it management

Der Motor für Innovation
November/Dezember 2023

INKLUSIVE 48 SEITEN
it security

PROJEKTMANAGEMENT

Die richtigen Fragen stellen

TWIN TRANSITION

Nachhaltig und digital

AUTOMATISIERUNG

Praktische Anwendung von KI

STARKE PARTNERSCHAFT

Innovative Lösungen und besserer Service

Jasmin Woll, TOPdesk Deutschland GmbH

zoi
Was wird 2024 wichtig?
ab Seite 14

www.it-daily.net

IT WELT.at is IT

IT NEWS

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

itwelt.at

IT TERMINE

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

itwelt.at/events

IT UNTERNEHMEN

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

itwelt.at/top-1001

IT JOBS

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

itwelt.at/jobs

FUTURE THINKING IN DER IT

LIEBE LESERINNEN UND LESER,

Niemand kann genau in die Zukunft schauen. Aber Themen kommen und gehen. Vor kurzem noch der Trend schlechthin, ist das Metaverse fast völlig in der Wahrnehmung verschwunden. Dennoch gibt es solche, die sich beharrlich halten. Nachfolgend unsere Top 10.

#1 **Künstliche Intelligenz und Maschinelles Lernen:** Fortschritte werden in allen Anwendungsgebieten sichtbar.

#2 **Cybersecurity:** Mit der zunehmenden Digitalisierung steigt auch das Risiko von Cyberangriffen. Proaktive Sicherheitslösungen sind gefragt.

#3 **Internet of Things (IoT):** Das IoT wird weiterhin wachsen.

#4 **Cloud- und Edge-Computing:** Rechenleistung und Services über die Cloud ermöglichen neue Anwendungsszenarien.

#5 **5G-Technologie:** Die Einführung wird die Geschwindigkeit, Zuverlässigkeit und Konnektivität verbessern und die Grundlage für AR schaffen.

#6 **Blockchain-Technologie:** Die Blockchain wird weiter eine wichtige Rolle spielen.

#7 **Nachhaltigkeit und Green IT:** Durch den Klimawandel werden nachhaltige IT-Lösungen und energieeffiziente Technologien wichtiger.

#8 **Human-Computer-Interaktion:** Fortschritte könnten die Art und Weise, wie Menschen mit Technologie interagieren, revolutionieren.

#9 **Datenschutz und Ethik:** Mit der Künstlichen Intelligenz kommt ein weiteres Anwendungsgebiet hinzu!

#10 **Quantencomputing:** Der Einsatz von Quantencomputern bietet neue Möglichkeiten für komplexe Berechnungen und Problemlösungen.

Herzlichst

Ulrich Parthier | Publisher it management & it security

INHALT

COVERSTORY

10 **Durch starke Partnerschaft zum Erfolg**
Innovative Lösungen und besserer Service

12 **Panik am Servicedesk**
Wie Sie die Panik in den Griff bekommen

IT MANAGEMENT

14 **Ganzheitliche Sicht wichtiger denn je**
Welche IT- und Technologietrends im Jahr 2024 wichtig werden

18 **Mobiler ERP-Zugriff**
Die Automatisierung fördern

21 **Der CO_2-Footprint eines IT-Leiters**
Mit der richtigen Lizenzierung die Umwelt schonen

22 **Holistischer Ansatz**
IT-Sustainability geht über eine ökologische Green-IT hinaus

26 **Twin Transition**
Nachhaltig und digital – eine Frage der Führung

30 **Green IT**
Wie Software-Entwickler ihre Produkte nachhaltiger gestalten können

34 **Simplify Sustainability**
Nachhaltigkeit ist keine Rocket Science

36 **Tier-IV-Rechenzentrum**
Die Vorteile von „fault tolerant" für Unternehmen

39 **Das große Reinemachen**
Zentraler Erfolgsfaktor für die SAP S/4HANA Migration

40 **Von der Krise zur Chance**
Mit IT-Monitoring Fachkräftemangel und steigende Anforderungen meistern

43 **Unternehmenskultur**
Technologien unterstützen neue Arbeitsmodelle

Farblich hervorgehobene Artikel sind von der Redaktion als besonders lesenswert empfohlen

44 Network Inventory Management
Infrastrukturtrends bei Telcos

47 Datenmanagement
Datenexperten sind die neuen Produktmanager

48 Master Data Management
Korrekte Daten sind die Basis für KI-Anwendungen

50 Testdatenmanagement
Erstellung von synthetischen und referentiell korrekten Testdaten

54 Cloudbasierte PPM-Lösung für den Mittelstand
Wettbewerbsvorsprung durch Projektportfolio-Management

56 Die richtigen Fragen stellen
Projekte zielgerichtet hinterfragen und verbessern

60 Die Zukunft der Automatisierung
Fünf praktische Anwendungen von KI

62 Was ist die CRM-Strategie?
Ein Weg aus der Hölle des Mittelmasses!

Inklusive 48 Seiten it security

GUT ZU WISSEN

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

PHISHING

DEUTSCHE FÜHRUNGSKRÄFTE SIND ANFÄLLIGER ALS IHRE ANGESTELLTEN

Das Bewusstsein für Cybersicherheit nimmt auch bei Führungskräften zu. Nach Untersuchungen von SoSafe geben 55 Prozent der deutschen Sicherheitsverantwortlichen an, dass der Fokus ihres Top-Managements auf IT-Sicherheit im Vergleich zum vergangenen Jahr gestiegen ist. Cyberrisiken werden dabei immer präsenter: Allein in den vergangenen drei Jahren ist jedes zweite deutsche Unternehmen (58 Prozent) Opfer einer Cyberattacke geworden.

Das Bewusstsein für Cyberrisiken in den Führungsetagen bestimmt laut SoSafe's Umfrage auch, ob erforderliche Ressourcen für IT-Sicherheit in einem Unternehmen verfügbar sind. Das heißt, ob das Unternehmen über genügend Personal und Budget verfügt, um potenzielle Cyberbedrohungen zu bekämpfen: In Organisationen, deren Führungsebene für Cyberrisiken sensibilisiert ist, ist die Wahrscheinlichkeit 33 Prozent höher, dass ausreichende Ressourcen für Sicherheitsbelange zugewiesen werden, als in Organisationen, in denen das Sicherheitsbewusstsein der Führungsetage niedrig ist. Von den Organisationen mit unzureichenden Sicherheitsbudgets priorisieren nur 21 Prozent ihre Sicherheitskultur.

Die Sensibilisierung des Top-Managements ist notwendig, um Cybersicherheit zu einem essentiellen Teil der Unternehmenskultur zu machen. Dies wird auch mit Blick auf das tatsächliche Risiko wichtig: So zeigen Daten von SoSafe, dass die Führungsetage anfälliger ist, auf Phishing-Links zu klicken, als ihre Angestellten. Die durchschnittliche Klickrate ist bei Führungskräften um 60 Prozent höher als bei anderen Nutzergruppen. Aus den Daten geht jedoch auch hervor, dass Führungskräfte verdächtige E-Mails auch eher melden (20 Prozent) als Angestellte (8 Prozent).

www.sosafe-awareness.com/de

TOP-PRIORITÄTEN

VON IT- UND SICHERHEITSTEAMS

1. Die Security Awareness der Mitarbeiter erhöhen

2. Identity und Access Management verbessern

3. Hybride Arbeitsmodelle besser absichern

4. Sicherheit bestehender Prozesse steigern

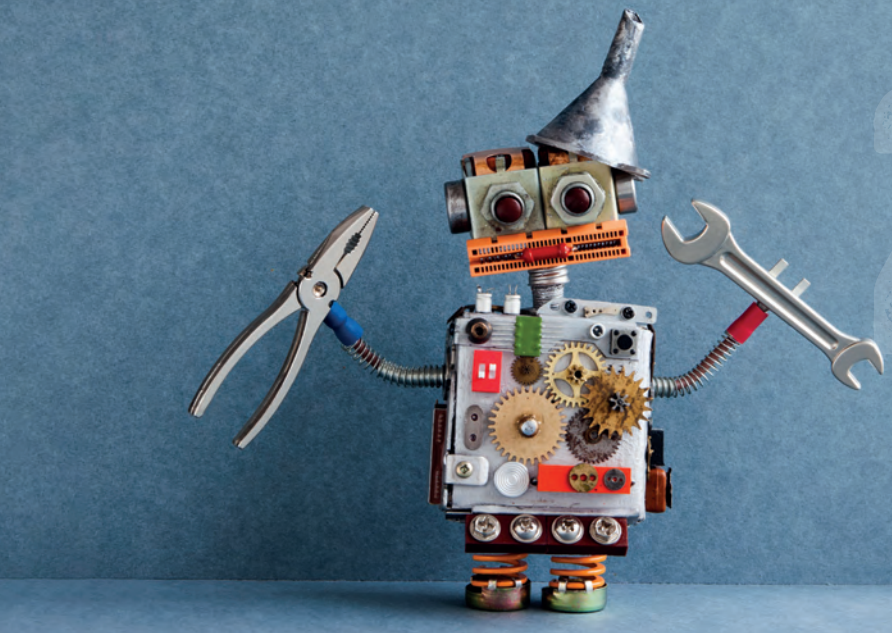
TOP 3 GRÜNDE,

DIE USER AM SECURITY AWARENESS TRAINING KRITISIEREN

1. Training ist zu zeitaufwändig

2. Informationen sind zu allgemein

3. Training ist zu eintönig



Servitization-Shift

WAS IST DIE WICHTIGSTE TECHNOLOGIE?

IFS hat die ersten Ergebnisse seiner jüngsten Studie „Industrial Servitization and Field Service Technology" veröffentlicht. Darin wird die Rolle der Technologien beim Shift von Unternehmen zu Service-orientierten Geschäftsmodellen (Servitization) untersucht. Dafür wurden 2.000 Entscheider ab der Position Vice President in Deutschland, Frankreich, Großbritannien, Japan, Südafrika und den USA befragt. Sie kommen aus Branchen wie Energieversorgung, Produktion, Konstruktion, Telekommunikation, Automatisierung und Digitalisierung oder Services.

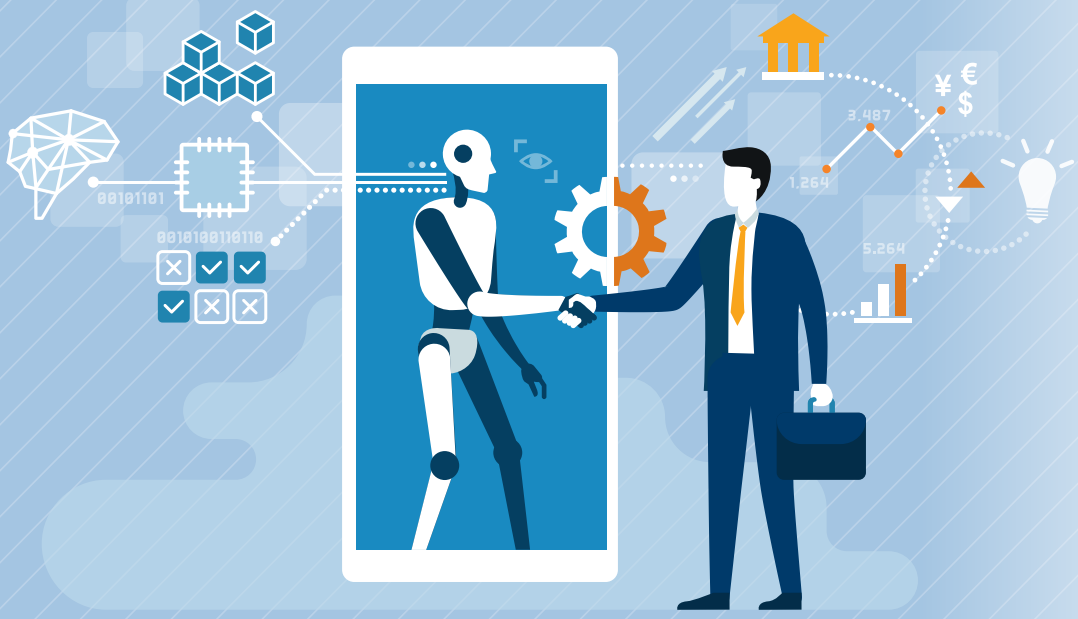
Die Ergebnisse zeigen, dass der Shift zum Servitization-Modell für 39 Prozent der Verantwortlichen in deutschen Unternehmen hohe Priorität besitzt. Als wichtigste Ursachen für schleppende Fortschritte werden dabei fehlende Vorgaben für Mitarbeiter, Prozesse und Technologien genannt.

Über alle Branchen hinweg ist Künstliche Intelligenz die wichtigste Technologie beim Servitization-Shift, auch in Deutschland. Sie verbessert die operative Effizienz laut Aussage deutscher Ansprechpartner um 25 Prozent, hilft bei der Eroberung neuer Kundensegmente und Märkte (25 %), erhöht die Kundenzufriedenheit (26 %) ebenso wie die Kundenbindung (25 %) und ist die Voraussetzung für höhere Margen (27 %).

Der Aufbau von KI-Fähigkeiten hat für den Produktionsbereich sowie den Luft-, Raumfahrt- und Verteidigungssektor in Deutschland mit 90 Prozent beziehungsweise 63 Prozent die größte Dringlichkeit. Dahinter folgen Services mit 54 Prozent, Telekommunikation mit 42 Prozent, Konstruktion und Ingenieurwesen mit 51 Prozent und der Energiesektor mit 44 Prozent. Innovation und klare Positionierung werden danach als Basis für Umsatzwachstum und Profitabilität gesehen.

Solide Finanzen und hohe Resilienz stehen für CEOs (54 %) und CFOs (49 %) in allen Ländern beim Servitization-Shift an erster Stelle der Agenda. Das zeigt die enge Verbindung zwischen dem Druck zur Modernisierung durch die digitale Transformation und den monetären Erwartungen bei den Vorständen in Bezug auf das Service-orientierte Geschäftsmodell. In Deutschland spielt der CEO übrigens die wichtigste Rolle beim Vorantreiben der Servitization, das haben 42 Prozent der Befragten angegeben.

www.ifs.com



Chancen für IT-Führungskräfte

MIT KI ZU MEHR EFFIZIENZ

Freshworks hat die Ergebnisse seiner zweiten jährlichen Studie „State of Workplace Technology" veröffentlicht, in der aufgezeigt wird, dass die Anzahl der Softwareanwendungen auf den Arbeitscomputern der IT-Teams im letzten Jahr um 71 Prozent gestiegen ist. Um diese zunehmende Komplexität in den Griff zu bekommen, setzen IT-Profis - vor allem Führungskräfte und jüngere Generationen - auf KI, um Arbeitsabläufe zu automatisieren und die Effizienz zu steigern.

KI kann Unternehmen Zeit und Geld sparen

Freshworks hat herausgefunden, dass Unternehmen in den USA jedes Jahr 15.603 US-Dollar pro IT-Mitarbeitenden einsparen könnten, wenn sie KI einsetzen, um Zeit für sich wiederholende Aufgaben zu sparen. Das bedeutet, dass ein Unternehmen mit mindestens 5.000 Mitarbeitenden und durchschnittlich 200 IT-Fachleuten durch den Einsatz von KI jährlich mindestens 3,1 Millionen Dollar einsparen könnte. Die Umfrage hat außerdem ergeben:

IT-Fachleute verwalten mehr Software als je zuvor und sehen eine Möglichkeit, die Verwaltung zu vereinfachen. Die Zahl der Softwareanwendungen auf den Arbeitscomputern der IT-Teams ist im letzten Jahr um 71 Prozent gestiegen. Trotzdem nutzen IT-Fachleute nur ein Drittel der ihnen täglich zur Verfügung stehenden Anwendungen (nur acht von 24), während es 2022 noch die Hälfte war.

IT-Teams stellen Effizienz in den Vordergrund. Benutzungsfreundlichkeit und Effizienz sind die wichtigsten Eigenschaften von Unternehmenssoftware, noch vor Funktionsumfang, Zuverlässigkeit und Kosteneffizienz.

KI eliminiert sich wiederholende Aufgaben. IT-Profis sind sich einig, dass KI Zeit spart, die sie sonst für sich wiederholende Aufgaben aufwenden müssten (49%), und es ihnen ermöglicht, komplexere, sinnvollere Aufgaben zu erledigen (45%). Darüber hinaus schätzen IT-Profis, dass sie durch den Einsatz von KI zur Erledigung sich wiederholender Aufgaben mehr als fünf Stunden pro Woche einsparen könnten.

Leitende IT-Führungskräfte sind von KI überzeugt

Leitende und höhere Führungskräfte berichten über eine stärkere Nutzung und organisatorische Unterstützung von KI. Zu den wichtigsten Ergebnissen gehören:

Die Nutzung von KI wird am Arbeitsplatz generell gefördert. Sieben von zehn (70%) IT-Führungskräften und höher geben an, dass der Einsatz von KI in ihrem Unternehmen aktiv gefördert wird, verglichen mit 44 Prozent der Teamleiter/Manager und 21 Prozent der einzelnen Mitarbeitenden.

IT-Führungskräfte sind maßgeblich an der Einführung von KI beteiligt. Mehr als neun von zehn (91%) IT-Führungskräften und höher setzen derzeit KI zur Unterstützung ihrer Arbeit ein, verglichen mit 66 Prozent der Teamleiter/Manager und 33 Prozent der Einzelmitarbeiter.

Es gibt eine KI-Bewegung der Jugend. Die jüngeren Generationen spielen eine entscheidende Rolle bei der Einführung von KI. Acht von zehn (81%) der Millennials und 75 Prozent der Gen Z IT-Profis nutzen derzeit KI zur Unterstützung ihrer Arbeit, verglichen mit 57 Prozent der Gen X und 27 Prozent der Boomer.

www.freshworks.com

DIGITAL NATIVES

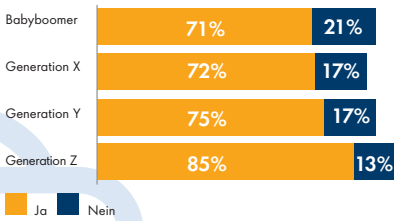
WANDEL DER ARBEITSWELT

In der heutigen Welt verbringen wir einen großen Teil unserer Freizeit digital. Insbesondere die junge Generation, die von klein auf mit dem Internet und IT aufgewachsen ist, kann sich ein Leben ohne moderne Technologie kaum vorstellen. Wir nennen sie daher „Digital Natives". Doch wie sieht es in der Arbeitswelt aus?

Die Software-Bewertungsplattform Software Advice hat in einer aktuellen Studie den Gebrauch digitaler Tools in verschiedenen Generationen von Arbeitnehmern untersucht. Hierfür wurden etwa 1.000 in Deutschland tätige Mitarbeiter befragt, die Computer in ihrer täglichen Arbeit verwenden. Die teilnehmenden Generationen umfassten:

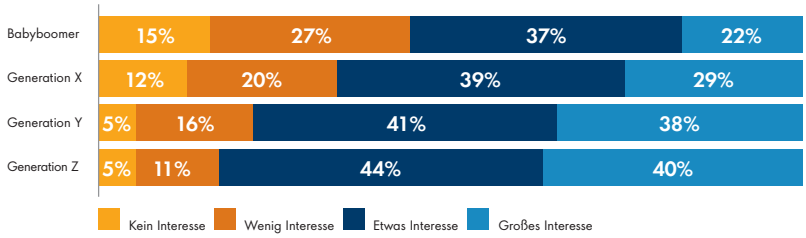
- Babyboomer (geb. 1946 – 1964)
- Generation X (geb. 1965 – 1979)
- Generation Y, bzw. Millennials (1980 – 1994)
- Generation Z (geb. 1995 oder später)

Sollte dein Unternehmen sich stärker darum bemühen, seine Angestellten im Umgang mit digitalen Tools zu schulen?



Quelle: Digital Natives-Umfrage 2023, n: 837, Hinweis: Die Antwort „Nicht sicher" wird nicht in der Grafik gezeigt (zw. 2 und 10%)

Wie würdest du dein Interesse an der Nutzung neuer Technologien einschätzen?



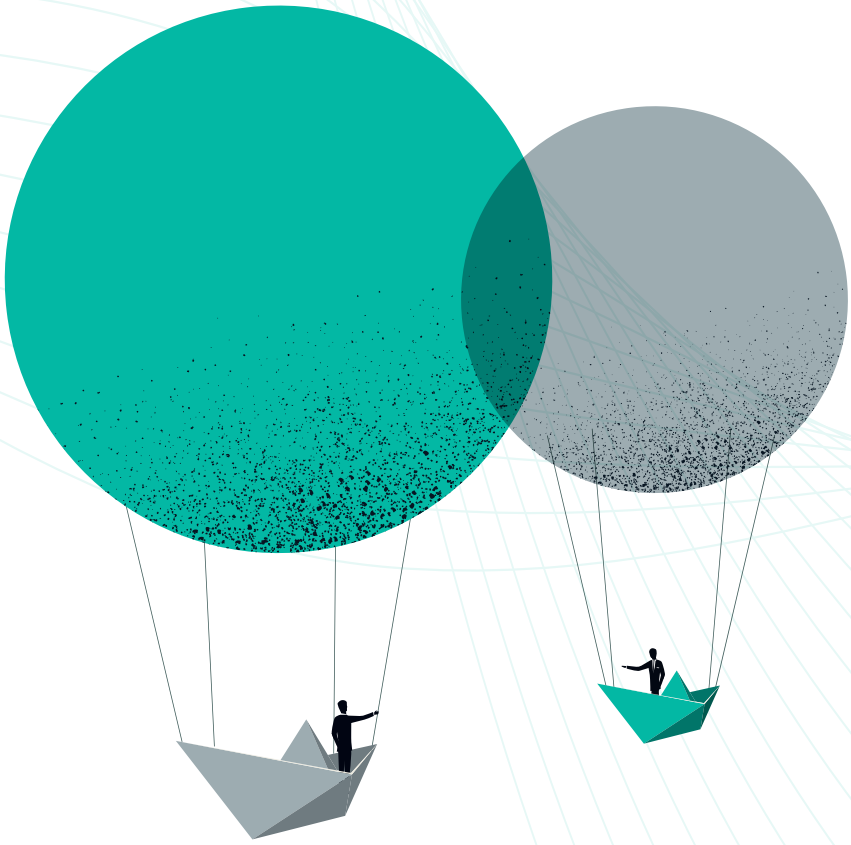
Quelle: Digital Natives-Umfrage 2023, n: 99, Hinweis: Durch Rundungen übersteigt die Gesamtsumme 100%

Wer sind die Digital Natives?

Als Digital Natives werden die Generationen bezeichnet, die mitten im digitalen Zeitalter aufgewachsen sind, geprägt durch die Entstehung und Verbreitung des Internets und später der Smartphones. Der Umgang mit digitalen Technologien gehört für sie ganz selbstverständlich zum Alltag. Die Bezeichnung „Digital Natives" umfasst die Mitglieder der Generationen Y (Millennials) und der Generation Z.

Im Gegensatz dazu stehen die „Digital Immigrants", die aus den älteren Kohorten wie der Generation X und den Babyboomern stammen. Diese Gruppe ist ohne digitale Medien aufgewachsen und erst im Erwachsenenalter damit in Kontakt gekommen.

www.softwareadvice.de/



Durch starke Partnerschaft zum Erfolg

INNOVATIVE LÖSUNGEN UND BESSERER SERVICE

Die enge Zusammenarbeit zwischen Anbietern und ihren Kunden ist in der Welt der IT-Servicemanagement-Software von entscheidender Bedeutung. Diese Partnerschaft ist der Schlüssel zu innovativen Lösungen und besseren Services.

Die Kreisstadt St. Wendel arbeitet seit September 2016 mit TOPdesk zusammen. Das nachfolgende Gespräch zwischen Marc Rauber, Abteilungsleiter für Informationstechnologie und Beschaffung, und Jasmin Woll, Account Managerin bei TOPdesk, bietet einen umfassenden Einblick in die Erfolgsgeschichte der Kreisstadt.

Jasmin Woll: *Können Sie uns einen Überblick über das Projekt mit der Kreisstadt St. Wendel und die Herausforderungen für die Suche nach einem ITSM-Tool geben?*

Marc Rauber: Es gab zwei Aspekte. Zum einen haben wir gemerkt, dass wir an unsere Grenzen kommen. Damals hatten wir im alten Intranet ein Kontaktformular mit HTML gestrickt. Die Mitarbeiter konnten dort ihre Meldungen weitergeben, so dass diese zumindest in unserem IT-Postfach landeten. Aber sonst lief alles über Telefon oder die Leute standen einfach mit ihrem Problem in der Tür. Das war auf Dauer keine Lösung. Wir brauchten etwas Professionelles. Zum anderen wurde unser damaliger Auszubildender übernommen und brauchte ein eigenes Projekt. Er hat dann verschiedene Ticketsysteme auf den Prüfstand gestellt. Wir besuchten damals TOPdesk on Tour in Stuttgart. Dort konnten wir uns sehr gut mit bestehenden Unternehmenskunden austauschen. Was wir gehört haben, klang alles sehr gut und wir waren von der hohen Melder-Akzeptanz überzeugt.

Jasmin Woll: *Wie hat die Kreisstadt St. Wendel von der Implementierung von TOPdesk profitiert? Gibt es messbare Ergebnisse, die Sie teilen könnten?*

Marc Rauber: Wir konnten zwei Fliegen mit einer Klappe schlagen. In dieser Software konnten wir neben dem Ticketsystem auch ein neues Intranet aufbauen. Ein super Benefit, denn die Akzeptanz des Self Service Portals war bei den Meldern von Anfang an da und so wurde die Nutzung des Systems zum Selbstläufer. Alles wurde digitalisiert und war übersichtlich, darauf kam es uns an.

Außerdem konnten wir jetzt viel besser mit unseren Kunden verhandeln. Wir sind IT-Dienstleister für die Stadtwerke St. Wendel, die Stadt Wadern, die Gemeinde Namborn und die Gemeinde Oberthal. Zudem betreiben wir die Servicestelle für alle acht Kreiskommunen in zwei Rechenzentren. Mit TOPdesk hatten wir erstmals die Möglichkeit auszuwerten, wie viel Dienstleistung wir erbracht haben. Dieser Report war ein sehr gutes Argument für die Budgetplanung der Pauschalverträge mit diesen Kunden.

Jasmin Woll: *Wie beurteilen Sie die Implementierung von TOPdesk?*

Marc Rauber: Die Implementierung verlief wirklich einfach. Alles hat von Anfang an super funktioniert. Besonders positiv war die persönliche Zusammenarbeit mit den TOPdesk Mitarbeitern. Egal welchen Ansprechpartner wir hatten, es war immer auf den Punkt. Alle Absprachen, die getroffen wurden, wurden auch eingehalten. Es gab kein Problem, das wir nicht zusammen lösen konnten. Bis heute haben wir eine sehr konstruktive und gewinnbringende Partnerschaft.

Jasmin Woll: *Welche Probleme konnten Sie außerdem lösen?*

Marc Rauber: Die IT hat bekanntlich immer zu wenig Personal. Wir sind deswegen ständig mit der Personalleitung und der Geschäftsführung im Gespräch. Vor TOPdesk hatte ich dafür nicht immer die passende Argumentationsgrundlage. Heute nehmen wir uns den jährlichen Report aus TOPdesk und vergleichen einfach die letzten Jahre in Bezug auf Ticketaufkommen und Lösungszeiten. Besonders während der Pandemie, konnten wir der Geschäftsführung schwarz auf weiß präsentieren, wie drastisch sich die Zahl der Tickets erhöht hat. Es gab keine Diskussion mehr.

PRINZIPIELL WÜRDE ICH JEDER ORGANISATION MIT KUNDENKONTAKT TOPDESK EMPFEHLEN. EGAL, OB ES SICH DABEI UM DIE IT- ODER EINE ANDERE SERVICEABTEILUNG HANDELT.

Marc Rauber, Abteilungsleiter für Informationstechnologie und Beschaffung, St.Wendel

Jasmin Woll: *Welche Funktionen bringen Ihnen den größten Mehrwert?*

Marc Rauber: Für mich als Abteilungsleiter, ist es hauptsächlich die Reporting-Funktion. Wovon wir in der IT auch sehr profitieren, ist der Ressourcenplaner. Diese Funktion ist ein essenzieller Bestandteil in unserer täglichen Arbeit. Wir tragen dort die Urlaubs- und Fehltage ein, sehen so auf einen Blick wie wir disponieren müssen und planen die Prioritäten entsprechend für den Tag. Mit drei Auszubildenden, Kollegen vor Ort und im Homeoffice gibt es immer Ressourcen zu verteilen. Das in Verbindung mit dem Incidentmanagement, ist dann auf den Punkt – jeder weiß was zu tun ist.

Jasmin Woll: *Gibt es für Sie noch weitere Faktoren, wie TOPdesk Sie in Ihrer täglichen Arbeit erfolgreich unterstützt?*

Marc Rauber: Wir setzen die Lösung schon sehr lange ein, das Tool wird von uns gelebt. Über die Zeit ist TOPdesk nicht nur mit uns gewachsen, sondern konnte auch auf weitere Serviceabteilungen, wie die Beschaffung, die Hauptabteilung und den technischen Hausmeister, ausgeweitet werden. Man kann Mehrwerte generieren und Transparenz schaffen. Seit der Einführung gibt es viel mehr Verständnis für die IT-Abteilung. Durch automatisierte Update-E-Mails wissen die Melder, ihre Anfragen sind in Bearbeitung. Das schafft Zufriedenheit und Akzeptanz.

Jasmin Woll: *Welche Vorteile hat die Kreisstadt St. Wendel besonders geschätzt?*

Marc Rauber: Dass die Software, neben der einfachen Implementierung, auch eine so intuitive Bedienung für Melder und Bearbeiter hat, ist ein eindeutiges Plus. Für uns war die Anpassbarkeit ebenfalls ein wichtiger Vorteil. Wir haben diese Flexibilität sowohl im Self Service Portal für unsere verschiedenen internen und externen Melder als auch im Bearbeiterbereich. So sieht jeder das, was er braucht und wozu er berechtigt ist.

