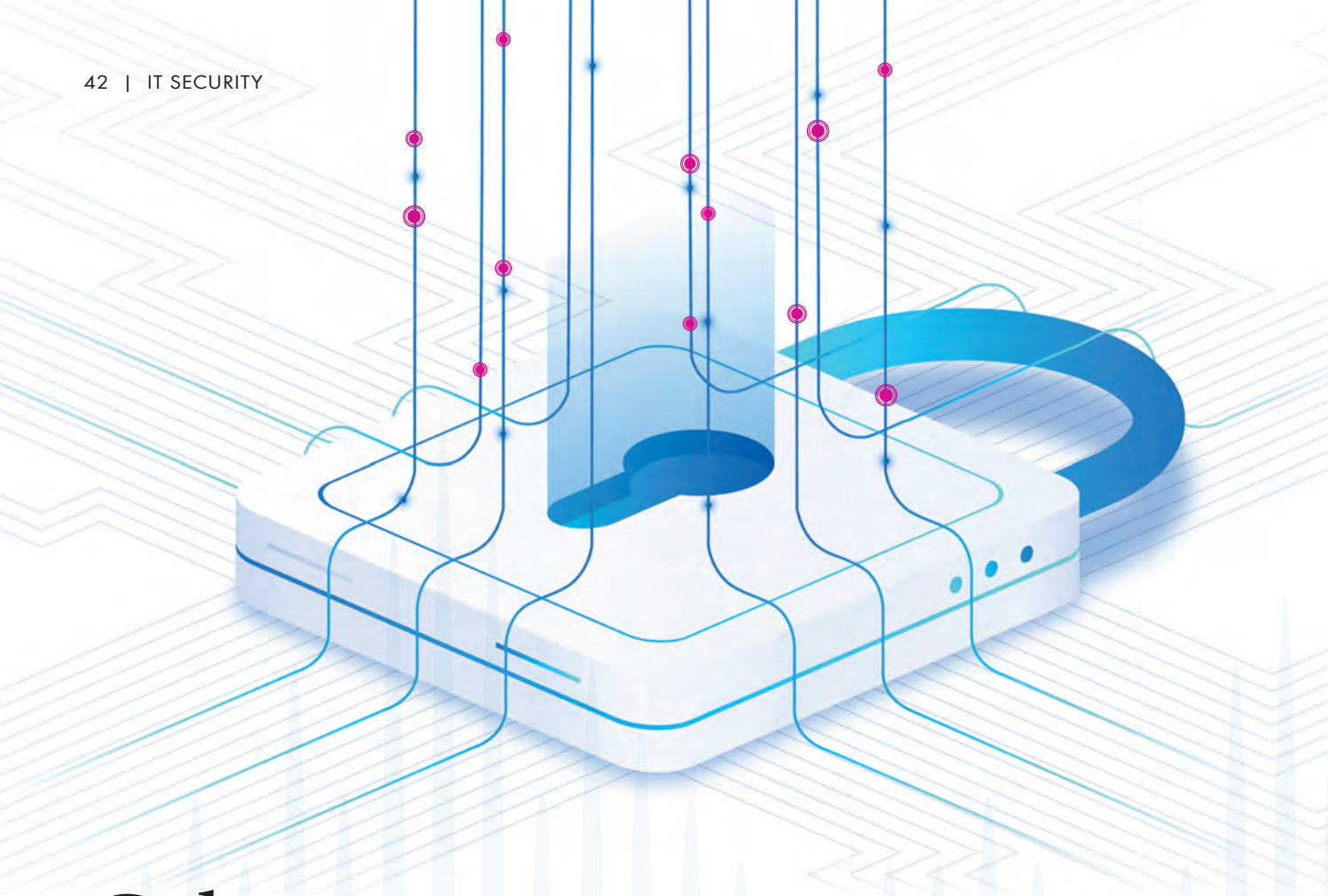
Wenn das KI-System jedoch nicht skalierbar ist, kann es Schwierigkeiten haben, mit der steigenden Anzahl von Anwendungen und Daten umzugehen. Dies könnte dazu führen, dass das KI-System nicht in der Lage ist, alle potenziellen Bedrohungen zu identifizieren oder dass es zu Fehlalarmen kommt, die unnötige Ressourcen verschwenden.



