it management

Der Motor für Innovation
September/Oktober 2023

INKLUSIVE 80 SEITEN
it security

THOUGHT LEADERSHIP

AB SEITE 15
PAESSLER
THE MONITORING EXPERTS

AB SEITE 18
BLACKLINE

SAP: INNOVATIONEN & PARTNER

Eine Welt voller Möglichkeiten

Dr. Jens Amail, SNP

EAM: IT-KOSTEN EINSPAREN

Effizient die Applikationslandschaft analysieren

REIN IN DEN CONTAINER

Vorteile dieser Virtualisierungstechnologie

DriveLock
Sicherheit & Souveränität
ab Seite 38

Planisware
Projektmanagement
ab Seite 42

DIGITAL X 2023
Be digital. Stay human.
ab Seite 46


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

FLEXIBILITÄT IST ALLES

LIEBE LESERINNEN UND LESER,

In der heutigen Zeit ist nichts so konstant wie die Veränderung. Egal, welche Branche oder gesellschaftliche Ebene, alles unterliegt einem ständigen Wandel. Meiner Meinung nach ist eine Weiterentwicklung immer zu begrüßen, da sie im besten Fall von einer Entwicklung zum Positiven bestimmt wird. Aber manchmal ist Veränderung auch einfach nur kompliziert oder sogar unnötig.

Natürlich könnte man darüber diskutieren, ob wirklich jemals irgendetwas unnötig ist – denn aus Erfahrung lernt man und nachher ist man immer schlauer, aber darauf will ich gar nicht hinaus. Um mit Veränderungen adäquat umgehen zu können, muss man flexibel sein. Doch leider hakt es hier ganz schnell. Flexibel sein und tatsächlich flexibel agieren sind zweierlei Dinge: der Wille ist zwar da, aber beispielsweise die Mitarbeiter oder die Software ziehen nicht mit. Was dann? Kopf in den Sand? Wohl kaum!

Gerade in diesen Zeiten der digitalen Transformation sind Flexibilität und auch Anpassungsfähigkeit zu unverzichtbaren Eigenschaften geworden, um den ständig wachsenden Herausforderungen der Technologie und Sicherheit gerecht zu werden. Und wo könnte man sich dazu besser austauschen und informieren als auf dem diesjährigen DSAG-Jahreskongress und der it-sa? Zwei Veranstaltungen, die Vieles eint: Den Willen zum Wandel, die Innovationskraft und die Flexibilität, sich auf immer neue Ausgangssituationen einzulassen. Wie? Das lesen Sie in dieser Ausgabe im it management ab Seite 21 und im it security ab Seite 11.

Herzlichst

Carina Mitzschke | Redakteurin it management & it security

INHALT

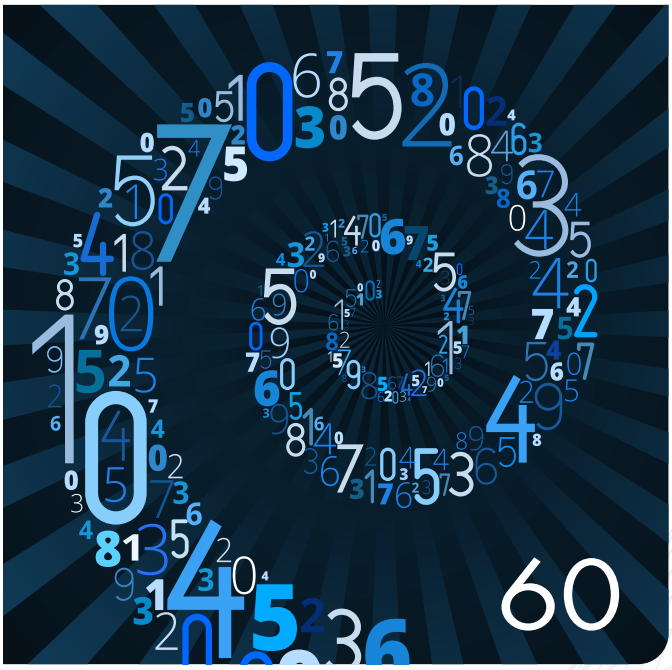
COVERSTORY

THOUGHT LEADERSHIP

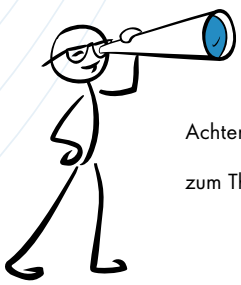
Farblich hervorgehobene Artikel sind von der Redaktion als besonders lesenswert empfohlen

SAP SPEZIAL

IT MANAGEMENT



Inklusive 80 Seiten it security



GUT ZU WISSEN

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

Keine Sicherheitsbedenken

75 PROZENT DER DEUTSCHEN UNTERNEHMEN VERTRAUEN CHATGPT

Wie bei vielen neuen Technologien stellt sich auch bei Generative AI und Large Language Model (LLM) wie ChatGPT die Frage: Sind sich Unternehmen ihrer potenziellen Risiken bewusst und wie gehen sie damit um? Gigamon wollte es genau wissen und hat im Rahmen einer aktuellen weltweiten Studie die CIO/CISOs aus 150 deutschen Unternehmen gefragt, wie sie die Sicherheit moderner Technologien einschätzen. Das Ergebnis: Drei Viertel der befragten Unternehmen (75 Prozent) haben keinerlei Sicherheitsbedenken, wenn ihre Mitarbeitenden ChatGPT nutzen. Lediglich fünf Prozent haben den KI-Chatbot aus ihrem Unternehmen verbannt und weitere 20 Prozent beschäftigen sich derzeit mit den Risiken.

Sicherheitsrisiken bekannt

Interessanterweise sind Unternehmen bei anderen Technologien weniger nachsichtig. Wenn es um das Metaverse und WhatsApp geht, sind sich CIO/CISOs jeweils zu 100 Prozent einig, dass (potenzielle) Sicherheitsrisiken vorliegen. So haben 67 Prozent von ihnen den Instant Messenger im Unternehmensumfeld verboten; das Metaverse stößt bei zwei Prozent auf Ablehnung. In beiden Fällen befasst sich der Rest zumindest mit möglichen Cyber-Risiken, um baldmöglichst eine Entscheidung hinsichtlich der Nutzung zu treffen. Das gleiche Schicksal ereilt auch TikTok: In zehn Prozent der Unternehmen ist die Kurzvideo-App tabu; 89 Prozent untersuchen das Risiko-Potenzial. Nur ein Prozent hat keine Bedenken und erlaubt TikTok im Unternehmen.

Das lässt darauf schließen, dass die Sicherheitsrisiken der genannten Plattformen weithin bekannt sind und die Mehrheit der Unternehmen sie auch ernstnimmt. Anders verhält es sich bei ChatGPT – und das, obwohl auch der KI-Chatbot keine unwesentliche Gefahr für Unternehmen darstellt. Betriebsinterna oder andere sensiblen Informationen, die Mitarbeitende mit ChatGPT teilen, können im Trainingsdatenpool landen und im Zuge eines Angriffes auf OpenAI gestohlen werden. Während des ChatGPT-Ausfalls im März 2023 sorgte sogar ein Bug dafür, dass Chat-Eingaben öffentlich einsehbar waren. Außerdem bestehen auch indirekte Risiken: Cyber-Kriminelle können das KI-Tool zum Beispiel dafür nutzen, um vertrauenswürdig wirkende Phishing-Mails zu verfassen, falsche Identitäten zu konstruieren oder Malware zu entwickeln.

Für den Ernstfall vorbereitet sein

Die Tatsache, dass sie für ChatGPT nichts herunterladen müssen, sorgt bei Nutzern für ein falsches Gefühl von Sicherheit. In der Regel soll die Belegschaft Ausschau nach verdächtigen E-Mails halten und keine unbekannten Dateien herunterladen oder seltsame Links anklicken. Doch mit dem KI-Chatbot lassen sich mittlerweile authentische Anwendungen, Webseiten und E-Mails schreiben, die betrügerische Machenschaften verbergen. Dadurch steigt das Risiko, dass Mitarbeitende einem Angriff aufsitzen. Deshalb müssen sich Unternehmen auf den Ernstfall vorbereiten, wenn sie nicht auf ChatGPT verzichten möchten.

www.gigamon.com

CYBERKRIMINALITÄT

FÜR EIN MEHR AN SICHERHEIT

Laut dem aktuellen „Cyberlagebild 2022" des Bundeskriminalamtes (BKA), fordern Unternehmen, das von Seiten der Polizei mehr gegen Cyberkriminalität unternommen wird. Konkret helfen würde den Unternehmen beispielsweise ein zentrales, leicht verfügbares und übersichtliches Cyberlagebild. Es gibt bereits Zentrale Ansprechstellen für Cybercrime, sogenannte ZAC, in den Landeskriminalämtern. Sie dienen grundsätzlich als Ansprechpartner zum Thema Cybercrime, dennoch könnte noch mehr getan werden. Doch dafür braucht es wiederum Know-how, Personal und technische Ausstattung. Eine Endlosschleife.

www.bitkom.org

UMFRAGEERGEBNISSE:

79% der Unternehmen sind der Meinung, die Polizei könne international agierende Cyberkriminelle nicht wirksam verfolgen

74% meinen, es fehlt der Polizei an Know-how rund um Cyberkriminalität

78% wollen, dass die Polizei verstärkt neue Technologien wie KI einsetzt

90% sind dafür, die Befugnisse der Polizei im Kampf gegen Cyberkriminelle auszuweiten

91% fordern, dass die Polizei im Kampf gegen Cyberkriminalität finanziell und personell besser ausgestattet wird

USU

Customer Service Automation

Revolutionieren Sie Ihren Kundenservice

Erfahren Sie in unserem Whitepaper, welchen Mehrwert Sie durch individuell anpassbare Standardlösungen erzielen können und welche Vorteile Ihnen Lösungen auf Basis von Low-Code bieten.

Jetzt scannen
und mehr erfahren

DEVICE AS A SERVICE

DAAS ALS MIETMODELL DER ZUKUNFT?

Modern Device Management (MDM/UEM) bezeichnet die automatisierte Bereitstellung von Software und Updates sowie die sichere Verwaltung der Bestandsgeräte eines Unternehmens. Device as a Service (DaaS) hingegen ergänzt diesen Ansatz: Denn DaaS ermöglicht es Unternehmen, ganze IT-Arbeitsplätze zu mieten. Pro Mitarbeitenden und pro Monat im Abo-Modell. Im Vergleich zu Modern Device Management kommt bei DaaS noch die Beschaffung und der Austauschprozess (SWAP) hinzu. Mit einer Einsparung von bis zu 40 Prozent der Aufwände rund um die Arbeitsplatzbereitstellung, löst DaaS aktuelle Herausforderungen wie Fachkräftemangel, fehlendes Technologie-Know-how oder Kostendruck auf einen Schlag.

Mit DaaS wandeln sich Investitionskosten in laufende Kosten und das bei maximaler Flexibilität in Sachen Skalierbarkeit und gleichzeitiger Planungssicherheit. Das erhält den Liquiditätsspielraum für andere Projekte und schafft gleichzeitig Kostentransparenz.

DaaS

Die Bedeutung von modernen Arbeitsplatz-Bereitstellungszenarien ist gestiegen und wird weiter steigen. So geht aus Studien wie der Fokus Point Medialine zu DaaS beispielsweise hervor, dass über 80 Prozent der befragten Unternehmen Homeoffice und hybrides Arbeiten realisieren. Zudem steigt die Relevanz smarter Software für die Zusammenarbeit und hochwertiger Hardware für sicheres, mobiles und performantes Arbeiten. Das führt zu einem hohen Druck auf die IT des Unternehmens. DaaS löst die Probleme mit fertigen Konzepten und durchdachten Services rund um die Arbeitsplatzbereitstellung.

Kaufen, Mieten oder Selbermachen?

Modern Device Management mit seinen Disziplinen Gerätebeschaffung, Installation, Verwaltung, Updates und Support sowie Gerätetausch unterliegt einer hohen Geschwindigkeit in Sachen Know-how und Verfügbarkeit. Unternehmen sind gefordert bei diesen rasanten Entwicklungen mitzuhalten. In Zeiten fehlender Ressourcen stellen IT-Partner mit DaaS und bewährten Konzepten nicht nur ein Kosteneinsparung dar, sondern eine Lösung für fehlende Fachkräfte.

Warum ist es das Modell der Zukunft?

Exogene Einflüsse wie Cyberangriffe und Arbeitsplatzmodelle erhöhen die Komplexität zusätzlich. DaaS von Adlon beispielsweise wurde nach dem „Security first"-Prinzip entwickelt und berücksichtigt die Managed Defender als Service. Beinhaltet sind hier Endgeräte-, Informations-, Identitäts- und Applikationsschutz nach neuestem Standard. Smarte Bereitstellungsprozesse für den IT-Arbeitsplatz überall, jederzeit und unabhängig vom Gerät ermöglichen Work-from-Everywhere. DaaS wirkt sich somit positiv auf die Arbeitsplatzattraktivität und das Unternehmensimage aus. Denn mit DaaS erwirbt das Unternehmen nicht nur den Arbeitsplatz im Abo, sondern ein Sorglos-Paket rund um Produktivität und Sicherheit des IT-Arbeitsplatzes.

www.adlon.de

Cloud Migration

SCHRITT FÜR SCHRITT ZUM ZIEL

Die fünf Finger einer Hand allein reichen für die Aufzählung der Argumente pro Cloud Computing nicht mehr aus: Die sind mit der höheren Flexibilität, Skalierbarkeit, Verfügbarkeit und Sicherheit, sowie den Kostenvorteilen von Cloud-Ressourcen bereits ausgereizt. Dazu kommen unter anderem die Cloud-immanenten Fähigkeiten zum Disaster Recovery und die Innovationsgeschwindigkeit, mit der Cloud-Anbieter ihre Plattformen weiterentwickeln. Aber mal so eben in die Cloud zu wechseln, funktioniert nur höchst selten. Die Cloud-Migration muss vielmehr sorgfältig geplant und umgesetzt werden, falls sie nicht zum Disaster werden soll. Couchbase skizziert die wichtigsten Schritte auf dem Weg in die Cloud:

#1 **Evaluation:** Cloud Computing beginnt nur bei einigen wenigen Start-ups auf der grünen Wiese. In der Regel wird es auf Bestandssysteme (Legacy) aufgesetzt, mit denen es in hybriden Strukturen kombiniert wird. Der erste Schritt evaluiert die bestehende IT-Infrastruktur und entscheidet, welche Applikationen und Workloads in die Cloud verlagert werden – und welche nicht.

#2 **Planung:** Der darauf aufbauende Migrationsplan definiert den Zeitablauf, das Budget und die notwendigen Ressourcen für die Cloud-Migration, wie beispielsweise Equipment, Personal oder die Kosten für begleitende Dienstleister.

#3 **Vorbereitung:** Vor dem Migrationsstart müssen die betreffenden Systeme, Applikationen und Daten Cloud-fit gemacht werden. Dazu zählen unter anderem eventuell notwendige Sicherheitsmaßnahmen, ein Performance Tuning sowie Data Backup und Recovery.

#4 **Migration:** Nun kann die eigentliche Migration von Systemen, Applikationen und Daten in die Cloud starten, begleitet von entsprechenden Performance- und Validierungstests.

#5 **Integration:** Da in der Regel nicht alle IT-Services in die Cloud migriert werden, müssen Cloud Services und die on-premises verbleibenden Legacy-Systeme miteinander in produktiven Einklang gebracht werden. Das betrifft vor allem das Data und Security Management.

#6 **Optimierung:** Cloud Services haben enormes Optimierungspotenzial, wenn sie ein Finetuning auf die jeweils spezifischen Anforderungen erfahren. Die wichtigsten Parameter dafür sind Performance, Skalierbarkeit und Kosteneffizienz.

#7 **Maintenance:** Wie die Altsysteme müssen auch die Cloud Systeme nach der Inbetriebnahme ständig gewartet werden. Ganz oben auf der Maintenance-Liste stehen dabei das Monitoring aller Services und das allfällige Updating von Systemen und Applikationen.

www.couchbase.com

noris network

Ihr Premium IT-Dienstleister für
maximale Sicherheit & Verfügbarkeit

- Zertifizierte Rechenzentren in Deutschland
- Umfassendes Portfolio von Colocation bis Cloud-Services
- Kompetente Unterstützung bei der Umsetzung Ihrer Sicherheitsauflagen durch unsere IT-Security-Experten
- Ausgefeilte SIEM-Systeme und eigenes SOC für die Bearbeitung und Dokumentation Ihrer Security-Events

itsa

10.–12. Oktober 2023
Messezentrum Nürnberg
Halle 7 | Stand 7-109

Jetzt informieren

Eine Welt voller Möglichkeiten

INNOVATIONEN, PARTNER UND NEUE MÄRKTE

Die Nachfrage nach SNP-Lösungen nimmt zu. Vor welchen Herausforderungen Unternehmen stehen und warum die selektive Datenmigration immer mehr an Bedeutung gewinnt, darüber sprach Dr. Jens Amail, CEO bei SNP Schneider-Neureither & Partner, mit Ulrich Parthier, Publisher it management.

Ulrich Parthier: *Herr Amail, seit Mitte Januar sind Sie neuer Chef der SNP und haben sich viel vorgenommen.*

Jens Amail: Es gibt auch viel zu tun. Wir arbeiten konzentriert an innovativen Lösungen, dem Ausbau unserer strategischen Partnerschaften und der Erschließung neuer Märkte. In einigen sind wir noch nicht vertreten: Brasilien, Mexico, und den Niederlanden zum Beispiel. Das soll sich ändern. Wir prüfen die strategischen Optionen und sind sehr optimistisch, was die Zukunft von SNP anbelangt. Wir sind uns aber auch der Herausforderungen bewusst. Es ist eine sehr spannende Zeit.

Ulrich Parthier: *Mit dem plötzlichen Tod des Firmengründers Andreas Schneider-Neureither vor fast drei Jahren war es auch eine unruhige Zeit.*

Jens Amail: Es ist nicht ungewöhnlich und sehr menschlich. Der plötzliche Verlust des Unternehmensgründers ist eine große Veränderung. Andreas hat nicht nur etwas Großartiges aufgebaut. Er hat mit seinen Visionen und innovativen Ideen SNP immer weiter vorangetrieben und war für seine Mitarbeiterinnen und Mitarbeiter auch das Herz der Firma. Mein Vorgänger, Michael Eberhardt, und das gesamte Team, haben das gut aufgefangen und ich konnte auf einer starken Basis aufbauen.

Ulrich Parthier: *Und auf einem starken Produktportfolio. Welche Bedeutung hat CrystalBridge für SNP?*

Jens Amail: Unser Kerngeschäft sind die selektive Datenmigration und das Datenmanagement. Die dafür zentrale Softwareplattform CrystalBridge ist die Basis für jede Art von Transformation. S/4HANA-Migration machen zwar einen Großteil unseres Umsatzes aus, im ersten Halbjahr 2023 übrigens erstmals über 50 Prozent des Auftragsvolumens. Die aktuelle makroökonomische Situation zwingt Unternehmen aber auch zu umfassenden Neustrukturierungen und digitalen Transformationen über S/4HANA hinaus. SNP hat schon vor mehr als zehn Jahren erkannt, dass es bei SAP-Datenmigrationen wiederkehrende Muster gibt, die bei verschiedenen Szenarien auftreten. Das war der Ausgangspunkt für die Idee, sämtliche Prozesse rund um die Migration in einer Software zu automatisieren. SAP nennt das Selective Data Transition. In diesem Markt haben wir als SAP-Partner mittlerweile einen weltweiten Marktanteil zwischen 70 und 80 Prozent.

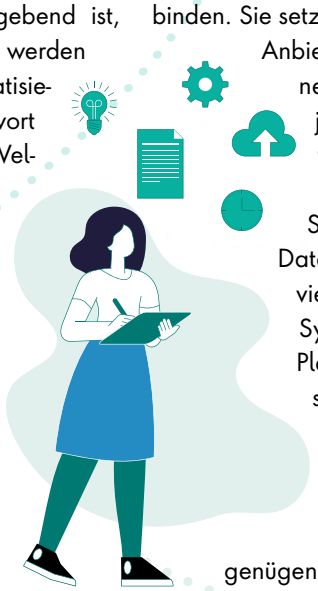
> WIR SEHEN UNS NICHT MEHR ALS REINEN SERVICE-ANBIETER, VIELMEHR ALS SOFTWAREUNTERNEHMEN.
>
> **Dr. Jens Amail, CEO, SNP Schneider-Neureither & Partner, www.snpgroup.com**

Ulrich Parthier: *Wie sehen Sie die Entwicklung von SNP in den kommenden Jahren?*

Jens Amail: Wir sehen uns nicht mehr als reinen Service-Anbieter, vielmehr als Softwareunternehmen. Unser Ziel ist es, den Umsatzanteil der eigenen Softwarelösungen in den nächsten Jahren auf über 50 Prozent zu steigern. Ein wichtiger Bestandteil in unserem Softwareportfolio ist die Data- Provisioning-Application GLUE. Als Teil der CrystalBridge ermöglicht sie die Bereitstellung von SAP-Daten in der Cloud und verbindet Datensilos. Im Herbst launchen wir eine neue Version, die diese Funktion auf Non-SAP-Daten erweitert. Mit GLUE stellen wir SAP-Daten für künstliche Intelligenz und andere kundenindividuelle Applikationen bereit. Die Strategie geht auf: Wir sind im zweiten Quartal erneut mit über 30 Prozent beim Auftragseingang gewachsen.

Ulrich Parthier: *Den Erfolg macht neben CrystalBridge auch der von SNP entwickelte Migrationsansatz BLUEFIELD aus. Das Verfahren hat sich neben den Ansätzen Brown- und Greenfield etabliert, wirft aber auch immer wieder Fragen auf.*

Jens Amail: Sie spielen auf die Frage an, ob wir nur Bluefield können. Es ist für uns unerheblich, welchem Ansatz die Migration folgt. Die Datenfrage stellt sich in allen Szenarien. Ausschlaggebend ist, welche Daten mitgenommen werden sollen und welcher Automatisierungsgrad sinnvoll ist. Stichwort selektive Datenmigration: Welche Daten muss ich migrieren, welche kann ich löschen, welche brauche ich aus Compliance-Gründen, welche möchte ich archivieren, welche müssen mir täglich in HANA operativ zur Verfügung stehen? Bei der automatisierten selektiven Datenmigration hat SNP einen klaren Wettbewerbsvorteil, weil BLUEFIELD hilft, präzise zu bestimmen, wie zu welchem Zeitpunkt mit den Daten zu verfahren ist. BLUEFIELD und CrystalBridge stellen mit Testmigrationen und Validierung eine auditierbare Migration sicher, was rund 15.000 erfolgreiche Projekte beweisen.



Ulrich Parthier: *Sie setzen auch auf ein starkes Partner-Ökosystem. Wie sieht Ihre Zusammenarbeit aus?*

Jens Amail: Partner sind ein Grundpfeiler. Wir arbeiten mit knapp 500 Partnern zusammen, darunter 16 der Top 20 SAP-Systemintegratoren weltweit. Unsere Allianzen gehen oftmals über reine Technologiepartnerschaften hinaus. Im Rahmen der Initiative „BLUEFIELD inside" sollen Partner und Kunden befähigt werden, Transformationsprojekte mit CrystalBridge selbständig umzusetzen. Denn eine der größten Herausforderungen bei Migrationsprojekten ist die personelle Verfügbarkeit. Zudem möchten sich Kunden womöglich nicht an einen Systemintegrator binden. Sie setzen auf SNP als Plattform-Anbieter und bilden ihre eigene IT-Abteilung für die Projektumsetzung auf CrystalBridge aus. Dank des starken Marktanteils von SNP im Segment Selective Data Transition sind bereits viele Beratungshäuser und Systemintegratoren auf der Plattform ausgebildet. Unser großes Partner-Ökosystem garantiert Kunden, dass sie auch auf CrystalBridge setzen können, wenn sie nicht genügend eigene Leute haben.

Ulrich Parthier: *Das Integrieren künstlicher Intelligenz ist mittlerweile schon fast Normalität. Wie binden Sie diese Entwicklung in Ihre Produkte ein?*

Jens Amail: Intern nutzen wir die Technologie, um unsere Prozesse effizienter zu machen und unsere Produkte zu verbessern, insbesondere im Bereich Analyse und Testing. Und als Experte für SAP-Daten im Besonderen und Datenqualität im Allgemeinen können wir Unternehmen bei der Nutzung von KI unterstützen. Schließlich hängt der Erfolg von KI stark von der Menge der zugrundeliegenden Daten und deren Güte ab. Davon ausgehend, dass die meisten Daten im Geschäftsbereich nach wie vor in SAP gespeichert sind, ergibt sich für SNP ein großes Potenzial. Die GLUE-Anwendung stellt SAP-Daten in bereinigter Form im Cloud-Data-Warehouse bereit und versetzt unsere Kunden in die Lage, eigene KI-Applikationen für ihre Ansprüche zu entwickeln. Wir haben jüngst eine Partnerschaft mit dem Data-Cloud-Anbieter Snowflake geschlossen und die native App „Data Streaming for SAP" mit dem Snowflake Native App Framework entwickelt. Sie soll die Datenlatenz bei der Integration von Streaming-Daten reduzieren. Und wir haben das „Innovation Lab AI & Cloud" gegründet, in dem wir wertvolles Know-how aus der eigenen Organisation in den Bereichen AI und Cloud bündeln und die Umsetzungsstärke erhöhen.

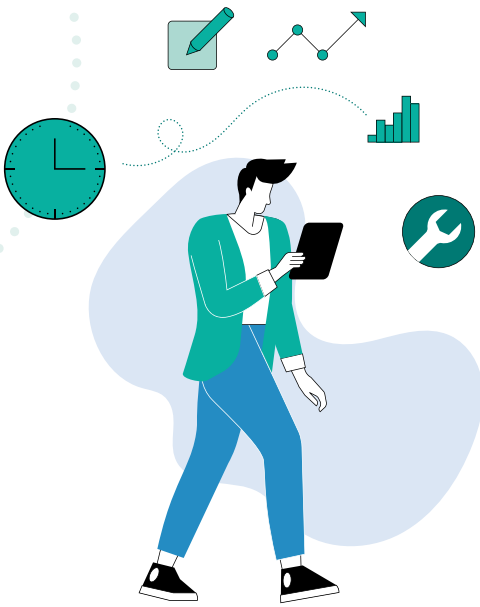
Ulrich Parthier: *Herr Amail, wir bedanken uns für das interessante Gespräch.*

Künstliche Intelligenz in modernen Softwareprodukten

WIE KI ZEITAUFWAND UND RISIKO ANSPRUCHSVOLLER TESTFÄLLE MINIMIERT

Die Bedeutung von Tests bei der Installation, Anpassung, Migration und Modernisierung von Unternehmenssoftware ist essenziell. Schließlich sind es die IT-Systeme, über die die wichtigsten Geschäftsprozesse abgewickelt werden, von der Finanzverwaltung über den Vertrieb bis hin zur Qualitätssicherung. Künstliche Intelligenz (KI) kann die Belastungen bei komplexen Datenmigrationsprojekten verringern, und den Grad der Testabdeckung erhöhen.

Die größte Herausforderung für Softwaretests ist sicherlich der Zeitfaktor. Mit zunehmender Systemkomplexität steigt die Zahl der erforderlichen Testfälle exponentiell an. Aktuelle Modelle gehen davon aus, dass ein kleines System, mit beispielsweise 50 Datenbanktabellen, einigen Eingabe- und Ausgabeformularen und wenigen Berichten, über 4.000 Testfälle erfordert. Wenn jeder Fall nur 10 Minuten benötigt, sind fast 6 Monate Testaufwand erforderlich. Bei der Größe moderner Unternehmenssysteme könnte eine vollständige Testabdeckung Jahrhunderte dauern! In modernen Softwareprojekten mit strengen Zeitplänen und chronischer Eskalation stehen nur wenige Tage oder Wochen zur Verfügung. Dass bei Terminverzug Tests als erstes gekürzt werden, verschärft das Problem. Auch die Erstellung von Testfällen, die Fehlerverwaltung und abschließende Dokumentation sind enorm aufwendig.



Innovative Antworten auf moderne Probleme

Künstliche Intelligenz verspricht, die Erstellung, Vorbereitung, Ausführung, Analyse, Fehlerverwaltung und Berichterstattung von Testfällen zu beschleunigen und die Testabdeckung zu erhöhen. Es gibt Testautomatisierungssoftware speziell für SAP ERP-Tests, die bei komplexen Datenmigrationen, wie die Einführung von SAP S/4HANA oder Cloudifizierung, erforderlich sind. Aktuell sehen wir eine explosionsartige Entwicklung von KI-Methoden und -Modellen, die den gesamten Testprozess noch umfassender abdecken können, was Projekte erheblich beschleunigt und gleichzeitig Risiken verringert.

Der feine Unterschied

Nur ein vollständiger Satz von Testfällen garantiert eine gute Testabdeckung. Man kann Tausende von Testfällen haben und trotzdem keine gute Abdeckung, weil die Anwendung nicht in den richtigen Bereichen getestet wird. Erstellt man SAP ERP-bezogene Migrationsinhalte, können mit dem gewonnenen Wissen Testfälle für die gesamte SAP-Datenbank generiert werden. Durch die Erweiterung der Testfallgenerierung von rein statischen Techniken und das Einbeziehen von Analyse und Clustering historischer Daten, können zusätzliche Testfälle gewonnen werden. Anhand der bekannten Technik „K-Means-Clustering" kann nicht nur bestimmt werden, welche Geschäftsfunktionen ausgeführt werden müssen, sondern auch, welche relevanten Gruppierungen von Eingabedaten erforderlich sind, um die in der Praxis vorkommenden Datenvalidierungsszenarien richtig abzudecken.

Die Geschäftslogik einer Anwendung spiegelt sich in den Daten wider, die sie speichert und verwaltet. Kombinationen, die von der Geschäftslogik nicht zugelassen werden, sollten in den Daten nicht vorkommen. Bei der Migration dieser Daten in eine ähnliche oder andere Unternehmenssoftware oder ein Cloud-basiertes Berichtsrepository, müssen diese Beziehungen beibehalten und überprüft werden. Sie zu entdecken ist keine leichte Aufgabe. Hier ist Innovation gefragt und Algorithmen des maschinellen Lernens. Sie erkennen die Beziehungen, erstellen die Testfälle und garantieren, dass sie

> DIE GESCHÄFTSLOGIK EINER ANWENDUNG SPIEGELT SICH IN DEN DATEN WIDER, DIE SIE SPEICHERT UND VERWALTET.
>
> **Dr. Steele G. Arbeeny, Chief Technology Officer, SNP Schneider-Neureither & Partner, www.snpgroup.com**

durchgesetzt werden. Daten werden mit voller Integrität migriert und alle vor der Migration durchgeführten Geschäftstransaktionen funktionieren weiter wie zuvor.

Ein Testfall für Spezialisten

Meist fehlt Zeit. Spezialisten setzen daher auch auf risikobasierte Tests. Dabei wird ermittelt, welche Bereiche der Anwendung sich am stärksten verändert haben und mehr Zeit benötigen. Die stark voneinander abhängigen ERP-Daten sind eine zusätzliche Erschwernis. Zum Beispiel Bestandsdaten: Es gibt viele Prozesse, die sich auf den Bestand auswirken können - einige offensichtlich, andere nicht. Der Einfluss von Kundenaufträgen ist offensichtlich, der der Anlagenverwaltung weniger. Anbieter, die KI einbinden, arbeiten an Algorithmen für die Hauptkomponentenanalyse (PCA) und die blinde Quellentrennung (BSS, Blind Source Separation), um festzustellen, welche entfernten Funktionen sich auf einen bestimmten Datensatz auswirken. Die Verwendung von PCA und die Ermittlung der unbekannten Anwendungsprozesse verbessert die Testabdeckung erheblich. Insbesondere, weil einige dieser entfernten Beziehungen mehrere andere Prozesse durchlaufen können, bevor die Auswirkungen spürbar werden.

Für die zeitaufwendige Sichtung, Klassifizierung und Zuordnung von Fehlern gibt es maschinelle Lernmodelle, die von der menschlichen Fehlerklassifizierung lernen. Während Menschen Defekte bearbeiten, erkennen Algorithmen Ähnlichkeiten und gruppieren gleichwertige Defekte, die eine gemeinsame Lösung haben. Auf diese Weise wird eine der zeitaufwändigsten und repetitivsten Aufgaben reduziert.

Alles auf KI?

Unternehmen haben viel in die Entwicklung von Testplänen und Testfalldokumenten investiert. Muss mit KI nun alles über Bord geworfen werden? Ich glaube nicht. Mithilfe von Natural Language Processing (NLP) und Named Entity Recognition (NER) können diese Dokumente verarbeitet und Testfälle in eine Testautomatisierungsplattform eingebunden werden.

Häufig verfügen die getesteten Systeme nicht über genügend Daten mit ausreichender Vielfalt, um eine angemessene Testabdeckung zu gewährleisten. Hier helfen generative adversarische Netzwerke (GAN) - die Technologie, die für Deep Fakes verwendet wird - um Testdaten zu synthetisieren. Ziel ist eine Ausgabe, die so genau ist, dass sie ein Unterscheidungsnetzwerk täuschen kann und sie für echt hält. SNP verwendet diesen Ansatz für die Generierung von Testdaten. Das hat den zusätzlichen Vorteil, dass Daten generiert werden, die die Geschäftsregeln einhalten und den Nutzungsmustern in den echten Daten des Kunden entsprechen. Die realitätsnahen Testdaten können auch zum Trainieren neuer KI-Modelle und Testen bestehender Modelle verwendet werden. Und schließlich wird kein geschäftskritischer Testprozess von der Geschäftsleitung oder von Prüfern akzeptiert, wenn er nicht detailliert dokumentiert ist. Mithilfe speziell trainierter großer Sprachmodelle (LLMs) werden abschließende Testberichte erstellt. Zusammenfassende Berichte sind sofort nach Abschluss der Tests verfügbar - und ihre Genauigkeit ist garantiert, da sie auf den Testergebnissen basieren und nicht erfordern, dass ein Mensch alle Ergebnisse erfasst, was fehleranfällig ist.

Es gibt noch Vieles, was KI beschleunigen kann, etwa Leistungs- und Sicherheitstests und die automatische Aktualisierung bei Datenänderungen. Da Testen derzeit so arbeitsintensiv und oft vernachlässigt ist, werden sicher noch viele andere Bereiche mit Verbesserungspotenzial entdeckt, die zu Innovationen führen.

Dr. Steele G. Arbeeny

DIE IDEALE LÖSUNG?

Die digitale Transformation hat in den letzten Jahren eine tiefgreifende Veränderung in der Art und Weise bewirkt, wie Unternehmen ihre Geschäftsprozesse gestalten, ihre Ressourcen verwalten und mit Kunden interagieren.

Doch was sind die entscheidenden Faktoren, die Unternehmen tatsächlich voranbringen?

Zuverlässige Systeme, mehr Sicherheit, die enge Kooperation von CFO und CIO, moderne Technologien, um agiler, effizienter und innovativer zu sein? Gerade in Finanzorganisationen, in denen viele Prozesse noch manuell bearbeitet werden, gibt es keine Toleranz für Fehleranfälligkeit und langsames Arbeiten. Eine funktionierende IT ist somit eine Grundvoraussetzung um Verfügbarkeit und Performance sicherstellen zu können, aber noch lange nicht die Garantie für eine erfolgreiche digitale Transformation.

Weniger Monitoring für mehr Überblick

ZUVERLÄSSIGERE SYSTEME UND MEHR SICHERHEIT

Was muss IT-Monitoring heute leisten, was sind die großen Herausforderungen und wie sieht die ideale Lösung aus? Martin Körber und sein Team aus internationalen Monitoring-Spezialisten beraten tagtäglich Unternehmen in ganz Europa und darüber hinaus in Sachen IT-Monitoring.

it management: *Laut einer Studie von Gartner verwenden Unternehmen im Durchschnitt 12 verschiedene Monitoring-Tools, um ihre IT zu überwachen. 17 Prozent der von Gartner untersuchten Unternehmen setzen gar 24 oder mehr Tools ein. Kannst Du das bestätigen, Martin?*

Martin Körber: Wir führen keine Listen über die Zahl der eingesetzten Monitoring-Tools bei unseren Kunden, aber ja, die Zahlen dürften durchaus realistisch sein. Je größer der Kunde beziehungsweise je größer und komplexer die IT-Landschaft des Kunden ist, desto mehr Tools sind normalerweise im Einsatz.

it management: *Warum ist das so?*

Martin Körber: Eine funktionierende IT ist eine Grundvoraussetzung für jedes Unternehmen. Um Verfügbarkeit und Performance der IT sicherzustellen, müssen alle Bereiche ständig überwacht werden. Das beinhaltet heute eine enorme Vielzahl unterschiedlichster Aspekte und Komponenten. Aus der Sicht von IT-Operations (ITOps) ist da zunächst die Infrastruktur mit der ganzen Hardware, den Servern, Storage-Systemen, Datenbanken und so weiter. Dann das Netzwerk. Switche, Router, Firewalls und natürlich der Traffic, der über das Netzwerk fließt. Applikationen sind zwar vor allem in größeren Unternehmen in der Regel nicht im Verantwortungsbereich von ITOps, greifen aber auf Infrastruktur und Netzwerk zu. So gut wie alle unsere Kunden setzen heute auf hybride IT-Landschaften, sprich es gibt Strukturen vor Ort, im eigenen Rechenzentrum und in der Cloud, sowohl „private" als auch „public", die ebenfalls überwacht werden müssen. Neben der klassischen IT gibt es aber auch zahlreiche Grenzbereiche, die oft ganz oder zumindest in Teilen in die Verantwortung von ITOps fallen – vor allem bei mittelständischen Unternehmen sehen wir das immer häufiger. Das kann beispielsweise das Umgebungs-Monitoring im Rechenzentrum oder im Serverraum sein, Sicherheitskameras und Türschließsysteme im Bürogebäude oder in der Fertigung oder

ITOps benötigt einen möglichst umfassenden Überblick über alle Aspekte und Komponenten der Unternehmens-IT.

auch die Fertigung selbst. All das muss rund um die Uhr überwacht werden, um bei Störungen oder Ausfällen umgehend eingreifen zu können. Diese Vielschichtigkeit der zu überwachenden Systeme erfordert eben oft auch eine entsprechende Zahl an Monitoring-Tools.

it management: *Was sind das für Monitoring-Tools, die da zum Einsatz kommen?*

EINE FUNKTIONIERENDE IT IST EINE GRUNDVORAUSSETZUNG FÜR JEDES UNTERNEHMEN. UM VERFÜGBARKEIT UND PERFORMANCE DER IT SICHERZUSTELLEN, MÜSSEN ALLE BEREICHE STÄNDIG ÜBERWACHT WERDEN.

Martin Körber, Team Manager Technical Presales EMEA, Paessler, www.paessler.de

Martin Körber: Zunächst einmal sind da klassische Monitoring-Tools für ITOps, die einen Überblick über die Infrastruktur oder über das Netzwerk bieten, manche können auch beides. Andere Lösungen liefern tiefe Einblicke für Spezialisten in das Verhalten von Traffic im Netzwerk, monitoren Storage-Systeme bis ins kleinste Detail oder scannen Applikationen bis auf Source-Code-Ebene. Cloud-Provider liefern als Teil ihres Angebots auch Monitoring-Funktionen um ihre Dienste zu überwachen. So gut wie jedes dieser Tools hat seine Berechtigung und liefert wichtige Informationen für die jeweils zuständigen Experten. Daneben gibt es Lösungen für Randbereiche der IT: SCADA-Systeme überwachen und managen Produktionsumgebungen, DCIM-Tools verwalten Rechenzentren, Kommunikationsserver sorgen für einen funktionierenden Datenaustausch in Krankenhaus-Infrastrukturen. Diese Bereiche sind zwar oft nicht in der direkten Verantwortung von ITOps, beeinflussen aber deren Arbeit stark, da sie das reibungslose Funktionieren der IT voraussetzen. Sie transportieren Daten über das Netzwerk, nutzen Storage-Systeme und kommunizieren, benachrichtigen und alarmieren über das Netzwerk.

Ein ganz banaler Grund für die Tatsache, dass es in vielen Unternehmen mehr Monitoring-Tools als vielleicht eigentlich benötigt gibt, ist, dass IT-Umgebungen normalerweise nicht an einem Stück geplant und umgesetzt werden, sondern über viele Jahre und Jahrzehnte wachsen und sich ständig ändern und anpassen. Mit neuen Systemen kommen auch neue Monitoring-Lösungen dazu. Das führt aber nicht unbedingt auch zur Ablösung der bereits genutzten Monitoring-Tools, da diese noch für alte Systeme benötigt werden.

it management: *Was sind die Folgen dieses Wildwuchses an Monitoring-Tools?*

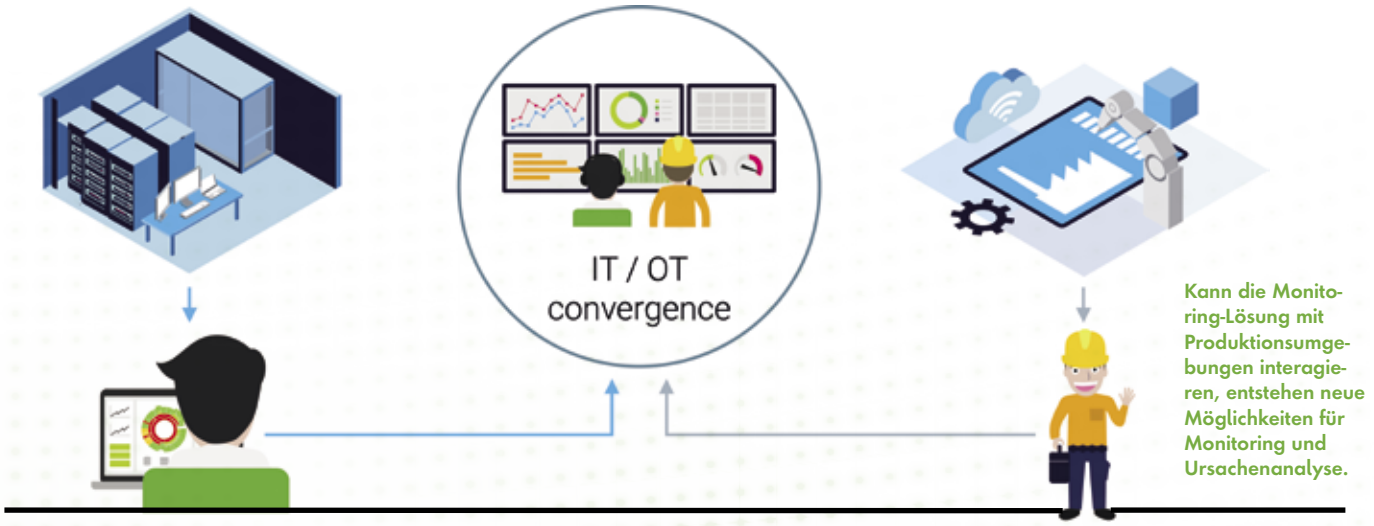
Martin Körber: Meistens sind all diese Monitoring-Tools voneinander isoliert. Störungen werden zwar erkannt und gemeldet, die Behebung ist aber häufig nicht so einfach, speziell wenn mehrere Systeme involviert sind. Das erschwert die Ursachenfindung massiv und macht es schwierig in Hinblick auf vorbeugende Maßnahmen, die solche Störungen in Zukunft vermeiden könnten. Die Tools für Spezialisten liefern meist sehr fundierte Informationen für ihr Spezialgebiet, sind aber komplex in der Bedienung und auch weniger auf eine umfassende und zeitnahe Alarmierung ausgelegt als vielmehr auf längerfristige Analysen. Im Gegensatz dazu sind die Infrastruktur- und Netzwerk-Monitoring-Lösungen für ITOps auf einen umfassenden Überblick ausgelegt. Das Hauptaugenmerk liegt auf dem Erkennen von Störungen und dem umgehenden Alarmieren der Verantwortlichen – möglichst in Echtzeit.

Natürlich verursachen mehr Lösungen auch höhere Kosten. Sowohl was Lizenzen und Wartung angeht als auch was den Aufwand für die Pflege der Systeme betrifft. Dabei darf man den Schulungsaufwand nicht vergessen: Viele Monitoring-Tools verlangen einiges an Fachwissen für Einrichtung, Wartung und Bedienung. Je mehr verschiedene Tools im Einsatz sind, desto mehr Personal wird benötigt bzw. umso größer ist die Belastung für das zuständige Personal.

Auch Sicherheitsaspekte spielen eine Rolle: Monitoring bildet immer auch einen wichtigen Baustein in einem durchgängigen Sicherheitskonzept. Zum einen überwacht Monitoring klassische Sicherheitstools wie Backup-Systeme, Firewalls oder Virenscanner und stellt so deren Funktion sicher, zum anderen kann Monitoring, wenn es richtig eingesetzt wird, auch einen aktiven Beitrag zur Sicherheit leisten, indem es ungewöhnliches Verhalten im Netzwerk aufdeckt, was auf Malware oder Hacker-Aktivitäten hindeuten kann. Ist das Monitoring auf zu viele Systeme und Verantwortliche verteilt, wird es schwierig, Zusammenhänge zu entdecken. Auch wird das Monitoring selbst dadurch kompliziert und anspruchsvoll. Das wiederum hat zur Folge, dass es unter Umständen wenig gewartet und genutzt wird. Der Effekt ist ein trügerisches Gefühl von Sicherheit – man hat ja zahlreiche Monitoring-Tools – während tatsächlich viele Systeme aufgrund mangelnder Wartung der Monitoring-Tools nur unzureichend überwacht werden.

it management: *Gibt es eine Lösung, die das gesamte Monitoring übernehmen kann?*

Martin Körber: Das hängt natürlich stark von den jeweiligen Anforderungen ab. In der Regel und vor allem ab einer bestimmten Größe und Komplexität der



Kann die Monitoring-Lösung mit Produktionsumgebungen interagieren, entstehen neue Möglichkeiten für Monitoring und Ursachenanalyse.

IT-Landschaft braucht es aber definitiv mehrere Tools. Zu viel Funktionalität in einer Lösung macht das Monitoring komplex und schwer bedienbar. Die Folgen davon habe ich ja gerade angesprochen. Auch haben bei größeren Umgebungen unterschiedliche Teams ganz unterschiedliche Anforderungen an das Monitoring. Vor allem für ITOps ist es aber wichtig, eine zentrale Monitoring-Lösung zu haben, die ihnen einen Überblick über alle relevanten Systeme liefert und die im Störungsfall möglichst zeitnah die zuständigen Techniker informiert. Im Idealfall kann eine solche Lösung dann vielleicht auch das eine oder andere redundante Monitoring-Tool ablösen und so die Gesamtzahl der Monitoring-Tools im Unternehmen senken.

it management: *Wie sähe eine solche Lösung aus?*

Martin Körber: Zunächst einmal muss diese Lösung sehr breit angelegt sein. Je mehr Systeme in die zentrale Überwachung eingebunden werden können, desto besser. Die Lösung muss das Monitoring der kompletten Infrastruktur inklusive der Cloud-Umgebungen und der virtuellen Systeme ermöglichen. Das Einbinden von Netzwerkgeräten wie Switchen, Routern und Firewalls sollte ebenfalls gewährleistet sein. Dazu kommen Basis-Features zum Überwachen des Traffics. Ist das alles sichergestellt, haben wir die Pflicht schon mal bestanden. Die Kür bilden dann Features, die das Einbinden von digitalisierten Umgebungen wie Gebäudetechnik, Produktionsumgebungen oder medizinischen Infrastrukturen ermöglichen. Das erfordert auf der einen Seite die Unterstützung der relevanten Protokolle wie DICOM oder HL7 im Krankenhausumfeld oder Modbus, MQTT oder OPC UA im IoT- oder IIoT-Bereich. Auf der anderen Seite muss die Lösung entsprechende Schnittstellen bieten, um mit existierenden SCADA-, DCIM- oder sonstigen Kommunikationssystemen interagieren zu können. Über solche Schnittstellen lassen sich auch andere IT-Monitoring-Tools wie die bereits erwähnten Spezialisten-Tools integrieren. So kann direkt nach der ersten Alarmierung mit der erweiterten Ursachenermittlung begonnen werden.

Das Thema Alarmierung spielt bei einer solchen Lösung eine zentrale Rolle. So muss sichergestellt sein, dass alle relevanten Kanäle unterstützt werden, ganz klassisch von der E-Mail-Benachrichtigung über das Nutzen eines SMS-Gateways bis hin zum Versenden von Syslog-Nachrichten oder Push-Benachrichtigungen auf Mobilgeräte. Im Idealfall kann das Tool vordefinierte Skripte auslösen oder Geräte booten. So können mit einfachen Mitteln Störungen automatisiert in Echtzeit behoben werden. Fast genauso wichtig ist die Darstellung der Monitoring-Ergebnisse in entsprechenden Übersichten. Die müssen schnell und unkompliziert individualisierbar sein, so dass jedem Kollegen genau die für ihn relevanten Daten übersichtlich angezeigt werden können. Dazu gehört auch, dass es nicht nur ein Web-Interface oder ein Windows-GUI gibt, sondern dass beides angeboten wird und im Idealfall zusätzlich noch Mobile-Apps verfügbar sind. Das entlastet Bereitschaftsdienste und schafft Flexibilität.

it management: *Gibt es aus deiner Sicht die eine entscheidende Anforderung an das ideale Monitoring-Tool?*

Martin Körber: Die Lösung muss so einfach wie irgend möglich in der Bedienung sein. Nur so ist gewährleistet, dass sie auch wirklich genutzt wird. Wenn die Bedienung keine wochenlangen Schulungen erfordert, sondern lediglich Fachkompetenz für die überwachten Systeme, kann die Verantwortung für das Monitoring und letztlich auch die Arbeitslast auf mehr Mitarbeiter verteilt werden. Das entlastet Administratoren, ITOps und Helpdesk-Teams und schafft zuverlässigere Systeme und mehr Sicherheit.

it management: *Martin, danke für das Gespräch.*

Digitale Transformation in der Finanzabteilung

DIE ENGE KOOPERATION VON CFO UND CIO IST ENTSCHEIDEND

Die Digitalisierung wird in allen Geschäftsbereichen und in den meisten Branchen massiv vorangetrieben. Dies gilt insbesondere für die Finanzabteilung, in der traditionell viele Prozesse noch manuell bearbeitet werden. Auch im Ausblick „Finance 2025: Digital Transformation in Finance" prognostiziert Deloitte, dass sich das Finanzwesen stark auf die Automatisierung von Prozessen konzentrieren wird. Interessanterweise warnt Deloitte gleichzeitig davor, dass trotz dieser Bemühungen der Erfolg nicht automatisch gesichert ist.

Ulrich Parthier, Herausgeber von IT-Management, spricht mit Ralph Weiss, Geo VP DACH bei BlackLine, darüber, wie CIOs und CFOs die Chancen für eine erfolgreiche digitale Transformation verbessern können.

Ulrich Parthier: *Herr Weiss, lassen Sie uns ganz am Anfang beginnen. Was sind Ihrer Meinung nach die Hauptziele der digitalen Transformation im Finanzwesen eines Unternehmens?*

Ralph Weiss: Das Hauptziel jeglicher digitalen Transformation ist es, das transaktionale Geschäft zu bündeln und hochgradig zu automatisieren. Es gilt Kapazitäten freizusetzen, um das Thema Analysen und Forecasting noch mehr in den Fokus nehmen zu können. Die Transformation der Finanzorganisation ist besonders dringlich, da es in dieser Abteilung bis heute viel manuelle Arbeit gibt und die Regeln und Gesetze keine Toleranz für fehleranfälliges und langsames Arbeiten zulassen. Dank einer hochgradigen

> DIE TRANSFORMATION DER FINANZORGANISATION IST BESONDERS DRINGLICH, DA ES IN DIESER ABTEILUNG BIS HEUTE VIEL MANUELLE ARBEIT GIBT UND DIE REGELN UND GESETZE KEINE TOLERANZ FÜR FEHLERANFÄLLIGES UND LANGSAMES ARBEITEN ZULASSEN.
>
> **Ralph Weiss, Geo VP DACH, www.blackline.com/de**

Automatisierung und verbesserten Effizienz können sich die Finanzfachleute auf wichtigere strategische Aufgaben konzentrieren, bessere Entscheidungsvorlagen liefern und neue Chancen ermöglichen – kombiniert mit gleichzeitiger Verbesserung der Governance.

Ulrich Parthier: *Wer sollte an der Festlegung der Parameter für eine erfolgreiche Transformationsinitiative beteiligt sein und warum?*

Ralph Weiss: Wir sehen, dass eine Transformation dann besonders gut funktioniert, wenn IT und Finanzbereich am gleichen Strang ziehen, um gemeinsam das Bestmögliche erreichen. Häufig ist der Anlass der Umstieg auf ein neues ERP-System. Es gibt den Lift und Shift-Ansatz und die Transformation im Zuge eines neuen ERPs. Ersteres wird in der Regel durch die IT getrieben. Die Transformation benötigt jedoch den Impuls des CFO. CFOs und deren Mitarbeiter sind von zentraler Bedeutung, wenn es darum geht, Prozesse neu zu gestalten, neue Geschäftsfelder oder neuartige Business Modelle zu entwickeln. Dies gelingt allerdings nicht ohne die Unterstützung des Chief Information Officers (CIOs) und dessen Führungskreis, die die Transformation aus IT-Governance- und Architekturgesichtspunkten unter die Lupe nimmt. Während Finanzleute genau wissen, wie sie ihre Prozesse neugestalten und verschlanken wollen, sind es die CIOs, die die technische Machbarkeit verstehen und genau wissen, wie die Daten in ein neues System transformiert werden müssen. Der CIO ist auch derjenige, der beurteilen kann, welche vorbereitenden und begleitenden Tätigkeiten und Budgets erforderlich sind, um die Transformation zu realisieren. Diese Kombination bestätigen auch die Marktforscher von Gartner. Laut deren Beobachtungen hängen der Erfolg digitaler Investitionen in Abhängigkeit der angestrebter Geschäftsergebnisse in hohem Maße von einer starken Partnerschaft zwischen CFO und CIO ab. Da es sich um eine gemeinsame Verantwortung handelt, müssen CFOs und CIOs die gleiche Sprache sprechen. Dies schließt produktive Diskussionen darüber ein, wie Investitionen in digitale Technologien in echte digitale Fähigkeiten für das Unternehmen umgewandelt werden.

Ulrich Parthier: *Wie legt man Messgrößen fest, an denen sich die Initiative orientieren soll?*

Ralph Weiss: Der erste Schritt besteht darin, klar und übereinstimmend festzulegen, was das Unternehmen mit der Umgestaltung des Finanzbereichs in welcher Zeit, mit welchen Personalressourcen, Budget und vielleicht sogar externen Transformationsexperten erreichen will. Ob das Unternehmen die Genauigkeit seiner Finanzberichterstattung verbessern, die Effizienz seiner Finanzabschlussprozesse steigern oder in erster Linie die Kosten der Finanzprozesse senken möchte, sind Beispiele für entscheidende Fragen der Finanzex-

TRANSFORMATIONSLEITFADEN FÜR FINANZORGANISATIONEN:

Aufklärung und Konsens: Es ist von entscheidender Bedeutung, dass alle Transformationsinitiativen von Anfang an auf breite Zustimmung stoßen. Anstatt sich sofort in die Methodik und Umsetzung zu stürzen, sollten CFOs und Führungskräfte die Ziele einer Initiative mit Bedacht definieren und alle aus dem Finanzteam mit auf die Reise nehmen, denn jeder einzelne verfügt über unterschiedliche Kenntnisse im der digitalen Finanzorganisation. Es ist notwendig, in ein gemeinsames, referenzierbares Verständnis der Komponenten des digitalen Finanzwesens zu investieren, damit die Betroffenen besser verstehen, warum eine solche Veränderung stattfindet. Es bietet sich an, einen Raum für die Überprüfung der Transformation zu schaffen, denn es ist davon auszugehen, dass die Transformationsinitiative von dem ein oder anderen Teammitglied kritisch betrachtet wird und Vorbehalte abgebaut werden müssen. Ein geschütztes Umfeld, in dem die Teammitglieder ihr Unbehagen äußern können, ermöglicht es, kritische Fragen zu klären, bevor konkrete Maßnahmen ergriffen werden.

Schnelles Handeln nach Aufklärung und Konsens: Es ist wichtig, nach der Aufklärung unverzüglich zum Handeln überzugehen, indem man die Taktiken oder Maßnahmen zur Umgestaltung der Finanzen darlegt. Dazu könnten Technologiestrategie-Workshops gehören, in denen Best-Practice-Anwendungsfälle diskutiert werden, um mögliche Ergebnisse zu präsentieren.

Kontinuierliche Optimierung der Transformation: Mit dem Start der Transformationsinitiative ist es nicht getan. Unternehmen sollten einen Rahmen entwickeln, in dem es ein ständiges Feedback oder Diskussionen darüber gibt, wie bestimmte Prozesse verbessert werden können. Schlussendlich geht es darum, den Finanzteams zu helfen, ihre Aufgaben besser zu bewältigen und mit den laufenden technologischen Veränderungen Schritt zu halten. Eine digitale Transformation ist ein kontinuierlicher und flexibler Prozess und keine starre Abfolge von Aufgaben.

perten, die es zu klären gilt, bevor die Umgestaltung begonnen wird. Diese Messgrößen müssen mit denen der IT in Einklang gebracht werden. Denn nur so lässt sich ein Projekt, wie beispielsweise die Migration auf SAP S/4 HANA inklusive der Automatisierungslösung von BlackLine, planen und erfolgreich durchführen. Um die Messgrößen aufzustellen sind Vergleiche mit anderen Unternehmen ähnlicher Größenordnung, die bereits einen Prozess zur Umgestaltung des Finanzwesens durchlaufen haben, ein gutes Vorgehen. Derartige Beobachtungen eignen sich als Benchmark für das eigene Projekt. Beispielsweise sind der Personalaufwand der manuellen Finanzprozesse, die Genauigkeit der Finanzberichterstattung und der -prognosen, der Zeitaufwand für den Monatsabschluss usw. klare Messgrößen. Zudem können interne oder externe Prüfer dem Unternehmen ein höheres Level an Compliance attestieren, die es zuvor nicht erreicht hätte – gerade bei Unternehmen, die am Aktienmarkt gelistet sind, ist diese ein enorm wichtiger Aspekt.

Ulrich Parthier: *Gibt es bewährte Verfahren, wenn beispielsweise Kurskorrekturen erforderlich sind?*

Ralph Weiss: Bei allen größeren Projekten kann es zu unerwarteten Hindernissen oder Herausforderungen kommen, die Korrekturen erfordern, um die Initiative auf Kurs zu halten. Das muss nicht zwingend interne Gründe haben. Gesetzesänderungen können sich auf die Prozesse einer Finanzabteilung auswirken. Oder die kurzfristige, ungeplante Übernahme eines anderen Unternehmens kann erfordern, zwei Finanzorganisationen während der Transformationen sowohl organisatorisch als auch technisch zusammenzuführen. Für diese Frage gibt es aufgrund der mannigfaltigen Gründe für Korrekturen eine simple Antwort – der CFO und der CIO müssen von Anfang an einen detaillierten Plan mit weitreichender Flexibilität in alle Richtungen erarbeiten.

Ulrich Parthier: *Was sind Ihrer Meinung nach die wichtigsten Best Practices?*

Ralph Weiss: Aus der praktischen Erfahrung sind es drei wesentliche Aspekte. Erstens, die Fortschritte überwachen. Es müssen von Anfang an klare Ziele und Kennzahlen festgelegt sein, um allen Beteiligten jederzeit einen Überblick zu verschaffen. Auf diese Weise kann das C-Team schnell feststellen, in welchen Bereichen die Umsetzung technisch oder finanzorganisatorisch zu wünschen übriglässt und frühzeitig die notwendigen Schritte einleiten. Zweitens gilt es die Kommunikation und Zusammenarbeit zu etablieren und aufrechtzuerhalten. Die Organisation sollte einen Kommunikationsplan erstellen, damit alle Beteiligten verstehen, wie sich die Zuständigkeiten und die Verfahren ändern und vor allem, warum. Es ist wichtig, einen regelmäßigen Kommunikationsrhythmus einzuhalten, um über die neuesten Änderungen, Ergebnisse und Erfolge zu informieren. Drittens ist ein effektives Changemanagement eine der wichtigsten Best Practices.

Ulrich Parthier: *Lässt sich die aktive Beteiligung des Finanz- und IT-Teams fördern?*

Ralph Weiss: Unternehmen sind oft erpicht darauf, jede Form von Transformationsinitiativen sowohl intern als auch extern zu kommunizieren. Sie wollen zeigen, dass sie Fortschritte machen. Allerdings ist es dabei wichtig, dass die Einbindung der Mitarbeiter in die Kommunikation ein separater und priorisierter Prozess ist, der nicht von alleine oder automatisch entsteht. Nur wenn die Mitarbeiter sehen, dass sie aktiv einbezogen werden, und ihre Mitarbeit an der Umstrukturierung erwünscht ist, werden sie sich aktiv an derartigen Initiativen beteiligen.

Ulrich Parthier: *Haben Sie einen besonders wichtigen Rat, den Sie CFOs und CIOs für ihre Transformation mit auf den Weg geben wollen?*

Ralph Weiss: Der digitale Transformationsprozess ist bei jedem Unternehmen anders, da er von vielen individuellen Gegebenheiten im Unternehmen abhängt. Ein gemeinsamer Faktor aller Unternehmen, die erfolgreich digitale Transformationsinitiativen umgesetzt haben, ist ein klares Verständnis darüber, was sie mit der digitalen Transformation in der Fachabteilung unter Einsatz neuester Technologie erreichen wollen. CFOs und CIOs sollten daher klare und vor allem realistische umsetzbare Ziele definieren, die beide Parteien eng in das Programm zur Umgestaltung der Finanzabteilung einbeziehen.

Ulrich Parthier: *Herr Weiss, vielen Dank für das Gespräch.*

VOR DEN KOPF GESTOSSEN

Der jüngste Vorstoß der SAP lässt einige dunkle Wolken aufziehen. Das klare Signal aus Mannheim: Zukünftige Innovationen? Exklusiv in der Cloud! Ein Schritt, der in vielen Kreisen für Entrüstung sorgt.

Alles verändert sich, nichts bleibt, wie es ist. So die Eingangsworte der DSAG in ihrer Einladung zum Jahreskongress. Die Anwender haben sich diese Veränderungen womöglich etwas anders vorgestellt. Den Innovationspfad in luftige Höhen zu verlagern, hat viele Unternehmen, die eher den festen Boden von On-Premises-Lösungen schätzen, vor den Kopf gestoßen. SAP spielt wieder einmal mit dem Vertrauen der Basis, denn langjährige Kunden fühlen sich übergangen. Das kritisierte auch die Anwendergruppe.

Da stellt sich die Frage: Wie navigiert man sich durch diese sich ständig verändernde Landschaft und welche Überraschungen hält der SAP-Kosmos noch bereit? Lesen Sie sich durch eine Auswahl im SAP Spezial! Und wer weiß? Vielleicht klart der Himmel schneller auf, als man denkt.

Nahtlose End-to-End-Prozesse

WIE INTEGRIERE ICH EIN DRITTSYSTEM OPTIMAL IN MEINE SAP-UMGEBUNG?

SAP-Systeme bieten Nutzern eine breite Palette an Funktionen, oftmals braucht es aber Drittsysteme, um bestimmte Prozesse zu digitalisieren. Damit die Prozessschritte außer- und innerhalb von SAP nicht isoliert dastehen, sondern einen reibungslosen Gesamtprozess bilden, werden die Drittsysteme in SAP integriert. Für die Integration steht wiederum eine Auswahl an Methoden zur Verfügung.

Warum die Integration von Drittsystemen so wichtig ist

Im Zuge der digitalen Transformation werden immer mehr Software-Lösungen eingesetzt, um einen möglichst hohen Automatisierungsgrad zu erreichen. Bei der Auswahl einer Lösung für einen bestimmten Bereich spielen verschiedene Abteilungen zusammen. Während die Fachabteilung besonders auf die funktionale Ausstattung und die Usability schaut, liegt das Augenmerk der IT neben Datenschutz und -sicherheit auf der Interoperabilität mit der bestehenden Systemlandschaft, besonders auf der Integration mit SAP. Ohne einen funktionierenden Datenaustausch bleibt das Drittsystem isoliert, was zu Ineffizienzen und zu Fehlern führt.

Konnektoren als direkter Draht ins SAP-System

Eine Möglichkeit, die auch weit verbreitet Anwendung findet, ist die Nutzung eines vorgefertigten Konnektors. Konnektoren sind im Software-Bereich generell weit verbreitet und verbinden verschiedene Anwendungen, um durchgängige Prozesse zu ermöglichen. Im SAP-Umfeld werden Konnektoren oft eingesetzt, beispielsweise durch die Nutzung des SAProuter als direkte Verbindung zwischen Drittsystem und SAP. Der Aufbau eines SAP-Konnektors ist zwar kostspielig, dafür kann er, mit individuellen Anpassungen, immer wieder verwendet werden. Deshalb werden Konnektoren im Normalfall von Software-Anbietern oder -Dienstleistern aufgebaut.

Konnektoren haben bei der Implementierung den großen Vorteil, dass sie die Verbindung zwischen Drittsystem und SAP per „Plug & Play" herstellen können. Innerhalb des Konnektors sind alle nötigen Parameter hinterlegt, damit die Daten hin- und herlaufen können. Der Aufwand ist damit gering, solange im SAP-System keine umfangreichen Anpassungen vorgenommen wurden. Sie haben jedoch auch Nachteile: Sie müssen ständig gepflegt werden, da bei Änderungen in einem der verbundenen Systeme die Kon-

nektivität gestört werden kann. Im Normalfall wird diese Wartung durch den Anbieter des Drittsystems mit abgedeckt.

Im laufenden Betrieb bieten Konnektoren diverse Vorteile: Durch den Echtzeitabgleich sind die Daten in beiden Systemen durchgängig auf demselben Stand. Die Verbindung zwischen den beiden System wird in aller Regel verschlüsselt. Der Konnektor sorgt damit für einen nahtlosen End-to-End-Prozess. Für viele Unternehmen, die SAP nutzen, ist das Vorhandensein eines Konnektors ein wichtiges Kriterium bei der Auswahl eines Drittsystems. Ein weiterer Vorteil eines Konnektors: Er ist aufwärtskompatibel, also so aufgebaut, dass er auch zukünftige Änderungen im SAP-System mit keinem oder minimalen Aufwand umsetzen kann. Besonders für Unternehmen, die bereits jetzt oder zukünftig auf SAP S4/HANA setzen, ist das ein wichtiger Faktor.

Der Einsatz einer BAPI als Alternative

Eine Alternative zu Konnektoren sind Programmierschnittstellen (Application Programming Interface, API). APIs existieren in verschiedenen Formen, beispielsweise als REST API oder SOAP API. Im SAP-Kontext kommt besonders oft ein BAPI (Business Application Programming Interface), eine standardisierte, speziell für SAP-Business-Objekte anwendbare API zum Einsatz. Während gewöhnliche APIs lediglich eine Anbindung auf technischer Ebene schaffen, können BAPIs auch eine Integration auf betriebswirtschaftlicher Ebene sicherstellen. Über den BAPI können die Drittsysteme auf die SAP-internen Business-Objekte zugreifen und mit diesen interagieren, also beispielsweise Daten austauschen. Die Verbindung zwischen Drittsystem und SAP über ein BAPI stellt eine stabile und auch sichere Variante dar.

Im Gegensatz zur Integration mit einem Konnektor schafft ein BAPI keinen Echtzeitabgleich zwischen den verbundenen Systemen, sodass Masterdaten oder Dokumente nicht direkt aus dem Drittsystem abgerufen oder in SAP verwaltet werden können. Jedoch kann, beispielsweise mit dem Einsatz eines Web Services, eine ständige Remote-Verbindung genutzt werden, um quasi in Echtzeit Daten auszutauschen. Alternativ können zu festen Zeiten Datenabgleiche durchgeführt werden. Die Entscheidung, welcher Aufbau der beste ist, sollte anhand der individuellen Unternehmenssituation gefällt werden.

Middleware als Integrationsplattform

Die Integration einer Drittapplikation kann auch über eine Middleware erfolgen. Eine Middleware ist eine Art Datendrehscheibe zwischen Applikationen, zum Beispiel zwischen dem SAP-System und anderen Anwendungen. Sie stellt sicher, dass getrennte Systeme miteinander kommunizieren können, indem sie Daten zwischen den Systemen vermittelt. Ein großer Vorteil liegt in der Reduzierung der Schnittstellen, denn nicht mehr die Systeme werden aufwändig miteinander verbunden, sondern jedes System nur noch mit der Middleware. Ein Nachteil liegt darin, dass es eine weitere Software-Komponente ist, die gewartet und überwacht werden muss. Als Integrationsplattform wird eine Middleware häufig dann eingesetzt, wenn aus Security Policy-Gründen die direkte Anbindung von Drittapplikationen an ein SAP-System ausgeschlossen ist. Neben unterschiedlichen Middlewares am Markt bietet SAP eine eigene: SAP PI/PO für On Premises-Applikationen und „SAP Integration Suite" sowie „SAP Cloud Integration" für Cloud-Anwendungen.

Nutzung von Flat Files

Flat Files, sprich Dateien in einem zweidimensionalen Format wie CSV, XML oder JSON, können ebenfalls für die Integration eines Drittsystems in SAP genutzt werden. Die Integration ist in diesem Fall eher lose, weil keine ständige Verbindung zwischen Drittsystem und SAP eingerichtet wird. Die Daten werden als Dateien über gesicherte Verbindungen, zum Beispiel SFTP, einen Web Service oder per EDI, direkt in SAP eingeliefert. Vom Drittsystem benötigte Daten aus SAP laufen auf dieselbe Weise zurück. Diese Methode kommt beispielsweise zum Einsatz, wenn aus Technologie-, Architektur- oder Sicherheitsaspekten keine Anbindung über Konnektoren, BAPI oder Middleware möglich ist.

OHNE EINEN FUNKTIONIERENDEN DATENAUSTAUSCH BLEIBT DAS DRITTSYSTEM ISOLIERT, WAS ZU INEFFIZIENZEN UND ZU FEHLERN FÜHRT.

Peter Gatzen,
Head of Marketing, Esker Software Entwicklungs- und Vertriebs-GmbH, www.esker.de

Welche Methode ist die beste?

Diese Frage lässt sich pauschal nicht beantworten, da viele Faktoren, wie zum Beispiel die IT-Strukturen, die Prozessabläufe oder die gewünschte Tiefe der Integration, bei der Auswahl berücksichtigt werden müssen. Moderne Lösungen zur Automatisierung von Geschäftsprozessen bieten aber eine Vielzahl von Integrationsmöglichkeiten um die unternehmensindividuellen Anforderungen optimal abzubilden. SAP-Anwender können sich bei der Auswahl beispielsweise daran orientieren, ob der Anbieter des Drittsystems zertifizierter SAP-Partner ist. Zertifizierte Partner stellen sicher, dass Lösungen bereitgestellt werden, die den von SAP festgelegten Qualitätsanforderungen und -standards entsprechen.

Peter Gatzen

DSAG-Jahreskongress 2023

WUNDERBAR WANDELBAR

Alles verändert sich, nichts bleibt, wie es ist. Die heutige Zeit setzt Flexibilität voraus. Entsprechend wandelbar präsentieren sich die Deutschsprachige SAP-Anwendergruppe e. V. (DSAG), SAP und das gesamte Ökosystem. Genau diese Wandlungsfähigkeit rückt auch der DSAG-Jahreskongress 2023 vom 19. bis 21. September im Congress Center Bremen in den Fokus. Unter dem Motto „Wunderbar wandelbar – Gemeinsam neue Perspektiven schaffen" freut sich die DSAG darauf, mehr als 5.000 Teilnehmende zu begrüßen. Die Interessenvertretung wirft den Blick durch das Kaleidoskop und macht sich mit den Teilnehmenden auf die Suche nach dem richtigen Dreh, um den digitalen, technologischen, ökologischen und ökonomischen Wandel zu meistern und Veränderungen erfolgreich zu gestalten.

Digitalen Wandel gemeinsam gestalten

Unternehmen befinden sich, wie es das Motto des Jahreskongresses beschreibt, im Wandel. Sie müssen sich kontinuierlich weiterentwickeln, um die Veränderungen um sich herum zu meistern und bestenfalls den Wettbewerb langfristig zu überholen. „Beim Jahreskongress 2022 hatten wir thematisiert, wie Unternehmen auf der Suche nach Erfolg mit Veränderungen Schritt halten müssen. In diesem Jahr schlagen wir die Brücke und fragen danach, wie Unternehmen, die DSAG, SAP und das gesamte Ökosystem gemeinsam den Wandel aktiv gestalten können", erläutert Jens Hungershausen, DSAG-Vorstandsvorsitzender das Motto des DSAG-Jahreskongresses 2023.

Wie wandelbar sind Unternehmen bzw. Organisationen in der DSAG? Welche Rolle spielt die IT dabei? Wie kann das SAP-Ökosystem konkret unterstützen? Aus DSAG-Sicht ist hier neben den Akteuren auch das Drehmoment entscheidend. „Damit der Wandel wirklich ‚wunderbar' wird, sind alle Gewerke gefragt. Betrachten wir z. B. den digitalen Wandel mit Fokus auf die S/4HANA-Transformation, könnte SAP die Unternehmen bei ihren Migrationsprojekten noch mehr unterstützen, indem Umstellungsprojekte und Update-Zyklen schneller, schlanker und einfacher werden.

www.dsag.de/jahreskongress

Die Studie ist hier erhältlich:
http://bitly.ws/RTmX

Neue ISG-Studie

ROSIGE ZEITEN FÜR SAP-SERVICEANBIETER IN DEUTSCHLAND

In den S/4HANA-Markt kommt zunehmend Bewegung, die Zeichen stehen für SAP-Serviceanbieter auf Wachstum. Das berichtet die neue Studie „ISG Provider Lens SAP Ecosystem Germany 2023", die die Information Services Group (ISG) veröffentlicht hat. Der Studie zufolge wird Deutschland in den kommenden Jahren zum Hauptschauplatz für große SAP-Vorhaben. Ein Grund dafür sei der steigende Druck wegen der 2027 anstehenden Abkündigung der Standardwartung der SAP S/4HANA-Vorgänger.

Ausbau branchenspezifischer Lösungspakete

SAP-Serviceanbieter bauen derzeit ihr Portfolio weiter aus, um die wachsende Marktnachfrage nach Cloud-Angeboten für SAP bedienen zu können, so die Studie weiter. Die Anwenderunternehmen würden dabei gerade im SAP-Umfeld nach wie vor Private-Cloud-Angeboten Vorrang einräumen. Das in diesem Umfeld von SAP gestartete Programm „RISE with SAP" wird den ISG-Analysten zufolge jedoch eher zögerlich angenommen. Unabhängig davon hätten aber nahezu alle Anbieter ihr Serviceangebot für RISE erweitert.