Jasmin Woll, Account Managerin, TOPdesk Deutschland GmbH
www.topdesk.com

Jasmin Woll: *Wem würden Sie TOPdesk empfehlen? Welche Ratschläge würden Sie Organisationen geben, die ähnliche Herausforderungen haben?*

Marc Rauber: Prinzipiell würde ich jeder Organisation mit Kundenkontakt TOPdesk empfehlen. Egal, ob es sich dabei um die IT- oder eine andere Serviceabteilung handelt. Wer strukturiert arbeiten möchte und Skalierbarkeit benötigt, ist hier genau richtig. Das Tool lohnt sich bereits ab dem ersten Bearbeiter, man hat aber immer die Möglichkeit weitere mit aufzunehmen. In TOPdesk geht nichts mehr verloren und man behält den Überblick. Dabei kann ich nur den Tipp geben „keep it simple" - installieren, schulen, anfangen. Einfach machen!

Jasmin Woll: *Herr Rauber, wir danken Ihnen für das Gespräch.*

THANK YOU

Panik am Servicedesk

WIE SIE DIE PANIK IN DEN GRIFF BEKOMMEN

Wäre es nicht schön, einen völlig stressfreien Arbeitsplatz zu haben? Leider ist das utopisch – denn Stress ist Bestandteil des Lebens. Folgend zeigen wir vier Situationen, welche das Paniklevel Ihres Servicedesks steigen lassen und wie Sie die Panik in den Griff bekommen.

Level 1: Auf sich allein gestellt sein

An wen wendet sich jemand mit einem allgemeinen Anliegen bei einer Organisation? Genau, die HR-Abteilung. Das stellt normalerweise kein Problem dar, schließlich gehört es zu den Aufgaben der Abteilung, Mitarbeitern behilflich zu sein und ihnen den richtigen Weg zu weisen. Ihr Posteingang und Ihre verfügbaren Zeitfenster werden mit den gleichen Fragen aus verschiedenen Quellen bombardiert. Viele betrachten das HR-Team als ultimativen Problemlöser, der für gleich welche Thematik eine Lösung findet. Es ist sehr zeitaufwändig jede einzelne Anfrage zu beantworten.

Die Lösung: Führen Sie mithilfe der IT ein Self Service Portal ein. Dieses ist mit FAQs, unterstützenden Informationen und jeglichem sonstigen Wissen gefüllt. Self Service Portale mit leistungsstarken Wissensmanagement-Komponenten verkürzen die Bearbeitungszeiten drastisch: Sie können wiederkehrende Melder einfach an das Portal verweisen und mit Ihrer eigentlichen Arbeit fortfahren. Selbstverständlich gibt es ab und zu eine Frage, die Sie selbst beantworten müssen.

Dies hat nicht nur für HR-Teams Relevanz – jegliche Serviceabteilung kann von der Implementierung eines Self Service Portals profitieren. Tritt ein bestimmtes Anliegen immer wieder auf, sollten Sie erwägen, die Lösung dafür Ihrem Self Service Portal hinzuzufügen. Eignen Sie sich eine „Lösen und Verbessern"-Vorgehensweise an: Ihr Wissensmanagement wird so jeden Tag besser werden.

Level 2: Sich verabschieden

Kollegen kommen und gehen, so ist einfach der Lauf der Dinge. Allerdings ist der Offboarding-Prozess komplizierter als auf den ersten Blick ersichtlich. Neben eini-

gen bürokratischen Aufgaben, müssen auch Aufgaben überwacht werden. Vielleicht stellen Sie sich, nachdem der Mitarbeiter weg ist die Frage: „Wurde der Laptop zurückgegeben?" Sie fragen schnell bei anderen Mitarbeitern nach. Einer verweist dabei an den anderen. Sie wissen nicht, wo sich der Laptop befindet, doch das stellt nicht einmal Ihr größtes Problem dar. Hat Ihr ehemaliger Mitarbeiter noch Zugriff auf alle internen Dokumente? Falls ja, müssen Sie schnellstmöglich den Zugriff unterbinden.

Die Lösung: Die meisten Organisationen verfügen über einen reibungslosen Onboarding-Prozess. Neue Mitarbeiter werden üblicherweise mit einem Getränk und einer kleinen Geschenktüte begrüßt. Sobald diese sich eingerichtet haben, erhalten sie vom Vorgesetzten eine Bürotour, die neuen Kollegen werden vorgestellt und es erfolgt ein allgemeines „Willkommen im Unternehmen".

Warum legen Sie dann nicht auch eine bestimmte Vorgehensweise dafür fest, wenn ein Mitarbeiter die Organisation verlässt?

Widmen Sie Mitarbeitern, die Sie verlassen, genau so viel Sorgfalt wie neuen Kollegen. Richten Sie einen detaillierten und leicht wiederholbaren Prozess ein, durch welchen sichergestellt wird, dass Laptops, Tastaturen, Schlüssel und andere Gegenstände, die der Organisation gehören, wieder zurückgegeben werden, bevor der Mitarbeiter die Organisation verlässt. Sie könnten beispielsweise eine digitale Checkliste erstellen, auf der sämtliche wichtigen Abläufe des Offboarding-Prozesses festgehalten sind. Dies zeigt ihnen schnell Schwachstellen in Ihrem Prozess auf und Sie können diese mit sofortiger Wirkung ausbessern.

Level 3: Der gebrochene Damm

Ihr bestehendes Servicedesk-System funktioniert fantastisch. Mitarbeiter reichen

DIE PROZESSE DES INCIDENTMANAGEMENTS STELLEN DAS FUNDAMENT EINES JEDEN ERFOLGREICHEN SERVICEDESK-TEAMS DAR.

Kristin Pitz, Marketing Manager, TOPdesk Deutschland GmbH, www.topdesk.de

Anfragen ein und Ihr Team bearbeitet diese gewissenhaft. Aber eines Tages ruft ein leitender Manager an und benötigt eine Problemlösung vor einem wichtigen Meeting – und zwar jetzt sofort.

Dieses eine Mal stimmen Sie zu sich sofort dem Problem zu widmen. Leider wird deshalb der Arbeitsalltag an Ihrem Servicedesk bald Kopf stehen. Es hat sich schnell herumgesprochen, dass Sie sehr zuvorkommend sind. Bald ist die Ansicht weit verbreitet, dass jeder nur dann eine schnelle Problemlösung erwarten kann, wenn er den Servicedesk anruft. Sobald das erst einmal eingerissen ist, schwimmen Sie nur noch gegen den Strom.

Die Lösung: Wie können Sie also den Frieden, die Ordnung und das Wohlbefinden Ihres Teams wahren? Indem Sie nicht nachgeben. Der Grundgedanke hinter dem Incidentmanagement ist, dass Ihr Team alle Anfragen schnell, effizient und effektiv abarbeiten kann: ausstehende Aufgaben werden erfasst, nach Auswirkung und Dringlichkeit klassifiziert und dann dem zuständigen Mitarbeiter zugewiesen. Wenn es richtig gemacht wird, ermöglicht Ihnen dieser Prozess eine kontinuierliche und gleichbleibend hohe Servicedesk-Qualität.

Level 4: Datenpannen

Der ultimative Albtraum einer jeden Organisation sind Datenpannen. Da ist Panik nachvollziehbar. Dabei geht es nicht nur um finanzielle Kosten. Organisationen, denen eine Datenpanne unterläuft, sehen sich Reputationsschäden ausgesetzt und können sich sogar in Rechtsstreitigkeiten wiederfinden. Sie aktualisieren Ihre Sicherheitspraktiken regelmäßig und die Cybersicherheit hatte in den letzten Jahren oberste Priorität für Ihre Organisation. Trotzdem kam es zu einer Sicherheitsverletzung – und niemand weiß, was zu tun ist. Ihr Servicedesk wird mit endlosen Anrufen von verzweifelten Mitarbeitern konfrontiert, die nicht wissen, was zu tun ist. Es herrscht das reinste Chaos.

Die Lösung: Es liegt in Ihrem Verantwortungsbereich, Ihren Mitarbeitern zu vermitteln, dass sie Sie immer darüber informieren sollten, falls sie das Gefühl haben, dass etwas komisch läuft. Vielleicht haben sie versehentlich auf einen verdächtigen Link in einer E-Mail geklickt, jemand Externen ihren Laptop nutzen lassen oder einen USB-Stick verloren.

Ganz gleich, um was es sich handelt, es ist wichtig, dass Ihre Mitarbeiter verstehen, dass niemand sie an den Pranger stellen wird, wenn sie glauben, dass wegen ihnen das Risiko einer Datenpanne bestehen könnte. Dabei geht es vor allem um Schnelligkeit: Es ist essenziell Datenpannen so schnell wie möglich zu unterbinden. Ein Bewusstsein hierfür zu vermitteln, stellt einen wichtigen Teil dar, insbesondere, wenn viele Mitarbeiter im Homeoffice sind. 90 Prozent aller Datenpannen passieren aufgrund menschlicher Fehler. Deshalb sollten Sie dafür sorgen, dass all Ihre Kollegen auf dem neuesten Stand in Sachen Cybersicherheit Best Practices sind. Woher sollen sie schließlich wissen, dass sie etwas falsch gemacht haben, wenn sie die Grundlagen der Cybersicherheit nicht verstehen?

Kristin Pitz

Ganzheitliche Sicht wichtiger denn je

WELCHE IT- UND TECHNOLOGIETRENDS IM JAHR 2024 WICHTIG WERDEN

2024 wird ein entscheidendes Jahr werden. Darin sind sich die Branchenexperten einig. Leuchtturmprojekte von Branchen-Primi glänzen, doch in der Fläche läuft die Digitalisierung in Deutschland noch immer ausbaufähig. Die gute Nachricht: Kapazitäten für hochqualifizierten IT- und Technologiesupport, selbst für aufwendige Projekte, sind in Deutschland vorhanden – noch. Welche Trends im Jahr 2024 wichtig werden, darüber hat it management mit Benjamin Hermann, Geschäftsführer Zoi, gesprochen.

it management: *Wann werden wir das erste Mal mit dem Chatbot von Benjamin Hermann sprechen?*

Benjamin Hermann: Es wird nicht mehr lange dauern, bis „BENI", das Binär-Empathische Neuro-Interface kommt, aber leider bleiben dann die persönliche Beziehung und die Dynamik eines Gesprächs auf der Strecke. Fakt ist aber, dass das Thema KI die Grundlage für funktionierende Chatbots ist. Das wird uns auch im nächsten Jahr stark beschäftigen. Viele Unternehmen – international wie auch in Deutschland – fangen bereits an zu verstehen, dass die großen Mengen von textbasiertem Wissen, das in jedem Unternehmen vorhanden ist, in allen Ebenen und für viele verschiedene Zielgruppen anders genutzt werden kann als bisher. Die Regel „Man muss es nicht wissen, man muss nur wissen, wo es steht" wird zunehmend abgelöst von „Ich muss nur wissen, wie ich frage!" Der Einsatz und das Arbeiten mit KI wird künftig so selbstverständlich werden, wie wir heute den Taschenrechner im Smartphone bedienen. Es ist einfach da und funktioniert.

it management: *Trotzdem bleibt die Verantwortung für das Quellwissen ...*

Benjamin Hermann: Das sehen wir genauso. Die Verantwortung und die Exaktheit sind nach wie vor ungeheuer wichtig und beides braucht die gleiche detaillierte Sorgfalt. Nehmen wir eine Standardanweisung in einem Unternehmen der Pharma-Industrie. Niemand muss nach der Produktion einer Charge mehr Ordner mit SOPs durchforsten, um zu sehen, wie die zuführenden Schläuche für die einzelnen Stoffe zu reinigen sind. Das kann die KI über ein Device viel einfacher und eleganter erledigen. Doch wenn die hinterlegten Quellen nicht zu einhundert Prozent stimmen, kann auch die KI nicht funktionieren. Das kann dazu führen, dass Verunreinigungen eine andere Charge beeinflussen oder dass es bei Audits auffällt.

it management: *Bleibt die KI einzig auf das textbasierte Wissen beschränkt?*

Benjamin Hermann: Ganz sicher nicht. Hier stehen wir am Anfang einer viel größeren technischen Revolution, die viele Unternehmenskulturen noch einmal richtig umkrempeln wird. Die KI spielt ihre weiteren Stärken aus, wenn sie sich von menschgemachten Prozessen entkoppelt. Dies kann beispielsweise durch den Einsatz von Sensoren und Aktoren in Verbindung mit IIoT-sein. Die Sensorik hat mittlerweile einen guten und verlässlichen Stand erreicht, so dass sich automatisierte Prozesse beim Über- oder Unterschreiten von festgelegten Messwerten einrichten lassen. So lassen sich etwa Abweichungen in laufenden Produktionsprozessen leichter erfassen und abstellen oder bei Not- und Zwischenfällen leichter Menschenleben retten. Predictive Maintenance lässt dabei sogar einen Beitrag zum aktiven Umweltschutz zu, etwa wenn die integrierten Sensoren erkennen, dass eine Maschinenwartung noch nicht notwendig ist, da alle Prozesse innerhalb normaler Parameter funktionieren.

it management: *Welches Thema wird 2024 noch an Fahrt aufnehmen?*

Benjamin Hermann: Mit Sicherheit wird es die Sicherheit sein. Wir konnten es gerade wieder am Beispiel einer relativ jungen Hotelkette sehen: Die Cyber-Kriminellen schlafen nicht. Im Gegenteil: Sie professionalisieren sich selbst immer weiter und nutzen KI-Tools, um ihre Schadsoftware zu programmieren. Das ist die Kehrseite der Medaille. Und damit müssen wir umgehen lernen. Es bleibt keine Frage ob, sondern wann der Cyber-Angriff kommt – er gilt mittlerweile als gesetzt. Die Frage ist, wie gut sind die IT-Systeme von den Unternehmen geschützt, um derartige Bedrohungen abzuwehren und einzudämmen. Wir vergleichen es gerne mit einem Auto. Wir gehen selbstverständlich mit ihnen um, benutzen sie zu verschiedenen Zwecken, aber wir würden nie auf die Idee kommen, selbst eines zu bauen, weil uns die bestehenden zu teuer oder zu unsicher sind. Ähnlich verhält es sich mit IT-Systemen. Die sichersten Varianten gibt es nur in der Public Cloud. Der Unterbau aus Sicherheitssystemen, an dem jeden Tag weltweit hunderte von Expertinnen und Experten arbeiten, ist aus sicherheitstechnischer Sicht unschlagbar.

it management: *Aber für viele Unternehmen ist der finanzielle Faktor ausschlaggebend und es gibt Unternehmen, die aufgrund der Kosten die Cloud ganz oder teilweise wieder verlassen.*

Benjamin Hermann: Das ist korrekt – und schade. Denn leider fehlt dann an den Stellen wieder der sogenannte Blick über den Tellerrand. Hier ist die Funktion des Managements nötig, um die anfangs realisierten Kostenvorteile der Cloud auch langfristig zu sichern. Wenn bei einem internationalen Großunternehmen hunderte von Entscheidern nicht wissen, dass es nach der Migration in die Cloud nun ein Teil ihres Jobs ist, die Kosten im Blick zu behalten, kann ich die ausufernden Kosten gut verstehen. Der Kulturwandel, der mit der Cloud einhergeht, hat dann nicht funktioniert. Hier zeigt sich deutlich, dass mit der Cloud die Kommunikation über die Cloud genauso wichtig ist. Nur so kann das Wissen über die Vorteile und Verantwortungen an die richtigen Stellen gelangen. Wenn dann noch Managementfunktionen wie FinOps zeitgleich zum Start in die Cloud-Migration angestoßen werden, passieren solche Desaster nicht. Glücklicherweise lässt sich FinOps auch im Nachhinein noch implementieren. Dann ist das Kind zwar in den Brunnen gefallen, aber es sind lediglich die Kleidungsstücke nass geworden.

it management: *Ist FinOps dann nicht wieder eine weitere Leistung, die eingekauft und implementiert werden muss?*

Benjamin Hermann: Niemand wird gehindert, von vornherein umfassende und nachhaltige Cloud-Konzepte aufzusetzen. Von daher ja, der iterative FinOps-Prozess kostet Geld, wenn er nicht von Anfang an mitgedacht wird. Aber wenn sich hunderttausende Euro im Jahr sparen lassen, warum dann nicht wenige Tausend Euro investieren, zumal sich diese Investition schon nach kurzer Zeit amortisiert.

Es ist unterm Strich wie bei so vielen Investitionen: Unternehmen brauchen für ihre neuen Technologien wie Cloud, KI und IIoT einfach eine hochkomplexe Sicherheit, die auch unter dem wirtschaftlichen Aspekt langfristig funktioniert. Neben den Einzelbausteinen wird dieser umfängliche Ansatz aus meiner Sicht der wichtigste Trend sein, der Einzug hält oder halten muss, wenn die Unternehmen in Deutschland nachhaltig wettbewerbsfähig bleiben wollen. Hochqualifizierter und zertifizierter Support ist im Markt dafür derzeit noch vorhanden. Ich kann nur empfehlen, sich rechtzeitig dieser Hilfe zu versichern, denn wenn die Cloud-/KI-und IIoT-Wellen richtig losbrechen, sind diese Kapazitäten schnell knapp.

it management: *Stichwort Umweltschutz ...*

Benjamin Hermann: Das ist auch mein abschließender, aber nicht minder wichtiger Punkt: Aus meiner Sicht wird die Notwendigkeit zum verantwortungsvollen Umgang mit Ressourcen sowie die Möglichkeit, den eigenen Carbon Footprint zu reduzieren, immer notwendiger. Wir müssen aus eigenem Antrieb nachhaltiger und vor allem transparent nachhaltiger werden. Auch hier sind die Lösungen vorhanden: Google beispielsweise weist direkt aus, welche Menge an CO_2 für die abgerufenen Leistungen freigesetzt wird. Das wiederum kann für eigene Ausgleichsmaßnahmen genutzt werden.

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

THANK YOU

DIE REGEL „MAN MUSS ES NICHT WISSEN, MAN MUSS NUR WISSEN, WO ES STEHT" WIRD ZUNEHMEND ABGELÖST VON „ICH MUSS NUR WISSEN, WIE ICH FRAGE!"

Benjamin Hermann,
Geschäftsführer, Zoi TechCon GmbH, www.zoi.tech/de

MICROSOFT DEFENDER

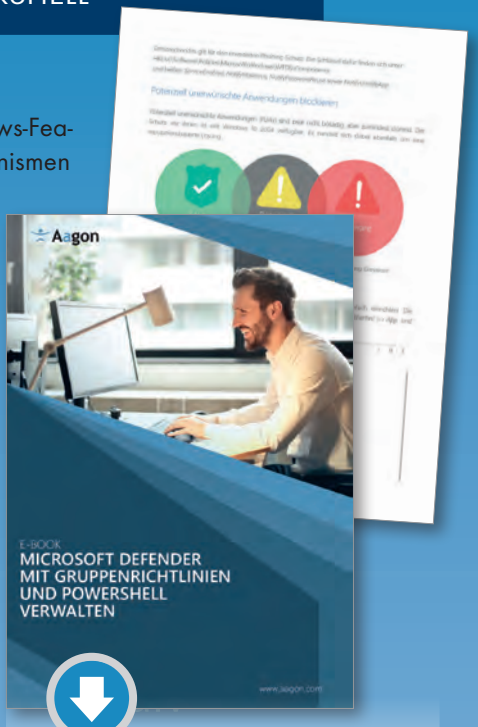
EINFACHE VERWALTUNG MIT GRUPPENRICHTLINIEN UND POWERSHELL

Unter der Marke Defender fasst Microsoft zahlreiche Windows-Features und Cloud-Services zusammen. Einige Schutzmechanismen sind erst kürzlich dazugekommen, andere wiederum wurden nachträglich umbenannt oder haben Namen, die sich schwer auseinanderhalten lassen (zum Beispiel Exploit-Schutz versus Exploit Guard).

Hinzu kommen Überlappungen in den Funktionen der diversen Komponenten. Um mit den Bordmitteln eine gute Abwehr gegen verschiedene Bedrohungen aufzubauen, muss man sich also erst einen Überblick über deren Fähigkeiten verschaffen.

Die Aagon GmbH bietet mit Defender Management eine zentrale Verwaltung des Windows-eigenen Malware-Schutzes, der in eine umfassende Client-Management-Lösung eingebettet ist und von der es auf vielfältige Weise profitiert.

Das folgende eBook widmet sich den Funktionen, die unmittelbar der Erkennung und dem Blockieren von schädlichen Programmen und Aktivitäten dienen.



Das eBook umfasst 57 Seiten und steht kostenlos zum Download bereit:
www.it-daily.net/download

Passgenaue Prozesse

WARUM SIE DER SCHLÜSSEL ZUR ERP-EFFIZIENZ SIND

Bei gehobenerer Mode ist es längt ein etabliertes Credo: Jeder Mensch ist einzigartig. Und damit ein Kleidungsstück wirklich optimal passt, muss es genau auf die Besonderheiten seines künftigen Trägers zugeschnitten sein. Eine Einsicht, von der auch Unternehmen in ihrem Tagesgeschäft profitieren können. Damit jeder Mitarbeiter seine oder ihre täglichen Aufgaben tatsächlich mit maximaler Effizienz erfüllen kann, bedarf es individueller, passgenauer Prozesse. Mit der richtigen ERP-Technologie werden diese im Handumdrehen Realität – ganz ohne teure Maßanfertigung.

Die klassische Herangehensweise an ERP-Prozesse ist nach wie vor der datenzentrierte Ansatz: In komplexen Masken erhalten Anwender Zugriff auf alle Informationen und Funktionen, die sie für ihre täglichen Aufgaben benötigen – und viele weitere darüber hinaus. Es liegt am Anwender, die richtigen Daten auszuwählen und die erforderlichen Arbeitsschritte in der sinnvollen Reihenfolge umzusetzen. Eine Freiheit, die in vielen Fällen unerlässlich ist – und doch nicht selten den Fokus auf das Wesentliche erschwert.

Um tatsächlich mit maximaler Effizienz arbeiten zu können, muss der datenzentrierte Ansatz durch eine prozesszentrierte Herangehensweise ergänzt werden. Durch passgenau zugeschnittene Prozesse erhält der Mitarbeiter einen Maßanzug für seine Abläufe. Solche individuellen Prozess-Flows sind nichts weniger als ein spürbarer Geschwindigkeits-Booster für die tägliche Arbeit und die zentralen Prozesse.

Passgenaue Prozesse – auf Konfigurationsbasis

Zeitgewinn in der täglichen Arbeit, schön und gut. Doch ein passgenaues Zuschneiden der Prozesse für jeden einzelnen Mitarbeiter assoziieren IT-Verantwortliche mit einem Mammutprojekt. Einem Projekt, das mit hohem Zeit- und Kostenaufwand verbunden ist und durch viele individuelle Anpassungen am Software-Standard künftige Update- und Wartungsprozesse beeinträchtigt.

Doch dies muss nicht so sein. Was Unternehmen benötigen, sind Möglichkeiten, erforderliche Prozesse auf einfache Art und Weise selbst zu modifizieren und auf ihre Anforderungen hin anzupassen. Denn wenn Mitarbeiter selbst zu Profi-Schneidern werden, ist der teure Gang zur Maßanfertigung obsolet.

APplus: Effizienz-Booster für das Innovationszeitalter

Mit ihrer ERP-Lösung APplus bietet die Asseco Solutions ihren Anwendern das Handwerkszeug, um genau das zu erreichen: Ihr innovatives Bedienkonzept verbindet die datenzentrierte Welt mit Prozessorientierung – und damit Einfachheit mit Flexibilität. Dies schafft die Basis für hochgradig effizientes Arbeiten in der täglichen Praxis.

Mit umfassenden Individualisierungsmöglichkeiten auf Basis der hochflexiblen Flow Boards macht es APplus seinen Anwendern dabei leicht, effiziente Prozesse auf ihre individuellen Anforderungen hin zuzuschneiden. Sei es rein auf Konfigurationsbasis oder mithilfe von Low-Code zur Entlastung der IT. Der Software-Standard bleibt stets unangetastet. Zusätzlich reduziert das passgenaue Arbeiten den Schulungsaufwand und verhindert durch das fließende Prozessdesign Fehler.

Passgenaue Prozesse also statt unbequemem „One Size Fits All" – und das zu deutlich geringeren Kosten. Dies ist der Schlüssel zur ERP-Effizienz für die dynamische Wirtschaftswelt von heute und morgen.

www.applus-erp.com

asseco SOLUTIONS

Mobiler ERP-Zugriff

DIE AUTOMATISIERUNG FÖRDERN

Je mehr Unternehmensprozesse mobil und damit digital werden, desto schneller und fehlerfreier können Produktionsunternehmen ihre Aufträge abwickeln. Vor diesem Hintergrund kommt dem ERP-System als zentraler Datendrehscheibe eine besondere Rolle zu. Welche Ansätze zum Erfolg führen können, fragten wir Nikas Schröder, Vorstand für die Bereiche Produkt, Entwicklung und IT bei ams.Solution.

it management: *Herr Schröder, welche Trends sehen Sie bei der mobilen Nutzung von ERP-Funktionalität bei Ihren mittelständischen Kunden und Interessenten?*

Nikas Schröder: Da das ERP-System in allen Unternehmensbereichen zum Einsatz kommt, sind die Möglichkeiten der mobilen Nutzung vielfältig. Dazu zählen klassischerweise die Lagerverwaltung, der Wareneingang, die Personal- und die Auftragszeiterfassung und die gesamte Materialwirtschaft. Um Baugruppen oder Halbfertigteile an ihrem jeweils aktuellen Standort im Unternehmen und an allen Unternehmensproduktions- und -lagerstandorten verorten zu können, arbeitet ams zudem gerade mit einem großen Pilotkunden an der Ent-

wicklung eines innovativen Logistikmoduls, über das innerbetriebliche Materialbewegungen getrackt werden können. Das Modul ams.erp Logistics wird ab dem vierten Quartal dieses Jahres als Add-on für weitere interessierte Kunden zur Verfügung stehen.

Insgesamt beobachten wir seit etlichen Jahren eine stetig wachsende Anzahl von Maschinen und Geräten, die in die mobilen Prozesse eingebunden werden. Der standortunabhängige Zugriff auf ERP-Funktionalitäten erfolgt über verschiedenste Gerätetypen hinweg – angefangen bei Notebooks und Laptops über Tablets, Smartphones und Rugged Devices bis hin zu Smartwatches oder Fahrzeugcockpits. Auch sogenannte IoT-Devices, also leichtgewichtige, netzwerkfähige Mini-Computer mit kostenlosen Betriebssystemen, die an Material, Bauteilen oder Containern angebracht werden, können jederzeit eigenständig ihre Position an entsprechende Cloud-Server senden.

it management: *Was ist der größte Vorteil des mobilen ERP-Zugriffs bezogen auf die Prozessabwicklung?*

Nikas Schröder: Der mobile ERP-Zugriff sorgt dank der zwangsläufig einhergehenden Automation für schnellere Abläufe. Werden ehemals manuelle und papierbasierte Tätigkeiten digitalisiert, reduziert sich die Fehleranfälligkeit immens, während zugleich die Transparenz rapide zunimmt. Die Prozessverantwortlichen erhalten nahezu in Echtzeit eine lückenlose Dokumentation, was zu wesentlich fundierteren Entscheidungen auf allen Ebenen führt.

it management: *Wo bringen mobile ERP-Prozesse den größten Nutzen?*

Nikas Schröder: Solange die Datensicherheit gewährleistet ist, lohnt sich der mobile ERP-Einsatz überall dort, wo die Verfügbarkeit aktueller Informationen die Unternehmensprozesse wie beschrieben beschleunigt. Letztlich kommt es für die Anwenderunternehmen immer darauf an, unter wirtschaftlichen Aspekten gemeinsam mit ihrem ERP-Anbieter zu eruieren, wo sich absehbar der größte Nutzen ergeben könnte, um von dort aus in angrenzende Bereiche vorzustoßen.

DER MOBILE ERP-EINSATZ LOHNT SICH ÜBERALL DORT, WO DIE VERFÜGBARKEIT AKTUELLER INFORMATIONEN DIE UNTERNEHMENSPROZESSE BESCHLEUNIGT.

Nikas Schröder,
Vorstand Produkt, Entwicklung und IT,
ams.Solution AG, www.ams-erp.com

In diesem Zusammenhang bietet ams mit ams.flex ein flexibles Werkzeug, das die unkomplizierte und schnelle Erstellung individueller Geschäftsprozesse mittels plattformunabhängiger Business-Apps ermöglicht. War die Abbildung mobiler Szenarien in der Vergangenheit mit einem recht hohen Zeit- und Personalaufwand verbunden, reduziert sich dieser Aufwand dank der Lösung auf einen Bruchteil. Programmierkenntnisse sind nicht erforderlich. Stattdessen erfolgt die App-Erstellung ohne Quellcode über eine webbasierte, grafische Konfigurationsoberfläche, auf der die neuen Prozesse auch gleich live getestet und ausgerollt werden können. Den sicheren und kontrollierten Zugriff auf ams.erp gewährleistet dabei das universelle Application Interface ams.erp API.

it management: *Welcher Vorkehrungen bedarf es, um den mobilen Zugriff performant und sicher zu gestalten?*

Nikas Schröder: Unabdingbar für den mobilen Zugriff auf die ERP-Funktionalität ist das Vorhandensein performanter Netzwerke, die allen Sicherheitsanforderungen entsprechen. In Deutschland gibt es leider noch zu viele Standorte ohne entsprechende Netzabdeckung. Dennoch nimmt die Breitbandnutzung im Zuge des Ausbaus der 5G-Technik insgesamt zu. Innerhalb der Unternehmensgebäude und in den Produktionshallen übernehmen gesicherte WLANs den Datentransport.

Industriespionage ist für unsere Kunden, die als Einzelfertiger in vielen Bereichen zu den weltweit führenden Unternehmen gehören, eine ernsthafte Bedrohung. Demnach müssen neben den Software-Produkten auch die Hardware- und Netzwerkkomponenten die entsprechenden Sicherheitsanforderungen erfüllen. Eminent wichtig ist es in diesem Zusammenhang, die Mitarbeitenden auf mögliche Gefahrenquellen hinzuweisen und sie fortwährend im Umgang mit Geräten und Software zu schulen.