#6 Menschliches Know-how

Obwohl KI-Systeme automatisch arbeiten, ist menschliches Know-how immer noch entscheidend. IT-Sicherheitsfachleute müssen KI-Systeme konfigurieren, überwachen und warten, um sicherzustellen, dass sie effektiv, sicher und transparent sind.

Ulrich Parthier | www.it-daily.net



Cyberstorage

SCHUTZ VOR RANSOMWARE-ANGRIFFEN

Cyberstorage ist ein aktueller Begriff, der sich laut Marktforschern zu einer neuen Kategorie entwickelt und Unternehmen mehr Datensicherheit und damit auch mehr IT-Resilienz bieten soll.

Nach wie vor arbeiten viele Unternehmen IT-Sicherheitsvorfälle ab, statt sie proaktiv zu verhindern. Das neue Ziel heißt, Cyberangriffe künftig zu absorbieren. Calamu ist ein Beispiel für solch eine Lösung der neuen Generation, die Daten unhackbar machen soll, um Datendiebstahl und -exfiltration zu verhindern.

Calamu Protect, so der Produktname, fragmentiert die Daten im Ruhezustand automatisch auf mehrere separate Speicherorte, eine Umgebung, die als Datenhafen bezeichnet wird und die Auswirkungen einer Datenverletzung oder eines Ransomware-Angriffs sofort zunichte macht.

Heute gibt es bereits zahlreiche Möglichkeiten, Ransomwarevorfällen zu begegnen. Dazu zählen Immutable Speicher, physikalisch getrennte Backup-Systeme oder Ransomware-Module in EDR-Lösungen.

Wie funktioniert eine Bereinigungsfunktion?

Die sogenannte Ransomware-Bereinigungsfunktion sichert Dateien wie Dokumente, Bilder, Videos oder Musik, um sicherzustellen, dass sie im Falle einer Ransomware-Verschlüsselung nicht beschädigt werden oder verloren gehen. Jedes Mal, wenn ein Ransomware-Angriff erkannt wird, blockiert beispielsweise Bitdefenders EDR-Lösung alle Prozesse, die an dem Angriff beteiligt sind, und startet den Sanierungsprozess, wobei der Benutzer auch benachrichtigt wird. Auf diese Weise können Anwender den Inhalt ihrer gesamten Dateien wiederherstellen, ohne das geforderte Lösegeld bezahlen zu müssen.

Ransomware-Wiederherstellungsprobleme

Hat es Unternehmen in Sachen Ransomware trotz aller oder eben wegen keiner Sicherheitsmaßnahmen erwischt, können auch Snapshots helfen. Hier kann man die Fähigkeit der Hybrid-Cloud-Technologien nutzen, die Notfallwiederherstellung zu verbessern, indem die Software unbegrenzt viele Snapshots von Daten an verschiedenen

Standorten in der Cloud erstellt. Bis 2025 werden laut Gartner mindestens 75 Prozent der Unternehmen mit einem oder mehreren Ransomware-Angriffen konfrontiert sein. Natürlich gibt es auch hierzu passende Anbieter. Nasuni etwa bietet eine Snapshot-basierte Continuous File Versioning-Technologie und damit eine zusätzliche, neue Möglichkeit, Daten zu sichern und zu schützen.

Cyberstorage

Zurück zum Aspekt Innovationen und dem neuen Schlagwort Cyberstorage. Warum ist überhaupt eine neue Sicherheitskategorie notwendig? Nun, scheinbar nimmt der Bedarf an proaktivem Datenschutz gegen Diebstahl und Ransomware zu. Cyberstorage ist zwischen der Netzwerkinfrastruktur und dem Speichersystem angesiedelt und bietet Unternehmen die Möglichkeit einen Angriff zu absorbieren, so dass Ausfallzeiten möglichst vermieden werden.