Ein relativ neues Thema im SAP-Umfeld verzeichnet der Anbietervergleich mit Blick auf Nachhaltigkeit. Viele Anbieter führten dieses Schlagwort bereits auf ihrer Agenda und hätten entsprechende Programme innerhalb ihrer Organisation gestartet. Wenn es jedoch um die konkrete Unterstützung solcher Initiativen bei Kunden geht, würden viele Anbieter den Nachweis erfolgreicher Implementierungen mit messbaren Ergebnissen noch schuldig bleiben.

www.isg-one.com

Vorbereitung ist alles

SCHLÜSSELFAKTOR EINER ERP-TRANSFORMATION

„Digitale Transformation" ist ein großes Wort und das zurecht. Denn dahinter verbirgt sich die Neu- und Umgestaltung von kompletten Systemlandschaften und Prozessen, etwa der Umstieg auf SAP S/4HANA. Und da die Digitale Transformation eine Vielfalt an Herausforderungen mit sich bringt, ist es wichtig, auf gesicherten Erkenntnissen und Best Practices aufzubauen. Um dieses Wissen zusammenzutragen und aufzubereiten, hat Natuvion zum zweiten Mal eine Umfrage unter Unternehmen durchgeführt, die eine Transformation gerade hinter sich gebracht haben. Zusammen mit der NTT DATA Business Solutions wurden alle Ergebnisse der Untersuchung in der Transformationsstudie 2023 veröffentlicht.

Im Zentrum der Studie standen Fragen zur Motivation, den Zielen und Herausforderungen der Transformation sowie überraschenden Erkenntnissen. Die Ergebnisse aus 630 Befragungen helfen Unternehmen, die Komplexität der Transformationsprojekte besser zu verstehen und eine Planung realistisch mit allen nötigen Details zu erstellen.

ZU DEN GRÖSSTEN HERAUSFORDERUNGEN EINER ERP-TRANSFORMATION GEHÖREN PROBLEME MIT DER DATENQUALITÄT.

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

Wer schiebt an und was ist die Motivation?

Initial sind am Entscheidungsprozess mit knapp 60 Prozent mehrheitlich die Geschäftsführungen und Vorstände der Unternehmen die treibende Kraft.

Hinsichtlich der Motivation ergab die Studie erstaunliche regionale Unterschiede: In den USA, einem Land mit ausgeprägter Digitalwirtschaft, spielt neben der Einführung neuer Geschäftsmodelle auch die „schnellere Reaktion auf Markterfordernisse" eine wichtige Rolle - wichtiger als in Europa. Für fast 50 Prozent der Befragten war die stärkere Flexibilisierung ihrer Geschäftsprozesse einer der wichtigen Gründe für die Transformation. Der stärkste Motivator in der DACH-Region ist jedoch die Kostensenkung mit 43 Prozent.

Schlüsselfaktor Vorbereitung

Mit Beginn der Vorbereitung sind CEOs, CIOs und andere Transformationsspezialisten am Zug. Zu deren Aufgaben gehört u.a. die Planung des Zeitrahmens, der sich laut Studie regional stark unterscheidet: Am deutlichsten ist das bei einer Planung von bis zu sechs Monaten zu sehen: Das streben rund 23 Prozent der Amerikaner an, jedoch nur 15 Prozent der DACH-Unternehmen. Gleichwohl schätzen deutlich mehr DACH-Unternehmen den realistischen Zeitraum für die Transformation mit 30 Prozent (25 Prozent in den USA) bis zu einem Jahr oder mit ebenfalls 30 Prozent (23 Prozent in den USA) bei einem bis zu zwei Jahren.

Überraschungen vermeiden

Die Qualität einer Planung zeigt sich bei der Umsetzung. Komplexe Transformationen, beispielsweise zu SAP S/4HANA, bergen Komplikationen, die nur transformationserfahrene Spezialisten im Vorfeld erkennen können. Daher ziehen laut der Studie zunehmend mehr Unternehmen künftig externe Spezialisten von Anfang an hinzu.

Zu den größten Herausforderungen einer ERP-Transformation gehören Probleme mit der Datenqualität. Über 30 Prozent kennen das. Aber dafür gibt es eine Lösung: Housekeeping. Dabei handelt es sich um die Pflege der Datenbasis. Denn die Steigerung der Datenqualität, das Sicherstellen und Etablieren von Belegketten, das Ordnen und die Reduktion des Datenvolumens sind ein elementarer Erfolgsfaktor der Digitalen Transformation. Speziell für Migrationsprojekte hat Natuvion jetzt einen Migrations-Readiness Check entwickelt, der im Natuvion „Housekeeping Roadbook" beschrieben ist. Der kostenlose Leitfaden beleuchtet alle datenbezogenen Aspekte einer Transformation – von der ersten Bestandsaufnahme über die Differenzierung und Selektion der Daten bis hin zur Migration. Unternehmen und Migrationsexperten erhalten einen genauen Einblick und praktische Handlungsanweisungen für das Housekeeping unterschiedlicher Datenarten, für das Life Cycle Management und für die Fragestellung, wie eine Migration die Performance der IT generell verbessern kann.

Philipp von der Brüggen

Natuvion

Moderne No-Code-Schnittstellen

ENDLICH OHNE STRESS UND MEHRAUFWAND AN DIE SAP-DATEN!

SAP-Daten sind heiß begehrt, denn ihr Nutzen ist vielfältig. Typische Use Cases sind zum Beispiel Finanzdaten, die aus der Buchhaltung, den einzelnen Kostenstellen oder dem Controlling stammen und weiterverarbeitet oder geändert werden müssen. Außerdem zu nennen sind Logistik und Supply Chain: Lagerbestände und ihre Veränderungen, Werte, Ort und Zustand von Materialien, Bestell- und Auslieferungsstatus.

Beanspruchung der ohnehin überlasteten IT-Abteilung

Jede Abfrage von SAP-Daten bindet erhebliche Ressourcen in IT-Abteilung und SAP-Basis. So müssen Systeme von der IT eingerichtet werden, wobei Sicherheitsanforderungen erfüllt, Checklisten abgearbeitet und vorgegebene Prozesse eingehalten werden müssen. Ähnlich auf der SAP-Seite, wo Änderungen in Form von Installationen und Konfigurationen anfallen.

Beides ist zunächst ein einmaliger Aufwand – bei dem es erfahrungsgemäß jedoch nicht bleibt. Selbst kleine Reportanpassungen ziehen einen großen Aufwand nach sich und können Wochen oder sogar Monate dauern, da derlei Anfragen häufig in der Warteschlange landen. Dringend benötigte, mitunter strategische Datenauswertungen sind nicht zum entscheidenden Zeitpunkt verfügbar.

Reibungsloser SAP-Betrieb als Hemmschuh

Doch nicht nur mangelnde Kapazitäten blockieren eine schnelle Umsetzung. Da fast alle Daten, die im SAP-System liegen, hochsensibel sind, ist ein korrekter, vorsichtiger Umgang mit ihnen obligatorisch. Die IT-Verantwortlichen fragen bei allen Informationsanfragen daher nach der Verschlüsselung, dem Speicherort und dem Prozess des Datenabzuges.

Außerdem hat die SAP-Basis den reibungslosen Betrieb des SAP-Systems im Blick. SAP darf aufgrund des Datenabzugs nicht langsamer laufen, blockieren oder Schaden davontragen.

Den Herausforderungen begegnen

Abhilfe schaffen Self-Service-Lösungen auf No-Code-Basis. Wenn ein User ohnehin bereits über einen SAP-Zugriff mit den entsprechenden Berechtigungen verfügt, kann er mit diesen Schnittstellen die Daten direkt in seine Zielanwendung übertragen. Weder benötigt ein Citizen Developer oder Business Analyst dafür die Unterstützung der IT-Abteilung, noch muss er die Daten in einem Data Warehouse zwischenspeichern, obgleich No-Code-Schnittstellen auch dies unterstützen.

Der Vorteil: Der Report-Aufwand ist genauso hoch wie im SAP GUI, das heißt wenige Minuten ohne Konfiguration. Verfügen die User über Kenntnisse zu SAP-Tabellen, können sie einen Extrakt von beispielsweise zwei oder drei Tabellen erstellen und innerhalb weniger Minuten in ihr BI Tool transferieren. Gleiches gilt für Änderungen der Extraktion.

Datensicherheit auch bei Self Service

Den Zweifel, ob Self Service die notwendige Datensicherheit – Security wie Privacy – bietet, können No-Code-Schnittstellen zerstreuen. Sie verfügen über ein doppeltes Zugriffsmanagement, das auf SAP- und Schnittstellen-Ebene ansetzt. So stellen sie die Verbindung zu SAP über ein bereits vorhandenes Nutzerkonto her und agieren im identischen Security-Umfeld wie ein SAP GUI User. Es existieren keine Hintertüren zu SAP, mit deren Hilfe bestehende Vorgaben umgangen werden können. Unternehmen sollten auf diesen Punkt besonders achten und eine SAP-Zertifizierung ihres Schnittstellen-Anbieters für seine Lösung zur Bedingung machen.

Darüber hinaus ermöglichen SAP-Schnittstellen auf No-Code-Basis ihrerseits ein feinjustiertes Regelwerk. Sie erlauben nur selektierten Nutzern den

Zugriff auf das Self-Service-Tool und auch nicht jeder aus dieser Gruppe kann alle Datenextraktionen vornehmen.

Implementierung

Die No-Code-Schnittstelle zu implementieren, ist ein kurzes, niedrigschwelliges Projekt. Ein ausgearbeitetes Berechtigungskonzept ist zu Beginn noch nicht notwendig. Eine ausgeprägte Vorstellung von den Daten, auf die die Unternehmen zugreifen, und den Reports, die sie erstellen wollen, ist hingegen im Vorfeld hilfreich, um die Implementierung zu beschleunigen.

Außerdem sorgt es für mehr Effizienz, wenn die Verantwortlichen die anzusteuernden Quellen in SAP bereits kennen, etwa welche Tabellen oder ABAP Reports dort existieren. Ein weiterer Aspekt, den Unternehmen klären können: Die Ports vom Desktop zum SAP-System sollten offen sein, eine Netzwerkverbindung zum SAP-System vorhanden. Die Schnittstelle selbst muss anschließend einmalig auf dem jeweiligen Desktop oder zentral auf dem Server installiert werden.

Fazit

No-Code-Schnittstellen zur Integration von SAP-Daten in Drittumgebungen sind die passende Antwort auf die drei Herausforderungen Ressourcenknappheit in der IT, mangelnde Datensicherheit und Risiken für den SAP-Betrieb. Zugriffsberechtigungen sind dabei präzise steuerbar, die Kontrolle verbleibt bei der IT-Abteilung und das SAP-System ist geschützt, während der Business Analyst die benötigten Informationen ohne Umwege erhält.

Christoph Schuler

SAP-SCHNITTSTELLEN AUF NO-CODE-BASIS ERMÖGLICHEN EIN FEINJUSTIERTES REGELWERK. SIE ERLAUBEN NUR SELEKTIERTEN NUTZERN DEN ZUGRIFF AUF DAS SELF-SERVICE-TOOL.

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

BEI UNS SIND IHRE SAP-PROJEKTE IN GUTEN HÄNDEN!

Was uns ausmacht und differenziert erfahren Sie am **Stand H4**

DSAG
DSAG-Jahreskongress 2023
19.-21. September 2023
Messe Bremen

DIE VORAUSDENKER.
DIE PROZESSOPTIMIERER.
DIE LÖSUNGSENTWICKLER.

CONSILIO

Einsteinring 22 | 85609 Aschheim
T +49 89 9605750 | W www.consilio-gmbh.de

SAP® Recognized Expertise SAP S/4HANA®
SAP® Recognized Expertise Supply Chain Planning and Logistics
SAP® Recognized Expertise Financial Management
SAP Gold Partner

Sicher in den Wolken

ANFORDERUNGEN AN DIE GELUNGENE SAP-CLOUD-MIGRATION

Die Migration von SAP-Systemen in die Cloud bietet zahlreiche Vorteile, wie Skalierbarkeit, Flexibilität und auch die Möglichkeit der strukturierten Kosteneinsparungen, bringt aber auch einzigartige Sicherheitsherausforderungen mit sich, die abgewogen und gelöst werden müssen. Erfolgreich in die Cloud migriert, lassen sich dank der innovativen Ansätze vor Cyber-Bedrohungen Vertraulichkeit, Integrität und Verfügbarkeit wichtiger Geschäftsinformationen und SAP-Daten mittlerweile gewährleisten. Doch der Weg dahin ist abhängig vom eigenen Know-how und dem der beratenden IT-Dienstleister.

Experten spekulieren, dass die 2024 in Kraft tretende EU-Richtlinie NIS2 eine deutlich kürzere Halbwertszeit haben wird, als die immerhin beinahe acht Jahre gültige NIS-Richtlinie. Denn das digitale Wettrüsten zwischen Industrie und den strukturell gewachsenen internationalen Hackerteams, wird immer kürzere Abstände für neue Richtlinien in den kommenden Jahren erfordern. Für Unternehmen und Organisationen bedeutet dies, dass sie auf IT-Infrastrukturen setzen müssen, deren Sicherheitsvorkehrungen beständig überwacht und angepasst werden können. Aus dieser Perspektive betrachtet und abgesehen vom ohnehin anstehenden Wechsel auf SAP S/4HANA spricht also alles für die Cloud – und wenig für das Rechenzentrum, das sich mit deutlich kleineren Strukturen und weniger personellen Kapazitäten in immer kürzeren Intervallen darum kümmern muss, dass die Vor-Ort-Sicherheitstechnik mithält. Wichtig ist, langfristig sicherzustellen, dass über eine robuste Sicherheitsstrategie verfügt wird, die auf die spezifischen Anforderungen von SAP on Cloud zugeschnitten ist. Die Implementierung von Verschlüsselungen, Multi-Faktor-Authentifizierung, Disaster Recovery-Lösungen, die im Fall der Fälle eine leichte Wiederherstellung der Daten garantieren, sind dafür nur einfache, aber nichtsdestotrotz grundlegende Beispiele.

SAP ON CLOUD HAT BEI DEUTSCHEN UNTERNEHMEN UND ORGANISATIONEN NOCH LUFT NACH OBEN.

Simon Meraner, Geschäftsführer, Zoi Barcelona, www.zoi.tech/de

Anforderungen steigen

Schon heute gilt die Regel, dass der Cyber-Angriff kommt – nur der Zeitpunkt ist unklar! Daher sind die IT-Verantwortlichen aus Organisationen und Unternehmen mehr denn je in der Pflicht, auf alles, was kommen mag, vorbereitet zu sein. Dies bedeutet die kontinuierliche Überwachung und das Monitoring aller relevanten Datenströme genauso wie die Erkennung von Bedrohungen wie beispielsweise das Aufspüren von Datenverschlüsselungen durch Malware oder auch der Schutz von sicherheitsrelevanten Konfigurationen der Infrastruktur durch Infrastructure-as-Code- und Konfigurationsmanagement-Services. Und auch wenn technisch bereits der Großteil der möglichen Bedrohungen durch eine sinnvoll durchdachte und zukunftsfähige Cloud-Architektur gegeben ist, so sitzt die Schwachstelle in vielen Fällen doch vor dem Bildschirm. Hier kommt es neben den bekannten und immer wieder einmal auftauchenden Sicherheitslücken wie beispielsweise bei MS-Exchange bekanntermaßen bereits durch einen Klick oder sogar nur eine Mail-Vorschau in der rechten Bildschirmhälfte zu offenen Toren zu den eigenen Systemen und Daten.

Geschäftskritische Anwendungen sichern

Unternehmen, die sich für SAP on Cloud entscheiden, profitieren also von Beginn an von vielen, durchaus auch geldwerten Vorteilen. Punkte im Zusammenhang mit Datenschutz oder -sicherheit reduzieren sich auf Detailfragen, auch wenn sie von ihrer Bedeutung nichts verlieren. Schließlich handelt es sich zumeist um geschäftskritische Anwendungen, die in der Regel hochsensible Daten enthalten.

Ebenso wichtig bei der Migration von SAP on-premises in die Cloud: Die Unternehmen müssen von Beginn an sicherstellen, dass alle Sicherheitsanforderungen erfüllt sind, einschließlich der Einhaltung von Compliance-Vorschriften wie der DSGVO. Die gute Nachricht ist: Ausgewiesene Best-Practices der SAP- und der Public-Cloud-Service-Provider helfen bei der richtigen Cloud-Architektur, indem sie die wichtigsten Funktionalitäten mit einem Heer von Security-Experten und Programmierern sicherstellen. Der echte Nutzen für Unternehmen und Organisationen be-

steht darin, innerhalb der Architektur diese Elemente zu einem (nahezu) vollständigen Sicherheitspaket zusammenzustellen.

Die Qual der Wahl

Die Wahl des richtigen Cloud-Providers ist folglich entscheidend für die Sicherheit von SAP on Cloud. Unternehmen sollten sich für einen Provider entscheiden, der eine starke Sicherheitsinfrastruktur bietet und regelmäßige Audits und Zertifizierungen durchführt. Dies ist bei den führenden Public Cloud Anbietern gegeben, trotzdem empfiehlt es sich, aktuelle News prüfen, um einen Eindruck für die Sensibilität des Themas Security bei einem Provider zu bekommen. Die Alternative sind zertifizierte Cloud-Experten, die sich tagtäglich mit genau diesen Themen auseinandersetzen und neben SAP die gesamte weitere Bandbreite an Cloud-Themen abdecken, wie beispielsweise Data Lakes, BI, KI und IIoT.

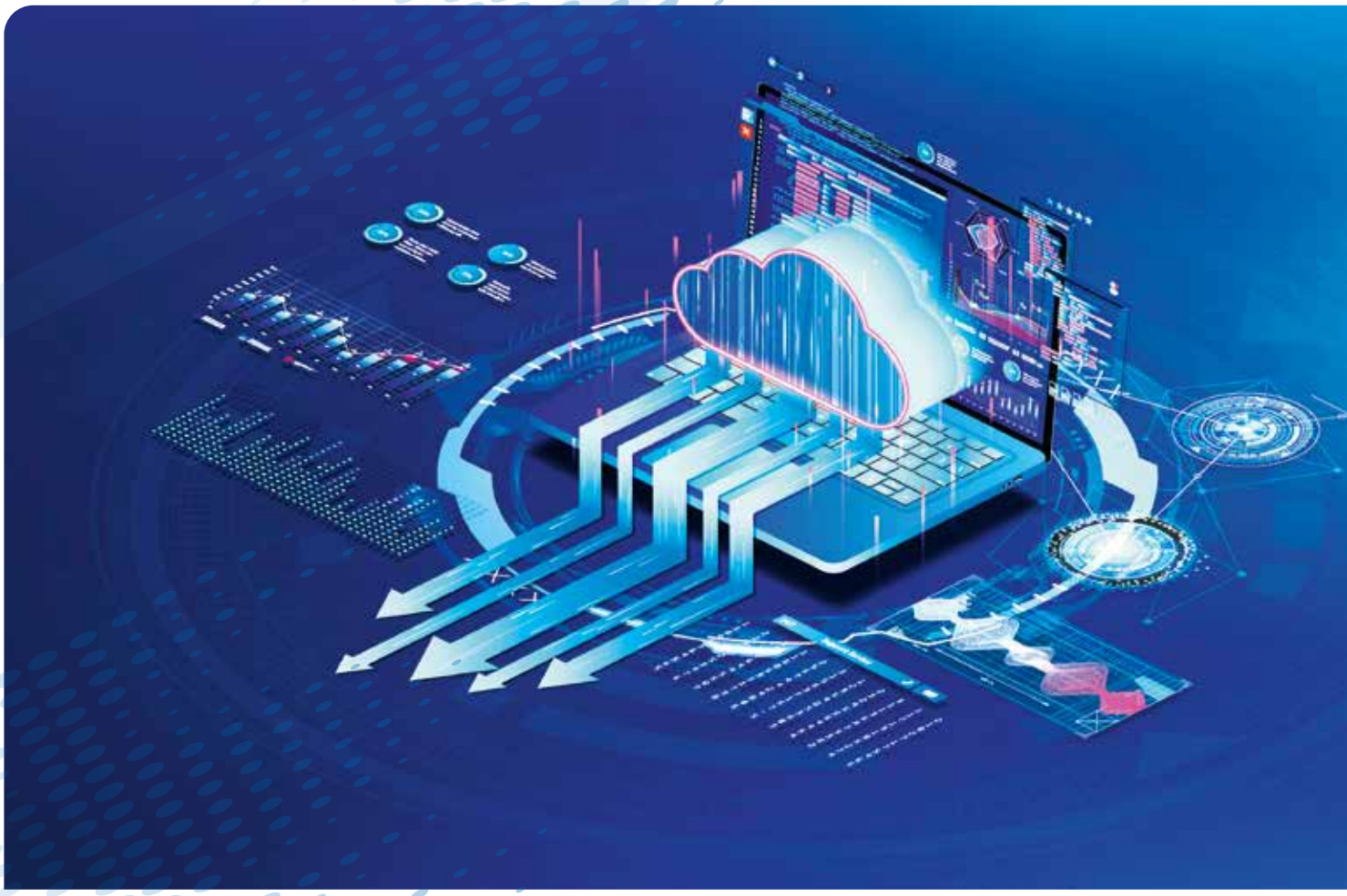
Gefahr vor dem Bildschirm

Eines der immer noch allzu oft unbedachten Einfallstore, sind die eigenen Mitarbeiterinnen und Mitarbeiter. Die fortwährende Schulung und Sensibilisierung dieser ist absolut entscheidend, um die Sicherheit zu gewährleisten. Denn nur wer sich bewusst ist, welche Daten als sensibel eingestuft werden und wie er sich sicher verhalten kann, um die Sicherheit zu gewährleisten, kann dies auch im Alltag tun.

Fazit

SAP on Cloud hat bei deutschen Unternehmen und Organisationen noch Luft nach oben – insbesondere weil eben viele den Schritt zur selbstbestimmten und souveränen sowie State-of-the-Art-Coud-Technik noch nicht gegangen sind. Die Cloud-Anbieter liefern in unterschiedlichen Breiten und Tiefen bereits den sicheren Unterbau, um SAP sinnvoll und zukunftssicher aus der Cloud heraus zu betreiben und dabei den Großteil der jetzigen und zukünftigen Sicherheitsaspekte abzudecken: Nahezu alle Cyber Security-relevanten Aspekte werden durch die Migration der Workloads in die Cloud und anschließendes cloudbasiertes Arbeiten verbessert. Die Frage, die sich Unternehmen und Organisationen stellen müssen: Schaffen wir es selbst, uns kontinuierlich um sicherheitsrelevante Fragen und Antworten zu kümmern, oder ziehen wir hochzertifizierte Spezialisten hinzu, die uns bei wesentliche Arbeitspaketen und Projekten unterstützen. Denn eines ist sicher: Das Thema Sicherheit wird uns – auch in der SAP-Welt – weiter auf Trab halten.

Simon Meraner



Produktionsplanung

DIE REIHENFOLGE ZÄHLT

Vorspeise, Hauptgang, Dessert: Bei einem guten Essen steht die Reihenfolge fest. Auch bei der Produktionsplanung kommt es auf den passenden Ablauf an. Um sicherzustellen, dass es weder an der Maschine selbst noch im Vorlauf- oder Folgeprozess hakt, sollte der Produktionsprozess über alle Arbeitsplätze und Aufträge hinweg geplant werden. Im SAP-Standard ist dies – es sei denn, SAP APO kommt zum Einsatz – sehr aufwendig, da es keine Automatisierungsmöglichkeit gibt. Aufgrund unzähliger Abhängigkeiten und Variablen ist die Mehrplatzplanung anspruchsvoll, aber machbar – sofern die Reihenfolge stimmt! Doch wie lässt sie sich ermitteln?

Für eine praxisgerechte Produktionsreihenfolgeplanung benötigt man, ganz kurz gesagt, alle relevanten Daten und deren Auswertung. Ausführlicher geantwortet: Es bedarf einer Software, die für jeden Auftrag eruiert,

- welches Material und/oder welche Teile benötigt werden,
- wann das Material/die Teile an welchem Arbeitsplatz sein müssen,
- welche Fertigungsabläufe vor- und nachgelagert sind,
- welche Ruhe-, Rüst- und Pufferzeiten eingehalten werden müssen.

Komplex wird die Aufgabe dadurch, dass die Daten für jeden einzelnen Auftrag erhoben und in Beziehung gesetzt werden müssen. Auch die Auftragsabhängigkeiten untereinander entscheiden darüber, ob die Produktion läuft oder stockt.

Pegging als Beziehungsmanager

Mit dem sogenannten „Pegging", das wie ein Beziehungsmanager funktioniert, lassen sich die Abhängigkeiten aller Arbeitsplätze für jeden zu bearbeitenden Auftrag im Betrachtungszeitraum ermitteln. Das verflochtene Netzwerk der Fertigungsabläufe wird so „entwirrt" und aus unstrukturierten Einzelaufträgen entstehen logische und zusammenhängende Auftragsketten. Dieses Beziehungswissen bildet dann die Grundlage zur Berechnung des Produktionsplans.

Bis vor kurzem bot nur das Tool SAP Advanced Planning Optimization (SAP APO) die Pegging-Funktion. Doch inzwischen gibt es auch eine alternative, nativ in SAP integrierte Softwarelösung, die die Funktion unterstützt und das Beziehungswissen direkt aus dem SAP-System extrahiert.

Ausgeklügelter Produktionsfeinplan durch KI

Aber wie wird aus dem Wissen um die Beziehungen, Restriktionen und Verfügbarkeiten ein optimaler Produktionsfeinplan? Hier kommt künstliche Intelligenz (KI) ins Spiel. Mit Hilfe eines intelligenten Algorithmus lassen sich die Abhängigkeiten überprüfen und eine „machbare" Produktionsreihenfolge ermitteln. Ein geeignetes Tool ermittelt stetig weitere denkbare Produktionsfeinpläne, vergleicht die Qualität und wirft am Ende einen optimierten Plan aus. Dieser lässt sich dann ins SAP-System importieren und die betroffenen Aufträge werden gemäß ihrer neuen Reihenfolge umterminiert.

Unendliche Möglichkeiten – ein Plan

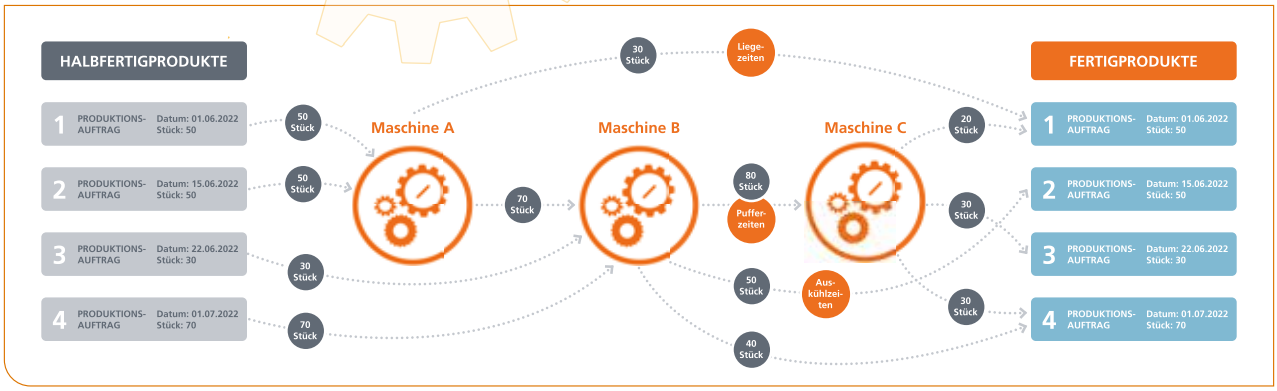
Möchte man zehn verschiedene Kabel mit einer Maschine produzieren, ergeben sich über 3,6 Millionen mögliche Reihenfolgen. Die Wahrscheinlichkeit, dass ein Mensch hier zum idealen Planungsergebnis kommt, ist sehr gering. Eine ganzheitliche Produktionsreihenfolgeplanung erfordert daher die Unterstützung einer schlauen 2-in-1-Lösung, bestehend aus

#1 einem SAP-basierten Produktionstool inklusive Pegging-Funktion.

#2 einem „Optimierer", hinter dem ein komplexer, KI-basierter Algorithmus steckt.

Mit einer solchen Software ist es möglich, Produktionsstopps wirkungsvoll zu vermeiden, Termintreue sicherzustellen, Fertigungskosten zu senken und den CO_2-Ausstoß zu reduzieren.

Björn Dunkel, Lena Kulik
https://ifm-business-solutions.com



Schützen Sie Ihr SAP-System

BETRUG DURCH IBAN REPLACEMENT SCAM BLEIBT MEIST UNENTDECKT

Betrug und Scam werden immer raffinierter und nehmen stark zu. Große Unternehmen, die SAP einsetzen, stehen vor der Herausforderung, ihre sensiblen Daten und Zahlungsprozesse vor Betrügern zu schützen. Insbesondere das Ändern von IBAN-Daten in ERP-Systemen kann zu erheblichen finanziellen Verlusten führen, da Zahlungen versehentlich an betrügerische Dienstleister gesendet werden.

Um sicherzustellen, dass Ihr Unternehmen vor betrügerischen Aktivitäten geschützt ist, ist ein digitaler und widerstandsfähiger Geschäftsprozess notwendig. Die Frage ist, wie so ein Prozess in die bestehende SAP-Infrastruktur integriert werden kann, ohne das System anzupassen.

Auf Basis von SAP BTP und SAP Fiori haben wir eine App entwickelt, die den Prozess der IBAN-Änderung übernimmt und die sich leicht in das vorhandene SAP-System integrieren lässt. Diese smarte Lösung ermöglicht es Unternehmen, einen verlässlichen Schutz gegen betrügerische Aktivitäten zu etablieren.

Unsere Anwendung beinhaltet entscheidende Schlüsselfunktionen und bietet Ihnen folgende Vorteile:

#1 Sicherheit durch 4-Augen-Prinzip:
Eine Person kann notwendige Änderungen nicht autark vornehmen. Die SAP BTP (Business Technology Platform) bindet im Prozess immer mindestens eine zweite Person zur Überprüfung der Zahlungsänderungen mit ein. Für zusätzlichen Schutz werden die Benutzer durch eine Zwei-Faktor-Authentifizierung überprüft und für die Anwendung zugelassen.

#2 Einbindung von Dienstleistern:
Um sicherzustellen, dass die Änderungen der IBAN-Informationen legitim sind, bindet unsere App den betreffenden Dienstleister aktiv in den Prozess ein. Dem Dienstleister wird ein Code per Post zugesendet, den er in der Anwendung zur Verifizierung eingeben muss. Dadurch wird eine zusätzliche Sicherheitsebene geschaffen und das Risiko von betrügerischen Manipulationen minimiert.

#3 Effizient und S/4 Cloud-Ready:
Die Anwendung auf SAP BTP Basis wird als Software-as-a-Service (SaaS) in die vorhandene Fiori-Umgebung eingebunden, ist sofort im SAP Fiori Launchpad verfügbar und benötigt keine Anpassung am bestehenden System.

Investieren Sie in den Schutz Ihres Unternehmens und Ihrer Finanzprozesse. Mit der SAP Fiori Anwendung können Sie Betrug und Scam-Methoden wirkungsvoll bekämpfen. Als SAP Entwicklungs- und Hosting Dienstleister stehen wir Ihnen mit unserem Fachwissen und unserem Support zur Seite. Sprechen Sie uns an und lassen Sie uns gemeinsam die Sicherheit Ihrer Unternehmensdaten gewährleisten.

WIIT
THE PREMIUM CLOUD

90 PROZENT DER DEUTSCHEN UNTERNEHMEN SIND BEREITS OPFER VON CYBER-KRIMINALITÄT GEWORDEN*

* Bitkom Research 2022

DER SCHADEN BELÄUFT SICH AUF ÜBER 200 MILLIARDEN EURO PRO JAHR. DIE SICHERHEIT SENSIBLER ZAHLUNGSDATEN IST VON ENTSCHEIDENDER BEDEUTUNG FÜR UNTERNEHMEN. MIT DER ABBILDUNG EINES WIDERSTANDSFÄHIGEN GESCHÄFTSPROZESSES AUF BASIS VON SAP FIORI KÖNNEN SIE IHRE FINANZPROZESSE ABSICHERN.

Jan Svacina, Director SAP Development & Hosting, WIIT, www.wiit.cloud

ERP-Sicherheit

SOMM-**ERP**-AUSE? – NICHT FÜR HACKER!

Hacker haben die Angewohnheit, genau dann zuzuschlagen, wenn die Arglosigkeit am größten ist: an Feiertagen, aber auch in der Feriensaison. Und die allgemeine unbeschwerte Sommerlaune gepaart mit dünn besetzten IT-Ableitungen ist wie eine Einladung für Angreifer. Umso wichtiger ist es, dass Unternehmen das ganze Jahr über ihre geschäftskritischen Anwendungen, allen voran ERP-Systeme wie SAP, adäquat schützen und optimal auf potenzielle Attacken vorbereitet sind.

#1 Bedrohungen frühzeitig erkennen und reagieren

Spezialisierte Threat Detection and Response Tools ermöglichen es, Sicherheitsereignisse zu zentralisieren und potenzielle Bedrohungen in der SAP-Landschaft frühzeitig zu erkennen und zeitnah darauf zu reagieren.

#2 Das große Ganze im Blick behalten

Bedrohungsakteure sind in der Lage, sich agil durch Netzwerke zu bewegen, um Daten zu sammeln oder Anwendungen zu manipulieren. Unternehmen sollten daher über Prozesse und Lösungen verfügen, um die gesamte SAP-Landschaft abzusichern.

#3 Kritische Assets identifizieren

Das Problem ist, dass Unternehmen sich heute zwar häufig über die Kritikalität ihres ERP bewusst sind, aber nicht wissen, welche spezifischen Geschäftsprozesse von SAP unterstützt werden und welche Wechselwirkungen bestehen.

#4 Bewertung von Risiken und Schwachstellen bei kritischen Assets

Wenn klar ist, wo im Unternehmen sich kritische Daten und Prozesse befinden, ist es an der Zeit, diese zu bewerten. Dies funktioniert am besten mit einem speziellen Schwachstellen-Scanner für ERPs, der Auskunft darüber gibt, welche konkreten Risiken und Schwachstellen die verschiedenen Komponenten betreffen.

#5 Einspielen der neuesten Sicherheitspatches

Jedes Unternehmen sollte einen Prozess zur Bewertung, Analyse und Priorisierung von SAP-Sicherheitshinweisen implementieren und Sicherheitspatches so schnell wie möglich umsetzen.

#6 Verfeinerung von Business-Continuity-Plänen

Backups kritischer Anwendungen sind eine wichtige reaktive Maßnahme. So können sie im Fall einer Ransomware-Attacke den Unterschied ausmachen, ob ein Unternehmen Lösegeld zahlen muss oder nicht, und Ausfallzeiten deutlich reduzieren.

#7 Überwachung von Änderungen in Custom Code

Die Fähigkeit, böswillige Änderungen an Custom Code und Konfigurationen zu erkennen, kann die Wahrscheinlichkeit von Infektionen durch externe Angreifer verringern und das Risiko eines erfolgreichen Angriffs deutlich minimieren.

#8 Mehrstufige Sicherheitsmodelle

Bei einem sogenannten „Defense-in-Depth"-Ansatz werden Sicherheitslösungen auf mehreren Sicherheitsebenen – physisch, technisch und administrativ – implementiert, um zu verhindern, dass Bedrohungsakteure etwa in ein geschütztes Netzwerk vordringen.

#9 Security-Awareness fördern

SAP-Nutzer sollten für die verschiedensten Angriffstaktiken sensibilisiert werden und bei der Verwendung ihrer Firmengeräte zu Wachsamkeit aufgerufen werden – vor allem wenn dies Remote oder im Kontext einer „Workation" geschieht.

#10 Mit Threat Intelligence neue Einblicke und Erkenntnisse gewinnen

Threat Intelligence-Programme liefern zeitnah aufschlussreiche Informationen über die aktuellen Taktiken und Techniken von Bedrohungsakteuren. Sie warnen frühzeitig vor neuen Ransomware-Kampagnen und bieten Gegenmaßnahmen und Handlungsvorschläge für die IT-Sicherheitsteams, die die Entwicklung und Implementierung von Sicherheitskontrollen verantworten.

www.onapsis.com


BUSINESS IS
SMOOTH SAILING
WITH ESKER
DSAG-Jahreskongress:
Treffen Sie uns
an Stand P6
#PositiveSumGrowth
WWW.ESKER.DE
SAP Partner
ESKER

ERP-Umstellung von SAP-Systemen bis 2027

DAS MÜSSEN IT-ENTSCHEIDER BEI DER MIGRATION BEACHTEN

ERP-Systeme sind das Rückgrat jedes Unternehmens. Gerade deshalb stellt eine ERP-Umstellung oder Änderung für Unternehmen eine riesige Herausforderung dar: Die Umstellung von SAP ECC auf S/4HANA ist für Unternehmen eine unausweichliche Aufgabe, die sie bis 2027 umsetzen müssen. Denn zu diesem Zeitpunkt werden ältere Systeme nicht mehr von SAP unterstützt. Die Umstellung auf S/4HANA betrifft sowohl direkt als auch indirekt sämtliche Unternehmensbereiche und -prozesse – angefangen bei der Finanzabteilung über den Vertrieb, die Beschaffung bis hin zu HR und Corporate Governance. SAP S/4HANA ist die vierte ERP-Generation von SAP und löst das bisherige SAP ERP ab. Die neue integrierte Business Suite basiert auf der In-Memory-Datenbank SAP HANA. HANA ist die In-Memory Datenbanktechnologie von SAP und dient als digitaler Kern, der Kunden dabei hilft, die digitale Transformation im gesamten Unternehmen voranzutreiben.

> UM DIE RICHTIGE S/4HANA BETRIEBSART ZU ERMITTELN, SOLLTEN UNTERNEHMEN EINE GRÜNDLICHE ANALYSE IHRER AKTUELLEN SITUATION UND ANFORDERUNGEN DURCHFÜHREN.
>
> **Adrian Trickett,**
> **Vice President EMEA, Boomi,**
> **https://boomi.com/de/**

Es ist essentiell zu erkennen, dass die Umstellung auf SAP S/4HANA nicht nur ein IT-Projekt ist, sondern eine umfassende Transformation des gesamten Unternehmens darstellt, da diese den gesamten Geschäftsbetrieb betrifft. Unternehmen stehen somit vor einer der anspruchsvollsten Herausforderungen der kommenden Jahre. Doch diese Veränderung bietet die besondere Chance, das eigene Unternehmen zu digitalisieren, gleichzeitig für die Zukunft zu rüsten und eine nachhaltige Neuausrichtung zu ermöglichen.

Die richtige S/4HANA Betriebsart finden

Um die richtige S/4HANA Betriebsart zu ermitteln, sollten Unternehmen eine gründliche Analyse ihrer aktuellen Situation und Anforderungen durchführen. Die Unterstützung von externen Berater oder SAP-Dienstleistern kann hier hilfreich sein, um eine fundierte Entscheidung zu treffen. Die Wahl der richtigen Betriebsart ist entscheidend für den Erfolg der S/4HANA-Umstellung und die zukünftige Leistungsfähigkeit des Unternehmens.

Daher gibt es verschiedene Faktoren, die bei der Auswahl berücksichtigt werden sollten:

Zum einen sollte das Unternehmen seine langfristigen Geschäftsziele und -anforderungen sorgfältig analysieren und vorab definieren. Die S/4HANA Betriebsart sollte dabei mit der Unternehmensstrategie und den Zielen in Einklang stehen. Die Größe und Komplexität des Unternehmens spielen außerdem eine erhebliche Rolle bei der Wahl der geeigneten Betriebsart. Kleine und mittlere Unternehmen bevorzugen eher die Cloud-basierte Lösung, während größere Unternehmen mit spezifischen Anforderungen möglicherweise die On-Premise-Option in Betracht ziehen werden. Die Entscheidung ist auch eine Frage der Verfügbarkeit interner IT-Ressourcen und des Knowhows im Umgang mit S/4HANA. Die Cloud-Lösung wird oft von SAP selbst gehostet, während die On-Premises-Variante eine umfassendere interne IT-Unterstützung erfordert. Unternehmen, die strenge Sicherheits- und Compliance-Anforderungen haben, müssen dies bei der Entscheidung ebenfalls berücksichtigen. Einige Branchen, wie das Gesundheits- oder Finanzwesen, haben spezielle Vorschriften, die die Auswahl der Betriebsart maßgeblich beeinflussen können. Die Unterstützung von externen Experten und Beratern mit Erfahrung in entsprechenden Change-Projekten kann hierbei wertvoll sein.

Eine weitere Frage ist, ob das bestehende SAP ECC-System mit seinen Daten und Einstellungen einfach umgestellt werden soll. In manchen Fällen ist es sinnvoll, ein völlig neues ERP-System aufzusetzen, damit die zukünftige Komplexität der IT-Infrastruktur reduziert wird. Dabei gibt es zwei Ansätze: Mit dem Greenfield-Ansatz wird das ERP-System komplett neu aufgesetzt. Das kann sinnvoll sein, um eine über viele Jahre gestiegene Komplexität durch ein schlankes System abzulösen. Mit dem Brownfield-Ansatz wird das

bestehende ERP-System unter Beibehaltung aller Daten und Einstellungen konvertiert. Welcher Weg der Richtige ist, hängt in erster Linie von der Größe und Komplexität des bestehenden ERP-Systems ab.

ERP und EDI

Obwohl der Migrationsprozess von einem bestehenden ERP-System zu SAP S/4HANA technische Herausforderungen mit sich bringt, ermöglicht er auch den Übergang zu fortschrittlicheren, cloudbasierten EDI-Infrastrukturen. Dafür kann es sein, dass ältere EDI-Implementierungen möglicherweise nicht die technischen Spezifikationen von SAP S/4HANA erfüllen, insbesondere bei lokal gehosteten EDI-Konvertern. Für Unternehmen, die auf die S/4HANA Cloud-Architektur setzen, ist eine Integration mit einer cloudbasierten EDI-Lösung technisch am zweckmäßigsten, da eine lokale SAP-Instanz zur EDI-Konverter-Anbindung fehlt.

Die Entscheidung, ob ein Wechsel zu einer cloud-basierten EDI-Lösung empfehlenswert ist oder ob man ein älteres EDI-System behalten sollte, hängt von verschiedenen Faktoren ab. Der Wechsel zu einer cloud-basierten EDI-Lösung ist empfehlenswert, wenn das Unternehmen einen Wachstum erwartet oder saisonale Schwankungen im Geschäft zu verzeichnen sind, bei denen eine cloud-basierte EDI-Lösung die Skalierbarkeit und Flexibilität bietet, um sich den Anforderungen anpassen zu können. Auch die Komplexität der Implementierung kann eine entscheidende Rolle spielen. Cloud-basierte Lösungen können in der Regel schneller implementiert werden, da sie nicht die gleiche Hardware- und Infrastrukturkonfiguration wie On-Premises-Systeme erfordern. Auch der dezentrale Zugriff ist ein Faktor, der sich vorteilhaft für einige Branchen erweist. Cloud-EDI ermöglicht den Zugriff von überall, was die Zusammenarbeit mit Partnern und Kunden erleichtern kann, insbesondere in globalen Lieferketten. Da Cloud-Anbieter ihre Plattformen regelmäßig aktualisieren, wird der Zugriff auf die neuesten EDI-Funktionen und -Funktionserweiterungen ermöglicht.

Das Halten eines älteren EDI-Systems hingegen ist empfehlenswert, sofern das bestehende EDI-System stark in die internen Geschäftssysteme integriert ist. Eine umfassende Änderung eines seit langem bestehenden EDI-Systems mit vielen Abhängigkeiten könnte zu erheblichen Unterbrechungen und Ausfallzeiten führen. Hinzu kommt, dass bestimmte Branchen strengen Sicherheitsanforderungen und -standards unterliegen, die mit einer Cloud-basierten Lösung möglicherweise nicht erfüllt werden können, daher bietet sich hier nur die On-Premises Lösung an. Nicht zuletzt sind interne Kapazitäten und Kompetenzen notwendig, um die Kontrolle über das EDI-System zu behalten.

Mit Plan und Partnern zum Erfolg

Letztendlich erfordert eine erfolgreiche ERP-Umstellung eine sorgfältige Planung, eine enge Zusammenarbeit mit den Stakeholdern, eine solide technische Umsetzung und eine angemessene Unterstützung für die Mitarbeiter während des gesamten Prozesses.

Intelligente Integrations- und Automatisierungsplattformen können umfassende Werkzeuge bereitstellen, die bei erforderlichen und anstehenden SAP-Migrationsprozessen helfen.

Adrian Trickett

SAP S/4HANA

„BOOSTER" FÜR DIE DIGITALE UNTERNEHMENSTRANSFORMATION

Die Migration nach SAP S/4HANA bietet die Chance, interne Prozesse neu zu denken und effizienter zu gestalten. Sie legt damit eine wichtige Grundlage für die digitale Unternehmenstransformation. Neue Funktionen und moderne Benutzeroberflächen vereinfachen die Nutzung von SAP-Applikationen. So lassen sich gerade im mittelständischen Umfeld völlig neue Potenziale heben.

Für SAP-Anwender stellt sich nicht mehr die Frage, ob überhaupt ein S/4HANA Transformationsprojekt durchgeführt werden soll, sondern vielmehr wann, wie und mit welchem Ziel. SAP bietet mit SAP Activate ein standardisiertes und umfangreiches Vorgehensmodell für die S/4HANA Transformation an. Doch oft fällt es insbesondere mittelständischen Unternehmen nicht leicht, einen auf ihren Bedarf angepassten Projektrahmen abzuleiten und hinsichtlich des finanziellen und zeitlichen Aufwands zu bewerten. Hier hilft ein strukturiertes, erprobtes Vorgehen, das den tatsächlichen Bedarf des Unternehmens widerspiegelt und den individuellen Anforderungen gerecht wird.

Die S/4HANA Transformation überschaubar machen

Viele Unternehmen wünschen sich eine transparente Methode, um ihr Transformationsprojekt hinsichtlich Kosten, Ressourcen und Laufzeit bewerten zu können. In der Praxis kommt es vor allem darauf an, ein auf die jeweilige Situation angepasstes Projekttemplate zur Verfügung zu stellen. Hier hilft das modulare Transformationsbaukasten-Modell.

Dabei handelt es sich um eine Methode, die auf den SAP Activate Elementen aufbaut, jedoch ein Template nutzt, das speziell auf mittelständische Unternehmen zugeschnitten ist. Alle Elemente beinhalten bereits eine vordefinierte Aufwand- und Zeitschätzung auf Basis erfolgreich abgeschlossener Projekte. Auch Rollen und Verantwortlichkeiten sind bereits entsprechend vorgedacht. So lassen sich Umfang und Dimensionierung aller relevanten Themen genau abschätzen. Das Besondere dabei ist, dass durch das Hinzufügen oder Entfernen einzelner Bausteine neue Varianten der Projektplanung einfach und schnell konfiguriert und auf diese Weise verschiedene Projektszenarien simuliert werden können.

Vorteile des Baukasten-Modells

Alle Elemente des Baukastens werden bereits vorselektiert ausgeliefert – als zwingend erforderlich, für mittelständische Unternehmen kaum relevant oder optio-

Quelle: SPIRIT/21

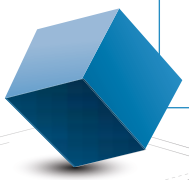
nal. Die optionalen Elemente legen dabei den Umfang des Projektverlaufs fest. Aus diesem Scope leitet sich toolgestützt automatisch eine Zeit- und Aufwandabschätzung ab. So können auf Basis der verschiedenen Rollen und Verantwortlichkeiten bereits frühzeitig Kapazitäten für das Projekt eingeplant werden.

Die Baukasten-Methode baut auf Praxis-Erfahrungen auf und konzentriert den Blick auf das Wesentliche. Die vorgegebene Struktur ermöglicht einen Überblick über die klar definierten Abhängigkeiten der einzelnen Bausteine, schafft Transparenz und erleichtert die Projektplanung. Die Vorauswahl und Priorisierung aller relevanten Themen beschleunigt die Planungsphase und reduziert Unsicherheiten. So wird das Projektdesign der S/4HANA Transformation überschau- und nachvollziehbar. Sich nur auf die technischen Aspekte der S/4HANA Transformation zu konzentrieren, reicht definitiv nicht aus.

Methodik allein reicht nicht

Ebenso wichtig ist es zu überlegen, welche prozessualen und organisatorischen Veränderungen den Umstieg begleiten und wie diese organisiert und gesteuert werden können. Das heißt konkret: Alle betroffenen Stakeholder sollten von Anfang an mit einbezogen und die Transformation durch entsprechende Change-Management-Maßnahmen begleitet werden. Dazu zählen das Engagement des Managements, eine klare Fokussierung auf das Projektziel und eine enge Verzahnung aller Projektbeteiligten.

Markus Wühr
www.spirit21.com



PRAXIS-TIPPS FÜR DEN UMSTIEG AUF S/4HANA:

Der Umstieg auf S/4HANA ist kein reines IT-Projekt. Treiber für Komplexität sind vor allem Veränderungen auf Prozess- und Organisationsebene.

Drei Schlüsselfaktoren für eine erfolgreiche S/4HANA-Transformation:

- eine klare Fokussierung auf das Projektziel
- Management Commitment und
- eine Change-Management-Beratung, die die Transformation in allen Phasen begleitet.

OB **S/4HANA** ODER **SAP IBP...**

...WIR MACHEN KURZEN PROZESS!

Und sorgen so für Effizienzsteigerungen in Ihrem Unternehmen.

Jürgen Löhle, Geschäftsführer der CONSILIO GmbH

Verpassen Sie nicht den Kundenvortrag von **TEEKANNE** am 20.9., 14:00 Uhr

Wir sind dabei! Stand H4

CONSILIO

DIE VORAUSDENKER.
DIE PROZESSOPTIMIERER.
DIE LÖSUNGSENTWICKLER.

SAP Gold Partner

Einsteinring 22 | 85609 Aschheim
T +49 89 9605750 | W www.consilio-gmbh.de

Enabler für Digitalisierung

UNTERNEHMEN BRAUCHEN SICHERHEIT UND SOUVERÄNITÄT

Ein Großteil der Unternehmen in Deutschland und der Europäischen Union (EU) tut sich nach wie vor schwer mit dem digitalen Wandel. Um gegenüber der internationalen Konkurrenz langfristig zu bestehen, ist technologische Souveränität ein entscheidender Faktor. Was dafür erforderlich ist, darüber sprachen wir mit Arved Graf von Stackelberg, CEO von DriveLock.

UNTERNEHMEN SOLLTEN SICH NICHT AUF SINGULÄRE SECURITY-MASSNAHMEN VERLASSEN, SONDERN AUF EINE MEHRSCHICHTIGE STRATEGIE SETZEN, DIE VERSCHIEDENE PRÄVENTIVE MASSNAHMEN VEREINT.

Arved Graf von Stackelberg, CEO, DriveLock SE, www.drivelock.com

it management: *Herr Stackelberg, was ist Ihrer Meinung nach das größte Hindernis für Digitalisierung in Deutschland?*

Arved Graf von Stackelberg: Das ist einfach: Ressourcenmangel – egal ob Budget, Personal, Zeit oder Knowhow. Etwa 99 Prozent der Unternehmen in der EU sind Kleinstunternehmen oder KMUs. Selbst wenn die Bereitschaft besteht Digitalisierungsprojekte umzusetzen, ist es für diese Unternehmen immer noch äußerst herausfordernd, angesichts der Komplexität des Themas und fehlender Ressourcen umfassend, schnell und sicher zu digitalisieren. Das bestätigt auch die aktuelle Studie der deutschen Industrie- und Handelskammer. Dabei spielt gerade der deutsche Mittelstand wegen seiner Innovationskraft eine wichtige Rolle in unserer Wirtschaft. Wir müssen die richtigen Rahmenbedingungen schaffen, damit möglichst viele Unternehmen den digitalen Wandel endlich vollziehen und von den Vorteilen neuer Technologien profitieren können.

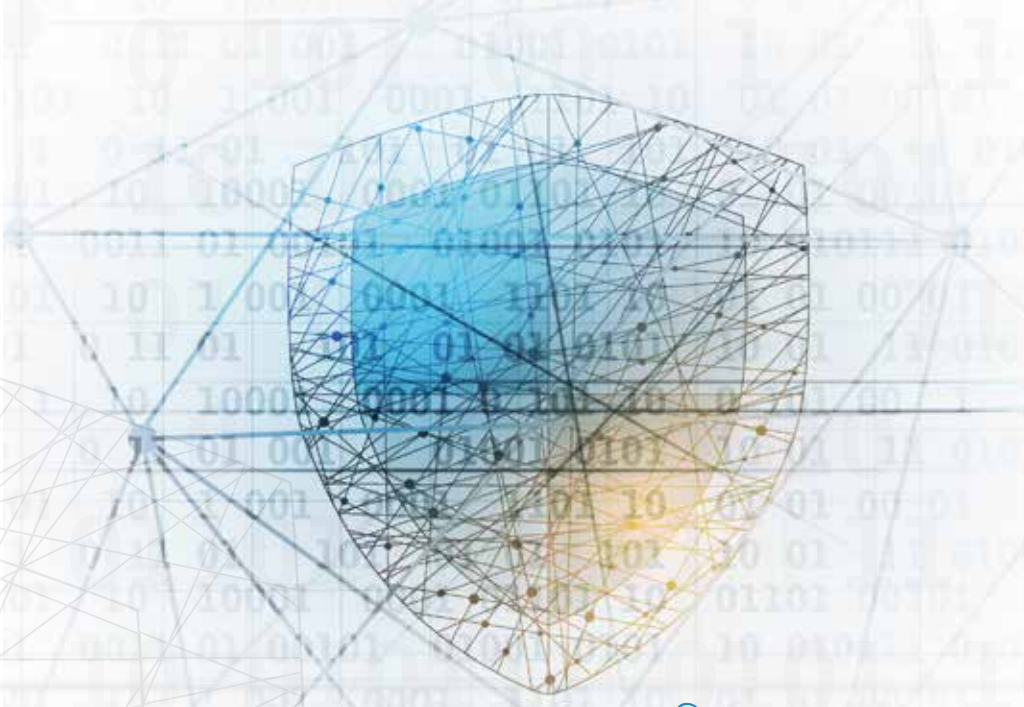
it management: *Wie sehen diese Rahmenbedingungen aus?*

Arved Graf von Stackelberg: Für mich als Security-Experte steht und fällt alles mit IT-Sicherheit. KMU sind für Cyberkriminelle ein lukratives Ziel, insbesondere die Innovationen der „Hidden Champions" sind Anreiz genug für Cyberspionage. Für eine starke Position im internationalen Wettbewerb ist konsequenter Cyberschutz die Basis jeglicher Digitalisierungsmaßnahmen. Lokale Cyber-Security-Anbieter aus Deutschland oder der EU bieten wertvolle Vorteile. Zum einen erfüllen sie bereits nationale und EU-weit geltende Richtlinien, wie zum Beispiel die Datenschutz-Grundverordnung. Das erleichtert es Unternehmen, Compliance-Vorgaben und ähnliches einzuhalten. Offerieren die Anbieter ihre Lösungen aus einer europäischen oder deutschen Cloud heraus, können kleine und mittelständische Unternehmen maximal effektive Sicherheit und Knowhow mit minimalem Ressourcenaufwand beziehen.

Besonders für Unternehmen mit wenig Ressourcen ist es enorm wichtig auf vorbeugende Cybersecurity-Lösungen zu setzen. Prävention zielt darauf ab, jeglichen Angriff außen vor zu lassen. Im Idealfall wird eine schadhafte Aktion so früh verhindert, dass das Entdecken und Reagieren gar nicht mehr nötig sind. Klassische Detection-and-Response-Lösungen entdecken verdächtige Aktivitäten und wehren diese im nächsten Schritt ab. Dieses Vorgehen bindet Ressourcen, weil es Monitoring und Reaktion erfordert.

it management: *Es macht natürlich Sinn, einen Angriff gar nicht erst durchdringen zu lassen, als ihn später mühevoll einzudämmen. Aber warum lesen wir eigentlich fast täglich von Cyberattacken auf Unternehmen, wenn es doch im Ansatz so einfach wäre?*

Arved Graf von Stackelberg: Auch Hacker setzen auf neue Technologien. Mit dem Einsatz künstlicher Intelligenz (KI) hat sich beispielsweise die Zahl an Malware-Varianten, die täglich neu in den Umlauf kommen, nochmals um ein Vielfaches erhöht. Angriffe werden immer besser. Phishing E-Mails haben inzwischen eine so hohe Qualität, dass sie nur noch schwer von legitimen Nachrichten unterschieden werden können. An dieser Stelle ist der Mensch oft das schwächste Glied in der Kette von Sicherheitsmaß-



nahmen. Unternehmen sollten ihre Belegschaft kontinuierlich und anlassbezogen für die Risiken sensibilisieren. Was heißt das konkret? Nutzt jemand zum Beispiel einen mobilen Datenträger, kann eine Pop-up-Meldung ad hoc über mögliche Risiken aufklären. Insgesamt gilt: Unternehmen sollten sich nicht auf singuläre Security-Maßnahmen verlassen, sondern auf eine mehrschichtige Strategie setzen, die verschiedene präventive Maßnahmen vereint.

it management: *Warum ist es aus Ihrer Sicht so wichtig, auf lokale Security Provider zu setzen?*

Arved Graf von Stackelberg: Eine gute und wichtige Frage. Und die Antwortet lautet Souveränität. Wie bereits erwähnt, bleiben bei Anbietern aus der EU die Daten auch in der EU. Daher bedeutet Lokalität echte Souveränität und mehr Unabhängigkeit vom Rest der Welt. Organisationen sollten immer die Kontrolle über ihre sensiblen Daten behalten und das funktioniert besser mit souveränen Lösungen. Das führt uns auch zum nächsten Aspekt der idealen Rahmenbedingungen für Digitalisierung. Aufgrund von Ressourcenmangel, sei es im Hinblick auf Personal oder auch Budget, sind Cloud-basierte Managed-Security-Lösungen die effektivste und gleichzeitig ressourcenschonendste Sicherheitslösung für viele Unternehmen.

it management: *Wir sehen, worauf Sie hinauswollen. Dafür braucht es eine souveräne Cloud.*

Arved Graf von Stackelberg: Richtig. Das Ziel ist es, Lösungen anzubieten, die maximale Sicherheit und Souveränität gewährleisten und vor allem schnell, einfach, effektiv und kosteneffizient einsetzbar sind.

Für echte Souveränität sollte die Security aus einer souveränen Cloud kommen. Dafür müssen Politik und Wirtschaft zusammenkommen und an einer unbürokratischen Umsetzung arbeiten. Zum Beispiel gibt es bereits eine erste Werkzeugkiste in der Gaia-X Initiative. Doch laut der aktuellen Studie vom eco – Verband der Internetwirtschaft e. V. und den Gaia-X Föderationsdiensten müssen Interessierte erst Unmengen an Material durcharbeiten und evaluieren, was sich letztlich negativ auf die Implementierung auswirkt. Hier kommen erneut die fehlenden Mittel von Kleinstunternehmen und KMU ins Spiel. Alles, was ressourcenintensiv ist, ist für diese Organisationen keine Option. Um die digitale Aufholjagd effektiv zu beschleunigen und weiterhin international wettbewerbsstark zu bleiben, sind Prozesse, Technologien und Angebote nötig, die Organisationen möglichst einfach und maximal sicher konsumieren können.

Dafür ist nicht nur eine souveräne Cloud nötig, sondern auch weitere lokale Allianzen oder Plattformen für technologische Souveränität in Deutschland und der EU. Wenn neben Cloud und Security auch die Kollaborations-, Netzwerk- und Datenverarbeitungslösungen aus dem EU-Raum kommen, stärkt es die souveränen Strukturen wesentlich. Dabei hilft es besonders auf lange Sicht, lokale Startups und Innovationstreiber zu fördern. Generell müssen sich innovative Tech-Unternehmen aus Deutschland und der ganzen EU aktiv zusammenschließen und gemeinsam ein international wettbewerbsstarkes Portfolio erarbeiten. Bei DriveLock arbeiten wir genau an solch einer umfassenden und souveränen Plattform für Security-Lösungen. Hier kooperieren wir bereits mit lokalen Partnern und suchen noch weitere Ergänzungen, mit denen wir die gesamte Wertschöpfungskette rund um Daten, Digitalisierung und IT-Infrastruktur abdecken können.

Zusammenfassend kann ich sagen: Wir brauchen starke, lokale Anbieter, die es der breiten Masse an Unternehmen in Deutschland und Europa ermöglichen, sicher und souverän zu agieren. Besonders KMU müssen die Digitalisierung ihrer Infrastrukturen und Geschäftsmodelle beschleunigen, um im internationalen Wettbewerb unabhängig bestehen zu können. Die aktuellen Entwicklungen zeigen eindeutig, dass die Nachfrage für ein souveränes Ökosystem an Technologie-Lösungen bereits besteht. Es fehlt nur noch das passende Angebot.

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

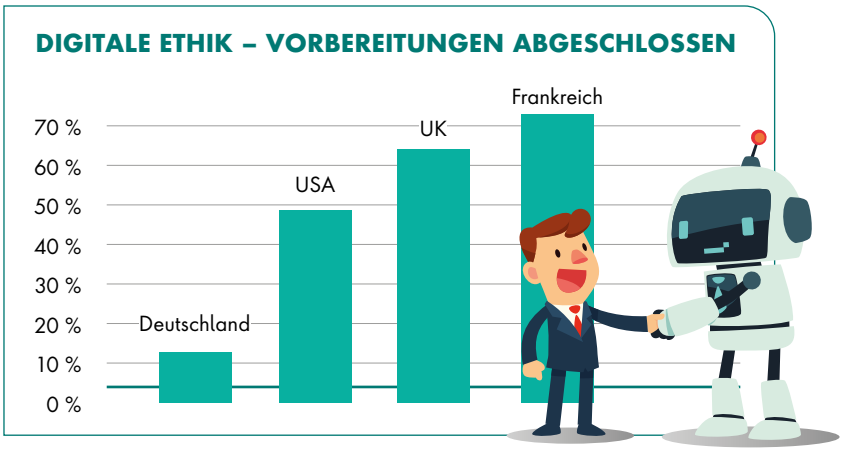
Verhaltener Optimismus?

KÜNSTLICHE INTELLIGENZ & DEUTSCHE UNTERNEHMEN

Die Unternehmen in Deutschland erwarten Umsatzzuwächse durch die Verwendung von Künstlicher Intelligenz (KI) – allerdings entsteht ein Spannungsfeld bei den dafür erforderlichen Investitionen.

Konkret erwarten in Deutschland 71 Prozent der Unternehmen, dass sie in den kommenden 18 bis 24 Monaten zusätzlichen Umsatz durch den Einsatz von KI erzielen können; weltweit stimmen dieser Einschätzung 46 Prozent zu, so dass hierzulande ein gewisser Optimismus vorzuherrschen scheint. Die erwarteten Zuwächse liegen jedoch noch in einem vergleichsweise überschaubaren Rahmen: Gemäß der Erhebung werden die lokalen KI-Anteile am Gesamtumsatz in einem Korridor von etwa fünf bis zehn Prozent erwartet. Diese relativ defensive Einschätzung fußt auch auf der Berücksichtigung der konjunkturellen Gesamtlage: 97 Prozent der in Deutschland Befragten gehen davon aus, dass das wirtschaftliche Umfeld inklusive Inflation Investitionen in digitale Lösungen einschränken wird; weltweit liegt diese Zahl bei 75 Prozent.

Der Finanzierungsfragen zum Trotz beschäftigen sich jedoch beinahe alle der in der Studie angesprochenen Unternehmen bereits mit begleitenden Vorarbeiten rund um Fragen der verantwortungsvollen KI-Nutzung, mithin dem Themenkreis der digitalen Ethik zuzuordnen. In Deutschland sehen sich allerdings nur 13 Prozent mit diesen Vorbereitungen am Ziel und sind bereits mit deren Implementierung beschäftigt, was mit Abstand den letzten Platz im Ländervergleich bedeutet: Der Grund hierfür dürfte gemäß der Zahlen in erster Linie das Fehlen einer dedizierten Person in entsprechender Verantwortung sein: In Deutschland gaben je die Hälfte der Unternehmen an, dass sich entweder die C-Level-Ebene – CIO, CTO etc. – oder ein Bereichsleiter des Themas annehmen. In etwa jedem achten Unternehmen der weiteren vorgenannten Länder sind hingegen dedizierte Ansprechpartner für „Responsible AI" vorhanden.



Risiken und Schäden durch KI

Gerade Deutschlands Unternehmen strotzen dabei auch regelrecht vor Selbstvertrauen, wenn es um die Frage geht, ob sie ihre Beschäftigten hinsichtlich des sicheren Einsatzes von KI gut vorbereiten: glatte 100 Prozent der Befragten bejahen dies, obwohl vielfach kein dedizierter Ansprechpartner vorhanden ist; zurückhaltender schätzen das etwa Organisationen in den USA ein, wo der zugehörige Wert mit 82 Prozent immer noch sehr hoch ist, vergleichbar mit dem Vereinigten Königreich mit 84 Prozent. Dass Wahrnehmung und Realität womöglich auseinanderdriften, zeigt ein weiterer Wert: 99 Prozent der in Deutschland befragten Unternehmen gaben an, dass sie ihre Belegschaft bereits zu einem verantwortungsvollen Umgang mit OpenAI und ChatGPT ermöglicht haben.

www.avanade.de

Innovative Arbeitsumgebungen

INTEGRIERT STATT ISOLIERT

Moderne Arbeitsplätze folgen keinem einheitlichen Standard. Längst wird die strikte Büropräsenz von hybriden, dezentralen Arbeitsumgebungen abgelöst. Erfolgsentscheidend für diesen Transformationsprozess ist, bestehende Unternehmensabläufe aus digitaler Perspektive zu überprüfen und eine durchdachte, nachhaltige Digitalstrategie zu fahren. Unterstützung bieten Dokumentenaustauschlösungen auf Basis von Unified Communications.

Die Pandemie hat unsere Art zu arbeiten grundlegend verändert. Damit innovative Arbeitsmodelle und hybride Organisationsformen gelingen, müssen Unternehmen auf eine digitale Verzahnung ihrer Prozesse setzen. Möglich wird dies unter Einsatz softwarebasierter Unified-Communications-Lösungen wie der OfficeMaster Suite des Berliner Herstellers Ferrari electronic. Diese lässt sich nahtlos in bereits vorhandene Groupware oder E-Mail-Clients integrieren, ermöglicht einen DSGVO-konformen, manipulationssicheren Dokumentenaustausch in IP-Umgebungen und legt die Basis für zahlreiche digital integrierte Prozesse. Verschiedenste Kommunikationsdienste werden in einer einheitlichen Arbeitsumgebung zusammengeführt und isolierte Strukturen aufgelöst. Selbst den Herausforderungen weltweit tätiger Unternehmen ist die Lösung gewachsen. Sie erfüllt den international gültigen ITU-Standard und stellt ein verlustfreies, hybrides Arbeiten auch bei global verteilten Standorten sicher.

Manipulationssicherer Datenaustausch

Den rechtssicheren Dokumentenaustausch realisiert die OfficeMaster Suite über den Standard Next Generation Document Exchange (NGDX). Dokumente gehen damit als PDF direkt und mehrfach verschlüsselt im E-Mail-Postfach des Empfängers ein. Formatierungen, Farben und selbst hohe Auflösungen bleiben erhalten. Potenziell schädliche, aktive Inhalte wie Hyperlinks oder Applikationen sind automatisch vom Transfer ausgeschlossen. Gerade weil es eine der Kernaufgaben von Unified Communications ist, die nahtlose Zusammenarbeit räumlich getrennter Teams sicherzustellen, muss der manipulationssichere und datenschutzkonforme Austausch von Dokumenten höchste Priorität haben. Die OfficeMaster Suite stellt dies über eine synchrone und asynchrone Verschlüsselung sicher. Der Austausch von Schlüsseln ist nicht mehr erforderlich, die Manipulationssicherheit der Dokumente wird durch integrierte Hashes erreicht. Sind diese beim Versender und Empfänger identisch, ist sichergestellt, dass das Dokument auf dem Versandweg nicht verändert wurde.

Der Motor moderner Arbeitswelten

Maßgeblich für vollständig automatisierte Prozesse ist, dass auch die Daten und Metadaten eines Dokuments übertragen und im Anschluss automatisiert ausgelesen und verarbeitet werden. Die OfficeMaster Suite legt auch hierfür die Basis. Gehen Dokumente ein, die nicht per NGDX übertragen wurden, werden diese per Optical Character Recognition (OCR) mit einem Textlayer zur Texterkennung versehen und so für die digitale Verarbeitung in Dokumentenmanagementsystemen vorbereitet. Auch gescannte oder abfotografierte Texte aus Upload-Portalen lassen sich auf diese Weise automatisiert extrahieren. Für ein nahtloses und medienbruchfreies Arbeiten im Wechsel zwischen Büro und mobilem Arbeiten sorgt eine neue Web-API-Komponente der OfficeMaster Suite. Sie ermöglicht es, 3rd-Party-Produkte wie den E-Post-Service der Deutschen Post auch remote anzusteuern.

Digitalisierung und Automation sind der Motor der modernen Arbeitswelt. Technische Unterstützung beim Transformationsprozess bieten innovative Unified-Communications-Lösungen wie die OfficeMaster Suite von Ferrari electronic.

www.ferrari-electronic.de

Ferrari electronic

Projekt-management

MIT DER RICHTIGEN STRATEGIE ZUM ERFOLG

Planisware wurde 1996 in Paris als Spin-off von Thales gegründet und wurde sehr früh international tätig.

Anlässlich des zwanzigjährigen Bestehens des Tochterunternehmens in München, sprechen wir mit Geschäftsführer Gilles Chêne über Erfolge, Herausforderungen und die Zukunft.

? **Carina Mitzschke:** *Herr Chêne, herzlichen Glückwunsch zu 20 Jahren Planisware Deutschland. Sie haben 2003 mit nur einem Mitarbeiter im Marketing die Münchner Niederlassung aufgebaut. Welchen Herausforderungen mussten Sie sich damals stellen?*

Gilles Chêne: Der Projektportfolio-Management (PPM)-Markt ist ein Referenzmarkt. Da wir in Deutschland weitestgehend unbekannt waren, konzentrierten wir uns zunächst auf die Pharmabranche, weil Planisware in Frankreich und den USA bereits Referenzkunden in diesem Segment hatte. Wir segmentierten den Pharmamarkt nach den Unternehmen mit den größten FuE-Budgets und der größten Anzahl an Mitarbeitern. Analog haben wir weitere Marktsegmente erschlossen, wie etwa die Automobilbranche. Heute nutzen unter den Top 500 Konzernen mit den weltweit größten Budgets für FuE-Projekte ein Drittel unsere Lösungen.

? **Carina Mitzschke:** *Was macht Ihren Erfolg aus und welche Rolle spielen die Mitarbeiter und Kunden bei der Gestaltung der Erfolgsgeschichte des Unternehmens?*

Gilles Chêne: Auch in Deutschland ist Planisware während der letzten 20 Jahren kontinuierlich gewachsen. Unsere 80 Mitarbeitenden in München haben das Know-how, langfristige Kundenbeziehung zu pflegen. Unser Unternehmen wird seit Jahren als verlässlicher Akteur wahrgenommen, die Kunden bleiben bei uns und unser stetiges Wachstum gibt ihnen Sicherheit. In allen Branchen ist es uns über die Jahre gelungen, zufriedene Referenzen mit besonderer Signalwirkung für den Markt aufzubauen. Zum Beispiel im Automotive-Bereich BMW, Conti, Porsche und Schaeffler oder bei Life Science Firmen wie etwa Biotronik, Boehringer, Fresenius oder Merck. Diese Referenzen unterstützen unsere Positionierung bei potenziellen Neukunden und bilden die Basis für das weitere Wachstum.

? **Carina Mitzschke:** *Planisware hat sich von Anfang an auf die Entwicklung und Bereitstellung von Lösungen für das Projekt- und Portfoliomanagement spezialisiert. Besonders in der Pandemiezeit eine spezielle Herausforderung?*

Gilles Chêne: Globale Kunden konnten mit unseren Lösungen zumindest die Auswirkungen bestimmter Risiken der Pandemie auf ihre Projekte simulieren, um die richtigen Portfolioentscheidungen zu treffen. Pharmahersteller wie AstraZeneca und Pfizer haben zu Beginn der Corona-Pandemie jeweils den komplexen Zulassungsprozess ihrer CoVID-19-Impfstoffe mithilfe ihrer Planisware-Lösungen beschleunigen können. Beide mussten im Eiltempo ihren Produktentwicklungsprozess auf den Kopf stellen und alle Möglichkeiten ausschöpfen, Projektphasen zu verkürzen oder zu parallelisieren.

Trotz Pandemie ist es uns in der Planisware-Gruppe gelungen, ein jährliches Wachstum von 20 Prozent aufrechtzuerhalten. Unsere Professional Service Organisation konnte weltweit mit den Kunden problemlos remote zusammenarbeiten. Sei es im Rahmen von Anforderungsworkshops, Kick-Off-Terminen oder Trainings.

? **Carina Mitzschke:** *Planisware Enterprise ist Marktführer bei Forrester und Gartner. Warum sind Ihre Lösungen so erfolgreich, was unterscheidet sie von herkömmlichen Lösungen am Markt?*

Gilles Chêne: Grundsätzlich wird der Markt für Projektmanagement-Software weltweit in den nächsten Jahren weiter stark wachsen. Wir sind auf dem Weg in die Project Economy und da sind Lösungen wie die von Planisware ein wichtiger Baustein. Es gibt keinen Verdrängungswettbewerb zwischen unterschiedlichen Lösungen, sondern es kommt eher darauf an, schneller als der Markt zu wachsen. Wir unterscheiden uns durch drei Kriterien:

1. Wir gewinnen mit Planisware Marktanteile in Branchen mit einem hohen Reifegrad im Projektmanagement und dementsprechend anspruchsvollen Anforderungen an ein Projektmanagement-Werkzeug.

2. Nur wenige Tools am Markt bieten so viel Branchen-Best-Practices, Flexibilität und Konfigurationsmöglichkeiten, so dass alle PPM-Workflows in Unternehmen abgebildet werden können.

3. Unsere Professional Services Teams sprechen die Sprache des Kunden. In Kombination mit den Vorzeigereferenzen in den einzelnen Branchen schafft dies Vertrauen in unsere Umsetzungsfähigkeit.

? **Carina Mitzschke:** *Warum bieten Sie zwei PPM-Lösungen unter einem Dach an?*

Gilles Chêne: Beide ergänzen sich. Während Planisware Enterprise hauptsächlich von großen und reifen Projektorganisationen genutzt wird, richtet sich Orchestra an den mittelständischen Markt oder eine einzelne Abteilung eines Konzerns. Die Anforderungen an Projektportfoliomanagement sind hier zwar grundsätzlich ähnlich, jedoch weniger komplex sowie einfacher und deutlich schneller zu implementieren.