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

Nachhaltige Zukunft

FÜNF WEGE, WIE 5G DIE NACHHALTIGKEIT FÖRDERT

Bei den globalen Bemühungen um Umweltschutz und nachhaltige Lebensweisen kommen den Einsparungen von Emissionen und der Förderung von ressourcenschonenden Technologien Schlüsselrollen zu. Viel Potenzial birgt dabei der Mobilfunkstandard 5G, der Daten schneller und effizienter übertragen kann als herkömmliche Technologien. G+D zeigt an fünf Beispielen, wie 5G im Alltag Emissionen einspart und Nachhaltigkeit fördert.

#1 Hohe Energieeffizienz

Je mehr Informationen Geräte über das Mobilfunknetz pro Energieeinheit senden und empfangen, desto geringer ist ihr Stromverbrauch. Im Vergleich zu 4G erwarten Experten mit dem 5G-Standard eine Effizienzsteigerung um den Faktor einhundert – wodurch Mobilfunkbetreiber in der Lage sind, hohe Energiemengen einzusparen und Emissionen zu reduzieren. Gleichzeitig ist die verbesserte Energieeffizienz eine wichtige Voraussetzung, um den erwarteten Anstieg der Datenübertragungen technisch umzusetzen.

#2 Steuerung und Automatisierung

Durch den Einsatz von Sensoren im 5G-Netz sind Unternehmen in der Lage, den Status von Anlagen wie Fertigungsmaschinen, Aufzügen, Windkrafträdern oder Lastwagen in Echtzeit zu überwachen. Indem Unternehmen die Wartungen exakt planen und Ausfallzeiten vermeiden, reduzieren sie den Energiebedarf und senken ihre Betriebskosten. Die Sensoren spielen auch bei der automatischen Anlagensteuerung eine zentrale Rolle, indem sie große Datenmengen in Analyseplattformen einspielen. Die gesammelten Informationen maximieren im Zusammenspiel mit Künstlicher Intelligenz und digitalen Zwillingen die Leistung der Anlagen, die als Ergebnis effizienter arbeiten und weniger Energie verbrauchen.

#3 Effektivere Produktionsketten

Schnelle Datenübertragung und geringe Latenzzeit sind die Voraussetzungen für die weitere Digitalisierung der industriellen Produktion. 5G öffnet die Tore für vernetzte Anlagen oder automatisierte Transportsysteme, die für ein Höchstmaß an Effizienz innerhalb von Produktionsprozessen sorgen. Auf diese Weise reduziert die Technologie den Energiebedarf und spart CO2-Emissionen ein.

#4 Kontrollierte Landwirtschaft

Die Agrar- und Ernährungswirtschaft ist nicht nur von entscheidender Bedeutung bei den Bemühungen um eine nachhaltigere Zukunft, sie bietet sich auch für den Einsatz von 5G-Technologien an, um Emissionen zu senken und den Ertrag zu steigern. Der Ansatz einer intelligenten Landwirtschaft nutzt 5G-IoT-Sensoren, um Daten für bessere Entscheidungen zu sammeln – beispielsweise indem sie den Feuchtigkeitsgehalt von Böden überwachen oder den optimalen Zeitpunkt zum Düngen bestimmen. Der 5G-Standard realisiert aber auch den Einsatz von Drohnen zur Analyse von Grünflächen, automatisierten Maschinen und die Überwachung der Gesundheit von Tieren.

#5 Smart Cities

5G ermöglicht die Entwicklung von Smart Cities, in denen vernetzte Geräte Echtzeitdaten sammeln und austauschen. Diese Daten können zur Optimierung des Energieverbrauchs, des Verkehrsflusses, der Abfallwirtschaft und mehr genutzt werden. Durch die effiziente Verwaltung von Ressourcen können Städte ihren CO2-Fußabdruck verringern und die Lebensqualität der Einwohner verbessern.

www.gi-de.com

Der CO_2-Footprint eines IT-Leiters

MIT DER RICHTIGEN LIZENZIERUNG DIE UMWELT SCHONEN

Den CO_2-Footprint, den kennt jeder. ‚Dank' ihm wissen IT-Verantwortliche jedenfalls, dass sie mit jedem neu angeschafften Computer für beachtliche Treibhausgasemissionen (etwa 700 Kilogramm je Desktop PC) verantwortlich sind. Betrieblich genutzte Hard- und Software verursacht enorme ökologische Schäden, hohe CO_2-Emissionen und Umweltverschmutzungen. Der Microsoft Solutions Partner VENDOSOFT bietet deshalb eine Lizenzberatung, die neben der Cloud auch gebrauchte Software umfasst. Denn mit älteren Programmen und hybriden Lösungen lässt sich CO_2 einsparen. Und ganz nebenbei eine Menge Geld.

Umweltschonend ohne Cloud

„Für immer mehr Kunden ist Nachhaltigkeit in ihrer IT jetzt ein Thema," sagt Geschäftsführer Björn Orth. So auch für einen Anlagenbauer aus dem Badischen, der 270 PC-Arbeitsplätze, Notebooks und Server mit gebrauchten Microsoft-Lizenzen ausstattete. Das spart im Vergleich zu neuen Lizenzen ein Drittel an Kosten. Vor allem aber „zahlt re-used Software genau wie re-furbished Hardware auf unsere Nachhaltigkeitsziele ein", erklärt der IT-Leiter. Gebrauchte Software helfe, die Lebensdauer der Geräte zu verlängern, weil Systemanforderungen an Prozessor, Festplatte und Arbeitsspeicher gleichblieben. „Bei großen Software Upgrades werden die APIs teilweise inkompatibel oder die Rechner benötigen signifikant mehr Leistung und Speicherkapazität." Früher wurden bei dem Anlagenbauer einfach neue Computer, Tablets und Server angeschafft. Heute sieht man das unter ökologischen Gesichtspunkten. Um den CO_2-Footprint zu verbessern, bleibt das Unternehmen bei Software-Versionen, die noch viele Jahre funktionstüchtig sind und Sicherheits-Updates erhalten, sich aber nicht permanent und automatisch selbst upgraden.

Hybrid hilft CO_2 sparen

Was in der Produktion funktioniert, ist nicht für jedes Unternehmen und nicht für jede Abteilung die Lösung. Remote-Arbeit oder standortübergreifende Kollaboration machen die Cloud zur unverzichtbaren Datendrehscheibe. Aber auch hier gibt es laut Björn Orth Einsparpotenziale. „Wir vernetzen natürlich viele Kunden über M365. Überall dort jedoch, wo das nicht erforderlich ist – und das ist bei sehr vielen Computerarbeitsplätzen der Fall – empfehlen wir die günstige und ressourcenschonende Gebrauchtsoftware." Um das herauszufinden, hinterfragen seine Lizenzprofis die vorhandene IT-Infrastruktur. Bei einer großen Spedition etwa kam kürzlich heraus, dass sich 60 Lagerarbeiter 25 Rechner teilen. Jeder Anwender war dort einzeln lizenziert. Anders lässt es die Microsoft Cloud nicht zu. Mit Office als gebrauchte On-Premises-Software ist jedoch eine Lizenzierung nach Geräten möglich. 25 einmalig anzuschaffende Office-Lizenzen standen damit 60 jährlich zu bezahlenden Business-Premium-Plänen gegenüber. Eine Kostenersparnis von 43 Prozent. Der Kunde zögerte nicht lange und wechselte auf ‚die Gebrauchten'. Dem CO_2-Footprint kommt das ebenfalls zugute – auch wenn sich der nicht ganz so einfach beziffern lässt.

www.vendosoft.de

FÜR MEHR NACHHALTIGKEIT IN IHREM FACHBEREICH KÖNNEN SICH IT-VERANTWORTLICHE FRAGEN: BRAUCHEN WIRKLICH ALLE UNSERE MITARBEITENDEN DIE NEUESTE VERSION EINER SOFTWARE BEZIEHUNGSWEISE DIE CLOUD? ODER ERFÜLLT EINE ON-PREMISES-VERSION WIE MICROSOFT OFFICE 2019/2021 NICHT ALLE FUNKTIONALITÄTEN? ZWEI EINFACHE FRAGEN, DIE DEN CO_2-FOOTPRINT EINES UNTERNEHMENS SIGNIFIKANT SENKEN KÖNNEN.

Björn Orth, Geschäftsführer, Vendosoft GmbH, www.vendosoft.de

PLUS

Lizenzoptimierung ist ein wichtiger Beitrag zu mehr Nachhaltigkeit im Unternehmen. Bei diesem Prozess unterstützt VENDOSOFT mit umfassender, ressourcenschonender und kosteneffizienter Lizenzberatung.
www.vendosoft.de/nachhaltige-it

Holistischer Ansatz

IT-SUSTAINABILITY GEHT ÜBER EINE ÖKOLOGISCHE GREEN-IT HINAUS

Nachhaltigkeit ist bei der Flender GmbH Chefsache, denn der CEO steht dem Corporate Social Responsibility-Board vor. Der freiwillige Nachhaltigkeitsbericht seit 2020/21 zeigt, dass das Thema CSR fest im Unternehmen verankert ist. CIO Stefan Heizmann möchte die Unternehmens-IT künftig zum „Trailblazer", also Wegbereiter, der Nachhaltigkeit transformieren. Dafür holte er die IT Management-Beratung kobaltblau ins Haus. Ihn überzeugte der holistische Ansatz.

Eine nachhaltige IT steht bei Unternehmen zunehmend auf der Tagesordnung. Laut einer aktuellen IDC Studie stellen zwei Drittel der befragten Firmen 2023 im Vergleich zum Vorjahr das gleiche oder ein höheres Budget für nachhaltige IT-Projekte zur Verfügung. Hinsichtlich ihrer eigenen IT-Infrastruktur messen Unternehmen bislang vor allem den Energieverbrauch und damit eine Kennzahl, die vor allem die ökologische Dimension der Nachhaltigkeit betrifft. Für eine ganzheitliche IT-Nachhaltigkeitsstrategie spielen jedoch weitere Faktoren eine ebenfalls wichtige Rolle. Unternehmen müssen sich von einer eindimensionalen Betrachtung der Green-IT lösen und einen ganzheitlichen Ansatz fokussieren, damit die IT ihren Beitrag zu einem nachhaltigeren, erfolgreichen Geschäft leisten kann und als internes sowie externes Positivbeispiel dient.

So auch die Flender GmbH: Das Münsterländer Unternehmen stellt sich dieser Verantwortung. Seit 40 Jahren produziert Flender für diverse Industriebranchen Getriebe, Kupplungen, Generatoren und Komponenten. Im Rahmen seiner Nachhaltigkeitsstrategie hat Flender die niedrig hängenden Früchte der Green-IT bereits geerntet. Das Unternehmen hat aus den Unternehmenszielen und -werten

TOP 5-HERAUSFORDERUNGEN BEI DER UMSETZUNG VON NACHHALTIGKEITSZIELEN

Quelle: IDC Studie „IT & Sustainability in Deutschland 2023, Juni 2023

eine neue IT-Strategie abgeleitet und will mit IT-Sustainability durch einen ganzheitlichen Ansatz deutlich mehr bewegen, als es der eindimensionale Blick auf ökologische Aspekte der IT, beispielsweise mit einer energieeffizienten Hardwareausstattung, vermag.

IT-Sustainability Health Check leitet die Transformation

Auf der Grundlage der 17 UN-Sustainable Development Goals (SDG) entwickelte kobaltblau den IT-Sustainability Health Check. Dieser enthält 21 IT-Sustainability Values, die sich an den ESG-Kriterien orientieren, die Nachhaltigkeit für Unternehmen greifbar machen. ESG steht für Environment, Social und Governance, also Umwelt, Soziales und Unternehmensführung. Der Health Check dient als Basis für Maßnahmenvorschläge, die priorisiert und passgerecht in die IT- und CSR-Strategie von Flender integriert werden. Bisher hat Flender eine nachhaltige IT vorrangig unter den Aspekten Energiekosten und CO_2-Emissionen betrachtet. Sie ist aber Enabler für alle drei ESG-Kategorien und muss diese Verantwortung ganzheitlich wahrnehmen. Die IT soll den Weg für Digitalisierung und Automatisierung, eine organisationale Agilität und nachhaltiges Verhalten ebenso bereiten wie für New Work und entsprechende Leadership-Kultur. Sie muss die Fachabteilungen stärken, um Compliance-Richtlinien (Governance) einzuhalten, Kunden und Mitarbeitende zu gewinnen und zu halten. Sie muss das Management mit Datenmodellen und -auswertungen in Echtzeit versorgen. Für die Transformation zu einer nachhaltigen IT wird der Mehrwert der IT im Kontext Nachhaltigkeit neben der Erhöhung der Effizienz im Unternehmen anhand des Beitrags für die ökologischen und sozialen Ziele bemessen.

kobaltblau begleitet Flender bei der Bewusstseinsschaffung, Erhebung der Baseline und Ableitung eines ganzheitlichen IT-Nachhaltigkeitszielbilds. Schon nach dem initialen Impulsworkshop konnte Flender nachvollziehen, dass das Unternehmen den IT-Fußabdruck und die Potenziale für das Business viel konkreter analysieren und weiterentwickeln muss.

DAS REIFEGRADMODELL ZEICHNET DEN WEG ZU EINER NACHHALTIGEREN IT VOR, DIE ALS ENABLER FÜR DAS GESAMTE BUSINESS DIENT.

Michaela Lackner, Senior Manager, kobaltblau Management Consultants GmbH, www.kobaltblau.de

Die 21 kobaltblau IT-Sustainability Values sind mit einem Reifegradmodell hinterlegt. Für jedes der fünf Level (von 0 – passiv bis 4 – innovativ) sind Maßnahmen beschrieben und wie sie erreicht werden können. Bei einigen der 21 Values konnte sich Flender auf Level 1 – reaktiv und 2 – proaktiv sowie 3 – prädiktiv, bei wenigen nur bei 0, einordnen. Das folgende Beispiel „Green Application Services" macht deutlich, welchen Entwicklungspfad Flender vom Einstiegslevel auf den Reifegrad Level 3 einschlagen wird.

Green Coding: Jede unnötige Code-Zeile spart CO_2 ein

Weniger Datenvolumen in Internetanwendungen verursachen weniger Emissionen. Im Durchschnitt haben mobile Webseiten 2,2 Megabyte Datenvolumen. Das hat die englische Digitalmarketingagentur Clickz 2017 ermittelt. 68 Prozent dieses Volumens entfiel auf Bilder. Würde das Volumen auf nur ein Megabyte bei gleicher Usability reduziert, würde das 50 Prozent der Emissionen bei der Anwendung einsparen. Bisher spielten diese Erkenntnisse für den Softwarekauf und die Anwendungsentwicklung bei Flender allerdings keine große Rolle. Neben dem Preis soll künftig eine Entscheidungsmatrix Kriterien berücksichtigen, um Level 1 zu erreichen. Neben Effizienz und dem CO_2-Fußabdruck einer gekauften Anwendung sollen Konfiguration

(Anpassbarkeit), Support, Wartungsaufwand, Virtualisierung und auch Kompatibilität mit bestehenden Anwendungen sowie die Anzahl der Code-Lines zu den Prüfkriterien gehören. Eine neue Guideline für „Green Coding" formuliert die Anforderungen an „Grüne Architektur", die sowohl die Bereiche Anwendungs-Logik, -Methodik und -Plattform umfasst. Architekturprinzipien wie Microservices, No-Code und Low-Code bringen Performance- und Effizienzvorteile.

Die Auswahl der Programmiersprache und der Anspruch auf „Zero Waste Code" haben ebenfalls Auswirkungen auf den CO_2-Fußabdruck einer Software. Die Löschung redundanter und nichtfunktionaler Code-Zeilen sowie die Vermeidung von übermäßigem Tracking oder JavaScript senken den Stromverbrauch. Methodisch gilt es, Datenbanken und Dateien zu komprimieren, speicheroptimierte Symbole einzusetzen und automatisch startende Videos zu meiden. Noch gibt es für „grüne" Software keine festgeschriebenen Standards oder Zertifizierungen. Green Coding-Aspekte tragen zu einer Optimie-

rung der Ökobilanz einer Software bei. Dies macht sie aber per Definition nicht gleich „nachhaltig".

Soziale Effekte und Business-Aspekte

Ein gesamtheitliches Verständnis für IT-Sustainability bedeutet mehr, als „nur" die Umweltkomponente zu berücksichtigen. Der IT-Sustainability Check von kobaltblau bewertet zusätzliche Aspekte, wie die Usability einer App, Barrierefreiheit, intuitive Bedienbarkeit und die Sprachgestaltung der Inhalte, um die Arbeitseffizienz zu erhöhen. Weitere soziale Aspekte beziehen sich auf die Fähigkeit der IT-Organisation, ihren Mitarbeitenden das notwendige Know-how zur Wartung und Weiterentwicklung von Software zur Verfügung zu stellen. So kann eine ältere Programmiersprache zwar weniger Energie bei der Ausführung verbrauchen. Aber: Es kostet Zeit und Geld, die Kenntnisse dieser Programmiersprachen aufrechtzuerhalten. Dies ist auf Dauer also weder gut für die ökologische noch die soziale und wirtschaftliche Nachhaltigkeit. Weitere Aspekte vor allem auch im Kontext Governance sind, ob eine Anwendung DevOps-fähig ist, neue Organisationsmodelle zulässt und welchen Schulungsbedarf sie auslöst. Aus Compliance-Sicht (Governance) sollte eine Programmiersprache „state-of-the-art" für Microservices, Clustering und Edge Computing sein. Sie muss alle Anforderungen für Daten- und Cybersicherheit sowohl der nationalen als auch internationalen Gesetze sowie Standards wie der ISO/ICE 270001 erfüllen. Zudem muss die Anwendung über ihren gesamten Lebenszyklus wartungsfähig sein.

MIT EINEM HOLISTISCHEN ANSATZ BEWEGEN WIR MEHR, ALS ES DER EINDIMENSIONALE BLICK AUF ÖKOLOGISCHE ASPEKTE ERLAUBT.

Stefan Heizmann, CIO, Flender GmbH, www.flender.com

Balance zwischen allen ESG-Kriterien finden

Sustainability zieht sich für Flender künftig durch alle Unternehmensbereiche, wobei die IT als Enabler für alle anderen dienen kann und sollte. Sie muss dabei immer wieder auf eine ausgewogene Balance aller ESG-Kriterien achten und dabei veraltete Logiken, Methoden und Architekturen kritisch hinterfragen und aufgeben. Die IT wird dadurch erst zum „Trailblazer" für die Digitalisierung, den sozialen Wandel in der Arbeitsorganisation sowie für eine dauerhaft innovative Unternehmensführung.

Michaela Lackner, Stefan Heizmann

T Systems

RETHINK
THE SYSTEM

WHO THINKS BEFORE AI ACTS?

Let's guide
Artificial Intelligence
in the right direction.

Künstliche Intelligenz soll vereinfachen, beschleunigen, verbessern. Und zwar am Menschen orientiert. Damit das gelingt, müssen wir die Entwicklung und Nutzung von KI neu denken: So unterstützt T-Systems Kunden bei ihrer Transformation hin zu einem verantwortungsvollen, KI-gesteuerten Unternehmen.

Jetzt mehr erfahren:
www.t-systems.com/ki

Twin Transition

NACHHALTIG UND DIGITAL – EINE FRAGE DER FÜHRUNG

Die intelligente Nutzung von Daten ermöglicht es, nicht nur effizienter, sondern auch nachhaltiger zu wirtschaften. Wenn sich Unternehmen mit Digitalisierungsstrategien auseinandersetzen, ist es daher sinnvoll, Nachhaltigkeitsthemen gleich mitzudenken.

Die Klimaziele der Zukunft lassen sich nicht mit den Technologien von gestern erreichen. Darum führt für Unternehmen kein Weg daran vorbei, den Übergang zu einem digitalen und nachhaltigeren Wirtschaften zu schaffen. Dabei spricht man von der sogenannten Twin Transition: Es geht darum, den CO_2-Fußabdruck zu reduzieren und durch Digitalisierung eine nachhaltigere und auch effizientere Arbeitsweise zu ermöglichen.

Doch wie weit ist dieses Bewusstsein bereits in Unternehmen angekommen? Eine aktuelle Studie von Futurice in Zusammenarbeit mit dem Marktforschungsinstitut YouGov, die 250 Führungskräfte unterschiedlicher Branchen befragt hat, zeigt: Es gibt noch immer deutlichen Aufholbedarf in Sachen nachhaltiger und digitaler Transformation. Obwohl neue Klimaschutzziele und Regulierungsvorgaben das Thema Nachhaltigkeit eigentlich in den Fokus von Unternehmen rücken sollten, sagen 46 Prozent der Befragten, dass Investitionen in diesem Bereich über die letzten Jahre stagnieren. Bei 36 Prozent der Unternehmen sind sie sogar zurückgegangen.

Das Weltwirtschaftsforum schätzt, dass durch den Einsatz digitaler Lösungen die weltweiten Emissionen um 20 Prozent ge-

senkt werden können, was einen enormen Einfluss auf die weltweite CO_2-Reduzierung hätte. Nachhaltigkeit – gerade in Verbindung mit der Digitalisierung – trägt jedoch nicht nur dazu bei, die Ressourcen unseres Planeten zu schonen, sondern ist auch wirtschaftlich sinnvoll, da sie ein besseres Preis-Leistungs-Verhältnis ermöglicht, Zeit spart und Mitarbeiter von ressourcenintensiven Tätigkeiten entlastet, was besonders wichtig ist, um den Fachkräftemangel zu bekämpfen. Doch in Unternehmen fehlt es an ganzheitlichen Strategien, um die Twin Transition voranzutreiben: 41 Prozent der befragten Führungskräfte geben an, dass es in ihren Unternehmen noch keine Strategie für eine nachhaltige und digitale Transformation gibt

Neben fehlenden Investitionen und unzureichenden Transformationsstrategien, gibt es noch weitere Herausforderungen, die Führungskräfte bei der Twin Transition sehen: 28 Prozent sehen eine große Hürde in der Komplexität der Themen, 25 Prozent beklagen mangelnde Unterstützung der Politik. Zudem sagen 23 Prozent der Befragten, dass ihnen für ein solches Vorhaben vor allem die notwendigen Ressourcen fehlen: digitale Infrastruktur, nachhaltige Technologien und Fachpersonal.

Mehr Integration: Silo-Denken abbauen

Damit Unternehmen innovativ und relevant bleiben, ist es notwendiger denn je, interne Silos aufzubrechen und die Zusammenarbeit auf breiter Ebene zu verbessern. Legt man eine ganzheitliche Strategie zugrunde, lassen sich zahlreiche Akteure erkennen, deren Zusammenarbeit bei der Umsetzung der Twin Transition von großer Bedeutung ist:

EINE DOPPELTE TRANSFORMATION LÄSST SICH NUR DURCH VERÄNDERUNGEN IN DER UNTERNEHMENSSTRUKTUR UND -KULTUR UMSETZEN.

Sven-Anwar Bibi, Managing Director, Futurice, https://futurice.com

- **Data Scientists:** Sie sind dafür zuständig, eine solide Datenarchitektur aufzubauen, um sicherzustellen, dass Sie Zugang zu den erforderlichen Daten haben und über die Mittel verfügen, diese zu interpretieren, um fundierte Entscheidungen treffen zu können.
- **Technology Experts:** Sie sind maßgeblich daran beteiligt eine Technologiearchitektur zu planen, aufzubauen und zu pflegen, um das Wachstum des Unternehmens nachhaltig zu unterstützen.
- **Agile Coaches:** Deren Aufgabe ist es, die Organisation anpassungsfähiger und reaktionsfähiger auf Veränderungen machen. Sie ermöglichen eine kontinuierliche Verbesserung von Prozessen und Ergebnissen.
- **Strategy & Culture Experts:** Sie entwerfen eine klare Vision und einen Fahrplan und bringen diese mit den Zielen und Werten des Unternehmens in Einklang. Sie beseitigen alle kulturellen Barrieren, die den Fortschritt behindern könnten und arbeiten an Strategien, wie alle in den Wandel mit eingebunden werden können.
- **Service Designer:** Sie entwickeln innovative Lösungen, die den Bedürfnissen der Organisation und ihrer Stakeholder entsprechen und gleichzeitig die sozialen und ökologischen Auswirkungen berücksichtigen.

Der Fokus liegt dabei vor allem auf den Bedürfnissen der Kunden: Welche Dienstleistungen und Lösungen wollen Kunden? Und welche leisten einen wirksamen Beitrag zu einer nachhaltigen Zukunft? Die Beantwortung dieser Fragen ist von entscheidender Bedeutung und erfordert eben eine umfassende Datenanalyse. Damit auch alle Mitarbeitenden mit den erhobenen Daten und Analysen sinnvoll arbeiten können, ist es daher unumgänglich in die sogenannte „Digital Literacy" der Belegschaft zu investieren. Durch gezielte Weiterbildungsmaßnahmen können Mitarbeitende befähigt werden mit Hilfe digitaler Technologien sicher und angemessen auf Informationen zuzugreifen, sie zu verstehen, zu bewerten und zu verwalten.

Ohne Kulturwandel keine Transformation

Neben den technologischen Anforderungen haben Transformationsprojekte immer auch einen kulturellen Aspekt: Lang etablierte Vorgehens- und Arbeitsweisen werden dabei häufig verändert. Dies ist auf Seiten der Arbeitnehmer häufig mit einem Gefühl von Unsicherheit verbunden. Deshalb treffen Transformationsvorhaben in der Belegschaft zu Beginn meist auf Widerstand. Mit einer nachhaltigen digitalen Transformation geht also immer auch ein Wandel der Unternehmenskultur einher, der gut moderiert und geführt werden muss. Damit Zweifel und Ängste erst gar nicht entstehen, ist also vor allem das Leadership gefragt. Es ist an den Füh-

rungskräften, eine klare Vision aufzuzeigen und Ziele zu definieren, auf die das gesamte Unternehmen hinarbeiten soll. Ohne diese Faktoren und ohne den Mut die gesetzten Pläne zu verfolgen, ist es schwierig die erforderliche Unterstützung und Akzeptanz im Unternehmen zu gewinnen. Nicht umsonst gibt ein Drittel der Befragten an, dass sie Führungskompetenz als eine der wichtigsten Voraussetzungen sehen, um eine nachhaltige und digitale Transformation zu meistern.

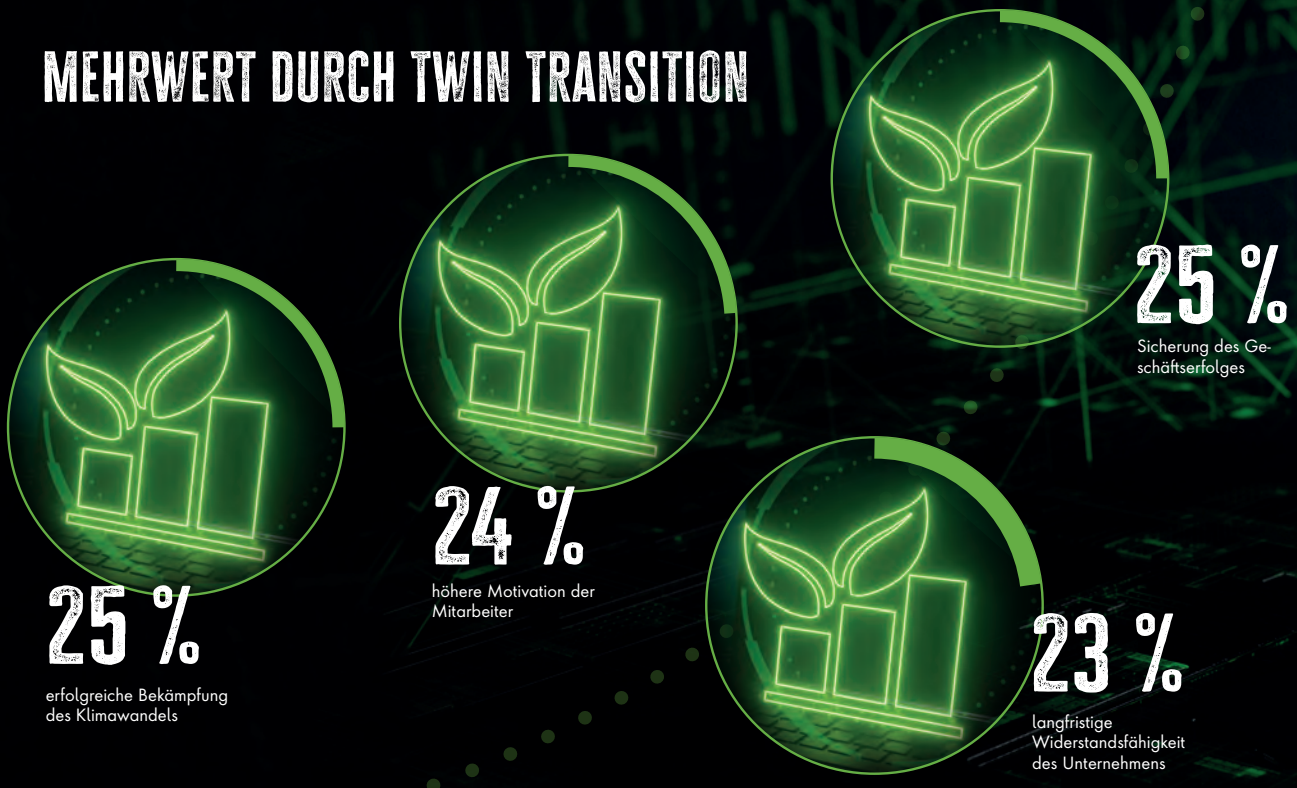
Kurz gesagt: Veränderungen müssen von der Unternehmensspitze angestoßen werden. Von dort aus geht der Wandel dann über die Leadership-Teams in die gesamte Organisation. Viele Beschäftigte sind begeistert und durchaus bereit, Veränderungen mitzugehen – wenn sie aber nicht genügend Unterstützung oder die entsprechenden Tools an die Hand bekommen, schlägt die Begeisterung schnell in Frustration um. Führungskräfte sind außerdem besonders gefordert, wenn es darum geht, Brücken zwischen den verschiedenen Stakeholdern zu schlagen. Es liegt auch an ihnen, eine gemeinsame Sprache zu finden und dieses neue Miteinander vorzuleben. Die wichtigsten Kompetenzen von Führungskräften, die notwendig sind, um eine Twin Transition zu gestalten, sind also: strategisches Denken und Handeln, Führungskompetenz sowie Kommunikations- und Kooperationskompetenz.