Viele Unternehmen haben sich mittlerweile auf die Ransomware-Bedrohung eingestellt, indem sie ein Sicherungs- und Wiederherstellungsprogramm implementiert haben, das sich nach einem solchen Angriff wiederherstellen lässt. Die Cyber-Banditen wissen das, und haben deshalb ihr Arsenal um eine neue Waffe erweitert: die doppelte Erpressung.

Was ist anders, was ist neu?

Die Lösung von Calamu ermöglicht es Unternehmen, Daten zu fragmentieren und diese dann automatisch auf mehrere separate Speicherorte zu legen. Das bedeutet, dass es keine zentrale Ressource gibt, auf die ein Angreifer mit Ransomware abzielen kann.

Dieser Ansatz bietet technischen Entscheidungsträgern ein Tool, mit dem sie nicht nur traditionelle Ransomware-Angriffe, sondern auch Ransomware 2.0, doppelte und dreifache Erpressungsversuche mit Multicloud-Datenschutzfunktionen vereiteln können.

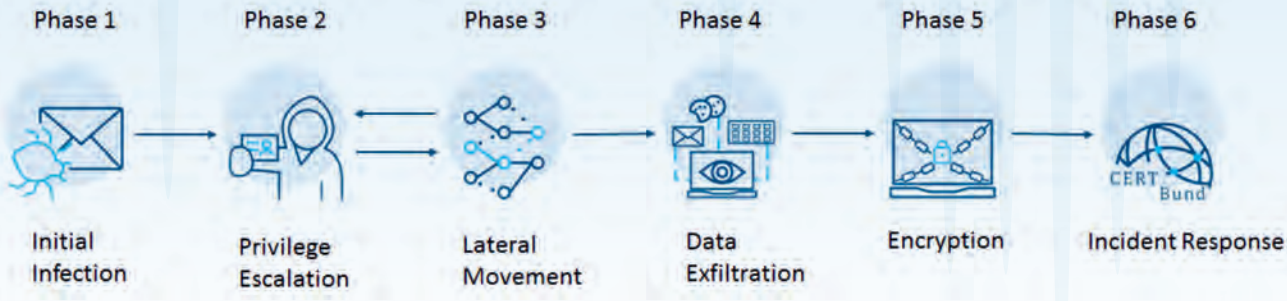
Das Unternehmen spricht in diesem Zusammenhang von einem virtuellen Datenhafen (Data Harbour). Die Daten im Datenhafen heilen nicht nur selbst, sie eliminieren auch das Risiko einer mehrfachen Erpressung, da alle exfiltrierten Daten von Natur aus unvollständig und für den Angreifer völlig nutzlos sind. Normalerweise wird bei einem Ransomware-Angriff mit doppelter Erpressung zunächst eine Kopie der Daten gestohlen oder exfiltriert, bevor sie verschlüsselt werden. Wenn das Lösegeld nicht gezahlt wird, droht der Angreifer damit, die Daten für die Öffentlichkeit zugänglich zu machen. Hier geht es um nicht mehr oder weniger als die Datenverteidigung, sagt Paul Lewis, CEO & Founder von Calamu.

Unternehmen sind aufgefordert sichere Lösungen zu finden, um die Daten über die Perimeterverteidigung hinaus zu schützen und sich darauf zu konzentrieren, was passiert, wenn der Schutzwall durchbrochen und auf die Daten zugegriffen wurde. Gibt es einen Weg, um sicherzustellen, dass die Daten geschützt bleiben, auch vor Angriffen?