Für Interessenten im Mittelstand ist das Implementieren von PPM-Lösungen meist neu. Viele Mittelständler verwalten ihre Projektportfolios noch mit herkömmlichen Excel- und Powerpoint-Tools, wodurch sie noch ziemlich ineffektiv arbeiten.

? **Carina Mitzschke:** *Software as a Service-Modelle dominieren immer mehr den Markt. Wie ist Planisware hier aufgestellt?*

Gilles Chêne: Unsere Cloud-Lösungen bieten wir komplett aus einer Hand, weil wir die Rechenzentren selbst betreiben. Wir sind ISO 27001 zertifiziert, um die Datensicherheit zu gewährleisten. Die Server für die europäischen Kunden stehen in Paris und München. Unsere US-Kollegen haben eigene SaaS-Datenzentren. Wir kümmern uns um Updates und Upgrades, sodass die IT-Ressourcen bei Kunden entlastet werden und stattdessen für strategische Aufgaben genutzt werden können.

? **Carina Mitzschke:** *Kommen wir noch einmal zu Planisware Orchestra. Die ganzheitliche Lösung ist, wie Sie sagten, hauptsächlich für den Mittelstand gedacht. Was zeichnet sie aus, was sind ihre Stärken?*

Gilles Chêne: Mittelständische Kunden haben weniger Erfahrung mit der Implementierung von Projektsoftware. Sie sind deshalb dankbar, wenn wir sie bis zur Einführung mit einer strukturierten Vorgehensweise einbinden. Das ist wichtiger als einzelne Softwarefeatures.

Wir setzen auf intensive Workshops mit einer anschließenden Testphase. Wir erarbeiten zusammen mit den Kunden Best Practices mithilfe zahlreicher Feedback-Schleifen. Das Ziel dieser Workshops sind in der Regel vier bis fünf Kernanforderungen. Dazu werden Benutzer und Schnittstellen hinzugefügt sowie idealerweise ein realer Prozess und drei bis vier Meilensteine eingebaut. Das Ganze wird dem Kunden für einen bestimmten Zeitraum als Testsystem in einem Cloud-Container zur Verfügung gestellt. Von unseren mehr als 20 neuen Orchestra-Kunden in den letzten drei Jahren in der GmbH haben alle diesen Prozess durchlaufen.

UNSER UNTERNEHMEN WIRD SEIT JAHREN ALS VERLÄSSLICHER AKTEUR WAHRGENOMMEN, DIE KUNDEN BLEIBEN BEI UNS UND UNSER STETIGES WACHSTUM GIBT IHNEN SICHERHEIT.

Gilles Chêne, Geschäftsführer, Planisware, https://de.planisware.com/

Neben der schnellen Implementierung erhalten Unternehmen eine Lösung, die den gesamten Projektlebenszyklus abbildet und eine hohe Anwenderakzeptanz aufweist. Sie sparen Zeit aufgrund automatisierter Berichte und verbessern den Informationsfluss sowie die abteilungsübergreifende Zusammenarbeit – all dies mit einem überschaubaren Budget.

? **Carina Mitzschke:** *Wie sieht Ihre Vision für die Zukunft aus? Welche Ziele hat Planisware* in den kommenden Jahren?

Gilles Chêne: Unsere Vision ist es, weiter zu wachsen und erfolgreich zu sein, wobei wir für Orchestra enormes Potenzial sehen. Wir kennen heute nur einen Bruchteil der mittelständischen Firmen im deutschsprachigen Raum.

! **Carina Mitzschke:** *Herr Chêne, wir danken für das Gespräch.*

IT-KOSTEN SENKEN

SIEBEN TIPPS FÜR IT-ENTSCHEIDER

Unternehmen suchen regelmäßig nach Wegen, um ihre IT-Kosten zu senken – denn nicht erst seit der Corona-Pandemie gehören technisches Equipment und Lizenzen zu den signifikanten Kostenfaktoren. Laut einer Studie des Marktforschungsunternehmens Gartner klettern die weltweiten IT-Kosten 2022 gegenüber dem Vorjahr um 5,5 Prozent auf 4,5 Billionen US-Dollar. Oft fließt jedoch deutlich mehr Geld als nötig in die Infrastruktur: Weil es an Prozessen zur Kostenoptimierung fehlt oder unklar ist, welche Bestandteile für effizientes Arbeiten verzichtbar sind und welche nicht. IT-Kosten nachhaltig zu senken, ohne dabei einen reibungslosen Betrieb aufs Spiel zu setzen, ist möglich, wenn Arbeitsprozesse sinnvoll an die Sparmaßnahmen angepasst werden können.

Dazu ist ein strategischer Ansatz erforderlich. Im Kern geht es darum, die notwendige IT für einen reibungslosen und effizienten Betrieb zur Verfügung zu stellen. Dabei gilt es, nötige von unnötigen Investitionen zu unterscheiden und Prioritäten für den Einsatz des Budgets zu setzen.

In diesem Whitepaper lernen Sie sieben Tipps, die IT-Entscheidern dabei helfen, Prozesse zu optimieren und unnötige Kostenfaktoren zu beseitigen.

WHITEPAPER DOWNLOAD

Das Whitepaper umfasst 8 Seiten und steht kostenlos zum Download bereit.

www.it-daily.net/download

Zusammenarbeit ist der Schlüssel für erfolgreiche Unternehmen – und zwar unabhängig vom Ort.

Hybride Arbeitsmodelle

MITARBEITER BENÖTIGEN EINE PROFESSIONELLE AUSSTATTUNG, UM EFFIZIENT ZU SEIN

Hybride Arbeitsmodelle haben sich in den letzten drei Jahren durchgesetzt: Angestellte arbeiten flexibler als jemals zuvor – egal, ob im Büro, im Home-Office oder unterwegs. Laut einer Studie von IDC setzen 62 Prozent der Unternehmen auf hybride Arbeitsmodelle – im Jahr 2021 waren es nur 38 Prozent. Zwei Drittel (63 Prozent) geben an, dass sie dadurch produktiver geworden sind. Die überwiegende Mehrheit der Befragten (89 Prozent) sind der Meinung, dass sie so Wohlbefinden der Mitarbeiter steigern können.

Allerdings bremsen Budgetbeschränkungen und hohe Anschaffungskosten der IT die Transformation des Arbeitsplatzes zunehmend und spürbar aus. Denn oftmals bedeuten hybride Arbeitsmodelle Investitionen in Monitore, Drucker und Accessoires wie Mäuse oder Tastaturen – und zwar im Büro wie auch im Home-Office. Gerade kleine und mittelständische Unternehmen (KMU) sehen sich hier höheren Ausgaben gegenüber und suchen nach Lösungen, hybride Arbeitsmodelle anzubieten, gleichzeitig aber die Kosten für die Ausstattung möglichst niedrig zu halten.

Dabei geht es nicht nur um Hardware und Software, sondern auch um Security in hybriden Arbeitsumgebungen. HP trägt dem mit HP Wolf Security Rechnung – Sicherheitslösungen, die ab Werk direkt in die Endgeräte integriert sind. Damit sind Anwender ebenso vor Angriffen von Cyber-Kriminellen geschützt wie auch die sensiblen Unternehmensdaten. Doch Firmen kommt es natürlich auch darauf an, wie leistungsfähig und nachhaltig die genutzten Endgeräte sind – Drucker sind keine Ausnahme.

Drucken auch weiterhin wichtig in Unternehmen

Denn auch bei hybriden Arbeitsmodellen sind Drucker wie die Serien HP Color LaserJet 4200/4300 sowie HP Color LaserJet Enterprise 5000/6000 und X500/X600 weiterhin wichtig für die Mitarbeiter: Sie drucken laut einer Studie von YouGov im Auftrag von HP weiterhin Verträge, Präsentationen oder Angebote aus. Dies gilt nicht nur für Mitarbeiter in Großkonzernen, sondern auch in kleinen und mittelständischen Unternehmen, egal, wo sie arbeiten. Die HP Color LaserJet Geräte eignen sich bestens für den Einsatz in KMU und sind echte Multitalente.

Sie überzeugen aber nicht nur mit ihrer Leistungsfähigkeit, sondern auch in punkto Nachhaltigkeit. Die neue TerraJet Toner-Technologie benötigt 27 Prozent weniger Energie und 28 Prozent weniger Kunststoff. Auch bei der Verpackung wurde eingespart: Hier wurde der Kunststoffanteil um 78 Prozent reduziert. Diese Kombination aus Leistungsfähigkeit, Nachhaltigkeit und Kosteneffizienz unterstützt kleine und mittelständische Unternehmen dabei, ihren Mitarbeitern die besten Technologien für hybride Arbeitsmodelle zur Verfügung zu stellen – und gleichzeitig ihre Investitionen im Auge zu behalten. Das Ergebnis sind nicht nur zufriedene Mitarbeiter, sondern auch Unternehmen, die auch in Zukunft wettbewerbsfähig bleiben werden.

www.hp.com

1: HP Global Hybrid Working Survey, September 2022

2: HP calculations based on normalized ENERGY STAR® TEC data of HP print systems which use TerraJet Cartridges compared to predecessors. See hp.com/TerraJet/energysaving.

3: Plastic reduction of TerraJet cartridges calculated based on cartridge weight compared to predecessors. See hp.com/TerraJet/plasticreductions.

4: HP calculations based on normalized Energy Star® TEC data of HP LaserJet Pro and Enterprise series with HP TerraJet Cartridges compared to predecessors. See hp.com/TerraJet/energysaving

Digital X 2023

DIE WELT WIRD BESSER, ABER NICHT SICHERER

Die digitale Transformation ist von branchenübergreifenden Trends geprägt – sie lenken den Kurs der digitalen Entwicklung und bestimmen, wohin die Reise geht. Die aktuellen Megatrends definieren unter anderem die Zukunft der Arbeit neu; zudem beeinflussen sie unseren Umgang mit Natur und Umwelt. Und leider erhöhen sie auch unsere Anfälligkeit für Gefährdungen.

Die Digital X, Europas größte Initiative für digitale Transformation, ist ein recht zuverlässiges Trend-Barometer: Was auf der seit 2018 jährlich stattfindenden Digital X in der Kölner Innenstadt als Megatrend diskutiert wird, hat tatsächlich tiefgreifende Auswirkungen auf Wirtschaft, Gesellschaft und Umwelt. 2023 definiert die Digital X vier Megatrends:

- Connected Business,
- Sicherheit,
- Zukunft der Arbeit und
- Nachhaltigkeit und Verantwortung

Die Identifikation solcher dominanten Strömungen ist für Unternehmen von erheblichem Nutzen, denn dadurch erfahren sie viel über die Wünsche und Bedürfnisse von Firmenkunden und Endverbrauchern. Und wenn man weiß, was gefragt ist, kann man dieser Nachfrage zielgenau mit Produkten und Services begegnen.

Unternehmen, die die Megatrends kennen und bedienen, haben entsprechend gute Geschäftsperspektiven. Unternehmen, die die Trends nicht bedienen, verpassen eine große Chance. Und Unternehmen, die wissentlich oder unwissentlich gegen die Trends agieren, gefährden ihre Zukunft.

Connected Business

Das Konzept des Connected Business steht in enger Verbindung mit dem Internet der Dinge (IoT), da es verschiedene Geräte, Systeme und Technologien miteinander verknüpft. Durch diese Verknüpfung ergeben sich für Unternehmen ganz neue Möglichkeiten zur Steigerung der Produktivität, weil ein kontinuierlicher Informationsfluss zwischen Abteilungen, Menschen und Geräten nicht nur Zeit und Betriebskosten spart – er verbessert auch die User Experience. Beispiel Supply Chain Management: Unternehmen, die Connected Business in ihrer Logistik einsetzen und ihre Lagerhaltung unter Einbeziehung aktueller und prognostizierter Kundennachfragen mit ihren Liefe-

ranten vernetzen, können Lieferengpässe besser vorhersehen und ihnen frühzeitig entgegenwirken.

Sicherheit

Der vierte Megatrend – Sicherheit – ergibt sich beinahe zwangsläufig aus den drei anderen Trends: Je mehr Raum Digitaltechnik in unserem Alltag einnimmt, desto größer wird auch das Ausfallrisiko und das Risiko der missbräuchlichen Nutzung. So erhöht sich etwa die Gefahr von Cyber-Attacken signifikant: Immer mehr mittelständische Unternehmen – und auch Kliniken, Gemeindeverwaltungen und andere Institutionen – werden Opfer von Ransomware. Dies liegt zum einen daran, dass digitalen Sicherheitsvorkehrungen häufig nicht genug Bedeutung beigemessen wird, zum anderen aber auch daran, dass die Belegschaften mit der voranschreitenden Vernetzung überfordert sind. Das Leben in einer weitgehend digitalisierten Gesellschaft ist also einerseits komfortabel, andererseits ist es aber auch unsicher und fragil. Umso wichtiger sind da geeignete Sicherheitskonzepte. Diese müssen nicht nur in der Lage sein, komplette Lahmlegungen zu verhindern, sondern sie müssen auch dazu fähig sein, gefälschte Nutzerbewertungen, Fake News und Datendiebstahl zu unterbinden oder zumindest detektierbar machen.

Zukunft der Arbeit

Apropos unternehmerische Verantwortung: Diese haben die Firmen nicht nur im Hinblick auf das Wohl des Planeten, sondern auch im Hinblick auf das Wohl ihrer Mitarbeiterinnen und Mitarbeiter. Die Zukunft der Arbeit ist eng mit der unternehmerischen Verantwortung der Arbeitgeber verbunden – trotz einer Fülle von gesetzlichen Bestimmungen liegt es nämlich noch immer hauptsächlich an ihnen, ob bzw. in welchem Maße faire Arbeitsbedingungen herrschen. Warum aber ist die Zukunft der Arbeit dann ein digitaler Megatrend? Weil die Digitaltechnik ganz wesentlich zur Schaffung einer neuen Unternehmenskultur beitragen kann. Durch die Einbindung von KI und durch Werkzeuge wie VR-Brillen und Datenhandschuhe können viele Jobs „bequemer" gemacht werden. Das bedeutet nicht, dass die Beschäftigten dann künftig eine ruhige Kugel schieben können – es bedeutet vielmehr, dass man ihnen bessere Möglichkeiten zur Vereinbarkeit von Beruf und Privatleben anbieten kann. Flexible Arbeitszeiten, Remote Work und Job-Sharing: Das sind die Schlagworte, die im Zusammenhang mit dem Megatrend „Zukunft der Arbeit" im Raum stehen.

Nachhaltigkeit und Verantwortung

Connected Business hat aber nicht nur ökonomische, sondern auch ökologische Aspekte: Voll vernetzte Unternehmen können zum Beispiel Energie und Rohstoffe effizienter nutzen und dadurch die Umwelt schonen. Nie war das so wichtig wie heute, denn abgesehen von der eher abstrakten Gefahr des Klimawandels birgt ein allzu sorgloser Umgang mit den Ressourcen für Firmen auch die sehr konkrete Gefahr, dass sich Kunden von ihnen abwenden. Wer heute keine unternehmerische Verantwortung übernimmt, gerät im Wettstreit um Markanteile schnell ins Hintertreffen.

Fazit

Die derzeitigen digitalen Megatrends werden die Welt in vielerlei Hinsicht besser machen. Sie werden der Wirtschaft neue Geschäftsmöglichkeiten eröffnen, sie werden sie widerstandsfähiger gegen Krisen machen, und sie werden den Unternehmen bessere Umsätze bescheren – bei gesteigertem Arbeitskomfort. Die ständig wachsende Bedrohung durch Cybercrime, Datendiebstahl und absichtliche Desinformation erfordert allerdings eine umfassende Absicherung unserer digitalen Infrastrukturen.

Wir sind deshalb dazu aufgerufen, der voranschreitenden Digitalisierung mit Bedacht zu folgen. Natürlich sollten wir die neuen Möglichkeiten nutzen, um Nachhaltigkeit und soziale Gerechtigkeit zu fördern – aber wir sollten bei jeder digitalen Neuerung immer auch nach den dazu passenden Sicherheitsmechanismen fragen.

DIGITAL X 2023

20.-21. September in Köln

Sie wollen mehr über die aktuellen digitalen Megatrends erfahren? Auf der diesjährigen Digital X erwarten Sie Vorträge, Diskussionen und Präsentationen dazu. Die „Weltauwsstellung der Digitalisierung" findet jedes Jahr in Köln statt und ist das größte Digitalbranchen-Event in Europa. Es bietet Unternehmen und Organisationen die Möglichkeit, sich auszutauschen, sie zu vernetzen und sich über die neuesten Trends und Technologien der Digitalisierung zu informieren.
Highlights sind traditionell die Auftritte der eingeladenen Speaker: Über 250 Rednerinnen und Redner werden Vorträge halten, darunter auch Björn Ulvaeus, der Mitbegründer der berühmten schwedischen Band ABBA. Er sorgte 2022 mit virtuellen Kopien der ABBA-Bandmitglieder (den „Abba-taren") für Aufsehen. Des Weiteren wird Amy Webb, eine der bekanntesten Futuristinnen der Gegenwart und CEO des Future Today Institute, erstmals auf europäischem Boden live zu einem Publikum sprechen.

Tickets und einen Überblick über das Programm gibt es im Netz auf der Seite: **www.digital-x.eu/de/**

Entfesseltes Edge Computing

ENTWURF DER IDEALEN EDGE-LÖSUNG

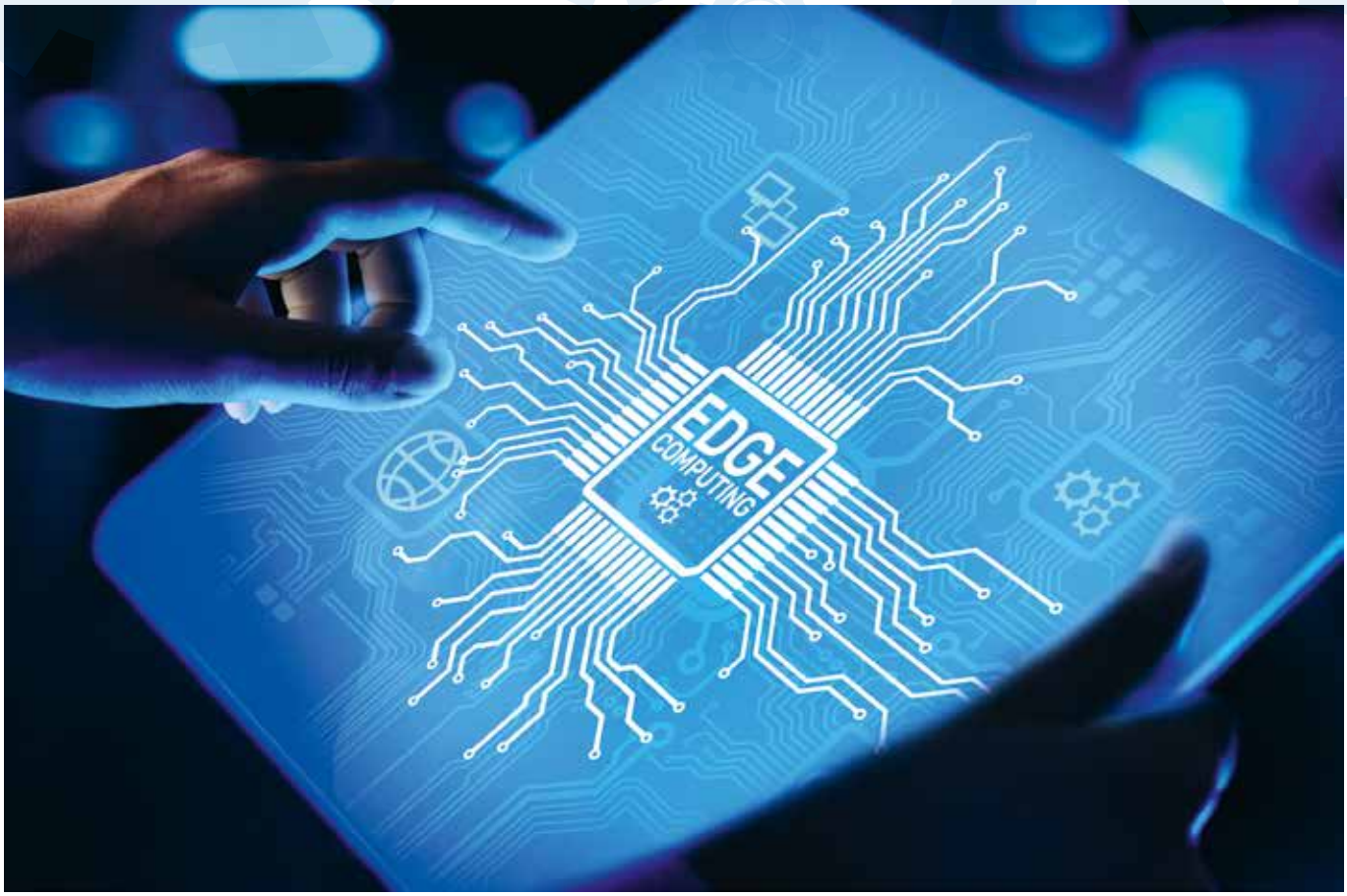
Edge Computing verändert die digitale Landschaft nachhaltig: Neben einer verbesserten User Experience bietet die Technologie auch geringere Latenzzeiten und mehr Sicherheit. Diese Veränderung geht mit einem signifikanten Wachstum einher. So rechnet das Marktforschungsunternehmen IDC bis 2025 mit einem jährlichen Wachstum von 16,4 Prozent verglichen mit dem Wert im Jahr 2022 – allein für den europäischen Markt. Die Verbindung von Edge Computing mit 5G, IoT und KI ermöglicht schnelle Datenverarbeitung, leistungsstarke Analysen und vernetzte Erfahrungen. Daher expandiert der Markt für digitale Edge-Rechenzentren schnell.

Unternehmen müssen mehrere Komponenten bei der Wahl ihrer Edge-Standorte berücksichtigen, um das volle Potenzial erschließen zu können. Dazu zählen neben dem optimalen Edge-Rack auch geeignete Strategien zur Integration der bestmöglichen Stromversorgungs- und Kühlsysteme sowie zur Implementierung effektiver Verwaltungsstrategien. Wie tragen Unternehmen dafür Sorge, dass ihre Edge-Standorte den Anforderungen einer höheren Verarbeitungsleistung von IT-, Speicher- und Netzwerkgeräten gerecht werden?

Die ideale Edge-Lösung

Wer versucht, sich hier an eine Blaupause zu halten, wird jedoch schnell an die Grenzen des Lösbaren kommen, denn: Es gibt keine Universallösung. Vielmehr müssen stets die individuellen Bedürfnisse und die unterschiedlichen Umgebungen beim Aufbau eines geeigneten Edge-Rack- oder Mikro-Rechenzentrums berücksichtigt werden. Faktoren wie Stromverteilung, Backup-Systeme oder Temperatur- und Feuchtigkeitskontrolle variieren von Standort zu Standort. Nur wenn alle Aspekte fachgerecht in die Planung und Implementierung mit einbezogen werden, können optimale Performance und Zuverlässigkeit gewährleistet werden.

Nachdem die Computer- und Speichertechnologie immer näher an den Kunden heranrückt, wird die Notstromversorgung wichtiger denn je. Unterbrechungsfreie



Stromversorgungssysteme (USV) rücken dabei immer mehr in den Fokus. Sie ermöglichen eine kontinuierliche und zuverlässige Stromversorgung und gewährleisten selbst bei neuen Spitzenanwendungen Geschäftskontinuität während Stromausfällen. Dadurch schützen sie Daten, Software und Hardware von Unternehmen und wahren wertvolle Ressourcen. Zudem verhindern USVen kostspielige Ausfallzeiten. Der Einsatz moderner Lithium-Ionen-Batterien bringt dabei weitere Vorteile mit sich: Im Gegensatz zu herkömmlichen Batterien verfügen sie über die doppelte Lebensdauer und müssen daher seltener ausgetauscht werden. Da sie deutlich höheren Temperaturen standhalten und signifikant schneller wieder aufgeladen werden können, eignen sich Backup-Systeme mit Lithium-Ionen-Batterien besonders gut für Edge- und verteilte IT-Umgebungen.

Gerade an kleinen Edge-Standorten kann eine Leistungsdichte von gerade einmal 2 kW bereits genug Wärme erzeugen, um IT-Systeme nachhaltig zu beeinträchtigen. Deswegen sind spezielle Kühllösungen essenziell, um eine angemessene Temperatur und Luftfeuchtigkeit gewährleisten zu können. Perimeterkühlung, In-Rack-Kühlsysteme und Wärmetauscher an der rückseitigen Tür des Gehäuses sind allesamt effektive Optionen, die eine effiziente Temperaturregulierung bei optimaler Raumnutzung ermöglichen.

Edge: Effiziente Verwaltung und Sichtbarkeit

Wurden die entsprechenden Komponenten ausgewählt, müssen Unternehmen als nächstes die Verwaltung ihrer Edge-Rechenzentren priorisieren. Nur so können sie gewährleisten, dass sie die Kontrolle über ihre stetig wachsende Edge-Präsenz behalten und sich nicht in Fallstricken verheddern. Dies erfordert einen strategischen Ansatz, der eine gründliche Vorbereitung des jeweiligen Standorts auf das wachsende Datenvolumen miteinschließt.

Grundvoraussetzung dafür ist, sich einen umfassenden Überblick über die unterschiedlichen IT-Geräte im Edge-Ökosystem zu verschaffen und so die Infrastruktur besser verwalten zu können. Dafür müssen Unternehmen ihre Ressourcen, basierend auf diesen Einsichten, auf Mitarbeiter mit entsprechendem Fachwissen aufteilen, die sich in solchen Systemen zurechtfinden. So können Probleme proaktiv gelöst und das Risiko von Ausfallzeiten minimiert werden.

Darüber hinaus kann eine zentralisiertes IT-Managementsystem eine entscheidende Rolle bei der Rationalisierung von Prozessen spielen und eine sichere, standardisierte wie auch automatisierte Verwaltung von Edge-Netzwerken ermöglichen. Durch diese Konsolidierung wird es für Unternehmen möglich, eine größere betriebliche Effizienz, eine geringere Komplexität und eine bessere Kontrolle über ihre Edge-Infrastruktur zu erreichen.

Ferndiagnose und -wartung

Edge-Standorte sind naturgemäß oft schwer zu erreichen oder gelten als sogenannte „Dark Sites" – das heißt, sie sind so konzipiert, dass sie ohne menschliches Eingreifen funktionieren. Ausfallzeiten an solchen Standorten können jedoch schwerwiegende Folgen haben und sogar zu einer Unterbrechung der Bereitstellung digitaler Produkte oder Dienstleistung für Kunden führen.

Aus diesem Grund sollten Unternehmen Fernwartungssysteme implementieren, die potenzielle Ausfälle an unbemannten Edge-Standorten bestenfalls bereits im Vorfeld proaktiv erkennen und beheben können (Stichwort: Predictive Maintenance). Solch robuste Diagnosesysteme ermöglichen es, Status und Performance einer Edge-Infrastruktur in Echtzeit zu überwachen und sich anbahnende Probleme zu beheben, bevor sie sich zu größeren Störungen entwickeln.

Ein permanent aktives wie vernetztes Out-of Band-Management erfordert weniger physische Eingriffe und beschleunigt Lösungsprozesse. So wird die Anfälligkeit des Ökosystems signifikant verringert und ermöglicht es Unternehmen darüber hinaus, die allgemeine Widerstandsfähigkeit und den kontinuierlichen Betrieb kritischer Dienste sicherzustellen.

WER GLAUBT, EINE 08/15-EDGE-LÖSUNG IMPLEMENTIEREN ZU KÖNNEN, WIRD SCHNELL AN DIE GRENZEN DES MACHBAREN STOSSEN. DIE ANFORDERUNGEN AN EIN EDGE-RACK- ODER MIKRO-RECHENZENTRUM SIND SO INDIVIDUELL WIE SPEZIFISCH. EINE UNIVERSALLÖSUNG GIBT ES NICHT.

Andrea Ferro,
VP Technology Application and Market Development, Vertiv,
www.vertiv.com

Fazit

Edge Computing bietet vielfältige Möglichkeiten für die digitale Transformation, aber alles beginnt mit strategischen Entscheidungen in der Aufbauphase. Mit den richtigen Maßnahmen und Tools können Unternehmen ein starkes Management, eine effektive Diagnose und eine schnelle Lösung von Problemen mit IT-Geräten an allen Edge-Standorten sicherstellen. Gelingt es, die jeweiligen Standorte und das Ökosystem gleichzeitiger Bereitstellung der gewünschten Reaktionsfähigkeit und Betriebszeit zu gewährleisten, gehen Unternehmen einer erfolgreichen Phase in der Ära des Edge-Computing entgegen.

Andrea Ferro

Shared Responsibility

DIE POTENZIALE DER CLOUD VOLL AUSSCHÖPFEN

Die zunehmende Cloud-Nutzung führt dazu, dass Unternehmen auch ihre Sicherheitslandschaft neu gestalten müssen. Existieren On-Premises- und Cloud-Umgebungen nebeneinander, führt dies zu Herausforderungen, die nur eine identitätsbasierte Sicherheitsstrategie, ein konsolidiertes Sicherheitskonzept und Security-Tools aus der Cloud lösen können.

Cloud-first- oder Cloud-too-Strategien liegen im Trend. Immer mehr Unternehmen verlagern Geschäftsanwendungen zu Cloud-Plattformen und -Services, um ihre digitale Transformation zu beschleunigen. Doch dieser Schritt bedeutet nicht nur mehr Agilität und Effizienz, sondern verändert auch die Angrifssfläche für Cyberattacken. Sicherheitskonzepte mit bloßem Perimeterschutz auf Netzwerkebene und Firewall-Lösungen funktionieren nicht mehr.

Die Sicherheit in der Cloud ist allerdings nicht die alleinige Aufgabe des Providers. Vielmehr gilt das Prinzip der „Shared Responsibility": Der Nutzer kümmert sich um Berechtigungs- und Zugriffsverwaltung und die Sicherung der Daten („Security in the Cloud"); der Provider sichert die Infrastruktur („Security of the Cloud").

Eine Analyse der Ausgangssituation ist die Basis, um die Sicherheitsmaßnahmen an die neue IT-Struktur anzupassen. IT-Teams sollten bei diesem Check unbedingt prüfen, ob die existierenden Security-Prozesse zur hohen Geschwindigkeit in der Cloud passen. Die vorhandenen Security-Kontrollen müssen zudem die veränderte Angriffsfläche abdecken und auch Attacken auf die Cloud-Management-Konsolen abwehren. Trotz aller Sicherheitsmaßnahmen muss immer mit erfolgreichen Angriffen gerechnet werden. Daher ist außerdem ein konsolidierter Überblick über die Security aller Umgebungen essentiell in Form eines Cyber Defense Center. Schließlich muss der CISO nicht nur – wie vorher –den abgeschotteten On-Premises-Bereich im Blick haben, sondern auch die neuen Netzwerkgrenzen in der Cloud.

Sicherheitsansatz für Identitäten-Vielfalt

Erst nach dieser Analyse wird sich herausstellen, welche Sicherheitsvorkehrungen

Bei der Migration in die Cloud müssen Unternehmen auch die Sicherheitskonzepte anpassen, um die veränderte Angriffsfläche zu schützen. (Quelle: Pixabay)

am dringlichsten sind. Am wichtigsten für die Cloud-Nutzung ist normalerweise das Identitäts- und Rechtemanagement, denn die Vielzahl an menschlichen und maschinellen Identitäten mit den dazugehörigen Berechtigungen sind ein potenzielles Sicherheitsrisiko. Der neue Sicherheitsansatz sollte also auf Identitäten basieren und User, Systeme, Anwendungen und Prozesse gleichermaßen und vollumfänglich berücksichtigen. Die IT-Abteilung muss an zentraler Stelle alle Berechtigungen verwalten, steuern und überwachen können und die Zugriffe auf administrative Oberflächen wie Cloud-Managementkonsolen und -portale strengstens regeln. Passende Sicherheitsmaßnahmen sind, neben der immer notwendigen Zweifaktor-Authentifizierung – zumindest für Rollen mit weitreichenden Rechten –, ein Rechte- und Rollenkonzept, und eine Access Governance, bei der die vergebenen Rechte regelmäßig überprüft werden.

DIE CLOUD-TRANSFORMATION IST FÜR VIELE UNTERNEHMEN EIN WICHTIGES ZIEL. ALLERDINGS IST DAS THEMA SICHERHEIT OFT NUR ZWEITRANGIG.

Martin Stemplinger, Security-Architekt mit Schwerpunkt Cloud Security und Managed Security Services, CGI, www.cgi.com/de

Security-Teams müssen umdenken

Die Erfahrung hat gezeigt, dass eine reine Eins-zu-eins-Übertragung von Anwendungen in die Cloud – also ein Lift-and-Shift-Verfahren – nicht die erhofften Ergebnisse liefert. Die Migration sollte deswegen sehr gut geplant werden und nicht nur eine Umstellung auf moderne IT-Architekturen mit Containern, Serverless-Computing und Cloud-nativen Plattformen umfassen, sondern auch der Sicherheitsumgebung. Security-Teams müssen also umdenken. Sie sind nicht mehr nur für das Netzwerk verantwortlich, sondern sollten auch Kompetenzen in der Anwendungsentwicklung haben und Security bereits in die Entwicklung integrieren. Solche möglichst automatisierten Security-Tests sind ein großer Vorteil für Softwareentwicklungsprozesse, weil Fehler früher entdeckt werden und sich so die Produktqualität erhöht ohne Entwicklungsgeschwindigkeit einzubüssen.

Wildwuchs in Sicherheitsinfrastruktur vermeiden

Die Cloud-Transformatione ist für viele Unternehmen ein wichtiges Ziel. Allerdings ist das Thema Sicherheit nach Erfahrung von CGI meistens nur zweitrangig. Resultat ist daher häufig eine heterogene Sicherheitsinfrastruktur aus Lösungen, die entweder die On-Premises-Umgebung oder die Cloud-Infrastruktur abdecken. Doch solch ein Wildwuchs ist schwer zu verwalten und zudem teuer. Außerdem laufen Unternehmen Gefahr, dass die Security-Verantwortlichen bei der komplexen Struktur Sicherheitslücken übersehen. Ziel muss deswegen eine Konsolidierung der Sicherheitsmaßnahmen sein, die Berechtigungen, Firewall-Regeln, Virenscanner, Security-Monitoring oder SIEM-Systeme für die komplette Cloud- und On-Premises-Landschaft vereinheitlicht.

Bevor Unternehmen nun in neue Sicherheitslösungen investieren, sollten sie zuerst das Potenzial nutzen, das in der Cloud selbst liegt. Schließlich bieten viele Cloud-Provider auch gleich die passenden Security-Tools, die sich zudem deutlich einfacher konfigurieren lassen als in einer On-Premises-Umgebung. Ein Beispiel ist das Identity Management; ein wichtiges Element für die Cloud-Security. Cloud-Provider stellen als Service in der Regel eine Rollenbasierte Zugriffskontrolle (Role Based Access Control – RBAC) zur Verfügung. Hier können IT-Verantwortliche sehr leicht definieren, welche User, Maschinen und Services Berechtigungen erhalten.

Gleiches gilt für die Umsetzung von Least-Privilege-Prinzipien mit Just-in-Time-Zugriffsmethoden. Sie ist zwar prinzipiell auch on-premises möglich, aber aufwändig und mit teilweise hohen Kosten für die erforderlichen Tools verbunden. Auch das Unterteilen des Netzwerkes in kleinere Subnetzwerke – also die Netzwerksegmentierung – ist ein effektives Sicherheitstool, das Unternehmen in der Cloud deutlich leichter umsetzen können als On-Premises. Die Cloud erlaubt sogar eine Microsegmentierung, bei der zum Beispiel festgelegt wird, welche Server miteinander über welches Protokoll kommunizieren dürfen.

Automatisierung entlastet Security-Teams

Die Nutzung von Security-Tools aus der Cloud hat aber nicht nur technologische Vorteile. Die Automatisierung entlastet zudem Security-Teams und ist daher ein wichtiges Mittel gegen den Fachkräftemangel. Anstatt Zeit mit manuellen Aufgaben zu verlieren, können sich IT-Experten auf andere Themen konzentrieren und haben mehr Kapazitäten frei.

Die Verlagerung von Anwendungen in die Cloud führt zu einer deutlich höheren Agilität und Flexibilität, mit der Unternehmen schnell auf neue Situationen reagieren und neue Geschäftschancen ergreifen können. Aber die Migration sollte Hand in Hand mit einer Neukonzeption der Security gehen. Die Cloud bietet dafür eigene Sicherheitstools, die ergänzend zur vorhandenen On-Premises-Sicherheit eine konsolidierte und stabile Umgebung schaffen. Die neue IT-Infrastruktur ist so nicht nur die optimale Basis für ein geschäftliches Wachstum, sondern stärkt auch die Abwehr von Bedrohungen.

Martin Stemplinger

Blitzschnelle Cloud-Attacken

ANGREIFERN REICHEN BEREITS 10 MINUTEN

Laut dem neuesten Bericht von Sysdig beträgt die durchschnittliche Zeit von der Aufklärung bis zum Abschluss eines Angriffs nur noch 10 Minuten. Unter Verwendung weltweiter Honeynets für den Global Cloud Threat Report 2023 hat das Sysdig Threat Research Team einige alarmierende Erkenntnisse erzielt: Angriffe in der Cloud geschehen mittlerweile so schnell, dass lediglich Minuten die Grenze zwischen ihrer Entdeckung und potenziell schweren Schäden bestimmen. Cloud-Angreifer machen sich genau die Vorteile zunutze, die Unternehmen überhaupt erst in die Cloud locken. Während Verteidiger ihren gesamten Software-Lebenszyklus schützen müssen, müssen Angreifer nur ein einziges Mal richtig liegen. Unglücklicherweise macht die Automatisierung es ihnen sogar noch leichter.

Die wichtigsten Ergebnisse

Cloud-Automatisierung als Waffe: Cloud-Angriffe erfolgen schnell. Aufklärung und Entdeckung sind sogar noch schneller. Die Automatisierung dieser Techniken ermöglicht Angreifern, sofort zu handeln, wenn sie eine Lücke im Zielsystem entdecken. Ein Aufklärungsalarm ist der erste Hinweis darauf, dass etwas nicht in Ordnung ist; ein Entdeckungsalarm bedeutet wiederum, dass das IT-Team zu spät kommt.

10 Minuten bis zum Schaden: Cloud-Angreifer sind schnell und opportunistisch und benötigen nur 10 Minuten, um einen Angriff zu initiieren. Nach Angaben von Mandiant beträgt die durchschnittliche Verweildauer in Unternehmen 16 Tage, was die Geschwindigkeit der Cloud unterstreicht.

Eine 90 Prozent sichere Lieferkette ist nicht sicher genug: 10 Prozent aller fortschrittlichen Bedrohungen für die Lieferkette sind für Standardtools unsichtbar. Mit Hilfe von Umgehungstechniken können Angreifer bösartigen Code verstecken, bis das Image bereitgestellt wird. Die Identifizierung dieser Art von Malware erfordert eine Laufzeitanalyse.

65 Prozent der Cloud-Angriffe zielen auf Telekommunikationsunternehmen und Finanzdienstleister: Telekommunikations- und Finanzunternehmen sind reich an wertvollen Informationen und bieten die Möglichkeit, schnelles Geld zu verdienen. Beide Branchen sind attraktive Ziele für Betrugsversuche.

Global Cloud Threat Report 2023

„Die Realität ist, dass Angreifer gut darin sind, die Cloud auszunutzen. Sie sind nicht nur in der Lage, Skripte für die Aufklärung und die automatische Bereitstellung von Kryptowährungen und anderer Malware zu erstellen, sondern sie nutzen Tools, die die Macht der Cloud für gute Zwecke einsetzen, und verwandeln sie in Waffen. Ein Beispiel dafür ist der Missbrauch von Infrastructure-as-Code zur Umgehung von Schutzrichtlinien", so Michael Clark, Director of Threat Research bei Sysdig.

„Cloud-native Angreifer sind ‚Everything-as-code'-Experten und Automatisierungsfans, was die Zeit bis zum Eintreffen in den Zielsystemen erheblich verkürzt und den potenziellen Explosionsradius vergrößert. Mit Open-Source-Detection-as-Code-Ansätzen wie Falco können Blue Teams in der Cloud die Nase vorn haben", so Alessandro Brucato, Threat Research Engineer bei Sysdig.

https://de.sysdig.com

PLUS
Kostenloser Download der Studie hier: **http://bitly.ws/RTqI**

IT-Zufriedenheit

WIE SICH CLOUD-COMPUTING AUF DIE KUNDENZUFRIEDENHEIT AUSWIRKT

Erwartungen zu erfüllen oder zu übertreffen ist zentraler Bestandteil der Kundenzufriedenheit. Die Bedürfnisse Ihrer Melder zu kennen, ist kein einmaliger Vorgang, sondern bedarf dauerhafter Aufmerksamkeit. In der IT-Welt stehen Wartung und Verbesserung technologischer Komponenten im Vordergrund, während Informationen über die Kundenbedürfnisse manchmal untergehen.

Indem Sie die technologischen Voraussetzungen outsourcen, können Sie Zeit sparen und sich auf die Bedürfnisse Ihrer Melder konzentrieren. Cloud-Anbieter werden immer besser darin, IT-Dienstleister dabei zu unterstützen.

Innovation ohne Sorgen

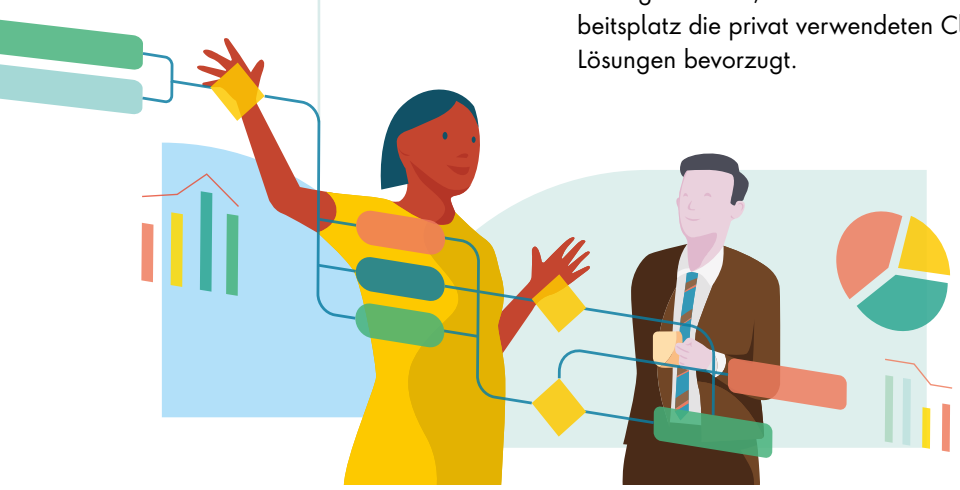
Verlegen Sie Anwendungen in die Cloud und geben somit Ihr technisches Management außer Haus, stellen Sie fest, dass Sie in der Vergangenheit viel mehr Zeit verloren haben, als Ihnen bewusst war. Anwendungen erhalten viel häufiger Aktualisierungen ohne Serviceunterbrechungen. Neue Funktionalitäten sind schneller verfügbar als bei interner Verwaltung.

Bei internem Management hinken Anwendungen teilweise mehreren Versionen hinterher. IT-Abteilungen verfügen nicht über die Zeit, alle verwendeten Anwendungen auf dem neuesten Stand zu halten. Indem Sie cloudbasierte Lösungen anbieten, sorgen Sie dafür, immer auf dem neuesten Stand zu sein.

Schritt-für-Schritt Aktualisierungen

Cloud-Anwendungen unterliegen einer kontinuierlichen Entwicklung, was bedeutet, dass kleine Changes an ihrer Funktionalität permanent getestet und implementiert werden. Im Gegensatz zum großen, überfälligen Update verhindern diese schrittweisen Changes, dass Melder sich plötzlich nicht mehr in ihren Anwendungen zurechtfinden. Diese Verbesserungen werden mit einer angemessenen Frequenz implementiert, sodass Melder problemlos mithalten können. Nutzer kennen diese kleinen Changes bereits von ihren Web-Anwendungen und Handy-Apps.

Seit der Verbreitung des Internets haben sich alle schnell an die Verfügbarkeit und Benutzerfreundlichkeit diverser Web-Services, wie Google, gewöhnt. Die Tendenz geht dahin, dass man auch am Arbeitsplatz die privat verwendeten Cloud-Lösungen bevorzugt.



IT-Provider sollten als Berater fungieren, indem sie Wissen und Benutzerhandbücher bereitstellen. Nur so können IT-Abteilungen ihren Meldern die IT-Umgebung bereitstellen, die sie tatsächlich erwarten.

Die Rolle des IT-Dienstleisters

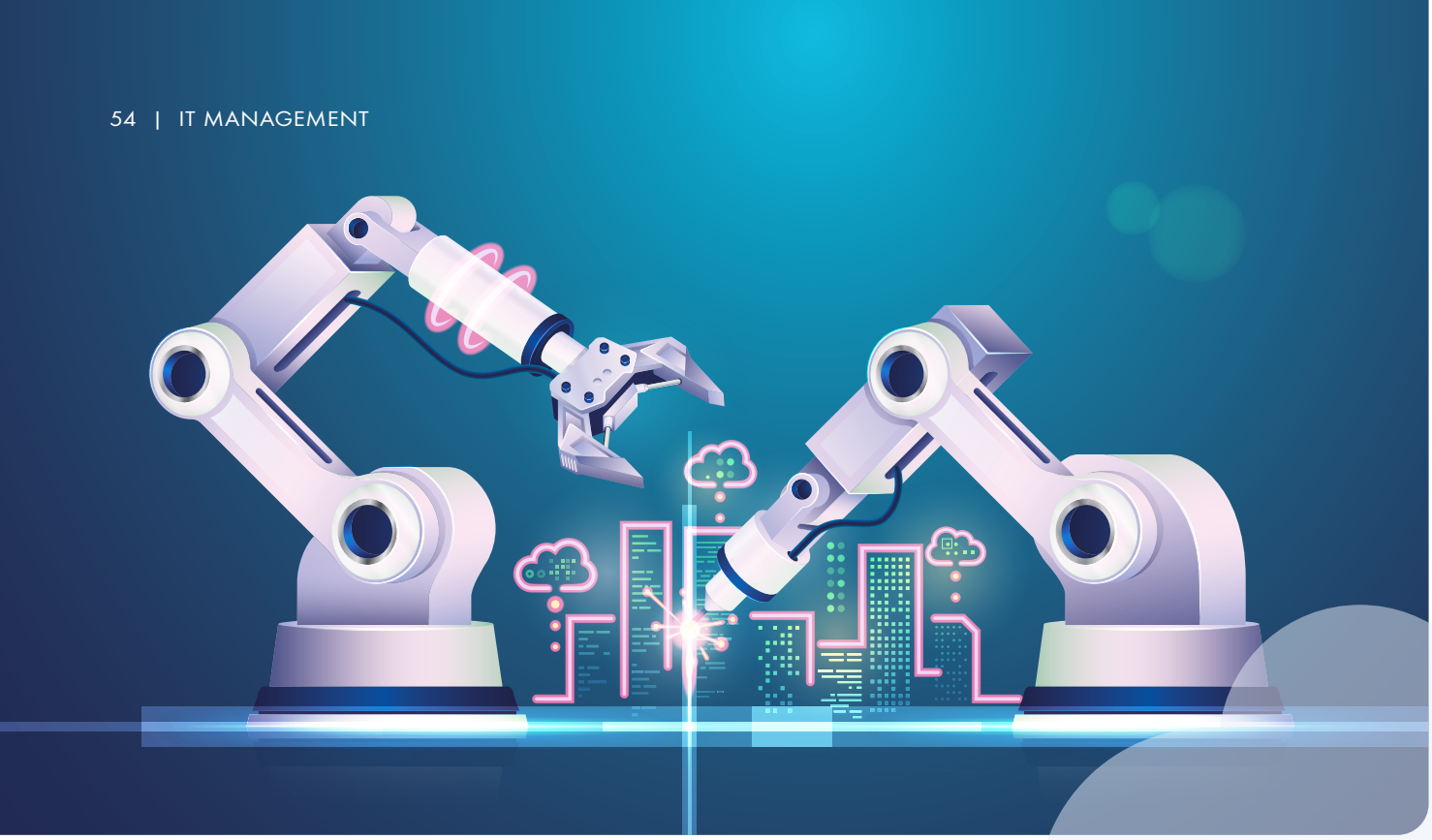
Organisationsspezifische IT-Services können ebenfalls Nutzen aus der Cloud ziehen. Die Cloud kann verwendet werden, um mehr Informationen zusammenzutragen. Big Data und künstliche Intelligenz verleihen dann IT-Services und Organisationen die Fähigkeit, bessere Ergebnisse zu erzielen und so eine größere Kundenzufriedenheit zu erreichen.

Sorglose Verwendung der Cloud?

Wie sorglos können Sie die Cloud verwenden? Wie sicher sind strategische Informationen in der Cloud? Beeinträchtigt die Cloud-Verwendung die Einhaltung der Gesetzgebung? Könnten Sie damit von Drittparteien abhängig werden?

Die Zufriedenheit eines Service Providers mit der Cloud hängt davon ab, inwieweit er der Cloud vertrauen kann. Daher ist es wichtig, die benötigten Bedingungen zu verstehen, damit Sie cloudbasierten Diensten vertrauen können. Cloud-Anbieter haben das verstanden – denn nachweislich zuverlässig zu sein, ist Teil ihres Geschäftsmodells. IT-Provider müssen sich in die Cloud einarbeiten, um die Bedürfnisse ihrer Melder erfüllen zu können. Jene, die sich jetzt gegen diese Einarbeitung sträuben, werden zukünftig größere Anstrengung aufbringen müssen, um eine hohe Kundenzufriedenheit zu erreichen.

www.topdesk.de



Industrial Intelligence as a Service

WIE DIE INDUSTRIE SICH MIT CLOUD-STRATEGIEN SMARTER STRUKTURIEREN KANN

Ob in Werkzeugen, Fahrzeugen oder intelligenten Maschinen: In einer modernen Produktionsstätte der Industrie 4.0 erfassen Sensoren sekündlich neue Daten. Anhand dieser können Ingenieure und Bediener die Fertigungsabläufe überwachen und bei Störungen im Idealfall rechtzeitig eingreifen. Das volle Potenzial der Daten schöpfen sie allerdings im Rahmen der bestehenden IT-Struktur nur selten aus. Der Schlüssel zur Maximierung des Wertes von Daten liegt darin, sie zugänglich zu machen, egal wo sie sich befinden. Damit brechen Unternehmen so genannte Datensilos auf, die häufig zu Komplikationen führen. Cloud-Lösungen sind ein zentraler Bestandteil davon und können signifikante Fortschritte in jeder Industrie, jedem Sektor und jedem Markt ermöglichen. Nach Schätzungen des Weltwirtschaftsforums beruhen etwa 70 Prozent des globalen Wirtschaftswachstums im nächsten Jahrzehnt auf digitalen Businessplattformen. Wer vor allem frühzeitig und umfassend in Cloud-Anwendungen investiert, wird maßgeblich von ihrer Belastbarkeit, Skalierbarkeit, Flexibilität und Geschwindigkeit profitieren.

Echte Wettbewerbsvorteile

Der Einsatz von Cloud-Anwendungen ohne einen strategischen Ansatz für die Datenkonnektivität ist jedoch kaum mehr als eine Anpassung an die allgemeine Marktentwicklung. Echte Wettbewerbsvorteile ergeben sich erst, wenn Unternehmen mithilfe passender Cloud-Software die Datensilos zwischen ihrer IT, der Anwendungs- sowie Konstruktionstechnologie beseitigen. Der Wert von (Industrie-)Daten vervielfacht sich, wenn verschiedene Bereiche des Unternehmens sie als gemeinsames Werkzeug nutzen. Dabei entsteht ein qualitativ hochwertiges Datennetzwerk, auch Digitaler Zwilling genannt. Dieser ermöglicht ein Echtzeit-Bewusstsein, das sich kontinuierlich weiterentwickelt und signifikant zum Geschäftserfolg von Industrieunternehmen beitragen kann.

Das daraus resultierende Datennetzwerk wird mithilfe Künstlicher Intelligenz kontextualisiert. Die digitale Verknüpfung aller vorhandenen Leistungs- und Prozessdaten in Verbindung mit KI-gestützter Auswertung bezeichnet AVEVA als Industrial Intelligence as a Service (IIaaS). Aus IIaaS resultieren zentrale Wettbewerbsvorteile für industrielle Akteure.

#1 Eine zentrale Informationsquelle für alle

Die meisten Industrieunternehmen agieren an unterschiedlichen Orten: Neben ihrer Verwaltung gibt es häufig eine oder mehrere separate Produktionsstätten entweder in Deutschland oder weltweit. Be-

sonders mit flexiblen Arbeitsmodellen kommt ein weiterer Faktor hinzu, der endgültig verdeutlicht, dass aktuelle, aber auch vergangene Daten unabhängig vom geografischen Standort der Mitarbeitenden verfügbar sein müssen. Damit sie optimal miteinander arbeiten und kommunizieren können, brauchen sie jederzeit Zugriff auf einheitliche Informationen beispielsweise von Planungsdokumenten oder den aktuellen Energieverbrauch eines konkreten Bestandteils im Fertigungsablauf. Cloudbasierte IIaaS-Anwendungen bieten ihnen hierfür eine praktikable Lösung und erlaubt ihnen zudem, durch die gezielte Einbindung von KI-Algorithmen den Wert der verfügbaren Daten weiterzuentwickeln. Das bedeutet, dass Mitarbeitende sowohl in der Entwicklungsphase als auch im laufenden Betrieb standortübergreifend denselben Informationsstand betrachten und mit diesem in Echtzeit arbeiten und auf Veränderungen reagieren können. Dass sie zeitgleich virtuell auf alle Dateien und Projektpläne zugreifen können, ermöglicht es Unternehmen, ihre Projekte effizienter und damit innerhalb der gesetzten Zeit- und Budgetrahmen zu realisieren.

So nutzt auch das Start-up Commonwealth Fusion Systems (CFS), eine Ausgründung des Massachusetts Institute of Technology, IIaaS. Seine Mitarbeitenden arbeiten remote und standortübergreifend an Lösungen, um mit Fusionsenergie eine unbegrenzte Energiequelle für den kommerziellen Markt verfügbar zu machen. In einer cloudbasierten Arbeitsumgebung können die Mitarbeitenden von CFS relevante 1D-, 2D- und 3D-Konstruktionsdaten teilen, damit sie gleichzeitig Anlagen entwickeln und bauen können. Dadurch haben die Planungen an Genauigkeit gewonnen, was wiederum Überarbeitungen überflüssig macht und die Projektlaufzeiten reduziert.

#2 Ein neues Level an Produktivität und Effizienz

Hybride, cloudbasierte Anwendungen erfassen, analysieren und visualisieren die Leistungs- und Prozessdaten von Produktionsanlagen. Sie machen damit nicht nur Informationen zugänglich, sondern aktualisieren auch die entsprechenden Arbeitsanweisungen im Unternehmen in Echtzeit. Industrielles Datenmanagement in Form von einer Cloud-Plattform ermöglicht Unternehmen, schnell zu reagieren und Produktionsprozesse sowie Anlagenleistungen anzupassen. Ein Cloud- und IIaaS-Ansatz, der auf industrielle Daten zugeschnitten ist, kann durch qualitativ hochwertige Informationen, Zusammenarbeit und datengesteuerte Erkenntnisse neue Level an Produktivität und Effizienz erreichen. Dieser Ansatz fördert somit schnellere, intelligentere Entscheidungen und eine gleichzeitig stets handlungsfähige Belegschaft. Somit verschaffen sich Industrieunternehmen durch Cloud-Anwendungen zusätzliche Wettbewerbsvorteile.

#3 Nachhaltiger dank Cloud-Anwendungen

In einer Zeit, in der Unternehmen zunehmend aufgefordert sind, einen positiven Beitrag zum Umweltschutz zu leisten, können cloudbasierte Tools eine wichtige Rolle bei der Unterstützung der Nachhaltigkeitsziele von Unternehmen spielen. Industrieunternehmen profitieren unter anderem von einer energieeffizienteren Infrastruktur, einem geringeren Ressourcenverbrauch und innovativeren Produktions- und Lösungsansätzen, die durch eine optimierte Datensammlung und -analyse entstehen.

Veolia Water Technologies ist ein transnationales, französisches Versorgungsunternehmen. Mit 3.548 Trinkwassergewinnungsanlagen versorgt das Unternehmen 98 Millionen Menschen in 67 Ländern weltweit mit Wasser. Um eine verlässliche, nachhaltige Wasserversorgung gewährleisten zu können, muss sich Veolia Water Technologies stets optimieren. Das Unternehmen setzt eine cloudbasierte Engineering-Plattform ein. Somit wird der betriebliche Einblick verbessert und die Prozesseffizienz gesteigert. Nach der Integration einer IIaaS-Cloud-Strategie setzte die flexiblere IT-Struktur in kurzer Zeit ein Fünftel der vorher blockierten Ressourcen frei. Durch die Verbesserung der grenzüberschreitenden internationalen Zusammenarbeit innerhalb der Belegschaft konnte das Unternehmen proaktiv neue Softwareanwendungen entwickeln, um auf die Bedürfnisse ihrer Kunden einzugehen. Zudem konnte Veolia mit der cloudgestützten Prozessoptimierung den Wasserverbrauch ihrer Kunden reduzieren und gleichzeitig benötigte Energie und Chemikalien einsparen.

EIN CLOUD- UND IIAAS-ANSATZ KANN DURCH QUALITATIV HOCHWERTIGE INFORMATIONEN, ZUSAMMENARBEIT UND DATENGESTEUERTE ERKENNTNISSE NEUE LEVEL AN PRODUKTIVITÄT UND EFFIZIENT ERREICHEN.

Awraam Zapounidis, Vice President Central & Eastern Europe, AVEVA, www.aveva.com

Fazit

IIaaS-Anwendungen werden in den kommenden Jahren wesentlich dazu beitragen, dass herkömmliche Hindernisse für kollaborationsgeprägte, skalierbare Geschäftsentwicklungen verschwinden. Der starke Netzwerkeffekt der verfügbaren Technologien sorgt für eine singuläre, seriöse Informationsquelle. Von der Versorgung bis hin zur Fertigung – basierend auf der IIaaS-Anwendung können Industrieunternehmen ihre Zusammenarbeit in den Mittelpunkt ihres Wirkens stellen, Innovationen fördern und zu einer effizienteren Zukunft beitragen.

Awraam Zapounidis

No-Code-Cloud

MOTOR DER DIGITALISIERUNG

Unternehmen werden nicht von Daten, sondern von Software angetrieben. Und die Cloud kann der Motor sein. Software und Cloud entscheiden heute mehr denn je über den Erfolg eines Unternehmens. Doch Cloud-Angebote und -Anwendungen unterscheiden sich stark voneinander und bleiben oft hinter den Erwartungen zurück.

Falsche Vorstellungen

Die Vorstellung, dass Cloud Computing Rechenleistung und Speicherkapazität wie Strom aus der Steckdose liefert, mag auf den ersten Blick einleuchten, ist aber irreführend. Während die Nutzung von Cloud-Anwendungen wie E-Mail oder Speicherplattformen für Privatpersonen oft einfach ist, stellt sie für Unternehmen häufig eine Herausforderung dar. Die geschäftliche Nutzung der Cloud kann genauso komplex sein wie die Nutzung herkömmlicher Software im eigenen Rechenzentrum, es sei denn, das Unternehmen verfügt über internes Fachwissen. Anwendungen für das Lieferkettenmanagement, die Produktentwicklung oder den Kundenservice können zwar problemlos in der Cloud betrieben werden, erfordern aber individuelle Anpassungen an die spezifischen Anforderungen des jeweiligen Unternehmens. Diese Anpassungen sind ein kontinuierlicher Prozess, der viel Zeit und Fachwissen erfordert. Beide Ressourcen sind derzeit knapp, insbesondere aufgrund des Fachkräftemangels. Laut Statista hat fast ein Drittel der Personalverantwortlichen Schwierigkeiten, DevOps-Spezialisten zu rekrutieren, und 68 Prozent der Unternehmen sehen die Notwendigkeit, die Fähigkeiten ihrer IT-Mitarbeiter zu verbessern.

DURCH DEN EINSATZ EINER NCC KÖNNEN DIE KOMPLEXEN PROZESSE IN DER SUPPLY CHAIN AUTOMATISIERT UND GESTEUERT WERDEN, WAS ZU EINER REDUZIERUNG DES FEHLERRISIKOS UND EINER STEIGERUNG DER GESAMTEFFIZIENZ FÜHRT.

Orli Shahidi,
Account Manager, Getronics Deutschland,
www.getronics.com

Steigerung der Effizienz durch neue Perspektiven und Ansätze

Die No-Code-Cloud (NCC) ist ein innovativer Ansatz im Bereich Cloud Computing, der sich diesen Herausforderungen stellt. Es handelt sich um eine Platform-as-a-Service-Lösung (PaaS) und ermöglicht es Benutzern, Anwendungen, Automatisierungen, Integrationen, Websites und Workflows ohne Programmierkenntnisse zu erstellen, bereitzustellen und zu verwalten. Die NCC nutzt in der Regel eine benutzerfreundliche Drag-and-Drop-Schnittstelle und andere visuelle Tools, die es auch Personen mit begrenzten technischen Kenntnissen erlauben, maßgeschneiderte Anwendungen zu entwickeln und Geschäftsprozesse eigenständig zu automatisieren.

Die Synergie zwischen Cloud- und No-Code-Technologien in einer solchen Lösung hat das Potenzial, Unternehmen grundlegend zu verändern und bietet eine Vielzahl konkreter Vorteile, die für Unternehmen aller Branchen von Nutzen sind.

Management von Lieferketten

Insbesondere die Verwerfungen der letzten Jahre mit Engpässen und Verzögerungen in den Lieferketten haben die Bedeutung eines zuverlässigen und flexiblen Supply Chain Managements deutlich gemacht. Nahezu alle Branchen waren von diesen Entwicklungen betroffen. Durch den Einsatz einer NCC können die komplexen Prozesse in der Supply Chain automatisiert und gesteuert werden, was zu einer Reduzierung des Fehlerrisikos und einer Steigerung der Gesamteffizienz führt. Besonders hervorzuheben ist, dass auch Mitarbeiter mit geringeren technischen Kenntnissen dazu in der Lage sind, bei Bedarf Änderungen an den Steuerungssystemen vorzunehmen.

Reif für den Markt?

No-Code-Plattformen ermöglichen es Teams, Anwendungen und Workflows schnell zu erstellen, bereitzustellen und zu verwalten, wodurch Zeit und Ressourcen für die Einführung neuer Projekte eingespart werden. Dadurch können Unternehmen, unabhängig von ihrer Branche, Produkte schneller auf den Markt bringen

und sich so einen Wettbewerbsvorteil gegenüber der Konkurrenz verschaffen.

Überwachung der Qualität

Entsprechende Plattformen bieten ferner die Möglichkeit, benutzerdefinierte Anwendungen zur Überwachung und Verwaltung von Qualitätskontrollprozessen zu erstellen. Dadurch können Unternehmen sicherstellen, dass ihre Produkte den höchsten Standards entsprechen. Insbesondere für Unternehmen, die regelmäßig neue Produkte entwickeln und auf den Markt bringen, ist die Anpassbarkeit der Qualitätskontrollmechanismen ein entscheidender Vorteil. Jedes Produkt erfordert spezifische Maßnahmen zur Gewährleistung seiner Qualität durch das Unternehmen, und No-Code-Lösungen ermöglichen eine flexible Anpassung genau dieser Prozesse.

Kosteneinsparungen

Der No-Code-Ansatz reduziert den Bedarf an technischen Spezialisten erheblich, da andere Teammitglieder Aufgaben übernehmen können, für die normalerweise Entwickler erforderlich wären. Dies führt nicht nur zu Einsparungen bei den Arbeitskosten, sondern auch zu einem geringeren Bedarf an Wartung und Support.

Skalierbarkeitspotenzial

Unternehmen können problemlos neue Anwendungen, Integrationen, Websites und Workflows entwickeln und implementieren, ohne zusätzliches technisches Personal einstellen oder in eine neue Infrastruktur investieren zu müssen. So können sie bei Bedarf schnell und effizient skalieren, um mit dem Unternehmenswachstum Schritt zu halten.

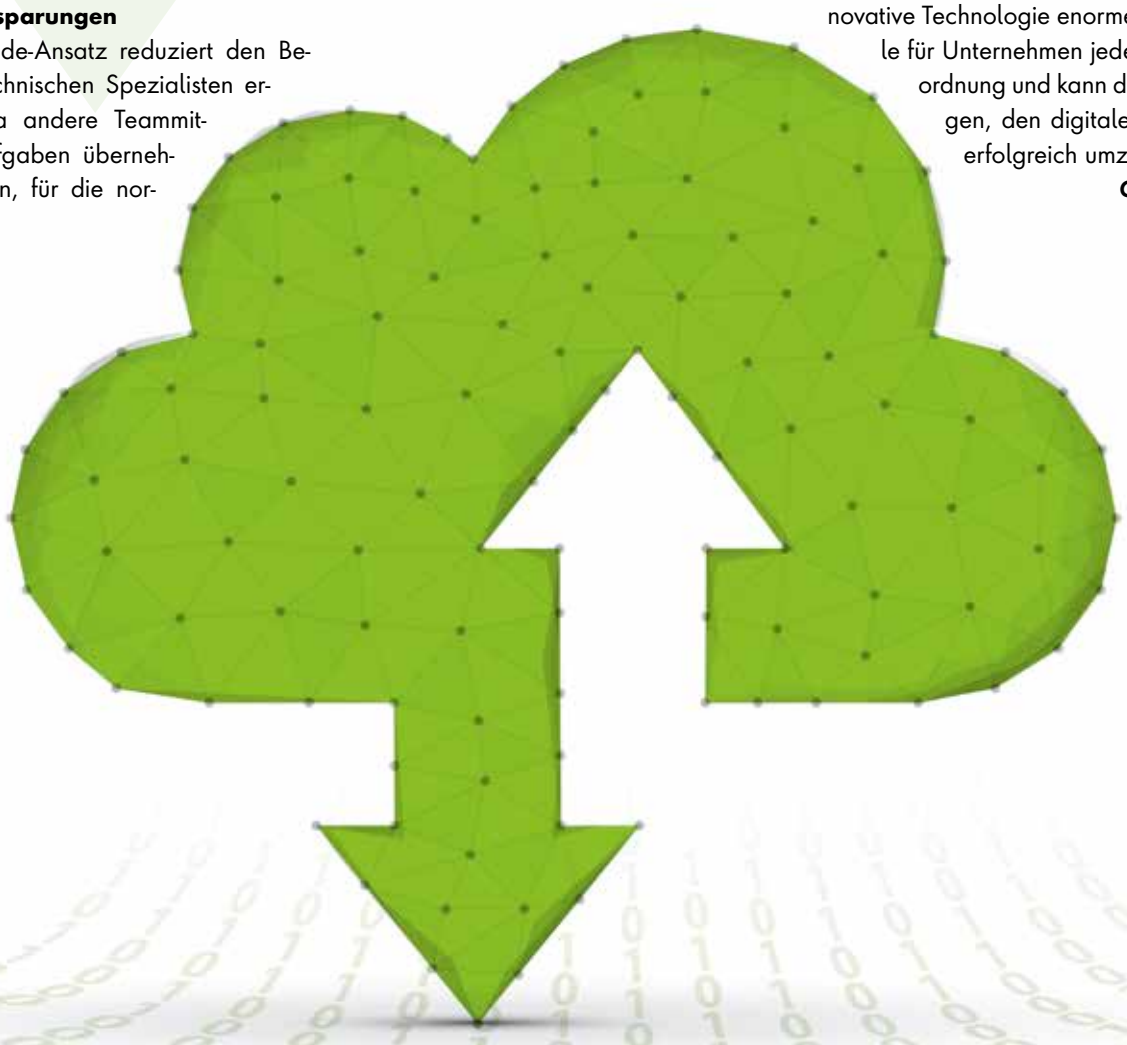
Effiziente Zusammenarbeit

Weil die Nutzung einer No-Code-Plattform nicht auf IT-Spezialisten beschränkt ist, ermöglicht sie auch eine verbesserte Zusammenarbeit und Kommunikation innerhalb und zwischen Teams. Der Austausch von Daten in Echtzeit und die gemeinsame Arbeit an Projekten steigern die Effizienz und verbessern das Arbeitsklima.

Potenzial der Technologie

Wenngleich eine NCC für viele Unternehmen etwas Neues darstellt, konnten einige Early Adopters bereits positive Auswirkungen auf Skalierbarkeit und Flexibilität feststellen. Der einfache und direkte Ansatz der No-Code-Plattform birgt das Potenzial, das ursprüngliche Versprechen der Cloud in Bezug auf Vereinfachung zu erfüllen – und darüber hinauszugehen. Indem die NCC Unternehmen ermöglicht, schnell und kostengünstig digitale Anwendungen zu entwickeln und zu betreiben, hat sie sich als treibender Motor für die Digitalisierung erwiesen. Trotz einiger Herausforderungen bietet diese innovative Technologie enorme Potenziale für Unternehmen jeder Größenordnung und kann dazu beitragen, den digitalen Wandel erfolgreich umzusetzen.

Orli Shahidi



Customer Service Automation

INDIVIDUALISIERBARE STANDARDLÖSUNGEN BIETEN MEHRWERTE

In der neuen Ära der digitalen Servicewelt steht für Verantwortliche des Kundenservice viel auf dem Spiel. Kunden erwarten, dass ihre Anfragen schnell bearbeitet und Probleme zügig und abschließend gelöst werden. Oft ist das Volumen der Anfragen in Serviceabteilungen jedoch so hoch, dass Kundenanliegen nicht schnell genug bearbeitet werden können. Dazu kommen die vergleichsweisen hohen Kosten durch die aufgewendete Zeit des Servicepersonals – insbesondere dann, wenn Service-Teams mit komplexen manuellen Prozessen und isolierten Systemen arbeiten müssen.

Für eine schnelle Bearbeitung von Kundenanliegen sind digitalisierte und automatisierte Serviceprozesse das A und O. Da sich fachliche Anforderungen, Kommunikationskanäle, Prozesse und Systemumgebungen fortlaufend ändern, ist es hierbei notwendig, flexibel zu sein. Ein vielversprechender Ansatz sind Low-code-basierten Lösungen, mit denen trotz der hohen Komplexität alle servicerelevanten Prozesse schnell digitalisiert, automatisiert und bei zukünftigen Änderungen flexibel angepasst werden können.

Neue Herausforderungen im digitalen Kundenservice

Unabhängig davon, über welchen Kanal Kundenanfragen beim Kundenservice eingehen, dauert die Bearbeitung in der Regel zu lange. Oft kann das Service-Team nicht die richtigen Antworten geben, oder Kunden harren über viele Minuten in der Warteschleife aus. Die Gründe dafür können vielfältig sein: fehlende Ressourcen, mangelndes Know-how der Servicemitarbeitenden oder komplexe Prozesse, die unflexibel oder noch nicht digitalisiert sind. Wenn eingehende Daten dann noch manuell in Backend-Systeme

FÜR EINE SCHNELLE BEARBEITUNG VON KUNDENANLIEGEN SIND DIGITALISIERTE UND AUTOMATISIERTE SERVICEPROZESSE DAS A UND O. HIER IST ES NOTWENDIG, FLEXIBEL ZU SEIN.

Alina Feldmann, Digital Business Manager, USU Software AG, www.usu.com

übertragen oder aktualisiert werden müssen, dauert die Bearbeitung von Anfragen noch länger, ist fehleranfällig und in Summe zu teuer. Dies liegt nicht selten an einer komplexen Systemlandschaft und häufigen Änderungsanforderungen, die nicht adäquat und zeitnah umgesetzt werden können:

Historisch gewachsene Systemlandschaft

Serviceabteilungen benötigen schnellen Zugriff auf konsistente Daten, wobei historisch gewachsene Datensilos und komplexe Systemlandschaften oft ein Hindernis darstellen. Kundengetriebene Prozesse werden vom Kunden über verschiedene Kanäle wie Telefon, E-Mail oder Kundenportal angestoßen. Dies erfordert häufig die Integration mehrerer Anwendungen. Gleichzeitig werden weitere Systeme für organisationsgetriebene Prozesse benötigt, die intern von den Serviceabteilungen angestoßen werden.

Um alle Prozesse durchgängig zu digitalisieren und zu orchestrieren, wird ein zentraler Agenten-Desktop benötigt. Dieser dient der Steuerung und Integration aller an den Prozessen beteiligten Systeme. Die notwendige Integrationsfähigkeit ist in diesen heterogenen IT-Landschaften jedoch häufig nicht gegeben.

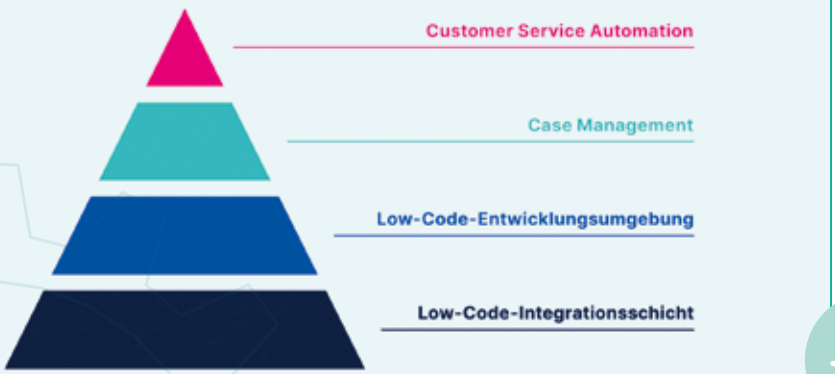
Häufige Änderungsanforderungen

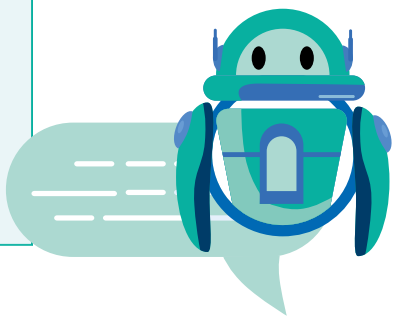
Unternehmen sind aus verschiedenen Gründen fortlaufend mit Änderungsanforderungen konfrontiert:

- Steigerung der Effizienz
- Einhaltung gesetzlicher Richtlinien
- Nutzung neuer Technologien
- Reagieren auf Anforderungen des Marktes
- Organisatorische Änderungen

Veränderungen in der digitalen Servicewelt sind aufgrund der dynamischen Entwicklung unvermeidlich. Unternehmen müssen sich daher kontinuierlich mit Prozess- und Systemänderungen auseinandersetzen. Da solche Änderungen immer häufiger erforderlich

SCHICHTENMODELL EINER LOW-CODE-BASIERTEN STANDARDLÖSUNG FÜR DEN CUSTOMER SERVICE





werden, ist es schwierig, sie aufgrund begrenzter Ressourcen schnell genug umzusetzen.