Twin Transition: Schlüssel zur Zukunftsfähigkeit

Eine doppelte Transformation lässt sich nur durch Veränderungen in der Unternehmensstruktur und-kultur umsetzen. Es gilt, interne Prozesse neu aufzusetzen oder anzupassen sowie die Belegschaft durch einen geführten Kulturwandel beim Transformationsprozess mitzunehmen. Da meist auch die Anschaffung neuer Tools und Technologien notwendig ist, kommen größere Investitionen in die IT beziehungsweise in die digitale Infrastruktur noch dazu. Hier kann KI in den nächsten Jahren zum großen Gamechanger werden.

Nehmen Unternehmen diese Herausforderungen an, entstehen dadurch auch zahlreiche Chancen. Gefragt nach dem Mehrwert, den die Twin Transition bringen kann, nennen 25 Prozent der Befragten die erfolgreiche Bekämpfung des Klimawandels, 25 Prozent die Sicherung des Geschäftserfolgs, 24 Prozent eine höhere Motivation der Mitarbeitenden und 23 Prozent die langfristige Widerstandsfähigkeit und finanzielle Leistungsfähigkeit des Unternehmens. Hinzu kommt, je schneller die Umsetzung gelingt, desto eher können Unternehmen eine Vorreiterrolle auf diesem Gebiet einnehmen. Gesetzliche Vorgaben, die in den nächsten Monaten und Jahren angesichts der immer drastischeren Auswirkungen der Klimakrise strenger werden, treffen Unternehmen, die sich bereits jetzt mit dem Thema Twin Transition auseinandersetzen, weniger hart, als Unternehmen, die sich erst dann Gedanken darum machen, wenn sie keine andere Wahl mehr haben.

Sven-Anwar Bibi

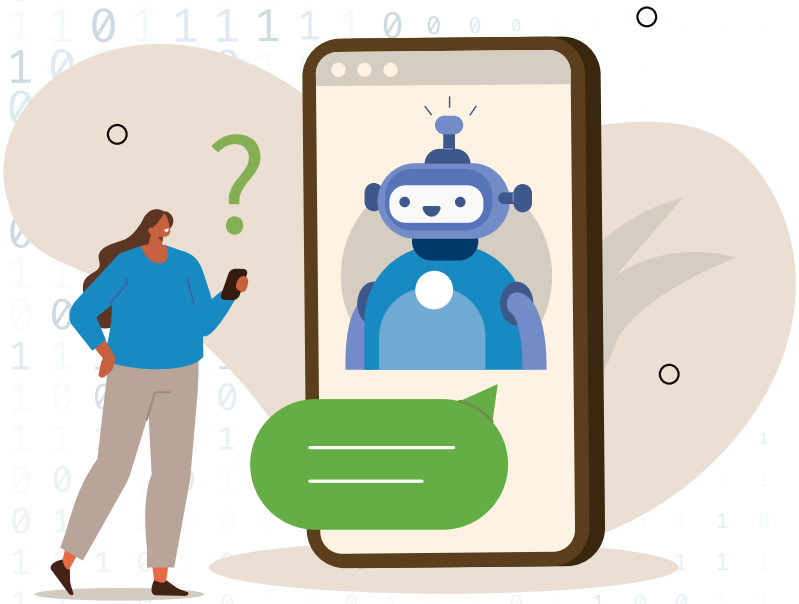


KÜNSTLICHE INTELLIGENZ

KAPIEREN & PROGRAMMIEREN

Du möchtest wissen, was hinter künstlicher Intelligenz und neuronalen Netzen steckt und deine eigenen selbstlernenden Programme schreiben?

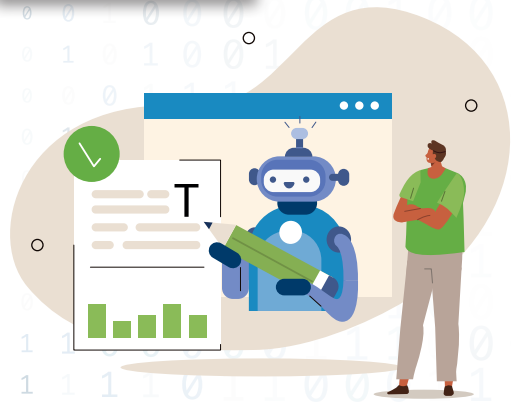
In diesem Buch erfährst du mit anschaulichen Erklärungen und vielen Bildern, wie KI funktioniert und wie du neuronale Netze ganz einfach selbst programmieren kannst. Dafür brauchst du keine Vorkenntnisse. Alle notwendigen mathematischen Konzepte werden von Grund auf und sehr anschaulich erklärt. Ganz nebenbei erhältst du eine Einführung in die Programmiersprache Python.



In jedem Kapitel erwarten dich spannende Projekte von ersten kleinen Programmen wie einem selbstlernenden Währungsrechner bis hin zu praxistauglicher Bilderkennung.

Denkaufgaben und Programmierübungen mit Lösungen zum Download helfen dir, dein Wissen zu testen und zu vertiefen. So lernst du Schritt für Schritt, wie du mit einfachen Programmiertechniken deine eigenen künstlichen neuronalen Netze entwickelst und trainierst.

Künstliche Intelligenz kapieren & programmieren: visuell lernen und verstehen; Michael Weigend, mitp Verlags GmbH & Co.KG, 2023



Green IT

WIE SOFTWARE-ENTWICKLER IHRE PRODUKTE NACHHALTIGER GESTALTEN KÖNNEN

Digitale Technologien können einen wichtigen Beitrag zum Klimaschutz leisten. Wichtig ist jedoch, dass sie selbst auch nachhaltigen Anforderungen entsprechen. Antrittspunkte für diese sogenannte Green IT gibt es viele; sie wollen aber richtig angegangen werden.

Dass digitale Technologien einen wichtigen Beitrag zum Erreichen der Klimaziele leisten können, darin sind sich die Experten hierzulande weitestgehend einig. Auch im Koalitionsvertrag der Bundesregierung ist eine klare Absichtserklärung enthalten, die den Zusammenhang zwischen Digitalisierung und Nachhaltigkeit verdeutlicht: „Wir wollen die Potenziale der Digitalisierung für mehr Nachhaltigkeit nutzen."

Wie groß das Potenzial digitaler Technologien für den Klimaschutz ist, beziffert beispielsweise eine Studie, die das Beratungsunternehmen Accenture zusammen mit dem Digitalverband Bitkom durchgeführt hat. Demnach könnten innovative Technologien dabei helfen, den Ausstoß an Treibhausgasemissionen in Deutschland im Jahr 2030 um rund 150 Megatonnen zu reduzieren. Das entspricht 41 Prozent dessen, was die Bundesrepublik insgesamt einsparen muss, um die gesteckten Klimaziele bis Ende des Jahrzehnts zu erreichen.

Bei aller Euphorie hat die Digitalisierung aber auch eine Schattenseite. Schließlich verbraucht der Einsatz von IT-Technologie selbst jährlich mehr und mehr Energie. Digitaltechnik wird eben nicht nur für den Klimaschutz eingesetzt. Bitcoin-Mining verbraucht weltweit bereits mehr Energie als mancher Industriestaat und Schätzungen beziffern den Anteil von Video-Streaming am globalen Datenverkehr auf mittlerweile weit über 50 Prozent. Soll sich die Digitalisierung nicht vom Segen zum Fluch wenden, muss auch Software selbst nachhaltiger – und damit ressourcenschonender – werden. Das Stichwort dazu lautet „Green IT".

Language	binary trees	fannkuch-redux	fasta
C	39.80 J	215.92 J	27.64 J
Java	111.84 J	311.38 J	35.86 J
JavaScript	312.14 J	413.90 J	64.84 J
Python	1793.46 J	12784.09 J	1061.41 J
% max / min	~4500%	~6000%	~4000%

Benchmark Energy

Quelle: Fraunhofer IESE

Stellschraube Nr. 1: die richtige Programmiersprache

Der Begriff fasst sämtliche Aspekte zusammen, die im Zusammenhang mit einem nachhaltigen Betrieb von IT-Technologien stehen: von den Umweltkosten bei der Herstellung von IT-Geräten über Kreislaufwirtschaft bis hin zu der Frage, wie der Energieverbrauch der Technologien auf ein absolut notwendiges Minimum reduziert werden kann. Auch in der Forschung ist Green IT ein derzeit viel diskutiertes Thema. Schließlich mangelt es der Softwarebranche noch immer an objektiven Qualitätsstandards, die ein nachhaltiges Softwaredesign und die dazugehörige Entwicklung beschreiben.

Auf den ersten Blick mag es so scheinen, als sei die Senkung des Energieverbrauchs von IT-Geräten insbesondere eine Herausforderung, mit der sich Elektroingenieure konfrontiert sehen. Tatsächlich haben jedoch insbesondere Software-Entwickler einen großen Einfluss auf diese Fragestellung. So lässt sich an dieser Stelle bereits vorab festhalten: Jeder Software-Engineer hat die Möglichkeit, Maßnahmen zu ergreifen, eine Software als grüneres Produkt zu gestalten. Einige dieser Stellschrauben werden im Folgenden näher dargelegt.

Zunächst einmal wirken sich Programmiersprachen erheblich auf die Energieeffizienz einer Software aus. Bereits 2017 haben beispielsweise portugiesische Forscher* den Energieverbrauch von insgesamt 27 verschiedenen Programmiersprachen anhand verschiedener Benchmarks untersucht. Das Ergebnis war eindeutig: Viele kompilierte Sprachen schnitten deutlich besser ab als interpretierte Sprachen oder solche, die auf einer virtuellen Maschine basieren. Im Gegensatz zu den beiden letztgenannten Sprachfamilien übersetzen kompilierte Sprachen den Programmcode direkt in maschinenlesbare Anweisungen und optimieren ihn dabei. Energieintensive Zwischenschritte können so ausgespart werden.

Konkret beläuft sich der Unterschied zwischen einer energieeffizienten Programmiersprache – zum Beispiel C – und einer weniger effizienten – etwa Python – auf typischerweise mehr als 4.000 Prozent beim Lösen der gleichen Rechenprobleme. Dies entspräche im Straßenverkehr dem Vergleich zwischen einem Fahrzeug mit 5 Litern Kraftstoffverbrauch pro 100 km mit einem anderen Modell, das über 200 Liter pro 100 km benötigt. Tatsächlich haben in der Praxis jedoch gerade Python und JavaScript in Serveranwendungen in den vergangenen Jahren vermehrt Einzug gehalten. Insbesondere bei intensiv genutzten Software-Modulen bestünde durch den Wechsel hin zu weniger energieintensiven Programmiersprachen ein erhebliches Einsparpotenzial.

Stellschraube Nr. 2:
die Software-Architektur

Allerdings kann die Migration sehr großer Codemengen in eine andere Sprache sehr teuer werden – insbesondere dann, wenn die Software bereits ein bestimmtes Maß an Komplexität erreicht hat. Insofern sollten Software-Entwickler im Idealfall bereits VORAB planen, welche Programmiersprache für welchen Anwendungsfall am besten geeignet ist; und dabei die jeweilige Energieeffizienz der Sprachen im Hinterkopf behalten.

Obwohl die Wahl der Programmiersprache bereits einen großen Hebel für eine nachhaltigere Software-Entwicklung darstellt, ist es mit dieser Stellschraube allein nicht getan. Denn selbst die energieeffizienteste Sprache nützt am Ende wenig, wenn die implementierten Algorithmen selbst ineffizient sind. Eine falsche Entscheidung an einem zentralen Punkt der Software-Architektur kann den Energieverbrauch der gesamten Anwendung um Größenordnungen in die Höhe treiben. Welche Methoden und Werkzeuge Software-Entwicklern an die Hand gegeben werden können, um ein solches Szenario zu vermeiden, ist eine zentrale Fragestellung in der IT-Forschung.

Stellschraube Nr. 3:
Cloud-Computing

Mobile und Cloud-Computing sind zwei anhaltend starke Trends der IT-Branche. So tragen beide zwar durch ihren vermehrten Einsatz dazu bei, den Energieverbrauch von IKT-Diensten insgesamt in die Höhe zu treiben. Umgekehrt gibt es beispielsweise beim Mobile Computing aber auch einen direkten Anreiz, um die Energieeffizienz der Anwendungen zu erhöhen: die Verlängerung der Akkulaufzeiten. Auch das Cloud-Computing bietet zumindest indirekt den Anreiz zur effizienteren Programmierung.

Demnach bestehen vor allem zwei, sehr beliebte Modelle, um Software in die Cloud zu verlagern: Infrastructure as a Service (IaaS) und Platform as a Service (PaaS). In beiden Fällen rechnet der jeweilige Cloud-Anbieter seine Kunden nach Verbrauch ab. Je weniger Server ein Unternehmen etwa im IaaS-Modell bucht, desto geringer sind die Betriebskosten. Das gleiche gilt für den PaaS-Anwendungsfall. Natürlich sind diese Betriebskosten zwar nicht gleichbedeutend mit Umweltkosten; dennoch besteht eine starke Korrelation. Denn: Steigt die Effizienz, sinken die Betriebskosten. Somit können Bestrebungen der Unternehmen, die Kosten möglichst niedrig zu halten, bereits dazu beitragen, auch die Nachhaltigkeit der Software selbst zu steigern.

Im direkten Nachhaltigkeitsvergleich schneidet das PaaS-Modell jedoch deutlich besser ab als das IaaS-Konzept. So werden bei letztgenannter Variante für jeden Kunden in höherem Maße Rechnerressourcen reserviert, was die Möglichkeit der gemeinsamen Hardware-Nutzung stark einschränkt. Beim PaaS-Modell kann die Hardware besser gemeinsam von mehreren Unternehmen genutzt werden, sodass ihre durchschnittliche Auslastung entscheidend erhöht wird. Darüber hinaus verteilen sich die Lastspitzen der verschiedenen Anwendungen über die Zeit, sodass insgesamt weniger Rechenreserve benötigt wird.

Unabhängig davon, welche der genannten Maßnahmen Software-Entwickler nun ergreifen, um ihre Produkte nachhaltiger zu gestalten, wird deutlich: In der sorgfältigen Anwendung bewährter Praktiken des Software-Engineerings liegt ein erhebliches Potenzial zur Ressourcenschonung. Werden Nachhaltigkeitsaspekte jedoch erst nachträglich beachtet, sind entscheidende Verbesserungen oft nur noch schwer zu erreichen. Deshalb ist es entscheidend, dass Nachhaltigkeit möglichst frühzeitig in der Erstellung der Anforderungen und beim Software Design berücksichtigt und konsequent in die Umsetzung gebracht werden.

Dr. Joachim Weber

Quelle: * Pereira et. al., 2017. Energy Efficiency across Programming Languages, Proceedings of the 10th ACM SIGPLAN International Conference on Software Engineering, pp. 256-267

JEDER SOFTWARE-ENGINEER HAT DIE MÖGLICHKEIT, MASSNAHMEN ZU ERGREIFEN, EINE SOFTWARE ALS GRÜNERES PRODUKT ZU GESTALTEN.

Dr. Joachim Weber,
Leiter Abteilung Architecture-Centric Engineering, Fraunhofer-Institut für Experimentelles Software Engineering IESE, www.iese.fraunhofer.de

BLOCKCHAIN

BEITRAG FÜR MEHR NACHHALTIGKEIT?

Eine knappe Mehrheit (54 %) der Unternehmen in Deutschland hält die Blockchain für eine wichtige Zukunftstechnologie, rund ein Drittel (37 %) zeigt sich dem Thema gegenüber interessiert und aufgeschlossen – aber nur 5 Prozent haben Blockchain-Technologie im Einsatz. Weitere 7 Prozent sind in einer Implementierungs- oder Test-Phase, 9 Prozent sind in der Analyse- und Informationsphase und 10 Prozent diskutieren den Einsatz. Das ist das Ergebnis einer repräsentativen Umfrage unter 653 Unternehmen ab 50 Beschäftigten im Auftrag des Bitkom. Vor zwei Jahren lag der Anteil der Unternehmen, die die Blockchain eingesetzt haben, erst bei 1 Prozent.

Das größte Potenzial (63 %) sehen die Unternehmen, die bereits Blockchain nutzen, planen oder darüber diskutieren, bei der Nachvollziehbarkeit der Aktivitäten aller Partner einer Wertschöpfungskette. Dahinter folgt die Blockchain als sicheres System zur Ausstellung von Zertifikaten oder Beglaubigungen (58 %), als Transaktionssystem für das Internet of Things (48 %), als interoperable Schnittstelle zum Datenaustausch (45 %), zur Verbriefung von realen Gütern und Finanztiteln (44 %) sowie ganz allgemein zur Abwicklung von Geschäften auf vermittlerfreien digitalen Marktplätzen (42 %).

Nachhaltigkeit: Chancen und Risiken

Beim Thema Blockchain und Nachhaltigkeit gehen die Meinungen auseinander. Zwei Drittel (64 %) meinen, dass mit Hilfe der Blockchain Unternehmen den CO2-Fußabdruck in Lieferketten transparent machen können. Die Hälfte (51 %) erwartet, dass mit der Blockchain der CO2-Zertifikatshandel verbessert werden kann und so ein Beitrag für mehr Nachhaltigkeit geleistet wird. Ebenfalls 51 Prozent sagen aber auch: Die Blockchain-Technologie verbraucht zu viel Energie.

www.bitkom.org

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

Hier geht's zum neuen

it-daily Weekend

ni: Ransomware ++ **Juli:** Quantencomputing ++ **August:** Zero Trust ++ **September:** Office 4.0

Simplify Sustainability

NACHHALTIGKEIT IST KEINE ROCKET SCIENCE

ESG (Environment, Social, Governance) und die damit verbundenen Themen spielen seit geraumer Zeit eine immer wichtigere Rolle in Wirtschaft und Gesellschaft. Dafür spricht auch, dass bereits 2020 Larry Fink, Gründer, Aufsichtsrats- und Vorstandsvorsitzender der weltgrößten Vermögensverwaltung BlackRock ankündigte, bei Umweltschutz und Menschenrechten künftig genauer hinzuschauen. „Wir sind überzeugt, dass Nachhaltigkeit unser neuer Investmentstandard sein sollte." Mittlerweise hat die Politik diese Ansichten EU-weit assimiliert und diesbezüglich Regeln beschlossen, dass Unternehmen künftig ihr Umwelt-Engagement – insbesondere den Carbon-Footprint (CO_2-Fußabdruck) – nachweisen müssen. Vor allem Investoren beziehen den ESG-Score bei ihren Finanzentscheidungen mit ein.

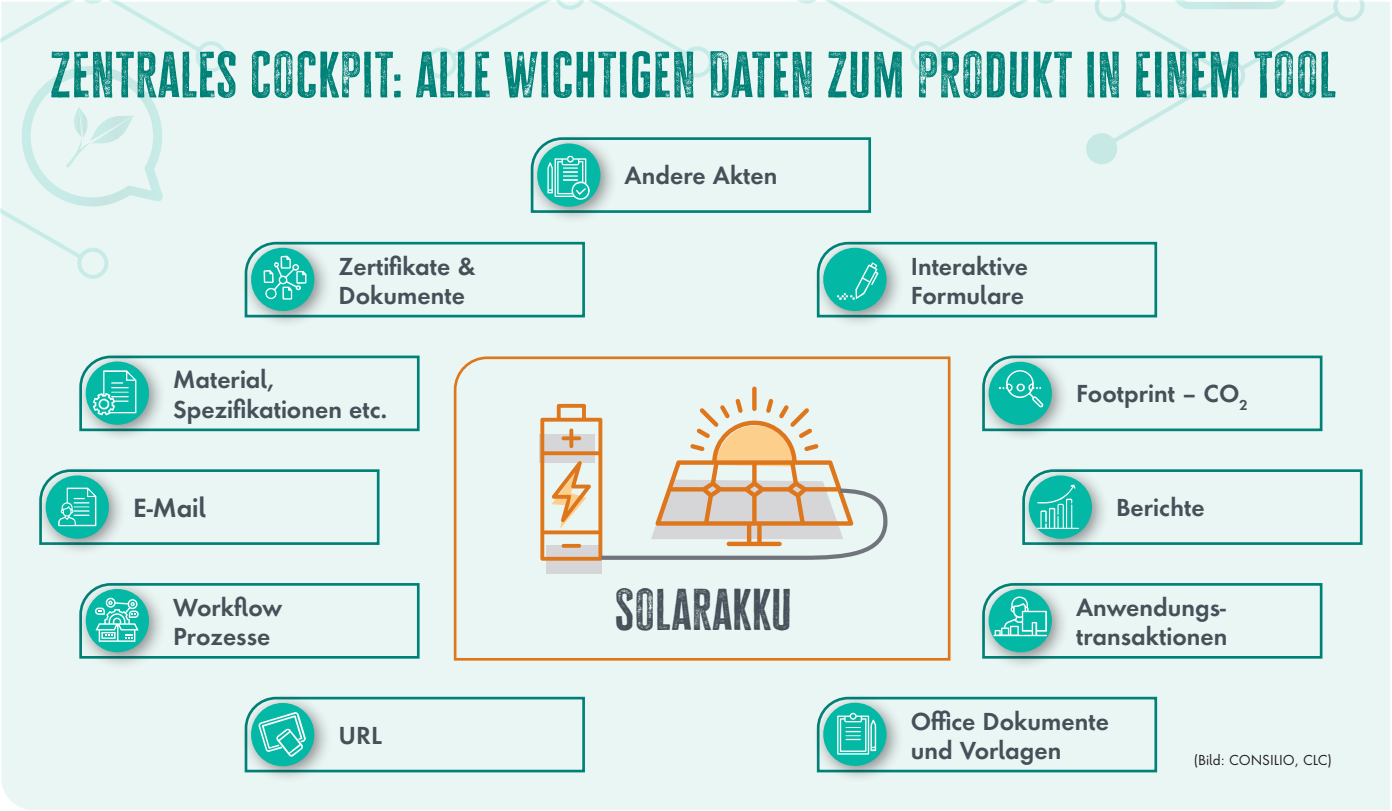
Als global aktives Unternehmen greift die SAP solche Strömungen auf und hat das Thema mit den Modulen SAP Sustainability und SAP Emissions im ERP abgebildet.

Zu groß für viele Unternehmen

Die SAP hat mit ihren Modulen ein System modelliert, das einen sehr holistischen Ansatz verfolgt. Die Walldorfer illustrieren ihre Vision am Beispiel eines Unternehmens, das den Grundstoff Kakao für seine Produkte weltweit von verschiedenen Lieferanten bezieht und dabei alle nötigen Daten erhält, die für die Berechnung des Carbon-Footprint nötig sind. Das SAP-Beispiel zeigt eine ideale Welt, doch sind viele Unternehmen weder umfassend global vernetzt, noch erhalten sie von ihren Lieferanten in Gänze die erforderlichen Daten. Sie sind daher dazu gezwungen zu improvisieren, damit sie so nah wie möglich an die erforderlichen Werte gelangen. CONSILIO und CLC arbeiten in dem Bereich Nachhaltigkeit zusammen an der Lösung „Simplify Sustainability", die den Prozess für Kunden erheblich vereinfacht.

Zusammen stark: Prozesse und Dokumente vereint

CONSILIO, ein unabhängiges Beratungsunternehmen und Experte für die Optimierung von Prozessen nach S/4HANA hat mit CLC, einem Spezialisten für prozessorientierte Akten- und Dokumenten-Management-Systeme im SAP-Umfeld, ein gemeinsames Projekt aufgesetzt, mit dem sie die Nachhaltigkeitsanforderungen für Unternehmen aller Klassen vereinfachen. Dazu bündeln beide SAP-Spezialisten ih-



(Bild: CONSILIO, CLC)

re Stärken und schaffen Synergien, von denen ihre Kunden profitieren. So lässt beispielsweise CONSILIO sein umfangreiches Know-how aus der Produktion einfließen, während CLC seine Expertise im prozessorientierten Akten- und Dokumenten-Management beisteuert. Als ausgezeichnete Partner der SAP wissen beide Unternehmen, wie sich die Ziele der Nachhaltigkeit im ERP rechtskonform umsetzen lassen.

Die Lösung im Detail

Simplify Sustainability ist eine Lösung, die sich nahtlos in bestehende SAP-Systeme integrieren lässt – egal ob es sich um ein S/4HANA- oder ein ECC-System handelt. Dabei bezieht die Lösung die erforderlichen Daten und Dokumente entweder direkt aus dem System, beziehungsweise aus dem ERP oder aus externen Quellen und bündelt sie in einer Produktakte.

Anwender dieser Lösung steigern damit die Transparenz und Übersichtlichkeit ihrer Produkte im SAP-System. Die Produktakte ist somit eine Single Source of Truth, wenn es darum geht, Details zu einem Material, Produkt oder einer Baugruppe zu erhalten. Über verschiedene Schnittstellen (REST, https oder WebDAV) sind Anbindungen der Simplify-Sustainability-App an externe Datenquellen relativ einfach realisierbar. So lassen sich etwa Zertifikate, Lieferanten oder BOMs integrieren. Dadurch ist es möglich, mit wenigen Klicks zu sehen, wo ein Produkt und seine Komponenten herkommen, wie sie zusammengesetzt und wie nachhaltig sie sind.

Beispiel Solar-Akku

Die Basis-Architektur von Simplify Sustainability ist in modularen Komponenten abgebildet, die beide Unternehmen an der Case Study „Solar-Akku" demonstrieren. In diesem Beispiel wird das Produkt über Referenzen zugeordnet – das Lithiumpaket und das Gehäuse. Beide Bausteine bezieht das Unternehmen von unterschiedlichen Herstellern. Das bedeutet, dass der Kunde theoretisch die Daten für beide Produkte integriert und zentral bearbeiten kann und nicht in unterschiedlichen Modulen pflegen muss. Damit kann auf Knopfdruck nachgewiesen werden, dass die Lieferkette nachhaltig ist und alle Anforderungen bezüglich Gefahrenschutz oder anderweitigen Bedingungen erfüllt werden.

SIMPLIFY SUSTAINABILITY IST EINE NACHHALTIGKEITSLÖSUNG, DIE DEN BÜROKRATISCHEN AUFWAND IN GRENZEN HÄLT UND MIT DEN ANFORDERUNGEN DES UNTERNEHMENS WÄCHST.

Dr. Fridtjof Schucht, Managing Consultant SAP EHS, CONSILIO GmbH, www.consilio-gmbh.de

Simplify Sustainability prüft permanent im Hintergrund, ob sämtliche Zertifikate gültig sind. Durch die Funktion „Eskalation und Statusmanagement" würde das System etwa einen Lieferanten darauf hinweisen, dass sein Zertifikat bald ausläuft und er ein neues bereitstellen muss. In diesem Fall verhängt das System bei Bedarf eine Sperre für den Lieferanten. Die Eskalation lässt sich über den klassischen Weg lösen, oder CLC/CONSILIO stellen eine entsprechende App zur Verfügung.

Fit für die Zukunft

Simplify Sustainability ist aber auch für künftige Herausforderungen gerüstet. So ist die digitale Produktakte bereits für mögliche weitere Zertifikate gerüstet, dazu zählen beispielsweise Nachweise zu Umwelt, Sicherheit, Menschenrechten und Arbeitssicherheit. Das flexibel anpassbare Footprint-Management ist zudem fähig, automatisch die gewünschten Daten aus standardisierten Quellen oder externen Quellen zu beziehen. Auf Basis dieser Daten lässt sich dann der Footprint konform berechnen und ausgeben.

Der Data Acquisition Layer – also die Quelle der Nachhaltigkeitsdaten – ist in vielen Fällen lieferantenseitig noch nicht ausreichend umgesetzt, weswegen viele Stellen Standardwerte anbieten. Diese Werte lassen sich sehr einfach in das System übernehmen. Auch der Import von Daten über Web- oder Adobe-Formulare ist möglich – etwa, wenn Hersteller nicht wollen, dass Lieferanten auf das Portal zugreifen. Zudem gibt es die Möglichkeit, externe Datenquellen/ Lieferantenportale oder E-Mails zu integrieren.

Dashboards für jeden Einsatzbereich

Simplify Sustainability ist auch skalierbar. Das bedeutet: Nachhaltigkeits-Reporting kann beliebig komplex sein. Das hängt einerseits vom Produkt ab und andererseits von der Architektur der Supply Chain. Um für alle Fälle gerüstet zu sein, bietet die Lösung ein Stücklisten-Cockpit, um verschiedene Relationen zu zeigen, beispielsweise für PLM oder Vertrieb in unterschiedlichen Versionen. So ist es vergleichsweise einfach, direkt aus der Stückliste einen realistischen CO_2-Footprint anzuzeigen oder zu berechnen. Darüber hinaus bietet der Reporting-Layer (CLC-PADD) ein Listreporting, integrated Analytics (Grafische Auswertung mit Drill-Down – Warengruppen, Produkte), ein O-Data-Interface für Power-BI oder SAP-BI. Damit lässt sich etwa mit wenigen Klicks ein CO_2-Ausweis für ein Produkt oder eine Baugruppe erstellen.

Fazit

Mit Simplify Sustainability bieten CONSILIO und CLC eine Nachhaltigkeitslösung, die den bürokratischen Aufwand in Grenzen hält, mit den Anforderungen des Unternehmens wächst, aber gleichzeitig die EU-Taxonomie in Bezug auf Nachhaltigkeit umfassend unterstützt.

Dr. Fridtjof Schucht

Tier-IV-Rechenzentrum

DIE VORTEILE VON „FAULT TOLERANT" FÜR UNTERNEHMEN

Der Einsatz eines Tier-IV-Rechenzentrums maximiert die Vorteile der Digitalisierung und der Cloud-Migration für Unternehmen. Durch seine Leistungsfähigkeit bietet es auch das optimale Umfeld für komplexe SAP-Systeme.

Aufgrund der zunehmenden Digitalisierung wandern immer mehr geschäftskritische Anwendungen und Prozesse in die Cloud. Die Migration ihrer Daten bietet Unternehmen zahlreiche Vorteile, sodass sich die Nutzung der Cloud zu einem wichtigen Wettbewerbsfaktor in allen Branchen entwickelt hat. Speziell bei ERP-Systemen wie den Lösungen von SAP setzen Unternehmen zunehmend auf die Cloud, um das Risiko von Betriebsausfällen zu minimieren und die optimale Leistungsfähigkeit und Skalierbarkeit zu gewährleisten.