Data-First-Cyberstorage-Strategie

Neue Anbieter im Bereich Cyberstorage sagen ja. Paul Lewis Meinung dazu: „Das Ziel einer echten Data-First-Cyberstorage-Lösung besteht nicht nur darin, die Auswirkungen eines Angriffs abzumildern, sondern den Angriff zu absorbieren, das Risiko der Datenexposition zu verringern und automatisierte Systeme einzusetzen, um die Ausfall-

RANSOMWARE KILLCHAIN



Die Ransomware Killchain. (Quelle BSI)

Der mehrstufige Calamu-Prozess.

sicherheit zu gewährleisten und Ausfallzeiten zu vermeiden. Wenn die Daten auch dann sicher bleiben, wenn auf die Speichermedien unberechtigterweise zugegriffen wird, hat das Unternehmen Zeit, den Einbruch zu versiegeln und forensische Untersuchungen durchzuführen, ohne dass sensible Daten sofort aus der kontrollierten Umgebung abgeschöpft werden."

Eine Cyberstorage-Schicht kann auch dazu beitragen, Backup-Daten sowie lokale Datenserver zu sichern, die schnell zum Ziel von Ransomware-Angriffen mit doppelter Erpressung werden. Jüngste Untersuchungen zeigen, dass 72 Prozent der Unternehmen im Jahr 2021 von Angriffen auf ihre Backup-Repositories betroffen waren. Darüber hinaus haben sich die Angriffe auf Cloud-Repositories im Vergleich zum Vorjahr verdoppelt, was viele IT-Teams dazu veranlasst hat, die Datenmigration in die Cloud zugunsten von On-Premises-Systemen zu stoppen. Aber auch Cyberkriminelle haben diesen Trend erkannt und wissen, dass der Zugriff auf On-Premises-Systeme eine Goldgrube darstellt. Angriffe auf On-Premises-Server wurden durch verschiedene kreative Maßnahmen gestartet, darunter CVE-Exploits, Backdoor-Schwachstellen und sogar elektromagnetische Signale, um Zugang zu Air-Gapped-Systemen zu erhalten.

Drei Säulen für mehr Widerstandsfähigkeit

Laut Gartner schützt Cyberstorage Speichersystemdaten vor Ransomware-Angriffen durch frühzeitige Erkennung und Blockierung von Angriffen, hilft bei der Wiederherstellung durch Analysen, und kann den Beginn eines Angriffs ermitteln. Bei der Evaluierung einer Cyberstorage-Verteidigungsschicht sollten Unternehmen daher folgende Punkte berücksichtigen:

- Integrierte, proaktive Technologie, die Anomalien erkennt und von sich aus in Aktion tritt, indem sie den Ort der Bedrohung automatisch unter Quarantäne stellt, eine Warnung ausgibt und die Aktivität für weitere Untersuchungen aufzeichnet
- Fähigkeit zur sofortigen Wiederherstellung und Fortsetzung eines Angriffs sowie zur Selbstheilung der angegriffenen Daten
- Sicherheitsvorkehrungen auf Datenebene, die die Daten vor Angriffen schützen, selbst wenn sie während eines Angriffs exfiltriert wurden

Bei einem Cyberangriff ist die Zeit immer von entscheidender Bedeutung. Cyberstorage-Lösungen, die leistungsstarke Sicherheitsanalysen und -intelligenz mit proaktiven Auslösern auf der Grundlage von Aktivitäten auf Datenebene integrieren, können die Zeit bis zum Handeln und letztlich bis zur Wiederherstellung verkürzen und somit die allgemeine Widerstandsfähigkeit des Unternehmens verbessern. Es wird geschätzt, dass die schnellste Ransomware ein System in weniger als 45 Minuten übernehmen kann. Darüber hinaus lauert der durchschnittliche Cyber-Angreifer nach dem Eindringen in ein Netzwerk 11 Tage lang unentdeckt, bevor er Ransomware einsetzt.

Unternehmen, die darauf warten, dass ihre IT-Teams auf verdächtige Aktivitäten reagieren, verlieren den Wettlauf mit der Zeit. Proaktive Erkennung bedeutet, den Angriff automatisch zu erkennen und zu stoppen, indem der Ort der Bedrohung unter Quarantäne gestellt wird. Es bedeutet auch, dass die Aktivitäten für weitere Untersuchungen aufgezeichnet und die Daten geschützt werden, auch wenn auf sie zugegriffen wird.