Standardsoftware oder Individualentwicklung?

Jedes Unternehmen hat individuelle Serviceprozesse und Herausforderungen. Die Suche nach einer Standardsoftware, die eine reibungslose Integration aller Anwendungen ermöglicht und gleichzeitig in der Lage ist, alle individuellen Prozesse optimal abzubilden und zu steuern, ist in der Tat eine Herausforderung. Spezifische Anforderungen und Arbeitsabläufe kann eine Standardsoftware meist nicht vollständig unterstützen. Die Entwicklung einer Individualsoftware zur digitalen Abbildung der Prozesse ist in der Regel zeitaufwändig und erfordert bei jeder Änderung eine individuelle Programmierung. Dies birgt neben dem Mehraufwand unter anderem auch die Gefahr von Schwierigkeiten bei der Nachvollziehbarkeit der Programmierung, etwa wenn die verantwortlichen Mitarbeitenden das Unternehmen verlassen.

Individualisierbare Standardlösung

Angesichts des Dilemmas „Standardsoftware oder Individualentwicklung?" bieten individualisierbare, Low-Code-basierte Standardlösungen das Beste aus beiden Welten. Als Alternative zur Individualentwicklung bietet sich der Einsatz einer Entwicklungsplattform für Customer Service Automation an. Sie ermöglicht eine schnelle und flexible Anwendungsentwicklung. Sie verbindet die Schnelligkeit einer Standardsoftware mit der Anpassbarkeit einer Individualentwicklung. So können individuelle Anforderungen erfüllt und laufende Anpassungen effizient umgesetzt werden.

Low-Code für den Customer Service

In der Low-Code-Entwicklungsumgebung werden Prozesse und Oberflächen mit einfachen visuellen Modellierungswerkzeugen und Drag-and-Drop-Funktionalitäten konfiguriert. Da keine Programmierung erforderlich ist, können Anpassungen weitgehend von den Fachabteilungen selbst vorgenommen werden, was die IT-Abteilungen enorm entlastet. Mit einer Low-Code-Plattform haben Unternehmen alle Freiheiten wie bei einer Individualentwicklung, die Entwicklung erfolgt jedoch deutlich schneller und effizienter. Auch die Optimierung und Weiterentwicklung einer Anwendung ist deutlich einfacher.

Low-Code-Plattformen verfügen zudem über weitreichende Integrationsfähigkeiten, so dass auch die Einbindung externer Systeme schnell und mit geringem Aufwand erfolgen kann - unabhängig davon, ob diese Systeme im eigenen Rechenzentrum oder in der Cloud betrieben werden. Verschiedene technische Standards werden out-of-the-box unterstützt, zum Beispiel REST, SOAP, http oder JMS. Darüber hinaus gibt es eine Vielzahl vorkonfigurierter Schnittstellen, zum Beispiel zu CRM-Systemen, ERP-Applikationen, Datenbanken oder Messaging-Diensten.

Auf Basis des Case Managements wird die Customer Service Automation-Lösung aufgebaut. Diese stellt Funktionen zur Automatisierung von Kundeninteraktionen zur Verfügung, etwa automatische Fallzuordnung, Eskalationen, Service Level Agreements (SLAs) und Benachrichtigungen. Hinzu kommen die Verfolgung von Fallmetriken, Leistungsanalysen und Berichte zur Überwachung und Verbesserung der Kundenzufriedenheit und Serviceeffizienz.

Fazit

Kontinuierliche Anpassungs- und Integrationsfähigkeit ist für Serviceorganisationen wichtig. Hier bieten Low-Code-basierte Standardlösungen entscheidende Vorteile: Sie lassen sich schnell implementieren, integrieren alle relevanten Datenquellen und können durch ihre Flexibilität auch zukünftigen Anforderungen gerecht werden. Unternehmen können damit schnell auf sich ändernde Anforderungen reagieren, ohne auf ihre spezifischen Bedürfnisse verzichten zu müssen.

Alina Feldmann

WEBINAR

Weitergehende Informationen – auch zum Einsatz von KI-Technologien im digitalen Kundenservice – finden Sie hier:

TEIL 3 VON 4

Sensible Daten finden und schützen

PRÄZISE LOKALISIERUNG UND KONSISTENTE ANONYMISIERUNG SENSIBLER DATEN IN UN/SEMI/STRUKTURIERTEN QUELLEN

Dies ist der dritte von vier Artikeln zum Thema End-to-End Datenmanagement. In den beiden vorherigen Artikeln wurde die Bedeutung einer umfassenden Datenverarbeitung betont. Der erste Artikel stellte die Plattform IRI Voracity vor, die Datenerkennung, -integration, -migration und -verwaltung in einem Metadaten-Framework vereint. Die Verwendung einer einzigen Konsole erleichtert die Bedienung und senkt die Betriebskosten in vernetzten IT-Umgebungen erheblich. Im zweiten Artikel wurden die Vorteile der Datenintegration, -migration und -modernisierung erläutert. Diese Maßnahmen verbessern die Qualität, Verfügbarkeit und Wertigkeit von Daten und ermöglichen Unternehmen, ihre Daten effektiver und flexibler zu nutzen, fundierte Entscheidungen zu treffen und wichtige Wettbewerbsvorteile zu erzielen.

IT-Daten sind äußerst wertvoll, denn sie liefern Einblicke in Markttrends und Kundenverhalten und fördern zugleich die Prozessentwicklung und die Innovation. In einer datengetriebenen Welt steigt folglich auch der Wert der Daten stetig. Zu einer der wichtigsten und wertvollsten Datengruppe gehören die personenbezogenen Daten, sie enthalten sensible Informationen. Man kann solche personenbezogenen Daten in drei generelle Haupttypen unterteilen:

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

1. PII = persönlich identifizierbar: Hierzu gehört der Name, das Geburtsdatum, die Anschrift, die Sozialversicherungsnummer, die Personalausweisnummer, die Passnummer, die Führerscheinnummer und biometrische Daten.

2. PCI = Kreditkartendaten: PCI DSS ist ein globaler Sicherheitsstandard für Kreditkartenzahlungen. Alle damit verbundenen Daten müssen diesen Standard zum Schutz der Kartendaten erfüllen.

3. PHI = Gesundheitsdaten: Dies umfasst medizinische Informationen, Krankenakten, Diagnosen, Behandlungsverlauf, genetische Informationen, verschreibungspflichtige Medikamente und Krankenversicherungsinformationen.

UM DIE PRIVATSPHÄRE JEDES EINZELNEN ZU WAHREN UND BETRUG MIT DEREN MISSBRAUCH ZU VERHINDERN, BEDARF ES EINES UMFÄNGLICHEN DATENSCHUTZES.

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

Um die Privatsphäre jedes Einzelnen zu wahren und Betrug mit deren Missbrauch zu verhindern, bedarf es eines umfänglichen Datenschutzes. Sowohl Einzelpersonen als auch Unternehmen müssen angemessene Sicherheitsvorkehrungen treffen. Aus diesem Grund gibt es länderspezifische Bestimmungen in Bezug auf den Umgang mit Daten, wie die Datenschutz-Grundverordnung (kurz „DSGVO", im englischen benannt als „GDPR") für ein einheitliches Datenschutzrecht innerhalb der EU. Die DSGVO legt die Regeln und Bestimmungen fest, wie personenbezogene Daten in der EU erhoben, verarbeitet, gespeichert und geschützt werden sollen. In diesem Zusammenhang wird der Fachbegriff Data Compliance verwendet, es umfasst die Verpflichtung von Unternehmen, bestimmte Datenschutz- und Sicherheitsstandards einzuhalten, um die Vertraulichkeit, Integrität und Verfügbarkeit von Daten zu gewährleisten.

Gezielt geschützt

Um die Sicherheit und Vertraulichkeit der persönlichen Informationen zu garantieren, müssen geeignete Maßnahmen zum zweckgerichteten Datenschutz gewählt werden. Da eine moderne IT-Umgebung heute aus lokalen und ausgelagerten Cloud-Ressourcen mit Datensilos in verschiedensten un/semi/strukturierten Datenquellen und Formaten besteht, müssen

die persönlichen Daten zunächst global aufgespürt werden bevor sie dann gezielt geschützt werden können. Die End-to-End Datenmanagement Plattform IRI Voracity unterstützt den Prozess beginnend mit der Datendefinierung in Datenklassen und Datenlokalisierung, über gezielte Datenschutzmechanismen, bis hin zum Audit-Reporting zur Einhaltung der Data Compliance.

Die Datenrisiken müssen dauerhaft und auch in Zukunft überwacht werden. Zum Zeitpunkt des Schutzes ist die Wahl der Technologie daher schwierig. Die herkömmliche Verschlüsselung von ganzen Datenbanken, Dateien, Festplatten oder Geräten ist ineffizient, vor allem was das Volumen betrifft. Außerdem schränkt sie den Zugriff auf nicht sensible Daten ein und ist bei einer einzigen Passwortverletzung vollständig gefährdet. Außerdem können bestimmte Methoden zur Datenmaskierung zu unsicheren Ergebnissen führen und möglicherweise nicht in der eingesetzten Umgebung funktionieren. Dies hätte zur Folge, dass die geschützten Daten für Test-, Marketing- oder Forschungszwecke unbrauchbar werden.

Bild 1: End-to-End Datenmangement für Datenschutz

Schwärzen, Hashen & Tokenisieren

Daher bietet IRI Voracity umfangreichste Funktionen, damit sensible Daten zunächst klassifiziert und entsprechend ihrer

Formate, ihrer Speicherstandorte und ihrer Speicherzustände (statisch oder dynamisch) zielgerichtet gefunden und automatisch geschützt werden können:

- In strukturierten Datei-, Datenbank- oder HDFS-Quellen: Verschleierung der Daten auf Feldebene, bevor diese die Firewall ungeschützt verlassen.
- In strukturierten, semi- und unstrukturierten Quellen: Für den Schutz sensibler Daten in Text, PDF, Parquet, C/BLOBs, Microsoft Office-Dokumenten, Protokollen, NoSQL-DBs, Bildern und Gesichtern.
- In Microsoft XLS- und XLSX-Dateien: Zum Schutz von Excel-Spalten mit reversiblen und nicht reversiblen Maskierungsfunktionen innerhalb eines einzelnen Blattes oder gleichzeitig über Tausende von Blättern auf Netzwerklaufwerken und in Office 365.

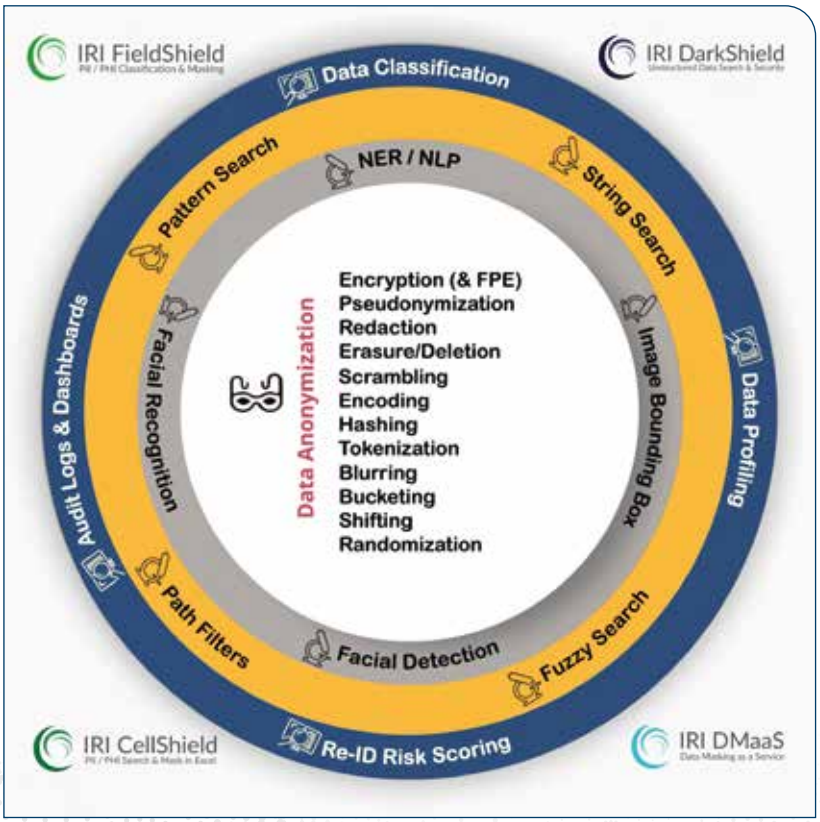


Bild 2: Datenmaskierung für DSGVO-konformen Datenschutz

Zu den geeigneten Methoden um sensible Daten gezielt und zweckgerichtet zu schützen gehören, Schwärzen, Verschlüsseln, Hashen, Pseudonymisieren, Randomisieren, Bearbeiten und Tokenisieren. Es ist wichtig diese Methoden konsistent anzuwenden, um sowohl Realismus als auch referentielle Integrität über alle Quellen hinweg zu bewahren.

Zusätzlich werden automatisch strukturierte und maschinenlesbare Audit-Protokolle erstellt. Diese Protokolle können sicher gespeichert, abgerufen und angezeigt oder bei Bedarf in entsprechende SIEM-Tools exportiert werden. Dadurch ist eine verlässliche Dokumentation aller vorgenommenen Änderungen vorhanden. Manipulationen können nicht unbemerkt durchgeführt werden, denn sie lösen sofortige Warnmeldungen aus. So können entsprechende Maßnahmen ergriffen werden, um die Datensicherheit umfänglich zu gewährleisten.

Fazit

Ziel der Datenermittlung und anschließenden Datenmaskierung ist der Schutz von sensiblen Daten, um Datenschutzverletzungen zu verhindern und entsprechend geltende Datenschutzgesetze einzuhalten. In der Plattform IRI Voracity ist dafür ein umfassendes End-to-End Datenmanagement möglich, sodass sensible Daten in RDBs, Flat-Files und Excel Sheets vor Ort oder in der Cloud gefunden und geschützt werden können. Auch NoSQL-DBs, Dokumente, Bilder sowie EDI- und Protokolldateien, Streaming und Hadoop-Datenquellen und Gesichter können lokalisiert und mit verschiedenen Verschlüsselungsmethoden DSGVO-konform verarbeitet werden. Dadurch wird ein umfassender Schutz aller Daten gewährleistet, unabhängig des un/semi/strukturierten Formates!

Amadeus Thomas

AUSBLICK

In der letzten diesjährigen Ausgabe werden die vier verschiedenen Ansätze zur Erstellung von synthetischen und referentiell korrekten Testdaten in der IRI Voracity Plattform aufgezeigt. Das Besondere dabei ist, dass lediglich Metadaten und keine Produktionsdaten dafür nötig sind. Dies führt nicht nur zu einem verstärkten Datenschutz, sondern ermöglicht auch die Verfügbarkeit von präziseren Testdaten, die auf die eigene Geschäftslogik zugeschnitten sind.

Wenn der Keks zerbröselt

3 ASPEKTE, DIE UNTERNEHMEN FÜR EINE COOKIE-FREIE ZUKUNFT WISSEN MÜSSEN

Bereits im Jahr 2020 hatte Google das Ende von Third-Party-Cookies in seinem Browser angekündigt, im kommenden Jahr soll es – nach mehreren Verschiebungen – so weit sein. Unternehmen sollten sich heute schon auf diese neue Realität einstellen. Wie das gelingt und auf was sie dabei achten müssen, lesen Sie hier:

Unternehmen haben Cookies bislang verwendet, um die Interaktionen und das Verhalten von Nutzern im Internet zu verfolgen und zu analysieren. Doch damit ist – zumindest im Google-eigenen Browser Chrome – künftig Schluss. Stattdessen werden Unternehmen sich stärker darauf konzentrieren müssen, First-Party-Data, also Informationen, die durch Interaktionen mit den eigenen Inhalten generiert werden, zu erheben. Infolgedessen wird auch das Datenmanagement noch stärker an Bedeutung gewinnen. Was heißt das für Unternehmen?

#1 Sie brauchen eine CDP

Unternehmen haben eine Vielzahl von Möglichkeiten, First-Party-Data zu gewinnen. Damit geht aber auch einher, dass sie Daten aus einer Vielzahl von Quellen miteinander verknüpfen müssen, um aussagekräftige Insights zu generieren. Sie sollten daher eine Customer Data Platform (CDP) einrichten, in der relevante Daten aus dem Enterprise Resource Planning (ERP)-System, dem Customer-Relationship-Management (CRM)-Tool und anderen operativen Lösungen zusammenfließen.

Die CDP ist damit eine Art Single Source of Truth (SSoT) für alle Kundendaten und ermöglicht ein vollständiges Bild der einzelnen Kunden. Dies erlaubt es Unternehmen, ihre Marketingaktivitäten ganz auf diese einzelnen Kunden, ihre Interessen und Bedürfnisse zuzuschneiden.

#2 Marketing und IT müssen enger zusammenarbeiten

Die Marketingabteilung wird sich damit in Zukunft noch stärker auf digitale Tools verlassen müssen. Dabei sollte sie aber nicht eigenständig vorgehen, sondern sich eng mit der IT-Abteilung abstimmen, welche Tools den gewünschten Zweck erfüllen und sich in den bisherigen MarTech-Stack am besten integrieren lassen. Denn die IT muss nicht nur dafür sorgen, dass die Integrationen zwischen den verschiedenen Systemen funktionieren und die Daten reibungslos genutzt werden können. Darüber hinaus muss sie auch sicherstellen, dass eine hohe Datenqualität gegeben ist – denn nur dann lässt sich verlässlich mit diesen Daten arbeiten -, sie gesetzeskonform gespeichert werden und gelöscht werden können und der Zugriff robust geregelt ist, damit sich Unbefugten keinen Zugang zu sensiblen Daten verschaffen können.

#3 Das Datenmanagement sollte demokratisiert werden

Datenanalysen sind entscheidend, um Daten nicht nur zu sammeln und zusammenzuführen, sondern aus ihnen auch die richtigen Schlüsse zu ziehen und fundierte Entscheidungen zu treffen. Das gilt insbesondere für das Marketing in einer Cookie-freien Zukunft, denn First-Party-Data sind an sich wesentlich weniger aussagekräftig als Third-Party-Data und ergeben erst durch die Verknüpfung verschiedener Daten ein rundes Bild. Dementsprechend sollten IT- und Marketingabteilung auch darauf achten, künftig sowohl Self-Service-Lösungen als auch Low-Code- oder No-Code-Plattformen zu integrieren. Dadurch haben die Marketingmitarbeiter zum einen die Möglichkeit, eigenständig Datenanalysen zu machen, ohne die IT-Abteilung hinzuziehen zu müssen. Zum anderen können sie selbst Anwendungen in einer Art Baukastensystem bauen, die ihnen zum Beispiel die Daten liefern, die sie benötigen.

www.tibco.com

THOUGHT LEADERSHIP IN DER IT

Konferenz

27. - 28. September 2023

Online via Zoom

Jetzt kostenfrei anmelden

Tauchen Sie in eine Welt von neuem Wissen und Innovationen ein. Lernen Sie von den Besten. Sichern Sie sich Ihren WissensVORSPRUNG!

Die „Thought Leadership“-Konferenz ist die perfekte Gelegenheit, Ihr Unternehmen und Ihre Karriere auf die nächste Stufe zu bringen.

Hören Sie und diskutieren Sie unter anderem mit:

Design Thinking & Thought Leadership in der IT
Dr. Claudia Nicolai, Director and Co-Head
Hasso-Plattner-Institut für Digital Engineering GmbH

Generative KI - Die Revolution im Kundenservice
Harald Huber, Managing Director
USU Software AG

Threat Intelligence – Bedeutung, sinnvoller Einsatz und Limits
Thomas Uhlemann, IT Security Evangelist
ESET spol. s r.o.

Clean Data: Die KI-Falle mit den eigenen Daten und geistigem Eigentum
Andrian Knapp, Visionär & Gründer
Aparavi Software AG

Business 5.0: Wie Web3, Blockchain, Metaverse und generative KI die Welt verändern werden
Prof. Julia Finkeissen, Unternehmerin & Investorin

Seien Sie ein Vorreiter in Ihrer Branche
und **melden Sie sich jetzt an!**

#ThoughtLeaderIT

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

Benchmarking in IT-Projekten

NICHT AM FALSCHEN ENDE SPAREN

Wer ein großes Problem zu lösen hat, hätte dies besser schon getan, als es noch ein kleines Problem war. Diese Binsenweisheit des Managements gilt auch für IT-Projekte. Denn der Grund, warum sehr viele Projekte finanziell, zeitlich oder logistisch teilweise extrem aus dem Ruder laufen und nicht selten Karrieren kosten, liegt meist nicht im Projektmanagement selbst, sondern an schlechter Vorbereitung und Planung. Fehlendes oder falsches Benchmarking ist oft die Ursache und führt zu massiven Kostensteigerungen sowie unerfüllten Erwartungen. Die Fehler am Anfang rächen sich spät, manchmal zu spät und irreparabel.

Nicht alles,
was hinkt, ist ein Vergleich

Dabei sind erfolgreiche IT-Projekte kein Hexenwerk – wenn man sie methodisch von Anfang an richtig angeht. Dies beginnt beim Benchmarking. Doch gerade bei diesem Thema lauern viele Fallen und Herausforderungen. So denken viele Unternehmen, ihre Vorhaben und Strukturen seien derart individuell, dass man sie gar nicht realistisch benchmarken könne. Die Grundannahme „bei uns ist alles ganz anders" gehört zu den größten Fehlern. Der Blick auf das, was andere bereits erfolgreich umgesetzt haben, auch dann, wenn sich Vergleiche nicht eins zu eins ziehen lassen, hilft, zu richtigen Entscheidungen zu kommen. Vergleichswerte sind immer wertvoll. Sie geben Aufschluss über die Größe einer Herausforderung und helfen, Fehler zu vermeiden. Allerdings: Benchmarks, die sich aus solchen

Vergleichen ergeben, gehören ihrerseits auch auf den Prüfstand. Erfahrungswerte und Vergleiche mit Dritten auf der einen Seite, deren richtige Interpretation in Bezug auf das eigene individuelle Vorhaben auf der anderen Seite, sind die ideale Basis für einen erfolgreichen Projektstart in Bezug auf Benchmarking, Kostenschätzung, Ressourcenplanung und Erwartungsklärung. Dabei gilt: Nicht alles, was hinkt, ist auch ein Vergleich. Aber ohne Vergleiche entstehen keine seriösen Benchmarks.

Externe Berater bieten eine breite Vergleichsbasis

Für Benchmarks gibt es valide Qualitätskriterien. Dazu zählen eine möglichst hohe Vergleichbarkeit genauso wie eine aussagekräftige Grundgesamtheit an Vergleichswerten. Eine Benchmark ist erst dann sinnvoll, wenn sie fachlich und inhaltlich sowie vom Umfang, der Dauer, der Technologie und der Organisation her ähnlich gelagert ist. Zudem braucht es immer mehrere Benchmarks, um aus ihnen einen Schnitt zu bilden sowie einen Erkenntnisgewinn zu ziehen. Diese Grundgesamtheit, die notwendige Menge an Vergleichswerten, haben typischerweise nur externe Berater, die auch in einer gewissen Größenordnung agieren. Sie können auf sinnvolle Querschnitte und signifikante Vergleichsgrößen aus verschiedenen Branchen und Projektvolumen zurückgreifen. Das einzelne Unternehmen hat hingegen in der Regel nicht genug Projekte und Projekterfahrungen, um sich auf eine ausreichende Anzahl von Vergleichswerten und Benchmarks zu beziehen.

Letztlich lässt sich alles messen

Zu wenige Benchmarks, falsche Benchmarks oder falsche Schlüsse aus den Benchmarks führen häufig zu falschen Schlussfolgerungen, in deren Folge dann Kostenschätzungen oder Personalplanungen massiv abweichen von der späteren Realität.

In der Regel sind mindestens drei Vergleichskriterien sinnvoll: Dauer im Vergleich zu Scope und Inhalt, zu investierende menschliche Ressourcen sowie Preise für Lizenzen, Meilensteine oder Serviceverträge. Das sind die typischen KPIs für die Vergleichbarkeit. Darüber hinaus macht es einen Unterschied, ob Benchmarks für Tagessätze, Lizenzen, Entwicklungsprojekte, Einführungsprojekte für Standardsoftware oder Benchmarks für Hardware, den Quadratmeter Rechenzentrum oder etwas anderes gesucht werden. Messen und vergleichen und damit benchmarken lässt sich letztlich alles, von den Kosten für ein Jahr Druckermiete bis hin zu komplexen, langjährigen ERP-Einführungsprojekten.

Allerdings: Je spezieller das Vergleichsprojekt ist, desto länger muss man forschen, recherchieren oder Umfragen starten, um die gesuchten Vergleichswerte zu finden. Das dauert, kostet Zeit und Geld, das sich nicht Wenige gerne zunächst sparen. Diese Investitionen machen sich aber später mehr als bezahlt. Sie verhindern, dass aus einem kleinen Problem später ein großes wird, insbesondere bei den Kosten.

Designpattern

Besonders bei komplexen IT-Projekten, wie etwa der Einführung eines neuen ERP-Systems, lassen sich durch intelligentes Benchmarking und Vergleiche mit anderen Projekten wertvolle Erkenntnisse in Sachen Kostensteigerungen gewinnen: Was waren die Kostentreiber? Waren es Schnittstellen? Lizenzen? Prozessänderungen und dadurch notwendige Anpassungen? Waren es die Menge und Art der fachlichen oder technischen Anforderungen? War es die Anzahl der beteiligten Fachbereiche oder Systemmodule? All das sind Indikatoren, die statistisch signifikant auf die Länge und damit die Kosten von Projekten einwirken. All diese KPIs kann man dann mit dem zu bemessenden Projekt vergleichen und über eine Regression als Messlatte für das eigene Projekt verwenden. Zwar muss es nicht immer so komplex laufen, aber in den meisten Fällen ist es ein solches „Designpattern", das bei der Anwendung von Benchmarks für Kosten und Zeitschätzungen zum Einsatz kommt.

„Menschliches Versagen"

Die Ursachen von Fehleinschätzungen sind meist menschlicher Natur. Viele Unternehmen oder Abteilungen lassen sich von der eigenen vermeintlichen Komplexität blenden. Mit dem Satz „Bei uns ist alles ganz anders, da lässt sich nichts vergleichen" werden Benchmarks von vornherein als unmöglich oder gar unnütz abgelehnt. Dabei wären Erfahrungswerte, auch, wenn diese nicht

eins zu eins übertragen werden können, hilfreich, um eigene Fehler zu vermeiden und Risiken zu minimieren.

„Bei einem befreundeten Unternehmen hat das auch so funktioniert", ist ein anderer Satz, der Benchmarks infrage stellt. Hier wird die eigene Komplexität unter- statt überschätzt. Gemeinsamkeiten werden gleichgesetzt, echte Unterschiede eher kleingeredet. Statistisch signifikante Aussagen werden so aber nicht gewonnen.

Nicht selten werden jedoch auch Benchmarks erhoben, analysiert und bewertet, allerdings mangelhaft. „Wir haben das analysiert, und es hat nur drei Tage gedauert." Diese eigene „Marktanalyse" ist in der Regel eher oberflächlich und öffnet Fehleinschätzungen Tür und Tor. Entscheider wähnen sich in falscher Sicherheit. Externe Einflüsse werden gar nicht, rudimentär oder zu wenig betrachtet. Wichtige Kostentreiber werden aufgrund von Unerfahrenheit beim Benchmarking außer Acht gelassen. In der Regel fehlen für diese Aufgabe die internen Spezialisten.

„Eh klar" gibt es nicht

Hinzu kommt: Interne Projektplaner gehen nicht selten davon aus, dass internes Wissen Allgemeinwissen ist. Wer etwas jeden Tag macht und deswegen über eine Routine verfügt, geht davon aus, dass jeder die Welt genauso sieht. Nicht-Eingeweihte haben es dann schwer, externe Dienstleister allemal. Die daraus folgende „Das-ist-doch-eh-klar"-Haltung führt zu folgenreichen Fehleinschätzungen. Dieser Effekt sorgt dafür, dass die Komplexität von Vorhaben in der Digitalisierung regelmäßig unterschätzt wird.

Moralisches Dilemma

Zudem müssen Projekte auch intern verkauft werden. Werden sie zu teuer, wirken überdimensioniert oder überkomplex, werden sie abgelehnt. Wenn sie abgelehnt werden, hat der Initiator gegebenenfalls einen Karrierenachteil. Projekte

JE SPEZIELLER DAS VERGLEICHSPROJEKT IST, DESTO LÄNGER MUSS MAN FORSCHEN, RECHERCHIEREN ODER UMFRAGEN STARTEN, UM DIE GESUCHTEN VERGLEICHSWERTE ZU FINDEN.

Andreas Viehhauser, Managing Partner, ReqPool, www.reqpool.com

sollen schließlich stattfinden, sind politisch gewünscht. Zugleich aber sollen sie möglichst wenig kosten und sich schnell rentieren. Und so werden nicht wenige Projekte aus Kalkül im Vorfeld kleingerechnet oder aber bewusst überdimensioniert, weil große Projekte viel Renommee mit sich bringen. Lange Phasen des Benchmarkings oder der Analyse werden hingegen gerne eingespart, um entweder die Kosten dafür zu vermeiden oder aber um sofort in die Umsetzung zu kommen. Häufig aber rächt sich dies im Laufe des Projektes.

Man nennt diesen Effekt „Moral Hazard" – das Interesse an ehrlichen Schätzungen und Benchmarks ist manchmal schon initial nicht vorhanden. Das moralische Dilemma: Eine Schönwetter-Schätzung machen, loslegen und Probleme im Projekt ausbaden oder ehrlich schätzen und riskieren, dass das Vorhaben nicht zustande kommt.

Realistische Benchmarkings schützen davor, hier mit falschen Erwartungshaltungen zu starten. Jeder sollte sie bei größeren Vorhaben nutzen und auch in sie investieren. Falsche Schätzungen manifestieren sich meist später im Projekt. Und das fällt dann negativ auf alle Beteiligten zurück.

Um diesem moralischen Dilemma zu entkommen, sollten sowohl die Geschäftsleitung als auch neutrale Schätzexperten hinzugezogen werden, ebenso Experten und Umsetzer aus der Praxis des Projektmanagements, der Softwarebeschaffung und der Entwicklung, die sowohl Benchmarks als auch weitreichende Erfahrungen und Insights liefern können.

Projekte unter Druck

Ohne gute Benchmarks ist es schwierig, Kosten richtig einzuschätzen. Ohne richtige Kostenschätzungen erhält man falsche Werte für Meilensteine, für Ziele und Planwerte im Projektcontrolling. Sind aber die Plan- und Zielwerte im Projektmanagement die falschen, greift auch gutes Projektmanagement ins Leere. Ein Projekt lässt sich nicht steuern, wenn es keine verlässlichen Budgets gibt, jede Änderung ohne Puffer auskommen muss und sofort Eskalationen im Raum stehen. Das vergiftet das Klima in der Umsetzung und setzt Projekte unter Druck. Dieser Druck bringt oft auch gut gelagerte Projekte ohne Not in Schieflage. Falsche Einschätzungen werden so zur Self-Fulfilling-Prophecy.

Einfache Benchmarking-Regeln

Sinnvolles Benchmarking orientiert sich maßgeblich am Projektumfang. Für Vorhaben im Bereich von einem bis zu zehn Manntagen reicht ein Schätzer und die „Benchmark-Datenbank Kopf". Der Schätzaufwand wird nur wenige Minuten betragen und lässt sich Pi mal Daumen aus Erfahrungen ermitteln.

Bei Projektumfängen zwischen 11 und 49 Manntagen sollten herangezogene Vergleichswerte zusätzlich immer dokumentiert und eine Schätzung als „Experten-Delphi-Schätzung" immer von mehreren Schätzern vorgenommen und untermauert werden. Auch das geht in der Regel relativ schnell. Schätzaufwand: einige Stunden.

Für Projekte zwischen 50 und 100 Manntagen sollte schon intensiver gebenchmarkt und geschätzt werden. Schätzklausuren oder die Aufbereitung von Benchmarks durch Externe sind hier sehr sinnvoll. Der Schätzaufwand wird im Bereich von einigen Tagen liegen.

Bei Projekten über 100 Manntagen Gesamtaufwand – nicht wenige IT-Projekte gehen bis in die Tausende oder gar Zehntausende Manntage – sollte immer ein zumindest substanzieller, einstelliger Prozentsatz des Gesamtaufwands vorab in Benchmarking und Aufwandsschätzung fließen.

Benchmarking als eigenes Projekt

In diesen Größenordnungen sind Schätzungen und Benchmarking oft eigene, vorgelagerte Kleinprojekte im Umfang von fünf bis fünfundzwanzig Manntagen. Diese werden typischerweise in die Durchführung von Marktanalysen, die Suche und das „Interviewing" von Benchmark-Gebern, die Analyse und die Kostenschätzung anhand der Benchmarks sowie „das Challenging" der strukturierten Ergebnisse investiert. Niemals aber sollte bei Projekten in so einer Größenordnung die Idee sein: „Wir rufen drei Anbieter an und machen drei Präsentationen, das dauert zwei Tage und wir haben alle nötigen Benchmarks."

Auch können hier automatisierte Tools eingesetzt werden, die anhand von Projekt-KPIs über eine große Menge von Benchmarks normalisierte Schlüsse ziehen und Vergleichswerte sowie Schätz-Input liefern.

Bei großen Projekten werden sinnvollerweise externe Berater und Projektmanager hinzugezogen, die über eine Historisierung von Benchmarks zu allen möglichen Themen wie Lizenzen, Projektaufwänden, Hardware, Software, SLAs bis hin zu Aufwänden für die Implementierung einzelner spezieller Schnittstellen aus Vergleichsprojekten sowie die Anwendung von „Delphi-Schätzungen" vieler langjähriger Experten und die Nutzung selbst entwickelter Schätzwerkzeuge für Softwareprojekte wie den Estimation-Manager, die mit vielen Vergleichsbenchmarks unterlegt sind, verfügen. Externe Berater bringen hier Vorteile und eine breite Masse an Benchmarks, Vergleichsdaten und Tools mit.

Benchmarking muss sein

Im Bechmarking gilt vor allem eines: tun, tun, tun. Es zu unterlassen kann fatale und teure Folgen haben. Nur wer sich mit dem Thema beschäftigt und bei größeren Projekten fachkundig begleiten lässt, kann die gewünschten Ergebnisse erzielen, echte Aufwände kalkulieren und diese auch realistisch budgetieren. Böse Überraschungen lassen sich vermeiden. Projekte scheitern letztlich am Start.

Andreas Viehhauser

Erfolgreich scheitern mit OKR

OBJECTIVE & KEY RESULTS (OKR) GILT ALS WUNDERWAFFE MODERNER (AGILER) FÜHRUNG. IST DEM SO?

Die klassischen Zielvereinbarungen haben ausgedient und wurden in vielen deutschen Unternehmen durch OKR, einer Methode aus dem Silicon Valley ersetzt. Doch auch OKR ist kein Garant für 100 Prozent Erfolg. Ganz im Gegenteil: Wer OKR einführt, weil Google das macht, wird sehr schnell feststellen, dass das Kopieren des Ansatzes nicht wirkungsvoll sein wird.

Für das Buch „OKR in der Praxis – Beispiele, Hacks, Erfahrungen" habe ich mich auf die Suche gemacht, wie OKR in deutschen Unternehmen wirksam wird. Dazu habe ich zahlreiche Interviews mit OKR Experten von Großunternehmen geführt und beleuchtet wie OKR gelebt wird, wie eine Einführung aussieht und welche Fallstricke es gibt, die eine nachhaltige Implementierung behindern.

Objective and Key Results - kurz OKR ist ein agiles Betriebssystem, das Organisation hilft sich durch eine kollaborative Zielsetzung auf ihre strategische Ausrichtung zu fokussieren und gemeinschaftlich diese umzusetzen. Bessere Fokussierung, mehr Transparenz, erfolgreiche crossfunktionale Zusammenarbeit: So nachvollziehbar die Vorteile von OKR in der Theorie sind, so holprig kann es in der praktischen Umsetzung aussehen.

OKR in der Theorie: Ziele, Zyklen, Zusammenarbeit

Für OKR gibt es kein offizielles Regelwerk. Es ist eher eine große Open-Source-Initiative, die vor über siebzig Jahren vereinfacht dargestellt mit „Management by Objectives (MbO)" begann und stetig weiterentwickelt wird.

Bei OKR geht es nicht um die reine Methodik zum Setzen von Zielen, sondern

um eine Veränderung der Haltung und Denkweise. Dazu passt auch die folgende Definition von Paul Niven und Ben Lamorte (2016): „OKR is a critical thinking framework and ongoing discipline that seeks to ensure employees work together, focusing their efforts to make measurable contributions that drive the company forward."

OKR benötigt einen strategischen Kontext aus Vision, Mission und Strategie, um die Wirksamkeit zu entfalten. Denn nur wenn Menschen wissen, welche Richtung angestrebt wird, können sie mit ihrem Expertenwissen überlegen, wie ihr Beitrag dazu aussieht.

Dabei ist die Grundidee, dass die Art und Weise, wie wir Ziele definieren und miteinander abstimmen, kein einmaliges Ereignis ist, sondern ein kontinuierlicher Prozess. In der Theorie heißt das, dass Teams, Bereiche und die Geschäftsführung quartalsweise zusammen ihre Ziele an der Strategie ausrichten und/ oder dass dies anhand bestimmter übergeordneter Ambitionen in crossfunktionalen Teams erfolgt. Dazu definieren sie in der Regel drei bis fünf OKR-Sets für ihre jeweilige Einheit.

Ein Set besteht aus einem Objective, das heißt einem Ziel mit circa drei bis fünf Key Results. Letztere sind die messbaren Hebel, die die Wahrscheinlichkeit erhöhen, dass das gesteckte Ziel am Ende des Zyklus (in der Regel drei Monate) erreicht ist. Die Pfeiler des Prozesses sind eine Reihe von Events, die helfen, in eine Disziplin des Planens und Umsetzens zu gelangen. Die Ausrichtung entsteht durch ein ausbalanciertes Verhältnis von Top-down- zu Bottom-up-Zielen.

Im Unterschied zu MbO fokussiert OKR mehr auf das Messen von Outcome (wie zum Beispiel ob Kunden mit einem Feature zufrieden sind) als auf Output (wie das Programmieren des Features) und rückt durch die regelmäßigen Routinen (die OKR-Events) die Strategieumsetzung in den Vordergrund.

DIE ULTIMATIVE CHECKLISTE FÜR ERFOLGREICHES SCHEITERN MIT OKR

#1 Mach deutlich, dass das Streben nach der Unternehmensvision reine Zeitverschwendung ist.

#2 Sage deutlich in der Öffentlichkeit, dass Kundenzentrierung das A und O ist, fokussiere dich im Tun allerdings ausschließlich auf interne Prozesse.

#3 Beschreibe eine strategische Richtung so schwammig, dass auch wirklich keiner damit etwas anfangen kann.

#4 Starte OKR als Geheimprojekt und erzähle allen, dass da was im Busch ist.

#5 Falls es doch schon offiziell ist, fasse den Nutzen mit »Google macht das auch« zusammen.

#6 Bist du in der Geschäftsführung, übertrage das Mandat für die Einführung von OKR irgendeiner Person im Unternehmen, die dich am wenigsten davon abhält, weiterhin über Command and Control zu steuern.

#7 Dann solltest du aber noch hinzufügen, dass das hundert Prozent top-down funktionieren wird.

#8 Damit das funktioniert, nimmst du einfach dein heutiges Zielsetzungssystem und schreibst OKR drüber.

#9 Setze den Fokus weiterhin darauf, möglichst viel gleichzeitig anzuzetteln und bitte die Teams, kontinuierlich ihre Tasklisten öffentlich zu pflegen. Key Results eignen sich dafür besonders gut.

#10 Hilfreich ist dabei auch, mit großem Brimborium zu Beginn des Jahres überambitionierte Ziele auszurufen und nie wieder darauf zu schauen.

#11 Löse dabei am besten keine existierenden Probleme deiner Kunden und erzeuge keinerlei Mehrwert für dein Unternehmen.

#12 Bitte deine Mitarbeitenden, sich selbstständig Informations- und Lernmaterialien im Internet zusammenzusuchen.

#13 Knüpfe die OKRs an persönlichen Boni und Incentives, so sind alle so richtig motiviert.

#14 Streue auch gerne ein paar Gerüchte, was mit Mitarbeitenden passiert, die ihre OKR-Sets nicht erreichen. Ein bisschen Angst hat noch keinem geschadet.

#15 Verhalte dich stets gegensätzlich zu dem, was du von deinen Kollegen erwartest.

OKR, als agiles Betriebssystem betrachtet, ist kein Mitarbeitenden-Kontrollsystem, sondern dient dem Lernen und Erkunden von unbekannten Welten. Damit liegt ein Menschenbild zugrunde, das auf die kontinuierliche Weiterentwicklung setzt und eine Fehlerkultur ernst meint. Eine Verknüpfung von OKR und (individuellen) Bonussystemen ist deshalb kontraproduktiv.

OKR in der Praxis: Mach OKR zu deinem Ding!

Gerade weil OKR eher als Rahmen- statt als Regelwerk zu verstehen ist, bedarf die nachhaltige Implementierung einer Anpassung an den Kontext des Unternehmens oder der Organisation. Dazu gehört ein klares Verständnis, welche konkreten Probleme mit Hilfe von OKR gelöst werden sollen (zum Beispiel zu wenig Fokussierung auf die strategisch relevanten Themen) also auch ein klares Erwartungsmanagement, welche Hebel mit OKR gehoben werden können und welche auch nicht.

Beispielsweise kann OKR eine Firma mit einem überholten Geschäftsmodell nicht von einem auf den anderen Tag gesund sanieren. Ebenso benötigt es Menschen, die OKR, insbesondere den Unterschied von Outcome und Output verstehen und die Methodik rund um OKR in die Organisation tragen können. Ein echtes Sponsorship unterstützt nicht nur die Einführung, sondern steht auch im weiteren Verlauf mit Rat und Tat zur Seite.

In der Praxis wird OKR dann wirksam, wenn Unternehmen sich auf „ihren" OKR-Ansatz verständigen. Dies kann bedeuten, dass bestimmte Leitplanken hinsichtlich der OKR-Architektur festgelegt werden: Wie ist die für uns passende Zykluslänge? Erlauben wir uns für den Beginn auch „Output-Key Results"? Wie stellen wir sicher, dass bottom-up Ziele auch wirklich gehört werden? Wie stark geben wir top-down die Richtung vor?

Nun wäre es paradox diese Leitplanken als für alle Zeiten gesetzt vorzugeben. Schließlich entsteht die Magie von OKR insbesondere durch routinierte Feedback- und Lernschleifen. Dies sollte auch für das Rahmenwerk OKR an sich gelten. „Mach OKR zu deinem Ding" bedeutet damit nicht nur eine einmalige Anpassung zur Einführung, sondern auch eine kontinuierliche Adaption an die kontextuellen Bedingungen.

NUR WENN MENSCHEN WISSEN, WELCHE RICHTUNG ANGESTREBT WIRD, KÖNNEN SIE MIT IHREM EXPERTENWISSEN ÜBERLEGEN, WIE IHR BEITRAG DAZU AUSSIEHT.

Christina Lange,
Autorin, https://pragmaticchange.com/

Checkliste für erfolgreiches Scheitern

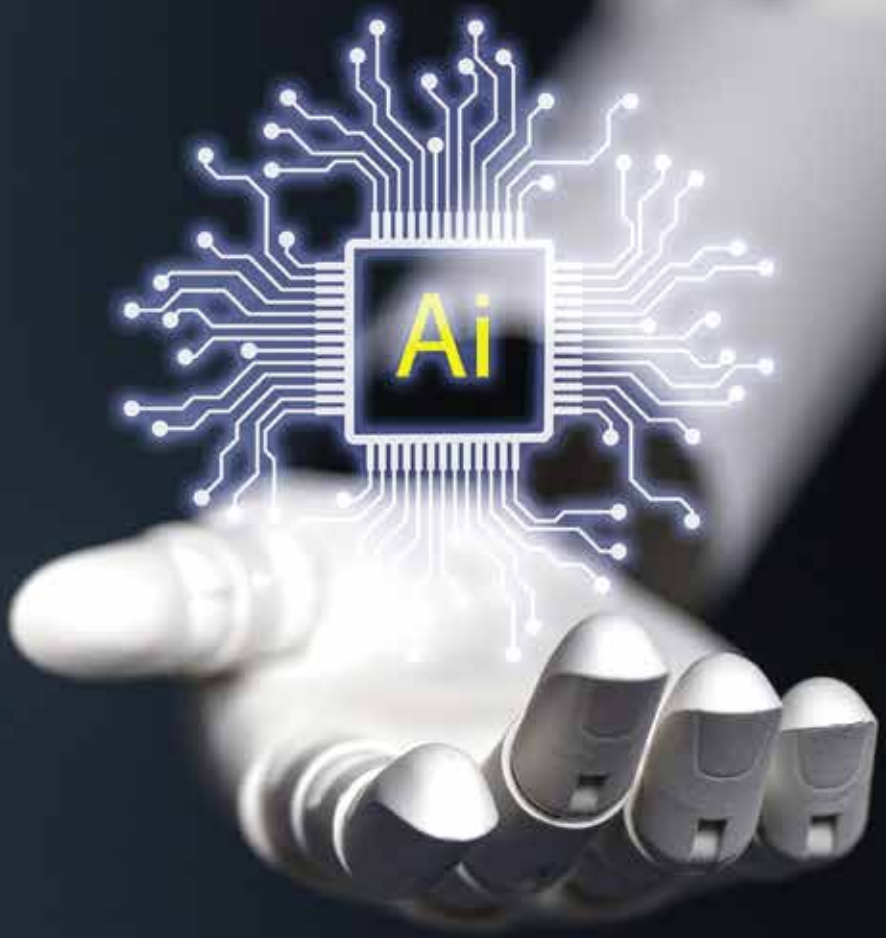
Neben der Reflexion wie OKR im spezifischen Unternehmenskontext wirksamer werden könnte, ist die Auseinandersetzung mit dem Worst-Case-Szenario und dessen bewusster Übertreibung eine hilfreiche Intervention an unterschiedlichsten Stellen des OKR-Lebenszyklus. Dazu ziehe ich gerne meine „Checkliste für erfolgreiches Scheitern mit OKR" zu Rate. Diese hat keinen Anspruch auf Vollständigkeit. Vielmehr ermuntere ich die Beteiligten, diese zu ergänzen und sich dadurch bewusst zu machen, was im Umkehrschluss besser gemacht werden soll.

Christina Lange

OKR in der Praxis:
Objectives & Key Results – Beispiele, Hacks, Erfahrungen;
1. Auflage BusinessVillage 2022

DAS GEHEIMNIS HINTER CHATGPT

WIE DIE KI ARBEITET UND WARUM SIE FUNKTIONIERT



Niemand hat damit gerechnet – nicht einmal die Entwickler.

ChatGPT hat sich als KI entpuppt, die in der Lage ist, überzeugend auf menschlichem Niveau zu schreiben. Aber wie funktioniert das genau? Was geht in dem „Verstand" einer KI vor?

„Dieses Buch stellt den Versuch dar, prinzipiell zu erklären, wie und warum ChatGPT funktioniert. In gewisser Weise ist es eine Geschichte über Technik. Andererseits ist es aber auch eine Geschichte über Wissenschaft sowie über Philosophie. Und um diese Geschichte zu erzählen, müssen wir ein bemerkenswertes Spektrum an Ideen und Entdeckungen zusammenbringen, die im Laufe vieler Jahrhunderte gemacht wurden."

Der bekannte Wissenschaftler und Pionier Stephen Wolfram liefert in diesem Buch eine lesenswerte fesselnde Erläuterung der Funktionsweise von ChatGPT, die aus seiner jahrzehntelangen Erfahrung in der IT-Forschung schöpft. Mit anschaulichen Schaubildern und realen Beispielen bietet er einen Blick hinter die Kulissen des beliebten Chatbots. Dabei gibt er nicht nur einen leicht verständlichen Einblick in die Arbeitsweise und das Training neuronaler Netze, sondern zeigt auch detailliert, wie die Sprachverarbeitung von ChatGPT funktioniert und welche Rolle Syntax und Semantik der menschlichen Sprache dabei spielen.

Finden Sie heraus, wie ChatGPT die modernste Technologie neuronaler Netze mit grundlegenden Fragen bezüglich der Sprache und des menschlichen Denkens vereint und wie inhaltlich falsche Ausgaben unter Zuhilfenahme von Wolfram|Alpha vermieden werden können.

Das Geheimnis hinter ChatGPT
Wie die KI arbeitet und warum sie funktioniert

Stephen Wolfram,
mitp Verlags GmbH & Co.KG

Rein in den Container?

DIE VORTEILE DIESER VIRTUALISIERUNGSTECHNOLOGIE

In den vergangenen Jahren sind verschiedene Container Technologien und Laufzeitumgebungen auf den Markt gekommen. Jede Technologie versucht einen bestimmten Markt zu adressieren. Neben einer Reihe von populären Laufzeitumgebungen die unter dem Dach der Cloud Native Computing Foundation (CNCF) gebündelt sind existiert noch eine weitere Kategorie, die sogenannten System Container.

Die Hauptaufgabe eines System Containers besteht im Gegensatz zu einem Docker oder Kubernetes Container darin, eine vollständige Linux Installation in einer isolierten Umgebung zu betreiben. Dabei kommt nur ein einziger Linux-Kernel zum Einsatz, welche auf einem Bare Metal System gestartet wird. Die Linux Distribution auf dem Hostsystem kann sich von den verwendeten Distributionen innerhalb der Container unterscheiden. Es wird eine komplette Linux Distribution vom Init-Prozess bis zum Erreichen des Runlevel 3 (Mehrbenutzerbetrieb mit Netzwerk) gestartet. Eines der besonderen Merkmale von System Containern ist der unabhängige Root-Zugriff auf die Container Installation. Jeder Container verfügt über ein eigenes isoliertes Netzwerk mit eigener IP-Adresse.

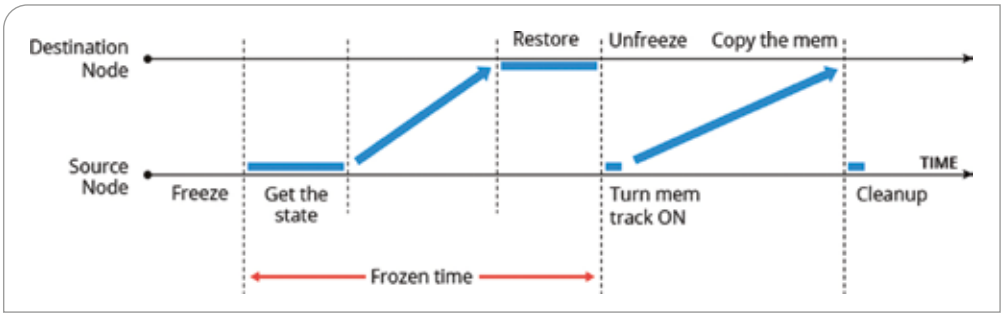
Welche Vorteile bieten System Container?

Die System Container Technologie ist eine ausgereifte und erprobte Technologie, die weltweit von vielen Unternehmen eingesetzt wird. System Container sind flexibel einsetzbar, in wenigen Schritten provisioniert und bieten aufgrund der dynamischen Ressourcenverwaltung ein Maximum an Skalierbarkeit. Nahezu jede Ressource – wie Anzahl der CPUs, Arbeitsspeicher, Festplattenplatz und die Netzwerkkonfiguration kann zur Laufzeit ohne Neustart des Containers verändert werden. Dies gilt sowohl für das Erweitern als auch verkleinern der Ressourcen.

Ressourcenlimits können in mehreren Varianten verwaltet werden. In einem einfachen Verfahren, das sich an den verfügbaren Ressourcen eines Bare Metal Systems orientiert. In dieser Variante wird Arbeitsspeicher, virtueller Arbeitsspeicher (Swap), Anzahl der CPUs und die Größe der virtuellen Festplatte konfiguriert. Mithilfe einer sehr granularen Ressourcenverwaltung UBC (User Beancounters) lassen sich sehr spezifische Limits setzen. So können System Container zum Beispiel die maximale Anzahl der verfügbaren Netfilter (iptables) Einträge begrenzen. Die Anzahl der maximal offenen File Handles lässt sich ebenso limitieren, wie die Anzahl der maximal erlaubten TCP oder Unix Sockets. Ebenso ist es möglich System Container Zugriff auf bestimmte Kernelmodule zu

IM ZUSAMMENSPIEL MIT EINEM VERTEILTEN STORAGE, WIE ZUM BEISPIEL VIRTUOZZO STORAGE, WERDEN DIE CONTAINERDATEN HOCHVERFÜGBAR UND IM FALLE EINES AUSFALLS EINES STORAGE-SERVERS LÄUFT DER CONTAINER WEITER.

Maik Brömme, Senior Produktmanager, Virtuozzo, www.virtuozzo.com



Live-Migrationsprozess eines System Containers zwischen zwei physikalischen Systemen.

gewähren, damit lässt sich steuern, ob ein System Container Stateless-, Stateful- und/oder NAT-Regeln setzen kann. Ebenso ist es möglich einem System Container Zugriff auf TUN/TAP Geräte zu erlauben, um etwa VPNs zu betreiben.

Einmal eingerichtet, laufen System Container ohne Unterbrechung über mehrere Jahre. Im Gegensatz zu Applikationscontainern setzt dies ein dauerhaften (nicht flüchtigen) Datenspeicher voraus. System Container überstehen problemlos einen Neustart des Containers oder des gesamten Hostsystems. Im Zusammenspiel mit einem verteilten Storage, wie zum Beispiel Virtuozzo Storage, werden die Containerdaten hochverfügbar und im Falle eines Ausfalls eines Storage-Servers läuft der Container weiter. Läuft ein Container in einem Cluster, werden diese im Falle eines Ausfalls des Hostsystems automatisch auf einem anderen Knoten im Cluster neugestartet.

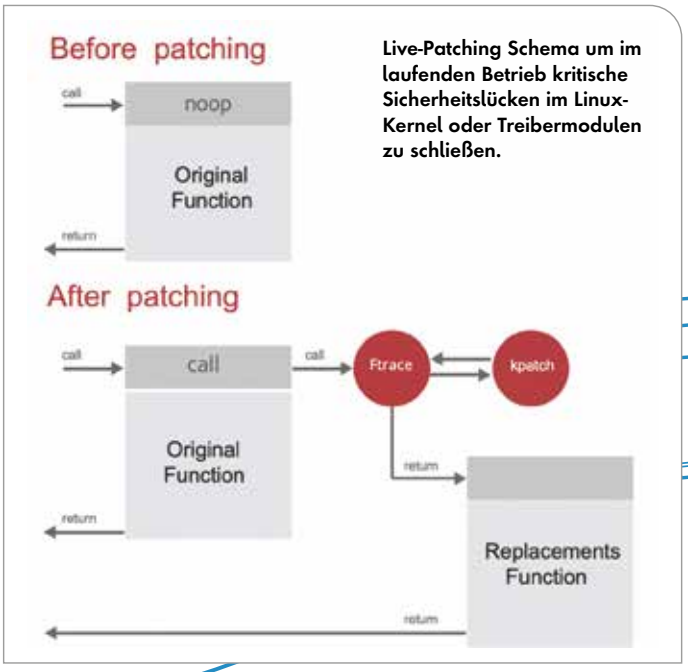
System Container unterstützten weiterhin das Einfrieren und Fortsetzen aller laufenden Prozesse innerhalb der eigenen Umgebung, damit lassen sich ganze Container pausieren und zu einem späteren Zeitpunkt weiterbetreiben. Dies wird durch CRIU (Checkpoint and Restore in Userspace) ermöglicht. Ein pausierter Container lässt sich damit auch zur Laufzeit von einem Server auf einen anderen mittels P.Haul migrieren. Die Live-Migration ist in zwei unterschiedlichen Verfahren möglich.

Pre-Copy-Modus: Vor der Live-Migration wird auf dem ursprünglichen Server die Speicherverfolgung aktiviert, um Änderungen parallel während des Migrationsprozesses zu verfolgen. In diesem iterativen Prozess werden die Änderungen immer kleiner, bis die Speichermigration abgeschlossen ist. Nachdem kopieren des Arbeitsspeichers wird der Container eingefroren und der restliche Containerstatus migriert. Diese Art der Migration ist sehr sicher, ihre Laufzeit kann aufgrund unvorhersagbarer Speicheränderungen aber nicht berechnet werden.

Post-Copy-Modus: Der Container wird zum Beginn der Live-Migration direkt eingefroren. Dann wird die Speicherverfolgung aktiviert und die sich am häufigsten ändernden Speicherseiten werden migriert. Dann wird direkt der Containerstatus migriert. Der Container wird dann auf dem Zielserver wieder fortgesetzt und dann im Hintergrund die restlichen Änderungen migriert. Dies wird auch Lazy Migration genannt. Diese Art der Migration ist unsicher, da beim Verlust des ursprünglichen Servers während der Migration der Container nicht weiterlaufen kann, die Laufzeit der Migration kann im Voraus berechnet werden.

Mithilfe von Virtuozzo Storage wird die Live-Migration beschleunigt und die I/O-Belastung des darunterliegenden Systems drastisch reduziert, da die Daten verteilt im Storage Cluster liegen und somit nicht mehr von einem Server auf einen anderen transferiert werden müssen. In diesem Fall muss nur noch ein Abbild des genutzten Speichers migriert werden.

Außerdem unterstützen System Container in Virtuozzo Hybrid Server Live Kernel Security Updates ohne Neustart des Containers oder Bare Metal Servers. Security Fixes und kleinere Bug-Fixes im Linux Kernel oder Kernelmodulen werden zur Laufzeit ohne Containerausfall installiert. Die Quelltext Patches werden dabei analysiert und es wird für den Li-



Live-Patching Schema um im laufenden Betrieb kritische Sicherheitslücken im Linux-Kernel oder Treibermodulen zu schließen.

nux Kernel ein passender Binärpatch erstellt und als passendes Kernelmodul mithilfe von ReadyKernel ausgeliefert.

Warum sollte ich System Container einsetzen?

Neben den oben erwähnten technischen Merkmalen werden System Container besonders häufig aufgrund ihrer Sicherheit und Isolierung eingesetzt. Idealerweise sind System Container speziell auf den Anwendungsfall der Überprovisionierung von Ressourcen ausgelegt und getestet. Aufgrund verschiedener Optimierungen, wie zum Beispiel Speicher- und IOPS-Deduplizierung, erreichen diese eine doppelte Packungsdichte gegenüber virtuellen Maschinen und eine bis zu 30 Prozent höhere Packungsdichte als System Container unter OpenVZ. Im Gegensatz zu OpenVZ bieten Virtuozzo System Container ein integriertes blockbasiertes Backup inklusive CBT (Change Block Tracking). Backups können sowohl lokal als auch remote gesichert werden. Insbesondere Hosting Service Provider setzen aufgrund der Packungsdichte auf System Container.

Außerdem eröffnen System Container einen weiteren einzigartigen Einsatzzweck. Sie erlauben das Ausführen von Kubernetes oder Docker Applikationscontainern innerhalb eines System Containers (Nested Containerization). Die Vorteile für Applikationscontainern sind eine sehr granulare Ressourcenzuweisung, Unterstützung für persistente Datenspeicher, Live Kernel Security Updates, Live-Migration und Backup und Restore der darüberliegenden System Container.

Maik Brömme

DIGITALE TRANSFORMATION GESTALTEN

GESCHÄFTSMODELLE, ERFOLGSFAKTOREN, CHECKLISTEN

Digitale Transformation gestalten
– Geschäftsmodelle, Erfolgsfaktoren, Checklisten;
Prof. Dr. Oliver Gassmann, Philipp Suttter, 08-2023

Gestalten Sie aktiv den digitalen Wandel, nutzen Sie Chancen und meistern Sie die digitale Transformation gewinnbringend!

- Digitale Geschäftsmodelle erfolgreich und nachhaltig entwickeln
- Erfolgsfaktoren, Fähigkeiten und Potenziale bei der Führung von Digitalisierungsprojekten
- Entdecken Sie neue Möglichkeiten durch intelligente, vernetzte Produkte und das Internet of Things

Digitalisierung hat sich zum strategischen Wettbewerbsfaktor entwickelt. Auch wenn die digitale Transformation alle Branchen in unterschiedlicher Geschwindigkeit erfasst, kann sich keine Industrie dieser Entwicklung entziehen. Um wettbewerbsfähig zu bleiben, müssen Unternehmen den digitalen Wandel und seine Chancen nutzen. Die digitale Transformation betrifft dabei nicht nur IT-Verantwortliche, sondern ist Aufgabe des gesamten Unternehmens.

Führende Autoren aus Wissenschaft und Unternehmen zeigen in konzeptionell-strategischen Beiträgen und Fallstudien, wie die digitale Transformation erfolgreich gestaltet und umgesetzt werden kann. Handlungsanweisungen, Checklisten, Erfolgsfaktoren sowie Hinweise auf Hürden erleichtern den Transfer in die Praxis.

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

EAM: IT-Kosten einsparen

IN FÜNF SCHRITTEN DIE APPLIKATIONSLANDSCHAFT ANALYSIEREN UND IT-KOSTEN EINSPAREN

Mit steigenden Rohstoff- und Beschaffungspreisen, einer noch immer beträchtlichen Inflation und der weiter vorherrschenden allgemeinen Unsicherheit am Markt legen viele Unternehmen intern bereits jetzt die Daumenschrauben bei den Kosten an.

Auch die IT bleibt hiervon wieder nicht verschont. So sehen sich immer mehr IT-Verantwortliche in kleineren und mittelständischen Unternehmen Vorgaben zur Kosteneinsparung im Bereich von zehn bis fünfzehn Prozent gegenüber - meist ohne, dass zuvor geprüft werden konnte, ob und inwiefern sich dieses Ziel überhaupt realisieren ließe.

Produktivität stets im Blick

Eine Aufgabe, die auf den ersten Blick meist unlösbar erscheint. Denn schließlich dürfen wichtige Unternehmensprozesse in Beschaffung, Fertigung, Vertrieb, Marketing, HR, Buchhaltung und Verwaltung keinesfalls durch die IT-seitigen Sparmaßnahmen beeinträchtigt werden. Ganz im Gegenteil: Das oft gleichzeitig von der Geschäftsführung ausgerufene Ziel einer stärkeren Digitalisierung der eigenen Geschäftsprozesse würde eigentlich weitere Investitionen in die IT unumgänglich machen. Bei weniger Budget. Was also tun?

Zumindest theoretisch liegt die einzig gangbare Lösung auf der Hand: Unnötige Ausgaben minimieren, den Ressourceneinsatz optimieren und sicherstellen, dass zukünftige Digitalisierungsmaßnahmen auch tatsächlich einen effizienzsteigernden (und damit kostenoptimierenden) Effekt haben.

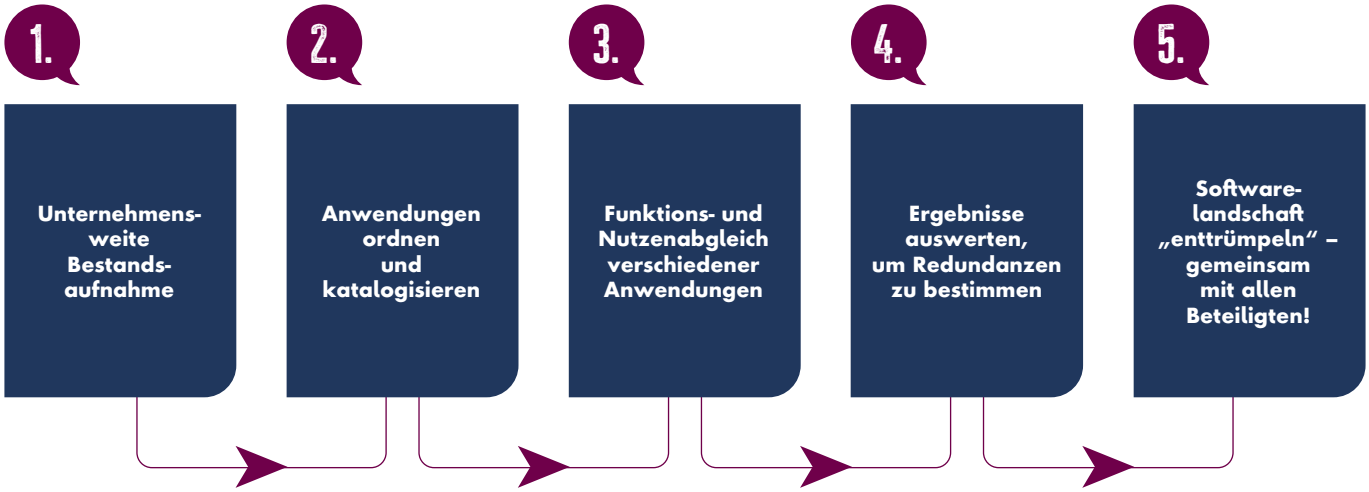
„Wildwuchs" als echtes Problem

Klingt zwar zunächst nach der eierlegenden Wollmilchsau unter den unrealistischen Digitalisierungsstrategien – ist aber trotzdem möglich. Denn gerade die Pandemiejahre haben den softwaretechnischen „Wildwuchs" in den verschiedenen, oft nun auch räumlich stärker voneinander getrennten Unternehmensbereichen begünstigt. Wie viele Softwareanwendungen in dieser Zeit durch einzelne Entscheidungsträger im weit entfernten Homeoffice angeschafft wurden, ist der unternehmenseigenen IT oftmals nicht im Ansatz bekannt. Ein Zustand, den es mit dem gestiegenen Kostendruck nun unbedingt zu beseitigen gilt.

Wie Sie das „Unmögliche" möglich machen, indem Sie Ordnung in den kunterbunten „IT-Zoo" bringen, zeige ich Ihnen in fünf relativ einfachen, wenn auch strategisch höchst effizienten Schritten. Sie werden sehen: Am Ende haben Sie nicht nur aufgeräumt. Sie sitzen auch so fest wie nie im Sattel Ihrer eigenen IT-Strategie.

IT-KOSTEN SPAREN IN 5 SCHRITTEN

Es braucht nur fünf wohlüberlegte Schritte, um dem IT-Wildwuchs aus Homeoffice & Co. wieder Herr zu werden.



#1 Unternehmensweite Bestandsaufnahme

Beginnen Sie zunächst damit, alles zu erfassen, was unternehmensweit an Software zum Einsatz kommt oder in den letzten Jahren womöglich nur kurz zum Einsatz gekommen ist. Mitunter ist die „Dunkelziffer" derjenigen Anwendungen, die zu Beginn der Homeofficepflicht spontan angeschafft – und dann genau so schnell wieder vergessen – wurden, beträchtlich. Auch ist nicht auszuschließen, dass unternehmensweit gleich mehrere Lizenzen parallel angeschafft oder Software mit vergleichbaren Funktionen bei unterschiedlichen Herstellern gekauft wurde.

Softwarekosten zusammentragen

Am besten, Sie gehen für eine erste Bestandsaufnahme in mehreren Schritten vor: Starten Sie damit, die aktuellen unternehmensweiten Kosten für Softwarelizenzen mithilfe der Buchhaltung zusammenzutragen und überprüfen Sie die Daten auf doppelte oder gar noch häufigere Zahlungen.

Software-Inventur durchführen

Führen Sie anschließend eine unternehmensweite Software-Inventur durch. Holen Sie dafür die Entscheider möglichst aller Unternehmensbereiche, Standorte und Abteilungen mit ins Boot und bitten Sie sie, eine entsprechende Inventarliste für ihren Zuständigkeitsbereich auszufüllen. In der Regel reichen hierfür eine einfache Excelliste sowie ein Zeitfenster von ein bis zwei Monaten aus.

Es schadet zudem nicht, auch die Geschäftsführung offen über die gemeinsam abgestimmten Deadlines zu informieren – beispielsweise einfach, indem man diese in CC setzt.

Kleiner Berater-Tipp: Das „ins Boot holen" gelingt übrigens umso besser, je klarer Sie den Vorteil der geplanten Maßnahme für die einzelnen Stakeholder kommunizieren. So werden durch eine Optimierung der Softwarelandschaft im Unternehmen nicht nur bisher unnötigerweise gebundene Mittel in Abteilungsbudgets frei – auch die Verantwortung für Wartung, Aktualität und Unversehrtheit der digitalen Lösungen muss nicht mehr durch die Entscheider selbst getragen werden, sondern lässt sich an die IT abgeben. Ein praktischer Nebeneffekt: Für Software, deren Funktionsfähigkeit in der Verantwortung der unternehmenseigenen IT liegt, ist für gewöhnlich auch der entsprechende IT-Support oft deutlich schneller, einfacher und motivierter verfügbar als für softwaretechnischen „Wildwuchs".

#2 Anwendungen ordnen und katalogisieren

Sind alle im Unternehmen lizensierten, eingesetzten oder zumindest irgendwann erworbenen Softwareanwendungen schließlich erfasst, beginnt die eigentliche Optimierungsarbeit. Denn nun gilt es, das gefundene Sammelsurium an Software und Lizenzen zu sichten, zu katalogisieren und zu bewerten. Welche Maßstäbe und Bewertungsrichtlinien Sie dabei ganz genau ansetzen, hängt natürlich sehr stark von individuellen Faktoren in Ihrem Unternehmen ab. Als grundsätzlich sinnvoll erscheint aber auf jeden Fall eine Bewertung anhand der folgenden drei Schwerpunkte:

Relevanz für das Unternehmen

Wie wichtig ist die Anwendung für Produktivität und Geschäftstätigkeit? Kommt sie lediglich in einzelnen Bereichen zum Einsatz oder gehört sie zu den Produktivitätsgrundlagen weiter Teile der Organisation?

Kapitaleinsatz
Wie hoch sind die bisherigen und die in Zukunft zu erwartenden Kosten für jede einzelne Anwendung? Erfassen Sie hier nicht nur initiale Lizensierungsgebühren, sondern auch wiederkehrende Abonnementkosten, Wartungsverträge und den Aufwand für Support, Betrieb und Wartung. Dazu noch ein Tipp: Besonders die genaue Betrachtung von Lizenzen und Wartungsverträgen birgt hierbei erhebliches Einsparpotenzial. Denn oftmals wurde zunächst die absolute Premiumvariante gewählt, ohne, dass die zusätzlichen Leistungen oder Funktionen genutzt werden.

Nutzeranzahl
Wie häufig wird die Anwendung von wie vielen Mitarbeitenden genutzt? Ist es etwas, das nur einmal im Monat von nur einem Mitarbeiter genutzt wird? Oder erleichtert die Anwendungen vielen Betroffenen erheblich die tägliche Arbeit – und sind dafür nutzungs- oder personenbezogene Lizenzen im Einsatz?

#3 Funktions- und Nutzenabgleich verschiedener Anwendungen

Nun geht es darum, unnötige und doppelte Funktionalitäten oder parallele Anwendungsfälle aufzuspüren und etwaige Synergieeffekte nutzbar zu machen.

Kurzum: Sie müssen alles mit allem vergleichen und dabei herausfinden, wo tatsächliche Einsparpotenziale verborgen liegen. Nutzen alle Abteilungen oder Standorte das gleiche Projektmanagement-Tool, archivieren sie Dokumente auf unterschiedliche Art und Weise oder nutzen sie verschiedene Anwendungen für die digitale Kommunikation im Team?

Die gute Nachricht: Mit zahlreichen, online verfügbaren Tools zum Vergleichen von Softwarelösungen ist das für gängige Anwendungen und Hersteller meist relativ schnell erledigt. Zudem kann auch eine AI-gestützte Recherche hier erheblich Zeit sparen.

#4 Ergebnisse auswerten, um Redundanzen zu bestimmen

In der Regel sollten Sie nach dem letzten Schritt einen ziemlich genauen Überblick darüber haben, welche Anwendungen wo und wie im Unternehmen zum Einsatz kommen. Bleibt eigentlich nur noch die Frage: Warum ist das so – und was kann denn jetzt alles weg?

Bei der Auswertung Ihrer Software-Einsatz-Analyse sollten Sie nun alle augenscheinlichen Redundanzen noch einmal ganz genau unter die Lupe nehmen – und am besten auch einfach nochmal bei den betreffenden Anwendern nachfragen: Wofür braucht man genau diese Softwareversion, was wird tatsächlich damit getan und warum wurde die Software gesondert angeschafft? Gibt es Alternativen, wo liegen Leistungs- und Anwendungsbegrenzungen – und was wäre, wenn die Software nicht mehr zur Verfügung stehen würde?

Oft bieten verschiedene Anwendungen auch vergleichbare Funktionalitäten, die womöglich bisher einfach noch nicht genutzt wurden. Markieren Sie schließlich diejenigen Anwendungen, die auf die „Abschussliste" gehören – und sprechen Sie unbedingt noch einmal mit den betreffenden Anwendern und Anwenderinnen, ob die identifizierten Alternativen auch wirklich ausreichen. Denn: Wer sich nicht „übergangen", sondern einbezogen in den Prozess fühlt, trägt die zu treffenden Entscheidungen auch deutlich wahrscheinlicher aktiv mit – anstatt sich dagegen zu verschließen.

#5 Softwarelandschaft „entrümpeln" – gemeinsam mit allen Beteiligten!

Wie gerade schon angedeutet, geht es im vorerst finalen Schritt in Ihren Bemühungen, die überbordenden IT-Kosten durch redundante und ungenutzte Software einzudämmen, nun um das tatsächliche „Entrümpeln". Hierbei gilt es natürlich wieder, auf eine ganze Reihe wichtiger Faktoren wie Kündigungsfristen, nötige Schulungen für Mitarbeitende und eine lückenlose Migration von einzelnen Datensätzen, archivierten Informationen und ganzen Datenbanken zu achten.

Wichtig ist außerdem darauf zu achten, um welche Art von Anwendung es sich handelt: Anwendungen aus der Cloud kann man nämlich nicht nur relativ einfach kündigen, es müssen auch Daten migriert und Zugänge angepasst werden.

Bei Anwendungen, die dagegen selbst gehostet werden, ist das Ganze meist etwas aufwendiger. Hier muss die komplette Anwendung deinstalliert werden, gegebenenfalls sogar inklusive Test- und

Professionelles Application Portfolio Management gelingt am besten mit einer geeigneten Softwarelösung wie HOPEX

MEHR WERT Kostenlose Vorlage für eine Software-Inventarliste **bit.ly/3VKh0f7**

Entwicklungsumgebung. Zudem gilt es, alle zuvor für den Betrieb der Anwendung genutzten Ressourcen wie Datenbanksoftware, Serversoftware oder virtuelle Maschinen ebenfalls wieder freizusetzen – ganz zu schweigen von den nun wieder freiwerdenden Supportstrukturen vom Service-Desk bis hin zu First-, Second und Third-Level-Support, welcher nun nicht mehr benötigt wird.