TIER-IV-RECHENZENTREN BIETEN EINE INFRASTRUKTUR, DIE ES UNTERNEHMEN ERMÖGLICHT, IHRE IT-RESSOURCEN FLEXIBEL UND OHNE GRÖSSERE UNTERBRECHUNGEN ZU ERWEITERN.

Christian Quandt,
Head of Sales Center, WIIT AG,
www.wiit.cloud/de/

Verlagern Unternehmen ihre Daten und Anwendungen, ändern sie ihre interne Organisation und stellen die Weichen für die Transformation zu einem digitalen Unternehmen. Vor allem hinsichtlich der Skalierbarkeit, der Geschwindigkeit und der Kosten bietet die Cloud-Nutzung bedeutende Vorteile. Zudem optimieren Unternehmen dadurch die Abläufe für schnelle Backups bei Ausfällen und gewährleisten den reibungslosen Einsatz komplexer SAP-Systeme ohne Verzögerung.

Bei der Cloud-Migration von Daten und Anwendungen ist die Einführung eines modernen As-a-Service-Modells die effektivste Herangehensweise. Dabei stellen die Provider ihre IT-Infrastruktur und Tools zur Verfügung. Je nach vereinbartem Servicemodell führt der Anbieter auch Updates und Wartungsarbeiten durch, sodass die Anwendungen der Nutzer ständig auf dem neusten Stand und damit nicht nur maximal leistungsfähig, sondern auch so sicher und gut geschützt wie möglich sind.

Trotz der zahlreichen Vorteile gegenüber On-Premises-Lösungen empfinden einige Unternehmen die Nutzung von Cloud-Angeboten als riskant und investieren lieber in die Anschaffung und die Wartung einer eigenen Infrastruktur. Die Performance von komplexen und regelmäßig aktualisierten On-Premises-Systemen kann mit der Zeit jedoch nachlassen und die Arbeit der Angestellten ausbremsen. Die Leistung lässt sich dann nur mit einer Reduzierung der Systemlast oder mit Investitionen in die Hardware wieder erhöhen. Eine Reduzierung der Systemlast ist allerdings ein komplexer Vorgang, bei dessen Umsetzung ein kompetenter Servicepartner von entscheidender Bedeutung ist. Investitionen in die Hardware sind nicht wirtschaftlich, da Hardware nicht flexibel skalierbar ist und deshalb bei fortgesetztem Unternehmenswachstum nur für begrenzte Zeit Abhilfe verschafft.

Die zentrale Rolle der Rechenzentren

Um ihre Daten und Anwendungen der Infrastruktur eines Providers anzuvertrauen, müssen sich Unternehmen auf den Cloud Provider, den sie sich für die Zusammenarbeit auswählen, verlassen können. Dabei sind die Resilienz und Zuverlässigkeit des Cloud Providers entscheidende Kriterien. Speziell Unternehmen in Branchen, die einer strengen Regulierung unterliegen, sind auf die Ausfallsicherheit, Leistungsstärke und Effizienz ihres Providers und ihrer Rechenzentren angewiesen.

Für Behörden und Unternehmen, die kritische Infrastruktur betreiben, sind zudem die Nutzung georedundanter Rechenzentren verpflichtend. Der Begriff beschreibt den Grundsatz, Daten an mindestens zwei Rechenzentren an verschiedenen Standorten zu speichern. Die physische Entfernung zwischen den Standorten soll gewährleisten, dass auch bei einem Ausfall eines Rechenzentrums aufgrund von Ereignissen wie Naturkatastrophen ein anderes Rechenzentrum den Betrieb übernehmen kann.

Nutzen Provider zertifizierte Rechenzentren und integrieren den Schutz der Daten in das Dienstleistungsmodell, sorgen sie für maximale Resilienz und Zuverlässigkeit. Das US-amerikanische Uptime Institute hat Zertifizierungsstufen für Rechenzentren entwickelt, die internationaler Standard für deren Klassifizierung sind.

Für die Einstufung eines Rechenzentrums bewertet das Institut zahlreiche Faktoren

hinsichtlich des Designs, des tatsächlichen Aufbaus und der operativen Effektivität und Effizienz der jeweiligen Einrichtung. Die Zertifizierungsstufen reichen bis Tier IV, welche ein Rechenzentrum als „Fault Tolerant" kennzeichnet. In einem Tier-IV-Rechenzentrum hat demnach ein einzelner Geräteausfall, eine Unterbrechung des Verteilungsweges oder die Wartung des Systems keinen Einfluss auf den Betrieb.

Verfügbarkeit und Redundanz

Die Gründe, die für die Nutzung eines Tier-IV-Rechenzentrums sprechen, sind zahlreich. Zunächst hängt die Entscheidung für Unternehmen von ihren Geschäftsanforderungen, ihren Budgetgrenzen und ihren Sicherheitsansprüchen ab. Entscheiden sich Unternehmen für die Nutzung eines Rechenzentrums mit Tier-IV-Zertifizierung, profitieren sie von der beispiellosen Verfügbarkeit und Redundanz.

Ein Rechenzentrum der höchsten Zertifizierungsstufe ist so konzipiert, dass es praktisch wartungsfrei ist und eine Ausfallzeit von weniger als 26,3 Minuten pro Jahr, also eine Betriebszeit von 99,995 Prozent aufweist. Dies ist besonders wichtig für Unternehmen, die auf ununterbrochene Dienstleistungen angewiesen sind, wie etwa Cloud-Service-Provider, Finanzinstitutionen oder E-Commerce-Plattformen.

Um die Betriebszeit von 99,995 Prozent zu gewährleisten, bieten Tier-IV-Rechenzentren sowohl eine physikalische als auch eine logische Redundanz in ihren Systemen, einschließlich Stromversorgung, Kühlung, Netzwerk und Hardware. Dadurch stellen die Betreiber des Rechenzentrums sicher, dass selbst bei einem Ausfall eines Elements der Betrieb reibungslos weitergehen kann. Die sorgfältige Planung und der hohe Standard von Tier-IV-Rechenzentren minimieren das Risiko von Ausfällen und bieten deutlich bessere Business Continuity.

Maximale Skalierbarkeit der Ressourcen

Aufgrund ihrer strengen Sicherheitsmaßnahmen und Redundanz bieten Tier-IV-Rechenzentren höheren Schutz vor physischen Bedrohungen wie Einbruch, Feuer oder Naturkatastrophen. Dies kann besonders für Unternehmen wichtig sein, die sensible Daten oder geschäftskritische Anwendungen hosten.

Neben dem Fokus auf die Sicherheit der Daten sind Tier-IV-Rechenzentren auf Skalierbarkeit ausgelegt. Sie bieten eine Infrastruktur, die es Unternehmen ermöglicht, ihre IT-Ressourcen flexibel und ohne größere Unterbrechungen zu erweitern.

Aufgrund der höheren Betriebskosten eines Tier-IV-Rechenzentrums sollten Sie Ihre Geschäftsanforderungen, das Budget und den Wert, den Sie aus der höchsten Stufe der Verfügbarkeit und Redundanz ziehen können, sorgfältig abwägen. In einigen Fällen könnte ein niedrigerer Tier-Standard ausreichend sein, während in anderen Fällen die Investition in ein Tier IV-Rechenzentrum die beste Wahl ist.

Die WIIT-Gruppe verfügt aktuell über zwei eigene Tier-IV-Rechenzentren in Mailand. Ein weiteres Rechenzentrum von WIIT in Düsseldorf wird in Kürze die Tier-IV-Zertifizierung erhalten. Mit Abschluss dieses Prozesses wird das Rechenzentrum das erste in Deutschland sein, das die höchste Bewertung des Uptime Instituts erhält. Dieser Standort wird die Heimat für geschäftskritische Anwendungen und Cloud Services der WIIT-Gruppe und ihrer Kunden.

Christian Quandt

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

Das große Reinemachen

EINE VALIDE DATENBASIS IST ZENTRALER ERFOLGSFAKTOR FÜR DIE SAP S/4HANA MIGRATION

Aktuell stehen zahlreiche Unternehmen vor der Herausforderung, wie sie die nächsten Schritte der Digitalisierung gestalten. Anwendungen in der Cloud stehen dabei weit oben auf der Liste, wobei SAP-Kunden unter einem besonderen Druck stehen. Denn das Ende des Supports für SAP ECC rückt näher und die Transformation eines ERP-Kernsystems ist nicht in wenigen Tagen oder Wochen erledigt. Was also sollten die IT-Verantwortlichen beim Wechsel in die Cloud mit SAP S/4HANA grundsätzlich beachten?

Mit Einführung der neuen SAP-Generation sind nicht nur Veränderungen in der Architektur verbunden, sondern auch Anpassungen in Infrastruktur und Technologie. Hinzu kommen die Herausforderungen beim Transfer der Daten, beim Schnittstellenmanagement, bei der Migration von Betriebssystemen sowie bei der Übertragung oder Neugestaltung von unternehmensspezifischen Prozessen. Das Zünglein an der Waage, das über den Erfolg eines Transformationsprojekts maßgeblich entscheidet, ist aber vor allem die Qualität der Daten.

Erst analysieren – dann machen

Um ein bestmögliches Migrationsergebnis zu erreichen, müssen zunächst die Systemlandschaft, Prozesse und Daten analysiert werden. Die Herausforderung: zu wenig Personal, das Erfahrung mit einer ERP-Migration und der Bewertung der Datenqualität hat. Deshalb empfiehlt es sich bereits zu Beginn eines Transformationsprojekts, erfahrene Partner ins Boot zu holen. Das belegt eine aktuelle Studie von Natuvion und NTT Data Business Solutions. Der Mangel an Personal und Know-how ist ein signifikanter Show-Stopper. Mehr als 35 Prozent der Unternehmen gaben an, während des Transformationsprozesses Wissenslücken identifiziert zu haben. Über 30 Prozent der Unternehmen hatten zudem im Rahmen der Transformation weder ausführliche Datenanalysen durchgeführt noch eine Vorabprüfung vorgenommen. Diese Faktoren tragen dazu bei, dass sich 45 Prozent der Unternehmen in DACH eingestehen mussten, ihre Transformationsziele nicht vollständig erreicht zu haben. Das Learning hieraus: Über 32 Prozent der befragten Unternehmen gaben an, zukünftig früher auf externe Berater setzen zu wollen.

DAMIT DIE QUALITÄT DER ZU MIGRIERENDEN DATEN PASST, MÜSSEN ZUNÄCHST DIE SYSTEMLANDSCHAFT, PROZESSE UND DATEN ANALYSIERT WERDEN.

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

Housekeeping

In der Regel sind SAP-Landschaften heterogen und bestehen meist aus mehreren einzelnen SAP-Systemen mit sehr vielen Eigenentwicklungen, die über die Jahre gewachsen sind und komplexe Prozess- und Datenstrukturen aufweisen. Oft wurde dabei lediglich die technische System- und Datenplattform an die spezifischen Prozessanforderungen der Fachbereiche angepasst, anstatt das übergeordnete Ziel der Standardisierung und Harmonisierung der Daten- und Prozessstrukturen zu verfolgen.

Diese Erkenntnis und die Ergebnisse der Studie sollten sich all diejenigen zu eigen machen, die am Anfang eines Umzugs auf SAP S/4HANA stehen. Gemeinsam mit Migrations-Profis haben Unternehmen die Chance, die Ausgangslage zielgerichtet zu analysieren und die richtigen Fragen bezüglich der existierenden Datenbasis zu beantworten. Erst dann werden die passenden methodischen Optionen für die Transformation festgelegt. Bei der Datenmigration wird zumeist auf eine Mischform aus Greenfield und Brownfield oder den Selective-Data-Transition-Ansatz (SDT) gesetzt. SDT nimmt dabei eine besondere Rolle ein: Es ist die Methodik, mit der definiert werden kann, welche Daten archiviert, gelöscht oder übertragen werden.

Das Fazit: Am Anfang sollte immer die Analyse und das Housekeeping stehen, um ein „bereinigtes" System erfolgreich in die Cloud zu überführen.

Philipp von der Brüggen

GUT ZU WISSEN

Transformation 2023

Von der Krise zur Chance

MIT IT-MONITORING FACHKRÄFTEMANGEL UND STEIGENDE ANFORDERUNGEN MEISTERN

IT-MONITORING BEZIEHT SICH AUF DIE KONTINUIERLICHE ÜBERWACHUNG VON IT-SYSTEMEN, ANWENDUNGEN UND NETZWERKEN, UM DEREN LEISTUNG UND SICHERHEIT ZU GEWÄHRLEISTEN.

Frank Laschet,
Produkt-Experte für IT-Monitoring-Lösungen,
USU Software AG, www.usu.com

Läuft die IT, läuft auch das Unternehmen. Auch KMUs sind mittlerweile stark auf die Verfügbarkeit und Leistung ihrer IT angewiesen. Ein Ausfall wichtiger IT-Komponenten kann oft die gesamte Organisation beeinträchtigen. Dabei geht es nicht nur darum, dass beim Ausfall eines E-Mail-Servers ein zentraler Bereich der Kommunikation brachliegt. Wenn der Onlineshop oder das Kundenportal nicht mehr funktionieren, kommt es neben einem möglichen Imageverlust schnell zu Umsatz- und Geschäftseinbußen, die an die Substanz gehen. Dabei spielen IT-Experten eine immer wichtigere Rolle, um die technologischen Anforderungen von Unternehmen zu erfüllen. Trotz dieser Wichtigkeit haben Unternehmen in Deutschland in den letzten Jahren Schwierigkeiten, qualifizierte IT-Experten zu rekrutieren und zu halten. Der anhaltende Fachkräftemangel in der IT-Branche hat einen neuen Höchststand erreicht, was Unternehmen vor die Herausforderung stellt, die steigende Nachfrage nach IT-Experten zu bewältigen.

Gleichzeitig sind in der gegenwärtig hochdigitalisierten Geschäftswelt Unternehmen in erheblichem Maße auf IT-Systeme und digitale Dienste angewiesen. Die nahtlose Funktionsweise dieser Systeme und Anwendungen ist von entscheidender Bedeutung. Um interne Prozesse, Kundeninteraktionen und Datenspeicherungen zu unterstützen, setzen Unternehmen immer neuere Technologien ein. Wenn diese Systeme nicht einwandfrei funktionieren oder ausfallen, können die Auswirkungen erheblich sein. Sie reichen von verringerter Produktivität bis hin zu Unzufriedenheit bei Mitarbeitern und Kunden sowie einem geschädigten Unternehmensimage.

Eine vielversprechende Strategie, um dem IT-Fachkräftemangel entgegenzuwirken, ist die Nutzung spezialisierter Softwarelösungen. Diese Tools können verschiedene Aspekte der IT-Infrastruktur überwachen, verwalten und optimieren, die normalerweise menschliche Expertise erfordern würden. Durch den Einsatz solcher Software können Unternehmen ihre bestehenden IT-Ressourcen effizienter nutzen und Engpässe in bestimmten Bereichen überbrücken.

So kann die Einführung eines IT-Monitoring-Systems bereits eine effektive Möglichkeit sein, die Belastung einer IT-Abteilung zu verringern, IT-Experten zu entlasten und gleichzeitig die Stabilität und Leistungsfähigkeit der IT-Infrastruktur zu erhöhen. IT-Monitoring bezieht sich auf die kontinuierliche Überwachung von IT-Systemen, Anwendungen und Netzwerken, um deren Leistung und Sicherheit zu gewährleisten.

Die System- und Infrastrukturüberwachung spielt dabei ein wesentlicher Bestandteil der modernen IT-Betriebsführung. Sie gewährleistet die reibungslose Funktion von Systemen, Anwendungen und Diensten, minimiert Ausfallzeiten und trägt zur Sicherheit von Daten und zur Einhaltung von Vorschriften und SLAs bei.

System Monitoring im Überblick

Viele IT-Abteilungen haben bereits seit geraumer Zeit IT-Monitoring-Lösungen im Einsatz. Häufig vertraut man hierbei noch immer auf mehrere, nicht integrierte Monitoring-Insellösungen. In der Praxis findet man auch bei großen, international agierenden Organisationen nicht selten bis zu 20 solcher isolierten Überwachungssysteme. Diese sind meist – analog zur Ausweitung der IT-Infrastruktur – historisch gewachsen. Der im Ernstfall so wichtige systemübergreifende 360-Grad- Blick ist bei diesem Überwachungsansatz nicht gegeben. Um solche Situationen zu vermeiden, bieten Monitoring-Spezialisten umfassende Lösungen für die ganzheitliche Überwachung ihrer IT-Infrastruktur. Unabhängig von ihrer Umgebung, sei es On-Premises oder in der Cloud, ermöglichen entsprechende System-Monitoring-Tools eine

MEHR WERT

Das detaillierte White Paper „360-Grad-Monitoring" beschreibt die Praxishürden, mit denen IT-Organisationen heute konfrontiert sind, enthält wertvolle Tipps zur IT-Überwachung:

https://bit.ly/3PpZ5HU

zuverlässige Kontrolle und Steuerung der gesamten hybriden IT-Welt.

Die Herausforderungen in der Praxis
Die Vorteile einer solchen Lösung liegen auf der Hand und erfüllen die typische Praxis-Anforderungen:

➤ **Echtzeitüberwachung:**
Das Tool ermöglicht die Echtzeitüberwachung Ihrer IT-Systeme, damit Sie sofortige Benachrichtigungen über Leistungsprobleme oder Ausfälle erhalten können.

➤ **Proaktive Fehlererkennung:**
Es kann automatisch nach Fehlern und Anomalien suchen und Sie benachrichtigen, bevor diese zu größeren Problemen eskalieren.

➤ **Leistungsanalyse:**
Das Tool bietet Einblicke in die Leistung Ihrer Systeme, einschließlich CPU-Auslastung, Speicherbedarf, Netzwerkverkehr und vieles mehr.

➤ **Kapazitätsplanung:**
Das System überwacht die Ressourcenauslastung und trifft Vorhersagen zur Kapazitätsplanung, um Engpässe zu verhindern.

➤ **Benachrichtigungen und Alarme:**
Benutzerdefinierte Benachrichtigungen und Alarme können eingerichtet werden, so dass Verantortliche umgehend informiert werden, wenn bestimmte Schwellenwerte überschritten sind.

➤ **Berichterstellung und Protokollierung:**
Das Tool kann Berichte und Protokolle generieren, die für die Analyse und Dokumentation der Systemleistung nützlich sind.

➤ **Skalierbarkeit:**
Es sollte in der Lage sein, mit einer wachsenden IT-Infrastruktur zu skalieren, sei es On-Premises oder in der Cloud.

➤ **Integration:**
Die Möglichkeit, sich nahtlos in andere IT-Management-Tools und -Systeme zu integrieren, ist wichtig, um eine ganzheitliche Überwachung und Verwaltung sicherzustellen.

Mehrwert Überwachung von Gebäudetechnik
In einer Ära, in der Technologie einen integralen Bestandteil unseres Lebens bildet, spielt die Überwachung von Gebäudetechnik inzwischen auch eine entscheidende Rolle bei der Gewährleistung der Sicherheit, Effizienz und Nachhaltigkeit moderner Gebäude. Brandmeldeanlagen, Klimaanlagen und Alarmanlagen sind Schlüsselkomponenten, die nicht nur den Schutz von Menschen und Vermögenswerten gewährleisten, sondern auch eine optimale Raumumgebung schaffen. Darüber hinaus wird mit dem Ansatz der Green IT zunehmend Wert darauf gelegt, diese technologischen Aspekte auf umweltfreundliche Weise zu überwachen und zu steuern. Auch dies ist mit Technologien für das Data Center & Building Infrastructure Monitoring möglich.

Fazit
Der Mangel an IT-Fachkräften ist eine Herausforderung, der viele Unternehmen gegenüberstehen. Die Einführung von IT-Monitoring-Systemen kann eine effektive Möglichkeit sein, diese Belastung zu reduzieren und gleichzeitig die Stabilität und Leistungsfähigkeit der IT-Infrastruktur zu erhöhen. Ein zentrales Systems Management arbeitet zwar hinter den „Systemkulissen", ist aber dennoch „System-relevant", denn es sorgt dafür, dass die Geschäfts-kritische IT läuft. Hochverfügbar und ausfallsicher. Allerdings zwingt die Überwachung neuer Technologien bzw. Trends wie Cloud, Container oder Mobile bzw. IoT-Devices Organisationen dazu, ihre IT-Monitoring-Strategien neu auszurichten. Der digitale Wandel in den Unternehmen erfordert zunehmend eine neue Generation von Systems Management-Lösungen, welche in der Lage sind, die komplexen und heterogenen Infrastrukturen flexibel, aktiv und weitestgehend automatisiert zu überwachen. Durch die frühzeitige Erkennung von Problemen und die automatisierte Überwachung können Unternehmen die Auswirkungen des Fachkräftemangels mindern und ihre Wettbewerbsfähigkeit in einer zunehmend digitalisierten Welt sicherstellen.

Frank Laschet

Dashboard-Ansichten des USU-Monitoring-Systems

Fachkräftemangel

UNTERNEHMEN SIND PERSONELL UNTERBESETZT

Eine aktuelle Studie von SD Worx bestätigt, dass der „War for Talent" nach wie vor aktuell ist. Im Rahmen der Studie wurden insgesamt 4.833 Arbeitgeber und 16.011 Arbeitnehmer in 16 europäischen Ländern befragt. Vier von zehn europäischen Arbeitgebern (45 Prozent) gaben an, Schwierigkeiten bei der Rekrutierung neuer Mitarbeiter zu haben. Im europäischen Vergleich teilen sich Deutschland und Italien mit 45 Prozent den dritten Platz. Spitzenreiter in Europa sind Belgien und die Niederlande mit 54 Prozent, dicht gefolgt von Frankreich (51 Prozent). Die Studie zeigt auch, dass ein Drittel der deutschen Unternehmen mit einer hohen Personalfluktuation zu kämpfen hat.

Dies führt dazu, dass gut die Hälfte (47 Prozent) der Unternehmen die anfallende Arbeit aufgrund von Personalmangel nicht erledigen kann. Vor allem französische Unternehmen haben hier besondere Schwierigkeiten (61 Prozent).

Eine Frage der Weiterbildung

Ein möglicher Lösungsansatz ist, die persönliche Entwicklung der Arbeitnehmer durch Weiterbildung zu fördern. 61 Prozent der europäischen Arbeitnehmer sind sich ihrer Fähigkeiten bewusst. 40 Prozent wissen, dass Weiterbildung und persönliche Entwicklung die eigene Attraktivität am Arbeitsmarkt steigern. Mit zunehmendem Alter nimmt der Wunsch nach Fortbildungsmaßnahmen ab, besonders bei Arbeitnehmern über 55. Die Hälfte der Suchenden wissen, dass Fortbildungsmaßnahmen die Suche nach einer neuen Stelle erleichtern können.

Trotz der unumstrittenen Bedeutung von Bildung geben 23 Prozent der befragten Unternehmen an, Schwierigkeiten bei der Aus- und Weiterbildung zu haben. Mehr als die Hälfte (57 Prozent) der Beschäftigten hat im letzten Jahr an keiner Weiterbildung teilgenommen. Ein Drittel der befragten Beschäftigten – insbesondere junge Menschen unter 25 Jahren (35 Prozent) – hat jedoch kein Interesse an Weiterbildung. Bei den 25- bis 29-Jährigen sind es 35 Prozent und bei den 45- bis 49-Jährigen 33 Prozent.

Digitale Weiterbildung

Menschen entwickeln ihre Fähigkeiten durch ihre Arbeit, mit oder ohne Anleitung. Etwas mehr als die Hälfte (51 Prozent) der Mitarbeiter gibt an, dass sie sich neue Fähigkeiten digital aneignen. 70 Prozent der Unternehmen verfügen über die notwendige technische Ausstattung, um Online-Schulungen anzubieten. Gut die Hälfte der europäischen Arbeitnehmer bevorzugt das soziale Lernen mit anderen. 41 Prozent bevorzugen individuelles Lernen. Außerdem wird das Lernen unter Anleitung eines Experten, Lehrers oder Coaches dem Lernen ohne Anleitung vorgezogen.

www.sdworx.com

WELCHE WEITERBILDUNG BEVORZUGEN SIE?

41 %
individuelles Lernen

47 %
soziales Lernen

34 %
Lernen ohne Anleitung

54 %
Lernen unter Anleitung eines Lehrers oder Coaches

Unternehmenskultur

TECHNOLOGIEN UNTERSTÜTZEN NEUE ARBEITSMODELLE

In den letzten drei Jahren hat sich die Art und Weise, wo, wann und wie Menschen arbeiten, maßgeblich verändert. Auch wenn die Pandemie dies beschleunigt hat, gibt es eine Reihe weiterer Faktoren, die neue Arbeitsmodelle ermöglichen oder sogar fordern. Dazu gehören Fortschritte bei Technologien ebenso wie der Ruf der Gen Z und Millennials nach einer höheren Flexibilität hinsichtlich ihrer Arbeit. Doch sind die Menschen auch glücklich mit ihrer Arbeit? Und wenn nicht: Was fehlt ihnen und wo müssen Unternehmen zumindest Teile ihrer Kultur verändern sowie ihre Technologien erneuern? HP hat in seinem Work Relationship Index untersucht, wie zufrieden Mitarbeiter mit ihrer Arbeit sind und Menschen in zwölf Ländern befragt – Deutschland ist eines davon.

Sechs Faktoren beeinflussen die Beziehung zur Arbeit

Insgesamt gibt es sechs Faktoren, die die Beziehung zur Arbeit maßgeblich beeinflussen – so ein Ergebnis der Studie. Dazu gehören Führung, Fokus auf die Mitarbeiter, deren Fähigkeiten und Verwirklichung im Job, auch der Arbeitsplatz beziehungsweise dessen Ausstattung und die eingesetzten Tools. Ein überraschendes Ergebnis: 74 Prozent der Deutschen sind bereit, auf einen Teil ihres Gehalts zu verzichten, wenn ihnen ihre Arbeit wieder mehr Freude bereiten würde. In einer Zeit, in der der Fachkräftemangel immer offensichtlicher wird, sollten Unternehmen ihre bestehende Belegschaft fördern. Doch nur ein Viertel der befragten Mitarbeiter weltweit gab an, dass ihre Firma ihnen Weiterbildungsangebote macht.

Dies sollte in vielen Ländern ein Weckruf sein: Denn laut Statistischem Bundesamt werden bis 2036 insgesamt 12,9 Millionen Erwerbstätige der Baby Boomer Generation das Rentenalter erreichen oder sogar bereits überschritten haben. Unternehmen sollten daher in bestehende Mitarbeiter investieren – egal, ob es sich um Trainings, Technologie oder ihre psychische oder physische Gesundheit handelt. Dann steigt auch die Zufriedenheit mit der Arbeit, die in Deutschland nur bei 21 Prozent liegt und damit viel Luft nach oben bietet.

Nicht nur bei Technologien muss nachgebessert werden

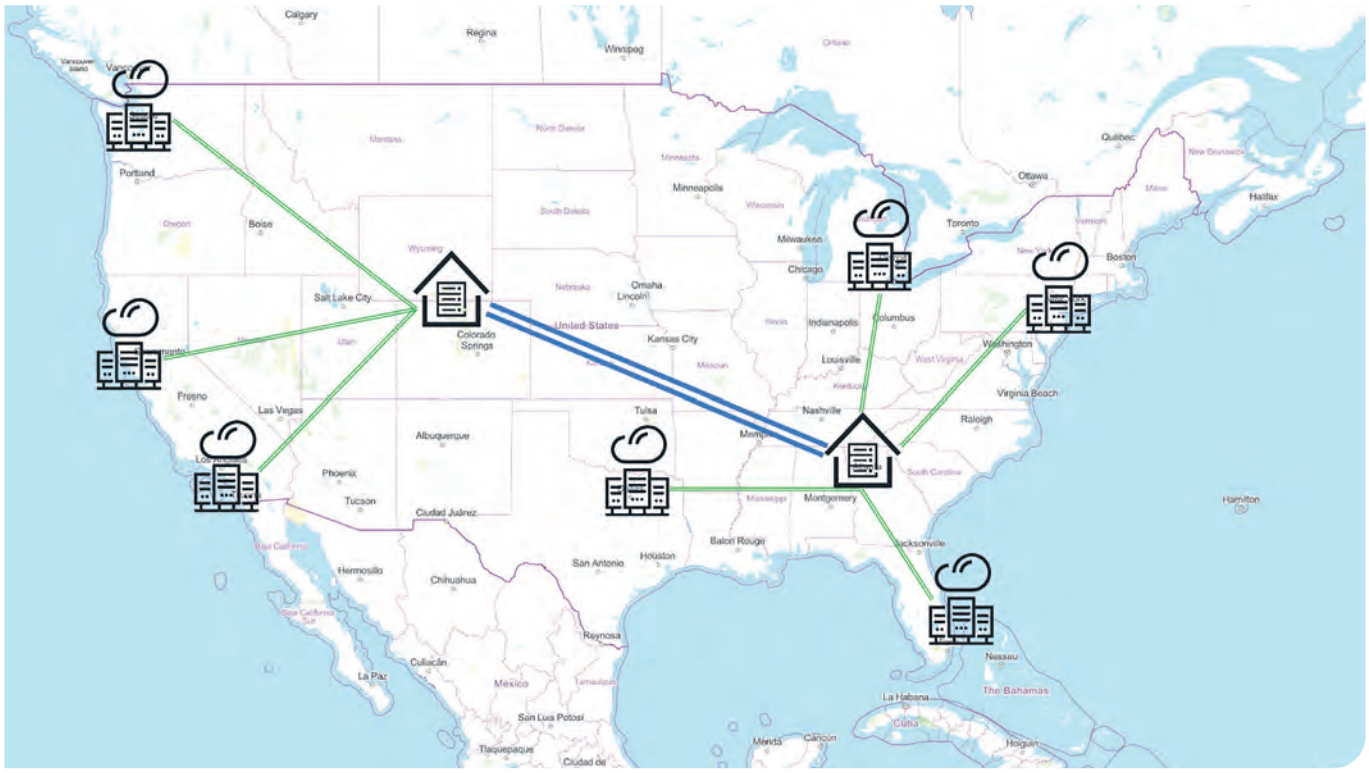
Die Beziehung zur Arbeit wird durch eine Reihe von Faktoren beeinflusst, die auch die Work-Life-Balance in Mitleidenschaft ziehen. Dazu gehören schlechte Führungskräfte oder ein Gefühl der Überforderung. Allerdings sind schlecht funktionierende Hardware, fehlende Headsets, oder der komplizierte Zugriff auf Daten vom Home-Office aus ebenfalls wichtige Faktoren, die die Freude an der Arbeit negativ beeinflussen – nur 21 Prozent der deutschen Befragten gaben an, dass sie mit den zur Verfügung gestellten Tools ihre Aufgaben gut erledigen können.