Cyberstorage-Bedeutung steigt exponentiell

Auch wenn die Methoden von Anbieter zu Anbieter variieren, ist das ultimative Ziel von Cyberstorage ein datenorientierter Sicherheitsansatz, der sich auf den Schutz der Daten selbst konzentriert und nicht auf die Medien, auf denen die 0en und 1en tatsächlich gespeichert sind. Diese Kategorie ist zwar noch jung, aber es gibt bereits vielversprechende Unternehmen, die dieses Problem durch innovative Technologien angehen.

Speichersysteme werden schnell in die Cloud verlagert und wachsen exponentiell in ihrer Größe, was einen unglaublichen Bedarf an dieser neuen Technologie schafft.

Während heute schätzungsweise nur 10 Prozent der Unternehmen einen integrierten Ransomware-Schutz für ihre Daten benötigen, erwartet Gartner, dass diese Zahl in den nächsten drei Jahren auf 60 Prozent ansteigen wird. Unternehmen brauchen heute kreative Lösungen, um ihre Daten zu schützen. Ein Sicherheitsansatz, bei dem die Daten im Vordergrund stehen, bietet genau das.Der neue Sicherheitsansatz konzentriert sich also auf den Schutz der Daten selbst, um Datenverletzungen, Datendiebstahlsversuchen und anderen Cyberangriffen standzuhalten und sie aufzufangen.

Der datenorientierte Sicherheitsansatz

Dieser Sicherheitsprozess der nächsten Generation sorgt dafür, dass die Daten für den täglichen Betrieb zugänglich bleiben, aber für unbefugte Benutzer wertlos werden und sich nach einer Verletzung selbst heilen, um die Widerstandsfähigkeit und Geschäftskontinuität zu gewährleisten.

Leistungssteigerungen werden durch horizontale Skalierung und parallele Verarbeitung erreicht. Selbst mit der fortschrittlichen Backend-Technologie, die die Next-Gen-Datensicherung ermöglicht, ist die Benutzererfahrung transparent und Änderungen der Latenz sind in der Regel nicht zu bemerken.

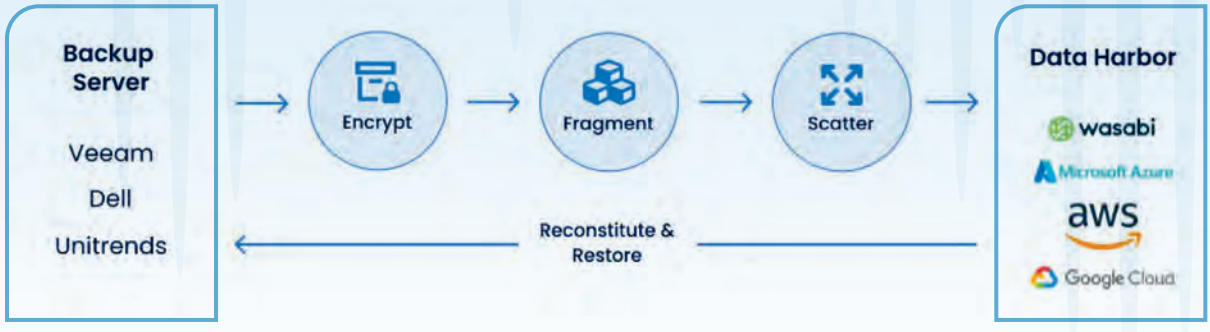
Fragmentierte Daten = null Angriffsvektor

Mit Calamu werden die Daten geschützt, indem die Dateien fragmentiert und so verteilt werden, dass nicht ein Speicherort über die zur Wiederherstellung einer Datei erforderlichen Daten verfügt und somit kein einziger Angriffsvektor vorhanden ist. Jedes der Fragmente ist mit einem anderen Schlüssel verschlüsselt, so dass es keinen einzigen Ausfallpunkt gibt, wenn ein Benutzer unerlaubten Zugang zu einem einzelnen Schlüssel erhält.