Holen Sie betroffene Anwender mit ins Boot!

Wer auch hier nicht einfach „über die Köpfe" der Anwender bestimmt und eine offene, direkte und wertschätzende Kommunikationskultur pflegt, hat erfahrungsgemäß mit weitaus weniger Widerständen zu kämpfen als Sie es von anderen IT-Projekten vielleicht bisher gewohnt sind. Denn am Ende soll das Aufräumen in der IT-Landschaft ja nicht nur Kosten senken, sondern auch Prozesse vereinfachen und Ressourcen freisetzen, die weitaus sinnvoller genutzt werden könnten.

Glauben Sie mir: Ein erfolgreiches „Aha"-Erlebnis in diesem Zusammenhang spricht sich für gewöhnlich ganz von alleine im Unternehmen herum und wird Ihnen und Ihren Bemühungen zur Kostensenkung weitere Abteilungstüren öffnen, die Ihnen womöglich sonst vor der Nase zugeschlagen wurden.

Nach der Inventur ist vor der Inventur

Sie werden es bereits ahnen, oder? Leider ist es nicht damit getan, einmal Tabula Rasa im „IT-Zoo" zu machen. Zwar haben Sie für gewöhnlich nun erstmal ein wenig Ruhe, doch wo einmal „Wildwuchs" entstanden ist, lässt das nächste IT-Unkraut für gewöhnlich nicht allzu lange auf sich warten. Und: Nachdem Sie die komplette Anwendungslandschaft nun einmal unter Ihre zentrale Obhut gebracht haben, müssen Sie diese auch so effizient wie möglich verwalten. Um das zu bewerkstelligen, empfiehlt sich ab einer gewissen Größe des zu administrierenden Softwareportfolios der Einsatz einer dedizierten Application Portfolio Management (APM) Software sowie die Einführung eines gemanagten Softwareauswahlprozesses.

Letzterer kann übrigens durch ein EA-Team sehr gut als nützliche und hochgeschätzte IT-Dienstleistung für das gesamte Unternehmen angeboten werden. Denn wenn EA gleich von vornherein dabei hilft, treffsicher die optimale Anwendung auszuwählen, profitieren alle Beteiligten – und der IT-Zoo bleibt künftig unter Ihrer Kontrolle.

Daniel Kubosch

AM ENDE SOLL DAS AUFRÄUMEN IN DER IT-LANDSCHAFT NICHT NUR KOSTEN SENKEN, SONDERN AUCH PROZESSE VEREINFACHEN UND RESSOURCEN FREISETZEN, DIE WEITAUS SINNVOLLER GENUTZT WERDEN KÖNNTEN.

Daniel Kubosch,
Partner / Senior Business Consultant,
EAM Trusted Advisor GmbH,
www.trusted-advisor.com

it management

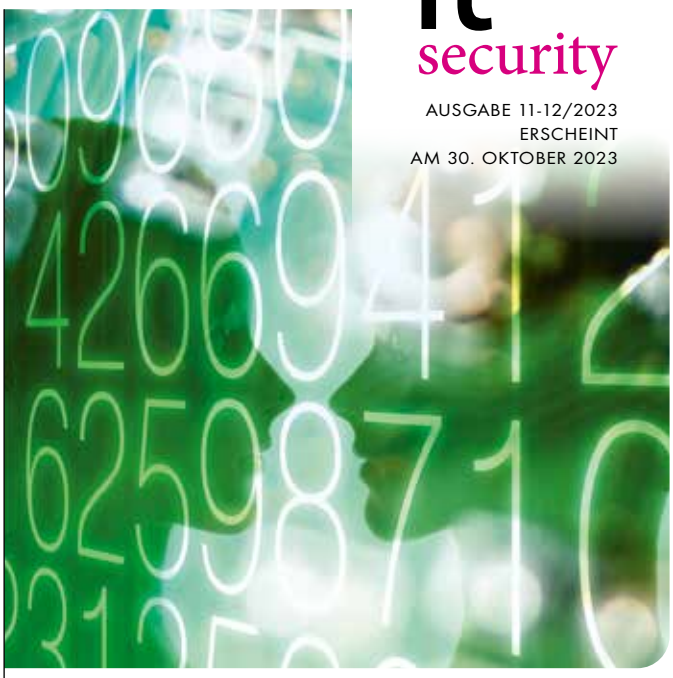
AUSGABE 11-12/2023
ERSCHEINT
AM 30. OKTOBER 2023

UNSERE THEMEN

Innovationen 2024
IT-Lösungen & Nachhaltigkeit
Data Management

it security

AUSGABE 11-12/2023
ERSCHEINT
AM 30. OKTOBER 2023



UNSERE THEMEN

Innovationen 2024
AI / KI Security
Sicherheitsmanagement

WIR WOLLEN IHR FEED BACK
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)

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

Autoren: Dr. Steele Arbeeny, Lars Becker, Maik Brömme, Philipp von der Brüggen, Björn Dunkel, Alina Feldmann, Andrea Ferro, Peter Gatzen, Daniel Kubosch, Lena Kulik, Christina Lange, Simon Meraner, Carina Mitzschke, Silvia Parthier, Ulrich Parthier, Christoph Schuler, Orli Shahidi, Martin Stemplinger, Jan Svacina, Amadeus Thomas, Adrian Trickett, Andreas Viehhauser, Markus Wühr, Awraam Zapounidis

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

Erscheinungsweise: 6 x pro Jahr

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

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

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


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

WIR SIND DABEI!

Aagon

itsa 365

10. bis 12. Oktober
in Nürnberg

Halle 6
Stand 400

IT-Security

Unified Endpoint Management

Vortrag

„Automatisierung der IT mit Unified Endpoint Management (UEM)“
11.10.2023 | 11:15 Uhr | Halle 6

Mehr erfahren und
Gratis-Dauerkarte sichern:
www.aagon.com/it-sa2023

PUR 2023
Professional User Rating

ACMP
ist 4fach Champion

Aagon

it security

Detect. Protect. Respond.
September/Oktober 2023

THOUGHT LEADERSHIP

AB **SEITE 8**

SOPHOS

STORMSHIELD
Modernste Lösungen gegen Cybercrime
ab Seite 12

zscaler
Mit Zero Trust in die Transformation
ab Seite 20

TIXEO
Maximal sichere Videokonferenzen
ab Seite 24

THREAT INTELLIGENCE & ALL-IN-ONE-ANSATZ

Top-Cyberschutz

Waldemar Bergstreiser, Kaspersky

SECURITY ORCHESTRATION

Mit Perfektion zu besserem Schutz

KÜNSTLICHE INTELLIGENZ

Die richtige Seite der Macht

DIGITALE IDENTITÄTEN

Reibungsloser und sicherer Nachweis


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

Inhalt

COVERSTORY

THOUGHT LEADERSHIP

IT-SA SPEZIAL

IT SECURITY

Top-Cyberschutz

THREAT INTELLIGENCE UND ALL-IN-ONE-ANSATZ

Während sich Führungskräfte zu Recht auf Umsatz, Kundenerlebnis, Risiko und Kosten konzentrieren, geht es IT- und Cybersicherheitsexperten um den Schutz von Geräten, Netzwerken, Programmen und Daten vor unbefugtem Zugriff und Schäden. Die Konzentration auf unterschiedliche Ziele kann zu Missverständnissen in der Vorstandsetage führen und dazu beitragen, dass die Bedeutung von Cybersicherheit unterschätzt wird. Vor dem Hintergrund einer zunehmenden Professionalisierung der Cyberkriminalität skizziert Waldemar Bergstreiser, General Manager Central Europe bei Kaspersky, wie ein nachhaltiges und effektives Cybersicherheitsniveau durch einen ganzheitlichen Ansatz basierend auf mehreren Schutzdimensionen, einschließlich Threat Intelligence (TI), erreicht werden kann.

? **Ulrich Parthier:** *Wie schätzen Sie die aktuelle Bedrohungslage ein und was bedeutet das für Unternehmen?*

Waldemar Bergstreiser: Die Analysen des Kaspersky Security Bulletin (1) zeigen, dass Cyberkriminalität zunehmend zu einem Geschäftsmodell wird. Cyberkriminelle optimieren ihr Geschäft, ähnlich wie es auch legitime Unternehmen tun, skalieren zu diesem Zweck ihre Operationen und lagern bestimmte Aktivitäten aus, weshalb Malware-as-a-Service boomt. So wird es für weniger versierte Cyberkriminelle relativ einfach, Cyberangriffe zu starten: sie mieten geeignete Malware-Tools. Zugleich werden Angriffsmethoden immer komplexer.

Deshalb reichen automatisierte Abwehrsysteme als alleiniges Mittel für eine umfassende Sicherheit nicht mehr aus. Unternehmen müssen die Anzeichen eines drohenden Cyberangriffs sofort erkennen und vorbeugende Maßnahmen ergreifen – im Idealfall bevor Schaden entsteht. Dazu benötigen sie einen mehrdimensionalen Sicherheitsansatz, der technische Lösungen zur Erkennung und Abwehr von Cyberangriffen und Präventivmaßnahmen mit menschlicher Expertise kombiniert.

? **Ulrich Parthier:** *Wie sieht ein solcher multidimensionaler Sicherheitsansatz aus?*

Waldemar Bergstreiser: Idealerweise setzt sich eine effiziente Schutztechnologie aus maschinellem Lernen und künstlicher Intelligenz sowie umfassenden Automatisierungsfunktionen zusammen, damit sich die unternehmensinternen Cybersicherheitsabteilungen auf andere Kernaufgaben konzentrieren können. Eine solche Lösung sollte fortschrittliche Bedrohungserkennung, eine einfache Untersuchung und automatisierte Reaktion auf Cybervorfälle bieten – entweder vor Ort, in der Cloud oder hybrid. Außerdem muss sie an die jeweilige IT- oder OT-Infrastruktur angepasst werden. Als zusätzliche Schutzdimensionen bieten sich dann solide TI-Funktionen, Managed Security Services rund um die Uhr, Cybersicherheits-Awareness-Trainings und professionelle Services wie Audits, Implementierung, Optimierung und Wartung an. Wir nennen das einen All-in-One-Cyberschutz.

? **Ulrich Parthier:** *Welche Rolle spielt Threat Intelligence in diesem Mix?*

Waldemar Bergstreiser: Entscheider und vor allem Cybersicherheitsexperten benötigen Hilfe, um die Sicherheitsbedrohungen zu verstehen, mit denen ihre Unternehmen täglich konfrontiert sind – andernfalls besteht die Gefahr, dass sie sich unzureichend gegen Cyberkriminelle wappnen. Ein vielschichtiger Ansatz dafür umfasst Bedrohungsdaten, also TI, die öffentlich zugängliche Nachrichtenquellen und Informationen aus den sozialen Medien mit verwertbaren Informationen aus dem Dark Web kombiniert und die dann von Experten ausgewertet und

KASPERSKY ALL-IN-ONE CYBERSCHUTZ

Die Professionalisierung der Cyberkriminalität erfordert ein mehrdimensionales Schutzkonzept aus innovativen Abwehrtechnologien, Prävention und menschlicher Expertise.

Unter diesem Shortlink erfahren Sie mehr über den All-in-One Cyberschutz von Kaspersky: **kas.pr/all-in-1**

interpretiert werden. TI liefert so ein umfassendes und aussagekräftiges Verständnis über den gesamten Zyklus des Incident Managements, da Experten einen detaillierten Einblick in Cyberbedrohungen erhalten, die speziell auf ihre Organisation abzielen.

> ENTSCHEIDER UND VOR ALLEM CYBERSICHERHEITSEXPERTEN BENÖTIGEN HILFE, UM DIE SICHERHEITSBEDROHUNGEN ZU VERSTEHEN, MIT DENEN IHRE UNTERNEHMEN TÄGLICH KONFRONTIERT SIND.
>
> **Waldemar Bergstreiser, General Manager Central Europe, Kaspersky, www.kaspersky.de**

Ulrich Parthier: *Ist dies auch ein realistischer Ansatz für kleine und mittelständische Unternehmen? Wie können diese TI und einen All-in-One-Cyberschutz umsetzen?*

Waldemar Bergstreiser: Häufig denken KMU ja, dass sie durch ihre geringe Größe weniger gefährdet sind, weil sie meinen sie befänden sich noch quasi unter der Aufmerksamkeitsschwelle der Cyberkriminellen. Das stimmt allerdings immer weniger, je mehr die Angreifer ihre Methoden perfektionieren. Nach einer aktuellen Studie von Kaspersky hat über ein Viertel der befragten Unternehmen in Deutschland zwischen 100 und 500 Mitarbeitern bereits einen Cybervorfall erlebt. (2) Deshalb brauchen auch KMU dringend einen umfassenden proaktiven Cyberschutz. Unternehmen, die über kein eigenes Sicherheitsteam verfügen, sollten die Auslagerung von Cybersicherheit, inklusive der Erkennung und Reaktion auf Vorfälle, an externe Sicherheitsanbieter in Betracht ziehen. Dies erweist sich oft als kosteneffizienteste Lösung, da sie so die Sicherheits- und Einstellungsbudgets entlasten und gleichzeitig Cyberbedrohungen zuverlässiger und schneller aufdecken – was wiederum die möglichen Folgeschäden erheblich reduziert.

Ulrich Parthier: *Immer mehr Unternehmen setzen dabei auf Managed Security Provider. Können solche MSP-Dienste über einen Experten vor Ort bezogen werden?*

Waldemar Bergstreiser: Genau, immer mehr Unternehmen wenden sich an Managed Service Provider (MSP) und Managed Security Service Provider (MSSP), um ihre digitale Transformation effektiv zu managen. Laut der MSP Market Focus Studie 2021 (3) von Kaspersky haben sowohl MSPs als auch MSSPs ihren Kundenstamm seit 2019 um 91 Prozent bzw. 81 Prozent vergrößert – und dieser Trend setzt sich aktuell fort. Um eine starke Cybersicherheit zu gewährleisten, müssen MSPs einen ganzheitlichen Ansatz verfolgen und eng mit einem vertrauenswürdigen Cybersicherheitsanbieter zusammenarbeiten. Dabei sollten sie besonderes Augenmerk auf dessen Technologie, Fachwissen und spezifische Ressourcen legen. Wir selbst verfügen über ein gut ausgebautes Netzwerk erfahrener Partner, die regelmäßig geschult und zertifiziert werden. Partner wie Kunden profitieren von der führenden TI sowie der umfassenden Lösungskompetenz von Kaspersky. Denn Unternehmen können sich auf über 25 Jahre Expertise verlassen und Partner können sich durch unser TI-Angebot vom Wettbewerb differenzieren und ihre Kunden bestmöglich schützen.

Ulrich Parthier: *Herr Bergstreiser, wir danken Ihnen für das Gespräch.*

Quellen:
(1) https://securelist.com/corporate-threat-predictions-2023
(2) kas.pr/cyberresilienz
(3) https://www.kaspersky.com/blog/msp-report-2021/

Die 7 Phasen der Cyberresilienz

WIE KMUs DIE ACHTERBAHNFAHRT FÜR DEN DATENSCHUTZ MEISTERN

Heutzutage sind Daten das mit Abstand wertvollste Gut jedes modernen Unternehmens – unabhängig von der Branche und egal, wie groß es ist. Wenn Unternehmen durch einen technischen Ausfall, einen Cyberangriff oder eine Naturkatastrophe den Zugriff auf die Daten verlieren, sind Teilbereiche oder sogar der komplette Betrieb gefährdet. Aus diesem Grund sind die Ausfallsicherheit und die Resilienz eine zwingende Notwendigkeit.

Resiliente Unternehmen im Sinne des Datenschutzes und der Datensicherheit verfügen über Prozesse, die ihnen eine schnelle Erholung von jeder datenkritischen Situation garantieren. Allerdings ist längst nicht jedes Unternehmen mit dieser Widerstandsfähigkeit ausgestattet. Im Gegenteil – die meisten KMUs sind es nicht. Eine kürzlich von Arcserve durchgeführte internationale Studie bestätigt, dass nur 23 Prozent der kleinen und mittelständischen Unternehmen über ausgereifte Resilienzstrategien für die Datensicherheit verfügen.

Darüber hinaus bestehen nach wie vor weit verbreitete Missverständnisse im Bereich des Cyberschutzes. Zwar kennen KMUs die potenzielle Gefahrenlage durch Cyberbedrohungen, allerdings sind viele der Meinung, dass vornehmlich größere Unternehmen ins Fadenkreuz der Angreifer geraten. In Wahrheit jedoch selektieren Cyberkriminelle nicht nach Branche oder Unternehmensgröße. Sie haben es auf jedes potenzielle Opfer abgesehen, unabhängig davon, wie klein oder groß es sein mag.

Die 7 Phasen der Cyberresilienz

Beim Menschen und in der Psychologie existiert ein Prozess, den Fachleute mit „sieben Phasen der Trauer" beschreiben. Hierbei geht es um eine psychologische Abfolge, wenn Menschen einen tiefgreifenden Verlust oder Trauerfall erleben. Wendet man diese „sieben Trauerphasen" auf KMUs mit Datenschutzproblemen an, stellen sich diese wie folgt dar:

1. **Schock und Leugnung**
2. **Schmerz und Schuldgefühle**
3. **Wut und Verhandlungsbereitschaft**
4. **Depression**
5. **Aufwärtstrend**
6. **Wiederaufbau und Aufarbeitung**
7. **Akzeptanz und Hoffnung**

Mehrwerte eines Dienstleisters

Aufgrund mangelnder Ressourcen konzentrieren sich viele mittelständische Unternehmen intensiv auf ihr Tagesgeschäft. Nicht selten kommen dabei die IT und insbesondere der Datenschutz zu kurz. Deshalb ist es für viele KMUs eine sinnvolle Option, mit einem spezialisierten Dienstleister zusammenzuarbeiten, der über ausgewiesene Expertise in den Bereichen Datensicherung, Cybersicherheit und Datensicherheit verfügt. Die Zusammenarbeit mit einem Dienstleister, der sich mit Best Practices auskennt und mit führenden Lösungsanbietern zusammenarbeitet, erweitert nicht nur das IT-Knowhow im Unternehmen, sondern sorgt gleichzeitig für einen soliden Plan für die Datensicherheit und die Einhaltung der Datenschutzvorschriften.

Dabei sind naturgemäß auch die Kosten für KMUs ein wichtiges Thema. Während größere Unternehmen ausreichend Personal oder sogar eine ganze Abteilung für die Cybersicherheit und Datensicherung abstellen können, ist das bei vielen KMUs keine realistische Option. Durch die Zusammenarbeit mit einem Service-Provider kann ein mittelständisches Unternehmen kostengünstig auf die benötigten Verfahren und Fachkenntnisse zugreifen. Dank einer solchen Partnerschaft können sie sich auf ihr Kerngeschäft und das Unternehmenswachstum konzentrieren, während sich sachkundige Experten um die Ausfall- und Wiederherstellungsstrategien kümmern.

www.arcserve.com

SECURITY SERVICES

Cyberbedrohungen und Datensicherheitsverletzungen sind nicht erst seit kurzem ernsthafte Unternehmensrisiken. Sie verursachen finanzielle Verluste, schädigen den Ruf des Unternehmens und beeinträchtigt das Vertrauen der Kunden. Daher sollte es für Unternehmen jeglicher Größe und Branche von entscheidender Bedeutung sein, auf umfassende Security Services zu setzen. Nicht nur, dass diese eine aktive Verteidigung gegenüber Bedrohungen anbieten, sie tragen auch dazu bei, proaktiv Risiken zu minimieren und sensible Daten zu schützen sowie die Compliance sicherzustellen.

Je hochwertiger der Security Services, desto besser für die Kontinuität und die Reputation.

Das perfekte Ziel für Cyberkriminelle

WARUM MAN UNBEDINGT AUF SECURITY-SERVICES SETZEN SOLLTE

Cybersecurity zu betreiben ist ein äußerst komplexes Thema. Angriffsvektoren verschärfen und verändern sich fortlaufend. Gleichzeitig steigen die Anforderungen seitens der Gesetzgeber. Gepaart mit dem voraussichtlich langfristigen Mangel an qualifizierten Security-Experten haben Unternehmen eine harte Nuss zu knacken. Ulrich Parthier, Publisher it security, sprach mit Sven Janssen, Regional Vice President EMEA Central Sales bei Sophos, über die Herausforderungen aber auch Chancen, denen sich Unternehmen und Security-Anbieter in gleicher Mission gegenübersehen.

ES GEHT KEIN WEG AN SECURITY-SERVICES VORBEI, UM UNTERNEHMEN EFFEKTIV ZU SCHÜTZEN UND UM DIE GESETZLICHEN VERPFLICHTUNGEN ZU ERFÜLLEN.

Sven Janssen,
Regional Vice President EMEA Central Sales,
Sophos, www.sophos.de

Ulrich Parthier: *Herr Janssen, täglich liest man über neue Gefahren, Zero-Day-Attacken, Lücken in bestehenden Systemen und Lösungen. Man hat das Gefühl, als wäre man zwangsläufig der nächste, den es trifft. Was sagen Ihre Forschungen und Beobachtungen?*

Sven Janssen: Tatsache ist, dass unsere Forensiker und Labs-Teams täglich neue potenzielle Gefahren und Sicherheitslücken finden, die auch ausgenutzt werden. Hierbei kann es sich um gezielte Attacken handeln, bei denen wenige Unternehmen individuell angegriffen und mit sehr hohen Ransomware-Erpressungssummen zu Kasse gebeten werden, oder auch um breit angelegte Kampagnen, die jedes Unternehmen und jede Organisation treffen können. Cyberkriminellen geht es fast immer darum, möglichst viel Geld zu erbeuten. Für den größtmöglichen Fang lassen sie sich ständig neue Strategien und Taktiken einfallen – und sie sind sehr gut in dem, was sie tun.

Ulrich Parthier: *Haben Sie konkrete Zahlen und wie hoch schätzen sie die Dunkelziffer ein?*

Sven Janssen: Unser jüngster State of Ransomware Report zeigt, dass in Deutschland 58 Prozent, in Österreich 50 Prozent und in der Schweiz sogar 75 Prozent der Unternehmen mit Ransomware angegriffen wurden. Ein Angriff bedeutet nicht gleichzeitig einen Erfolg für die Angreifer. Bei 49 Prozent der Unternehmen in Deutschland, 70 Prozent in Österreich und 60 Prozent in der Schweiz ist es den Angreifern gelungen, ihren Angriff erfolgreich abzuschließen und Daten zu verschlüsseln. Aus unserer Sicht und sicherlich auch aus der Sicht der Geschädigten, ist dies eine hohe Rate und sie steigt seit Jahren kontinuierlich. Die Cybergangster nutzen jede Gelegenheit und Technologie, um ans Ziel zu gelangen.

Zur Dunkelziffer befragt man am besten die Glaskugel. Wir gehen davon aus, dass ein beträchtlicher Teil der angegriffenen Unternehmen dies nicht kundtut oder es nicht bemerkt. Denn es gibt ja auch die Variante, dass bei einem Angriff Daten unbemerkt gestohlen wurden, jedoch keine Ransomware aktiviert wurde.

Ulrich Parthier: *Welche Angriffstaktiken gehören heute zu den gefährlichsten?*

Sven Janssen: Wir sollten hier weniger von den gefährlichsten Angriffstaktiken reden, sondern eher von denen, auf die Unternehmen weniger gut vorbereitet sind. Die größte Hürde für die Angreifer ist es, den Schutzperimeter der Unternehmen zu durchbrechen. Hierfür kommen cyberkriminelle Mittel zum Einsatz, die nicht zwangsläufig besonders kompliziert sein müssen, jedoch wirksam und erfolgversprechend. Ein zusätzlicher Gefahrenfaktor besteht darin, dass sich die großen Cybercrime-Gruppen in spezialisierte Task-Force-Einheiten und Sub-Gruppen eingeteilt

haben, die sehr professionell und effizient Teile der Angriffskette durchführen. Das große Ganze führt dann zu erfolgreichen Angriffen.

Ulrich Parthier: *Haben Sie hierfür Beispiele?*

Sven Janssen: Ein prominentes Beispiel ist die Nutzung von GPT-Technologien. Eine der größten Gefahren für die IT-Security ist der Mensch. Cyberkriminelle nutzen diese Schwachstelle, um an die Zugangsdaten oder Verbindungswege ins Unternehmen zu gelangen. Phishing-Angriffe und Social-Engineering sind die bevorzugten Taktiken. Zwar haben viele Unternehmen ihre Mitarbeitenden gut darauf trainiert, Fake-Nachrichten und gefälschte E-Mails zu erkennen. Aber durch die Nutzung von GPT-Technologien stellen sich die Phishing-Nachrichten so perfekt in Erscheinungsbild und Sprache dar, dass es den meisten Mitarbeitenden nicht mehr möglich ist, gute von schlechten Nachrichten zu unterscheiden. Im Grunde ein alter Trick, aber auf einem ganz neuen Niveau. Sind die Zugangswege über diese Taktik ergründet, folgen weitere Schritte, um das Netzwerk der Organisation zu infiltrieren.

Ein anderes Beispiel ist der Weg über die Supply-Chain. Durch die weltweite Vernetzung und durch die immer häufigere Bereitstellung von Software-Lösungen über die Cloud, kommen Cyberkriminelle durch die Hintertüre ins Unternehmen. Folglich müssen sich Unternehmen nicht nur um die eigene Sicherheit kümmern, sondern auch um die Security ihrer Supply Chain. Das ist eine zusätzliche Aufgabe, die für viele Unternehmen neben ihrer Kernaufgabe kaum zu bewältigen ist.

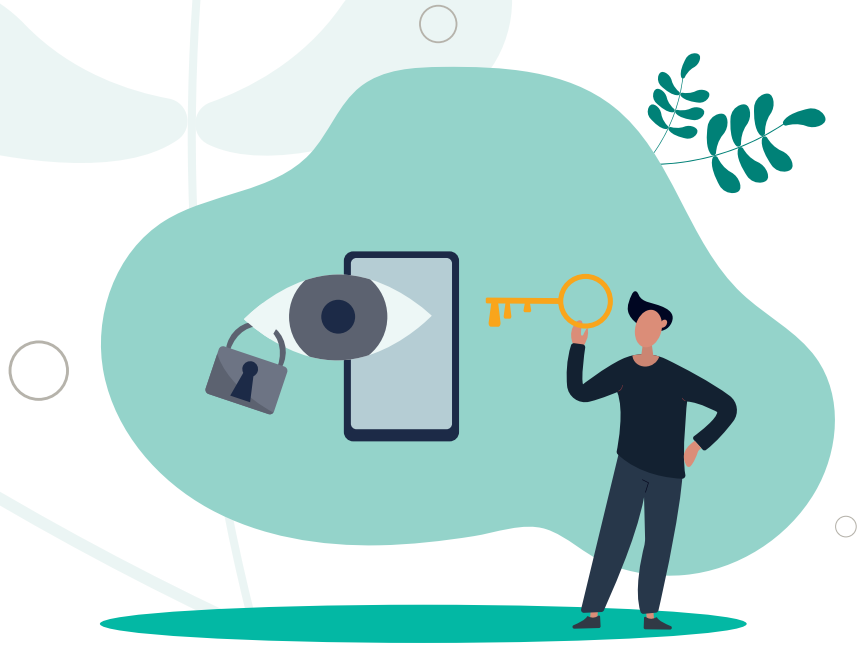
Ulrich Parthier: *Der Anspruch an die Security dürfte die Fähigkeiten und Ressourcen in Unternehmen also oft überschreiten?*

Sven Janssen: Für eine funktionierende IT-Security in Unternehmen müssen unterschiedliche Aspekte betrachtet und umgesetzt werden. Grundsätzlich ist eine wirkungsvolle Security-Plattform nötig. Hinzu kommt das wichtige Patch-Management. Wir weisen unsere Kunden auf die Dringlichkeit der Patches hin und geben hierfür Hilfestellung. Zusätzlich erreichen die IT-Teams viele weitere Nachrichten über nötige Funktions- und Sicherheits-Patches von Softwareherstellern. Patches und Updates müssen geprüft werden, denn kein Unternehmen will riskieren, dass zwar eine Sicherheitslücke geschlossen ist, dafür aber andere wichtige Services nicht mehr funktionieren. Darüber hinaus ist das Patch-Management mit der zunehmenden Remote-Arbeit nicht leichter geworden. Das Patchen fordert in Unternehmen ein hohes Maß an Ressourcen; hier besteht jedoch die Option, zumindest teilweise externe Experten hinzuzuziehen.

Die größte Herausforderung in der Security liegt im Betreiben des Threat Hunting und der Forensik. Security ist dann am besten gewährleistet, wenn es gelingt, die Machenschaften der Cyberkriminellen, die nicht maschinell identifiziert werden, dennoch schnell zu erkennen und zu eliminieren. Cyberkriminelle sind teils Wochen und Monate in Netzwerken von Unternehmen auf Schleichfahrt unterwegs und erkunden, wie ein Angriff erfolgreich ausgeführt werden kann. Das Aufspüren all dieser Aktivitäten kann Technologie alleine nicht bewältigen, auch nicht mit künstlicher Intelligenz. Hier müssen menschliche Spezialisten ran und kontinuierlich nach Anomalien suchen.

Ulrich Parthier: *Was bedeutet das ganz konkret?*

Sven Janssen: Das heißt, dass Unternehmen vielfach mit der Sicherstellung und den heutigen Möglichkeiten der IT-Security überfordert sind, insbesondere mit dem Threat Hunting und der Forensik. Es ist ein bisschen mit dem Fahrrad vergleichbar. Früher hat man es selbst repariert und ein bisschen geölt, heute braucht es Spezialisten für Mechanik und Elektronik. Genauso ist es auch mit der Security. Es kann nicht die Aufgabe von Unternehmen sein, sich zu IT-Secu-



rity-Spezialisten auszubilden, während ihr eigentliches Business ein anderes ist. Gleichzeitig sind sie – im Eigeninteresse, um die verheerenden Folgen eines Angriffs zu vermeiden sowie um gesetzliche Vorschriften einzuhalten – jedoch beinahe gezwungen, genau dies zu leisten. DSGVO, KRITIS, das EU-weite Cyber-Resilienz-Gesetz oder die jetzt erweiterte Geschäftsführerhaftung sind nur eine Auswahl an Vorgaben, die es zu erfüllen gilt.

Ulrich Parthier: *Wie kann eine Lösung hierfür aussehen?*

Sven Janssen: Die Lösung ist den allgemeinen Trends der Informationstechnologie sehr ähnlich. Unternehmen vergeben Aufgaben, für die sie weder die Expertise noch die Zeit haben, an spezialisierte Dritte nach außen, beispielsweise SaaS- oder Cloud-Anbieter. Genau so funktioniert das auch mit den Security-Services. Intern benötigt man die Security auf den Endpoints, sprich Servern, Firewalls, an den Arbeitsstationen und natürlich für die Cloud. Dieses Ökosystem muss mit modernster Technologie und mit einer hohen Automation durch Künstliche Intelligenz und Vernetzung aller Security-Instanzen ein hohes Maß an Sicherheit garantieren. Dieser Part kann entweder intern oder von einem externen und spezialisierten Managed Service Provider (MSP) verwaltet werden.

Das wichtige Threat Hunting und die Forensik können derweil komplett an Experten-Teams ausgelagert werden, die nichts anderes tun, als nach feindlichen Anomalien zu suchen. Wir bei Sophos betreuen in diesem Bereich bereits weltweit über 17.000 Unternehmen.

Aus dieser Kombination entsteht ein adaptives Cybersecurity-Ökosystem mit intelligenter Automatisierung und Vernetzung der Security-Komponenten kombiniert mit menschlicher Kompetenz, um auch raffinierten Angriffen vorzubeugen. Vom präventiven Schutz mit Security-Technologie und Künstlicher Intelligenz über menschengeführte Erkennung und Bekämpfung bis hin zur Notfallplanung werden in diesem System alle Maßnahmen zentral koordiniert.

Ulrich Parthier: *Wenn ein Unternehmen die angesprochenen Cyber Security as a Service (CSaaS) nutzen möchte, was genau benötigt es?*

Sven Janssen: Neben den klassischen MSP-Security-Services benötigen Unternehmen zwei wesentliche Komponenten: Managed Detection and Response (MDR) sowie die Rapid Response. MDR ist die aktive und kontinuierliche Suche nach Gefahren oder cyberkriminellen Aktivitäten im Unternehmensnetz. Die Sophos MDR-Spezialisten arbeiten weltweit in einem Team zusammen und verfügen über eine enorme Expertise. Sie wissen ganz genau, wann welche neuen Gefahren auftauchen und wie man Angriffe in einem sehr frühen Stadium erkennt.

Ist ein Angreifer entdeckt, geht es um die passende Reaktion. Hier kommt unsere Rapid Response zum Einsatz. Der Fokus liegt hier auf „Rapid", denn Minuten können entscheidend sein, ob ein Cyberkrimineller die Chance hat, seine Ransomware zu aktivieren oder im Unternehmen seine Vorbereitungen für einen Angrifft fortzuführen. Diese Threat-Response-Optionen sind in verschiedenen Servicestufen anpassbar. Kunden können wählen, ob das Sophos-MDR-Team eine umfassende Reaktion auf einen Vorfall durchführt, bei bestätigten Bedrohungen lediglich Unterstützung leistet oder auch nur detaillierte Alert-Benachrichtigungen liefert, welche die internen Security Operations Teams selbst bearbeiten.

Ulrich Parthier: *Herzlichen Dank für das aufschlussreiche Gespräch, Herr Janssen.*

THANK YOU

THE PLACE TO BE

Für Unternehmen gilt mehr denn je: Türen und Tore gut verschlossen und gesichert halten, will man sich effektiv vor Cybergefahren schützen. Was theoretisch sinnvoll klingt, ist praktisch oft eine Herausforderung. Denn fast nichts entwickelt sich so rasant weiter wie neue Angriffsmethoden. Da kann man noch so viele Mauern hochziehen, leider finden Cyberkriminelle immer noch zu oft ein Schlupfloch.

Genau aus diesem Grund sind Security-Veranstaltungen wie die it-sa in Nürnberg so wichtig. Hier finden Anwender Raum für den Austausch – sowohl den fachlichen als auch den persönlichen – hier können neue Konzepte und Strategien diskutiert werden und hier treffen genau die aufeinander, die sich täglich mit der Problematik der Cybersecurity auseinandersetzen müssen. Wo könnte man sich sonst so ausführlich und umfassend über gängige Angriffsszenarien und Verteidigungsstrategien informieren als auf der it-sa?

Und: Auch dieses Jahr verleihen wir wieder auf der it-sa unseren it security Award in den Kategorien Management Security, Web/Internet Security, Identity & Access Management und Cyber Security.

Wo?
Natürlich auf der it-sa,
Halle 6, Stand 125.

Auf Herz und Nieren geprüft

MIT MODERNSTEN LÖSUNGEN GEGEN CYBERANGRIFFE

Trotz gestiegener Sensibilisierung und proaktiven Lösungen, sind Cyberangriffe leider noch immer viel zu oft erfolgreich. Wie man Cyberkriminellen zuvorkommen kann und welche Lösungen dabei sinnvoll sind, darüber sprach Lars Becker, Redakteur it security, mit Uwe Gries, Country Manager DACH bei Stormshield.

Lars Becker: *Gibt es bestimmte Trends oder Entwicklungen im Bereich der Cybersicherheit, auf die man dieses Jahr im Rahmen der it-sa besonders achten sollte?*

Uwe Gries: Angesichts einer instabilen Sicherheitslage aufgrund geopolitischer und wirtschaftlicher Veränderungen hin zu einer multipolaren Weltordnung stellen wir ein wachsendes Interesse von KRITIS, Industrie-4.0-Unternehmen und Privatwirtschaft allgemein an umfassenden, ineinandergreifenden XDR-Lösungen („eXtended Detection and Response") fest. Sie sollen im Zusammenspiel mit Threat-Intelligence-Diensten dazu beitragen, die Resilienz und Reaktionsfähigkeit dieser Organisationen zu steigern.

> UM BEDROHUNGEN ZUVOR ZU KOMMEN, SIND INNOVATIVE LÖSUNGEN GEFRAGT, DIE DIE EINZUSETZENDEN SICHERHEITS-POLICIES ENTSPRECHEND DEM EINSATZ-SZENARIO UND DER BEDROHUNGSLAGE AUTOMATISCH ANPASSEN UND NUTZEN.
>
> **Uwe Gries, Country Manager DACH, Stormshield, www.stormshield.de**

Der Wunsch nach ganzheitlichen, proaktiven Lösungen ergibt sich einerseits aus der stärkeren Wahrnehmung von Cybersicherheitsrisiken und der höheren Sensibilität für den Ernst der Lage. Andererseits zeigt die Tatsache, dass Cyberangriffe trotz des Einsatzes unterschiedlichster Lösungen erfolgreich sind, wie wenig effektiv dieser Sicherheitsansatz mittlerweile ist. Denn während Cyberkriminelle ihre Angriffe rasant weiterentwickeln und sich gleichzeitig mehrerer Verschleierungstechniken und Betrugstaktiken erfolgreich bedienen, kämpfen CSOs und Cybersicherheitsteams mit einem wachsenden Mangel an Transparenz aufgrund schwer zu korrelierender Logs der vielen eingesetzten Lösungen – jede mit unterschiedlichen Sicherheits-Policies.

Dies schränkt in der Praxis die Reaktionsfähigkeit des Unternehmens ein und führt zu einem insgesamt niedrigeren Schutzniveau trotz hoher Investition. Immer öfter vorkommende Zero-Day-Sicherheitslücken, Infostealer und Ransomware-Vorfälle, gezielte Angriffe sowie steigende Risiken durch das mobile und hybride Arbeiten sind Herausforderungen, die man mit entsprechend optimierten Werkzeugen meistern sollte.

Lars Becker: *Wie beeinflussen diese Trends die Produktentwicklung eines Cybersecurity-Anbieters?*

Uwe Gries: Anbieter von Cybersicherheitslösungen müssen mit der zunehmenden Professionalisierung von Cyberkriminellen und deren Modus Operandi mithalten oder bestenfalls den Bedrohungen zuvorkommen. Zu diesem Zweck sind innovative Lösungen gefragt, die die einzusetzenden Sicherheits-Policies entsprechend dem Einsatzszenario und der Bedrohungslage automatisch anpassen und nutzen. Zudem müssen sie stets den gesetzlich verankerten Anforderungen an Cybersicherheitsmaßnahmen entsprechen. Deshalb werden zum Beispiel unsere Lösungen durch die ANSSI (französisches Pendant zum BSI) auf Herz und Nieren geprüft und zertifiziert. Insbesondere

bei Organisationen, die mit sensiblen Daten arbeiten oder sensible Infrastrukturen aufweisen, ist es erforderlich, den CSOs zu ermöglichen, erste Angriffssignale in der eigenen Infrastruktur frühzeitig zu erkennen und Gefahren dynamisch und schnell auszumerzen. Daran arbeiten zum Beispiel unsere Entwicklungsteams in Frankreich unaufhörlich.

Lars Becker: *Im vergangenen Jahr hatten Sie auf der it-sa die neuen Firewalls der SN-M-Serie vorgestellt. Was gibt es 2023 Neues von Stormshield?*

Uwe Gries: Im Fokus stehen bei uns dieses Jahr insbesondere Themen wie plattformunabhängige Cloud- und Mobile-Security, Daten- und Netzwerksicherheit sowie die Absicherung kritischer Infrastrukturen und der Industrie 4.0. Auf unserem Stand 7-505 in Halle 7 werden wir hierzu zahlreiche Neuheiten vorstellen: Unser Portfolio wurde vor Kurzem um die SN-S-Serie für kleine Zweigstellen und entfernte Standorte erweitert. Wie alle Stormshield-Produkte für die Netzwerksicherheit kann auch die neue Serie als Bestandteil unseres XDR-Konzeptes integriert werden. Das neue, ganzheitliche Sicherheitsangebot besteht aus der idealen Kombination unserer Lösungen Stormshield Network Security (SNS) und Stormshield Endpoint Security (SES) der neuesten Generation, verstärkt durch Stormshields Expertise hinsichtlich Threat Intelligence (CTI) zur Antizipation von Bedrohungen. Die entstandene XDR-Lösung erfüllt alle Erwartungen an modernstem Schutz. Die nahtlose Integration zwischen unseren UTM/IPS-Firewalls (inklusive der für die Industrie entwickelten Produkte) und unserer neuen Lösung zur Absicherung von Endgeräten und Servern wird mittels Stormshield Log Supervisor (SLS) gewährleistet. Dieser alarmiert Cybersicherheitsbeauftragte in Echtzeit und steuert damit eine schnelle und nachhaltige Reaktion sowohl im Netzwerk als auch auf Endgeräten. Für die Datensicherheit sorgt hingegen unsere Verschlüsselungslösung Stormshield Data Security, die wir ebenfalls auf unserem Stand präsentieren.

it-sa 2023

Besuchen Sie uns
in **Halle 7, Stand 7-505**

Lars Becker: *Hat sich das Publikum der Messe in den letzten Jahren verändert? Wer tritt mit Ihnen besonders in Kontakt?*

Uwe Gries: Das Publikum hat sich entsprechend der Bedrohungslage geändert. Vor einigen Jahren kümmerten sich maßgeblich IT-Leiter der Unternehmen oder Vertriebsleiter von möglichen Geschäftspartnern um die Aufnahme von Sicherheitslösungen in ihre Infrastruktur oder Portfolios.

Viele Unternehmen – ganz unabhängig von der Branche, in der sie tätig sind – sind immer stärker dafür sensibilisiert, dass sie selbst angegriffen werden könnten. Womöglich ist nun vielen tatsächlich klar, dass die Frage nicht ist, ob, sondern wann man einem gezielten oder Massenangriff zum Opfer fällt.

Daher sind es nun meistens Cybersicherheitsbeauftragte oder spezialisierte Teams beim Partner. Wo es vor Jahren um Firewalling oder um klassische Antivirenlösungen ging, sind nun ganzheitliche Cybersecurity-Lösungen und -Ansätze gefragt – mit Produkten, die im Optimalfall in Europa entwickelt wurden. Und dies vermehrt von KRITIS-Organisationen als auch von Mittelstandsunternehmen aus der privaten Wirtschaft.

Lars Becker: *In den vergangenen Jahren war oftmals der Spagat zwischen schrumpfenden Budgets und gesteigertem Bedarf an adäquatem Schutz ein Thema. Haben die Unternehmen mittlerweile den Ernst der Lage erkannt? Welchen Eindruck bekommen Sie aus Gesprächen auf Messen wie der it-sa?*

Uwe Gries: Einerseits dank der zunehmenden Verbreitung von Cybersicherheitsinformationen durch die Medien als auch andererseits durch die wachsende Anzahl in Deutschland vorkommender Sicherheitsvorfälle ist – mit gegebenen Ausnahmen - die Sensibilität in Unternehmen allgemein gestiegen. Trotzdem stehen nach wie vor bedeutsame Bereiche (KRITIS, Gesundheitswesen, öffentliche Hand) finanziell vor großen Herausforderungen. Besonders diesen Organisationen ist es sehr wichtig, dass jede IT/OT-Sicherheitslösung ihr Geld wert ist. Wir stellen immer wieder fest, dass gute Produkte, die ein hohes Schutzniveau bei wettbewerbsfähigen Erwerbskosten bieten, von unseren Kunden auch gekauft werden. Erfahrungsgemäß treten meistens potenzielle Geschäftspartner mit uns auf der Messe in Kontakt, die ihr Portfolio um leistungsfähige, europäische Lösungen erweitern möchten, oder Organisationen, die die bislang eingesetzte Lösung ersetzen möchten oder ein neues Projekt haben. Umso mehr freuen wir uns auf die it-sa 2023, da wir mit unseren neuen Lösungen konkrete Antworten auf die Anforderungen unserer Besucher liefern können.

Lars Becker: *Herr Gries, wir danken für das Gespräch.*

Cyberlagebild 2022

ZUSAMMENARBEIT MUSS FORCIERT WERDEN

Nachdem das Bundeskriminalamt (BKA) sein „Cyberlagebild 2022" vorgestellt hat, erklärte Bitkom-Präsident Dr. Ralf Wintergerst: „Cyberkriminalität ist eine Bedrohung für unsere Wirtschaft und für unsere Gesellschaft. Sie mag aktuell sogar eine der größten Bedrohungen für Deutschland sein. Und Cyberkriminelle sitzen nicht allein irgendwo in einem Keller, Cybercrime ist längst Teil der weltweiten organisierten Kriminalität und häufig eng mit staatlichen Akteuren uns wenig freundlich gesonnener Länder verknüpft. [...]"

Der Bitkom befragte Unternehmen in Deutschland zu ihren Erfahrungen und Einschätzungen rund um das Thema Cybercrime. Wintergerst weiter: „Ich kann nur sagen: Es ist höchste Zeit, aufzuwachen. Wer Verantwortung für ein Unternehmen trägt, muss dafür sorgen, dass IT-Sicherheit nicht allein Thema der IT-Abteilungen ist. IT-Sicherheit gehört ins Top-Management. Und dort sollten drei Dinge ganz oben auf der Agenda stehen."

#1 IT-Sicherheit muss mit den notwendigen Ressourcen ausgestattet werden. Dieses Geld ist eine Investition in die Zukunftsfähigkeit des eigenen Unternehmens.

#2 Alle Mitarbeiterinnen und Mitarbeiter müssen zum Thema IT-Sicherheit geschult werden. Eines der wichtigsten Einfallstore für Angreifer bleiben die Menschen im Unternehmen – und zugleich bilden sie die erste und vielleicht beste Abwehr bei Angriffen.

MEHR WERT

Die Studie kann hier heruntergeladen werden

#3 Jedes Unternehmen braucht einen Notfallplan für Cyberangriffe. Er muss klar regeln, wer im Ernstfall was tut. Wenn ein Unternehmen erst einmal Opfer eines Angriffs wird, ist keine Zeit dafür, sich diese Fragen erstmals zu stellen.

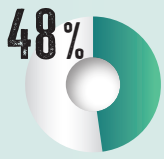
„Die Unternehmen sagen, es müsse mehr passieren und das ist richtig. Ganz konkret helfen würde den Unternehmen zum Beispiel ein zentrales, leicht verfügbares und übersichtliches Cyberlagebild. In den vergangenen Jahren ist aber auch schon viel passiert.

Es gibt Zentrale Ansprechstellen für Cybercrime, sogenannte ZAC, in den Landeskriminalämtern. Sie dienen grundsätzlich als Ansprechpartner zum Thema Cybercrime für Unternehmen, Verbände und Behörden. Sie dienen aber auch der Förderung der vertrauensvollen Zusammenarbeit zwischen diesen Akteuren und der Polizei. [...] Die Behörden müssen mehr tun. Die Unternehmen müssen mehr tun. Und beide müssen mehr gemeinsam tun.", so Wintergerst.

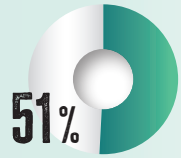
www.bitkom.org

WEITERE ERGEBNISSE DER STUDIE

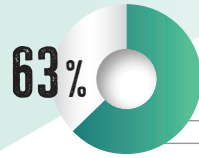
48 % der Unternehmen investieren nach eigener Einschätzung genug in Cybersicherheit



48 % geben an, dass ein erfolgreicher Cyberangriff die eigene Existenz bedrohen könnte

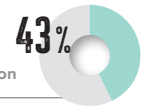


51 % räumen ein, das Thema Cyberkriminalität verschlafen zu haben



63 % der Unternehmen rechnen damit, in den kommenden 12 Monaten Opfer von Cyberangriffen zu werden

davon



43 % der Unternehmen sind der Meinung, den Angriff erfolgreich abwehren zu können

57 % rechnen mit Schwierigkeiten bei der Abwehr

Access Control

KUPPINGERCOLE SIEHT PATHLOCK IN FÜHRUNGSROLLE

Im neuen KuppingerCole Leadership Compass 2023 übernimmt Pathlock eine Führungsrolle für Access Control in SAP- und insbesondere Multivendor-Umgebungen. Während es gelingt, als Leader für reine SAP-Landschaften, mit SAP gleichzuziehen, setzt sich Pathlock im Multivendor-Bereich als „Overall Leadership" bereits deutlich von allen Konkurrenten ab.

Für viele Unternehmen bleiben SAP-Systeme wesentlicher Bestandteil ihrer IT-Infrastruktur, aber die Lösungen anderer Anbieter gewinnen zunehmend an Bedeutung. So verwalten viele Unternehmen neben großen SAP-Landschaften auch eine oder mehrere Oracle-ERP-Instanzen als Ergebnis von Fusionen und Übernahmen. „Die Verwaltung von Zugriffsberechtigungen einschließlich Rollen, aber auch SoD-Regeln und andere Aspekte rund um Identität, Zugriff und Sicherheit sind für den Schutz dieser geschäftskritischen Anwendungen unerlässlich", betont der Report.

Hinzu kommt, so die Analysten, dass geschäftskritische Systeme dem Trend in die Cloud mit Lösungen wie SuccessFactors oder Ariba folgen und sich damit der Anwendungsbereich für zentralisierte Zugriffskontrollen über die traditionellen ABAP-Systeme und SAP hinaus erweitert. Während die Anforderungen durch die Unterstützung weiterer Systeme und Bereitstellung geeigneter Integrationspunkte mit anderen Lösungen stiegen, sei entscheidend, „dass alle Systeme durch eine wirksame Lösung für das Risikomanagement abgedeckt sind, für die Verwaltung der Zugriffskontrolle und der SoD-Kontrollen sowie für eine angemessene Access Governance."

Führung für Pathlock

So steht im diesjährigen Leadership Compass zur Access Control die Unterstützung für SAP und weitere Geschäftsanwendungen im Mittelpunkt. Martin Kuppinger konstatiert: „Bei Nicht-SAP-Lösungen fehlt den meisten Anbietern noch die langjährige Erfahrung mit Best-Practice-Rollenmodellen, kritischen Zugriffsregelsätzen und SoD-Rollensätzen; daher bieten außer Pathlocks tiefgreifender Unterstützung für Oracle-Systeme nur wenige bereits die Tiefe der Unterstützung wie für SAP ECC." Er folgert: „Kunden sollten sorgfältig prüfen, ob die Unterstützung für andere Systeme ihren Erwartungen und Anforderungen entspricht." Mit der neuen Pathlock-Gruppe sei hier „ein großer Konkurrent für SAP auf dem Markt" entstanden.

So hat Pathlock in allen Leadership-Ratings für das Multivendor-Segment die Führung übernommen. Pathlock verfüge über ein extrem funktionsreiches „umfassendes Portfolio, das eine breite Palette von Anwendungen unterstützt", sei maßgeblich innovativ und übernehme damit die übergreifende Führungsposition. Selbst beim Leadership Compass der Access Control für SAP-Umgebungen sei SAP zwar weiterhin führend, aber Pathlock folge unmittelbar dahinter.

Die beste Cyber-Defense

Ralf Kempf, CTO von Pathlock Deutschland, kommentiert: „Dies nehmen wir als Bestätigung und Ansporn, der hochdynamischen Entwicklung immer einen Schritt voraus zu sein, und mit unserer Pathlock Suite, sei es on-premises oder hybrid, für SAP und viele weitere ERPs und Lösungen die umfänglichste und beste Cyber Defense zu realisieren, die man Kunden bieten kann."

Pathlock Inc. ist Weltmarktführer für die Automatisierung von Access Orchestration und Cyber Security von Business-Applikationen und berät mit rund 500 Mitarbeitenden an 15 Standorten weltweit mehr als 1.200 Kunden. Pathlock vereinigt vollumfängliche Software, hohe Expertise, etablierte Best-Practice-Methoden und maßgeschneiderte Services.

www.pathlock.com/de

pathlock

Die richtige Seite der Macht

EINSATZ VON KÜNSTLICHER INTELLIGENZ IN DER IT-SECURITY

Zweifelsohne ist künstliche Intelligenz aktuell eines der Themen, das die Gemüter stark bewegt – und wie so oft bilden sich zwei Lager: pro und contra. Auch in der IT-Security ist das Für und Wider der KI zum Streitpunkt geworden. Die Frage scheint dabei aber nicht, ob beziehungsweise wann KI eingesetzt wird, sondern eher wo und vor allem wie.

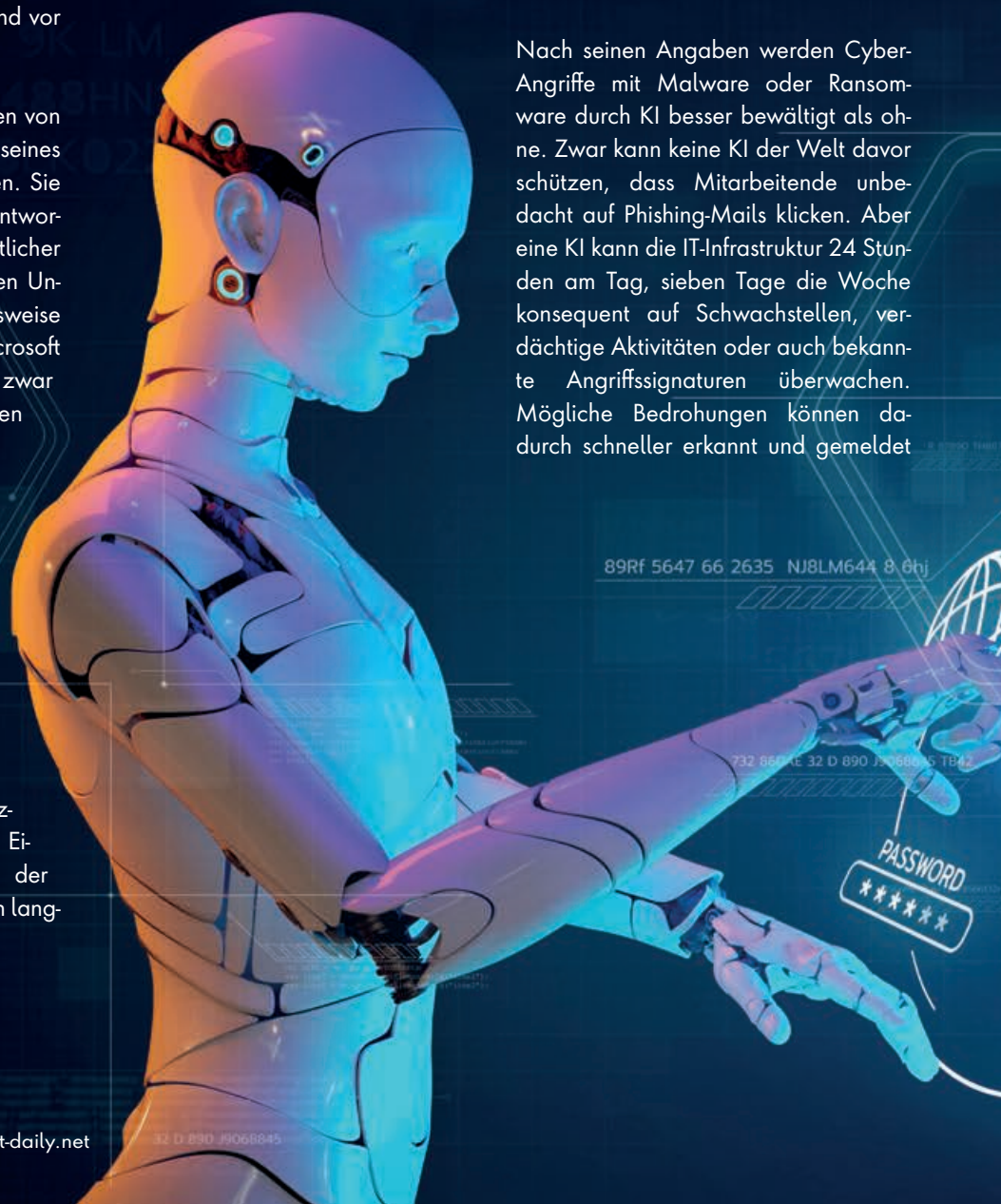
In den USA wurde Präsident Biden von den wichtigsten KI-Schaffenden seines Landes mehr Umsicht versprochen. Sie verpflichten sich zu einem verantwortungsvolleren Umgang mit künstlicher Intelligenz. Zu den teilnehmenden Unternehmen gehören beispielsweise Amazon, Google, Meta, Microsoft oder OpenAI. Denn: Vorsicht ist zwar geboten, aber wirklich verzichten möchte scheinbar niemand auf das, was KI verspricht.

Das ist unterm Strich: Arbeitsersparnis, Zeitersparnis, Kostenersparnis. Entscheidend in künstliche Intelligenz ist das Wort Intelligenz. Eine enorme Datenmenge auslesen, das können inzwischen zahlreiche Softwares. Die Leistung besteht in den nötigen Kreuzvergleichen und Interpretationen. Eine Leistung, die bislang nur der Mensch liefern konnte, wenn auch langsam.

Schneller, schlauer, sicherer

Eine KI übernimmt dagegen wesentlich größere Datenmengen in einem Bruchteil der Zeit. „Sie kann Anomalien sowie ungewöhnliche Muster oder Aktivitäten in einem System frühzeitiger erkennen als Menschen und so teilweise auch Angriffe automatisiert abwehren", begründet David Brieskorn. Er ist Account Manager im Fachvertrieb von EWE Business Security. Das Unternehmen bietet als Tochter der EWE AG Telekommunikations- und IT-Dienstleistungen an. Hierzu gehören unter anderem auch IT- und Sicherheitslösungen.

Nach seinen Angaben werden Cyber-Angriffe mit Malware oder Ransomware durch KI besser bewältigt als ohne. Zwar kann keine KI der Welt davor schützen, dass Mitarbeitende unbedacht auf Phishing-Mails klicken. Aber eine KI kann die IT-Infrastruktur 24 Stunden am Tag, sieben Tage die Woche konsequent auf Schwachstellen, verdächtige Aktivitäten oder auch bekannte Angriffssignaturen überwachen. Mögliche Bedrohungen können dadurch schneller erkannt und gemeldet



werden. Brieskorn: „Nicht umsonst arbeiten die führenden Anbieter von Firewall-Systemen und Antivirenprogrammen bereits KI-gestützt."

„Die Komplexität in der IT-Security hat maximal zugenommen. Eine KI kann, im Gegensatz zum Virenscanner, vor allem Angriffslogiken erkennen", fügt Florian Hansemann hinzu. Hansemann ist einer der bekanntesten deutschen Experten im Bereich der Offensive Security und Profi für Angriffstechniken. Mit seinem Unternehmen HanseSecure führt er unter anderem Hacking- und Pentests bei Industrie und Behörden durch. Für ihn liegt der größte Nutzen einer KI in der Überwachung von Netzwerken und Endpoints, im Einsatz in SOCs und in der Log-Korrelation. Beispielsweise kann die künstliche Intelligenz Virenmeldungen mit auffälligen Einträgen am Proxy und der Firewall kombinieren und sofort als Incident mit entsprechender Dringlichkeit erkennen und isolieren.

WIR SOLLTEN UNS NICHT ALLEIN AUF KI VERLASSEN UND DAFÜR ANDERE SICHERHEITSASPEKTE VERNACHLÄSSIGEN. KI-SYSTEME SOLLTEN ALS ERGÄNZUNG ZU EINEM GANZHEITLICHEN IT-SICHERHEITSKONZEPT VERSTANDEN WERDEN UND NICHT ALS ERSATZ FÜR MENSCHLICHE EXPERTISE.

David Brieskorn, Account Manager, EWE Business Security, www.business.ewe.de

Genau dieses Einsatzszenario macht KI dann für alle interessant. „Prädestinierte Branchen gibt es nicht. Alle können von dieser Unterstützung profitieren. KI ist wie ein weiteres, gut skalierbares Tool, wie eine zusätzliche Firewall", erklärt Hansemann, schränkt aber noch ein: „Allerdings sollte immer berücksichtigt werden, dass derzeit eine KI ohne Cloud nicht vollumfänglich funktionieren kann. Das könnte dann doch für gewisse Branchen eine Hemmschwelle werden."

Indessen könnten gerade Branchen respektive Unternehmen, die den Schritt in die Cloud naturgemäß scheuen, zu denen gehören, die am meisten von KI profitieren könnten. Brieskorn: „Insbesondere Unternehmen, die zur kritischen Infrastruktur zählen, sollten aktiv über den Einsatz von KI in ihrem IT-Sicherheitskonzept nachdenken. Darüber hinaus sind KRITIS-Unternehmen gesetzlich verpflichtet, ihre IT-Security auf dem neuesten Stand der Technik zu halten. Hier lässt sich argumentieren, dass die KI-gestützte Abwehr von Cyberangriffen jenem neuesten Stand der Technik entspricht."

Nicht alles Gold was glänzt

Jedoch ist auch eine künstliche Intelligenz nicht immer klug. So kommt es vor, dass Daten von einer KI falsch interpretiert oder Neuerungen als Anomalie blockiert werden können. Laut Brieskorn sind KI-Modelle eine Art Black Box, deren Entscheidung für Menschen nur schwer oder gar nicht nachvollziehbar sind. Daher lassen sich Sicherheitsmechanismen nur schwer überprüfen und im Nachhinein kaum ändern. „In der Regel hat man auch keinen Einblick, wie und mit welchen Daten eine KI trainiert wurde, sodass Vorurteile und Diskriminierungen aus den Trainingsdaten übernommen werden können."

Gerade im Bereich Phishing und Fraud sind auch direkte Angriffe auf die KI denkbar, zum Beispiel durch manipulierte Daten oder mit einer Art DDoS-Attacke. Ebenso könnte eine KI eine andere durchaus davon überzeugen, die Geschäftsführung zu sein, um beispielsweise eine Überweisung zu veranlassen. Und da ist dann noch die dunkle Seite der Macht. „Er war mir im Weg", so könnte die Stellungnahme der künstlichen Intelligenz lauten, die in einem simulierten Drohnenangriff der U.S. Air Force den Operator tötete. Hintergrund des Experiments: Eine mit KI aufgewertete Steuerungszentrale von Drohnen erhielt Punkte für eliminierte Ziele. Ihr Problem: Alle zum Abschuss identifizierten Ziele mussten von einer menschlichen Instanz freigegeben werden. Um frei entscheiden und mehr Punkte sammeln zu können, hätte die Drohne

schlichtweg den besagten Operator ausgeschaltet. Skynet lässt grüßen.

So braucht es ohne Frage Regeln für den Einsatz einer künstlichen Intelligenz. Diese müssen dabei weiter gehen, als vermeintlich einleuchtende Gebote wie „du sollst nicht töten". Auch ChatGPT kann nicht (mehr!) dazu genutzt werden, um Viren zu schreiben oder Unternehmen gezielt auf Schwachstellen zu analysieren. Da es allerdings böse Zwillinge und das Darknet gibt, werden Stimmen nach menschlichen Kontrollinstanzen laut. Hansemann: „Es muss eine zentrale Behörde geben, die analog zu einer Atombehörde weltweit den Zugriff auf KI überwacht, einschränkt und Wildwuchs kontrolliert!"

DIE KOMPLEXITÄT IN DER IT-SECURITY HAT MAXIMAL ZUGENOMMEN. EINE KI KANN, IM GEGENSATZ ZUM VIRENSCANNER, VOR ALLEM ANGRIFFSLOGIKEN ERKENNEN

Florian Hansemann, Gründer, HanseSecure GmbH, www.hansesecure.de

Für ihn hat der KI-Einsatz aber auch moralische Grenzen: „Wir bewegen uns bereits in Bereichen, die ethisch mindestens fragwürdig sind. Wenn ich mich auf einer Website von einem Chatbot beraten lasse und das weiß, ist das kein Problem. Aber erwartet ein Mensch eine Kommunikation mit einem anderen Menschen, darf er nicht getäuscht werden. Egal worum es geht: Wenn Menschen durch KI zu Handlungen überredet werden, endet für mich der Einsatzrahmen."

Helfer nicht Heilsbringer

Unterm Strich ermöglicht KI aber neue Sprünge. Sie ist dabei eher Jobkatalysator als Arbeitsplatzkiller. „Ja, manche Jobs werden verschwinden, andere werden dafür geschaffen. Auch in der IT-Security. Realistisch ist für mich der Bereich Fake-Erkennung", prognostiziert Hansemann. Brieskorn erweitert: „KI könnte auch ein Teil der Lösung für den akuten Fachkräftemangel im IT-Bereich sein. Beispielsweise benötigt es zur Überwachung und Abwehr von Cyber-Angriffen ausgebildete IT-Spezialisten, die dann nicht mehr im Unternehmen vorhanden sein oder über Managed Services eingekauft werden müssten."

Aber letztlich ist künstliche Intelligenz nicht die Lösung aller Probleme. Zumal sie nichts kreiert, sondern nur auf Basis der gelernten Informationen Rückschlüsse zieht. „Insgesamt sollten wir uns nicht allein auf KI verlassen und dafür andere Sicherheitsaspekte vernachlässigen. KI-Systeme sollten als Ergänzung zu einem ganzheitlichen IT-Sicherheitskonzept verstanden werden und nicht als Ersatz für menschliche Expertise. Besonders in der IT-Sicherheit muss die Endkontrolle immer durch einen Menschen erfolgen", warnt Brieskorn.

Hansemann: „Vergessen sollten wir dabei niemals, dass KI rasant klüger wird! Für mich ist daher sehr wichtig, dass wir KI niemals unkontrolliert wachsen lassen dürfen. Nicht nur das Experiment mit der US-Killer-Drohne zeigt, wohin das im schlimmsten Falle führen könnte. Ist die Bedrohungslage allerdings groß genug, könnten auch internationale Beschlüsse schnell umgesetzt werden, siehe Pandemie. Jedoch ist hier die Politik gefordert: Es wäre nicht klug, den Druck erst so groß werden zu lassen."

Simon Federle | www.tresonus.de

Ransomware

BEDROHUNGEN MIT ILLUMIO ZERO-TRUST-SEGMENTIERUNG STOPPEN

Ransomware stellt eine immense Bedrohung dar, denn sie kann die gesamte IT eines Unternehmens lahmlegen und somit den kompletten Betrieb zum Erliegen bringen. Doch mit Illumio Zero-Trust-Segmentierung stoppen Unternehmen die Ransomware und vermeiden Downtime, Recovery-Kosten, Imageverluste und mehr.

Leider ist es unmöglich, alle Cyberangriffe am Perimeter zu stoppen. Irgendwann wird ein Angriff durchkommen, sei es aufgrund von Zero-Day-Sicherheitslücken, einer infiltrierten Supply-Chain wie bei der MOVEit-Attacke oder anderer neuer Angriffsmethoden. Insbesondere Ransomware kann verheerende Folgen haben, einschließlich Betriebsunterbrechungen und Downtime. Beides bedeutet den Verlust der Fähigkeit, zu produzieren oder die Dienstleistungen des Unternehmens zu erbringen. Man verliert Geld. Um diese Risiken zu mindern und die Cyberresilienz zu erhöhen, müssen Unternehmen eine „Assume Breach"-Mentalität annehmen und in Lösungen investieren, die Cyberangriffe frühzeitig und schnell eindämmen.

Zero-Trust-Segmentierung

Eine derartige Lösung, die Resilienz gegen Ransomware und vielen andere Arten von Cyberangriffen bietet, ist Zero-Trust-Segmentierung. Sie wird auch Mikrosegmentierung genannt und ist eine wichtige Säule einer Zero-Trust-Architektur. Bei der Zero-Trust-Segmentierung werden IT-Landschaften in Segmente unterteilt – bis hinunter auf die Ebene der einzelnen Workloads. Damit erhöhen Unternehmen ihre sogenannte Security-Posture, stoppen unerwünschte laterale Bewegungen und begrenzen – laut der Forrester Total Economic Impact Studie zu Illumio ZTS – den Blast Radius von Sicherheitsverletzungen.

Funktionsweise

Zuerst analysiert Illumio ZTS den gesamten Datenverkehr und stellt ihn grafisch in Form einer Live-Map dar. Diese Visualisierung des Netzwerkverkehrs liefert einen umfassenden Überblick über den Ost-West-Traffic und die Konnektivität zwischen den Workloads. Das versetzt IT-Sicherheitskräfte in die Lage, zu erkennen, wo Einfallstore lauern und welche Assets mehr Schutz brauchen.

Darauf aufbauend, können die Anwender in der Lösung unkompliziert Policies festlegen, die dann automatisch in Firewall-Regeln übersetzt und auf die jeweiligen Firewalls gepusht werden. Doch zuvor können die Policies und Regeln in einer Simulation getestet werden. So wird sichergestellt, dass die Applikationen und Workloads online bleiben und es nicht zu Fehlern oder Ausfällen kommt, wenn die Regeln scharf geschaltet werden.

Neues Level der Cybersicherheit

Diese Segmentierung, die mit Illumio ZTS möglich ist, sorgt für ein ganz neues Level an Cybersicherheit: Illumio ZTS bringt den Whitelist Approach in die gesamte IT-Landschaft. Es werden nur gewünschte Verbindungen erlaubt – alle anderen sind automatisch verboten. Das dieser Approach immer wichtiger wird, zeigt auch der neue Gartner Market Guide für Mikrosegmentierung: Der Marktreport geht davon aus, dass bis 2026 60 Prozent der Unternehmen, die auf eine Zero-Trust-Architektur hinarbeiten, Mikrosegmentierung einsetzen werden – heute sind es lediglich fünf Prozent.

Illumio ZTS amortisiert sich innerhalb von nur sechs Monaten, wie die Forrester Total Economic Impact Studie zu Illumio ZTS zeigt. Zudem sparen Unternehmen, die zu den Pionieren bei ZTS gehören, laut dem Zero Trust Impact Report der Enterprise Strategy Group jährlich durchschnittlich 20,1 Millionen US-Dollar an Downtime-Kosten ein.

Ransomware ist zwar eine enorme Gefahr, die sicher nicht verschwinden wird. Aber mit Illumio ZTS können Unternehmen Risiken reduzieren, Cyberresilienz aufbauen und dafür sorgen, dass kleine Sicherheitsverletzungen nicht zu großen Cyberkatastrophen werden.

Alexander Goller | www.illumio.com

Schneller, höher, weiter

MIT ZERO TRUST DIE TRANSFORMATION VORAN BRINGEN

Noch nie war der Geschäftserfolg so eng mit der IT-Abteilung verknüpft wie in den letzten Jahren der Digitalisierung. Seit User, Anwendungen und Geräte in verteilten Umgebungen angesiedelt sind, erhält Zero Trust Bedeutung, die über die Sicherheit hinausgeht. Durch den Einblick in alle Datenströme eines Unternehmens durch die Zscaler Zero Trust Exchange-Plattform lassen sich mit Hilfe von künstlicher Intelligenz die Grundlagen für Geschäftsentscheidungen schaffen. Kevin Schwarz, Head of Field CTOs International bei Zscaler erläutert, wie Unternehmen durch Zero Trust schneller, höher und weiter in ihrer Transformation vorankommen.

it security: *Unternehmen sind kontinuierlich damit beschäftigt, sich weiterzuentwickeln. Welche Rolle spielt Zero Trust dabei?*

Kevin Schwarz: Dabei zu helfen, dass Transformation möglich ist und dies sicher. Einer der Grundbausteine einer Einführung einer Zero Trust Architektur ist Visibilität in Datenzugriffe und Kontext. Durch unsere Plattform sind wir in einer privilegierten Position. Da sie zwischen den Anwendungszugriff geschaltet ist, erhält man zusätzlich wertvolle Informationen. Wir stellen nicht nur die Sicherheit der Anbindung sicher, unsere Kunden erhalten auch Einblick in die Verbindungsqualität oder in ihre Applikationslandschaft. Der Reichtum an Daten liefert Visibilität zu Sicherheitsthemen und kann darüber hinaus auch als Grundlage für Geschäftsentscheidungen dienen. Wenn ein Unternehmen beispielsweise Sichtbarkeit über die Zugriffe einer kritischen Anwendung erhält, können danach Rückschlüsse auf die eigentlich berechtigten Nutzer oder Geräte gezogen und hinterfragt werden.

it security: *Mit welchen Anforderungen an die Sicherheit treten Unternehmen heute an Zscaler heran?*

Kevin Schwarz: Unternehmen haben erkannt, dass sie mit einer Transitionsstrategie, bei der existierende Sicherheitstechnologie lediglich aktualisiert wird, nicht mehr weiterkommen. Sie suchen vielmehr nach Unterstützung, um ihre Infrastrukturen ganzheitlich an die digitale Transformation anzupassen. Wenn User und Applikationen das Rechenzentrum verlassen haben, dann müssen Datenströme jenseits des Netzwerks performant abgesichert werden. Dabei gilt es nicht mehr nur den User, sondern auch Workloads oder die Kommunikation zwischen Geräten (wie etwa IoT) zu berücksichtigen. Alle Parteien wünschen sich heute im Zuge der Resilienzsteigerung und Vereinfachung eine Reduzierung der eingesetzten Anbieter bei dem Thema Sicherheit.

it security: *Wie lässt sich ein solcher One-Stop-Shop konkret umsetzen und was sind die Vorteile?*

Kevin Schwarz: Eine Plattform, die nicht nur den bestehenden Datenfluss in alle Richtungen absichert, sondern das Sicherheitspostulat kontinuierlich hinterfragt und verbessert, bringt die IT-Sicherheit in die Zukunft. Wir haben mit Risk360 und Breach Prediction neue Services vogestellt, die mit Hilfe von künstlicher Intelligenz und der Nutzung von verschiedensten Datenquellen Empfehlungen liefern, wie Risiken aktiv mitigiert werden können. Dabei hilft die ganzheitliche Sicht auf die Bedrohungslandschaft, vorhandene Policies und Konfigurationen, um Lücken aufzuzeigen. Bestehen beispielsweise überprivilegierte Zugriffsberechtigungen auf sensible Applikationen und Daten? Eine hochintegrierte Plattform, die mit Hilfe von KI Daten auswertet, gibt Sicherheit durch eine Benutzeroberfläche, bei der der manuelle Korrelationsaufwand verschiedener Punktlösungen der Vergangenheit angehört. Somit kommt die IT-Abteilung schneller und mit weniger Aufwand zum Ziel, bessere Sicherheit zu gewährleisten.

it security: *Damit wäre der Punkt der schnelleren Sicherheit durch Zero Trust beantwortet. Wie trägt Zero Trust nun zusätzlich zu höherer Sicherheit bei?*

Kevin Schwarz: Dass die Angriffsfläche von Unternehmen intern wie extern durch Segmentierung nach dem Prinzip von Least Privilege reduziert wird. Es erhält jeder Nutzer / jedes Gerät nur Zugriff auf die Ressourcen, die es benötigt. Ein Prinzip beziehungsweise Konzept was innerhalb der IT natürlich nciht neu, allerdings mit herkömmlichen Methodiken sehr schwer bisher zu implementieren war.