Da hybride Arbeitsmodelle mittlerweile Alltag sind, möchten Angestellte genauso komfortabel vom Home-Office oder unterwegs arbeiten wie sie dies vom Firmenbüro gewohnt sind. Während der Wandel der Unternehmenskultur längere Zeit in Anspruch nimmt, lässt sich ein gut ausgestatteter Arbeitsplatz mit modernen Technologien recht schnell realisieren – und zwar im Büro wie auch im Home-Office oder unterwegs. Dazu gehören leichte und gleichzeitig leistungsstarke Notebooks, Monitore und Headsets, die eine aktive Teilnahme an Videokonferenzen ermöglichen. Diese relativ kleinen Stellschrauben können eine große Wirkung haben: Mitarbeiter fühlen sich gehört und wertgeschätzt, mit positiven Auswirkungen auf ihre Beziehung zum Unternehmen und zu ihrer Arbeit.

Adrian Müller

DA HYBRIDE ARBEITSMODELLE MITTLERWEILE ALLTAG SIND, MÖCHTEN ANGESTELLTE GENAUSO KOMFORTABEL VOM HOME-OFFICE ODER UNTERWEGS ARBEITEN WIE SIE DIES VOM FIRMENBÜRO GEWOHNT SIND.

Adrian Müller,
Vice President & Managing Director,
HP Germany/Austria/Switzerland,
www.hp.com



Network Inventory Management

INFRASTRUKTURTRENDS BEI TELCOS

Die rasante Virtualisierung etablierter Telekommunikations-Technologie und technische Weiterentwicklungen wie 5G setzen Telekommunikationsunternehmen (Telcos) gehörig unter Druck. Sie müssen jetzt nicht nur Telekom-Infrastrukturen managen, sondern sich um hybride Cloud-Umgebungen und das Data Center Management kümmern. Angesichts der schwierigen Fachkräfte-Situation lässt sich das nur mit viel Automatisierung und einem modernen Network-Inventory-Management-System erreichen.

Ohne leistungsfähige Datennetze wären ein modernes Leben und hochgradig digitalisierte Prozesse in Wirtschaft und Gesellschaft nicht denkbar. Die Corona-Pandemie mit dem Zwang zu Home-Office, der Einsatz von Videokonferenzen, 5G, neue Anwendungen wie gestreamte VR-Welten oder Remote-Operationen in einer Klinik sind nur einige Beispiele, die die Branche vor enorme Herausforderungen stellt.

Schnellere Leitungen sind ein Baustein, um zu reagieren. Die Kapazitäten lassen sich aber nicht immer so schnell erweitern, wie die Anforderungen steigen. Das macht zum Beispiel den Einsatz von Edge Data Centern notwendig, die Telekommunikationsanbieter remote und möglichst automatisiert managen können müssen. Außerdem brauchen sie durchgängige Transparenz, wo Bandbreiten-Flaschenhälse sind, damit die versprochene 5G-Performance auch zuverlässig im Netz zur Verfügung steht.

Telco wird zu NetCo und ServCo

Hinzu kommen die starken Trends zur Virtualisierung und Software-Defined-Networks, die ein ausgefeiltes Hybrid-Ressource-Management erforderlich machen. Die Transformation, bisher in „Bare-Metal" abgebildete Funktionen nun als Software-Anwendung zu implementieren, eröffnet zwar zahlreiche neue Möglichkeiten des automatisierten Provisioning. Allerdings müssen solche Netzwerke ebenso ausfallsicher und einfach zu managen sein. Dafür eignen sich Anwendungen, die die Service- und Network-Orchestration optimal unterstützen. Deshalb setzen große Telekommunikationsanbieter bereits heute Catalog Driven Provisioning ein. Damit wandeln sie sich zunehmend in Netzwerkanbieter (NetCo) für den Netzausbau und Infrastruktur-

dienste und in Serviceanbieter (ServCo) für Kundendienst und B2C, B2B und B2O. Was so harmlos klingt, bedeutet einen grundlegenden Wandel in der zugrundeliegenden Infrastruktur, die neue Prozesse und Tools erfordert. FNT gibt – basierend auf zahlreichen Projekten in diesem Umfeld – im Folgenden vier Empfehlungen, mit denen Telcos die digitale Transformation in Bezug auf ihre Infrastrukturen besser meistern.

Empfehlung 1: Ein zentrales System implementieren, das alles managen kann

Für die Vielzahl an verschiedenen Technologien setzen Telcos auch heute noch viele verschiedene Management-Lösungen ein: Für Gebäude-Pläne kommt Visio zum Einsatz, beim IT-Netzwerk wird ein Monitoring-System verwendet, die Telekom-Infrastruktur wird in Network-Ressource-Management-Systemen abgebildet, virtuelle Maschinen verwalten Cloud-Plattform-Manager und die passive Infrastruktur samt der Kabel eine selbstgestrickte Datenbank. Für Software-Lizenzen ist wieder eine andere Anwendung zuständig. Oft „sprechen" die Systeme nicht miteinander, was immer wieder zu Inkonsistenzen führt, schnelle Antworten verhindert, Planungen erschwert und die vielfach gewünschte Business Agility einschränkt. Die Empfehlung geht daher hin zu einem zentralen System für alles: Telekom- und IT-Hardware, Software, hybride Anwendungslandschaften, Kabel- und Netzwerk-Management, Versionsverwaltung, GIS-Informationen, Vertrags- und Service-Management, Dienstleistersteuerung und einiges mehr.

Empfehlung 2: Eine Plattform nutzen, die offen und flexibel ist

Viele IT-, DC- oder TK-Infrastruktur-Managementsysteme können zwar Daten importieren und manchmal auch Teile davon wieder exportieren, haben aber häufig keine offene Schnittstelle, die eine vollständige Integration mit bestehenden Systemen erlaubt. Integration ist jedoch notwendig, um aus Fremdsystemen heraus auch Datensätze anzulegen, zu modifizieren, zu löschen oder hinterlegte Workflows anzustoßen. Fehlende Integrationsfähigkeit erschwert auch die Prozessabwicklung und Entwicklung von Lösungen, die die eingesetzte Plattform nicht beherrscht. Telcos sollten daher Plattformen bevorzugen, die sich zum einen flexibel anpassen lassen und sich zum anderen über eine offene API problemlos an bestehende Provisioning-, Monitoring-, Service- und Ticketing-Systeme anbinden lassen – und das auch nur mit Bordmitteln und ohne jedes Mal den Hersteller damit beauftragen zu müssen.

Empfehlung 3: Umfangreiche Automatisierungen etablieren

Kombinieren Unternehmen die Fähigkeit einer Plattform, die gesamte Telekom- und IT-Infrastruktur in einem zentralen Inventory zu erfassen und zu steuern, mit der Flexibilität, dieses System mit allen anderen Anwendungen im Unternehmen zu vernetzten, ergeben sich ungeahnte Automatisierungsmöglichkeiten. So können die Rollout- und Netztransformationsprojekte automatisiert mit der Netzdokumentation verbunden werden. Die end-to-end Netzdienste, die quer über physikalische, logische und virtuelle Ebenen laufen, lassen sich dann automatisiert bereitstellen. Eine vollumfängliche API, wie sie die FNT Command Platform bietet, kann sogar dazu genutzt werden, andere Systeme zu automatisieren, die diese Automatisierungsfunktionen gar nicht anbieten.

TELCOS SOLLTEN PLATTFORMEN BEVORZUGEN, DIE SICH ZUM EINEN FLEXIBEL ANPASSEN LASSEN UND SICH ZUM ANDEREN ÜBER EINE OFFENE API PROBLEMLOS AN BESTEHENDE SYSTEME ANBINDEN LASSEN.

Daria Batrakova,
Director Business Line Telecom Solutions, FNT GmbH,
www.fntsoftware.com

Empfehlung 4: Integriert aus dem Network Inventory Management (NIM) heraus planen

Eine integrierte Planungsfunktionalität direkt aus dem Network Inventory Management heraus ist nicht nur in der Lage, technische Details unter Einbeziehung von GIS-Daten vorzuplanen und bei Implementierung auch gleich die passenden Bestellungen auszulösen. Sie verwaltet auch alle Informationen zum rechtlichen Rahmen. Beim Aufstellen neuer Antennen gehören dazu beispielsweise auch die Vertragsbedingungen, Grundbuch-Dienstbarkeiten, die Leitungsplanung und vieles mehr. Genauso können die Anwendenden alle geographischen Gegebenheiten visualisieren und interaktiv in einer 2D-Ansicht ausgestalten. Ist die Planungsfunktionalität ins NIM integriert, basiert sie immer auf dem aktuellen Datenbestand. Technikteams können den geplanten Soll-Zustand nach Planungsumsetzungen mit einem Klick zum neuen Ist-Zustand machen. Durch diesen Closed-Loop bleibt das NIM immer auf dem aktuellen Stand und liefert verlässliche Informationen.

Der Schlüssel zum Erfolg

Mit einem zentralen Network Inventory Management, das umfangreiche Funktionalitäten von der Erfassung über das Management bis zur integrierten Planung besitzt, reagieren Telcos schneller auf Veränderungen und arbeiten effizienter. Es hilft, mit den rasanten Veränderungen ihrer Branche leichter Schritt zu halten.

Daria Batrakova

E-Mail-Management

WARUM SICH FINANZUNTERNEHMEN DAMIT AUSEINANDERSETZEN SOLLTEN

Was die Erhebung, Speicherung und Verarbeitung von (Kunden-)Daten betrifft, sehen sich Unternehmen aus dem Finanzsektor seit einigen Jahren verschärften Regularien gegenüber.

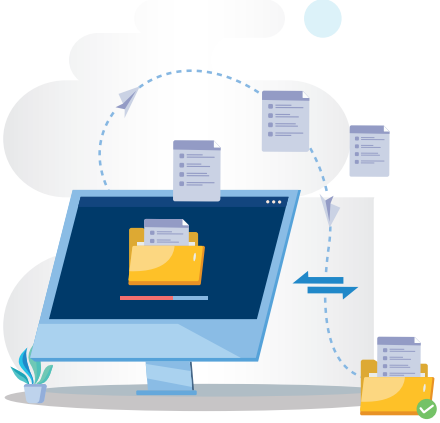
Da Finanzunternehmen personenbezogene und andere sensible Daten verarbeiten, müssen auch sie die Grundsätze der EU-DSGVO befolgen. Diese umfassen unter anderem Zweckbindung, Datenminimierung, Integrität, Vertraulichkeit sowie weitere Betroffenenrechte wie das Recht auf Löschung (Art. 17).

Viele dieser Informationen werden auch via E-Mail versendet. Besonders seitdem hybride Arbeitsansätze beliebter werden, müssen Unternehmen ihren Umgang mit personenbezogenen und anderen sensiblen Daten prüfen und überdenken. Empfehlenswert ist daher für IT-Entscheider eine umfassende E-Mail-Management-Strategie einzuführen. Im Rahmen dieser Strategie müssen sie definieren, wie sie ihre elektronische Kommunikation verarbeiten, verwalten und archivieren – zum Beispiel mithilfe einer professionellen E-Mail-Archivierungslösung.

Besseres E-Mail-Management

Im Zusammenhang mit dem E-Mail-Management kommt häufig die Frage auf: Reicht es nicht, wenn ich bereits ein Backup-System im Einsatz habe, das unter anderem Kopien meiner E-Mails und ihrer Anhänge erstellt? Die kurze Antwort ist: Nein. In erster Linie unterscheidet sich die E-Mail-Archivierung in ihrem Ziel von herkömmlichen Backups. Während Backup-Kopien kurz- bis mittelfristig auf einem externen Speichermedium vorgehalten werden und sich daher eher für die Disaster Recovery eignen, ist das Hauptziel der E-Mail-Archivierung die vollständige, revisionssichere, langfristige und jederzeit verfügbare Aufbewahrung der Nachrichten. Das spielt unter anderem dann eine wichtige Rolle, wenn Aufsichtsbehörden die Daten prüfen möchten. Beispiele wären eine Steuerprüfung oder eine Prüfung durch Datenschutzaufsichtsbehörden.

Außerdem ist eine gute E-Mail-Archivierungslösung in der Lage, das gesamte E-Mail-Archiv des Unternehmens effizient



zu durchsuchen und bei Bedarf einzelne E-Mails zu extrahieren und/oder zu löschen. Im Idealfall hat ein Finanzunternehmen sowohl entsprechende Backups als auch eine E-Mail-Archivierungslösung parallel im Einsatz, da sich beide Ansätze ergänzen.

Dafür stehen IT-Managern in Finanzunternehmen zwei strategische Archivierungsansätze zur Verfügung: Bei der Journalarchivierung steht die rechtskonforme Archivierung im Mittelpunkt, bei der Postfacharchivierung die Entlastung des E-Mail-Servers. Auch eine Kombination beider Ansätze ist möglich.

Dadurch kann E-Mail-Archivierung nicht nur die Einhaltung von rechtlichen Vorgaben ermöglichen, sondern steigert auch das Sicherheitsniveau. Kommt es zu einem technisch bedingten Systemausfall oder einem Cyber-Angriff, senkt sie das Risiko des Datenverlusts – die archivierten Datensätze lassen sich vollständig wiederherstellen.

Speicherstandort, Datenhoheit und Verarbeitung durch Dienstleister

Im Rahmen des E-Mail-Managements stellt sich zudem unweigerlich die Frage, wo die Daten gespeichert werden sollen – auf dem unternehmenseigenen Server oder über einen SaaS-Anbieter in der Cloud? Entscheiden sich Finanzunternehmen für die Cloud gilt es zwei Dinge zu beachten: Zum einen sollten sie branchenspezifische Richtlinien wie zum Beispiel die Richtlinien der Europäischen Bankenaufsichtsbehörde (EBA) oder auch der Europäischen Aufsichtsbehörde für das Versicherungswesen und die betriebliche Altersversorgung (EIOPA) berücksichtigen.

Zum anderen müssen sie sicherstellen, dass – sollten die betroffenen Rechenzentren in einem Land außerhalb der EU liegen – das Datenschutzniveau, dem der EU entspricht. Andernfalls wird es schwer, personenbezogene Daten rechtskonform in Drittländer zu übertragen.

www.mailstore.com

Datenmanagement

DATENEXPERTEN SIND DIE NEUEN PRODUKTMANAGER

Digitales Datenmanagement fristet in vielen Unternehmen immer noch ein Schattendasein. Das Aufkommen KI-basierter Anwendungen ist jetzt ein weiterer Grund, diesen Umstand dringend zu ändern, Silos einzureißen und langfristige Strategien zu entwickeln.

Die meisten Unternehmen würden sich wohl als datengetrieben bezeichnen. Dass dies nicht der Realität entspricht, belegen immer wieder Studien, so wie jüngst eine Zoho-Umfrage über digitale Gesundheit, die unter anderen auch deutsche Unternehmen unter die Lupe nimmt. Sie zeigt: Nur ein Viertel der Befragten ist digital gesund, hat sich also erfolgreich digital transformiert. Weniger als die Hälfte (41 Prozent) verfügt über einen durchschnittlichen Digitalisierungsgrad, und rund ein Drittel (34 Prozent) hat noch nicht einmal richtig damit angefangen. Diese Ergebnisse verdeutlichen auch: Hat sich ein Unternehmen nicht oder nur zu einem bestimmten Grad digitalisert, kann es auch keine digitale Datenstrategie umsetzen, und damit auch kein effizientes Datenmanagement.

Den Firmen entstehen durch diesen Umstand klare Nachteile, denn wenn sie umsetzbare Erkenntnisse aus ihren Daten ziehen wollen, wird es ohne effizientes Datenmanagement nicht funktionieren. Erst wenn alle Mitarbeitenden Zugriff auf für sie freigegebene Daten haben, können sie Schlüsse daraus ziehen und Aktionen einleiten. Eine umgesetzte Datenstrategie führt also zu mehr Produktivität und einer verbesserten Wettbewerbsfähigkeit.

Jüngst kam noch ein weiterer Faktor hinzu. KI-basierte Anwendungen versprechen die Automatisierung von Prozessen und geschäftliche Innovationen. Jedoch: Algorithmen lernen aus bestehenden Daten. Sind diese mangels eines Datenmanagement falsch oder nicht auffindbar, können Unternehmen auch nicht von den Vorteilen der KI-Tools profitieren.

Datenstrategie sollte alle Abteilungen umfassen

Keine Firma kann sich drohende Umsatzeinbußen und verpasste Wettberbsvorteile leisten – denn das ist die Tragweite eines mangelnden Datenmanagements. Deswegen ist es höchste Zeit zu handeln. Die Basis sollte eine Datenstrategie sein, die alle Abteilungen einschließt. Oft arbeiten Datenexperten noch isoliert vom Rest der Organisation und verwahren die Daten so hermetisch in Silos, dass nur sehr wenige damit arbeiten können. Doch dieser Umstand behindert eine unternehmensübergreifende Zusammenarbeit, bei der im Sinne des Datenproduktmanagements wertvolle Datenlösungen entstehen. Kundenorientierte Datenprodukte wirken sich nachweislich direkt auf das Unternehmensergebnis aus. Aber auch interne Datenprodukte erfordern die Mitwirkung mehrerer Abteilungen, von Design und Webentwicklung bis hin zu Finanzen und Personalwesen, um optimale Ergebnisse zu erzielen.

EIN GROSSER GEWINN AUS EINEM DIGITALEN DATENMANAGEMENT IST DIE FÄHIGKEIT, AUS DIESEN INFORMATIONEN DATEN-PRODUKTE ZU ENTWICKELN

Sridhar Iyengar, Managing Director, Zoho Europe, www.zoho.com

Eine Lösung bieten cloudbasierte BI-Plattformen. Auf solch ein zentrales Datenzentrum haben alle Abteilungen Zugriff. Für eine hohe Datenqualität müssen strenge Grundsätze für die Datenverwaltung und -standardisierung sorgen. Die Zentralisierung gewährleistet, dass Daten genauer und kontextbezogener sind, so dass Mitarbeitende schnell Informationen finden und Datenteams ein exaktes Bild bekommen, bevor sie mit der Entwicklung von Datenprodukten beginnen. Deren Wert und die zunehmende Produktmanagement-Mentalität der Datenexperten sind der wahre Wettbewerbsvorteil, der Unternehmen durch Datenmanagement entsteht.

Sridhar Iyengar

Master Data Management

KORREKTE DATEN SIND DIE BASIS FÜR KI-ANWENDUNGEN

Frau Meier, Frau Meyer oder Frau Maier? Gleich mehrfach findet sich der Datensatz in der digitalen Kundenkartei, immer mit der gleichen Adresse – welche Schreibweise stimmt wohl? Solche offensichtlich duplizierten und falschen Stammdaten, also Grundinformationen für einen effizienten Geschäftsbetrieb, sind ein großes Problem. Schließlich stecken die Unternehmen mitten in der digitalen Transformation, und erhoffen sich dadurch datenbasierte und somit bessere Entscheidungen treffen zu können. Nur, wenn sie sich auf ihre Daten nicht verlassen können, wird dieser Umstand nicht eintreten. Frau Meier, Frau Meyer oder Frau Maier wird nicht nur sauer sein, dass eine ihrer Lieblingsmarken ihren richtigen Namen nach jahrelanger Kundenbeziehung immer noch nicht weiß, auch die internen Vertriebs- und Marketingteams werden Probleme haben, mit fehlerhaften Datensätzen Customer Journeys auf verschiedenen Kanälen zu verfolgen und zu optimieren. Neben den falschen Daten ist auch die Menge an Informationen, die in digitalisierten Märkten entstehen, eine Herausforderung. Aktuelle Unternehmenssysteme sind häufig mit dem Volumen und der Vielfalt überfordert und stellen die nötigen Daten nicht schnell genug zur Verfügung.

VIELE UNTERNEHMEN MÖCHTEN SCHNELLSTMÖGLICH KI-ANWENDUNGEN IN IHRE GESCHÄFTSPROZESSE INTEGRIEREN. DAS GRÖSSTE HINDERNIS AUF DIESEM WEG SIND FEHLERHAFTE STAMMDATEN, DESWEGEN IST JETZT EIN GUTER ZEITPUNKT, UM RICHTIG AUFZURÄUMEN.

Daniel Pott,
Leiter Geschäftsbereich Data & Application Innovation, Macaw, www.macaw.de

Aus falschen Daten entstehen schlechte KI-Anwendungen

Neben ineffizienten Prozessen und verärgerter Kundschaft verursachen fehlerhafte Datensätze noch ein weiteres Problem: Es ist unmöglich, daraus KI-Anwendungen zu entwickeln. Jetzt, da viele Unternehmen Künstliche Intelligenz in ihre Prozesse integrieren möchten, müssen sie unbedingt Ordnung schaffen. Schließlich lernen ML- (Machine Learning) und KI-Algorithmen aus Daten; sind diese fehlerhaft, hat das negative Auswirkungen.

Die beste Möglichkeit, um wichtige Stammdaten über Produkte, Lieferanten, Kundschaft, Mitarbeitende, Standorte und Inventar zu bereinigen, ist das Stammdatenmanagement (Master Data Management, MDM). Durch die Zusammenführung und Bereinigung von Daten aus verschiedenen Quellsystemen in eine MDM-Plattform soll ein „Golden Record" entstehen: ein zuverlässiger und eindeutiger Datensatz, der die Grundlage für fundierte strategische Entscheidungen und die Rationalisierung von Geschäftsprozessen bildet.

Auch, wenn viele Unternehmen am liebsten gleich zur technischen Umsetzung einer MDM-Plattform schreiten würden, müssen sie vorher einige theoretische Überlegungen anstellen und Prozesse verändern. MDM umfasst viel mehr als die Auswahl des richtigen Tools: Es ist eine Geschäftsthematik und kann nur gelingen, wenn eine Organisation das Projekt gemeinsam angeht. Häufig kommt es vor, dass verschiedene Abteilungen und Teams sich für die gleichen Daten zuständig fühlen und Prozesse unterschiedlich angehen. Es ist daher entscheidend, im Vorfeld eines MDM-Projektes im Sinne von Data Governance klare Eigentumsverhältnisse der Daten festzulegen. Nur, wenn Verantwortlichkeiten und Befugnisse klar definiert sind, können konsistente und korrekte Daten im gesamten Unternehmen vorliegen. Sind die nötige Datenreife, Zuständigkeiten und Prozesse geklärt, kann die Implementierung eines MDM-Systems erfolgen.

Data-Steward-as-a-Service

Je nachdem, wie schnell Unternehmen eine hohe Datenqualität brauchen, sollten sie auch die Methode für die Umsetzung des Projektes wählen. Eine Einführung nach dem klassischen Wasserfallmodell, bei dem die Beteiligten Schritt für Schritt ein theoretisches technisches Konzept entwickeln und dann ausrollen, nimmt häufig viel Zeit in Anspruch. Wer rasche Ergebnisse sehen möchte, sollte lieber agil vorgehen. Hierbei helfen externe Experten, die bei der Prozessberatung unterstützen, eine Roadmap erstellen, die technische Umsetzung planen – und parallel schon ein-

Viele Mitarbeitende entwickeln heute auf Basis von Daten neue Produkte, etwa für Kundenakquise, -betreuung und -bindung. Daher ist es äußerst wichtig, dass sie auf richtige und eindeutige Informationen zurückgreifen können.

(Quelle: Campaign Creators / Unsplash)

mal aufräumen. Zum Beispiel mit einem Data-Steward-as-a-Service, bei dem Dienstleister den Job des Data Steward übernehmen – einer Schlüsselposition im Data Management, die dafür sorgt, dass Datenqualität und strategische Vorgaben eingehalten werden.

Am besten funktioniert die Zusammenarbeit zwischen Unternehmen und externen Data Stewards über cloud-basierte MDM-Plattformen wie Profisee oder anderen benutzerfreundlichen Tools, in der Teams im Sinne des Data Mesh auf die bereinigten Daten zugreifen und sie dort auch gleich für die Entwicklung neuer Produkte nutzen können. Mitarbeitende jeder Unternehmensstufe müssen jederzeit auf sämtliche Erkenntnisse aus Daten zugreifen können, um ihre Arbeit effizient erledigen und Kunden besser betreuen zu können. Zum Beispiel indem sie Datenlösungen nutzen, die die Kombination von Front- und Backoffice ermöglichen und mit verschiedenen Informationskanälen verbunden sind.

Die drei goldenen Regeln des MDM

Überhaupt spielen Mitarbeitende beim MDM eine sehr große Rolle. Die Thematik funktioniert nur, wenn sich alle an die drei goldenen Regeln halten: korrekte Dateneingabe, die Einhaltung von Prozessen und die Aufrechterhaltung einer hohen Datenqualität. Alle Beschäftigten müssen diese verinnerlichen. Anfangs ist die Einführung von MDM sicher eine Herausforderung, denn das Einrichten neuer Prozesse, die Einführung von Technologien und die Neudefinition von Arbeitsabläufen kann Widerstand hervorrufen. Deshalb sind Aufmerksamkeit für solche Veränderungen und Anleitung ein Muss. Es geht nicht nur darum, die Belegschaft im Umgang mit den neuen Tools zu schulen, sondern die Mitarbeitenden sollten auch verstehen, warum MDM wichtig ist, welchen Nutzen es bietet und wie es ihre täglichen Aufgaben vereinfachen kann.

Schließlich bieten hochwertige Daten Unternehmen und ihren Mitarbeitenden sehr viele Möglichkeiten. Marketers, Business Developer und Senior Managerinnen und Manager entwickeln damit etwa neue Geschäftsmodelle zur Kundenakquise, -betreuung und -bindung. Das Talent von Mitarbeitenden, kreativ sämtliche Möglichkeiten zu nutzen, die Daten und Technologie bieten, wirkt sich direkt auf die Wettbewerbsfähigkeit von Unternehmen aus. Die Voraussetzung dafür ist jedoch, dass die Daten gut unter Kontrolle sind und richtig bei den Mitarbeitenden ankommen.

Daniel Pott

Testdatenmanagement

ERSTELLUNG VON SYNTHETISCHEN UND REFERENTIELL KORREKTEN TESTDATEN

TEIL 4 VON 4

Dies ist der letzte Artikel einer vierteiligen Serie zum Thema End-to-End Datenmanagement mittels der Plattform IRI Voracity. In den vorherigen Artikeln wurde die Wichtigkeit einer umfassenden Datenverarbeitung betont, so wurde im ersten Artikel der Umfang von IRI Voracity vorgestellt. Sie vereint Datenerkennung, -integration, -migration, -verwaltung in einem Metadaten-Framework. Die Verwendung einer einzigen Konsole ermöglicht eine effizientere Bedienung und führt zugleich zu Kosteneinsparungen in vernetzten IT-Umgebungen.

Im zweiten Artikel wurden die Vorteile der Datenintegration, -migration und -modernisierung aufgezeigt, denn diese Maßnahmen verbessern die Qualität, Verfügbarkeit und Wertigkeit der Daten.

Der dritte Artikel ging auf die Funktionen ein, um sensible Daten in verschiedenen Formaten und Quellen automatisch zu lokalisieren, zu schützen und DSGVO-konform zu verarbeiten. So ist eine durchgängige Datensicherheit sichergestellt, unabhängig von der Datenstruktur oder dem Format.

End-to-End-Datenmanagement ist von zentraler Bedeutung, denn es gewährleistet, dass Daten über ihren gesamten Lebenszyklus hinweg effizient und zuverlässig verwaltet werden. Aus mehreren Gründen spielt in diesem Kontext auch das Thema des Testdatenmanagement (TDM) mit der Generierung und Verwaltung von Testdaten eine sehr wichtige Rolle:

#1 Qualitätssicherung: Anwendungen und Systeme müssen reibungslos funktionieren und unter realistischen Bedingungen getestet werden. Die erstellten Testdaten sollten die Produktionsdaten widerspiegeln, um potenzielle Probleme frühzeitig zu erkennen.

#2 Datenschutz: Bei der Entwicklung und Durchführung von Tests müssen personenbezogene Daten und sensible Informationen geschützt werden. Testdaten müssen demnach echte Daten maskieren oder anonymisieren, um Datenschutzvorschriften einzuhalten.

#3 Skalierbarkeit: Die Testdaten müssen in ausreichender Menge und Vielfalt vorhanden sein, um unterschiedliche Testszenarien und -umgebungen abzudecken. Die Testdatengenerierung ermöglicht die Erstellung von Datensätzen, die die Skalierbarkeit der Anwendung überprüfen.