MIT CALAMU WERDEN DIE DATEN GESCHÜTZT, INDEM DIE DATEIEN FRAGMENTIERT UND SO VERTEILT WERDEN, DASS KEIN EINZIGER SPEICHERORT ÜBER DIE ZUR WIEDERHERSTELLUNG EINER DATEI ERFORDERLICHEN DATEN VERFÜGT UND SOMIT KEIN EINZIGER ANGRIFFSVEKTOR VORHANDEN IST.

Paul Lewis, CEO & Founder, Calamu Technologies, www.calamu.com

CYBERSTORAGE ORCHESTRATION



Ablauf der Cyberstorage-Orchestrierung bei Calamu.

Derzeit unterstützt Calamu Amazon Web Services (AWS), Microsoft 365, Microsoft Azure, Google Cloud Platform (GCP), Wasabi und On-Premises wie ein lokales Laufwerk oder ein Netzlaufwerk. Das Tool wird jedoch ständig um zusätzliche Funktionen erweitert. Die neueste Freigabe ermöglicht dem Anwender die Backup-Daten in einem gehärteten, manipulationssicheren Cloud-Repository zu sichern, so das Ransomware daran gehindert wird, Daten zu stehlen, und sie auch bei einem Cloud-Ausfall verfügbar hält! Die Lösung funktioniert mit den wichtigsten Backup-Lösungen und Cloud-Anbietern.

Und sonst?

Neben der Sicherheit wurde bei der Entwicklung von Calamu auch auf Skalierbarkeit und einfache Implementierung geachtet. So bietet die Lösung eine 100-prozentige API-Abdeckung und verfügt über Skripte, die die Bereitstellung einfach machen. Darüber hinaus werden Docker und Kubernetes für die containerisierte Bereitstellung unterstützt.

Die inhärente Methode, die Calamu Protect zum Schutz von Daten verwendet, vereinfacht die Einhaltung von Vorschriften und gesetzlichen Bestimmungen erheblich.

Calamu verfügt über mehrere eingebaute Redundanzen, um die volle Ausfallsicherheit zu gewährleisten, so dass die Daten immer nur für authentifizierte Benutzer verfügbar sind. Wenn ein Speicherort nicht mehr verfügbar ist, können Fragmente von anderen gesunden Speicherorten innerhalb des Datenhafens abgerufen werden, um die Datei wiederherzustellen, die sogenannte Selbstheilung. Das Tool repariert dann automatisch den „schlechten" Speicherort an einem neuen, gesunden Speicherort und stellt so die volle Ausfallsicherheit des Datenhafens wieder her.