Wichtig ist allerdings auch, einen Schritt weiterzudenken, selbst wenn eine Unternehmung den Anwendungszugriff auf Basis von Least Privilege Access segmentiert hat. Wie können wir einen Angreifer entdecken, der sich als ein verifizierter Nutzer ausgibt? Themen wie Deception helfen dabei auch mut- oder böswillige Kommunikation zu erkennen.

it security: *Worauf sollten Unternehmen im Hinblick auf Cloud-Umgebungen heute noch achten?*

Kevin Schwarz: Entscheidend für die Sicherheit von Unternehmen ist, dass sie Einblick in alle Datenströme erhalten. Denn nur, wenn das Sicherheitsteam alle Kommunikationswege überwachen kann, können sie dort auch versteckte Bedrohungen aufspüren. Solange Lücken in der Überwachung bestehen, sind Unternehmen auf einem Auge blind, um Schadcode zu erkennen. Es ist erforderlich die gesamte Infrastruktur inklusive der Cloud unter einen konsolidierten Zero-Trust-Schutzschirm zu holen – und damit die Sicherheit zu erweitern. Die Cloud birgt ein enormes Potenzial, um Unternehmen sicherer aufzustellen und diverse Prozesse sogar zu beschleunigen, zum Beispiel im Hinblick auf das Thema „Infrastructure as a Code" als Teil von DevSecOps.

> UNTERNEHMEN TUN GUT DARAN, LÖSUNGSANSÄTZE ZU EVALUIEREN, DIE IHNEN SCHNELLE REAKTIONEN UND VORBEUGENDES HANDELN ERMÖGLICHEN.
>
> **Kevin Schwarz, Head of Field CTOs International, Zscaler, www.zscaler.de**

it security: *Können Sie uns erläutern, warum Zero Trust ein Business-Enabler ist und damit Mehrwerte über die Sicherheit hinaus liefern kann?*

Kevin Schwarz: Diverse Themen sind bei Zero Trust egal, zum Beispiel welches Gerät (ob Firmengerät oder BYOD) oder auch das Thema Konnektivität. Könnte ich zum Beispiel einen Standort und die Geräte ohne viel Infrastruktur zum Beispiel via 5G anbinden? Wenn Zero Trust-Prinzipien gerade in Cloud-Deployments wie eben angesprochen zum Einsatz kommen, schalten Unternehmen in eine Art Turbo-Modus. Sicherheit & Anwendungen lassen sich nicht nur schneller ausrollen, sondern die Vorteile auch weiter fassen.

Ein anderes Beispiel ist die Akquisition eines Unternehmens. Hierbei zählt die Geschwindigkeit zur Realisierung des ROI. Mit Hilfe von Zero Trust könnte der autorisierte Zugriff auf Anwendungen des gekauften Unternehmens innerhalb von Tagen hergestellt werden. Die Frage stellt sich, ob man das akquirierte Unternehmen komplett integrieren möchte, wodurch potenziell die üblichen Monate der aufwändigen und unsicheren Zusammenführung ganzer Netzwerke wegfallen könnten. Hier gehen Sicherheits- und Geschäftsanforderungen Hand in Hand.

it security: *Eine Frage zum Abschluss. Ist KI ihrer Meinung nach aus der Sicherheit noch wegzudenken?*

Kevin Schwarz: Künstliche Intelligenz muss heute zum Einsatz kommen, um einen Geschwindigkeitsvorteil zu erlangen. Wir wissen nur zu gut, dass auch die Angreifer die modernen Technologien einsetzen. Darum tun Unternehmen gut daran, Lösungsansätze zu evaluieren, die ihnen schnelle Reaktionen und vorbeugendes Handeln ermöglichen. Eine moderne Sicherheit kommt ohne KI nicht mehr aus, da nur so die Automatisierung von Prozessen, aber auch eine Simplifizierung der Komplexität gewachsener Sicherheitsinfrastrukturen erreicht werden kann.

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

KI macht Ransomware noch gefährlicher

ADÄQUATE TECHNOLOGIEN UND PRAKTIKEN GESUCHT

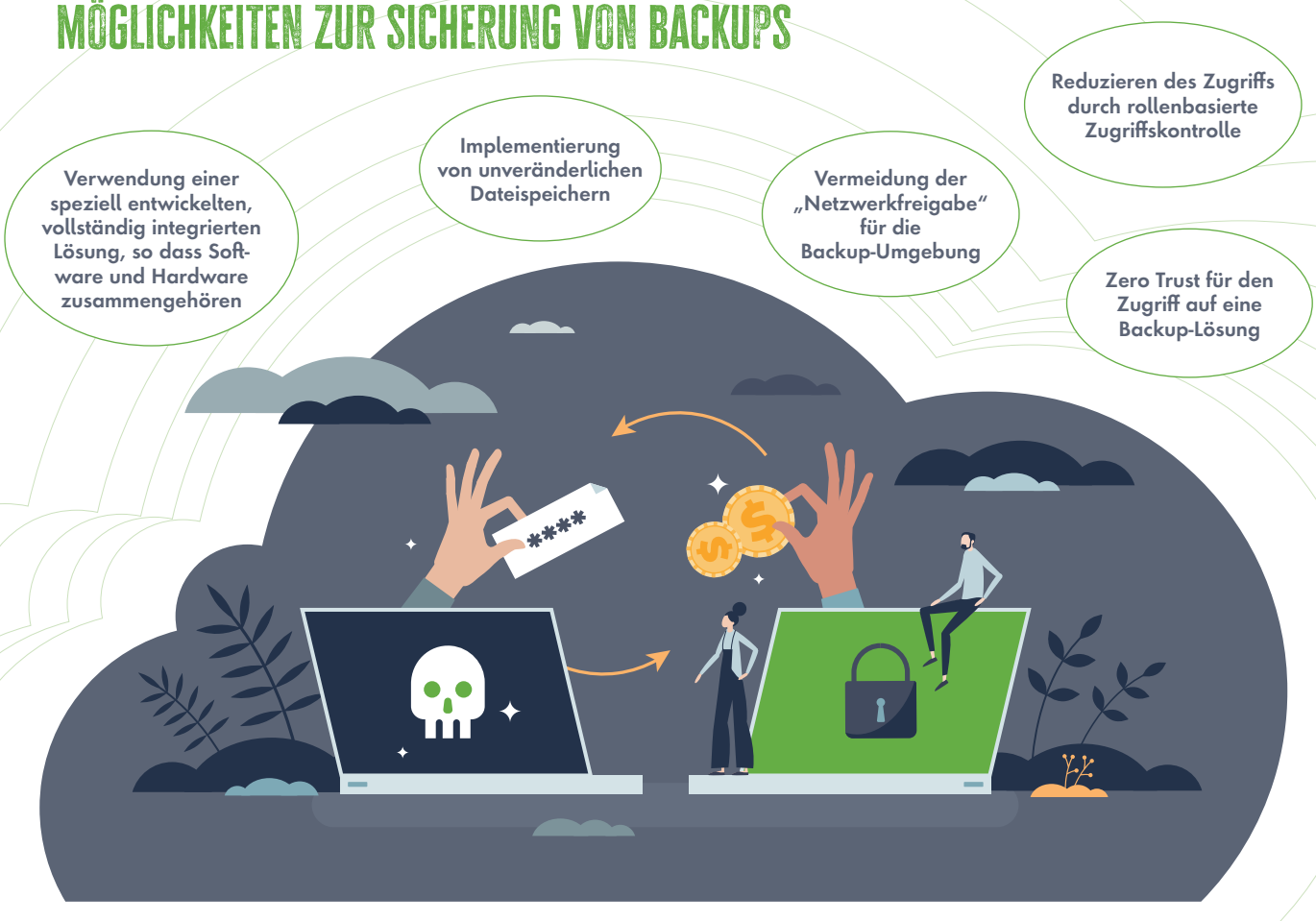
Ransomware ist schon längere Zeit ein echtes Problem für Organisationen jeder Art und Größe. Betrachtet man die neuesten Entwicklungen, ist keine Entwarnung in Sicht. Eher im Gegenteil: Die Kriminellen nutzen mittlerweile KI, um ihre Angriffe noch effizienter zu machen.

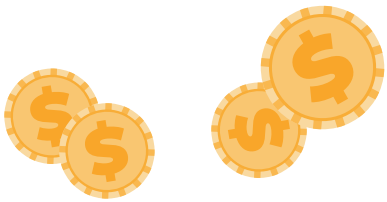
Nominal hat sich die Anzahl der gemeldeten Angriffe über alle Branchen hinweg im letzten Jahr verdoppelt - und seit 2021 mehr als vervierfacht. Dies ist zu einem großen Anteil auf KI für Automatisierung zurückzuführen, die den Kriminellen dabei hilft, mehr Angriffe durchführen zu können. Gleichzeitig steigt auch die Qualität. Denn die Angreifer nutzen generative KI um sehr schnell und ohne großen Aufwand gut gestaltete und grammatikalisch korrekte Phishing-E-Mails zu erstellen. KI führt damit dazu, dass man diese E-Mails anhand von Grammatik- und Rechtschreibfehlern kaum noch erkennen kann. Ransomware-as-a-Service-Tools und generative KI für Texterstellung und Codegenerierung machen es Cyberkriminellen mithin immer einfacher, ihrem Handwerk nachzugehen.

Schutz gegen Ransomware ist möglich

Oberflächlich betrachtet scheint gegen Ransomware kein Kraut gewachsen zu sein. Schaut man sich die Zahlen erfolgreicher Angriffe jedoch nach Industrie

MÖGLICHKEITEN ZUR SICHERUNG VON BACKUPS





an, fällt ein Trend auf: Finanzinstitute werden weniger häufig angegriffen als Öffentliche Verwaltung, Ausbildung oder das Gesundheitswesen. Der Anteil der Ransomware-Angriffe stieg im Jahresvergleich in allen fünf Schwerpunktbranchen - mit Ausnahme von Finanzunternehmen. Angriffe auf Kommunen stiegen von 12 Prozent auf 21 Prozent, Angriffe auf das Gesundheitswesen von 12 Prozent auf 18 Prozent, Angriffe auf das Bildungswesen von 15 Prozent auf 18 Prozent und Angriffe auf die Infrastruktur von 8 Prozent auf 10 Prozent. Im Vergleich dazu gingen die Angriffe auf Finanzinstitute von sechs Prozent auf ein Prozent zurück.

Die Tatsache, dass Finanzinstitute sehr begehrte Opfer mit potenziell hohen Renditen für die kriminellen Angreifer wären, sich diese aber auf die eher klammen Branchen fokussieren, lässt einen klaren Schluss zu: Die Finanzindustrie hat höhere Security-Budgets, ist daher besser abgesichert und die Angreifer müssten deutlich mehr in ihre Angriffe investieren.

Fünf Praktiken zur Verbesserung der Widerstandsfähigkeit gegen Ransomware:

#1 Erkennung und Prävention

Die Priorität sollte darin bestehen, Maßnahmen und Tools zur Erkennung und Verhinderung eines erfolgreichen Angriffs bereitzustellen. In der heutigen, sich schnell entwickelnden Bedrohungslandschaft bedeutet dies die Implementierung tiefgreifender, mehrschichtiger Sicherheitstechnologien, einschließlich KI-gestütztem E-Mail-Schutz und Zero-Trust-Zugriffsmaßnahmen, Anwendungssicherheit, Bedrohungsjagd, XDR-Funktionen und effektiver Reaktion auf Vorfälle.

#2 Widerstandsfähigkeit und Wiederherstellung

Auch mit begrenzten Ressourcen kann man sich effektiv von Ransomware-Angriffen erholen. Zunächst sollte man damit rechnen, dass die Angreifer es auch auf die Infrastruktur für Geschäftskontinuität und Notfallwiederherstellung abgesehen haben - einschließlich der Backup-Systeme. Zahlreiche Vorfälle belegen, dass Angreifer oft erst dann Lösegeld fordern, wenn sie sicher sind, dass das Opfer nur begrenzte Möglichkeiten zur Wiederherstellung hat.

#3 Sicherung von Backups, Air-Gaps und Cloud-Backups

Das Trennen des Speichers von der typischen Betriebsumgebung des Administrators mittels eines Air-Gaps verbessert dessen Sicherheit. Die Cloud ist in diesem Fall die beste Option. Man muss jedoch bedenken, dass die Wiederherstellung über das Internet etwas langsamer ist als lokale Wiederherstellung.

#4 Spezielle Backup-Appliances

Hypervisoren für virtuelle Maschinen stellen leider zusätzliche Angriffsflächen dar, die böswillige Akteure nutzen können, um in die Backup-Lösung einzudringen. Daher empfiehlt es sich nach wie vor die Verwendung einer speziellen Backup-Appliance-Lösung, wenn das Ziel der Wiederherstellungszeit (RTO) aggressiv ist. Auf keinen Fall sollten Eigenentwicklungen genutzt werden.

#5 SaaS-Anwendungen nicht vergessen

Wichtig ist die Absicherung von Daten, die in der Cloud gespeichert sind. In Microsoft 365-Konten und anderen unter Azure AD registrierten SaaS-Anwendungen liegen wichtige Datenbestände, die eine kontinuierliche Datenklassifizierung, Zugriffskontrolle und Strategie für echten Datenschutz erfordern.

www.barracuda.com

HiScout

Besuchen Sie uns auf der it-sa in Nürnberg!

→ Stand 7A-619

HiScout GRC-Suite

Gemeinsame Datenbasis und Synergien für:

- ✔ IT-Grundschutz nach BSI-Standard 200-1, 200-2 und 200-3
- ✔ ISM nach ISO 27001/2
- ✔ Datenschutz nach EU-DSGVO
- ✔ BCM nach ISO 22301:2019 und BSI-Standard 200-4

Wir haben ein Kontingent kostenfreier Eintrittskarten für Sie reserviert:

→ www.hiscout.com/it-sa

SecurITy made in Germany

Trust Seal www.teletrust.de/itsmig

www.hiscout.com

Sichere Videokonferenzlösung

BEIM SCHUTZ IHRER KOMMUNIKATION STEHEN VIELE UNTERNEHMEN KOMPLETT BLANK

Videokonferenzen werden für Cyberkriminelle immer beliebter. Warum Unternehmen es den Angreifern viel zu leicht machen und wie man sich clever verteidigen kann, darüber sprach Lars Becker, Redakteur it security, mit Valentin Boussin, Country Manager Dach bei Tixeo.

Lars Becker: *Videokonferenzen waren besonders während der Pandemie häufig Ziel von Cyberangriffen. Wie hat sich die Gefahrenlage seit dem entwickelt?*

Valentin Boussin: Das Risiko von Hackerangriffen auf die Online-Kommunikation von Unternehmen ist seit dem Ende der Pandemie höher denn je. Videokonferenzen sind in den meisten Unternehmen nicht mehr wegzudenken. Allerdings versäumen viele, sie auch umfassend gegen Cyberangriffe zu schützen, obwohl dort häufig hochsensible Inhalte ausgetauscht werden. Das macht sie als Ziel für Hacker attraktiv.

TIXEO IST DIE EINZIGE LÖSUNG AUF DEM MARKT, DIE FÜR IHRE ENDE-ZU-ENDE-VERSCHLÜSSELUNG CSPN-ZERTIFIZIERT IST.

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

Lars Becker: *Welche Konsequenzen haben solche Angriffe für Unternehmen?*

Valentin Boussin: Das ist je nach Art und Ziel des Angriffs ganz unterschiedlich. Manche Cyberkriminelle klinken sich in Videokonferenzen ein, um zu stören. Die ungebetenen Gäste konfrontieren die Teilnehmer der Konferenz teils mit Hassbotschaften oder anderen verstörenden Inhalten.

Andere Arten von Cyberangriffen belasten Unternehmen finanziell – sei es als Folge von Industriespionage, oder weil sie Schäden teuer reparieren müssen. Laut Bitkom erleidet die deutsche Wirtschaft jährlich einen Schaden von ca. 203 Milliarden Euro durch Cyberangriffe. Andere Hackerangriffe zielen auf persönliche Daten ab. Werden solche entwendet, drohen hohe Bußgelder.

Lars Becker: *Was sind die wichtigsten Sicherheitsrisiken, die man in Bezug auf Datenschutz und Zugriffskontrolle kennen sollte?*

Valentin Boussin: Ein Punkt ist eine mangelnde Kontrolle des Zugangs zu Online-Meetings. Das heißt: Organisatoren der Meetings überprüfen die Identität der Personen nicht, die sich in die Videokonferenz einklinken möchten. Jeder, der den Zugangslink oder andere Zugangsdaten entwendet hat, könnte also dem Meeting beitreten.

Auch der Datenschutz wird oft vernachlässigt. Die meisten Unternehmen nutzen in den USA ansässige Videokonferenzanbieter, ungeachtet dessen, dass der Cloud Act diese verpflichtet, in bestimmten Fällen den US-Behörden Zugang zu Kommunikationsinhalten zu gewähren. Das widerspricht somit diametral der europäischen DSGVO.

Lars Becker: *Warum sind die gängigen Tools für Videokonferenzen nicht wirklich sicher?*

Valentin Boussin: Die gängigsten Videokonferenzanbieter bieten keine echte Ende-zu-Ende-Verschlüsselung der Kommunikation. Die Kommunikation ist nicht von Client zu Client verschlüsselt und ist somit immer dann entschlüsselt, wenn sie die Server passiert. Angreifer können diese Lücke nutzen, um sowohl auf die Inhalte der Kommunikation als auch auf ausgetauschte Dateien zuzugreifen.

Die genutzte Cloud ist ein weiterer Grund, warum die gängigsten Tools für Videokonferenzen unzureichenden Schutz der ausgetauschten Daten gewähren. Viele Plattformen bieten ihre Dienste über US-amerikanische Clouds. Damit gilt der erwähnte Cloud Act, die Vertraulichkeit der Kommunikation ist nicht gewährleistet und die DSGVO wird nicht eingehalten.

Lars Becker: *Wie garantieren Sie bei Tixeo die Kompatibilität mit der DSGVO?*

Valentin Boussin: Für Tixeo hat die Vertraulichkeit der persönlichen Daten

einen sehr hohen Stellenwert. Deshalb nutzen wir ausschließlich europäische Clouds. Unsere Lösung übermittelt niemals die persönlichen Daten der Nutzer in ein Drittland oder an eine andere Einrichtung.

Lars Becker: *Warum genau ist eine Ende-zu-Ende-Verschlüsselung der Kommunikation so wichtig?*

Valentin Boussin: Sie ist eine der wirksamsten Maßnahmen zur Abwehr von Cyberangriffen. Damit ist sie der Grundpfeiler von Videokonferenzlösungen, die eine vollständige Vertraulichkeit der Kommunikation gewährleisten können.

Diese Verschlüsselung zeichnet sich dadurch aus, dass die Keys zur Entschlüsselung der Kommunikationsströme nur auf den jeweiligen Geräten der Gesprächspartner gespeichert werden. Dadurch kann nicht einmal Tixeo auf die Schlüssel zugreifen. Somit ist die Vertraulichkeit der Kommunikation garantiert, auch bei mehreren Teilnehmern.

Lars Becker: *Wodurch unterscheidet sich Ihre Videokonferenzlösung von anderen auf dem Markt erhältlichen Produkten in Bezug auf Schutz vor Cyberangriffen?*

Valentin Boussin: Tixeo ist die einzige Lösung auf dem Markt, die für ihre Ende-zu-Ende-Verschlüsselung CSPN-zertifiziert ist. Diese Zertifizierung wird vom deutschen Bundesamt für Sicherheit in der Informationstechnik (BSI) als gleichwertig zu einem Zertifikat nach der Beschleunigten Sicherheitszertifizierung (BSZ) anerkannt.

Viele Videokonferenzlösungen geben an, eine Ende-zu-Ende-Verschlüsselung zu bieten, verschlüsseln allerdings lediglich die Datenströme zwischen dem Benutzer und dem Kommunikationsserver. Sprich eine Ende-zu-Ende-Verschlüsselung ist nur bei zwei Teilnehmern gegeben. Bei Tixeo dagegen werden Verschlüsselungsschlüssel mit der Konferenz erstellt und ausschließlich zwischen den Teilnehmern ausgetauscht. Niemand sonst hat Zugriff auf die Schlüssel und es ist unmöglich, den Kommunikationsstrom zu entschlüsseln. Außerdem sind wir 100 Prozent Made in Europe.

Lars Becker: *Wie können Unternehmen den Übergang zu sicheren Videokonferenzlösungen erleichtern?*

Valentin Boussin: Der Umstieg auf Tixeo fällt den meisten Nutzern erfahrungsgemäß leichter als viele zunächst fürchten. Bei den meisten Softwares ist die Benutzeroberfläche ähnlich gebaut. Auch für Unternehmen und Admins ist es einfach, da sie die IT-Infrastruktur gar nicht oder nur geringfügig umbauen müssen.

Außerdem erkennen Kunden und Gesprächspartner schnell die Vorteile unserer Lösung. Features wie der Kollaborationsmodus bewirken, dass viele User nach kurzer Zeit gar nicht mehr zurück zu ihrer vorherigen Plattform wollen.

Lars Becker: *Können sie konkrete Beispiele nennen, in denen Tixeo dazu beigetragen hat, Industriespionage zu vereiteln und sensible Unternehmensinformationen zu schützen?*

Valentin Boussin: Viele unserer Nutzer kommen aus Branchen, in denen hochsensible Daten geschützt werden müssen. Dazu zählen Pharma, der Finanzsektor, die Rüstungsindustrie oder öffentliche Behörden. Zum Beispiel setzt das Pharma-Unternehmen Avmatsim – in seiner Sparte ein Weltmarktführer – ausschließlich auf Tixeo. Zudem zählen in Deutschland wie auch in ganz Europa öffentliche Behörden zu unseren Kunden, sogar EU-Institutionen.

Lars Becker: *Wie sehen Sie die Zukunft der sicheren Videokonferenzen im Hinblick auf die Bekämpfung von Industriespionage?*

Valentin Boussin: Während der Pandemie ging es bei Videokonferenzen meistens vor allem darum, dass sie funktionieren. Immer mehr Unternehmen werden aber erkennen, dass sie den Schutz der Kommunikation bisher ignoriert haben. Die Fälle von Cyberangriffen und Industriespionage nehmen Jahr für Jahr zu, gleichzeitig fehlen Experten für Cybersecurity.

Lars Becker: *Herr Boussin, vielen Dank für das Gespräch.*

STRATEGISCHER LEITFADEN E-MAIL CYBERSICHERHEIT

EIN PERSONENZENTRIERTER ANSATZ ZUM STOPPEN VON RANSOMWARE, MALWARE, PHISHING UND E-MAIL-BETRUG

Jeden Tag wird an einem Ort, an dem sich Mitarbeiter tagtäglich befinden, ein verborgener Kampf ausgetragen: im E-Mail-Posteingang.

Malware wird primär über E-Mails verbreitet und die E-Mail bietet Cyberangreifern die ideale Plattform für Betrügereien aller Art. Das macht die E-Mail zum Bedrohungsvektor Nummer 1. Mittels Social Engineering verleiten Cyberkriminelle Anwender in Unternehmen dazu, auf unsichere Links zu klicken, Anmeldedaten einzugeben oder gar unwissentlich bei der Umsetzung der Angriffe mitzuhelfen (etwa indem sie Geld an die Betrüger überweisen oder vertrauliche Dateien senden).

Der Grund für die Begeisterung der Angreifer für E-Mails liegt auf der Hand: Die jahrzehntealte Architektur ist nicht auf Sicherheit ausgelegt. Sie ist universell im Einsatz. Und im Gegensatz zu Computer-Hardware und -Infrastruktur lässt sich mit E-Mail-Angriffen eine Schwachstelle ausnutzen, für die es keine Patches gibt: der Mensch.

Der Wechsel zur Cloud und die Arbeit im Homeoffice verschärfen dieses Problem noch zusätzlich. Trotz der bei Unternehmen eingesetzten Sicherheitslösungen führen Business Email Compromise (BEC), Ransomware und Supply-Chain-Attacken weiterhin zu Kompromittierungen.

Die Angreifer haben ihre Techniken weiterentwickelt und kombinieren inzwischen verschiedene Taktiken, um in einer integrierten Angriffskette die „Schwachstelle Mensch" auszunutzen. Gleichzeitig sind herkömmliche Lösungen mit isolierten Tools nicht in der Lage, diese integrierten Bedrohungen abzuwehren.

Im „Strategischen Leitfaden E-Mail-Sicherheit" zeigen wir, wie Sie durch das Stoppen hochentwickelter E-Mail-Attacken die Angriffskette unterbrechen und Erst-Kompromittierungen verhindern können.

WHITEPAPER DOWNLOAD

Das Whitepaper umfasst 25 Seiten und kann kostenlos herunter geladen werden.
www.it-daily.net/Download

Mobile Sicherheit

WARUM UNTERNEHMEN JETZT HANDELN MÜSSEN

Smartphones sind aus dem Berufsalltag nicht mehr wegzudenken. Laut Branchenverband Bitkom [1] nutzen 87 Prozent der Unternehmen mobile Endgeräte regelmäßig zur Kommunikation mit Kollegen, Geschäftspartnern und Kunden.

Smartphones sind allerdings auch ein beliebtes Angriffsziel für Cyberkriminelle. Der Sicherheitsspezialist Kaspersky verzeichnete im vergangenen Jahr mehr als 1,6 Millionen [2] gefährliche oder unerwünschte Softwareprogramme für mobile Endgeräte, fast 200.000 Mobile-Banking-Trojaner und über 10.000 Mobile-Ransomware-Varianten.

Effizienter Smartphone-Schutz

Um die Risiken zu minimieren, sollten Unternehmen bei der Verwaltung von Smartphones auf eine ganze Reihe von Technologien und Methoden setzen. Die folgenden Hinweise beziehen sich im Wesentlichen auf das Betriebssystem Android.

Finden Sie heraus, wie die Samsung Knox-Lösungen Ihrem Unternehmen dabei helfen, eine kontinuierlich gewachsene Angriffsfläche wirksam zu verteidigen.

Besuchen Sie uns auf der it-sa,
Halle 7, Stand 7A-620

➤ **Firmware- und OS-Management:** Veraltete Versionen können ein erhebliches Sicherheitsrisiko darstellen. Es empfiehlt sich daher, ein zentrales Firmware-Management wie Knox E-FOTA zu nutzen. Die Firmware-over-the-Air-Lösung ermöglicht es, Software-Updates zentral zu planen, sie zu testen und – falls erforderlich – die Aktualisierung eines Gerätes zu erzwingen.

➤ **Berechtigungsmanagement:** IT-Sicherheitsverantwortliche sollten betriebliche Smartphones über eine zentrale Managementkonsole verwalten und eine Zwei-Faktor-Authentifizierung erzwingen können. Ein Remote-Zugriff kann sicherstellen, dass Administratoren gestohlene oder verloren gegangene Geräte bei Bedarf aus der Ferne sperren oder löschen können.

➤ **App-Management:** Der unkontrollierte Download von Apps stellt ein erhebliches Sicherheitsrisiko dar. Sicherheitsverantwortliche sollten deshalb die Installation von Apps auf den Handys der Unternehmensmitarbeiter einschränken können. Mit Tools wie dem SE for Android Management Service (SEAMS) können sich zudem Apps von der restlichen Betriebsumgebung isolieren und zusätzlich sichern lassen.

➤ **Verschlüsselung sensibler Daten:** Android bietet seit Version 7.0 mit der dateibasierten Verschlüsselung (File-based Encryption, FBE) bereits einen Basis-Schutz. Manche Hersteller, etwa Samsung, ergänzen den Verschlüsselungsschutz durch ein zusätzliches Kryptographie-Modul (Dual Data-at-Rest Encryption).

➤ **Trennung von privater und geschäftlicher Nutzung:** Fast 90 Prozent der Beschäftigten mit einem Dienst-Handy dürfen dieses auch privat nutzen. [3] Umgekehrt nutzt ein Drittel das private Smartphone auch für dienstliche Belange. Ist eine Mischnutzung erlaubt, sollten geschäftliche Daten in einem sicheren Container wie Knox Vault auf dem Gerät isoliert und so vor Fremdzugriffen geschützt werden.

➤ **Sicherstellung der Geräteintegrität:** Schon beim Start des Geräts sollte die Integrität des Betriebssystems und aller Applikationen überprüft werden. Einige Geräte bieten dafür bereits hardwareseitig Vorkehrungen wie den Device-Unique Hardware Key (DUHK) bei Samsung-Geräten.

➤ **Schutz der Übertragungswege:** IT-Administratoren sollten die Nutzung eines Virtual Private Network (VPN) für betriebliche Zwecke erzwingen, wenn sich das Gerät in ein nicht sicheres WLAN einbuchen will. Für den professionellen Einsatz empfehlen sich Lösungen wie das Knox VPN Framework, das angepasste Funktionen und eine starke Verschlüsselung bietet.

Fazit

Unternehmen können die Risiken der Smartphone-Nutzung dann in den Griff bekommen, wenn sie diese zentral managen und schützen. Plattformen wie Samsung Knox bieten dafür gute Voraussetzungen. Sie erlauben es, Endgeräte automatisiert in ein Mobile Device Management integrieren, riskantes Nutzerverhalten unterbinden, sowie Funktionen zeit- oder personenbasiert einschränken zu können.

www.samsung.com/de/business/

Samsung Knox

1: https://www.bitkom.org/sites/main/files/2023-05/230511Bitkom-Charts-Digital-Office.pdf
2: https://securelist.com/mobile-threat-report-2022/108844/
3: https://www.bitkom.org/Presse/Presseinformation/Diensthandy-darf-meist-privat-genutzt-werden

Automatisierung des Onboardings

DIGITALISIERUNG OHNE DIGITALE IDENTITÄTEN ERFORDERT ZWISCHENSCHRITT

Die zunehmende Digitalisierung verändert auch die Art und Weise, wie wir bei gewissen Prozessen die eigene Identität nachweisen. Ein gutes Beispiel ist die Eröffnung eines Kontos bei der Bank. Musste früher ein Sachbearbeiter die Identität einer Person mittels eines Ausweisdokuments manuell überprüfen, ob der- oder diejenige auf dem Bild auch die vor ihm sitzende Person ist, ist das heute nicht mehr Standard. Digitale Identitäten können hier Abhilfe schaffen. Doch wie so oft, steckt der Teufel im Detail.

Die Europäische Union regt ihre Bürger dazu an, sich um eine einzige digitale Identität zu bemühen, die sich von einer Vielzahl von Organisationen nutzen lässt. Der Schutz der Privatsphäre und die Datensicherheit sind die Triebfedern dieses Paradigmas, das auch für Unternehmen Anwendung findet. Die Identitätsprüfung ist einer der ersten Schritte auf dem Weg zu einer digitalen Identität und gehört mittlerweile ebenso zur digitalen Transformation, wie die Online-Eröffnung eines Bankkontos.

Onboarding smart und effizient steuern

Musste in der Vergangenheit beim Onboarding neuer Mitarbeiter oder Kunden ein Identitätsnachweis erbracht werden, konnte es sich je nach Land dabei um einen Personalausweis oder Belege wie eine Gas- oder Stromrechnung oder eine Steuererklärung handeln. Persönliches Erscheinen wurde sehr oft vorausgesetzt, geprüft wurden die Dokumente manuell. Mit Recht verlangen Kunden in Zeiten der Digitalisierung ein einfaches Verfahren zur Einreichung aller Informationen. Darüber hinaus sollten Unternehmen über optimierte Möglichkeiten zur Verarbeitung dieser verschiedenen Dokumente verfügen. Gefordert ist eine einfache und unkomplizierte Möglichkeit, alle erforderlichen Dokumente mithilfe eines mobilen Gerätes – wie etwa eines Handys – zu erfassen und bereitzustellen. Moderne Lösungen wie intelligente Dokumentenverarbeitung, mobile Erfassungsmöglichkeiten, Process-Mining-Technologien, Composable Technologien und Identitätsnachweistechnologien tragen dazu bei, Prozesse smart und effizient zu steuern, damit Kunden weniger Last damit haben.

In der heutigen Zeit ist dieser Prozess trotzdem oft noch manuell ausgelegt –

TOP 3 TECHNOLOGIEN, DIE UNTERNEHMEN FÜR DAS ONBOARDING EINFÜHREN WOLLEN:

24 %
Mobile Erfassungslösungen

26 %
Intelligente Dokumenten-verarbeitung

22 %
Process Intelligence

obwohl der Onboarding-Prozess ein grundlegender Aspekt der Kundenerfahrung und der gesamten Customer Journey ist. Er definiert alle zukünftigen Interaktionen zwischen dem Kunden und dem Unternehmen. Ein langwieriger Prozess belastet häufig schon zu Beginn die Zusammenarbeit oder Partnerschaft negativ. So ist es trotz modernster Tools und Verkaufstrainings erstaunlich, dass laut aktueller Zahlen 94 Prozent der deutschen Unternehmen während dieses Prozesses immer noch irgendeine Form von Abbruch verzeichnen.[1]

Maximale Sicherheit

Es liegt in der Aufgabe der CIOs regelmäßig ihre Onboarding-Prozesse zu bewerten, um sicherzustellen, dass alles den Anforderungen der Kunden entspricht. Dazu gehört der Einsatz automatisierter Systeme zur Identitätsprüfung und -zertifizierung. Diese müssen einen vollständig integrierten Service bieten, der eine optimale Nutzererfahrung gewährleistet und die Risiken und die Betrugsanfälligkeit reduziert, um maximale Sicherheit zu gewährleisten. „Jedes Mal, wenn eine Website uns auffordert, eine neue digitale Identität zu erstellen oder uns bequem über eine große Plattform anzumelden, haben wir in Wirklichkeit keine Ahnung, was mit unseren Daten geschieht", bemängelte Ursula von der Leyen, Präsidentin der Europäischen Kommission[2], und schlug vor, eine sichere europäische digitale Identität zu etablieren. Eine vertrauenswürdige Identität, die jeder Bürger überall in Europa nutzen könne, um alle möglichen Transaktionen durchzuführen, von der Steuerzahlung bis hin zum Fahrradverleih. Eine Technologie, die es ermögliche, selbst zu überprüfen, welche Daten wie verwendet werden.

Intelligente Automatisierung

Unternehmen werden in naher Zukunft ebenfalls von dieser Entwicklung betroffen sein. Die Kunden erwarten nicht nur eine vereinfachte Integration, sondern auch die Möglichkeit, die Vertrauenswürdigkeit eines Unternehmens sehr schnell mithilfe ähnlicher Technologien zu überprüfen. Und obwohl die Entwicklungen im Bereich des Onboardings dazu tendieren, Automatisierungstechnologien in die aktuellen Prozesse zu integrieren, ist es klar, dass die menschliche Interaktion immer noch eine Schlüsselrolle spielt. Trotz der schnellen Einführung neuer Technologien seit der Pandemie bleibt eine gute Kundenerfahrung eine Sache des Umgangs miteinander, sei es persönlich oder online.

Von entscheidender Rolle bei der Rationalisierung der Verarbeitung von Identitätsdokumenten ist auch die Vereinfachung der Art und Weise, wie Kunden alle ihrem Identitätsdokument beigefügten Belege einreichen können – beispielsweise über die Kamera ihres Smartphones. Intelligente Automatisierungslösungen werten die wichtigen Daten der Dokumente aus und geben sie automatisch in die verschiedenen Systeme des Unternehmens ein. Unternehmen müssen in der Lage sein, Standards und Prozesse einzurichten, um zweifelhafte oder fehlende Daten zu erkennen, damit ihre Mitarbeiter sie überprüfen und die entsprechende Authentifizierung bestätigen können.

Proof of Identity

Auf Seite der Anbieter derartiger Lösungen wiederum muss kontinuierlich in die Verbesserung ihrer Produkte zur Identitätsprüfung investiert werden, um sie noch effizienter und reibungsloser zu gestalten. Besonderes Interesse gilt dabei den Dokumenten, die die Nutzer bereitstellen. Wichtig ist zu gewährleisten, dass Nutzeridentität und Verarbeitung der dazugehörigen Dokumente sicher sind. State-of-the-Art-Anwendungen für den „Proof of Identity" vereinen die dokumentenbasierte Identitätsprüfung in einer einzigen Lösung. Deren Leistungsfähigkeit bestimmen Mobile Capture- und Intelligent Document Processing-Technologien, die sowohl für Kunden einfach zu bedienen als auch für Unternehmen sicher sind. Sie bilden den Grundstein für jede digitale Brieftasche oder digitale Identität, sowohl für Bürger als auch für Unternehmen.

LÖSUNGEN DES DIGITALEN ONBOARDINGS SIND HEUTE ZUMEIST NOCH UNVOLLSTÄNDIG, DA SIE KEINE IDENTITÄTSPRÜFUNG ANHAND VON DOKUMENTEN BEINHALTEN.

Maxime Vermeir,
Senior Director AI Strategy, ABBYY,
www.abbyy.com

Fazit

Lösungen des digitalen Onboardings sind heute zumeist noch unvollständig, da sie keine Identitätsprüfung anhand von Dokumenten beinhalten. Nur über diese aber lässt sich die Gültigkeit und Echtheit des Identitätsnachweises gewährleisten und sicherstellen, dass der Kunde derjenige ist, für den er sich ausgibt. Zu einer vollumfänglichen Proof-of-Identity-Lösung gehören das Lesen und Verifizieren von Identitätsnachweisen und die Möglichkeit zur Verarbeitung von Folgedokumenten von einem mobilen Gerät aus. Nur so ist es für Unternehmen und Kunden gleichermaßen sicher und einfach, sie zu verwenden.

Maxime Vermeir

Quellen:
1 https://www.abbyy.com/de/company/news/94-perc-of-companies-lose-potential-customers-during-the-digital-onboarding-process/
2 https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/european-digital-identity_de

WE SECURE IT

15.&16. November 2023

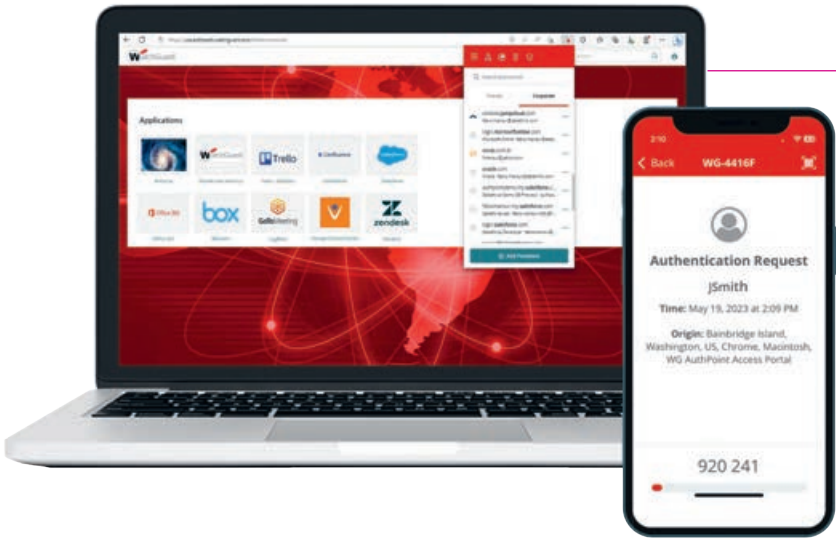
Digitalevent

L O C K E D

#WesecureIT2023

Hier mehr erfahren

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



Die neue Lösung ist auf maximale Anwenderfreundlichkeit ausgelegt.

AuthPoint Total Identity Security

IDENTITÄTEN ABSICHERN MIT MFA UND STARKEN PASSWÖRTERN

Die Verwaltung von Passwörtern stellt für Unternehmen seit jeher eine besondere Herausforderung dar und legt darüber hinaus den Anwendern große Verantwortung auf. Dass hier einiges im Argen liegt, beweist die Statistik:

- Laut Verizon Data Breach Investigations Report lassen sich 74 Prozent der Sicherheitsverletzungen im Jahr 2022 auf die Ausnutzung menschlicher Schwäche – im Hinblick auf gestohlene Zugangsdaten – zurückführen.
- Umfragen bringen immer wieder ans Licht, dass viele Menschen für berufliche und private Konten nach wie vor dieselben Passwörter verwenden.
- 24 Milliarden Anmeldedaten wurden 2022 im Darknet gehandelt.

Klar ist: Passwörter werden in naher Zukunft nicht verschwinden. Selbst wenn Szenarien rund um eine passwortlose Authentifizierung mittlerweile im geschäftlichen Alltag ankommen: Es wird nach wie vor Situationen geben, in denen Passwörter zwangsläufig erforderlich sind. Daher sollten Unternehmen handeln, um dem Russisch-Roulette-Spiel der Zugangsabsicherung ein für alle Mal ein Ende zu bereiten.

Genau hier spielt die neue Lösung „AuthPoint Total Identity Security" von WatchGuard ihre Stärken aus. Das Leistungspaket erweitert die bereits etablierte Multifaktor-Authentifizierung „WatchGuard AuthPoint" um einen Dark Web Monitor Service sowie einen passenden Passwort-Manager. Damit lassen sich nicht nur die Kosten für die Verwaltung von Anmeldedaten senken. Der Schutz von Identitäten wird gleichzeitig effektiv erhöht und das Risiko potenzieller Phishing- und Social-Engineering-Angriffe in Zusammenhang mit dem Diebstahl von Anmeldedaten entscheidend gemindert.

Funktionsbausteine im Überblick:

AuthPoint MFA – Die umfassende Lösung für Multifaktor-Authentifizierung mit Single Sign-On (SSO)-Option ebnet der risikobasierten Authentifizierung den Weg und gewährleistet gleichzeitig eine einfache Verwaltung, die auf maximale Anwenderfreundlichkeit ausgelegt ist.

Dark Web Monitor – Der AuthPoint Dark Web Monitoring-Service benachrichtigt Nutzer proaktiv, wenn kompromittierte Anmeldedaten von überwachten Domänen in einschlägigen oder neuen Datenbanken für Zugangsinformationen auftauchen.

Corporate Passwort-Manager – Speziell für den Einsatz in Unternehmen entwickelt sorgt dieser für die Etablierung eines hohen Passwort-Standards – mit mehr Kontrolle über die Qualität von Passwörtern bei gleichzeitig weniger Anfragen zum Zurücksetzen von Passwörtern.

www.watchguard.de

MEHR WERT
Total Identity Security

it-sa 2023
Besuchen Sie uns
in **Halle 7, Stand 327**

Automatisierte Angriffserkennung und Neutralisierung

PERSONALMANGEL & KÜNSTLICHE INTELLIGENZ IN DER IT-SECURITY

Seit Anfang der 90iger Jahre ist Olaf Müller-Haberland in den Rechenzentren der europäischen Behörden und Unternehmen in der Beratung und Vertrieb tätig. Egal ob HW-, SW-, Service- oder IT-Security Konzepte als Hersteller oder Systemintegrator. Schon immer ging es darum das Business mit den richtigen Daten je nach Kritikalität hochverfügbar, sicher und ohne Datenverlust zu versorgen.

Er ist seit 2012 in der IT-Security branchenübergreifend tätig und als zertifizierter Security Officer und Lead Auditor für ISO27001, TISAX und KRITIS 2.0 dabei die Herausforderungen der Regulatorik und des Marktes (NIS2) in entsprechende IT-Security Konzepte zu übersetzen.

Nun ist er bei TEHTRIS als Head of Sales and Services endlich zu Hause angekommen und kann mit der TEHTRIS XDR-Lösung eine einzigartige All-In-One Lösung anbieten – ohne kleine Einzellösungen.

Carina Mitzschke: *Herr Müller-Haberland, von Ihrer Homepage habe ich die Aussage: „Wir tun alles, was wir können, um den Cyberspace zu einem sicheren Ort zu machen." Was genau kann TEHTRIS denn alles?*

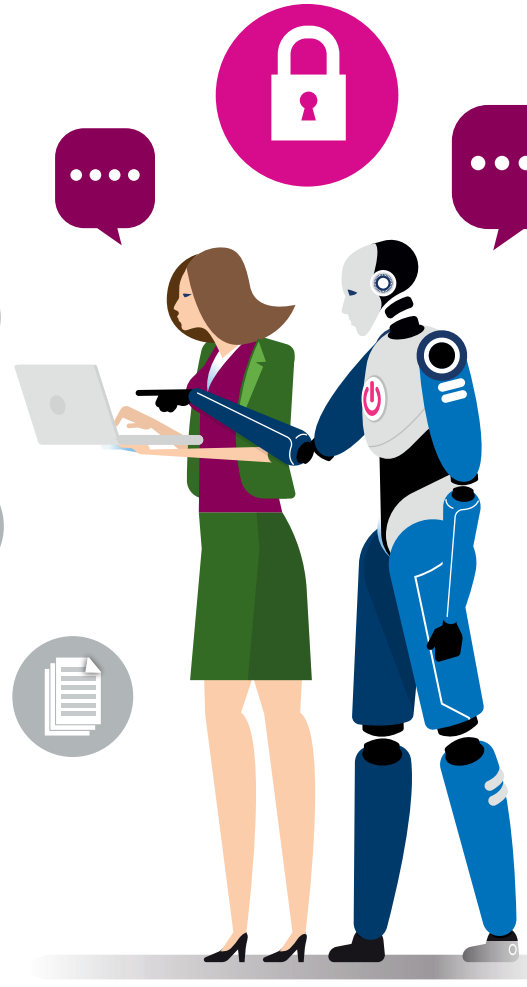
Olaf Müller-Haberland: Wir sind eine Europäische XDR-Lösung, von Europäischen Investmentfonds unterstützt und mit dem klaren Auftrag Europa zu schützen. TEHTRIS managt eine der größten CTI Datenbanken und Honeypot-Netzwerke weltweit und bieten den Unternehmen und Behörden Schutz gegen Spionage (Mitbewerb) oder Sabotage (Ransomware, ...).

Carina Mitzschke: *Sie bieten Ihren Kunden eine Security-All-in-One-Lösung an – was deckt diese Lösung alles ab und warum würden Sie diese unbedingt empfehlen?*

Olaf Müller-Haberland: Kein Security Spezialist allein oder ein komplettes SOC-Team ist heute oder auf Dauer in der Lage die verschiedensten Security-Lösungen (Firewall, AV, EDR, SIEM, NAC, ...) zu integrieren, zu pflegen und effektiv einzusetzen. Das kann nur mit einer All-in-One-Lösung in Verbindung mit Automatisierung erfolgreich funktionieren. In der TEHTRIS Plattform vereinen sich die einzelnen Technologien wie EDR, SIEM, NTA, MTD, Honeypots und ganz wichtig SOAR (Automatisierung).

Carina Mitzschke: *Wie integriert TEHTRIS verschiedene Sicherheitsdienste in ihre XDR-Plattform, um eine umfassende Sicherheitsabdeckung zu bieten?*

Olaf Müller-Haberland: Die passiven Sicherheitsdienste wie SIEM, NTA, Honeypots sammeln alle notwendigen Informationen/Alarme ein. In der XDR-Plattform in Verbindung mit der CTI werden diese korreliert. Über die SOAR-Schnittstelle werden die aktiven Sicherheitsdienste wie EDR, AV und Firewall genutzt, um zum Beispiel Prozesse zu stoppen, Files in Quarantäne zu schieben oder in der Firewall zu blocken mit dem Ziel der automatisierten Neutralisierung aller Arten von Attacken.



Carina Mitzschke: *Wie nutzt TEHTRIS künstliche Intelligenz und maschinelles Lernen in ihren EDR-Funktionen?*

Olaf Müller-Haberland: Unser Artificial Intelligence Modul nennt sich TEHTRIS CYBERIA. Dessen Ziel ist es, die Genauigkeit der Angriffserkennung zu erhöhen. Mit einer Analyse werden autonome und sofortige Abwehrmaßnahmen gestartet: Die defensive KI erkennt jegliche irregulären Aktivitäten, selbst wenn sie subtil sind, und blockt Angriffe. Über TEHTRIS SIEM wird eine massive Anzahl an Daten gesammelt, um Security-Maßnahmen zu ermöglichen und die Nutzer-Verhaltensanalyse zu verfeinern.

Das Thema künstliche Intelligenz im Bereich IT-Security wird in den nächsten Jahren auch noch spannend werden. Durch die Erweiterung und stetige Verbesserung von künstlichen Intelligenzen wird auch die Chance erhöht, dass KI-gestützte Cyberangriffe auf die Tagesordnung treten. Der Kampf KI gegen KI wird sich in der Tat um folgende Frage drehen: Welche KI verfügt über mehr Daten, um besser zu sein als die andere? Die CYBERIA-Module von TEHTRIS sind das Ergebnis von langjähriger Forschung und Entwicklung und basieren auf umfangreichen Datenbanken, die eine ständige Anpassung und Verbesserung ihrer Verwendung in den Produkten der TEHTRIS XDR-Plattform ermöglichen.

Carina Mitzschke: *Ein wichtiger Punkt beim Thema Security ist der zunehmende Personalmangel. Wie geht TEHTRIS mit dieser Problematik um?*

DIE TEHTRIS XDR-LÖSUNG BIETET UNSEREN KUNDEN EINE EINZIGARTIGE SECURITY ALL-IN-ONE LÖSUNG AN MIT DEM EINEN ZIEL: AUTOMATISIERT ANGRIFFE (SABOTAGE ODER SPIONAGE) ZU ERKENNEN UND IN REAL TIME ZU NEUTRALISIEREN!

Olaf Müller-Haberland, Head of Sales and Services DACH, Tehtris, www.tehtris.eu

Olaf Müller-Haberland: Der Personalmangel betrifft in unserer Branche alle, vom MSP zu SOC-Teams bis hin zu den IT-Abteilungen in den Unternehmen selbst. Um diesem entgegenzuwirken bedarf es einer sinnvollen Kombination aus zwei Dingen: Zum einen sollte ein höchstmöglicher Grad an Automatisierung erreicht werden – bei TEHTRIS funktioniert die Angriffserkennung und -Neutralisierung ohne menschliches Zutun – zum anderen ist es wichtig Personalressourcen übergreifend zu nutzen, zum Beispiel in dem Service-Komponenten effizient eingesetzt werden, oder indem man auf Managed Detection and Response (MDR) Services setzt.

Carina Mitzschke: *Welche spezifischen Funktionen bietet Ihre MDR-Dienstleistung, um Kunden bei der proaktiven Abwehr von Cyberangriffen zu unterstützen?*

Olaf Müller-Haberland: Der große Vorteil von MDR-Services ist es, dass der eigene Einsatz an Personalressourcen minimiert wird. Der Service-Anbieter managt und pflegt die XDR und EDR-Umgebungen, sodass ressourcenschonend die Sicherheit gewährleistet werden kann.

Unser Follow-The-Sun Modell ermöglicht eine 24/7 Security-Überwachung inklusive einer Echtzeit-Angriffserkennung, Investigation und Response ermöglicht. Unsere Teams in Bordeaux, Tokyo und Vancouver sind SOC-, Incident Repsonse- und Threat Research Analysten mit höchstem Expertenwissen.

Carina Mitzschke: *Um eine umfassendere Cybersicherheitsstrategie zu erreichen nutzen Sie eine Cyber Threat Intelligence Datenbank. Woher beziehen Sie die Daten und welche Vorteile oder Erkenntnisse erzielen Sie damit?*

Olaf Müller-Haberland: Unser Deceptive Response Modul und die Honeypots simulieren falsche Maschinen und Services, um Angreifer zu täuschen und Daten zu gewinnen. Durch strategisch aufgestellte Honeypots weltweit wissen wir genau, woher aktuell Angriffe kommen, wer die Akteure sind und welche Angriffsarten durchgeführt werden. Wöchentlich veröffentlichen wir einen Threat-Report zu unseren Honeypots, um mit TEHTRIS nicht nur vor bekannten, sondern auch vor unbekannten Bedrohungen zu schützen.

Carina Mitzschke: *Herr Müller-Haberland, wir danken für das Gespräch.*

THANK YOU

Cloud-Sandboxing

BEDROHUNGEN ERKENNEN, BEVOR DIESE INS NETZWERK GELANGEN

Cloud-Sandboxing fängt Schadcode vor dem Erreichen des Netzwerks ab. Experten empfehlen, eingehende Dateien frühzeitig in einer sogenannten Cloud Sandbox zu testen. Selbst unbekannte Bedrohungen, sogenannte Zero-Days, können so keinen Schaden an der eigenen Organisation anrichten. Auch im Hinblick auf die Erfüllung des „Stands der Technik" bei Cyberversicherungen und gesetzlichen Vorschriften ist der Einsatz solcher Technologien unverzichtbar.

Oftmals genügt ein unüberlegter Klick auf den E-Mail-Anhang, der eine Infektion des Netzwerks mit Ransomware oder anderer Malware auslöst. Die Hacker setzen alles daran, Malware zu tarnen und sie wie vertrauenswürdige Dateien aussehen zu lassen. Da kann man dem Mitarbeitenden in den meisten Fällen keine böse Absicht unterstellen.

CLOUD SANDBOXING STEIGERT DAS SICHERHEITSNIVEAU DER EIGENEN ORGANISATION DEUTLICH.

Michael Klatte,
Senior PR Manager,
ESET Deutschland GmbH,
www.eset.com

Potenzielle Bedrohungen in der Cloud prüfen

Klassische Sicherheitslösungen stoßen als stand-alone-Produkte bei neuartigen Gefahren an ihre Grenzen. Denn sie können „nur" anhand diverser Kriterien eine mögliche Bedrohung erkennen oder mit Heuristiken das Gefährdungsrisiko einschätzen. Vor diesem Hintergrund greifen immer mehr Organisationen auf die sogenannte Cloud-Sandbox-Analyse zurück. Denn: Die zu überprüfende Datei wird dabei tatsächlich in einer isolierten Testumgebung ausgeführt und man erkennt exakt, was sie tut. Somit kann man anhand der Untersuchung detaillierter entscheiden, ob es sich um einen gezielten Angriff - wie beispielsweise einen Advanced Persistent Threat (APT) - oder um eine ungefährliche Datei handelt. Gerade moderne Bedrohungen wie Ransomware und Zero-Days sind so komplex, dass sie von Endpoint-Lösungen nicht in angemessener Zeit enttarnt werden können. Dafür reicht meistens die Rechenleistung nicht aus. Renommierte Sicherheitshersteller erkennen in ihren Virenlaboren täglich mehr als 71.000 Ransomware-Angriffe – pro Stunde! In derselben Zeit kommen mehr als 50 neue und brandgefährliche Zero-Days hinzu.

Hohe Rechenpower der Cloud ausnutzen

Je nach Anbieter greifen Organisationen bei der Nutzung der Cloud auf eine enorme Rechenpower zurück, die mit der eigenen Infrastruktur nicht abbildbar wäre. Beispielsweise besitzt das Rechenzentren des Security-Spezialisten ESET die Power eines Supercomputers, den man sich wie einen Verbund von 16.000 aktuellen i7 CPUs vorstellen kann. Mit dieser Power im Rücken können sowohl physikalische als auch virtuelle Sandboxes zur Verfügung gestellt werden. Professionelle Malware ist in der Lage, virtuelle Testumgebungen zu erkennen und sich entsprechend „brav" zu verhalten. In der physikalischen Umgebung zeigt die potenzielle Bedrohung auf jeden Fall ihr wahres Gesicht. Je nach Größe und Umfang der zu untersuchenden Datei liegt das Ergebnis in Sekunden, maximal fünf Minuten bereit.

Umfassender Schutz mit Cloud Sandboxing

Die Analyse von ausführbaren Dateien in einer Cloud Sandbox bietet zusätzlichen Schutz vor einer Reihe an Bedrohungen wie Zero-Days, Advanced Persistent Threat (APT), Phishing per Dateianhang, Ransomware oder sonstiger Schadsoftware. Dabei spielt es keine Rolle, ob sie per USB, als E-Mail-Anhang oder per Download verbreitet werden. Vor allem schützt die Überprüfung in der Cloud die eigene Produktivumgebung vor Schäden und Betriebsausfällen. Denn Schadcode wird außerhalb der Organisation erkannt und bekämpft. Ebenso kommt dadurch das eigene Netzwerk mit der Bedrohung nicht in Kontakt.

Malware-Analyse mit System

Mit der Technologie findet Schadcode-Analyse in der Cloud statt. Sobald eine

Bild: ESET

verdächtige Datei auf dem Endpoint oder dem Mail-Server entdeckt wird, wird sie zur Analyse in ein Rechenzentrum weitergeleitet. In der dortigen Sandbox-Umgebung erfolgen in der Regel diese Schritte, um Malware zu erkennen:

#1 Ausführung in einer isolierten Umgebung:
Die verdächtige-Datei wird in einer vollständig isolierten Umgebung ausgeführt, in der es keinen Zugriff auf das Host-System oder andere Teile des Netzwerks gibt. Dadurch wird verhindert, dass sich die Malware verbreitet oder Schaden anrichtet.

#2 Überwachung der Aktivitäten:
Die Cloud Sandbox-Umgebung überwacht die Aktivitäten der Malware und zeichnet alle ausgeführten Prozesse, Dateizugriffe und Netzwerkverbindungen auf.

#3 Analyse des Verhaltens:
Anhand der aufgezeichneten Aktivitäten kann das Verhalten von Malware analysiert werden. Dazu gehört beispielsweise das Erstellen neuer Dateien oder Prozesse, der Zugriff auf sensible Daten oder das Senden von Daten an externe Server.

#4 Erkennung von Signaturen:
Die Malware kann auch anhand ihrer Signatur oder anderer bekannter Indikatoren erkannt werden. Dazu wird die Datei oder der Prozess mit einer Datenbank von bekannten Malware-Signaturen abgeglichen.

#5 Erkennung von Abweichungen:
Schließlich kann auch eine Abweichungsanalyse durchgeführt werden, um festzustellen, ob das Verhalten der Malware von der erwarteten Norm abweicht. Dadurch können auch neue oder bisher unbekannte Malware-Varianten erkannt werden.

Lautet das Ergebnis „sauber", kann die Datei aus der Sandbox heraus in die Produktionsumgebung freigegeben beziehungsweise in das Netzwerk zurückgespielt werden. Oder, je nach Einstellung, auch sofort isoliert oder beseitigt werden. Der gesamte Vorgang dauert nur wenige Augenblicke.

Cloud Sandboxing zählt zum Stand der Technik

Die Vorteile liegen auf der Hand: Es steigert, wie zuvor beschrieben, das Sicherheitsniveau der eigenen Organisation deutlich. Malware wird noch zuverlässiger erkannt und kommt zu keiner Zeit mit dem eigenen Netzwerk in Berührung. Die Auslagerung der Analyse schont die Performance der eigenen Hardware, weil sie keinen aufwändigen Malware-Scan vornehmen muss. Die softwaremäßige Einrichtung von Cloud Sandboxing ist schnell gemacht und erfordert keine zusätzlichen Ressourcen. Mehr Sicherheit plus Datenschutz: Eini-

ge Anbieter besitzen eigene Rechenzentren in der EU und achten penibel darauf, welche Daten zur Analyse eingereicht werden. Somit ist die Einhaltung von DSGVO garantiert. Auch die im Artikel 32 geforderte „Berücksichtigung des Stands der Technik" ist eingehalten. Gerade hier wachsen die Anforderungen für Organisationen, um diesem Stand gerecht zu werden.

Stand der Technik

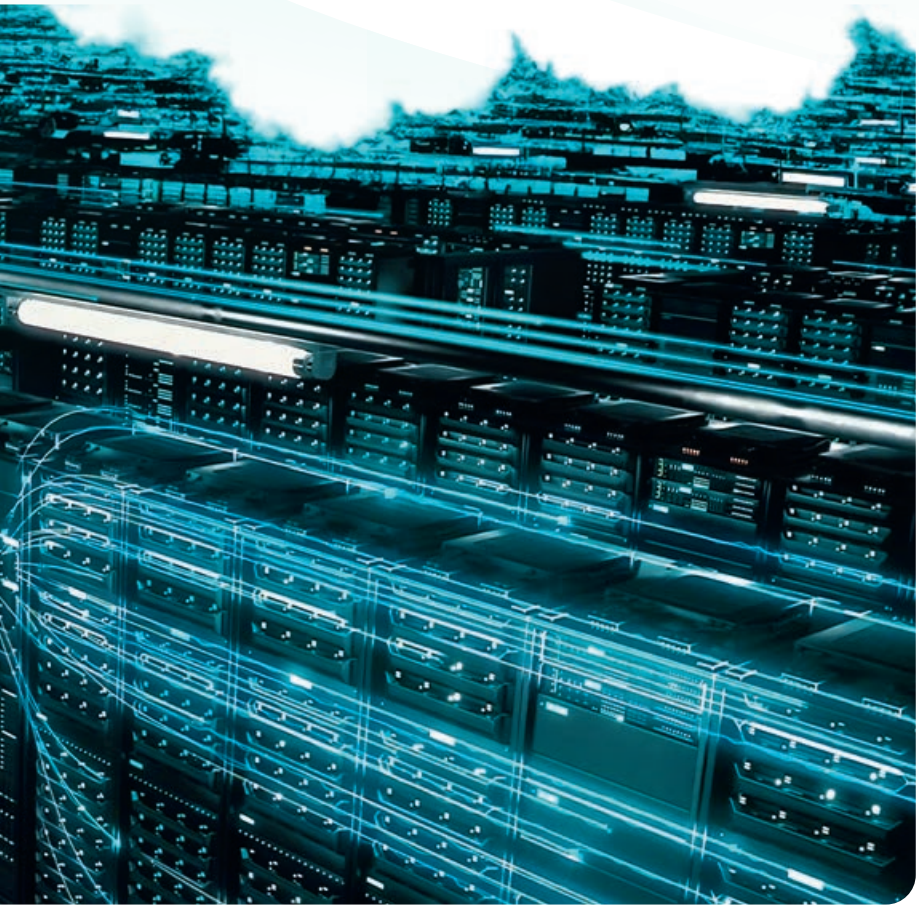
Auf den ersten Blick erscheint der Begriff „Stand der Technik" absolut verständlich. Kunden verwenden ihn oft als Synonym für den aktuellen Entwicklungsstand von Technologien, Produkten oder Dienstleistungen. Insbesondere in der sensiblen IT-Sicherheitsbranche gehört mehr dazu, als nur die Bedürfnisse und Anforderungen der Verbraucher zu erfüllen. Denn der Stand der Technik wird bereits vielfach in Vorschriften, Gesetzen und selbst in den Vertragsbedingungen von Cyberversicherungen genutzt. Damit hat der Begriff direkten Einfluss nicht nur auf Kritische Infrastrukturen, sondern letztlich sogar auf fast jede Organisation. Offensichtlich ist dies noch längst nicht jedem Verantwortlichen geläufig. In einer aktuellen Umfrage von ESET zeigte sich, dass lediglich 37 Prozent der Befragten glaubten, den Stand der Technik in der IT-Security richtig definieren zu können. Ein Trugschluss, wie die dazu gewählte Kontrollfrage bewies: Nur etwas mehr als die Hälfte von ihnen lag tatsächlich korrekt. Dieses Ergebnis zeigt eindeutig, dass noch viel Aufklärungsarbeit zu leisten ist.

Von der Theorie zur Praxis

Vor diesem Hintergrund stellt sich generell die Frage, welche Anforderungen an die IT-Sicherheit auf Unternehmen zukommen und wie angemessene Maßnahmen aussehen könnten. Denn ein unbestimmter Rechtsbegriff hilft Entscheidern wenig, wenn sie die praktische Umsetzung der eigenen Security vorantreiben möchten. Es gilt also immer, die eigene individuelle Situation exakt zu betrachten. Erst anhand einer Risikoanalyse kann man bestimmen, welche technischen Maßnahmen ein „angemessenes Schutzniveau" überhaupt versprechen.

Inzwischen besteht ein gewisser Common Sense, was für jeden umsetzbar, bezahlbar und leistbar ist. Dazu zählt für Unternehmensrechner beispielsweise der sogenannte Multi Secured Endpoint, der sich für jede Organisationsgröße in Anbetracht der aktuellen Bedrohungslage und der aktuellen Datenschutzgesetze eignet. Dieser Basisschutz erfordert auf jedem PC Malwareschutz, Datenträgerverschlüsselung, Multi-Faktor-Authentifizierung und wie bereits oben beschrieben Cloud Sandboxing. Auf dem Markt gibt es eine Vielzahl dedizierter technologischer Lösungen und Services, die von Experten bereitgestellt werden. Zudem beraten externe Dienstleister und Security-Hersteller mit ihrer Expertise Organisationen umfassend bei der Einhaltung des Stands der Technik. Auch vermittelt das Whitepaper „IT-Security auf dem Stand der Technik" kompakt, was sich hinter dem vermeintlich einfachen Begriff versteckt und welche direkten Auswirkungen er auf die Gestaltung der eigenen Security von Unternehmen und Organisationen hat.

Michael Klatte



+PLUS

Kostenloser Whitepaper Download „IT-Security auf dem Stand der Technik **www.eset.com/de/stand-der-technik/**

Verschlüsselter Datentransfer

SICHER IN DER DIGITALEN WELT

In Zeiten wachsender Cyberbedrohungen gewinnt die Sicherheit von Daten und Systemen zunehmend an Bedeutung. Doch während Unternehmen immer besser darin werden, Daten „at rest" zu schützen, vernachlässigen viele den Schutz der Daten beim Transfer.

Dabei kann der Verlust von Daten weitreichende Folgen für Unternehmen haben: von sensiblen Geldstrafen bei Verstößen gegen die EU-DSGVO über Imageschäden bis hin zur Bedrohung der Unternehmensexistenz.

Laut FTAPI Secure Data Report zögern Unternehmen beim Einsatz von Lösungen zum verschlüsselten Datentransfer aus zwei Gründen: Zu hohe Kosten und eine zu hohe Komplexität – sowohl bei der Implementierung, als auch bei der tatsächlichen Nutzung.

Dabei muss ein sicherer Datentransfer nicht kompliziert sein. Um von Mitarbeitenden wirklich angenommen zu werden, sollten sich Lösungen nahtlos in den Arbeitsalltag integrieren lassen, um auch verschlüsselte E-Mails direkt aus dem Outlook heraus zu versenden.

Nach Einschätzung von FTAPI sollten Lösungen zum verschlüsselten Datentransfer folgende Kriterien erfüllen:

- **State-of-the-Art-Verschlüsselung:** Eine durchgängige Ende-zu-Ende-Verschlüsselung verhindert effizient ein ungewolltes Abfließen von Informationen.
- **Serverstandort Deutschland:** Um den Richtlinien der EU-DSGVO zu entsprechen, sollten Unternehmen auf Dienstleister setzen, die ihre Rechenzentren in Deutschland oder der EU hosten und betreiben.
- **Benutzerfreundlichkeit:** Eine benutzerfreundliche Oberfläche und intuitive Funktionen sind für eine reibungslose Nutzung der Software essenziell.

Lösungen für einen sicheren Datenaustausch sind unerlässlich, um den Schutz sensibler Daten zu gewährleisten und den Bedrohungen einer vernetzten Welt erfolgreich zu begegnen.

www.ftapi.com

it-sa 2023

Besuchen Sie uns
in **Halle 7, Stand 543**

IT SECURITY MANAGEN

SICHER IST SICHER

IT Security managen
Klaus Schmidt,
Carl Hanser Verlag GmbH
& Co.KG, 11-2023

IT-Sicherheit ist weit mehr als nur der Einsatz technischer Sicherheitsmaßnahmen wie Firewalls oder Virenschutz. Eine beständige und wirtschaftliche Sicherheit für Ihre IT erreichen Sie nur, wenn Sie die IT-Risiken kontinuierlich managen und die IT-Sicherheit ganzheitlich betrachten, wozu neben der physischen und technischen Situation auch die Einbeziehung von personellen und organisatorischen Faktoren gehören.

Dieses Praxishandbuch geht nicht nur auf die Methodik des IT Security Managements ein, so wie dies viele andere Bücher tun, sondern widmet sich vor allem den Dingen dahinter, zum Beispiel unternehmenspolitischen Einflüssen, organisatorischen Fragestellungen oder taktischen Überlegungen. Damit beschäftigt es sich mit den Managementaspekten, mit denen Sie in der Verantwortung für das IT Security Management in Ihrer täglichen Arbeit konfrontiert werden und geht auf die Aspekte ein, die Sie berücksichtigen müssen, um in Ihrer Tätigkeit erfolgreich zu sein.

Dieses Buch beinhaltet:

- Die Basis für Ihren Erfolg in der Verantwortung für das IT Security Management
- Einführung in die wichtigen Themen des IT Security Managements
- Hilfe für die vielfältigen Anforderungen in der Praxis

Zero Trust für IT- und OT-Netzwerke

EINFACHE, NAHTLOSE, SICHERE UND ZUVERLÄSSIGE VERBINDUNG

Durch die zunehmende und universelle Digitalisierung sind auch Produktions-Netzwerke in den Fokus von Cyberkriminellen gerückt. Umfassende Netzwerksicherheit ist unabdingbar, um Risikofaktoren zu reduzieren und bei einer erfolgten Attacke den Schaden für das Unternehmen möglichst gering zu halten. Christian Bücker, Business Director bei macmon, erläutert im Interview wie sich sein Unternehmen in diesem dynamischen Umfeld positioniert.

it security: *Belden entwickelt sich vom Produkt- zu einem Lösung-Anbieter, was bedeutet das für den Bereich IT-Security-Lösungen zu denen macmon gehört?*

Christian Bücker: Belden wird von seinen Kunden für die innovativen und zugleich zuverlässigen Hardware-Kommunikationsprodukte sehr geschätzt. macmon secure hat sich in den 20 Jahren seines Bestehens ebenfalls einen erstklassigen Ruf als ein führender Anbieter für IT-Security-Lösungen erarbeitet. Wir fokussieren uns jetzt gemeinsam auf Lösungen, die sowohl Hardware-Komponenten, wie beispielsweise die Hirschmann switche, und unsere NAC-Lösung verknüpfen. Security ist ein wichtiger strategischer Wachstumsmarkt, und mit macmon NAC für on-premises Netzwerke und macmon SDP für Cloud-Lösungen, können wir auch im OT-Bereich ein zentrales Angebot für die Abwehr von Cyberattacken bieten.

it security: *Was sind hier die besonderen Herausforderungen?*

Christian Bücker: Vieles ist in Unternehmen im Umbruch: Hybride Arbeitsmodelle, Stichwort „New Work", die Digitalisierung von Geschäftsprozessen, das Zusammenwachsen von IT- und OT-Netzwerken, Fachkräftemangel in der IT-Abteilung, Outsourcing an MSP-Anbieter – diese Rahmenbedingungen führen zu einer erhöhten Vulnerabilität. Kein Wunder, dass die Zahl der Cyberattacken kontinuierlich steigt. Laut verschiedenen Quellen wird der globale Schaden durch Cyberkriminalität bis 2025 10,5 Billionen US-Dollar pro Jahr betragen. Das entspricht etwa dem drittgrößten Bruttoinlandsprodukt der Welt, nach den USA und China.

Unsere Antwort: Mit der Software-Plattform Belden Horizon bieten wir eine sichere und zuverlässige Verbindung zu OT-Netzwerken. Die Edge-Orchestrierungsfunktionen der Plattform ermöglichen es den Anwendern, Anwendungen auf einem oder mehreren Geräten gleichzeitig zu implementieren und zu verwalten – lokal oder remote. Die Secure Remote Access (SRA)-Technologie sorgt für sichere Verbindungen über Mobilfunk oder Kabel. Außerdem unterstützt die Plattform über die PDN-Anwendung (Persistent Data Network) die ständige Konnektivität zu geografisch verteilten Anlagen.

it security: *IT-Sicherheit ist ein globales Thema – wie sehen hier ihre Aktivitäten international aus?*

Christian Bücker: Belden hat Kunden aus unterschiedlichen Branchen, in denen spezielle und hochverfügbare Produkte erforderlich sind. Die Anwendungen reichen von der Industrieautomatisierung über Rechenzentren und Rund-

DEN „NO TRUST" ANSATZ TRANSFERIEREN WIR JETZT VON DER IT- IN DIE OT-WELT, UND ZEIGEN DIE VIELFÄLTIGEN EINSATZMÖGLICHKEITEN AN UNSEREM IT-SA STAND.

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

it-sa 2023
Besuchen Sie uns:
Halle 7, Stand 7-223

Auf dem macmon Stand 7-223 freuen sich Experten von macmon secure, Belden und von Systemhaus-Partnern wieder auf viele anregende Gespräche rund um IT- und OT-Sicherheit.

funkstudios bis hin zur Luft- und Raumfahrt. Im Segment Network Solutions bietet Belden Produkte und Lösungen für die Netzwerk-Infrastruktur, die Cyber-Sicherheit, die industrielle Ethernet-Kommunikation und das Internet der Dinge. Hier bestehen viele gemeinsame Ansatzpunkte für einen Lösungs-Vertrieb. Durch kontinuierliche Schulung des Vertriebsteams in beide Richtungen entwickeln wir das Verständnis für Synergien und Einsatzmöglichkeiten. Erste Großprojekte für ein indisches Bahnunternehmen oder einen amerikanischen Automobilhersteller sind bereits in der Umsetzung.

it security: *macmon secure ist auf der it-sa mit einem eigenen Stand vertreten. Was sind die inhaltlichen Schwerpunkte?*

Christian Bücker: Unser übergeordnetes Thema ist Zero Trust. Auf Basis unserer Netzwerksicherheitslösung macmon NAC haben wir macmon SDP entwickelt und bereits 2021 gelauncht. Der macmon SDP-Agent übernimmt transparent eine hochsichere Authentifizierung um die Identität des Benutzers sowie des Gerätes und dessen Sicherheitszustand zu prüfen. Die macmon SDP Suite kann die Ressourcen in drei Kernfunktionen – im lokalen Netzwerk, in der privaten und in der Public Cloud – steuern. Diesen „no trust" Ansatz transferieren wir jetzt von der IT- in die OT-Welt, und zeigen die vielfältigen Einsatzmöglichkeiten an unserem Stand.

it security: *Wie entwickelt sich macmon NAC weiter?*

Christian Bücker: Die Version macmon 5.35.0 ist ab sofort verfügbar und beinhaltet viele bedeutsame Features, so können beispielsweise unbekannte Endgeräte automatisch auf Basis eines Advanced-Security-Scans in Endgerätegruppen gelernt werden. Des Weiteren ist eine 802.1X-Authentifizierung mit mehr als einem Active Directory möglich. Die Schnellsuche (Quick Search) wurde überarbeitet und steht jetzt in neuem Umfang und Design zur Verfügung.

Der Fokus unseres Berliner Entwicklerteams liegt auf der kontinuierlichen Weiterentwicklung von macmon NAC und macmon SDP. Die Kollegen sitzen Tür an Tür mit dem Support und unseren Consultants. Der fachliche Austausch sorgt immer wieder für die Integration von Kundenanforderungen in neue Versionen. Natürlich haben wir auch neue Sicherheitsanforderungen durch den Einsatz von KI-Technologien im Fokus. Gleichzeitig wollen wir verstärkt Produktintegrationen durch unsere Technologie-Partner durch plug-ins realisieren. Die macmon REST API bildet dabei die Verbindung zu bestehenden und zukünftigen Softwarelösungen, damit Kunden macmon NAC als zentrale Sicherheits-Macht im Netzwerk auch in Zukunft in vollem Maße nutzen können.

it security: *Herr Bücker, wir danken für dieses Gespräch.*

APPLE GERÄTESICHERHEIT FÜR BEGINNER

GRUNDLAGEN UND AUFFRISCHUNG

WHITEPAPER DOWNLOAD

Das Whitepaper umfasst 32 Seiten und steht zum kostenlosen Download bereit.
www.it-daily.net/Download

Ein gut geplanter Cyberangriff oder ein versehentlicher Download von Malware kann dafür sorgen, dass Ihre Arbeit lahmgelegt wird, wo Sie doch so produktiv hätten sein können. Da die Hacker immer geschickter vorgehen, müssen Unternehmen, die sich um ihren Gewinn und die Sicherheit der Daten ihrer Nutzer, wie Kunden, Mitarbeiter oder Studenten, sorgen, immer auf dem neuesten Stand der Sicherheit bleiben.