> DIE TESTDATENGENERIERUNG TRÄGT DAZU BEI, DIE QUALITÄT, SICHERHEIT, EFFIZIENZ UND SKALIERBARKEIT VON ANWENDUNGEN UND SYSTEMEN IM RAHMEN DES END-TO-END-DATENMANAGEMENTS SICHERZUSTELLEN.
>
> **Amadeus Thomas, Geschäftsführer, Jet-Software GmbH, www.jet-software.de**

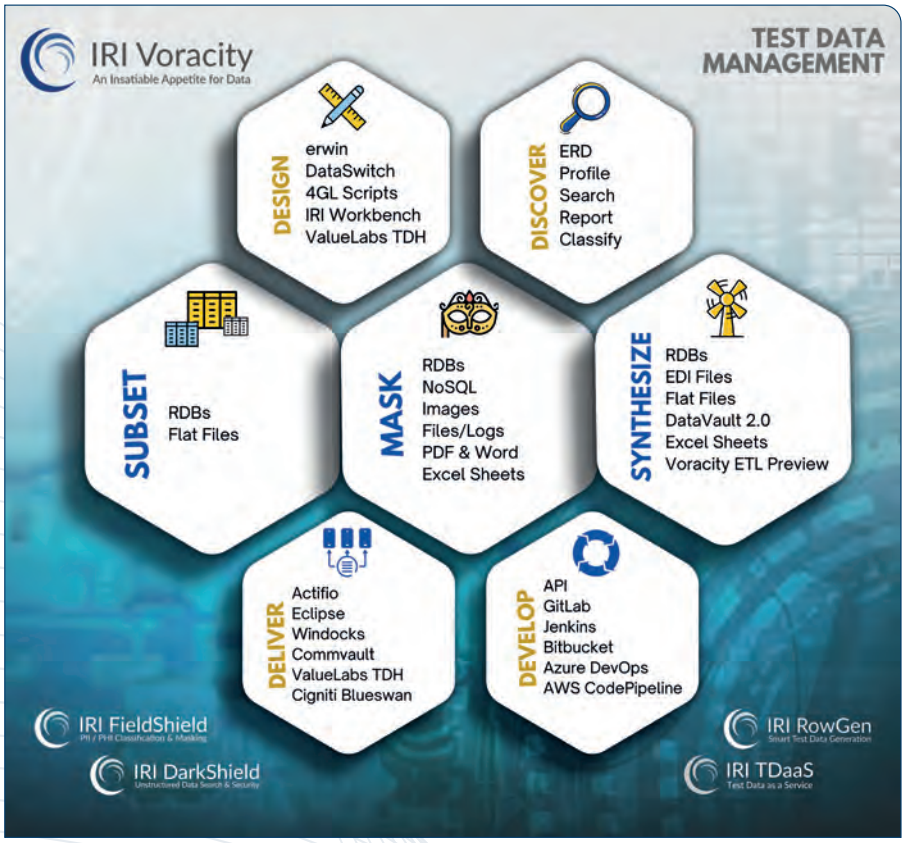
#4 Effizienz: Die manuelle Erstellung von Testdaten ist sehr zeitaufwändig und fehleranfällig. Durch automatisierte Testdatengenerierung können wiederholbare und umfangreiche Tests effizient durchgeführt werden.

#5 Wiederverwendbarkeit: Testdaten müssen wiederverwendbar sein, um die Konsistenz der Tests über verschiedene Entwicklungs- und Testphasen hinweg sicherzustellen. Das spart Zeit und Ressourcen.

Die Testdatengenerierung trägt dazu bei, die Qualität, Sicherheit, Effizienz und Skalierbarkeit von Anwendungen und Systemen im Rahmen des End-to-End-Datenmanagements sicherzustellen. Um effektive Tests durchzuführen, ist es entscheidend, dass Tabellenansichten, Indexreihenfolgen, Schlüsselbeziehungen sowie Datei- und Berichtsinhalte die Realität widerspiegeln. Die Erzeugung von realistischen Werten und Formaten, insbesondere in sicheren Datenbereichen und das Auffüllen großer Datensätze, kann zeitaufwändig sein.

Mit der IRI Voracity-Plattform können verschiedene Testdatenziele erstellt werden, darunter Testdatenbankladungen, Dateistrukturen und benutzerdefinierte Berichtsformate. Das Besondere dabei ist, dass lediglich Metadaten und keine Produktionsdaten dafür nötig sind. Dies führt

Bild 1:
Testdatenmanagement



nicht nur zu einem verstärkten Datenschutz, sondern ermöglicht auch die Verfügbarkeit von präziseren Testdaten, die auf die eigene Geschäftslogik zugeschnitten sind. Alternativ können natürlich auch reale Daten in Produktions-, On-Demand- oder virtualisierten Testumgebungen verwendet und diese mit IRI Voracity anonymisiert, unterteilt oder maskiert werden.

Insgesamt stehen vier Methoden zur Erzeugung sicherer und intelligenter Testdaten zur Verfügung, die sowohl für referenziell korrekte Datenbanken als auch für Flat-Files, semistrukturierte Dateien, formatierte Berichte und sogar unstrukturierte Dateien (Dark Data) geeignet sind:

#1 Maskierung von Produktionsdaten

#2 RDBMS-Tabellen-Subsetting und Spaltenmaskierung

#3 Synthese strukturierter Daten (Zufallsgenerierung/-auswahl)

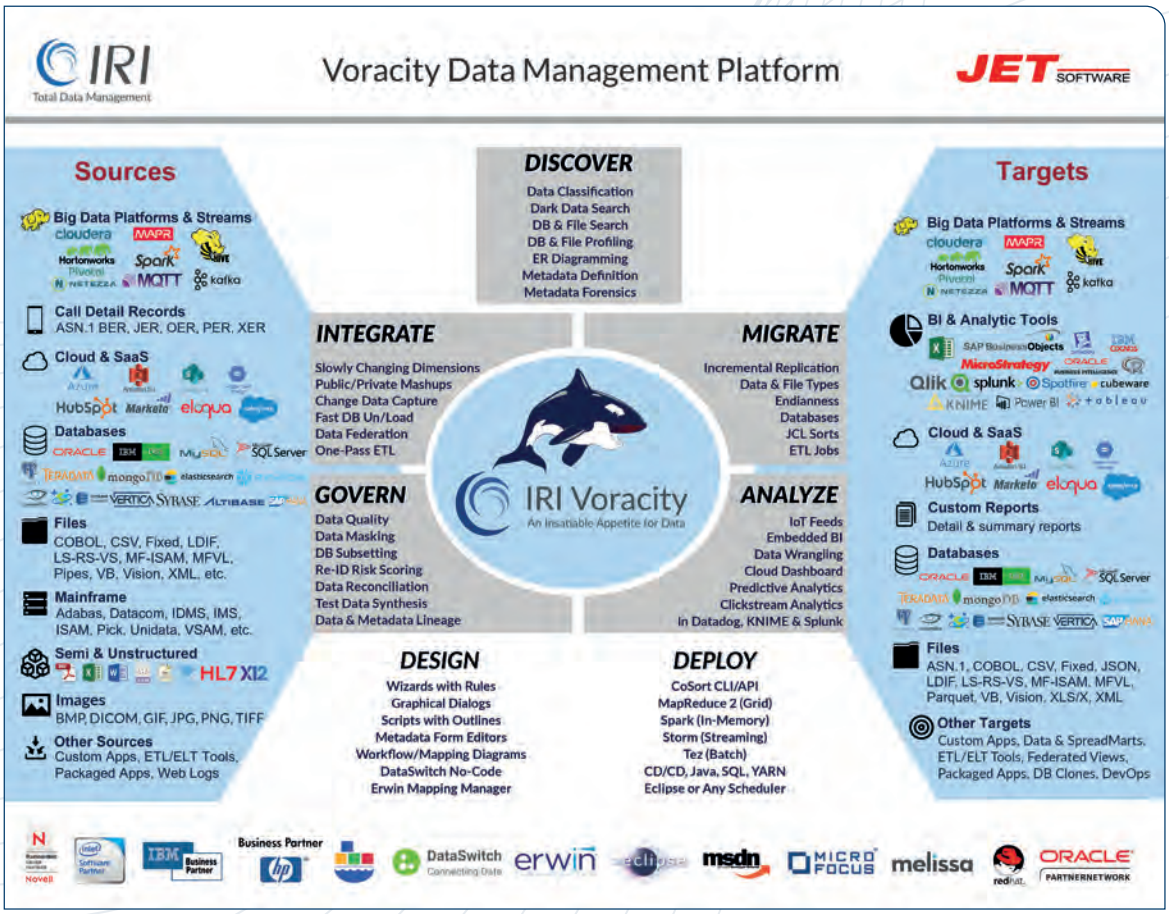
#4 Beliebige Kombination der vorher drei gelisteten Funktionen

Die integrierten Assistenten für Tabellenersetzung und die Generierung von Testdaten vereinfachen die Entwicklung von Datenbanken und Enterprise Data Warehouses (EDW) sowie die Erstellung virtueller Testdaten für DevOps. Dies gewährleistet, dass Kopien von Produktions-Tabellenauszügen, die maskiert und referenziell korrekt sind, die Sicherheit der Produktionsdaten bewahren und gleichzeitig realistische Testdaten bereitstellen. Die Testdaten sind strukturell und referenziell korrekt und können für verschiedene gängige relationale Datenbankmanagementsysteme (RDBMS) mit definierten Beschränkungen sowie für benutzerdefinierte Berichtsformate oder gängige Datei- und Feed-Formate auch synthetisch generiert werden:

- Record, Zeilen, oder variabel sequentiell
- ASN1. CDRs
- COBOL index (MF ISAM, Vision)
- CSV, LDIF, JSON und XML
- Excel (XLS/X)
- FHIR, HL/7 und X12 EDI
- Festgelegter Text und Mainframegeblockt
- HDFS
- Bilddateien und PDFs
- MQTT und Kafka Themen
- BIRT (via ODA) und KNIME (Analyse- und Visualisierungsknoten) in Eclipse

Es können entweder zufällige Feldwerte in mehr als 100 Datentypen generiert werden, oder zufällige Daten aus Set-Dateien auf Feldebene ausgewählt werden. Diese Batch-Jobs können entweder direkt in IRI Voracity, via Value Labs TDH, per Befehlszeile oder in Windocks ausgeführt werden. Zusammen mit benutzerdefinierten/zusammengesetzten Datenwerten, Wertebereichen und Verteilungen wird die Realitätsnähe von Testdaten verbessert. Auch Standard- und komplexe Datentransformationen sowie die Verwendung von Set-Dateien und bedingter Auswahl tragen zur Werterhöhung der Testdaten bei, insbesondere bei der Simulation von Produktionstabellen und Dateiformaten für verschiedene Anwendungen. Zudem werden DDL-Informationen

Bild 2:
End-to-End Datenmanagement



für verschiedene Datenbankplattformen wie Oracle, DB2 UDB, SQL Server, Sybase, Teradata und Andere genutzt, um realistische Tabellen mit struktureller und referentieller Integrität zu erstellen. Dies ermöglicht die Befüllung eines gesamten Test-EDW oder DataVaults. Unter Einsatz der eigenen Datenmodelle und Metadaten sowie optionaler Verwendung von Produktionsdaten stehen somit diverse unkomplizierte und zeiteffiziente Vorbereitungsmöglichkeiten zur Verfügung:

- Erstellung von Test-Datenbanken mit referenzieller Integrität
- Simulation und gemeinsame Verwendung von Datei-, Bild- und Berichtslayouts
- Einhaltung von nationalen und internationalen Datenschutzgesetzen
- Entwicklung und Durchführung von Belastungstests der Anwendungen
- Benchmarking von neu geplanter Hardware und Software
- Durchführung von ETL-Tests für Enterprise Data Warehouse
- Erstellung von umfangreichen virtuellen Szenarien

Fazit

Dank einer mehr als 40-jährigen Erfahrung im Bereich Big Data Management und kontinuierlicher Weiterentwicklung der IRI Voracity Plattform ist es möglich, ein umfassendes und gesetzeskonformes End-to-End Datenmanagement zu realisieren – und das alles innerhalb einer einzigen Konsole. Wie in diesem Artikel beschrieben, schließt dies DSGVO-konforme Verwaltung von Testdaten ein, wobei die integrierten Funktionen eine breite Unterstützung für verschiedene Datenbanken und Dateiformate bieten, die auf verschiedenen Betriebssystemen genutzt werden können.

Diese vielseitige Lösung ist äußerst nützlich für die Erstellung von Datenbanken, EDW- und Data Vault-Prototypen, Belastungstests von Anwendungen, DevOps, Benchmarking und datenschutzkonforme Demonstrationen, einschließlich der Verwendung großer Mengen von vorsortierten (und vollständig vorkonfigurierten) Testdaten für Massenladungen. Die Plattform ist auf Windows sowie allen Varianten von Linux und Unix (einschließlich z/Linux und MacOS) einsatzbereit und kann zudem in Cigniti BlueSwan TDM-Umgebungen für Softwaretests und Qualitätsmanagement integriert werden.

Amadeus Thomas

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

Industrielle Revolution

DIE FÜNFTE WELLE?

Heutzutage werden pro Stunde mehr Daten erzeugt als noch vor zwei Jahrzehnten in einem ganzen Jahr. Das Potenzial, das in ihnen steckt, ist noch lange nicht ausgeschöpft. Das ändert sich jetzt: Generative KI-Modelle wie ChatGPT ermöglichen es Maschinen, menschliche Sprache zu verstehen und menschliche Dialoge und Inhalte zu produzieren.

Aufgrund dieser rasanten Datenentwicklung werden wir in Zukunft nicht mehr von Gigabytes oder Terabytes sprechen, denn schon heute bewegt sich das digitale Universum im Bereich von Yottabytes, was der Datenmenge von 250 Billionen DVDs entspricht. Die digitale Zukunft werden Geopbytes sein.

Industrie 5.0 dank KI

Dank KI surfen wir gerade auf der fünften Welle der industriellen Revolution, kurz Industrie 5.0. Industrie 5.0 ist geprägt von menschlichen Robotern, Interaktion, kognitiven Systemen. Bis vor kurzem konnte KI nur lesen und schreiben, aber keine Inhalte verstehen. Inzwischen sind Anwendungen wie ChatGPT in der Lage, natürliche Sprache zu verstehen und Dialoge und Inhalte zu produzieren. Analysten sprechen bereits von einem „iPhone-Moment" für KI. Kein Produkt vor ChatGPT wurde jemals schneller angenommen.

Profiteure der KI-Revolution

Künstliche Intelligenz und maschinelles Lernen werden die meisten Branchen beeinflussen. Bei künstlicher Intelligenz geht es vor allem um Berechnungen. Dafür braucht man Rechenleistung und Datenspeicher. Eine ChatGPT-Suche zum Beispiel kostet zwischen 10-und 100-mal mehr als eine normale Google-Suche.

https://dnbam.com/de

Cloudbasierte PPM-Lösung für den Mittelstand

WETTBEWERBSVORSPRUNG DURCH PROJEKTPORTFOLIO-MANAGEMENT

Mittelständische Unternehmen können auf Veränderungen meist flexibler als größere Firmen reagieren, weil ihre Führungsstrukturen schlanker sowie die Entscheidungsprozesse kürzer sind und sie aufgrund ihrer Spezialisierung ihre Märkte sehr gut kennen. Da sich jedoch globale Entwicklungen, ob Krisen oder positive Trends, immer schneller auswirken und stärker wechselseitig beeinflussen, sind schnell verfügbare Informationen hierüber und deren Folgen so wichtig wie nie, um wettbewerbsfähig zu bleiben.

Vom Projektmanagement ...

Egal, welche strategische Ziele ein Unternehmen selbst verfolgt – ob Kostensenkung, Prozessoptimierung, Produktivitätssteigerung oder Verbesserung der Innovationskraft werden Führungskräfte und Beschäftigte immer mehr mit Aufgaben in Projekten zu tun haben. Um diese Vielzahl an Projekten samt Daten über Termine, Personen, Ressourcen und Budgets zu koordinieren, wenden Mittelständler seit längerem Projektmanagement-Methoden an. Dabei haben sie erkannt, dass sie ein professionelles Projekt-Tool einsetzen sollten, um schneller und bessere Entscheidungen treffen zu können. Zu den typischen Fragen in ihren Entscheidungsprozessen zählen zum Beispiel:

Welche unserer Projekte bringen uns den größten Gewinn? Wo können wir Kosten einsparen und wie wirkt sich dies aus? Welche kritischen Ressourcen können wir wo am sinnvollsten einsetzen? Welche Innovationsprojekte können wir beschleunigen? Inwieweit sind andere Projekte dadurch betroffen? Welche Risiken gibt es?

Bei solchen wirtschaftlichen Fragen stoßen jedoch die im Mittelstand heute noch sehr weit verbreiteten manuellen Office-Tools wie etwa Excel oder PowerPoint schnell an ihre Grenzen. Denn damit lassen sich weder Ressourcen verwalten noch die Projektinformationen über Bereiche oder Standorte sinnvoll konsolidieren. Zudem verursachen sie Mehrarbeit und sind sehr fehleranfällig.

... zum Projektportfolio-Management

Mit Projektportfolio-Management-(PPM)-Tools, hingegen, können Firmen ihre Daten aus den unterschiedlichen Projekten auch über Fachbereiche hinweg in einer Informationsquelle zusammenführen und transparent aufbereiten. Tools, wie etwa Planisware Orchestra, sind daher im Mittelstand längst angekommen, weil sie Unternehmen eine konsolidierte Sicht auf alle Projektaktivitäten in Echtzeit bieten. Ihr Einsatzgebiet erstreckt sich über viele Bereiche: vom Aufgabenmanagement, über Terminplanung und Ressourcenmanagement bis hin zur Steuerung komplexer Innovationsprojekte mit Fokus auf Produktentwicklung.

Beschleunigte Entscheidungsprozesse

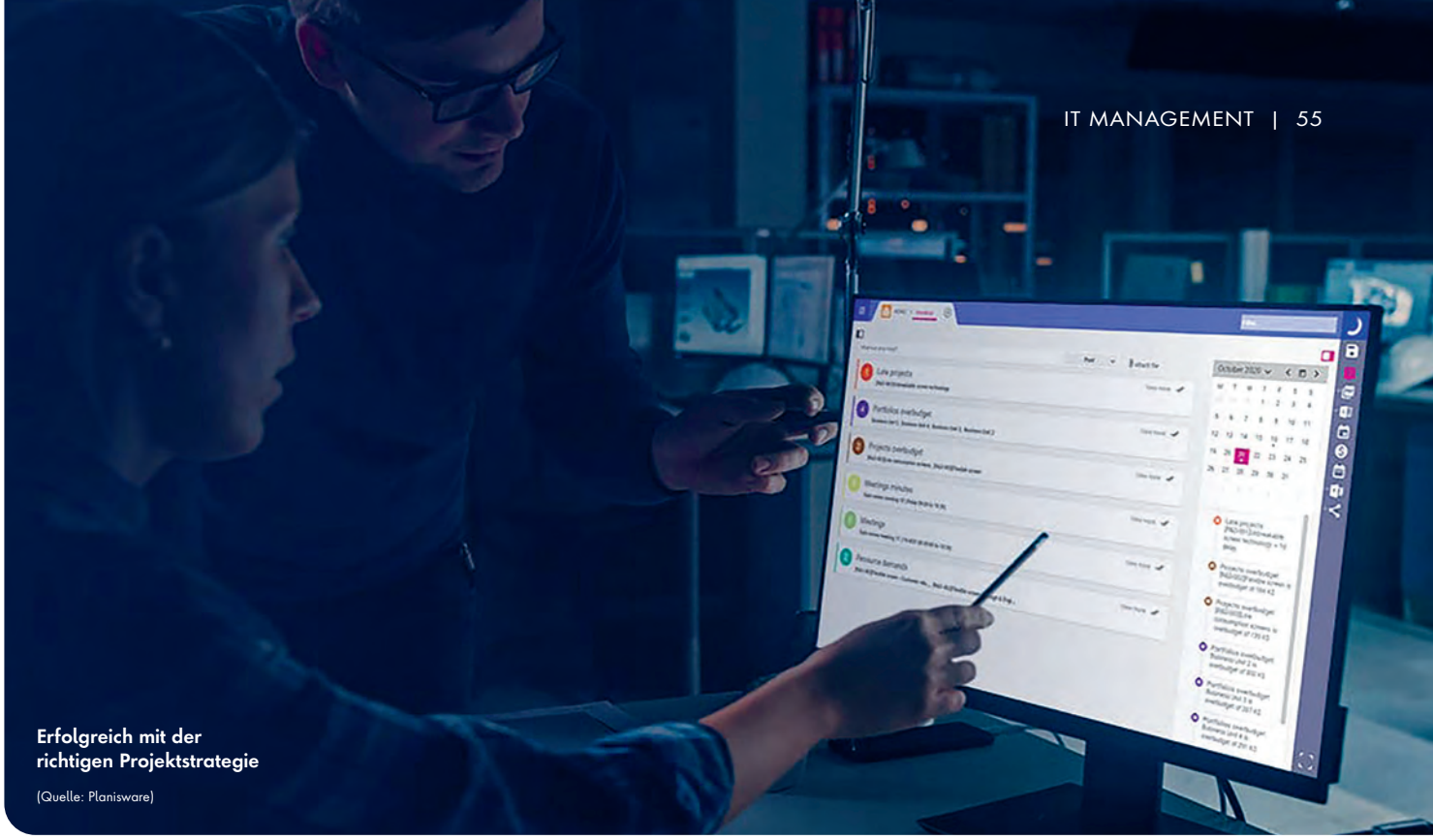
Der Nutzen von PPM-Lösungen besteht darin, dass Unternehmen ihre Entscheidungsprozesse beschleunigen und Projekte effizient umsetzen. Dies lässt sich erzielen, indem die PPM-Lösungen den Informationsfluss sowie die abteilungsübergreifende Zusammenarbeit in Projekten verbessern. Im PPM-Tool ist auch jederzeit der Status von verfügbaren Ressourcen abrufbar. Entlang der Kapazitäten und Termine kann dann durchgespielt und ermittelt werden, welche Projekte parallel abgearbeitet beziehungsweise synchronisiert werden können.

Mit Multiprojektmanagement ein Unternehmen digitalisieren

So steuert zum Beispiel Oase, ein internationaler Anbieter von Aquaristik, Springbrunnen und Teichzubehör, seine mehr als 100 Innovations- und Organisationsprojekte mit Orchestra. Für diese Lösung wurde OASE 2023 als „TOP 100-Innovator" im Mittelstand Deutschlands ausgezeichnet. Der Leiter Forschung und Entwicklung schätzt es sehr, dass sich die PPM-Lösung an den bestehenden Innovationsprozess der Oase GmbH anpassen ließ, so dass Meilensteine und Checklisten 1:1 übertragen werden konnten. Neben dem Überblick über Meilensteine und Projektfortschritte ermöglicht die Lösung auch einen systematischen Einblick

DER NUTZEN VON PPM-LÖSUNGEN BESTEHT DARIN, DASS UNTERNEHMEN IHRE ENTSCHEIDUNGSPROZESSE BESCHLEUNIGEN UND PROJEKTE EFFIZIENT UMSETZEN.

Gilles Chêne, CEO,
Planisware Deutschland GmbH,
www.planisware.com



Erfolgreich mit der richtigen Projektstrategie

(Quelle: Planisware)

in die Ressourcenauslastung. So können Engpässe erkannt werden und behoben werden. Im nächsten Schritt wird Oase dann die gesamte Wirtschaftlichkeit der Prozesse transparent darstellen können.

Effizienter Planen

Mitunter kann auch Wachstum Hindernisse auftürmen. Generell stehen alle Organisationen vor dem Problem, dass sie ihre Flexibilität und Agilität verlieren, wenn sie wachsen ohne ihre Managementpraktiken weiterentwickelt zu haben. Manche haben ein Rezept gefunden, wie etwa die Carl Zeiss Meditec AG. Laut Programm Manager Dr.-Ing. Martin Kelp war die Einführung von Planisware Orchestra im Unternehmen die richtige Entscheidung: „Die Software hilft uns die Herausforderungen, die mit einer schnell wachsenden Organisation einhergehen, zu meistern. Insbesondere unsere Produktentwicklungsprojekte und die eingesetzten Ressourcen lassen sich effizienter planen und verwalten."

Bewährte Praktiken als Einstiegshilfen

Erfahrungsgemäß sind mittelständische Firmen sehr fokussiert, an raschen Ergebnissen interessiert und auch kostenorientiert. Doch was die Einführung von PPM-Lösungen anbelangt, so haben Mittelständler sowie auch Behörden erfahrungsgemäß hierfür selbst zu wenig Zeit, Mitarbeiter und auch Know-how. Dies gilt sowohl für die Auswahl geeigneter PPM-Tools und deren Implementierung als auch den späteren Betrieb in Cloud-Infrastrukturen. Um Unsicherheiten zu vermeiden, lohnt es sich, dass Softwareanbieter mehr Unterstützung bei Prozessen und bei der Implementierung anbieten.

Daher hat Planisware einen effektiven Best-Practice-Ansatz entwickelt, der auf intensiven Anforderungs-Workshops mit einer anschließenden Testphase basiert. Die Best Practices werden dabei zusammen mit den Kunden im Rahmen von Feedback-Schleifen erarbeitet. Denn für mittelständische Firmen ist es entscheidend, möglichst praxisnah beurteilen zu können, dass die Lösung für sie geeignet ist. Während der Implementierungs-Workshops werden Kernanforderungen entwickelt, Benutzer angelegt und Schnittstellen definiert. Das Testsystem kann dann in einem Container in der ISO zertifizierten Planisware-Cloud mehrere Wochen genutzt werden. Während dieser Testphase werden zusätzliche Fragen geklärt, die sich durch die Nutzung des Testsystems ergeben. Diesen Prozess haben in den letzten Jahren alle Orchestra-Anwender durchlaufen.

Dadurch bleibt der durchschnittliche Implementierungszeitraum für Planisware Orchestra in einem Rahmen zwischen zehn bis 30 Beratungstagen durch das Professional Services Team – je nach Anforderungskatalog und gewünschten Anpassungen. Die Unternehmen profitieren schließlich mehrfach: Sie nutzen eine Cloud-Lösung mit kalkulierbaren Kosten, die den gesamten Projektlebenszyklus abbildet, eine hohe Anwenderakzeptanz aufweist und nach einer kurzen Implementierungsphase rasch Ergebnisse liefert.

Effektiver, effizienter und agiler

Zusätzlich zu beschleunigten Prozessen, einer höheren Transparenz und effektiveren Zusammenarbeit erzielen die Unternehmen weitere messbare Vorteile. So lassen sich zum Beispiel durch das Verwenden von Echtzeitdaten und die Automatisierung im Durchschnitt 50 Prozent der Zeit einsparen, die früher für das Erstellen von Berichten benötigt wurde. Außerdem steigern die Unternehmen ihre Projekteffizienz im Schnitt um 35 Prozent, weil sie Ressourcen, langfristige Kapazitäten, Finanzmittel und ihre Best Practices in Einklang gebracht haben. Darüber hinaus werden die Unternehmen durchschnittlich um 15 Prozent agiler, weil sie eben alle Beteiligten umfassend einbinden, sofern Anpassungen im Projektportfolio notwendig sind.

Gilles Chêne

Die richtigen Fragen stellen

PROJEKTE ZIELGERICHTET HINTERFRAGEN UND VERBESSERN

Fragen helfen generell, sich mit einem Thema auseinanderzusetzen und auch gegebenenfalls eine neue Sicht zu gewinnen. Entscheidend sind hier die „richtigen" Fragen, auf die es nicht komplett eine umfassende, fertige Antwort gibt. Weiterhin kommt es darauf an, wer diese Fragen stellt und welche Kompetenzen und Grundlagen dieser Personenkreis hat. Schlecht, aber auch gutlaufende Projekte können extrem davon profitieren.

Die richtigen Fragen in Projekten

Wenn Projekte nicht optimal laufen, ist es nicht immer leicht, die Ursachen zu finden und die Projekte zu optimieren. Wenn niemand erkennt, dass ein Projekt schlechter läuft als es sollte oder niemand die Rolle hat, dieses zu hinterfragen, ist das potenzielle Problem intransparent und die Lösung in weiter Ferne.

Projekte laufen über einen längeren Zeitraum. Die agierenden Personen verschmelzen oft mit dem Projekt und verlieren einen objektiven Blick.

Im Ergebnis sind Projekte in der Gefahr, mangels kritischer Auseinandersetzung oder fehlender Distanz in einen Abwärtsstrudel zu geraten. Das bedeutet höhere Kosten, verlängerte Laufzeiten und geringere Qualität. Die Motivation der Mitarbeiter, Kunden und weiterer Stakeholder sinkt und weitere Probleme werden erzeugt. In Summe kann dies zum kompletten Scheitern der Initiative führen

Die „richtigen Fragen" helfen, ein Projekt wieder in die richtige Bahn zu leiten und dort zu stabilisieren. Stellt diese Fragen niemand, besteht eine große Gefahr, den richtigen Weg nicht zu finden oder ihn unterwegs zu verlassen, ohne dass die entscheidenden Personen dies merken und gegensteuern können.

Fehlender Abstand und Objektivität

Betriebsblindheit ist ein gern genutzter Ausdruck um zu beschreiben, dass involvierte Personen den rationalen Blick auf die Projekt- oder Betriebssituation ganz oder teilweise verlieren. Was steckt eigentlich dahinter beziehungsweise wie ist es möglich, zu einem gewinnbringenderen Blick zu kommen?

Macht ein Mitarbeiter über einen längeren Zeitraum eine ähnliche Tätigkeit oder ein Manager bekommt ähnliche Informationen und Entscheidungsvorlagen, kann ein Gewöhnungseffekt eintreten, der die Sicht auf Alternativen verschließt. Dies wird verschärft, wenn der Personenkreis dies zusätzlich länger innerhalb eines Unternehmensumfelds oder in einem vergleichbaren Umfeld tut.

Beispielhafte Situationen aus der Praxis und beispielhafte Fragen

➤ **Projektstatus**

Fragen über den Lebenszyklus eines Projektes können durch den bisherigen Ablauf eine Prognose auf die zukünftige Entwicklung ermöglichen beziehungsweise Ansätze für eine Optimierung aufzeigen.

Aussage: „Das Projekt läuft schlecht"

Beispielhafte Fragen:

- Gibt es eine fundierte Analyse, die über individuelle Gefühlslagen hinausgeht, was „schlecht läuft" und die Gründe dafür?
- Gibt es regelmäßige Retros und Verbesserungen?
- Hat der Projektleiter die notwendigen Kompetenzen für die Aufgabe?

Das Gefühl, dass Projekte „schlecht" laufen, kann bei unterschiedlichen Stakeholdern auf unterschiedlichen Basiserwartungen begründet sein. Ein Gefühl kann ein Indikator sein, sollte aber nicht die alleinige Grundlage für Entscheidungen darstellen. Für letzteres ist eine fundierte Faktenlage entscheidend.

Fazit: Schlecht laufende Projekte können auf sehr unterschiedlichen Gründen basieren. Dies zu ermitteln bedeutet, mit den richtigen Fragen die Problemstellung zu erörtern.