Der Markt

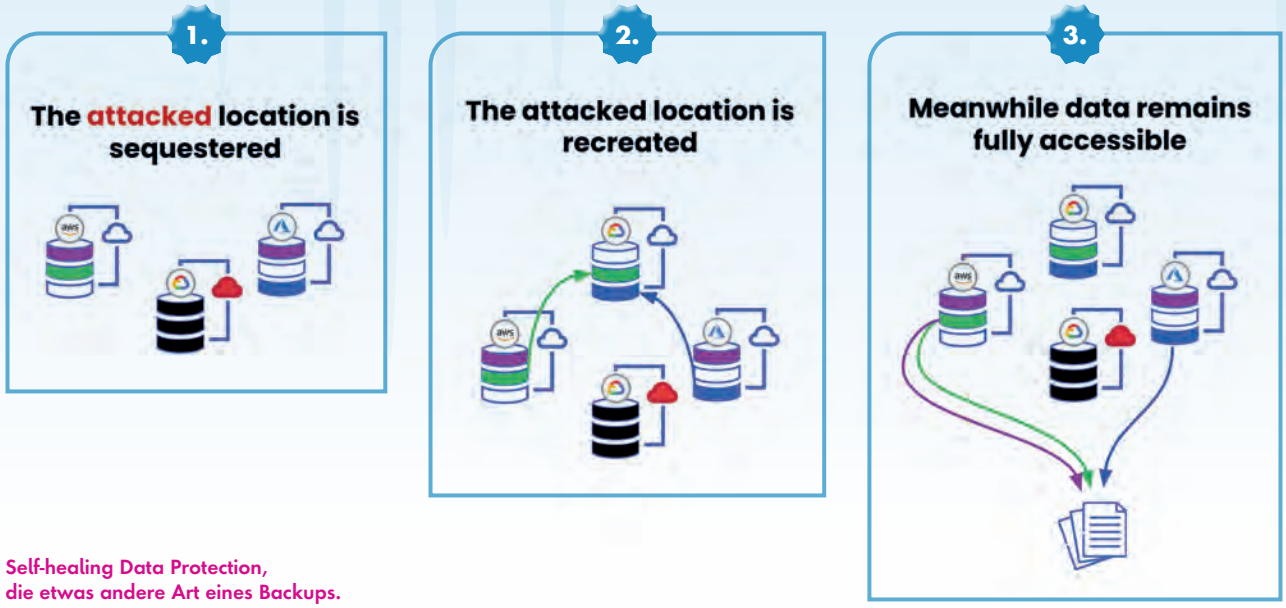
Calamu konkurriert mit mehreren Anbietern auf dem Markt, darunter Cloudian, das eine Ransomware-Protection-as-a-Service-Lösung anbietet. Es ermöglicht Unternehmen, Kopien ihrer Daten zu erstellen, die sie auf einen zweiten Cloudian-Standort oder eine Deep-Archive-Speicherlösung wie AWS Glacier replizieren können.

Ein weiterer Konkurrent ist Rubrik, der eine Ransomware-Schutzlösung anbietet, die Daten speichert, damit Ransomware-Akteure auf Backups zugreifen oder diese ändern können.

Calamu hingegen arbeitet mit dem Konzept der fragmentierten Daten in einer Multi-Cloud-Umgebung und unterschiedet sich damit schon konzeptionell von allen anderen Lösungen.

Ulrich Parthier | www.it-daily.net

DER SELBSTHEILUNGSPROZESS



Self-healing Data Protection, die etwas andere Art eines Backups.

SECURITY AWARENESS TRAININGS

UNWISSENHEIT SCHÜTZT NICHT VOR CYBERATTACKEN

Autofahren und IT-Sicherheit haben mehr gemeinsam, als es auf den ersten Blick scheint. In beiden Fällen schützen technologische Maßnahmen vor schweren Unfällen oder deren Folgen. Die Realität führt uns aber tagtäglich vor Augen, dass wir Menschen ebenfalls eine zentrale Rolle spielen, wenn es darum geht, Unfälle zu vermeiden. Ein vergessener Schulterblick, ein falsch eingeschätzter Abstand und schon kracht es. Richtiges Verhalten im Straßenverkehr lernen wir in der Regel in der Fahrschule, aber richtiges Verhalten im digitalen Raum?

Das vorliegende Whitepaper beschäftigt sich mit der Frage, welche Rolle Mitarbeitende beim Thema IT-Sicherheit spielen (Spoiler: eine sehr wichtige) und wie E-Learnings helfen, das Bewusstsein der Menschen für einen sicheren Umgang mit der IT zu verbessern.

WHITEPAPER DOWNLOAD

Das Whitepaper umfasst 11 Seiten und steht kostenlos zum Download bereit.
www.it-daily.net/Download

INHALT

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:
Uwe Gries, Clemens Güter, Raphael Kelbert, Carina Mitzschke, Silvia Parthier, Ulrich Parthier, Jannik Pewny, Dirk Reimers, Timo Sablowski, sMarkus Scharra, Michael Veit, Sebastian Weber

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.

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

We secure IT

11.05.23 | Digitalevent

SAVE THE DATE

SCAN ME

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

#WesecureIT2023