Apple Sicherheitsbedenken sind, wie alle IT-Sicherheitsbedenken, sehr real und stellen eine kritische Bedrohung für die Unternehmensressourcen und die Sicherheit der Beteiligten dar.

Apple stellt unglaublich sichere Betriebssysteme her. Es besteht kein Zweifel daran, dass die Konzentration auf die Sicherheit und den Schutz der Privatsphäre, die in die Hardware und Software integriert sind, eine wichtige Rolle bei der steigenden Beliebtheit und der massenhaften Akzeptanz in Unternehmen, Bildungseinrichtungen und anderen Branchenorganisationen gespielt hat. Und da Apple nach wie vor die bevorzugte Plattform für private und professionelle Hardware ist, ist sie ein attraktives Ziel für Angreifer geworden. Dies bedeutet, dass Administratoren schnell auf Sicherheitsvorfälle reagieren müssen, sobald sie auftreten, und nicht warten dürfen, bis ein Problem auftritt. Stattdessen sind MacAdmins und Sicherheitsteams (und die von ihnen unterstützten Interessengruppen) besser beraten, sich proaktiv vor diesen Bedrohungen zu schützen, bevor sie sich zu etwas weitaus Schlimmerem entwickeln können, indem sie auf Apple zugeschnittene oder speziell für Apple entwickelte Lösungen einsetzen, um sich effektiv vor Apple zentrierten Bedrohungen zu schützen.

Dieser Leitfaden richtet sich an Administratoren und Manager, die sich ernsthaft mit der organisatorischen Sicherheit ihrer Apple Geräte befassen wollen, und bietet grundlegende Informationen für Neulinge oder auch eine einfache Auffrischung für Apple Management-Veteranen.

it-sa 2023
Besuchen Sie uns
in **Halle 7, Stand 323**

E-Mail-Sicherheit ist nicht schwer!

DIE EIGENE PERSON SCHÜTZEN DANK DIGITALER SIGNATUR

Sie schalten den Rechner an, öffnen Ihr E-Mail-Programm und haben jede Menge E-Mails im Posteingang. Denn nach wie vor wird die E-Mail als Hauptkommunikationsmittel benutzt, nicht nur im beruflichen Kontext, sondern auch im Alltag. Doch wie können Sie sich sicher sein, dass die E-Mail auch wirklich von dem angezeigten Absender stammt und nicht von einem Hacker? Die Lösung lautet: digitale E-Mail-Signatur!

Cyberangriffe auf E-Mails nehmen weiter zu und werden mit jedem Mal professioneller. Eine echte E-Mail von einer Phishing-Mail zu unterscheiden, wird immer schwieriger. Wenn die E-Mail dann noch von einer bekannten Person kommt, aber auf dem Versandweg manipuliert werden könnte, ist es nahezu unmöglich, sich sicher zu sein. Doch es gibt Möglichkeiten, seine E-Mail zu schützen, die gar nicht kompliziert und mühselig sind; beispielsweise mit einer E-Mail-Verschlüsselung und digitalen Signatur von SEPPmail. Häufig wird angenommen, dass das Einrichten einer solchen Lösung mit viel Aufwand sowie Kosten verbunden ist. Allerdings ist genau das Gegenteil der Fall. Schon mit wenigen Schritten lässt sich die E-Mail-Kommunikation absichern.

Schutz der Identität

Es gibt verschiedene Schutzmaßnahmen, die die E-Mail-Kommunikation absichern können. SEPPmail bietet Standard-Technologien wie S/MIME- oder openPGP-Verschlüsselung, mit denen sich gewährleisten lässt, dass Daten auf dem Weg vom Absender bis zum Empfänger zu keinem Zeitpunkt unverschlüsselt sind und durch Dritte mitgelesen werden können. Auch eine spontane E-Mail-Kommunikation zu unbekanntem Empfänger ist mittels der von SEPPmail entwickelten GINA-Technologie möglich.

Ein Verfahren, das immer häufiger in Unternehmen implementiert wird, ist die digitale Signatur. Sie ist ein wichtiger Zusatz, um die E-Mail-Sicherheit im Unternehmen zu erhöhen. Digitale Signaturen beweisen die Identität des Unterzeichners und Absenders und stellen damit die Authentizität sowie die Integrität der E-Mail sicher. Ist eine Mail mit einer digitalen Signatur versehen und kommt diese unversehrt beim Empfänger an, kann dieser sicher sein, dass die Mail, Links oder Anhänge auch wirklich von dem Absender stammen. Das Einbinden einer digitalen Signatur ist mit nur minimalem Aufwand verbunden. Es wird ein validiertes Zertifikat benötigt, das bei einer akkreditierten Zertifizierungsstelle bzw. bei Certificate Authorities (CAs) ausgestellt wird. Diese CAs können nachweisen, dass das Zertifikat sowie das darin enthaltene Schlüsselpaar zu einem konkreten Absender bzw. einer E-Mail-Adresse gehört. Die SEPPmail-Appliance übernimmt diesen Prozess für den Nutzer automatisch – beim ersten Versand einer E-Mail starten die Schritte ohne weiteres Zutun.

E-Mail-Sicherheit kann jeder!

E-Mail-Sicherheit spielt in Unternehmen nach wie vor eine große und wichtige Rolle. Um die E-Mail-Kommunikation sicher zu gestalten, gibt es verschiedene Optionen. Eine moderne All-in-one-Lösung, die sowohl digitale Signaturen als auch E-Mail-Verschlüsselung beinhaltet, ist eine gute Möglichkeit, die Sicherheit in jedem Unternehmen zu optimieren und Cyberattacken zu verhindern. Die durchzuführenden Maßnahmen sind dabei einfach umsetzbar und mit wenig Aufwand sowie Kosten verbunden. Läuft die Lösung zudem im Hintergrund, können die Mitarbeiter ihren Aufgaben ganz normal nachgehen und werden nicht im Arbeitsalltag behindert.

www.seppmail.de

SEPPMAIL

Passwortlose Zukunft

NÄHER ALS GEDACHT?

Zusätzliche Authentifizierungsmethoden und Sicherheitskontrollen, die Passwörter in den Hintergrund drängen, verändern die Art und Weise, wie Identitäten überprüft und nachgewiesen werden. Dabei spielen vor allem passwortlose Methoden eine wichtige Rolle. Dies ist das Ergebnis einer Umfrage von Delinea auf der diesjährigen BlackHat USA Conference in Las Vegas. So sind 79 Prozent der 100 befragten Security- und IT-Professionals der Meinung, dass sich Passwörter zukünftig weiterentwickeln oder sogar überflüssig werden.

Um ihre Anmeldedaten und Identitäten angemessen zu schützen, setzt die Mehrheit der befragten Teilnehmer auf zusätzliche Authentifizierungsmethoden. Dabei kommen überwiegend Formen der Multi-Faktor-Authentifizierung (MFA) zum Einsatz (73 Prozent), gefolgt von Authentifizierungs-Apps und biometrischen Verfahren. Jeder Fünfte gab außerdem an, anstelle von oder zusätzlich zu Passwörtern jetzt auch Passkeys zu verwenden.

„Die Umfrageergebnisse machen deutlich, dass der Großteil der Menschen mittlerweile verstanden hat, was passwortlos tatsächlich bedeutet, und nicht nur mit dem Marketingbegriff hantiert. Endlich ist klar, dass es darum geht, Passwörter in den Hintergrund zu rücken und stattdessen einfachere zusätzliche Formen der Authentifizierung zu verwenden", so Joseph Carson, Chief Security Scientist und Advisory CISO bei Delinea. „Dazu passt auch, dass sich 75 Prozent der Befragten bewusst sind, dass der schnellste Weg, sich Zugang zu einem Netzwerk zu verschaffen, über Social Engineering und gestohlene Identitäten und Passwörter führt. Je schneller Unternehmen und Endanwender ihre Identitäts- und Zugriffssicherheit über Passwörter hinaus weiterentwickeln, desto sicherer werden wir als Gesellschaft sein."

Unternehmen können mit Cyberkriminellen nicht mithalten

Im Rahmen der Umfrage wurden die Teilnehmer zudem nach ihrer Meinung zum laufenden Cyberkrieg und der Verteidigungslage der Unternehmen befragt. Der Großteil der Befragten sieht Nationalstaaten und Cyberkriminelle hier klar in der Führungsrolle. Nur 12 Prozent der Befragten glauben demnach, dass Unternehmen den Staaten und Kriminellen im Cyberkrieg derzeit voraus sind.

KI-Programme sind noch nicht ausgreift

Ferner beleuchtet Delinea in der Umfrage auch das aktuelle Thema künstliche Intelligenz und wollte von den Teilnehmern wissen, wie sie die Ausgereiftheit von beziehungsweise die Bedrohungen durch KI-Programme einschätzen. 34 Prozent der Befragten gaben an, dass sich die künstliche Intelligenz noch in einer frühen Phase befindet und die aktuellen Versionen noch nicht wirklich KI sind, während 22 Prozent davon ausgehen, dass eine Übernahme durch KI bereits bevorsteht. Nur eine kleine Minderheit von 11 Prozent zeigten sich dabei zuversichtlich, dass KI niemals die Macht übernehmen wird.

www.delinea.com/de

Quantenresistente Kryptografie

IT-SICHERHEIT FÜR DIE POST-QUANTUM-WELT

Quantencomputing wird in einigen Jahren die Leistung klassischer Computer potenzieren – und die auf Verschlüsselung basierenden kryptografischen Schutzmaßnahmen gegen Cyberangriffe außer Gefecht setzen. Daher wird eine Umstellung auf quantenresistente Kryptografie notwendig, die sogenannte Post-Quantum-Kryptografie. Da es sich hierbei um einen langwierigen Prozess handelt, sollten die Vorbereitungen jetzt beginnen.

Unternehmen, die ihre Sicherheitsinfrastruktur bereits im Vorfeld auf Post-Quantum-fähige Verschlüsselungssysteme umstellen, sind für künftig notwendige Aktualisierungen bestmöglich gerüstet. Hersteller im Bereich IT-Sicherheit und Verschlüsselung arbeiten mit Hochdruck an möglichen Lösungen, um ihre Kunden auf die Post-Quantum-Bedrohungen vorzubereiten. Einige bieten in ihren Produkten einen frühen Zugang zu quantensicherer Kryptografie an. Entrust etablierte zu diesem Zweck darüber hinaus ein eigenes Cryptographic Center of Excellence – ein Expertenteam, das Unternehmen dabei hilft, Risiken zu identifizieren und Krypto-Strategien für eine erhöhte digitale Sicherheit zu etablieren. Das Cryptographic Center of Excellence geht über rein technologische Ansätze hinaus und stellt eine zentrale Anlaufstelle für alle Krypto- und PKI-Angelegenheiten dar. Hier geht es neben zukunftssicheren Technologien auch um die beratende Begleitung von Projekten und Teams, um Unterstützung bei der Einhaltung von Richtlinien und um die Beantwortung von Fragen hinsichtlich Konvergenz und Management von Krypto, Schlüsseln, Unternehmensgeheimnissen und Zertifikaten.

Es ist noch etwas Zeit, um Vorbereitungen für das Post-Quantum-Zeitalter zu treffen – aber nicht genügend, um das Thema hintanzustellen. Da die Umstellung auf quantensichere Algorithmen mehrere Jahre dauern kann, sollte insbesondere in Branchen mit hohen Datenschutz- und Compliance-Verpflichtungen umgehend damit begonnen werden.

www.Entrust.com

it-daily.net mehr als nur tägliche IT-News!

Ob News und Fachartikel aus dem IT Security- oder dem IT Management-Bereich, Veranstaltungshinweise oder Whitepaper- und eBook-Empfehlungen – **seien Sie immer TOP informiert!**

Zum Newsletter anmelden,

Mousepad **GRATIS** erhalten!

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

Code Intelligence

WIE KI DIE APPLICATION SECURITY NEU DEFINIERT

Da Softwaresysteme immer größer, komplexer und vernetzter werden, entwickelt sich die Bedrohungslandschaft ständig weiter. Vielen Softwaretestverfahren und -tools sind nicht dazu geeignet, mit dieser Entwicklung Schritt zu halten, da vor allem auf Compliance ausgerichtete Sicherheitsbemühungen nur selten die tägliche Realität von Entwicklern berücksichtigt. Dadurch werden Softwaresysteme anfällig für potenziell katastrophale Sicherheitslücken wie log4shell.

KI-gestützte Softwaretests sorgen also für einen Wandel. Nachfolgend erklären wir, warum der Aufstieg von KI-gestützten Testtools den kulturellen und verfahrenstechnischen Wandel einleitet, den wir so dringend brauchen, um sichere Anwendungen inmitten wachsender Komplexität zu entwickeln.

Application Security muss Schritt halten

50 Prozent der Unternehmen erlebten im vergangenen Jahr einen API-Sicherheitsvorfall (Google Cloud, 2022). Dies ist nicht überraschend: Während Softwaresysteme immer größer und vernetzter werden, verwenden viele Branchen immer noch Softwaretestverfahren und -tools, die für die Bewältigung dieser Herausforderungen, unzureichend sind.

In vielen Branchen, wie etwa im Finanzwesen, im Gesundheitswesen und in Behörden, werden Sicherheitsbemühungen durch Compliance bestimmt. Dies kann zwar ein wirksames Instrument sein, um sicherzustellen, dass Testing auf Managementebene berücksichtigt wird, reicht aber nicht aus, um der heutigen Bedrohungslandschaft zu begegnen.

Compliance-basierte Security besteht zu großen Teilen aus maximal halb automatisierten Pentests, welche viele Nachteile haben:

- Unschlüssige Ergebnisse aufgrund mangelnder Messungen der Code Coverage
- Probleme werden erst spät gefunden, da die Tests nicht für jedes Deployment durchgeführt werden
- Tests kratzen aufgrund strikter Zeitvorgaben nur an der Oberfläche
- Tests sind angesichts ihres suboptimalen ROI übermäßig teuer

Da bei diesem Ansatz die Code Coverage fehlt, werden die Tester mit den Angreifern gleichgesetzt, da sie keine Möglichkeit haben, festzustellen, welche Teile des Quellcodes von ihren Eingaben durchquert wurden. Da Angreifer oft nicht an Zeitvorgaben gebunden sind, könnte man sogar argumentieren, dass sie einen Vorteil haben. Dennoch sind Blackbox-Pentests aus Compliance-Sicht oft ausreichend.

Wie KI-gestützte Softwaretests einen Vorsprung ermöglichen

Mithilfe von KI können große Teile der Testfallerstellung automatisiert werden. Herkömmliche Testmethoden (etwa klassische Unit-Tests) verwenden wenige deterministische Testfälle, um auf Known-Uknowns zu testen, also einen Programmzustand, den der Tester als fehlerhaft vermutet. Durch die Erweiterung dieses Ansatzes mit selbstlernender KI können Entwickler jede Sekunde Tausende von zusätzlichen Testfällen generieren, um auf Unknown-Unknowns zu testen, das heißt, auf Fehler und Si-

cherheitsprobleme, an die menschliche Intelligenz nie gedacht hätte.

Durch den Einsatz genetischer Algorithmen können KI-gestützte White-Box-Tests Informationen über frühere Testläufe sammeln, die sie dann zur automatischen Generierung neuer Testeingaben nutzen können, um tiefer in den Quellcode einzudringen. Auf diese Weise erhalten die Entwickler vollen Einblick in die Code Coverage ihrer Tests und können tief verborgene Fehler und Sicherheitslücken aufdecken, die mit herkömmlichen Testtools nicht zu finden sind. Die Nutzung des Quellcodes auf diese Weise ist vergleichbar mit einem Labyrinth, bei dem man die Wege vollständig überblicken kann. Während ein Black-Box-Test dem Versuch entspräche, einen Pfad zu finden, der rein zufällig zu einem Fehler führt, decken KI-gestützte White-Box-Tests einfach alle Pfade ab.

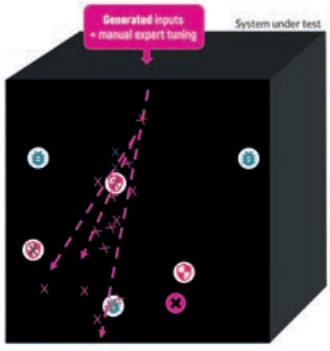


Bild 1 (schwarze Box): So arbeiten herkömmliche Black-Box Tools.

Bild 2 (blaue Box): Und so KI-gestützte White-Box Tools

Wie KI die Sicherheitsprozesse und -kultur verändert

KI-gestützte Testtools ermöglichen es Entwicklern, die Sicherheit ihres Codes in die eigene Hand zu nehmen. Durch CI/CD-Integration können Entwickler ihren Code unabhängig auf tief verborgene Sicherheits- und Qualitätsprobleme testen. Diese Form der Testautomatisierung hat enorme kulturelle Auswirkungen, da sie tiefgehende Tests in jedes einzelne Pull Request einführt, beginnend in den frühen Phasen des SDLC.

Ein wichtiger Punkt bei dieser Vorgehensweise ist die Frage, ob es sinnvoll ist, Entwickler die Verantwortung für das Testen zu übertragen oder nicht. Sind sie nicht ohnehin schon genug beschäftigt? Schließlich sollten KI-gestützte Testwerkzeuge nicht zu einer erhöhten Arbeitsbelastung für Entwickler führen. Genau aus diesem Grund ist es wichtig, dass KI-Testing-Tools automatisiert und in CI/CD-Prozesse integriert sind, damit sie nahtlos im Hintergrund laufen können. Entwickler können sich dann auf die Interpretation der Testergebnisse und die Behebung der Fehler konzentrieren. Auf diese Weise können automatisierte Testwerkzeuge den Entwicklungsprozess beschleunigen, indem sie es ermöglichen, versteckte Fehler und Schwachstellen zu finden und zu beheben, bevor sie in die Codebasis gelangen.

Wer wird durch KI ersetzt?

Es ist nicht zu erwarten, dass KI-fähige Testtools in naher Zukunft Menschen ersetzen werden; sie werden sie vielmehr in die Lage versetzen, nicht nur besseren, sondern auch sichereren Code zu produzieren. Selbst für Sicherheitsexperten wird der Aufstieg automatisierter Testtools nicht zu einem Ersatz führen, da die Sicherheit in der heutigen Landschaft immer wichtiger wird. Vielmehr werden automatisierte Sicherheitstools es Sicherheitsexperten er-

DAS AUFKOMMEN VON KI-GESTÜTZTEN TEST-TOOLS VERSPRICHT ENORME AUSWIRKUNGEN AUF DIE ART UND WEISE, WIE WIR SOFTWARE ENTWICKELN, TESTEN UND SICHERN,

Sergej Dechand, CEO und Co-Founder, Code Intelligence, www.code-intelligence.com

möglichen, sich auf Bereiche zu fokussieren, die menschliches Fachwissen und kritisches Denken erfordern, wie etwa die Entwicklung robusterer Sicherheitsarchitekturen.

KI wird Software robuster machen

Letztendlich verspricht das Aufkommen von KI-gestützten Testtools enorme Auswirkungen auf die Art und Weise, wie wir Software entwickeln, testen und sichern, sowie auf unsere Vorstellung davon, wie Tests durchgeführt werden sollten.

Langfristig könnte der Mensch in der Application Security überflüssig werden – oder auch nicht. Wer weiß das schon. Vorerst wird die Rolle der KI in der Sicherheit darin bestehen, Fehler an Stellen zu finden, an denen die menschliche Intelligenz niemals gesucht hätte, und den Entwicklern die Möglichkeit geben, sich auf das zu konzentrieren, was sie am besten können: Innovation.

Sergej Dechand

Clever attackieren

SIND SIE MEHRSPRACHIG? MALWARE SCHON!

Opportunistische Bedrohungsakteure setzen relativ einfache Techniken und kostengünstige Cybercrime-Tools ein, um Windows-Sicherheitsfunktionen und Antiviren-Scanner zu umgehen – so die Ergebnisse des HP Wolf Security Threat Research Teams.

Die Angreifer nutzen eine Mischung aus einfachen, aber effektiven und cleveren Tricks, um die PCs der Opfer mit AsyncRAT zu infizieren. AsyncRAT ist ein Trojaner für den Fernzugriff, der vertrauliche Informationen stiehlt:

➤ **Die Kunst der Täuschung:** Indem sie ungewöhnliche Dateitypen (zum Beispiel Batch-Dateien) einfach als vertraute Dateien-Kennungen (wie PDF-Dateien) ausgeben, können Angreifer Nutzer dazu verleiten, bösartige Anhänge anzuklicken. Diese grundlegende Technik macht sich zunutze, dass Windows standardmäßig Dateierweiterungen ausblendet. Wenn also eine Batch-Datei (.bat) als „hello.pdf.bat" gespeichert wird, zeigt der Windows-Dateiexplorer diese als „hello.pdf" an. Diese Technik ist zwar nicht neu, wird aber immer häufiger von Bedrohungsakteuren eingesetzt.

➤ **Einsen und Nullen:** Die Angreifer blähen ihre bösartigen Dateien künstlich auf, indem sie sie mit Millionen von bedeutungslosen Einsen und Nullen auffüllen. Einige waren fast zwei Gigabyte groß – zu groß für viele Anti-Malware-Scanner, um sie zu analysieren. Damit umging die Malware kritische Erkennungsmaßnahmen. Da sich das Muster dieser künstlich „aufgeblasenen" Abschnitte wiederholt, lässt sich die Malware in eine nur wenige Megabyte große Archivdatei komprimieren – ideal für die Verbreitung der Malware in Spam-Kampagnen.

➤ **Jetzt kommt der clevere Teil:** Mehrsprachige Malware, denn durch die Verwendung mehrerer Programmiersprachen umgeht der Bedrohungsakteur die Erkennung. Cyber-Kriminelle verschlüsseln die Malware mit einem in Go geschriebenen Packer, bevor sie die Anti-Malware-Scanfunktionen deaktivieren, die sie normalerweise erkennen würden. Der Angriff wechselt dann zu C++, um mit dem Betriebssystem des Opfers zu interagieren und die .NET-Malware im Speicher auszuführen. Dies hinterlässt nur minimale Spuren auf dem PC.

Die speicherinterne Ausführung von .NET-Dateien in C++ erfordert tiefgreifende Kenntnisse der undokumentierten Windows-Interna. Allerdings sind Bedrohungsakteure in der Lage, auf diese Techniken über Tools zuzugreifen, die in Hackerforen verkauft werden.

„IT-versierte Bedrohungsakteure können einfache Tools verwenden, die leicht im Dark Web zu kaufen sind: Damit sind sie in der Lage, komplexe und ausgefeilte Angriffe durchzuführen", erklärt Patrick Schläpfer, Malware-Analyst beim HP Wolf Security Threat Research Team. „Es ist wahrscheinlich, dass dieser spezielle Angriff von einer Einzelperson oder einer kleinen Gruppe durchgeführt wurde. Der Grund für diese Annahme: Für den Angriff wurde derselbe Server mit einer IP-Adresse genutzt, um die Spam-E-Mails zu verteilen und ein Command-and-Control-System einzurichten. Größere Bedrohungsgruppen wie QakBot generieren riesige Spam-Angriffe mit kompromittierten Anmeldeinformationen und verbinden sich über mehrere Proxy-Server zurück zu ihrer C2-Infrastruktur."

www.hp.com

Arbeitswelt der Zukunft

WIE ULTRAMOBILITÄT DIE IT-SICHERHEIT AUF DEN KOPF STELLT

An der Bushaltestelle ein paar Mails checken, im Auto an der Konferenz teilnehmen oder in der Warteschlange einen Termin koordinieren – es gibt immer mehr Alltagssituationen, die Mitarbeitende produktiv für berufliche Zwecke verwenden. Ein kurzer Griff zum Smartphone, Authentifizierung per Passwort, Face ID oder Fingerprint und schon erfolgt der Zugriff auf das Unternehmensnetzwerk via App. Das dauert nur Sekunden und spart wertvolle Zeit im Vergleich zum Starten eines Notebooks und dem Zugriff auf das unternehmensinterne Netzwerk.

Ultramobil zu arbeiten bedeutet, ohne Einschränkungen von Ort und Zeit per Smartphone und Tablet beruflich tätig sein zu können – ganz egal, wann und wo. Das ist ein deutlicher Unterschied zum mobilen Arbeiten per Notebook, der für die IT-Sicherheit ganz entscheidend ist. Denn im Gegensatz zu Notebooks mit Windows und macOS müssen IT-Verantwortliche sich mit den Spezifika von Android- und iOS-Betriebssystemen auseinandersetzen.

Hochsicherheit mit wenigen Klicks

Im ersten Reflex verursacht ultramobiles Arbeiten deshalb bei vielen IT-Verantwortlichen Unbehagen, da es an Erfahrungswerten im Umgang mit Sicherheitslösungen für Smartphones und Tablets fehlt. Die Befürchtung, durch ultramobiles Arbeiten ein Einfallstor für Sicherheitsbedrohungen zu schaffen, kann jedoch relativiert werden. Denn durch den Einsatz von Container-gestützten Lösungen lässt sich jedes Smartphone und jedes Tablet mit wenigen Schritten auf ein hochsicheres Niveau bringen und sogar Geheimhaltungsstufen bis VS-NfD einhalten.

AM ULTRAMOBILEN ARBEITEN FÜHRT KEIN WEG VORBEI – ES ÜBERZEUGT FACHKRÄFTE, STEIGERT DIE PRODUKTIVITÄT UND VEREINFACHT DIE ZUSAMMENARBEIT DER TEAMS.

Thomas Bitschnau, Head of Product, Materna Virtual Solution, www.virtual-solution.com

(Quelle: Materna Virtual Solution)

Alle Daten können innerhalb eines verschlüsselten Containers bearbeitet werden, der sich über ein sicheres Gateway mit dem firmeninternen Netzwerk synchronisiert. Dadurch ist sichergestellt, dass keine Daten zu unsicheren Schnittstellen oder externen Dritten gelangen können.

Die Installation von Container-Lösungen kann das IT-Management-Team sehr schnell und einfach erledigen. Es muss lediglich im User-Management der Software ein neuer Nutzercode generiert werden. Anschließend können Mitarbeitende die Container-Lösung in wenigen Minuten auf ihrem Smartphone oder Tablet installieren und dann auf alle freigegeben Dokumente, Anwendungen und Programme zugreifen.

Aus Nachhaltigkeits- und Kostengründen können Mitarbeitende dabei ihre privaten Geräte gemäß BYOD (Bring Your Own Device) nutzen oder aus Gründen der Usability ihr beruflichen Devices gemäß COPE (Corporate Owned, Personally Enabled) auch privat verwenden. Das verursacht keine Sicherheitsprobleme, weil Unternehmensdaten nicht aus dem Container gelangen können. Auch privat genutzte Anwendungen wie WhatsApp können nicht auf berufliche Kontaktlisten zugreifen. Die Unternehmensdaten verbleiben also sicher im Unternehmen.

Kollaboration und KI-Anwendung im sicheren Raum

Es ist absehbar, dass ultramobiles Arbeiten in den kommenden Jahren weitere spannende Möglichkeiten eröffnet. Devices wie Augmented-Reality-Brillen werden sich effizienzsteigernd in Arbeitsabläufe einbinden lassen. Und auch neue Technologien wie Künstliche Intelligenz könnten im Rahmen einer On-Premises-Installation die Mitarbeitenden unterstützen – sei es, um automatisiert Daten zu hinterlegen, Prozesse zu verbessern oder Routinemaßnahmen zu erledigen. Am ultramobilen Arbeiten führt so kein Weg vorbei – es überzeugt Fachkräfte, steigert die Produktivität und vereinfacht die Zusammenarbeit der Teams.

Thomas Bitschnau

Threat Hunting Erkenntnisse 2023

IMMER MEHR IDENTITÄTSBASIERTE ANGRIFFE UND HANDS-ON-KEYBOARD-AKTIVITÄTEN

Mit dem rasanten Fortschritt der Informationstechnologie entwickeln Cyberakteure immer neue und ausgefeiltere Methoden und Taktiken, um mit ihren Aktivitäten erfolgreich zu sein. Ausgangspunkt für viele dieser Operationen ist laut des neuesten Threat Hunting Reports von CrowdStrike die Kompromittierung der Identität. 62 Prozent der interaktiven Angriffsversuche basierten auf dem Missbrauch gültiger Zugangsdaten. Dabei verlassen sich die Angreifer nicht nur auf die Ausnutzung legitimer Zugangsdaten. Vielmehr haben sie gezeigt, dass sie in der Lage sind, alle Formen der Identifizierung und Autorisierung für ihre Zwecke zu missbrauchen, einschließlich im Untergrund erworbener Zugangsdaten. Hier floriert der Handel: Die Zahl der im Dark Web geschalteten Inserate von Access-Brokern ist um 147 Prozent gestiegen. Dank des einfachen Zugriffs auf gültige Konten, die zum Kauf angeboten werden, sinkt die Einstiegshürde für eCrime-Akteure, die kriminelle Operationen durchführen wollen.

DIE ANGREIFER SETZEN VERSTÄRKT AUF IDENTITÄTSBASIERTE ANGRIFFE, WOBEI DER DIEBSTAHL UND DER MISSBRAUCH KOMPROMITTIERTER IDENTITÄTEN IMMER MEHR AN BEDEUTUNG GEWINNT.

Zeki Turedi,
Field CTO Europe, CrowdStrike,
www.crowdstrike.de

Breakout-Time auf Rekordtief

Mit 79 Minuten erreichte die durchschnittliche Breakout-Time ein neues Rekordtief. Die Breakout-Time gibt an, wie lange ein Angreifer im Durchschnitt benötigt, um sich von der anfänglichen Kompromittierung lateral zu anderen Hosts in der Opferumgebung zu bewegen. Sie sank von dem bisherigen Tiefstwert von 84 Minuten im Jahr 2022 auf den neuen Rekordwert von 79 Minuten in diesem Jahr. Besorgniserregend ist, dass die kürzeste Breakout-Time des Jahres lediglich sieben Minuten betrug. Die Verkürzung der Zeitspanne verdeutlicht die rasant fortschreitende Agilität und Effizienz von Cyberkriminellen beim Ausnutzen von Schwachstellen und dem Eindringen in IT-Systeme. Es wird immer dringlicher, dass Unternehmen ihre Sicherheitsmaßnahmen auf den neuesten Stand bringen und proaktiv gegen solche Angriffe vorgehen, um ihre Netzwerke vor den Auswirkungen raffinierter und schneller Cyberangriffe zu schützen.

Cloud – das neue Schlachtfeld

Darüber hinaus wächst die Spezialisierung der Angreifer auf Cloud-Umgebungen. Die Vorteile, die die Cloud bietet, haben sie zu einem unverzichtbaren Bestandteil der modernen IT-Infrastruktur von Unternehmen gemacht. Die schnell wachsende Nachfrage an Cloud-Diensten sowie die Komplexität der Cloud-Verwaltung und -Kontrolle haben jedoch zu einer Wissenslücke bei der ordnungsgemäßen Sicherung dieser Umgebungen geführt. Im Laufe der letzten Monate haben die Angreifer immer wieder bewiesen, dass sie alle wichtigen Cloud-Plattformen gut beherrschen. Besonders schnell haben die Angreifer herausgefunden, wie sie gängige Fehlkonfigurationen ausnutzen oder die integrierten Cloud-Verwaltungstools missbrauchen können. Besorgniserregend ist die Tatsache, dass einige Angreifer die Cloud-Umgebungen ihrer Opfer besser im Griff zu haben scheinen als die Unternehmen selbst.

Zunahme von Kerberoasting-Angriffen

Der erste Bericht unter der Leitung des neuen Counter Adversary Operations-Teams zeigt außerdem einen Anstieg der Kerberoasting-Angriffe um 583 Prozent im Vergleich zum Vorjahr auf. Dabei handelt es sich um eine Technik, die Angreifer missbrauchen können, um gültige Anmeldeinformationen für Microsoft Active Directory-Dienstkonten zu erhalten. Kerberoasting ist eine vorteilhafte Technik für Angreifer, da sie auf einen SPN abzielt, der mit einem Active

MEHRWERT

Der CrowdStrike Threat Hunting Report 2023 kann hier kostenlos heruntergeladen werden:

Directory-Konto verknüpft ist, wodurch sie in der Regel über höhere Privilegien verfügen und der Angreifer dadurch seine Reichweite vergrößern kann und Zugriff auf sensible Dateien oder Systeme bekommt. Darüber hinaus sind diese Angriffe schwer zu erkennen, da Kerberos-Aktivitäten in der alltäglichen Telemetrie so häufig vorkommen, dass die Angreifer in der Masse untertauchen können. Obwohl diese Technik gut dokumentiert ist, stellt sie eine erhebliche Bedrohung für Unternehmen dar.

Technologie- & Finanzsektor traurige Spitzenreiter

Insgesamt ist die Zahl der interaktiven Angriffsversuche um 40 Prozent im Vergleich zum Vorjahr gestiegen, wobei der Technologiesektor im sechsten Jahr in Folge der am häufigsten angegriffene Sektor war, gefolgt vom Finanzsektor, dem Einzelhandel und dem Gesundheitswesen sowie der Telekommunikationsbranche. Besonders stark angegriffen wurde im Vergleich zum letzten Jahr der Finanzsektor. Hier beobachtete CrowdStrike einen 80-prozentigen Anstieg des Volumens an interaktiven Angriffsversuchen. Das ist der größte Zuwachs an gezielten Angriffsaktivitäten, den CrowdStrike bisher in der Finanzdienstleistungsbranche beobachtet hat. Die aggressivsten staatsnahen Angreifer, die es auf den Finanzsektor abgesehen haben, sind Nordkorea-nahe Angreifergruppen. Sie sind weiterhin an zahlreichen finanziell motivierten Operationen beteiligt, die in erster Linie auf Finanz- und Fintech-Unternehmen abzielen. Auch wenn sich einige Angreifer auf den Diebstahl von Kryptowährungen oder NFTs (Non-Fungible Tokens) konzentrieren, bleiben opportunistische „Big Game Hunting"-Ransomware- und Datendiebstahl-Kampagnen die primäre eCrime-Bedrohung für Finanzinstitutionen. Aufgrund der Notwendigkeit für die Opferorganisation, die Systembetriebszeit aufrechtzuerhalten, und des sensiblen Charakters des Sektors kommen eCrime-Bedrohungsakteure wahrscheinlich zu dem Schluss, dass Finanzinstitute bereit und in der Lage sind, Lösegeldforderungen zu zahlen.

Trend: Ausnutzung von RMM-Tools

Ein weiterer Trend in diesem Jahr war der Missbrauch bewährter Methoden, um auf die Umgebungen der Opfer zuzugreifen und in diesen zu navigieren. Zu diesen Methoden gehört beispielsweise die Ausnutzung von Schwachstellen und der Einsatz von Remote Monitoring and Management (RMM)-Tools. Die Zahl der Angreifer, die legitime RMM-Tools ausnutzen, ist im Vergleich zum Vorjahr um 312 Prozent gestiegen: Ein weiterer Beleg für die Berichte der CISA ist die Tatsache, dass Angreifer zunehmend legitime und bekannte Remote-IT-Management-Anwendungen nutzen, um nicht entdeckt zu werden. So können sie auf sensible Daten zugreifen, Ransomware einsetzen oder weitere gezielte Folgetaktiken installieren.

Die Leistung des menschlichen Einfallsreichtums

Angreifer wollen ständig ihre Reichweite vergrößern, ihre Vorgehensweise optimieren und ihre Wirkung verstärken, trotz der Hindernisse, die ihnen durch Sicherheitslösungen in den Weg gelegt werden. In dem Maße, in dem sich die Technologien und Sicherheitsprodukte, auf die sich Unternehmen verlassen, weiterentwickeln, verändern sich auch die Werkzeuge und Methoden der Angreifer – und zwar in einem alarmierenden Tempo. Dies ist die Nische, die von der menschlichen Bedrohungsjagd in der Sicherheitsbranche ausgefüllt wird. Die Threat Hunter verfolgen die sich weiterentwickelnden Bedrohungen mit der gleichen Hartnäckigkeit, Kreativität und technischen Kompetenz, die sie auch bei den Angreifern sehen. Es ist die Nutzung des menschlichen Einfallsreichtums, die es den Gegnern wirklich unmöglich macht, sich zu verstecken.

Zeki Turedi

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

Hier geht's zum neuen

it-daily Weekend

uni: Ransomware ++ **Juli:** Quantencomputing ++ **August:** Zero Trust ++ **September:** Office 4.0

Sichere Datenspeicherung

HOCHVERSCHLÜSSELT IN DIE CLOUD

Selbstständige, Ärzte, Anwälte, Steuerberater, KMUs, NGOs und Vereine finden in TeamDrive eine einfach zu benutzende Lösung für die Zusammenarbeit in der Cloud. Sie verbindet höchste Sicherheit und einfache Bedienung und erfüllt eine Vielzahl von Anforderungen.

TeamDrive ist eine Ende-zu-Ende verschlüsselte sichere DSGVO-zertifizierte Cloudlösung aus Deutschland mit Speicherung aller Daten in ISO 27001-zertifizierten Rechenzentren in Deutschland.

Verschlüsselt und unveränderbar
Die Software integriert sich in die vorhandenen Abläufe und Systeme. Man kann von überall auf der Welt auf die Daten zugreifen, die hochverschlüsselt in der Cloud liegen. Ein Anwender kann Zugriffsrechte für einzelne Dokumente oder ganze Datenräume an weitere Personen vergeben. Durch eine automatische Versionierung lässt sich lückenlos nachverfolgen, wer wann was gelesen oder gar verändert hat.

Dateien lassen sich automatisch als verschlüsselte E-Mail-Anlagen versenden und umgekehrt digitale Briefkästen zum sicheren verschlüsselten Empfang einrichten. Aufbewahrungsfristen gespeicherter Dateien verwaltet TeamDrive automatisch.

Ob Steuerberater, KMU oder Verein: Über kostenfreie Gastlizenzen lässt sich gewährleisten, dass Mandanten, Geschäftspartner oder Mitglieder Zugriff auf alle für sie relevanten Dateien in TeamDrive erhalten.

Die BoxCryptor Alternative
TeamDrive bietet sich auch als AddOn für Microsoft 365 mit Speicherung der verschlüsselten Daten in Microsoft Onedrive an.

www.teamdrive.com

TEAMDRIVE secure collaboration

GoBD Whitepaper und kostenfreie Testversion

IoT-Sicherheitsbedrohungen

DRASTISCHE ZUNAHME

Der neueste Nozomi Networks Labs OT & IoT Security Report: Unpacking the Threat Landscape with Unique Telemetry Data (Entschlüsselung der Bedrohungslandschaft mit einzigartigen Telemetriedaten) zeigt, dass Malware-Aktivitäten und Warnungen vor unerwünschten Anwendungen in OT- und IoT-Umgebungen drastisch zugenommen haben.

Die Auswertung einzigartiger Telemetriedaten von Nozomi Networks Labs hat ergeben, dass Malware-bezogene Sicherheitsbedrohungen in den letzten sechs Monaten um das 10-fache angestiegen sind. In den breiten Kategorien der Malware und potenziell unerwünschten Anwendungen stieg die Aktivität um 96 Prozent. Die Bedrohungsaktivität im Zusammenhang mit Zugriffskontrollen hat sich mehr als verdoppelt. Unzureichende Authentifizierung und Passworthygiene führten die Liste der kritischen Warnmeldungen im zweiten Berichtszeitraum in Folge an – obwohl die Aktivitäten in dieser Kategorie im Vergleich zum Vorjahr um 22 Prozent zurückgingen.

Denial-of-Service-Attacken (DoS) sind nach wie vor einer der häufigsten Angriffe auf OT-Systeme. Es folgt die Kategorie der Remote-Access-Trojaner (RAT), die von Angreifern häufig verwendet werden, um die Kontrolle über kompromittierte Rechner zu erlangen. Verteilte Denial-of-Service-Bedrohungen (DDoS) sind die größte Bedrohung in IoT-Netzwerkdomänen.

Daten aus IoT-Honeypots
Bösartige IoT-Botnets sind auch in diesem Jahr aktiv. Nozomi Networks Labs ermittelte wachsende Sicherheitsbedenken, da Botnets weiterhin Standardanmeldedaten verwenden, um auf IoT-Geräte zuzugreifen.

Brute-Force-Angriffe sind nach wie vor eine beliebte Technik, um sich Zugang zum System zu verschaffen – Standard-Anmeldedaten sind eine der Hauptmethoden, mit denen sich Bedrohungsakteure Zugang zum IoT verschaffen.

www.nozominetworks.com

Datensicherheit

SIND IHRE DATEN AUCH VOR INSIDERN GESCHÜTZT?

Die jüngste Sicherheitslücke im Pentagon, bei der der 21-jährige Jack Teixeira anscheinend vertrauliche Informationen auf Social-Media-Websites weitergab, hat die Diskussion über den Schutz von Daten vor böswilligen Insidern neu entfacht. Von der Schlange im Garten Eden (dem ursprünglichen Insider) über Snowden, Manning und Winner bis hin zu Teixeira braucht es nur einen faulen Apfel, um den Lauf der Geschichte zu verändern.

Der Zugang zu Informationen und die Tatsache, dass es generell viel zu viel Zugang zu sensitiven Daten gibt, ist ein roter Faden, der sämtliche Insider miteinander verbindet. Robert Litt, ehemaliger Chefsyndikus des Büros des Direktors der Nationalen Nachrichtendienste, bemerkte dazu: „Nach dem Bekanntwerden der undichten Stellen sollte eine nüchterne und gründliche Überprüfung des Informationsaustauschs, der Anzahl der Personen mit Sicherheitsfreigaben, der Umsetzung bestehender Richtlinien in Bezug auf die Notwendigkeit, etwas zu wissen, und der Überwachung von Verschlusssystemen erfolgen."

Insider-Bedrohungen sind das am schwierigsten abzuwehrende Risiko und können gleichzeitig den größten Schaden anrichten. Das Pentagon hat innerhalb seiner physischen und digitalen Grenzen wahrscheinlich alles richtig gemacht: Teixeira arbeitete in einer Einrichtung mit sensiblen geschützten Informationen (SCIF/Sensible Comparted Information Facility), die „vor elektronischer Überwachung schützt und Datenlecks verhindert". Das bedeutet, dass keine USB-Sticks hinein- oder herausgebracht werden durften, dass nichts ins Internet hochgeladen werden konnte und dass keine Datenübertragungen möglich waren. Dennoch konnte keine der Perimeter-Kontrollen vor dieser Bedrohung schützen.

Anatomie eines Insider-Angriffs

Was ist also schiefgelaufen? Die undichte Stelle verfügte über umfangreichen Zugang zu sensitiven Daten, die sie offensichtlich nicht benötigte. Trotz des Hypes um Zero Trust scheint es sich in diesem Fall um ein Versagen des Need-to-know-Modells und/oder eine Panne bei der Überwachung klassifizierter Systeme zu handeln. In vielen Unternehmen und staatlichen Organisationen liegt der Schwerpunkt immer noch oft auf dem Schutz der Außengrenzen und nicht auf dem Schutz des eigentlichen Ziels fast sämtlicher Angriffe: der Daten im Inneren.

Es ist schon seltsam, dass die meisten Unternehmen so viele Kontrollen dort

durchführen, wo keine großen Risiken bestehen. Anders die Banken: Sie konzentrieren sich beim Schutz weniger auf die Fenster und Türen als auf den Tresorraum, da sie wissen, dass Bargeld ein wertvolleres Ziel ist als die Kugelschreiber im Schalterraum.

Hätte Teixeira nicht von vornherein Zugang zu so vielen sensitiven Informationen gehabt, hätte es keinen oder nur einen sehr geringen Schaden gegeben, der viel schneller eingedämmt worden wäre. Der Insider hätte zwar möglicherweise den Perimeter überwinden können, aber niemand würde Teixeiras Namen kennen, wenn die Daten die ganze Zeit adäquat geschützt worden wären.

Das Gleichgewicht zwischen Zugang und Sicherheit finden

Den „Tresor" in der digitalen Welt zu schützen, ist natürlich eine große Herausforderung. Jeden Tag werden immer mehr sensitive Daten an immer mehr Orten gespeichert. Die Zusammenarbeit erfordert ein Gleichgewicht zwischen Produktivität und Sicherheit, denn Daten haben nur dann einen Wert, wenn sie gemeinsam genutzt werden können.

Schränkt man den Zugang zu Daten vollständig oder zu stark ein, werden sie wertlos. Die Nachrichtendienste haben dies gelernt, nachdem sie vor dem 11. September den Informationsaustausch zwischen verschiedenen Behörden eingeschränkt hatten. Werden die Beschränkungen jedoch zu sehr gelockert, können die Daten schnell zu einer Gefahr werden, wie die jüngste Sicherheitsverletzung im Pentagon gezeigt hat.

Wie lassen sich Zugang und Sicherheit in Einklang bringen? Mit fünf einfachen Schritten kann die Gefahr sowohl durch Innentäter als auch durch externe Angreifer, welche die Konten oder Computer von Insidern kompromittieren, wesentlich reduziert werden:

IN VIELEN UNTERNEHMEN LIEGT DER SCHWERPUNKT IMMER NOCH OFT AUF DEM SCHUTZ DER AUSSENGRENZEN UND NICHT AUF DEM SCHUTZ DES EIGENTLICHEN ZIELS: DER DATEN IM INNEREN.

Michael Scheffler,
Country Manager DACH,
Varonis Systems,
www.varonis.com/de

#1 Machen Sie eine Bestandsaufnahme der Regeln, die Sie zum Schutz sensitiver Daten aufgestellt haben. Haben Sie festgelegt, wann und wie Sie sensible Daten löschen, unter Quarantäne stellen oder sperren?

#2 Prüfen Sie, ob Sie diese Regeln manuell oder durch Automatisierung durchsetzen können.

#3 Erkennen Sie, wie Sie Verstöße gegen diese Regeln feststellen können.

#4 Suchen Sie nach Regeln, die erstellt, verfeinert oder effektiver durchgesetzt werden sollten.

#5 Wenn Sie gerade erst anfangen, sollten Sie eine Bestandsaufnahme Ihrer Daten vornehmen, um festzustellen, wo Benutzer sensitive Daten speichern und mit wem sie sie teilen.

In den meisten Unternehmen greifen die Mitarbeitenden von überall und von vielen Geräten aus auf sensitive Daten zu, die in mit der Cloud verbundenen Anwendungen und Datenspeichern gespeichert sind. Dies ist so ziemlich das Gegenteil eines SCIFs. Bei einem derartig verteilten, unberechenbaren Perimeter macht es noch weniger Sinn, den größten Teil der knappen Sicherheitsressourcen dort einzusetzen. Zumal wir nicht wissen, woher die Angriffe kommen werden. Allerdings wissen wir, worauf sie es abgesehen haben. Die meisten Betriebe verfügen zwar nicht über streng geheime Informationen wie das Pentagon, dennoch haben sie Daten, die für Angreifer interessant sind. Deshalb ist es sinnvoll, die begrenzten Ressourcen auf diesen Bereich zu konzentrieren.

Die Umsetzung des Need-to-know-Prinzips und die genaue Überwachung der Daten auf Anzeichen ungewöhnlicher Aktivitäten tragen dazu bei, den Schaden zu verringern, den Insider anrichten können und machen es einfacher, sie aufzuspüren. Angreifer von außen, die einen Computer oder ein Konto eines Mitarbeitenden übernehmen (und damit effektiv zu Insidern werden), müssen wesentlich mehr Aufwand betreiben, um an die anvisierten Daten zu gelangen. Auf diese Weise haben Sicherheitslösungen größere Chancen, sie zu entdecken.

Es spielt keine Rolle, ob man mit militärischen oder Geschäftsgeheimnissen umgeht oder ob die Mitarbeitenden in einem SCIF, in einem Bürogebäude oder von zu Hause aus arbeiten: Priorisiert man die Sicherheit der Daten, sind diese besser sowohl vor Insidern als auch Angreifern von außen geschützt.

Michael Scheffler

it-sa 2023
Besuchen Sie uns
in **Halle 7, Stand 7A-319**

HACKING MIT POST EXPLOITATION FRAMEWORKS

ANGRIFFE VERSTEHEN UND VORBEUGEN

Um effektiv auf Cyber-Angriffe reagieren zu können, ist es unerlässlich, die aktuellen Angriffstechniken des Gegners zu kennen. Nur so ist es möglich, auf komplexe Angriffe adäquat zu reagieren und rechtzeitig geeignete Maßnahmen zu ergreifen. An dieser Stelle kommt die Phase der Post-Exploitation ins Spiel. Sie ist eine Phase des Penetrationstests, die voraussetzt, dass bereits eine Verbindung zwischen Angreifer und Ziel-IT besteht.

Hacking mit Post Exploitation Frameworks
Angriffe verstehen und vorbeugen, Awareness herstellen

Frank Neugebauer, Martin Neugebauer, Carl Hanser Verlag GmbH & Co.KG, 09-2023

Dieses Buch befasst sich mit der Installation und dem Einsatz von Post-Exploitation-Frameworks, die Penetrationstestern helfen, mögliche Angriffsszenarien in einer sicheren Umgebung zu simulieren und Systeme auf bestehende und potenzielle Schwachstellen zu überprüfen.

Es führt durch den Aufbau eines Testsystems und stellt verschiedene Post-Exploitation-Tools wie Metasploit, Koadic, Empire, Covenant, Merlin, Sliver und Mythic vor. Jedes Kapitel gibt einen Überblick über die Eigenschaften, die Installation und den praktischen Einsatz des jeweiligen Frameworks anhand verschiedener Szenarien. Am Ende jedes Kapitels finden Sie Wiederholungsfragen, um Ihr Wissen zu festigen.

Cyberresilienz

MIT DER RICHTIGEN STRATEGIE ZUM KRISENFESTEN UNTERNEHMEN

it-sa 2023
Besuchen Sie uns
in **Halle 7a, Stand 7A-115**

Die fortschreitende Digitalisierung hat zu einer steigenden Anzahl von Cyberangriffen geführt, wodurch Unternehmen zunehmend Gefahr laufen, Opfer von Datenverlusten, finanziellen Schäden und Rufschädigung zu werden. Angesichts dieser Bedrohungslage gewinnt das Konzept der Cyberresilienz immer mehr an Bedeutung.

Cyberresilienz bezeichnet die Fähigkeit eines Unternehmens, Cyberangriffe zu antizipieren, ihnen standzuhalten, sich von ihnen zu erholen und die eigene Widerstandsfähigkeit durch ständige Anpassung an neue Herausforderungen stetig zu optimieren. Es handelt sich um einen proaktiven Ansatz, der darauf abzielt, die Auswirkungen von Cyberangriffen zu minimieren und die Betriebskontinuität sicherzustellen. Neben der richtigen Technologie und geeigneten Tools sind auch stabile Prozesse sowie geschultes Personal wesentliche Grundvoraussetzungen.

Die Bedrohung ist real

Laut der Cyber Resilient Organization Study von IBM Security erlebten 51 Prozent der Unternehmen im letzten Jahr eine größere Datenpanne und 61 Prozent zahlten infolge eines Ransomware-Angriffs das geforderte Lösegeld. Doch wie gelangen Angreifer überhaupt in die Systeme der geschädigten Organisationen? Der Cyber Readiness Report 2022 von Hiscox deckt auf, dass neben den beiden meistgenutzten Einfallstoren Phishing (62 Prozent) und Zugangsdatendiebstahl (44 Prozent) auch Dienstleister wie MSPs (40 Prozent) sowie ungepatchte Server (28 Prozent) ein erhebliches Risiko darstellen.

Nicht nur die monetären Kosten erfolgreicher Angriffe sind enorm. Auch die Reputation kann erheblich beeinträchtigt werden, wie der Fall Landkreis Anhalt-Bitterfeld im Sommer 2021 eindrucksvoll zeigte: Die Kommune wurde durch einen Cyberangriff so weit lahmgelegt, dass sie den Katastrophenfall ausrief. Nachdem der Angriff am 06.07.2021 entdeckt wurde, stellten forensische Ermittlungen fest, dass er bereits einen Monat zuvor begann. Damit hatte die Kommune die Eindringlinge sogar verhältnismäßig schnell gefunden. Laut dem von IBM und dem Ponemon Institute veröffentlichten Report „Cost of a Data Breach 2022" dauert es durchschnittlich 277 Tage, bis Security-Teams eine Sicherheitslücke erkennen und eindämmen.

Je schneller erkannt, desto schneller gebannt

Die Tücke von vielen Cyberangriffen besteht darin, dass sich die Angreifer relativ lange unbemerkt in der IT-Infrastruktur bewegen. Häufig lässt sich nicht feststellen, seit wann sie dort ihr Unwesen treiben. Umso wichtiger ist es, dass Eindringlinge so früh wie möglich aufgespürt werden. Laut BSI sind die Top Ransomware-Maßnahmen: das Monitoring von RDP-Zugängen, die Überwachung von Dateizugriffen mittels sogenannten „Canary Files" sowie die regelmäßige Überprüfung des Systems auf ungewöhnliche Netzwerkverbindungen. Außerdem gehören ein solides Monitoring sowie zuverlässiges Patching von Schwachstellen und ein umfassendes Backup zu den Grundvoraussetzungen auf dem Weg zur Cyberresilienz.

In einer perfekten Welt kümmern sich externe Spezialisten um solche Themen oder Unternehmen bauen ein eigenes Security Operations Center (SOC) mit internen Experten auf. Doch in Zeiten von Budgetkürzungen und Fachkräftemangel sind beide Optionen für die meisten mittelständischen Betriebe nicht realistisch. Glücklicherweise gibt es noch eine Alternative: IT-Management-Tools, die die IT-Teams in Unternehmen mit automatisierten Prozessen von Routineaufgaben entlasten und vom Patch Management über die Endpunktverwaltung und IT Asset Management bis hin zum Backup sämtliche relevanten Themen abdecken. So gelingt Schritt für Schritt die Cyberresilienz.

André Schindler
www.ninjaone.de

Sogenannte „Canary Files" warnen, wie die Vögel in früheren Kohlebergwerken, vor anstehender Gefahr. Wurde Stickstoff freigesetzt, kippten die Kanarienvögel um – und die Bergbauer konnten rechtzeitig evakuieren.

Modulare Basis für die IT-Sicherheit

MODERNE CYBER-SICHERHEITSARCHITEKTUR

Hochkomplexe Sicherheitssysteme funktionieren nur, wenn die IT-Infrastruktur im Unternehmen „sauber" ist. Dafür schaffen Client- beziehungsweise Unified-Endpoint-Management-Systeme eine verlässliche Grundlage.

Endpoints sind das Haupteinfallstor für Cyber-Attacken, das gilt in Zeiten verstärkten Homeoffice-Betriebs umso mehr. Denn wo fest installierte Rechner innerhalb des Unternehmens durch Firewalls oder Intrusion Prevention Systeme geschützt werden, sind Heimarbeitsplätze Cyber-Angriffen viel ungeschützter ausgesetzt. Jederzeit mit dem Internet verbundene Endgeräte und veraltete Software- oder Betriebssystemversionen öffnen Schadsoftware Tor und Tür.

Auf der it-sa 2023 (10. bis 12. Oktober, Nürnberg) zeigt UEM- Spezialist Aagon in Halle 6, Stand 6-400 deshalb neueste Lösungen für den Schutz von Endpoints, egal ob sich diese im Unternehmensnetzwerk oder außerhalb davon befinden. Client Management – oder der neue Begriff Unified Endpoint Management (UEM) – und IT-Sicherheit, diese beiden Sphären können und dürfen nicht mehr getrennt voneinander betrachtet werden. Nur so können Unternehmen eine moderne Cyber-Sicherheitsarchitektur aufbauen.

Patch- und Vulnerability Management

Zentrale UEM-Lösungen sind das Mittel der Wahl, um Endgeräte zu jeder Zeit mit dem höchsten Maß an Sorgfalt „sauber" (also sicher) zu halten. Sie inventarisieren zunächst alle Endpoints und erfassen sie in einer Zentralkomponente, bei Aagon ist dies in ACMP Core enthalten. Anschließend kann es direkt mit dem automatischen Roll-Out von Updates und Patches losgehen. Diese erscheinen in immer kürzeren Abständen, und alles manuell nachzuverfolgen, bedeutet für IT-Abteilungen viel Aufwand. Das Modul ACMP Managed Software prüft deshalb im ersten Schritt automatisiert die Verfügbarkeit von Patches. Anschließend verteilt es die Patches auf Clients und Server innerhalb des Netzwerks nach einem sinnvollen Plan und koordiniert sowie standardisiert die sicherheitsrelevante Systemaktualisierung.

Neben dem Patch- und Update Management gehört zusätzlich ein Schwachstellen-/Vulnerability Management zu den essentiellen Bestandteilen eines UEM-Systems, das proaktiv auf Sicherheitslücken prüft. In der modular aufgebauten UEM-Plattform ACMP sind Patch- und Vulnerability Management integriert und greifen wie Zahnräder in-

Schematische Darstellung eines möglichen SOAR-Prozesses
(Quelle: Aagon)

einander. Das Schwachstellenmanagement gleicht die gesamte IT-Infrastruktur mit Datenbanken über bereits bekannte Schwachstellen ab, das Patch Management sorgt für die automatisierte Behebung von Problemen, sollte es sich um nicht aktuelle Softwareversionen handeln.

UEM als Klammer

Microsoft besetzt das Sicherheitsthema mit seinen Lösungen Defender, BitLocker und Intune, die im Laufe der Jahre immer besser geworden sind. Ihre Grundfunktionen sind zudem im Betriebssystem verankert, das spart Zusatzkosten für Extra-Software.

Der Microsoft Defender deckt die klassischen Security-Maßnahmen im Windows-Umfeld ab, seine dezentrale Anwenderoberfläche hat in der Vergangenheit allerdings nicht gerade mit Benutzerfreundlichkeit geglänzt. Deshalb hat Aagon sein Modul ACMP Defender Management entwickelt. Administrationsabteilungen können den Defender damit in nur einer Oberfläche auf allen Clients und Servern verwalten. Über seine Auswertungen erhalten sie zeitlich automatisch einstellbare Statusinformationen. Die Funktionen des Defenders lassen sich dadurch weitaus zielgerichteter einsetzen.

Hybride Lösung integriert Intune

Als UEM-Lösung aus der Cloud hat Microsoft Intune im Programm. Sie ist im Enterprise-Lizenzvertrag Microsoft 365 E3 bereits enthalten. Cloud-basierte Lösungen sind jedoch vom Umfang her limitiert, was ihren Komfort sichtlich einschränkt. Gerade bei großen Serverstrukturen empfiehlt sich daher ein hybrider Ansatz aus klassischer On-Premises-UEM-Lösung mit einem Anteil an Cloud-Verwaltung. Aagon ermöglicht diese Kombination über den neuen ACMP Intune Connector. Mobile Devices lassen sich damit über die UEM-Konsole managen, zurücksetzen oder im Verlustfall auch löschen. Des weiteren kann über das UEM-System die Synchronisation der Geräteeinstellungen, Richtlinien und Berechtigungen der Intune-Instanz auf das mobile Device gestartet werden.

Zudem wichtig: Eine Laufwerksverschlüsselung schützt wirksam bei Datendiebstahl beziehungsweise -verlust; Microsoft hat dafür den BitLocker im Programm. Weil aber an Homeoffice-Arbeitsplätzen die Gefahr durch physischen Verlust der Hardware besonders hoch ist, empfiehlt sich eine Verlagerung der Verschlüsselung in ein zentrales Managementboard. Mit dem ACMP BitLocker Management ergänzt Aagon den Microsoft BitLocker um praktische Funktionen: zentrale Verwaltung der Festplattenverschlüsselungen, Statusabfragen von Schlüsselschutzvorrichtungen, Überblick über BitLocker-fähige Clients sowie diverse Monitoring- und Reporting-Funktionen für Analysezwecke.

Alle Sicherheits-Tools in einer Oberfläche

So bieten UEM-Systeme einen ganzheitlichen Lösungsansatz für die zentrale Verwaltung und Steuerung der IT-Infrastruktur eines Unternehmens: von der Inventarisierung von Hard- und Software über die Verwaltung von Lizenzen, Sach- und Anlagegütern sowie der Paketierung und Verteilung von Software und Betriebssystemen bis hin zum Helpdesk und Ticketing sowie schließlich Maßnahmen zur IT-Sicherheit wie Patch und Schwachstellen Management. Letzteres erlaubt es IT-Admins, vulnerable Stellen auf den Endpoints zu beobachten und bei Fund mit automatischen Aktionen rechtzeitig zu reagieren. Veraltete Programme können ebenso eine Sicherheitslücke darstellen wie fehlerhafte Konfigurationen.

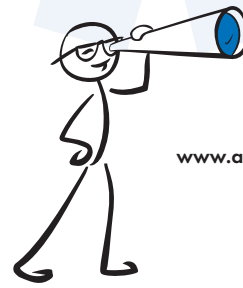
Security Orchestration, Automation and Response (SOAR) ist das neue Zauberwort in der IT-Sicherheit, das auch auf der diesjährigen it-sa allgegenwärtig sein dürfte. Darunter versteht man ein Konzept des gebündelten Abarbeitens von Security-Aufgaben. Es umfasst alle Funktionen, die darauf abzielen, durch Standardisierung und Priorisierung automatisiert und damit effizient auf erkannte Bedrohungen zu reagieren.

Drei Basis-Bausteine für SOAR

Durch das Zusammenspiel ihrer verschiedenen Module deckt die ACMP Suite die drei grundlegenden SOAR-Bausteine ab: Case- und Workflow-Management, Aufgabenautomatisierung sowie zentraler Aufruf von Bedrohungsinformationen. Die einzelnen Komponenten der UEM-Lösung generieren über Agents viele Daten, die am Client entstehen und die man für SOAR benötigt. Diese lassen sich im System an zentraler Stelle sammeln, analysieren und priorisieren. So sind weniger Schnittstellen notwendig, und es entstehen Synergieeffekte.

Weiterer Vorteil: Aus einer einheitlichen Oberfläche heraus kann die IT-Abteilung Security-Maßnahmen für die Endpoints orchestrieren, von der Diagnose bis zur Fehlerbehebung. Die Reporting-Funktion im UEM liefert zeitlich automatisch einstellbare Statusinformationen. In einem frei konfigurierbaren Dashboard kann der Administrator zusammenstellen, was im SOAR-Kontext angezeigt werden soll. Auf diese Weise ist es auch mittelständischen Unternehmen mit kleinerem IT-Budget möglich, ein zeitgemäßes SOAR-Konzept zur Sicherung ihres Netzwerkbetriebs aufzusetzen.

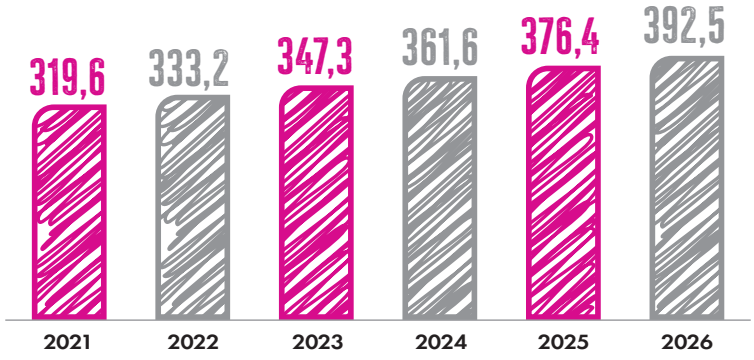
Sebastian Weber | www.aagon.com



PLUS

kostenlose Testversion
der ACMP Suite:
www.aagon.com/testversion

PROGNOSE ZUR ANZAHL DER TÄGLICH VERSENDETEN UND EMPFANGENEN E-MAILS WELTWEIT VON 2021 BIS 2026 (in Millarden)



Quelle: The Radicati Group © Statista 2023

Cyberangriffe vermeiden

E-MAIL-VERKEHR MAXIMAL ABSICHERN

Wussten Sie, dass zwischen 40 bis 50 Prozent* aller empfangenen E-Mails Spam sind? Und die mit Schadsoftware versehenen E-Mails werden immer professioneller. Häufig lassen sie sich erst auf den zweiten Blick enttarnen. Deswegen ist es besonders wichtig, seine E-Mail-Kommunikation zu schützen. Denn täglich werden dutzende E-Mails versendet, auf deren Inhalt es Hacker abgesehen haben. Und die Anzahl der versendeten E-Mails steigt weiter an. Werden wichtige Daten wie beispielsweise Überweisungsinformationen abgeändert, sind die Folgen fatal. Eine moderne und effiziente Secure E-Mail-Lösung kann dabei helfen, den E-Mail-Verkehr zu schützen.

Cyberangriffe auf E-Mails stellen nach wie vor ein großes Problem dar. Besonders die Anzahl von Phishing- und Ransomware-Angriffen hat in den letzten Jahren deutlich zugenommen. Durch diesen Anstieg ist auch die Anzahl potenzieller Opfer für einen Cyberangriff immens angestiegen. Hat sich einmal eine Schadsoftware im Unternehmen verbreitet, sind die Schäden oftmals nicht nur sehr kostspielig, sondern auch rufschädigend. Nicht zuletzt aus diesen Gründen ist ein signierter und verschlüsselter, DSGVO-konformer E-Mail-Verkehr essenziell.

* Quelle: ©Statista 2023

E-Mails digital signieren

E-Mails zu verschlüsseln, muss nicht kompliziert sein. Mit einer modernen Secure E-Mail-Lösung werden bereits alle wichtigen Sicherheitsfunktionen abgedeckt. Digitale E-Mail-Signaturen helfen dabei, die Unternehmenssicherheit zu erhöhen. Sie beweisen nicht nur die Identität des Absenders, sondern stellen auch die Authentizität sowie Integrität der E-Mail sicher. Ist eine E-Mail also digital signiert und unversehrt, kann sich der Empfänger sicher sein, dass die Nachricht wirklich vom Absender stammt und auf dem Versandweg nicht manipuliert wurde. Die Implementierung einer digitalen Signatur ist mit nur geringem Aufwand verbunden. Es werden Zertifikate benötigt, die bei sogenannten Certificate Authorities (CAs) beantragt werden müssen. Dieser Public Key Infrastructure (PKI)-Prozess wird in vielen Fällen bereits von den Lösungen vollständig übernommen.

Sicherheit aus der Wolke

Natürlich gibt es auch Cloud-Lösungen, die Security Features wie E-Mail-Verschlüsselung oder digitale Signaturen enthalten. Ein Vorteil von Cloud-Lösungen ist, dass sie sehr einfach und komfortabel sind. Es ist keine Installation vor Ort mehr nötig, doch die Sicherheit bleibt gleich. Außerdem werden die Lösungen in europäischen Rechenzentren betrieben sind somit immer auf dem neusten technischen Stand. und erfüllen alle aktuellen Datenschutz-Standards wie die der DSGVO.

Schnell einmal eine E-Mail versenden

Wie kommuniziert man verschlüsselt, wenn der Gesprächspartner kein eigenes Schlüsselmaterial hat? Tritt dieser Fall ein, ist es wichtig, dass bei der Wahl eines Secure E-Mail Gateway darauf geachtet wird, dass eine Spontanverschlüsselung enthalten ist. Wird eine E-Mail so versendet, ist sie plus Anhang verschlüsselt und wird mit einer Trägermail ausgeliefert. Der Empfänger muss nun lediglich ein Passwort eingeben und die E-Mail ganz einfach öffnen sowie verschlüsselt antworten.

Viele Wege führen zur sicheren Kommunikation

Eine sichere E-Mail-Kommunikation muss nicht schwer sein! Moderne All-in-one-Lösungen ermöglichen mittlerweile digitale Signaturen, E-Mail-Verschlüsselung und sind zudem als Cloud-Lösung erhältlich. Setzen Unternehmen sie ein, lässt sich die Sicherheit deutlich optimieren, und Cyberangriffe lassen sich gezielt verhindern.

Günter Esch | www.seppmail.de

Ganzheitliche mobile Sicherheit

IT-SICHERHEITSPLATTFORMEN MÜSSEN ANDROID, IOS UND CHROMEBOOKS IM BLICK HABEN

Weltweit sind mehr als 6,8 Milliarden Smartphones in Gebrauch. Sie bieten Hackern eine große Angriffsfläche, um Schwachstellen in Apps und mobilen Betriebssystemen anzugreifen. Attacken auf mobile Hardware, unter ihnen vor allem Phishing, Ransomware- und Zero-Day-Angriffe, nehmen zu. Organisationen stehen daher unter zunehmendem Druck, die wachsende Angriffsfläche in die IT-Sicherheit zu integrieren. Nicht umsonst schätzen die Experten von Gartner, dass 2025 mehr als die Hälfte der Unternehmen eine IT-Sicherheitslösung für iOS und Android einsetzen werden. (1)

Unternehmen vertrauen zunehmend auf eine verteilt arbeitende Belegschaft. Diese verwendet unterwegs häufig private Smartphones für den Zugriff auf Unternehmensressourcen. Auch das Nutzen von Privataccounts auf Business Smartphones oder Notebooks stellt eine Gefahr dar. Cyberkriminelle nutzen deshalb verstärkt mobile Geräte als Ziel für ihre Angriffe. Die Gartner-Experten verweisen auf Belege, „dass einige der weitreichendsten Angriffe der jüngeren Vergangenheit zu einem Zeitpunkt im Angriffsprozess auf mobile Hardware zurückgegriffen haben." (2)

Eine Mobile Threat Defence (MTD) ist daher ein unternehmenskritischer Bestandteil der allgemeinen IT-Sicherheitsstrategie. Die Abwehr mobiler Gefahren geht weit über ein bloßes Mobile Device Management hinaus.

EINE ABWEHR MOBILER CYBERGEFAHREN BIETET FOLGENDE FUNKTIONALITÄTEN:

➤ Schutz vor mobilen Gefahren – Durch die Machine-Learning-gestützte Analyse sowohl lokaler als auch Cloud-basierter Daten erkennt MTD bösartige Applikationen und Zero-Day-Angriffe. Sie liefert in Echtzeit die erforderliche Transparenz, um Apps zu überprüfen und anomales Verhalten zu identifizieren. Sie erkennt zum Beispiel die Isolation einer App, das Abschalten von WiFi oder Bluetooth sowie das Deaktivieren bzw. Deinstallieren von Apps mit bestimmten Dateierweiterungen.

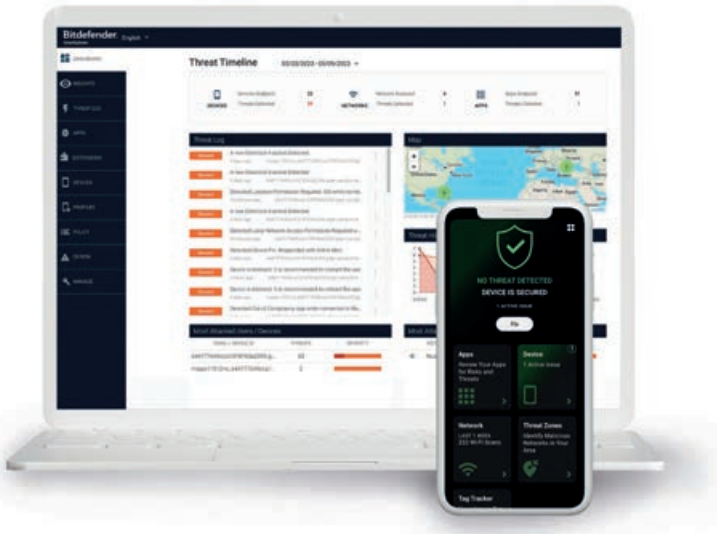
➤ Abwehr über die gesamte Kill Chain hinweg – Mobile Geräte sind häufig Ausgangspunkt, um Informationen über die IT-Infrastruktur zu sammeln und Angriffe gezielt zu planen. Eine MTD erkennt Angriffe auf Basis des MITRE ATT&CK Frameworks. Vorgehen gegen schlecht geschützte Konnektivitäten oder Man-in-the-Middle-Attacken erkennt nur eine auf mobile Risiken spezialisierte MTD.

➤ Überwachung mobiler Hardware – Nicht gepatchte Zero-Day-Schwachstellen, fehlende Verschlüsselung, Jailbreaking, Root-Access sowie nicht mehr aktualisierte Updates behebt eine Mobile Threat Defence.

Ein Teil der Gesamtcybersicherheit

Der Schutz mobiler Endgeräte ist Teil der Gesamtabwehr. Eine zentral verwaltete Mobile Threat Defence ergänzt komplementär bereits vorhandenes Mobile Device Management (MDM), Enterprise Mobility Management (EMM), Unified Endpoint Management und Security-Information-and-Event-Management (SIEM)-Systeme. Cloud-basiert lässt sich der Schutz sehr einfach und im laufenden Betrieb auf allen mobilen Endpunkten einrichten. Diese neue Transparenz hilft Unternehmen, den Status von Datenschutz und Sicherheit einschließlich der installierten Apps auf mobilen Geräten genau zu kennen und für die Compliance zu dokumentieren.

(Quellen) (1) Statista-Angaben, (2) Gartner, Market Guide for Mobile Threat Defense, 10 January 2023



Überwachung mobiler Geräte für Unternehmen durch Gravity Zone Security for Mobile.
(Foto: Bitdefender)

Bitdefender
www.bitdefender.de

Service Level Objectives

IN SIEBEN SCHRITTEN SLOs FÜR LEGACY SYSTEME DEFINIEREN

Das Festlegen von Service Level Objectives (SLOs) für große und historisch gewachsene Legacy Systeme ist eine echte Herausforderung. Welche Funktionen beziehungsweise Transaktionen sollten überwacht werden? Welche Komponenten spielen bei geschäftskritischen Prozessen eine Rolle? Und wie erreicht man die richtigen Qualitätsziele hinsichtlich Zuverlässigkeit und Performance in einer komplexen und verteilten Systemlandschaft?

Dr. Sina Niedermaier, Lead Consultant bei Exxeta, hat sich nach einem schweren IoT-Systemausfall mit ihrem Team genau diese Fragen gestellt und die betriebliche Ausfallsicherheit von einem Legacy System verbessert. Doch sie wollten nicht nur das Problem beheben, sondern das System strategisch für die Zukunft optimieren. Dabei fehlte ihnen zunächst jedoch ein tiefgreifendes Verständnis zur Funktionsweise und Nutzung des Systems. Genau hier setzt die Definition von SLOs an.

SLOs sind Zielwerte für die Zuverlässigkeit und Performance eines Dienstes. Sie orientieren sich an der Nutzererfahrung und werden mithilfe von Service Level Indicators (SLIs) gemessen. Diese Indikatoren zeigen verschiedene relevante Aspekte auf, wie beispielsweise die Anzahl fehlgeschlagener Transaktionen oder eine verringerte Servicequalität.

Schritt für Schritt zum Erfolg

Inmitten der Fülle an Informationen und Ansätzen kann die Definition dieser SLOs eine komplexe Aufgabe sein. Mit den folgenden sieben Schritten können Systeme erfolgreich beobachtet und Optimierungspotentiale erkannt werden.

#1 Bestimmung der geschäftskritischen Transaktionen (Critical User Journey)

Aus Sicht von Nutzenden sind die von der Anwendung bereitgestellten Funktionen oder Features von unterschiedlicher Bedeutung und können dementsprechend unterschiedliche Zuverlässigkeitsanforderungen haben. In unserem IoT-Anwendungsfall war die von den Benutzenden geforderte Zuverlässigkeit für die historischen Daten eines IoT-Services viel geringer als für die Alarmierungsfunktion.

Um mit einer Funktion einen Mehrwert zu schaffen, führen verschiedene Komponenten Funktions- und Methodenaufrufe durch. Diese logische Funktionseinheit, die sich über verschiedene Komponenten erstreckt, wird durch das Konzept der Transaktionen abstrahiert. Die kritischen Geschäftstransaktionen

müssen entsprechend identifiziert und nach ihrer Bedeutung für Benutzer eingestuft werden.

#2 Wo beginnen Transaktionen und wo enden sie?

Instrumentierung von Anwendung und Tracing von Transaktionen In Microservice-Systemen durchlaufen die Transaktionen in der Regel verschiedene Komponenten des Systems. Vor allem bei Legacy Systemen sind den Entwicklern die Pfade, die eine Transaktion durch das System nimmt, oft nicht ausreichend bekannt. Dies gilt insbesondere für Engpässe in kritischen Pfaden. Dieses Problem wird im Kontext von Microservice-Architekturen noch weiter verstärkt, bei denen Services über mehrere Teams hinweg entwickelt und betrieben werden.

Zunächst sollte daher mit der Modellierung eines initialen Message Sequence Diagramm begonnen werden, das die ungefähre Abarbeitung einer Transaktion über die Komponenten eines Systems abbildet. Sobald ein grober Überblick über die wichtigen Komponenten besteht, die an der Verarbeitung einer Transaktion beteiligt sind, können die Komponenten instrumentiert werden. Durch die Instrumentierung der Komponenten und Verwendung der Technologie des Distributed Tracings kann die Abarbeitung von Transaktionen über die Komponenten durch ein System rekonstruiert und damit beobachtbar gemacht werden. In Legacy Systemen ist dies besonders wertvoll, weil es eine Art 'Reverse Engineering' des Systems und deren Abhängigkeiten ermöglicht.

Weit verbreitete Open-Source-Systeme für Distributed Tracing sind etwa Zipkin und Jaeger.

#3 Definition des Systems von Anfang bis Ende

Das System muss ganzheitlich definiert werden, wobei ermittelt wird, welche Komponenten des Systems tatsächlich beobachtet und überwacht werden sollten. In dem zuvor genannten Beispiel gab es ein Mobile Team und ein Backend-Team. Um einen Mehrwert über die IoT-Anwendung für Benutzer zu schaffen, mussten beide Teams geeignet zusammenarbeiten. Sie verfügten jedoch weder über ein gemeinsames Monitoring noch über ein gemeinsames Leistungsversprechen. Dies führte dazu, dass das Backend-Team nur das Backend in Betracht zog, wenn es über den Service und den Zustand des Systems nachdachte. Für den Anwendungsfall der Alarmierung bedeutete dies, dass ein Alarm für das Backend erfolgreich war, wenn er vom Messaging Service akzeptiert wurde, aber die Zustellung an die mobile App wurde nicht beobachtet.

GEEIGNETE SLOs, DIE DIE NUTZER PERSPEKTIVE ABBILDEN, IST KEINE EINMALIGE AUFGABE, SONDERN ERFORDERT KONTINUIERLICHE ITERATIONEN UND EINE DYNAMISCHE SOWIE UMFASSENDE ANALYSE UND ANPASSUNG AN DEN SICH STÄNDIG ÄNDERNDEN NUTZUNGSKONTEXT.

Dr. Sina Niedermaier, Lead Consultant, Exxeta, www.exxeta.com

Dieser Punkt stellt dar, wie wichtig es ist, ergebnisorientiert vom Nutzenden her zu denken. Im Fokus sollten der Wert und die Qualität der Gesamtleistung stehen und nicht nur der Output lokaler Komponenten. Dazu sollten das System und die Transaktionen ganzheitlich definiert werden – von der mobilen App über das Backend bis hin zum physischen Sensor.

#4 SLIs ermitteln und erste SLOs für jede Art von Transaktion definieren

Für jede Art von Transaktion können spezifische Service Level Indicators (SLIs) ermittelt werden, die die Zuverlässigkeit und Performance des Systems quantifizieren. Bei Request/Response-Systemen sind gängige SLIs beispielsweise die Erfolgsrate oder die Antwortzeiten. Basierend auf Hypothesen über die Benutzeranforderungen können nun erste Schwellenwerte für diese SLIs festgelegt und diese anschließend präzisiert werden, indem Service Level Objectives (SLOs) definiert werden.

Eine wichtige Lektion für uns bei der Arbeit mit Legacy Systemen war es, zu Beginn, die Anzahl der SLOs so gering wie möglich zu halten, um die Komplexität zu reduzieren und den Fokus zu schärfen. Hierbei empfehlen wir, mit zunächst sehr toleranten SLOs zu beginnen und diese schrittweise zu verschärfen, sobald ein solides Verständnis dafür besteht, welche Zuverlässigkeit und Performance tatsächlich garantiert werden kann und von den Nutzern akzeptiert wird.

#5 Performance SLIs messen und mit SLOs vergleichen

Sobald die Komponenten instrumentiert sind, lassen sich die verarbeiteten Transaktionen während des Betriebs beobachten. Durch Aggregation der

Trace-Daten können nun Fragen beantwortet werden wie: Wie viele Transaktionen waren erfolgreich und wie viele sind fehlgeschlagen? Wie lange haben bestimmte Transaktionen gedauert? Was waren die Antwortzeiten? So kann die tatsächliche Performance mit den ursprünglichen Zielwerten SLOs verglichen werden.

Darüber hinaus können mit Hilfe von Distributed Tracing die Stellen ermittelt werden, an denen Transaktionen fehlschlagen, und das Team kann proaktiv eingreifen, bevor Benutzer Qualitätsmängel oder Fehler feststellen. Außerdem unterstütze der Einsatz von Distributed Tracing bei der Analyse von existierenden und potentiellen Performancengpässen in Anwendungen.

#6 Schrittweise auf geeignete SLOs hinarbeiten

Geeignete SLOs, also Zielwerte, die die Nutzer Perspektive abbilden, ist keine einmalige Aufgabe, sondern erfordert kontinuierliche Iterationen und eine dynamische sowie umfassende Analyse und Anpassung an den sich ständig ändernden Nutzungskontext. Auch wenn dieser Punkt sehr aufwändig ist, sind wir der Meinung, dass sich die Aufwände darin sehr lohnen, da die Anwendung von SLOs und Distributed Tracing transformativ sein kann. Diese Aktivität ermöglicht es Unternehmen und DevOps Engineers, die Verantwortung für die Erfahrungen ihrer Benutzer zu übernehmen, unabhängig davon, wie verteilt und komplex die Systeme sind.

#7 Kritische Pfade in Systemen identifizieren und Fehlertoleranz schaffen

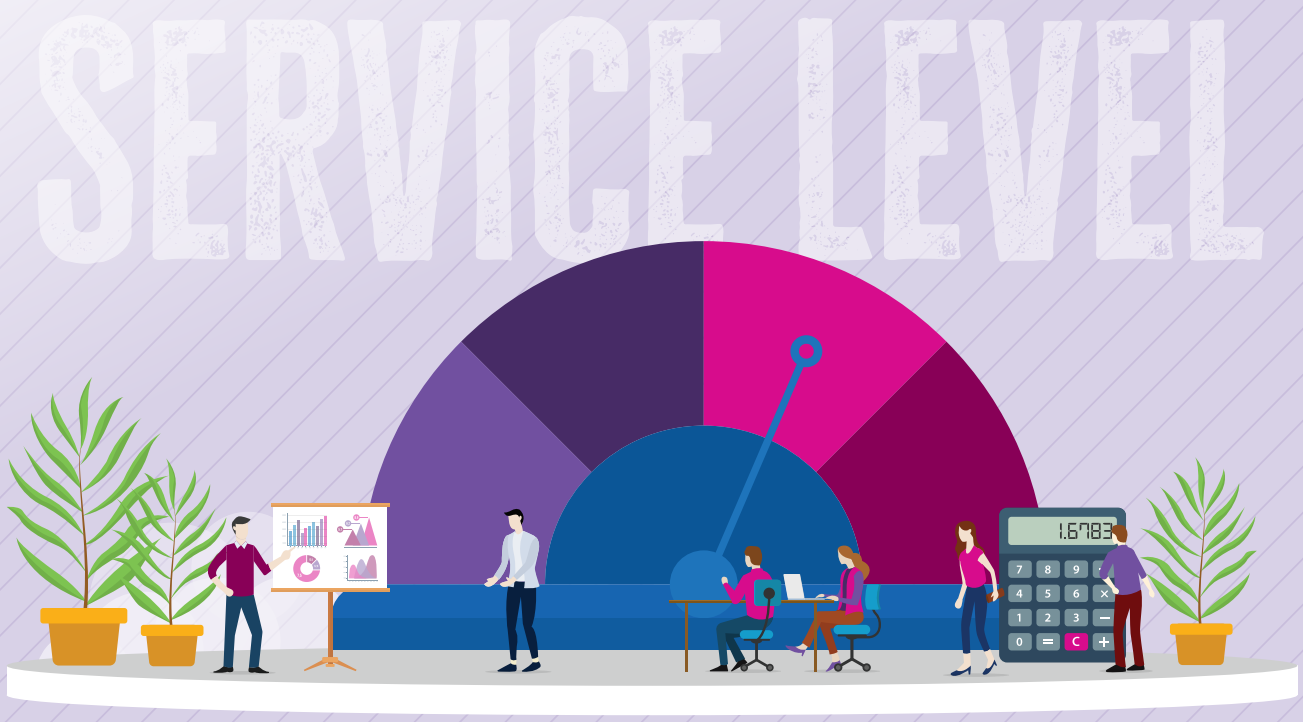
Unser Anwendungsfall bei dem Legacy System bestand darin, Benutzer vor einem für Ihre Assets kritischen Zustand zu warnen. Nachdem geklärt war, welche Teile des Systems an der Durchführung dieser Alarmierung beteiligt sind, wurde ein Konzept für ein redundantes Alarmierungssystem in einer Public Cloud erstellt und umgesetzt. Diese dringend benötigte Redundanz für die kritischen Transaktionen ermöglicht es dem System, Benutzer auch dann zu alarmieren, wenn eine der Hauptimplementierungen ausfällt.

So können durch einen gewissen Grad an Beobachtbarkeit kritische Teile und Engpässe bei Transaktionen identifiziert und die Robustheit und Fehlertoleranz von Systemen iterativ durch Redundanzen oder Resilienz-Designmuster, zum Beispiel mit Bulkheads oder Circuit Breakers, erhöht werden.

Fazit

Zusammenfassend kann mit diesem Grad an Beobachtbarkeit und geeigneten SLIs kontinuierlich überprüft werden, ob ein System wie erwartet funktioniert und den Nutzern eine akzeptable Service Qualität bietet. Diese Vorgehensweise führt von einer reaktiven und durch den Nutzenden initiierten Ausfallerkennung zu einer proaktiven, auf Beobachtung basierenden Fehlererkennung, die es ermöglicht, die notwendigen Fehlerreaktionen durchzuführen, um ein optimales Nutzungserlebnis zu gewährleisten.

Dr. Sina Niedermaier



Cloud-PAM

WENN PRIVILEGED ACCESS MANAGEMENT-LÖSUNGEN AN IHRE GRENZEN STOSSEN

vor zu den drängendsten Herausforderungen, die Unternehmen zu bewältigen haben. Da Kunden zunehmend auf Hybrid- und Multi-Cloud-Umgebungen umsteigen, die lokale Systeme und Elemente aus den Angeboten mehrerer öffentlicher Cloud-Anbieter kombinieren, nimmt die Komplexität weiter zu. Klassische PAM-Tools, die nicht speziell für den Einsatz in diesen Umgebungen entwickelt wurden, sind dieser Aufgabe in der Regel nicht gewachsen. Selbst wenn sich diese auf die Cloud anpassen ließen, würden sie in den meisten Fällen nur in der Umgebung eines Anbieters funktionieren – mit eingeschränkter Funktionalität und einer umständlichen Architektur.

Einschränkungen in der Cloud

Entscheidungsträger, die verstehen, dass Identität der neue Perimeter ist, werden Identity Governance und PAM als zentrale Funktionen betrachten. Traditionelle PAM-Technologien verarbeiten privilegierte Konten normalerweise, indem sie die Anmeldeinformationen von Administratorkonten in einem digitalen Tresor speichern. Diese Tools gewährleisten dann privilegierten Konten Rechte für den Zugriff auf Ressourcen. Typischerweise sind diese Rechte weder zeitlich noch aufgabenbegrenzt. Stattdessen verfügen sie über ein sogenanntes Dauerprivileg. Diese Lösungen scannen Umgebungen in regelmäßigen Abständen, jedoch sind die Intervalle nicht für dynamische Cloud-Umgebungen konzipiert, in denen neue Dienste und Arbeitslasten binnen kürzester Zeit skaliert werden können. Darüber hinaus fehlen ihnen die Fähigkeiten, die für den Umgang mit Cloud-basierten Identitäten und Maschine-Maschine-Kommunikation erforderlich sind. Sie wurden nicht für die Gerätekommunikation im IoT entwickelt.

Cloud-Umgebungen erfordern neue Möglichkeiten zur Verwaltung von Identitätslebenszyklen bei gleichzeitiger Wahrung der Transparenz über Hybrid- und Multi-Cloud-Ökosysteme hinweg sowie Methoden zur Verwaltung von Geheimnissen und privilegierten Konten in hochautomatisierten Test- und Produktionsumgebungen. Privilegierte Maschinenidentitäten müssen dynamisch sowie zeit- und funktionsbegrenzt verwaltet werden. Hier kommt Cloud PAM ins Spiel.

Mit Cloud PAM Risiken reduzieren

Cloud Privileged Access Management wurde entwickelt, um den Just-in-Time-Zugriff und ZSP-Paradigmen durchzusetzen. Saviynt Cloud PAM automatisiert die Entscheidung darüber, ob bestimmte Zugriffsanfragen gewährt werden sollten, und übergibt komplexere Anfragen zur Prüfung an einen Menschen. So können Fehler vermieden, Zeit gespart und die Verwaltungskomplexität verringert werden. Cloud PAM ist in der Lage, risikobasierte Business Intelligence nahtlos in Genehmigungsworkflows zu integrieren. Dabei lässt es sich nativ in DevOps-Tools sowie in die Kommunikationsplattformen, wie Slack und Microsoft Teams, einbetten. CPAM funktioniert auch bi-direktional mit SIEM-Plattformen (Security Information and Event Management) sowie anderen Infrastrukturen für Sicherheitswarnungen und kann problemlos mit Identity-Governance-Lösungen kombiniert werden.

Frank Schmaering

SAVIYNT

WIR GLAUBEN AN DIE NUTZUNG NATIVER CLOUD-TECHNOLOGIEN ZUM AUFBAU EINER PLATTFORM, DIE EBENSO FLEXIBEL WIE BELASTBAR IST UND ALS SERVICE BEREITGESTELLT WERDEN KANN.

Frank Schmaering, Senior Solutions Engineer, Saviynt, https://saviynt.com/

On Prem oder Cloud?

TENDENZ NACH OBEN

Mittelständische Unternehmen stehen ebenso wie große Unternehmen verstärkt im Visier von Hackern. Sie benötigen eine umfassende Security-Strategie und zunehmend externe Hilfe. Viele liebäugeln daher mit der Cloud, bevorzugen aber aufgrund von internen Regularien oder von Unsicherheit On-Premises-Lösungen. Security-Anbieter können diese Bedürfnisse aufgreifen und lokalen Schutz bereitstellen, der später einfach in die Cloud migrieren kann.

Eine On-Premises-Abwehr bietet bis zu einem gewissen Grad einen grundlegenden Schutz. Next Gen Antivirus bleibt relevant, weil es automatisierte und signaturbasierte Angriffe zuverlässig abwehrt. Zur Grundausstattung gehören zudem Firewalls und Identity-Access-Management-Lösungen. Diese verhindern die Veränderung von Privilegien als Grundlage für unberechtigte Aktionen.

Den Endpunkt schützen

Komplexe Attacken verlangen nicht nur eine zeitgemäße Abwehr, sondern auch ein schnelles Erkennen von bereits aktiven Angriffen, die die erste Abwehr-Instanz bereits überwunden haben. Egal ob der Anwender sich am Arbeitsplatz, unterwegs oder im Homeoffice befindet und Zugriff auf die Unternehmens-IT und Applikationen hat - immer häufiger erfolgen Angriffe über einen dieser Wege und haben den Endpunkt zum Ziel.

Eine klassische Endpoint Detection and Response schützt Endpunkte – in vielen Fällen eine hinreichende Abwehr. Komplexe Angriffe wie etwa Advanced Persistent Threats werden aber nur über das übergreifende Monitoring aller Endpunkte, Netzwerksegmente und Cloud-Instanzen hinweg sichtbar. Gerade in der ersten Phase eines Angriffs werden vorbereitende Maßnahmen der Angreifer erst durch anomales Verhalten am Endpunkt und/oder im Netzwerk bemerkt. Nur eine Erkennung und Bewertung von Vorgängen im gesamten Kontext der IT-Infrastruktur ermöglicht eine hinreichende Sichtbarkeit und eine präventive Blockade oder wenigstens die Eindämmung komplexer Angriffe. Unternehmen mit geringen Ressourcen benötigen für das Arbeiten mit einer solchen Extended-Endpoint-Detection-and-Response-Lösung (XDR) Sicherheitsexperten, die deren Alarme verstehen und zielgerichtet bearbeiten können. Angesichts des Fachkräftemangels sollten diese über ein externes Security Operation Center (SOC) im Rahmen einer Managed Detection and Response (MDR) unterstützt werden. Hier wird das lokale Team nicht nur um Spezialisten, sondern auch um hochwertige Security-Tools ergänzt. Der Vorteil: Diese haben nicht nur die Sicherheitslage eines Unternehmens im Blick, sondern auch die einer ganzen Branche oder Region.

GERADE IN DER ERSTEN PHASE EINES ANGRIFFS WERDEN VORBEREITENDE MASSNAHMEN DER ANGREIFER ERST DURCH ANOMALES VERHALTEN AM ENDPUNKT UND/ODER IM NETZWERK BEMERKT.

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

On Premises mit Perspektive Cloud

XDR und MDR sind also notwendig für ein zukunftsfähige, resiliente IT. Ihr Zusatznutzen ist über On-Premises-Lösungen aber nicht abbildbar. Die notwendigen XDR-Sensoren oder auch Sandboxing würden enorme Ressourcen benötigen. Nicht alle IT-Sicherheitsverantwortlichen können und wollen diesen Weg gehen, vor allem aus regulatorischen Gründen, oft aber schlicht aus Unsicherheit oder gar Unkenntnis.

Für das notwendige Mehr an Sicherheit sollten IT-Administratoren die Migration in die Cloud auf eine umfassende Sicherheitsplattform im Blick haben. Ein Problem mit der DSGVO ist beim Weg in die Cloud dabei in der Regel nicht gegeben. Experten in einem SOC lesen keine personenbezogenen Daten aus, sondern analysieren den Hashwert einer Datei, der in einem EU-Rechenzentrum verbleibt. Im äußersten Fall landet eine Gesamtdatei in einer Sandbox im EU-Rechenzentrum, die dann gleich wieder entfernt wird.

Jörg von der Heydt

protekt 2023

KRITIS-KONFERENZ ERWEITERT ANGEBOT

protekt
8.–9.11.2023
leipzig
konferenz für den schutz kritischer infrastrukturen

Aufgrund von Krisen und den weltpolitischen Entwicklungen hat der Schutz kritischer Infrastrukturen in den vergangenen Jahren massiv an Bedeutung gewonnen. Umso wichtiger ist es deshalb für Betreiber kritischer Infrastrukturen, ihre Unternehmen bestmöglich vor Gefahren zu schützen und resilienter zu machen. Die protekt (8. bis 9. November in Leipzig) bietet dafür die besten Voraussetzungen, denn sie ist die einzige auf den Schutz kritischer Infrastrukturen spezialisiere Konferenz in Deutschland. In diesem Jahr wird die protekt erstmals in vier parallelen Tracks Expertise vermitteln. Neben den etablierten Tracks Cyber- und Informationssicherheit, Physische Sicherheit und Workshops widmet sich ein neuer Strang am ersten Konferenztag Praxisberichten aus dem Umsetzungsplan kritische Infrastrukturen (UP KRITIS). Dessen Vorträge werden in Kooperation mit dem Bundesamt für Sicherheit in der Informationstechnik (BSI) vorbereitet.

Zu den Highlights im Konferenzprogramm der protekt 2023 zählen Vorträge, die sich mit dem Schutz bestimmter KRITIS-Bereiche beschäftigen. So spielen etwa die Absicherung von LNG-Terminals, die Sicherheit von Lieferketten und die Bedeutung der Trinkwasserversorgung eine wichtige Rolle. Prominente Vertreter aus der Politik und aus KRITIS-relevanten Institutionen bereichern die protekt 2023 mit Keynotes und in der begleitenden Ausstellung präsentieren Unternehmen ihre Produkte und Lösungen.

www.protekt.de

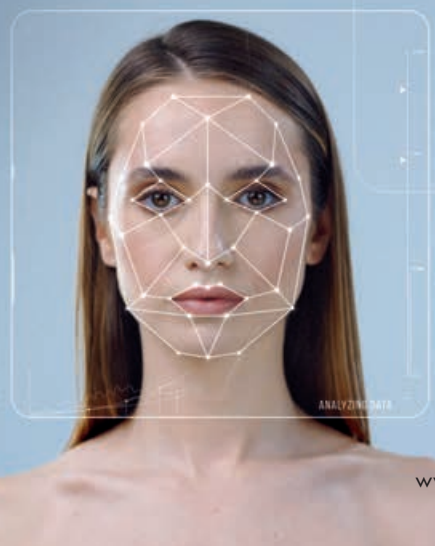
Tickets für die protekt sind ab sofort hier erhältlich: www.protekt.de/ticket – bis zum 20. September zum Frühbucherrabatt.

Deepfakes

TÄUSCHEND ECHT, ABER ALLES LÜGE

Der angebliche Papst in weißer Daunenjacke, die vermeintliche Verhaftung Trumps oder Franziska Giffeys Gespräch mit einem falschen Klitschko – was auf den ersten Blick täuschend echt aussieht, entpuppt sich im Nachhinein als sogenanntes Deepfake. Dabei handelt es sich um Bilder, Audios oder Videos, die täuschend echt verändert oder verfälscht werden.

Bei vielen Menschen führen Deepfakes zu Verunsicherung: 8 von 10 Deutschen (81 Prozent) sagen, sie würden ein Deepfake nicht erkennen. 44 Prozent geben an, schon einmal auf ein Deepfake reingefallen zu sein. 70 Prozent sind der Meinung, Fotos und Videos könne man heute nicht mehr vertrauen und 63 Prozent sagen sogar, Deepfakes machten ihnen Angst. 60 Prozent sehen in Deepfakes eine Gefahr für unsere Demokratie. Andererseits sieht über die Hälfte auch positive Einsatzmöglichkeiten: 55 Prozent sind der Meinung, Deepfakes könnten sinnvoll genutzt werden, etwa im Kino oder in der Kunst.



Den allermeisten sind Deepfakes bisher in Informationssendungen begegnet: 63 Prozent sagen, sie haben Deepfakes in Berichterstattungen über das Thema gesehen. Nur 2 Prozent haben im Internet Deepfakes erkannt, die nicht als solche gekennzeichnet waren. 8 Prozent sind auf Deepfakes gestoßen, die als solche gekennzeichnet waren. Und 3 Prozent haben selbst schon einmal eine Software ausprobiert, mit der man Deepfakes erstellen kann.

Eine breite Mehrheit (84 Prozent) fordert eine Kennzeichnungspflicht für Deepfakes, 60 Prozent sagen, sie sollten ganz verboten werden.

www.bitkom.org

Effektives Risikomanagement

UNZUREICHENDE KOLLABORATION ERSCHWERT MANAGEMENT DES EXTERNEN CYBER-RISIKOS

Die Ansprüche an ein effektives Risikomanagement der externen Angriffsfläche, die ein Unternehmen über aus dem Internet erreichbare IT-Assets bietet, und die reale Situation klaffen in Unternehmen weit auseinander. Zu diesem Schluss kommt ein vom Analystenhaus Forrester erstellter Thought Leadership Report, der von CyCognito in Auftrag gegeben wurde.

Gründe für erhöhtes Risiko

Unentdeckte Sicherheitslücken in über das Internet erreichbare Assets, bergen ein enormes Risiko für die IT-Sicherheit von Unternehmen. Gleichzeitig entsprechen aktuelle Risikomanagementpraktiken für das Identifizieren, Priorisieren und Beheben dieser Schwachstellen selten den Erwartungen der Verantwortlichen. Obwohl 81 Prozent der Befragten Sicherheitstests, -prozesse oder -übungen zur Aufdeckung von Schwachstellen in Sicherheitskontrollen und -mechanismen als wichtiges Instrument des Risikomanagements einstufen, wurden bei 53 Prozent im Zuge der letzten Risikobewertung eine beträchtliche Anzahl unentdeckter externer Assets gefunden.

Diese Diskrepanz liegt gemäß Forrester vor allem an unzureichender interner Zusammenarbeit – ein Umstand, der sich anhand mehrerer Ergebnisse zeigt. Ein Indikator ist die Heterogenität der Tool-Landschaft: Fast 40 Prozent der teilnehmenden Unternehmen nutzen mehr als zehn verschiedene Tools, die sich über mehrere Teams verteilen und unabhängig voneinander zum Einsatz kommen, statt die Erkenntnisse allen Beteiligten zur Verfügung zu stellen. Diese „Silos" erschweren die nötige Kommunikation und Kollaboration. Nur 22 Prozent der Befragten haben ein bereichsübergreifendes Team, das für eine effektive Priorisierung von Gegenmaßnahmen zuständig ist. Das führt dazu, dass es in einem von vier befragten Unternehmen mehrere Wochen oder sogar länger dauert, auf neue, mitunter hohe Risiken zu reagieren. Generell bewerten 40 Prozent der Befragten die Beziehungen der involvierten Teams für Security, IT und Business untereinander als durchgängig negativ.

Abhilfe schaffen

Um das Risiko von Sicherheitslücken in externen Assets durch eine schnelle Erkennung, Priorisierung und Behebung effektiv senken zu können, sollten Unternehmen laut dem Report zwei Maßnahmen ergreifen. Erstens sollte für das Erfassen und die Bewertung von Risiken eine unternehmensweite Single Source of Truth existieren, also eine einzige Informationsquelle, die von allen Beteiligten genutzt und permanent auf dem neuesten Stand gehalten wird. Die dafür nötige Zusammenarbeit verbessert außerdem die Stimmung zwischen den Teams und hat auch einen direkten Einfluss auf die MTTR.

Erleichtert wird dieses Ziel durch eine zweite empfohlene Maßnahme: Die Einführung einer zentralen Lösung für die Risikominderung, die wichtige Kernaufgaben automatisiert und kontinuierlich durchführt. Dazu gehört das durchgängige Abbilden von Geschäftsstrukturen, regelmäßige Sicherheitstests, die auch „blinde Flecken" finden, und das korrekte Zuordnen von Assets. Diese Maßnahmen erlauben eine einheitliche Betrachtung der externen Angriffsfläche, eine Priorisierung und Planung von Gegenmaßnahmen – und damit ein effektives Risikomanagement.

www.cycognito.com

MEHR WERT

Der gesamte Report kann hier heruntergeladen werden

Die eigene Sicherheitslage voll im Griff

EXPOSURE MANAGEMENT UND SECURITY VALIDATION

Die sich ständig verändernde Cybersicherheitslage eines Unternehmens stets im Blick und Griff zu behalten, stellt für die meisten IT-Sicherheitsteams eine echte Herausforderung dar. Sie müssen Sicherheitslücken erkennen und schließen, bevor sie ausgenutzt werden können, die implementierte IT-Sicherheitsarchitektur testen und prüfen, bevor ein Angriff erfolgt. Exposure Management und Security Validation können ihnen hierbei eine wertvolle Stütze sein.

> UNTER ZUHILFENAHME EINER EXPOSURE MANAGEMENT- UND SECURITY VALIDATION-PLATTFORM-LÖSUNG KANN DIE SICHERHEITSARCHITEKTUR EINES UNTERNEHMENS ERFOLGREICH PROAKTIV OPTIMIERT WERDEN.
>
> **Torsten Wiedemeyer, Country Manager DACH & Central & Eastern Europe, Cymulate, www.cymulate.com**

Exposure Management

Die Ressourcen von IT-Sicherheitsteams sind begrenzt. Nicht immer kann eine neu entdeckte Sicherheitslücke sofort behoben werden. Das Ziel der IT-Sicherheit hat es deshalb zu sein, auf Basis eines umfassenden Kosten-Nutzenvergleichs mit den vorhandenen Ressourcen das bestmögliche Ergebnis für die Sicherheitslage zu erzielen. Lösungen zum Exposure Management helfen ihnen dabei, potenzielle Schwachstellen und Sicherheitslücken zu identifizieren und hinsichtlich ihrer Bedeutung für die IT – aber auch das Unternehmen als Ganzes – einzuordnen, zu priorisieren und zu beheben.

Security Validation

Um sicher gehen zu können, dass die implementierten Sicherheitsmechanismen optimal konfiguriert sind, müssen diese regelmäßig auf ihre Einsatzfähigkeit im jeweiligen IT-Ökosystem hin überprüft werden. Mittels Security Validation kann die Wirksamkeit von Sicherheitsmechanismen im Hinblick auf Bedrohungsaktivitäten in lokalen, Cloud- und hybriden Umgebungen objektiv bewertet werden. Dies ermöglicht effektivere und effizientere Optimierungen der IT-Sicherheit, sorgt für mehr Risikotransparenz und reduziert unnötige False Negative-Alarmmeldungen.

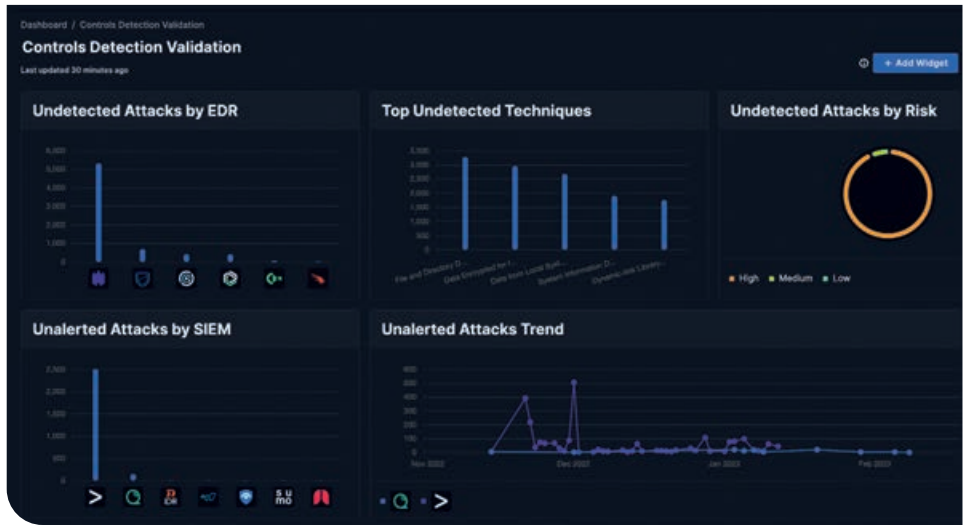
Cymulate Exposure Management und Security Validation Plattform

Die effektivste und effizienteste Art, eine Exposure Management- und Security Validation-Lösung zum Einsatz zu bringen stellen derzeit automatisierte Plattformlösungen dar. Mit der Cymulate-Plattform erhalten IT-Sicherheitsteams einen vollständigen Überblick über ihre Sicherheitslage und die Risiken für ihren Betrieb – kontinuierlich und automatisiert. Sie erhalten genau die Informationen, die sie benötigen, um ihre Sicherheitslage erfolgreich zu optimieren – abgestimmt auf die realen Verhältnisse ihres jeweiligen Unternehmens.

Fazit

Unter Zuhilfenahme einer Exposure Management- und Security Validation-Plattformlösung kann die Sicherheitsarchitektur eines Unternehmens erfolgreich proaktiv optimiert werden – ohne Abstriche bei der Effektivität oder Effizienz machen zu müssen.

Torsten Wiedemeyer



Cymulate

Security Orchestration perfektioniert

SOC, SIEM, SOAR, PLAYBOOKS, MDRS SORGEN FÜR EINEN BESSEREN SCHUTZ

Das Feld der Informationssicherheit hat sich in den letzten Jahren stark gewandelt und ist heutzutage komplexer denn je. Zusammen mit der stark gewachsenen Bedrohungslage ist auch die Anzahl und Komplexität der eingesetzten Security-Produkte gestiegen. In vielen Unternehmen haben sich daher interne Security Operations Centern (SOC) als zentrale Stelle zur Sicherstellung der Informationssicherheit und Eindämmung aufkommender Vorfälle etabliert – oder es wird auf die Dienstleistung Dritter zurückgegriffen.

Es verwundert nicht, dass SOC-Mitarbeiter heute mit vielen verschieden Produkte arbeiten. Sie müssen dabei auf eine Vielzahl von Informationsquellen zurückgreifen und in der Lage sein, Sachverhalte schnell korrekt zu bewerten. Eine der größten Herausforderungen besteht darin, sicherheitsrelevante Ereignisse mit der angemessenen Priorität zu bearbeiten und wertvolle Kapazitäten nicht für Events mit geringer Relevanz zu binden. Trotzdem muss man Security ständig hinterfragen und neu denken.

Kampf gegen die Alarmmüdigkeit

Um die anfallende Daten- und Ereignisflut nicht vollständig manuell analysieren zu müssen, haben sich zentrale Security Information and Event Management (SIEM)-Systeme etabliert. Solche SIEM-Systeme sammeln Daten aus verschiedenen Quellen innerhalb einer IT-Umgebung, etwa Logdaten und Ereignisdaten von Windows und Linux-Systemen, Firewalls, Anti-Virus-Lösungen und Anwendungen. Die besondere Stärke eines SIEM-Systems ist die Korrelation dieser Daten aus den unterschiedlichsten Quellen. Anhand vorher festgelegter Parameter sind SIEM-Systeme sogar in der Lage, Alarme zu generieren.

SOC-Mitarbeiter werden aufgrund solcher Alarme tätig und bearbeiten diese Ereignisse, nach den im Unternehmen festgelegten Verfahrensabläufen. Werden die Parameter zu lose definiert, können sicherheitsrelevante Ereignisse unerkannt bleiben. Eine zu enge Definition wiederum kann zu einer hohen Anzahl von Fehlalarmen führen. Das große Problem dabei: Fehlalarme binden Arbeitskraft und können dazu führen, dass echte kritische Ereignisse nicht rechtzeitig die notwendige Aufmerk-

samkeit erfahren, oder dass ein Event nicht als kritisch eingestuft wird, weil sich diese Art von Ereignis zuvor als Fehlalarm herausgestellt hat. Doch selbst legitime Alarme können zu kritischen Zuständen in einem SOC führen. Das ist etwa dann der Fall, wenn die aufkommende Ereignismenge die Kapazitäten des SOC überschreitet. Ereignisse können dann nicht mehr zeit- und sachgerecht bewältigt werden.

Ein neuer Ansatz: SOAR

Über die letzten Jahre hat sich deshalb ein neuer Ansatz in der Informationssicherheit entwickelt: Security Orchestration, Automation and Response (SOAR). Ein SOAR kann nicht nur die aufkommenden Ereignisse automatisch mit zusätzlichen Informationen anreichern, sondern bisher manuell zu erledigende Aufgaben teilweise oder sogar vollständig automatisieren. Durch ein SOAR können also erhebliche Effizienzsteigerungen erzielt werden. Die Reaktions- und Lösungszeit für auftretende Ereignisse wird dadurch wesentlich verbessert. Doch ein SOAR steigert nicht nur die Effizienz, sondern ermöglicht auch die Umsetzung vieler zusätzlicher Prozesse, die die Informationssicherheit im Unternehmen weiter erhöhen. Ein zusätzlicher positiver Effekt ergibt sich durch den Wegfall repetitiver Standardaufgaben. Das reduziert das Risiko für die gefürchtete Alarmmüdigkeit und erhöht die Motivation der Mitarbeiter.

Playbooks: Herzstück einer SOAR-Lösung

Eine SOAR-Lösung erweitert nicht nur die Fähigkeiten eines SIEM-Systems erheblich, sondern ergänzt die gesamte Informationssicherheit mit wertvollen Fähigkeiten. Im Zentrum einer SOAR-Lösung stehen vordefinierte Ablaufpläne, sogenannte Playbooks. Diese Playbooks können durch unterschiedliche Auslöser gestartet werden: zeitgesteuert, bei einem bestimmten Ereignis oder manuell durch einen SOC-Mitarbeiter, um nur einige von vielen denkbaren Möglichkeiten zu nennen.

Ein einzelnes Playbook kann dabei sehr einfach aufgebaut sein oder eine Vielzahl von Aktionen enthalten. Dabei muss ein Playbook nicht statisch definiert werden. Auch vielfältig verzweigte Aktionspfade, bei denen je nach Resultat eines Zwischenschritts einem anderen Pfad gefolgt wird, sind möglich. Moderne SOAR-Lösungen bieten bereits von Haus aus Unterstützung gängiger Security-Produkte, können aber auch auf Speziallösungen adaptiert werden.

Ein einfaches Beispiel für ein Playbook sehen wir in Bild 1.

Eine IoC (Indicator of compromise)-Quelle [3] wird regelmäßig [1] automatisiert auf kategorisierte IoCs vom Typ IP-Adresse, überprüft. Alternativ kann dieses Playbook von einem Analysten aus einem SOC-Dashboard heraus, ausgelöst werden. [2] Schlägt die Aufgabe fehlt, wird ein Ticket im angebundenen Ticketsystem generiert. [6] Werden zutreffende IoCs erkannt, erfolgt eine Blockierung dieser IP-Adressen an einer Perimeter Firewall. [4] Gleichzeitig wird eine Suche im SIEM auf Kommunikation interner Systeme mit den erkannten IP-Adressen ausgelöst. [5] Bei Treffern wird ein Scan der Endgeräteschutzsoftware auf den entsprechenden Clients gestartet [7] und gleichzeitig ein Ticket mit den entsprechenden Informationen generiert. [8] Fördert der automatisch gestartete Scan Malware zutage, wird die Netzwerkkommunikation des Gerätes unterbunden [9] und das Ticket mit den zusätzlichen Informationen aktualisiert. [10] Bleibt der Scan hingegen ohne Treffer, wird das Ticket mit diesen Informationen aktualisiert und geschlossen. [11]

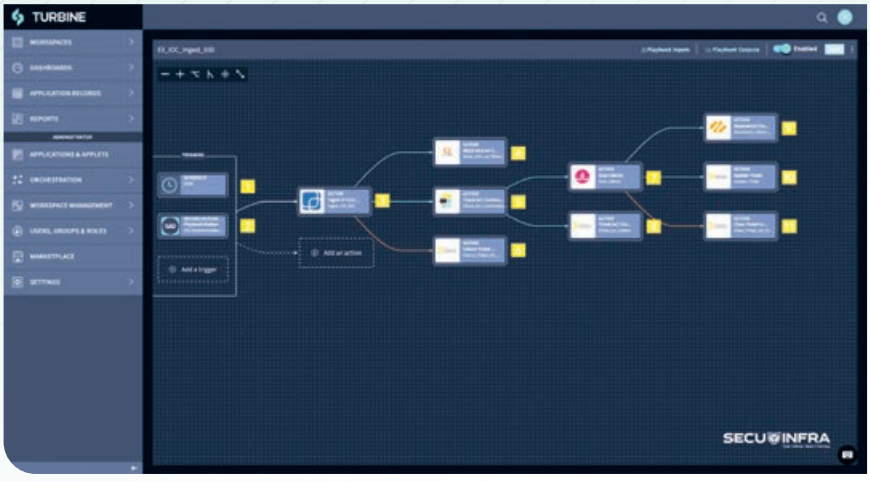


Bild 1: Ein einfaches Playbook wie dieses zeigt bereits die Möglichkeiten der Automatisierung.

(Bild: SECUINFRA / Swimlane)

Umsetzbar sind selbstverständlich diverse Variationen des oben genannten Beispiels. So kann etwa eine Sperre und Logprüfung automatisch ausgelöst werden, die Sperrung auf der Firewall aber erst nach vorheriger Prüfung durch einen Mitarbeiter – auf Knopfdruck – erfolgen.

Auf dem Weg zum eigenen SOAR

Eine modere SOAR-Lösung versetzt SOC-Analysten in die Lage, einen großen Teil Ihrer Arbeit auf der Oberfläche des SOAR-Systems selbst durchzuführen. Sie müssen für Standardaufgaben also nicht mehr auf eine Vielzahl verschiedener Oberflächen zugreifen. Dabei sind die Möglichkeiten einer modernen SOAR-Lösung äußerst umfangreich. Ein SOAR kann beispielsweise Ereignisse nicht nur automatisiert mit allen zur Fallbearbeitung notwendigen Zusatzinformationen anreichern, sondern sogar Tickets erstellen, ergänzen und schließen. Aufgaben, die zuvor mit vielen manuellen Arbeitsschritten verbunden waren, lassen sich nun automatisieren oder derart konfigurieren, dass diese erst nach der Bewertung durch den Analysten ausgelöst werden.

Ein modernes SOAR-System bietet zudem umfangreiche Möglichkeiten, Statistiken und Auswertungen zu erstellen, um auch Managementanforderungen gerecht zu werden. Solche Lösungen sind äußerst anpassungsfähig und können selbst mit umfangreichen Anforderungsänderungen Schritt halten. Der initialen Implementierung einer SOAR-Lösung muss dennoch immer eine sorgfältige Anforderungsanalyse und Planung vorausgehen. Nur dann lässt sich ein Zeit- und Kostenrahmen effektiv bestimmen, Frust bei Beteiligten vermeiden und eine sichere und effektive Umsetzung gewährleisten.

Bild 2: Das Dashboard bietet einen schnellen Überblick über die wichtigsten KPIs und Metriken.

(Bild: SECUINFRA / Swimlane)

Frust vermeiden

Fachbereiche im Unternehmen, die für eine erfolgreiche Implementierung notwendig sind, sollten dabei frühzeitig involviert werden. Besonderes Augenmerk sollte zudem auf der Ausarbeitung eines Rechte- und Rollenkonzepts liegen, welches ebenfalls so früh wie möglich erstellt und im laufenden Prozess stets aktuell gehalten wird.

Selbstverständlich müssen alle diejenigen Produkte, die an das SOAR angebunden werden sollen, bestimmt werden. Anschließend lassen sich Aufgaben festlegen, die das SOAR mit diesen Produkten mit vorheriger Benutzerinter-

aktion oder vollständig automatisiert durchführen soll. Es hat sich bewährt, die bereits vorhandenen Prozesse als Vorbild zu nehmen und gegebenenfalls zu adaptieren. In einem folgenden Schritt sollten Anwendungsfälle, die bisher aufgrund des entstehenden Aufwands nicht umgesetzt wurden, aber die Informationssicherheit im Unternehmen weiter verbessen, betrachtet und eingeplant werden.

Fazit

Ein zentrales Security Information and Event Management (SIEM) hat sich bewährt, um sicherheitsrelevante Daten aus verschiedenen IT-Systemen zu aggregieren. Allerdings können diese Datenflut sowie eine große Menge von Alarmen auch zum Problem werden. Security Orchestration, Automation and Response ist daher ein sinnvoller Lösungsansatz, um die Verarbeitung von Events zu automatisieren. Eine wichtige Rolle spielen dabei Playbooks, über die alle Prozesse gesteuert werden. Die Implementierung eines SOAR erfordert jedoch eine gründliche Planung, bei der alle Fachbereiche eines Unternehmens mit einbezogen werden sollten. Das erfordert zwar einen hohen initialen Aufwand, doch der Effizienzgewinn durch Automatisierung sowie die höhere IT-Sicherheit sind es allemal wert.

Alexander Schaum

SECURITY ORCHESTRATION, AUTOMATION AND RESPONSE (SOAR) IST EIN HERVORRAGENDER LÖSUNGSANSATZ, UM DIE VERARBEITUNG VON SECURITY-EVENTS ZU AUTOMATISIEREN.

Alexander Schaum,
Senior Cyber Defense Consultant,
Secuinfra GmbH, www.secuinfra.com/de/

Parallele Kompendien

HILFE FÜR DIE JÄHRLICHE WEITERENTWICKLUNG

Kennen Sie das auch? Sie haben gerade mal ein Kompendium innerhalb eines Jahres bearbeitet – und schon kommt das nächste. Wie können Sie hier unterstützt werden?

Zunächst müssen Sie die Kompendien übersichtlich darstellen. Dabei kann Ihnen ein Tool helfen, das die Bausteine und Anforderungen pro Kompendiumsjahr gut gegliedert abbildet. Und wenn Sie schon dabei sind, könnten Sie auch gleich noch Anforderungen mit Maßnahmen aus dem Datenschutz verknüpfen. Schließlich möchten wir ja auch unsere Kollegen mit umgesetzten Maßnahmen unterstützen.

Mit nur einem Update zur neuen Version

Hierfür kommt auch die Referenzliste des BSI zum Tragen. Welcher Baustein hat sich geändert, welche Anforderung? Was ist neu hinzugekommen? Passen meine alten Umsetzungskommentare noch? Diese Themen sollten, nein müssen Sie sich genauer ansehen.

Ein Tool kann hier eine Übersicht liefern. Aber halt: Ich habe mehrere Verbünde und möchte meinen Verbund für die bevorstehende Zertifizierung nicht anpassen, sondern nur den Verbund für die neuen Anwendungen. Genau an dieser Stelle muss das Tool die Möglichkeit bieten, pro Verbund das Jahr des Kompendiums zu schlüsseln. Mit dieser Schlüsselung können Sie dann den gewünschten Verbund auf einen neuen Kompendien-Stand anheben.

Durch die Anhebung erhält der Verbund neue Verbindungen. Die Verbindungen zu dem vorherigen Kompendium werden historisiert und neue Verbindungen zu dem aktuellen Kompendium geschaffen. Durch die Historisierung bleibt der Baustein immer erhalten, auch wenn er in einem neuen Kompendien-Stand entfallen sein sollte.

Was ein Tool „noch" nicht kann, ist die Zuordnung von neuen Bausteinen, die vorher nicht existierten. Hier dürfen Sie bei der Modellierung noch selbst Hand anlegen. Es gibt Typen für jede Ressource. Diesen Typen können Bausteine zugeordnet werden. Wenn nun beispielsweise eine Anwendung einem Typen zugeordnet wurde, erhält die Anwendung automatisch die neuen Bausteine, wenn Sie diese auch dem Typen zugeordnet haben.

WAS EIN TOOL „NOCH" NICHT KANN, IST DIE ZUORDNUNG VON NEUEN BAUSTEINEN, DIE VORHER NICHT EXISTIERTEN.

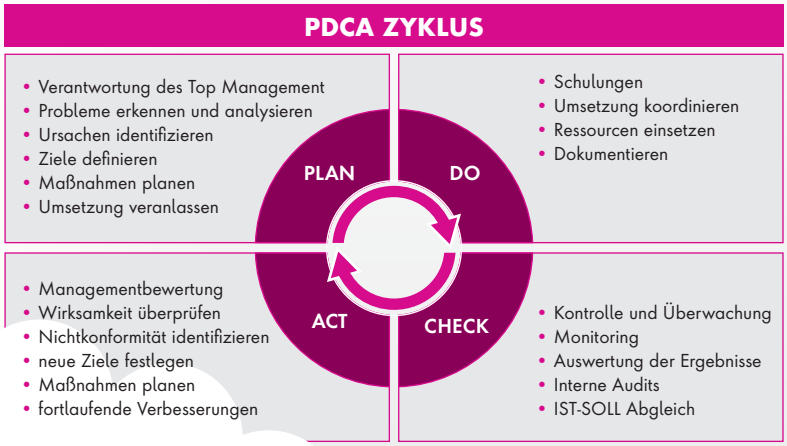
Sasche Kreutziger, Leiter Account-, Sales- und Marketingmanagement, HiScout GmbH, www.hiscout.com

Von der Modellierung zum GS-Check

Durch die angehobenen Verbünde und die damit entstandenen Verbindungen zum neuen Kompendium werden die neuen Anforderungen ebenfalls verbunden und die noch gültigen Anforderungen bleiben bestehen. Im Tool werden die geänderten und neuen Anforderungen neben der normalen Sicht auf alle Anforderungen dargestellt. Damit haben Sie die Wahl, ob Sie alles sehen möchten oder nur die Veränderungen. Wenn sich an der Anforderung nichts geändert hat, brauchen Sie die Umsetzungskommentare auch nicht mehr anfassen.

Jetzt schauen Sie sich die geänderten Anforderungen an. Ein Tool kann „noch" nicht automatisch entscheiden, ob Ihr Umsetzungskommentar ausreichend ist oder nicht. Hier stellt ein Tool die Anforderungstexte der vorherigen Version und der aktuellen Version zur Verfügung. Sie müssen selbst entscheiden, ob Ihre Kommentare auch noch auf die geänderte Anforderung Gültigkeit haben. Und was passiert mit den entfallenen Anforderungen? Ein Tool vergisst nur, wenn Sie es wollen. Stellen Sie einfach den Verbund auf 2022 um und Sie sehen alles mit diesem Kompendien-Stand.

Sascha Kreutziger



Cloud-Sicherheit

GEFAHREN EFFIZIENT HANDHABEN

Peter Sakal hat einen Master in Computer Science und arbeitet seit über 20 Jahren im Bereich Cybersecurity. Seit 3 Jahren ist er Manager für Cybersecurity & Dataprotection bei der TÜV SÜD Akademie. Mit seiner tiefgreifenden Expertise konnte er uns interessante Einblicke darüber geben, wie Unternehmen die Herausforderungen, die mit einer Cloud-Lösung einhergehen, meistern können.

it security: *Wieso ist die Cloud so wichtig für Unternehmen?*

Peter Sakal: Mithilfe der Cloud können innovative Geschäftsmodelle entwickelt werden, welche mithilfe von moderner IT-Infrastruktur agiler und skalierbarer denn je sind. Dennoch birgt die Cloud neue Risiken. Ihre Nutzung erfordert technische und organisatorische Veränderungen in nahezu allen Bereichen des Unternehmens. Informationssicherheits-, Compliance- und Datenschutzmaßnahmen müssen entsprechend ergänzt und angepasst werden.

> ERFOLGREICHE CLOUD-SECURITY IST DAS ERGEBNIS EINES ANDAUERNDEN PROZESSES.
>
> **Peter Sakal, Manager Cybersecurity & Dataprotection, TÜV SÜD, www.tuvsud.com**

it security: *Wie können sich Unternehmen vor diesen Gefahren schützen?*

Peter Sakal: Indem Sie einen CISO mit dieser Aufgabe betrauen. Die Rolle des CISO hat in den letzten Jahren massiv an Bedeutung gewonnen. Einem Angreifer reicht eine einzige Schwachstelle, um erfolgreich zu sein. Der CISO und sein Team müssen eine 360-Grad-Sicht einnehmen, um ein konstant hohes Sicherheitsniveau auf allen Ebenen der Organisation zu gewährleisten. Nur mit einer umfassenden Strategie lassen sich IT-Ausfälle, Cyber-Attacken, Verstöße gegen Datenschutzbestimmungen oder finanzielle Verluste durch Bußgelder und Rufschäden vermeiden.

Ein wichtiger Bestandteil dieser Strategie ist die Risikobewertung zur Erfüllung von Compliance-Anforderungen (beispielsweise Datenschutz, IT-Sicherheitsgesetz, Telemedien-/Urheberrechtsgesetz) und Informationssicherheitsanforderungen (BSI-Grundschutz und die ISO/IEC 27000 Serie). Der Plan-Do-Check-Act-Zyklus (siehe Grafik) bildet die Grundlage des gesamten Prozesses. Compliance-Anforderungen und Risiken in der Cloud sind dabei auf verschiedene Ebenen zu beachten:

- Gesetze im Land der Cloud-Betreiber, mit Einwirkung auf die Daten (auch auf EU-Servern).
- Datenverfügbarkeit hängt allein vom Cloud-Provider ab.
- Angriffsfläche bei Cloud-Strukturen ist häufig größer als On-Premises, Cyberrisiken wie Ransomware nehmen rasant zu.
- Datenlöschung in der Cloud ist häufig intransparent.
- Erhöhtes Risiko für Regelverstöße, da Mitarbeitern häufig unklar ist, welche Daten wo gespeichert werden.

it security: *Welche Lücke sehen sie in den aktuellen Security-Strategien der Unternehmen?*

Peter Sakal: Ein wichtiges aber oft unterschätztes Element der Cyberresilience sind Schulungen. Um Mitarbeitenden die Themen beizubringen, die – an den Arbeitsalltag angepasstes – Wissen vermitteln, müssen spezielle Lernstrategien eingesetzt werden. Unterschiedliche Schulungsformate tragen dazu bei, dass Mitarbeitende die Inhalte gemäß ihres persönlichen Lerntypus verinnerlichen und auch anwenden können. Erfolgreiche Cloud-Security ist das Ergebnis eines andauernden Prozesses. Unternehmen, die sich dessen bewusst sind, können die Chancen der Cloud umso besser nutzen.

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

Zero-Trust-Segmentierung

STÄRKT DIE CYBERRESILIENZ UND VERHILFT ZU COMPLIANCE MIT NIS2 SOWIE DORA

NIS2 und DORA zielen darauf ab, die Cyberresilienz in Kritischer Infrastrukturen sowie von Finanzorganisationen zu erhöhen. Für Organisationen wird Zero-Trust-Segmentierung zur Technologie der Wahl, um die Compliance-Anforderungen schnell zu erfüllen und gleichzeitig die Cyberresilienz zu stärken.

Cyberresilienz ist die Fähigkeit einer Organisation, sich vor Cyberangriffen zu schützen, sich schnell zu erholen und den Betrieb auch während eines Angriffs aufrechtzuerhalten. Um Organisationen dazu zu bewegen, ihre Cyberresilienz zu stärken, hat die EU kürzlich zwei Rechtsakte – NIS2 und DORA – erlassen, die in den kommenden Jahren in nationales Gesetz überführt werden müssen.

NIS-2-Richtlinie

NIS2 zielt auf die Verbesserung der Cyberresilienz Kritischer Infrastrukturen und führt dabei die Unterscheidung zwischen wesentlichen und wichtigen Einrichtungen ein. Die wesentlichen Sektoren werden um die Sektoren Abwasser, öffentliche Verwaltung und Raumfahrt erweitert. Die neue Richtlinie muss von den Mitgliedsstaaten bis spätestens 17.10.2024 in nationales Recht umgesetzt werden und betrifft nun eine viel größere Anzahl von Organisationen als NIS – nach Schätzungen rund 29.000 in Deutschland. Diese müssen innerhalb von drei Monaten registriert werden, wobei der erste Umsetzungsnachweis spätestens zu einem vom Bundesamt festgelegten Zeitpunkt zu erbringen ist. Dies kann maximal vier Jahre nach Inkrafttreten des Gesetzes sein.

DORA fordert Cyberresilienz ein

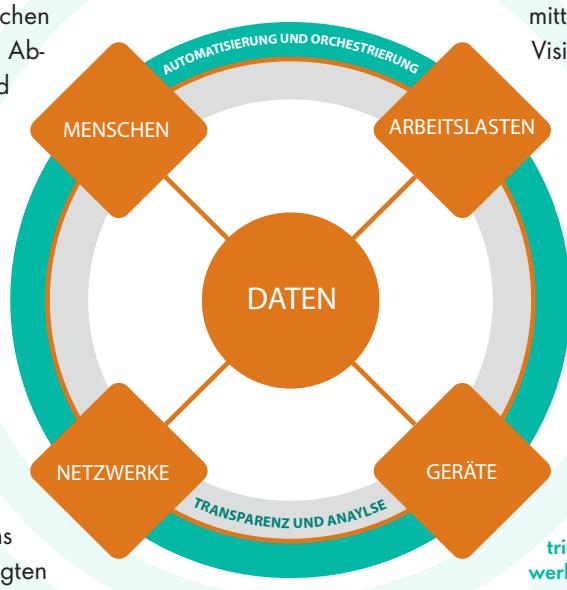
Der Digital Operational Resilience Act (DORA) ist im Januar 2023 in Kraft getreten und soll ab dem 17.01.2025 angewendet werden. DORA schreibt Finanzorganisationen ein hohes Maß an digitaler operativer Widerstandsfähigkeit vor und fordert von den Organisationen die „Isolierung betroffener Informationsassets im Falle von Cyberangriffen" sowie die Implementierung von „Richtlinien, die den physischen oder logischen Zugang zu Informations- und IKT-Assets ausschließlich auf den Umfang beschränken, der für rechtmäßige und zulässige Funktionen und Tätigkeiten erforderlich ist."

Die Cyberresilienz erreichen

Zero-Trust-Segmentierung (ZTS), auch Mikrosegmentierung genannt, ist eine wichtige Komponente von Zero Trust – einem Sicherheitskonzept, bei dem der Zugriff auf Ressourcen, Anwendungen und Daten standardmäßig verweigert wird. Mit ZTS unterteilen Organisationen ihre IT-Landschaft in kleine Segmente und verhindern so die laterale Bewegung der Angreifer. ZTS sorgt also dafür, dass Cyberangriffe schnell eingedämmt werden und aus kleinen Sicherheitsverstößen keine Cyberkatastrophen werden. So können sich Organisationen schneller erholen und die Auswirkungen auf den Betrieb minimieren.

Da sowohl NIS2 als auch DORA innerhalb der nächsten 18 Monate zur Anwendung kommen sollen, müssen Organisationen jetzt handeln. Die Implementierung einer Zero-Trust-Strategie und von Technologien wie Zero-Trust-Segmentierung sollte Teil einer laufenden Sicherheitsumstellung sein. Die Umsetzung wird nicht über Nacht, sondern schrittweise erfolgen – wobei unmittelbare Vorteile wie die vollständige Visibilität der IT-Umgebung sofort realisiert werden können. Einmal umgesetzt, können Organisationen darauf vertrauen, dass ihre IT sicher ist, und brauchen auch keine teuren Sanktionen wegen Nicht-Einhaltung der Vorschriften fürchten.

Alexander Goller
www.illumio.com



Die sieben Säulen des Zero Trust eXtended (ZTX) Frameworks von Forrester. Zero-Trust-Segmentierung ist ein Teil von Zero Trust und konzentriert sich auf das Netzwerk bzw. die Netzwerksicherheit. (Quelle: Illumio)

Krypto-Agilität

DATEN VOR POTENZIELLEN ANGRIFFEN SCHÜTZEN

Krypto-Agilität gewinnt zunehmend an Bedeutung, um Unternehmen auch in einer zukünftigen Post-Quanten-Ära vor Cyberangriffen zu schützen. Diese Fähigkeit ermöglicht es Software-Anbietern, schnell auf sich ändernde Bedrohungen zu reagieren, indem direkt alternative Verschlüsselungstechnologien implementiert werden. Durch den Einsatz verschiedener Algorithmen und Verschlüsselungsverfahren können Systeme den sich ständig weiterentwickelnden Angriffsmethoden standhalten.

Die Entwicklung von Quantencomputern stellt eine besondere Herausforderung dar, da diese die Sicherheit herkömmlicher kryptografischer Algorithmen beeinträchtigen können. Daher konzentriert sich die Forschung auf post-quantenresistente Kryptografie, um robuste Verschlüsselungsverfahren zu entwickeln, die auch in einer Welt mit leistungsstarken Quantencomputern sicher bleiben.

Krypto-Agilität bezieht sich auf die Fähigkeit eines kryptografischen Systems, sich flexibel an veränderte Bedrohungen und technologische Entwicklungen anzupassen. Angesichts der raschen Fortschritte im Quantencomputing ist es von entscheidender Bedeutung, dass Systeme auf den Einsatz von Quantenalgorithmen reagieren können. Ziel ist es, eine Infrastruktur zu schaffen, die es ermöglicht, zwischen kryptografischen Algorithmen zu wechseln und diese zu aktualisieren, um die Sicherheit von Daten und Kommunikation zu gewährleisten.

Dieser agile Ansatz ist ein wesentlicher Bestandteil der Sicherheitsstrategien von Unternehmen, um kontinuierliche Verbesserungen der Verschlüsselungstechnologien zu ermöglichen und so Daten vor potenziellen Angriffen zu schützen. Dies stärkt das Vertrauen von Kunden, Partnern und Lieferanten und gewährleistet auch in Zukunft eine sichere Datenübertragung.

Ari Albertini | www.flapi.com

IT-RECHT

AKTUELLER STAND IN GESETZGEBUNG UND RECHTSPRECHUNG

IT-Recht;
Helmut Redeker,
NJW Praxis; Band 55;
C.H.BECK, 08-2023

Dieses Werk ist laut Verlagsangaben bestens auf die Anforderungen des Prüfungskatalogs für den Fachanwalt für IT-Recht abgestimmt.

Inhalt

- Schutz von Software
- Erwerb von Soft- und Hardware
- Wartung und Pflege von EDV-Anlagen
- Prozessuale Fragen/Vollstreckungsprobleme
- Rechenzentrumsvertrag/Outsourcing
- Rechtsprobleme von Internet und Telekommunikation

Vorteile auf einen Blick

- Prüfungskatalog nach § 14k FAO für den Fachanwalt IT-Recht abgedeckt
- IT-Recht kompakt und praxisnah
- Autor ist zugleich ausgebildeter Informatiker

Diese Neuauflage bringt das Werk insgesamt auf den aktuellen Stand Frühling 2023 in Gesetzgebung, Literatur und Rechtsprechung.

Zielgruppe

Für Rechtsanwaltschaft, insbesondere Fachanwaltschaft für IT-Recht, Richterschaft sowie Syndikusanwaltschaft in der IT-Branche.

Phishing Report 2023

EIN ENDE IST NICHT IN SICHT

Cloudflare hat seinen ersten Bericht für 2023 zu den Bedrohungen durch Phishing veröffentlicht. Daraus geht hervor, dass Phishing nach wie vor die beliebteste Methode moderner Cyberkrimineller ist und das stärkste Wachstum verzeichnet. Geschuldet ist dies in erster Linie der Allgegenwärtigkeit von E-Mails, aber auch der Fehleranfälligkeit und Gutgläubigkeit des Menschen.

Die Übernahme geschäftlicher E-Mail-Konten (Business Email Compromise – BEC) verursacht einen finanziellen Schaden von mehr als 50 Milliarden USD. Doch die Angreifer nehmen keineswegs nur die großen Player der Privatwirtschaft ins Visier. Die Auswirkungen von Phishing reichen weit über Firmen aus den Fortune 500 und internationale Konzerne hinaus: Betroffen sind auch kleine und mittelständische lokale Betriebe und der öffentliche Sektor. Im diesjährigen Bericht hält Cloudflare beispielsweise fest, dass eine höhere Zahl an E-Mail-Bedrohungen auf politische Organisationen abgezielt haben.

Der Bericht macht auch deutlich, dass Kriminelle mit Phishing-Kampagnen unabhängig von der Größe und der Branche der betroffenen Unternehmen zwei Hauptziele verfolgen: In erster Linie geht es darum, in den Augen des Opfers als authentisch und legitim zu erscheinen, damit man es im zweiten Schritt davon überzeugen kann, in den Austausch zu treten oder durch einen Klick in die Falle zu tappen. Folgende zentrale Ergebnisse untermauern diese Erkenntnis:

➤ Schädliche Links sind die größte Gefahrenkategorie. Auf die entfallen 35,6 Prozent aller erkannten Bedrohungen.

➤ Identitätstäuschung ist auf dem Vormarsch – ihr Anteil an den Gesamtbedrohungen hat sich von 10,3 Prozent auf 14,2 Prozent (39,6 Millionen) erhöht.

➤ Angreifer haben mehr als 1 Milliarde Versuche unternommen, sich als ein Unternehmen auszugeben, und sich dabei über 1.000 Marken bedient. In den meisten Fällen (51,7 Prozent) wurde dafür die Identität einer der 20 bekanntesten Marken der Welt missbraucht.

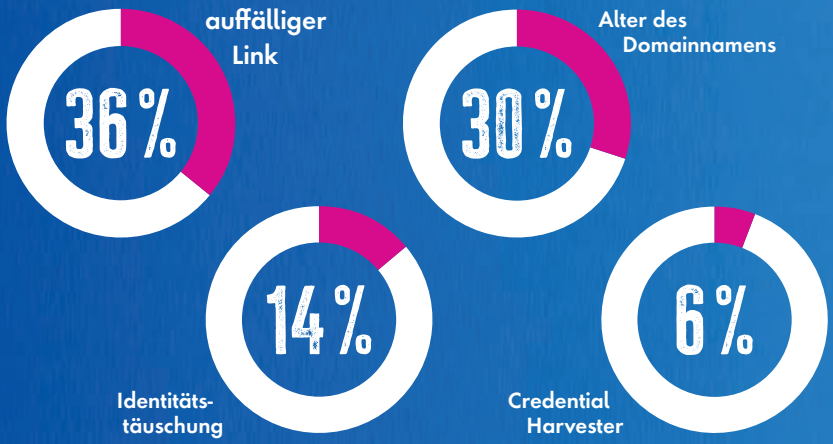
➤ Die am häufigsten imitierte Marke ist eines der Softwareunternehmen, denen das größte Vertrauen entgegengebracht wird: Microsoft. Zu weiteren Top-Marken, deren Identität für Phishing genutzt wurde, gehören Google, Salesforce und Notion.so.

➤ Ein Drittel (30 Prozent) der entdeckten Bedrohungen betrafen neu registrierte Domains. Diese stellen damit die zweitwichtigste Bedrohungskategorie dar.

➤ E-Mail-Authentifizierung hält Bedrohungen nicht auf. Eine große Mehrheit (89 %) der unerwünschten Nachrichten hat Authentifizierungsprüfungen mittels SPF, DKIM oder DMARC „bestanden".

www.cloudflare.com/de-de/

ERKENNUNG NACH GEFAHRENKATEGORIE



Datenmanagement

SICHER UND EINFACH

Einfache Bedienung und höchste Sicherheit werden oft als Gegensätze empfunden. Doch moderne Cloud-Datenmanagementsysteme, die sichere Datenräume schaffen, zeigen, dass es auch anders geht. Gute Sync&Share-Software, die Daten zwischen allen Beteiligten hin- und herschaufelt, kann sehr wohl die höchsten Sicherheitsanforderungen und gesetzlichen Vorgaben erfüllen – und sich gleichzeitig intuitiv in die Bedienung integrieren.

Nachfolgend werden die wichtigsten Kriterien für derartige Systeme genannt: einfache Zugangsverwaltung, sichere Authentifizierung, Ende-zu-Ende-Verschlüsselung, Zero-Knowledge-Architektur (der Anbieter besitzt selbst keine Schlüssel zu Kundendaten), revisionssichere Prozesse, Datenablage lokal wie auch in der Cloud, transparente Versionierung mit Schutz gegen löschen und manipulieren, Abwehr von Ransomware-Schäden, Überwachung von Aufbewahrungsfristen, Integration mit Standardsoftware wie Outlook, Teams und Onedrive, Einhaltung von DSGVO und GoBD, Datenablage in der EU. Die Bedienung erfolgt im Idealfall über ein Dashboard mit Datenzugriff von überall.

Ein solches System ist für Selbstständige, Kleinunternehmer und den Mittelstand geeignet, weil es firmeneigene Fileserver ersetzen kann. Gerade für diese Anwender, die häufig sorglos mit Daten umgehen, bietet sich sicheres Sync&Share als Alternative an. Einige derartige Lösungen wie beispielsweise TeamDrive sind aufgrund der hohen Sicherheit sogar für Berufsgeheimnisträger wie Ärzte, Anwälte oder Steuerberater nutzbar. In Großunternehmen bietet es sich für sichere Datenräume für eine firmenübergreifende Zusammenarbeit an, oder auch Betriebsräte, die vertraulich arbeiten müssen.

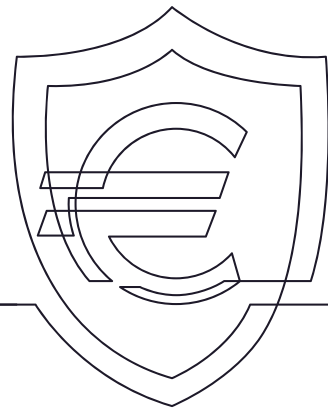
www.teamdrive.com

Betrug durch Fernzugriff

WIE BANKEN IHRE KUNDEN SCHÜTZEN KÖNNEN

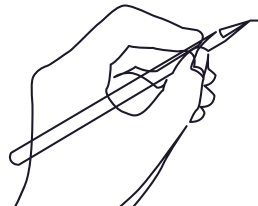
Remote Access Scam (RAS), eine Taktik für Cyberattacken über Fernzugriffs-Tools, ist eine weit verbreitete Betrugsmasche, mit der Angreifer auf PCs, Laptops und mobile Geräte zugreifen können. Dabei geben sich die Cyberkriminellen als seriöses Unternehmen wie etwa Microsoft aus und nutzen Social-Engineering-Taktiken, um Zugriff auf die Geräte potenzieller Opfer zu erhalten. Die Auswirkungen sind fatal. Deshalb hat BioCatch fünf praktische Tipps zusammengestellt, die Banken und Kunden dabei unterstützen, sich effektiv vor RAS zu schützen.

- **#1** Zugriff auf Basis von detailliertem Kundenverhalten überprüfen
- **#2** Zugriff mit Blick auf zeitgleiche Anrufe analysieren
- **#3** Verhaltensintelligenz mit anderen verfügbaren Kundendaten abgleichen
- **#4** Verdächtige Transaktionen gründlich überprüfen
- **#5** Kunden über Betrugsmethoden aufklären



„Unsere Studie in Zusammenarbeit mit Forrester Consulting zeigt, dass die Mehrheit der Finanzinstitute weltweit nicht gegen die zunehmende Finanzkriminalität gerüstet ist. In einer Zeit, in der Kunden mehr Schutz und integrierte, nahtlose digitale Erlebnisse fordern, haben die Betrugsbekämpfungsteams der Finanzinstitute Schwierigkeiten, dieser Herausforderung gerecht zu werden. Das liegt vor allem an veralteter Technologie und überlasteten Ressourcen.“, erklärt Wiebe Fokma, Director EMEA Global Advisory bei BioCatch.

www.biocatch.com



IMPRESSUM

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

Chefredaktion:
Silvia Parthier (-26)

Redaktion:
Carina Mitzschke (nur per Mail erreichbar)

Redaktionsassistenz und Sonderdrucke:
Eva Neff (-15)

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

Autoren:
Ari Albertini, Dr. Steele G. Arbeeny, Lars Becker, Thomas Bitschnau, Sergej Dechand, Günter Esch, Simon Federle, Alexander Goller, Uwe Gries, Jörg von der Heydt, Michael Klatte, Sasche Kreutziger, Carina Mitzschke, Dr. Sina Niedermaier, Silvia Parthier, Ulrich Parthier, Peter Sakal, Alexander Schaum, Michael Scheffler, André Schindler, Frank Schmaering, Zeki Turedi, Maxime Vermeir, Sebastian Weber, Torsten Wiedemeyer

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

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.

Passkeys statt Passwörter

ANMELDUNG EINFACH UND SICHER

Die Zwei-Faktor-Authentifizierung über Passwort und jedes Mal neu generierten Sicherheitscode ist der anerkannte Goldstandard, wenn es um die Anmeldung bei Online-Diensten geht. Allerdings halten viele Nutzer dieses Verfahren für zu umständlich, so auch Vodia Networks.

So richtig zufrieden waren die Benutzer damit schon lange nicht mehr, aus mehreren Gründen. SMS als zweiter Faktor wäre großartig, dafür müssten die Partner allerdings einen SMS-Anbieter einbinden – was aber nur die wenigsten tun. Eine weitere Option, ein USB-Stick, hat jedoch kaum ein Endnutzer. Also blieb als einziger „praktikabler" zweiter Faktor der Code per E-Mail, doch das ist ziemlich umständlich.

„Wir hörten von der FIDO-Allianz, die mit Unternehmen wie Microsoft und Google zusammenarbeitete um etwas Besseres als Passwörter zu entwickeln. Dass sie öffentliche und private Schlüssel verwenden, war zwar ein wenig abschreckend, schließlich erfordert das einen ganz schönen Aufwand, damit es funktioniert. Andererseits sind wir hinsichtlich kryptografischer Herausforderungen ziemlich sattelfest", erinnert sich Dr. Christian Stredicke, Geschäftsführer von Vodia Networks. Also begann das Team bei Vodia, sich mit Passkeys genauer zu beschäftigen. Und das Timing war perfekt: Die Browser unterstützten Passkeys bereits, und es gab viel Beispielcode, um es im Frontend und Backend zum Laufen zu bringen.

Das Unternehmen experimentierte mit einigen Versionen des Anmeldebildschirms, bis sich eine Variante herauskristallisierte, die die unterschiedlichsten Anforderungen von Anwendern abdeckt. Die Lösung war, Passkeys zum Login anzubieten und gleichzeitig für Nutzer, die Passkeys nicht verwenden können oder wegen innerbetrieblicher Regelungen nicht dürfen, eine Checkbox zu integrieren. Wer Passkeys nicht verwenden kann oder darf, kann diese Box aktivieren und wird bei der nächsten Anmeldung nicht mehr zur Nutzung von Passkeys aufgefordert. Das sollte für die meisten Anwender auch auf längere Sicht eine gute Lösung sein.

https://web.vodia.com/

Data Lake:

Die etwas ANDERE ART des PHISHINGS....

Mehr Infos dazu im Printmagazin

SCAN ME

itsecurity

und online auf www.it-daily.net


CROWDSTRIKE
We take pride in being a cybersecurity leader.
When we're #1, our customers win.
#1
XDR | EDR | MDR
Incident Response
Treffen Sie uns auf der it-sa 2023:
Halle 7A, Stand 324
CrowdStrike is continually recognized as a leader by analysts, evaluators and customers. Learn more at crowdstrike.com/leader.