ALS FAZIT KANN MAN SAGEN, NICHT DER DER DAS UMFELD KENNT, IST OFT DER OPTIMALE FRAGESTELLER, SONDERN DER, DER DAS UMFELD NICHT KENNT.

Martin Besemann, Berater und zertifizierter Projektmanager (PMP, Prince2 Practitioner/ Agile, Senior Project Manager IPMA Level B), www.conpromas.de

Projektmethodik

Die Projektmethodik nimmt entscheidenden, aber oft unterschätzen Einfluss auf das Projekt. Dies kann von einer deutlichen Verteuerung bis zum Scheitern des Projektes führen.

Aussage: „Die Projektvorgehensweise ist Standard im Haus“

Beispielhafte Fragen:

- Gibt es eine Methode gemäß anerkannten Standards oder ist das Vorgehen eher „Freestyle“?
- Passt die Methode wirklich zu dem individuellen Projekt?
- Verstehen alle Beteiligten die Methode?

Ein Projekt, nur um einem vermeintlichen internen Standard zu genügen, mit einer nicht passenden Methode durchzuführen, ist genauso ein grundlegendes Problem wie gar keine professionelle Methodik anzuwenden. Es ist vergleichbar mit einer unpassenden Taktik für eine Fußballmannschaft. Das wird weder auf dem Spielfeld (Projektteilnehmer) noch auf den Rängen (Stakeholder) zu einem Erfolg werden.

Fazit: Die richtige Methode lässt sich nur mit dem Hinterfragen des Projektinhalts, der Ziele und des Umfelds finden.

Auftragsklarheit

Wenn die Auftragsdefinition nicht für alle Beteiligten transparent ist, nicht auf aktuellem Stand oder nie final abgestimmt ist, ist die Gefahr von teuren Missverständnissen erheblich.

Aussage: „Die Anforderung ist doch klar“

Beispielhafte Fragen:

- Was heißt klar genau?
- Ist dies wirklich allen Beteiligten gleich „klar“?
- Ist der Stand der Klarheit aktuell, vollständig, dokumentiert und abgenommen?

Die Anforderung ist in der Praxis zumeist nicht für alle involvierten Personen gleich „klar“. Hier gibt es neben unterschiedlichen Bedürfnissen und Meinungen auch unterschiedliche Interessen und Lösungsansätze. Hinzu kommen wirtschaftliche Aspekte auf der Ein-

AUS WELCHER PERSPEKTIVE SOLLTEN FRAGEN GESTELLT WERDEN?

	Projektintern	Außenstehender
Vorteile	• Erfahrung im Projekt • Tieferes Wissen um Inhalte	• Unabhängigkeit vom Umfeld • Unvoreingenommener Blick • Vergleichsmöglichkeiten mit anderen Umfeldern
Nachteile	• Abhängigkeit zum Arbeitgeber • Hierarchien • Kein unvoreingenommener Blick • Ggf. reduzierte Vergleichsmöglichkeiten	• Reduziertes Wissen um betreffendes Projekt

NICHT DER DAS UMFELD KENNT, IST OFT DER BESSERE FRAGENSTELLER, SONDERN DER, DER DAS UMFELD NICHT KENNT.

nahme- und Ausgabeseite, die einer ganzheitlichen Klärung bedürfen. Hier würde sich zum Beispiel eine unabhängig voneinander durchgeführte Umfrage zu Auftrag und Lösung im Projekt- und Stakeholderkreis anbieten. Die Ergebnisse könnten verwundern.

Fazit: Wenn niemand hinterfragt, wie Stakeholder den Projektauftrag verstehen, wird es mit hoher Wahrscheinlichkeit zu unterschiedlichen Sichten kommen.

➤ Projekteilnehmer

Die handelnden Personen und notwendigen Kenntnisse und Fähigkeiten entscheiden über den Erfolg des Projektes.

Aussage: „Die Mitarbeiter sind seit Jahren im Umfeld tätig und dadurch die vorhandenen und richtigen Ressourcen"

Beispielhafte Fragen:

- Gibt es (noch) die notwendige Distanz zum Projektinhalt?
- Hat der Projektleiter die notwendigen Skills und Kompetenzen zur Steuerung des Projektes?
- Hat das Management die richtigen internen oder externen Berater, um unter Beachtung ihrer zeitlichen Verfügbarkeit projektspezifisch zu entscheiden?

Eine eingefahrene Sicht, die sogenannte „Betriebsblindheit", oder auch das Drängen zu Tätigkeiten, die ein Mitarbeiter nicht ausführen kann oder möchte, kann zum Scheitern, zumindest aber zu Ineffizienz des Projektes führen.

Oft kann eine Innovation von außerhalb des Standardteams frischen Wind und Erkenntnisse in das Projekt bringen. Das liegt zum Beispiel an der Distanz zum Projekt, einer neuen Sicht oder auch der Erfahrung aus anderen Projekten. Wichtig ist vor allem die Unabhängigkeit. Das zeigt sich gerade beim Projektleiter. Unpopuläre Entscheidungen, für die die Person später in der Linie Konsequenzen befürchten muss, werden schwerer fallen als bei eigener Unabhängigkeit und Distanz zu Linienorganisation und dem Projekt.

Fazit: Die regelmäßige Sicherstellung einer rationalen Projektbetrachtung wird durch unabhängige Außenstehende gestützt.

Die richtigen Fragen stellen

Eine Frage führt zum Überdenken der Situation. Das Ergebnis ist entweder eine Bestätigung des aktuellen Zustands oder die Erkenntnis, dass eine Änderung des aktuellen Zustands notwendig ist. Das ist im Ergebnis ähnlich einem Audit, beziehungsweise einer Vorstufe dazu.

Im ersten Fall bedeutet dies eine Bestätigung des aktuellen Vorgehens. Daraus folgt einerseits die Sicherheit auf dem richtigen Weg zu sein und andererseits eine seriöse Situationsanalyse, um potenzielle Probleme zu reduzieren.

Im zweiten Fall eröffnet sich die Chance, den aktuellen Zustand zu ändern und damit die zukünftigen Ergebnisse inhaltlich, wirtschaftlich und zeitlich zu optimieren. Weiterhin kann man dadurch sogar ein Projekt insgesamt wieder auf den richtigen Weg zu führen.

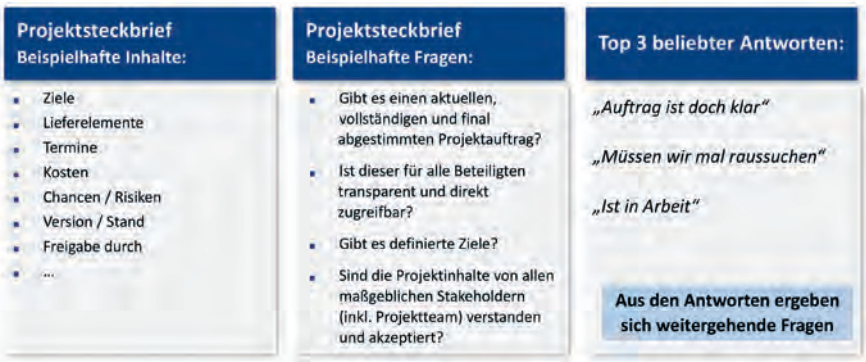
Die Genehmigung, die richtigen Fragen zu stellen

Bei aller Offenheit und auch in Methoden beschriebenen Vorgehensweisen ist eine „Genehmigung" sinnvoll oder gar notwendig, dass Fragen gestellt werden dürfen und das Ergebnis akzeptiert oder zumindest zur Kenntnis genommen wird.

Fragen können Antworten bringen, die unangenehme Ergebnisse offenbaren oder politisch nicht immer verträglich sind. Das bringt mit sich, dass nicht jeder sich berufen fühlt, diese Fragen offen zu stellen. An dieser Stelle ist es wichtig, die Fragen zuzulassen und gegebenenfalls einen Rahmen und eine Empfängergruppe für die Ergebnisse zu definieren. Dies hilft, die Angst zu überwinden, Fragen zu stellen, die Antworten erzeugen können, die nicht immer populär oder gewünscht sind.

An dieser Stelle kann die Position des Fragestellenden von entscheidender Bedeutung für das Ergebnis sein.

ERSTE STATUSBESTIMMUNG AM BEISPIEL PROJEKTSTECKBRIEF/AUFTRAG



DER PROJEKTSTECKBRIEF IST EIN SCHEINBAR KLARER UND SELBSTVERSTÄNDLICHER TEIL DER PROJEKTPLANUNG. EINE ABSTIMMUNG KANN VIELE UNKLARHEITEN UND MISSVERSTÄNDNISSE AUFZEIGEN UND BESEITIGEN.

Wer kann die notwendigen Fragen stellen?
Beschäftigt sich die betreffende Person länger mit dem Umfeld, besteht wahrscheinlich ein tiefer Einblick und es gibt viele Erklärungen, warum etwas in einem gewissen Schema läuft.

Das kann einen Vorteil mit sich bringen, aber auch Nachteile. Vorteil ist die Erfahrung im Umfeld und damit einhergehende tiefere Kenntnisse.

Betrachtet man dieses Szenario, ergibt sich die Frage, warum ist noch keine Änderung der Situation herbeigeführt, wenn die Person ausreichend Erkenntnisse hat? Fehlt die entscheidende Erkenntnis oder die Möglichkeit, das Gehör und die zugehörige Handlungsbereitschaft bei der zuständigen Managementebene zu erzeugen?

WEITERE BEISPIELFRAGEN

Ein paar Fragen als Denkanstoß

- Wer leitet Projkete tatsächlich? Ein Fachexperte oder ein ausgebildeter Projektmanager?
- Welche Ressourcen stellen Lieferanten/Partner zum Beispiel in IT-Projekten?
- Wer ist (intern) Ansprechpartner für Projektmanagement für das Management?
- Wer (extern) berät Management und Lenkungsausschüsse in Projekten?
- Wie ist das Ansehen von Projektmanagement allgemein und wie sind Projektmanager in der Hierarchie angesiedelt?
- Wird eher eine günsitge „Lösung" für Projektmanagement bevorzugt?

Die Fragen und die Beantwortung sind nicht als repräsentativ oder generell zu sehen, sondern als Anregung. Projekte sind wie Menschen verschieden.

Nicht der oder die, die immer davorstehen, sondern jemand mit genereller Fachkenntnis im Projektmanagement und Abstand zum Umfeld bieten sich alternativ an. Dieses weitere Szenario wäre damit eine Entfernung von Umfeld. Im ersten Schritt optional unternehmensintern und im weiteren Schritt unternehmensextern.

Je größer die Unabhängigkeit zum Umfeld, desto größer auch die Unabhängigkeit für Fragen und Ergebnisse und damit die Glaubwürdigkeit. Weiterhin wird in der Praxis auch häufig die Möglichkeit zur Platzierung der Erkenntnisse und die Bereitschaft im Management, sich mit den Ergebnissen zu befassen, durch externe Fachexperten größer. Das liegt schlicht an der Vorstellung, dass jemand der stetig viele verschiedene Umfelder betrachtet, große Erfahrung hat und einen hohen Mehrwert erzeugen kann.

Notwendige Grundlagen für die richtigen Fragen
Die Notwendigkeit, inhaltliches Fachwissen zu besitzen ist erst einmal sekundär. Im ersten Schritt geht es darum, die Situation des Projektmanagements zu erkennen. Auch ein inhaltlich nicht Involvierter sollte das Projekt schnell generisch überblicken. Für die Beurteilung der fachlichen Objekte können in einem strukturierten Umfeld Subject Matter Experts (SME's) eingebunden werden.

Als Ergänzung sei erwähnt, wenn jemand in seiner Laufbahn drei Unternehmen und zugehörige Projekte gesehen hat, ist dies ein Unterschied zu einer Person, die durch ihre Tätigkeit in 20,30 oder mehr Unternehmen in Projekte eingebunden war. Nicht nur erfolgreiche Projekte sind hier wichtig, sondern auch gerade Projekte, die nicht optimal laufen erweitern den Erfahrungsschatz.

Als Fazit kann man sagen, nicht der der das Umfeld kennt, ist oft der optimale Fragesteller, sondern der, der das Umfeld nicht kennt.

Die persönlichen Kenntnisse und Skills des Fragestellers sind eine erfolgskritische Basis. Neben einer breiten praktisch geprägten Sicht ist eine methodische Grundlage notwendig. Um zu beurteilen, welche Projektmethodik passt oder nicht passt, muss das übergreifende Wissen vorhanden sein.

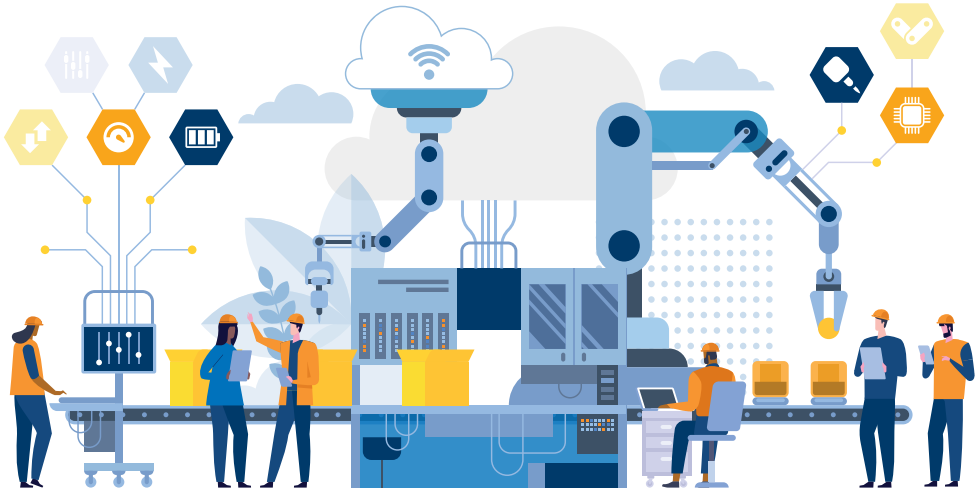
Zur Fragestellung gehört auch die Überzeugungskraft, eine Verbesserung im Fokus zu haben und nicht eine Schuldzuweisung für eventuelle Missstände.

Das Potenzial zum Aufzeigen von Verbesserungsvarianten stellt gegenüber dem reinen Darstellen von Defiziten eine wertvolle Ergänzung dar und kann den Prozess der Optimierung unterstützen.

Projektmanager tun gut daran, verschiedene Unternehmen und Projektumfelder kennenzulernen, bevor sie „sesshaft" werden. Dies bringt sowohl der eigenen Persönlichkeit wie auch dem Unternehmen einen Vorteil. Als externer Berater und Projektmanager sieht man viele verschiedene Projektumfelder. Dies baut einen umfangreichen Wissensschatz auf.

Hier wächst auch die Erkenntnis, dass viele und auch sehr unterschiedliche Projekte von einer geübten Fragestellung profitieren können. Dies geschieht am besten von unabhängiger Seite mit der notwendigen Distanz.

Martin Besemann



Die Zukunft der Automatisierung

FÜNF PRAKTISCHE ANWENDUNGEN VON KI

Sowohl KI als auch Automatisierung verändern, wie wir heute arbeiten. Wenn diese beiden Technologien zusammen eingesetzt werden, können sie unsere Produktivität erhöhen und bestehende Geschäftsprozesse effizienter machen. Der Fokus der Medien lag in letzter Zeit vor allem auf generativen KI-Anwendungen wie ChatGPT, aber in der Automatisierung gibt es viele andere praktische KI-gestützte Anwendungen, die sowohl die interne Produktivität als auch das Kundenerlebnis verbessern können.

DIE GENERATIVE KI KANN EINE WICHTIGE ROLLE BEI DER AUTOMATISIERUNG BESTIMMTER MENSCHLICHER AUFGABEN SPIELEN.

Jakob Freund, CEO, Camunda, www.camunda.com

Diese Technologien lassen sich in drei allgemeine Wirkungsbereiche einteilen: generative, prädiktive und erweiterte Intelligenz.

- **Generativ:** Generative KI-Algorithmen können verwendet werden, um auf Basis von Trainingsdaten neue Inhalte zu erstellen oder Code zu generieren.
- **Prädiktiv:** Teams können prädiktive KI-Algorithmen zur Entscheidungsfindung einsetzen, oder um Prozesse auf der Grundlage früherer Ergebnisse zu verbessern.
- **Erweiterte Intelligenz:** Diese Art von KI kann dazu beitragen, Entscheidungen (die normalerweise von Menschen getroffen werden) zu beschleunigen. Dadurch kann die Prozesseffizienz erhöht werden.

Werfen wir also einen Blick auf fünf praktische Anwendungsfälle von KI, die sich in diese drei Kategorien einteilen lassen, und darauf, wie sie die Automatisierung in Unternehmen verbessern können.

Kontinuierliche Prozessoptimierung

Durch die Kombination von Prozessorchestrierung und künstlicher Intelligenz können End-to-End-Prozesse verbessert werden. Ein System zur Prozessorchestrierung sammelt beispielsweise Daten zur Prozessausführung und -leistung über eine Vielzahl von Endpunkten hinweg (etwa über Menschen, Systeme und Geräte, die an einem Prozess beteiligt sind). Diese Daten können in ein prädiktives KI-Modell eingespeist werden, um auf der Grundlage der vergangenen Leistung ähnlicher Prozesse vorherzusagen, wie bestimmte Prozesse ablaufen werden, wie lange sie dauern oder welche Ergebnisse sie liefern werden.

Durch die neuen Modelle der erweiterten Intelligenz ist der heilige Gral der sich selbst verbessernden Prozesse nicht mehr weit entfernt. Diese Technologie könnte Engpässe in Prozessen erkennen, Verbesserungsvorschläge machen und Modelle nach einer Prüfung durch einen Menschen oder sogar völlig autonom aktualisieren.

Generierung von Prozessprüfungsdaten

Eine äußerst nützliche Anwendung generativer KI ist die Erstellung von Prozessprüfungsdaten. In Formularen gibt es beispielsweise viele Möglichkeiten für typisch menschliche Fehler – man denke nur an die verschiedenen Möglichkeiten, ein Datum zu schreiben (1.15.23 vs. 15.1.23 vs. 15. Januar 2023). Basierend auf früherem menschlichem Verhalten könnte das System Tests generieren, um zu prüfen, was ein Formular fehlerhaft

macht, wie etwa falsche numerische Felder oder eine Überschreitung der Zeichenbegrenzungen.

Schnellere Entscheidungsfindung

Viele Unternehmen nutzen Automatisierung bereits zur schnelleren Entscheidungsfindung, zum Beispiel bei der Annahme oder Ablehnung eines Hypothekenantrags auf Grundlage der Kreditwürdigkeit und des wahrgenommenen Risikoprofils der oder des Antragstellenden. Prädiktive KI kann zusammen mit Entscheidungsmodellen eingesetzt werden, um einige Entscheidungen schneller zu fällen. Ein Beispiel dafür liegt in der Betrugsprävention: Hier könnten durch prädiktive KI Betrugsfälle auf Grundlage früherer Nutzerdaten vorhergesagt werden. Unternehmen mit einem höheren KI-Reifegrad können für maschinelles Lernen geeignete Datensätze aus einem Prozessorchestrierungssystem in Kombination mit anderen internen Datensätzen nutzen, um Muster vorherzusagen und sinnvolle Entscheidungen abzuleiten.

Automatisierung menschlicher Aufgaben

Die generative KI kann eine wichtige Rolle bei der Automatisierung bestimmter menschlicher Aufgaben spielen. Nehmen wir zum Beispiel einen Marktplatz, der Bewerbungen für neue Händler bearbeiten möchte. Mithilfe der ChatGPT-API, die in ein Prozessmodell integriert ist, kann der Markt automatisch relevante Informationen aus Formularen extrahieren, um eine Zusage oder Absage zu generieren. Anschließend kann ChatGPT automatisch entsprechende E-Mails an die Händler generieren und direkt auch Produktbeschreibungen der Händler mit Zusage für die Website des Marktes erstellen.

Entwicklung von Prozessmodellen

Software-Architekten oder Entwickler, die den Code für Prozessmodelle schreiben, können ebenfalls von generativer KI profitieren. Teams können mit Code-Generatoren experimentieren (GitHub Copilot), um ein Prozessmodell zu entwickeln und zu codieren, das auf früheren Modellen des Unternehmens basiert. Anstatt bei Null anzufangen, können diese Technologien dazu beitragen, die knappen Entwicklungsressourcen optimal zu nutzen und den Automatisierungsgrad im gesamten Unternehmen zu erhöhen.

Inzwischen gibt es viele Begriffe, um den optimierten Einsatz von KI in Kombination mit anderen Automatisierungstechnologien zu erklären. Letztlich kann die Prozessorchestrierung als effektiver Ausgangspunkt für den Einsatz von KI und Automatisierung dienen, indem sie sicherstellt, dass die verschiedenen Endpunkte eines Prozesses, die Komponenten der Hyperautomatisierung und des Business Stacks aufeinander abgestimmt sind. Das ultimative Ziel ist ein effizienter, optimierter End-to-End-Prozess, der sowohl das Mitarbeitererlebnis als auch die kundenorientierten Anwendungen verbessert. Dieses Ziel ist in greifbare Nähe gerückt, seit Unternehmen beim Thema Prozessorchestrierung und KI einen Gang zulegen.

Jakob Freund

Was ist die CRM-Strategie?

EIN WEG AUS DER HÖLLE DES MITTELMASSES!

Mittlerweile hat sich die Erkenntnis durchgesetzt, dass für die Entwicklung einer jeden CRM-Strategie der Fokus weg vom Unternehmen hin auf die Bedürfnisse der Kunden gelenkt werden muss. Aber wie? Vielen Unternehmern fehlt die Anleitung für die Entwicklung der CRM-Strategie. Oft sind die Erwartungen der Kunden weder bekannt noch erhoben.

Währenddessen steht jedes Unternehmen immer wieder mit seinen Kunden in Kontakt: informiert über neue Produkte, berät vor Ort etc. Das Wissen über die Kunden verteilt sich auf Einzelpersonen, verschiedene Kundenkontaktpunkte und Abteilungen. Werden quer durch das Unternehmen alle Erkenntnisse zusammengetragen und harmonisiert, ergibt sich ein erstes Bild. Doch dazu später mehr.

Die Grundidee von CRM

Die CRM-Strategie bezeichnet ein Konzept, das darauf abzielt, die Beziehungen zwischen Unternehmen und Kunden zu optimieren. Verschiedene Maßnahmen, die auf die Bedürfnisse und Wünsche der Kunden ausgerichtet sind, sollen langfristige Kundenbeziehungen aufbauen und pflegen. Ziel einer CRM-Strategie ist es, die Kundenzufriedenheit zu steigern, Kundenbindung zu fördern und letztlich den Unternehmenserfolg zu steigern. Eine gut durchdachte und umgesetzte CRM-Strategie kann Firmen helfen, sich von der Konkurrenz abzuheben und eine starke Marktposition zu erlangen.

Die Grundidee der CRM-Strategie lässt sich am einfachsten anhand von zwei Quadraten erklären. Jede Kundenbeziehung hat einen Anfang und ein Ende. Das erste Quadrat zeigt auf der Zeitachse die durchschnittliche Dauer und auf der Margenachse wird die mittlere Umsatzrendite dargestellt. Die Fläche des Quadrates ergibt den Gesamtgewinn aus einer Kundenbeziehung. Das zweite Quadrat folgt der kundenzentrierten Strategie. Es zeigt eine längere Beziehungsdauer und höhere Profitabilität. Beides ist das Resultat der hohen Kundenzufriedenheit. Zufriedene Kunden bleiben länger und akzeptieren einen höheren Preis. Der Erfolg der CRM-Strategie lässt sich über den Gesamtgewinn pro Kunde messen.

CRM und der Wettbewerb

Die beiden Quadrate illustrieren eindrucksvoll das Ziel der CRM-Strategie: rentable und langfristige Kundenbeziehungen. Auslöser für eine kundenzentrierte Unternehmensstrategie ist der steigende Wettbewerb. Je mehr Lieferanten, desto schneller wechseln Kunden. Umso wichtiger wird die CRM-Strategie.

Dem US-amerikanischen Ökonom Michael E. Porter zufolge gibt es zwei strategische Richtungen, um in einem engen Markt zu bestehen: die Preisführerschaft oder die Qualitätsführerschaft. Interessanterweise sind beide Richtungen CRM-Strategien. Ryan Air ist Preisführer bei den Billig-Airlines und verspricht seinen Kunden zum Beispiel einen Flug für neun Euro nach Barcelona. Das ist ein unverschämt günstiges Angebot und bindet alle preissensiblen Kunden. Die CRM-Strategie liegt hierbei in dem Versprechen, immer und überall der günstigste Anbieter zu sein.

Sofern ein Unternehmen nicht über den Preis verkaufen will oder kann, wird die kundenzentrierte Unternehmensstrategie obligatorisch. Neben den primären Erfolgsfaktoren (Produkt, Preis) werden sekundäre Erfolgsfaktoren (Beratung, Services, Innovationen und Image) konsequent aus-

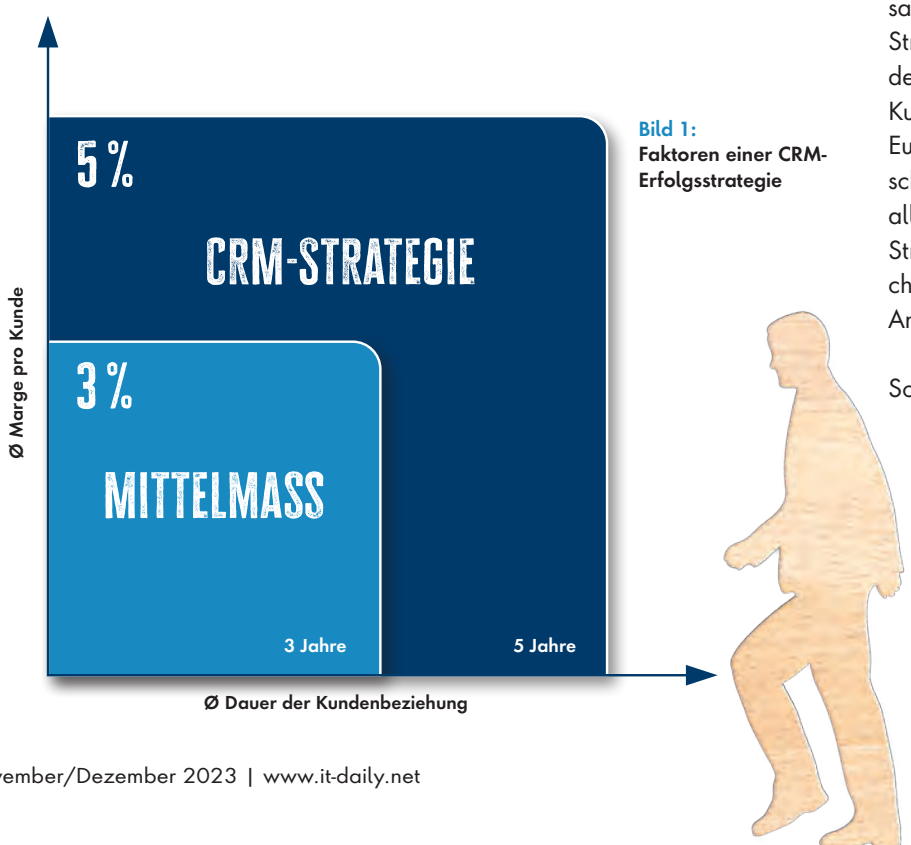


Bild 1: Faktoren einer CRM-Erfolgsstrategie

gebaut. Der Kunde kauft kein Produkt, sondern eine auf seine Bedürfnisse zugeschnittene Lösung. Durch positive Erfahrungen erwächst das Vertrauen, aus Vertrauen entsteht Loyalität und am Ende steht der Qualitätsführer, eine starke Marke.

Die Qualitätsfaktoren

Der Clou liegt darin, in den für den Kunden wichtigen Qualitätsfaktoren der Beste zu sein. Mit steigenden Preisen wachsen die Erwartungen der Kunden und es wird zwingend erforderlich, der Beste in seiner Kategorie zu sein. Betrachten wir ein griffiges Beispiel: Der Geschäftsreisende wird für seine Übernachtung, das aus seiner Sicht beste Hotel im Rahmen seines Budgets wählen. Die Auswahlfaktoren können vielfältig sein: der Parkplatz, das Restaurant, die Zimmer oder der Wirt. Sofern das beste Hotel am Platz verfügbar ist, wird er nicht das zweitbeste Hotel buchen. Aus dem Blickwinkel des Kunden wird deutlich, warum das zweitbeste Hotel weniger gebucht wird, das drittbeste Hotel noch überlebt und das Vierte bereits geschlossen hat. Andere Geschäftsreisende haben andere Präferenzen, aber in der Regel mögen alle ein großes Zimmer, gutes Essen und einen freundlichen Wirt.

Nach Michael E. Porter gibt es nur zwei Gewinner im Markt: den Günstigsten und den Besten. Alle anderen Hotels haben ein strategisches Problem. Sie offerieren ein Angebot, das weder attraktiv noch günstig ist. Es nennt sich das Stuck-in-the-Middle-Phänomen. Eine CRM-Strategie kann aus dieser Hölle des Mittelmaßes führen.

Strategieentwicklung

Für das Customer Relationship Management gibt es in der Literatur und im Internet viele gut gemeinte Ratschläge: Gehen Sie auf den Kunden ein, seien Sie die erste Wahl, schaffen Sie Erlebnisse! Doch niemand, nicht einmal ein CRM-Systemanbieter, kann Ihnen substanziell erklären, wie Sie eine erfolgreiche Strategie definieren. Deshalb entscheiden sich Projektleiter, die die Strategie über die Einführung eines Systems stellen, oft für professionelle Unterstützung im Entwicklungsprozess.

In unserer Beratung zeigt sich, dass die Werte des Gründers und Geschäftsführers einen hohen Einfluss auf die Unternehmenskultur ausstrahlen. Erfährt der Kunde vom Top-Management die erforderliche Wertschätzung, ist das Unternehmen für eine CRM-Strategie prädestiniert.

Andererseits geht es bei der CRM-Strategie darum, für die vom Kunden gefor-

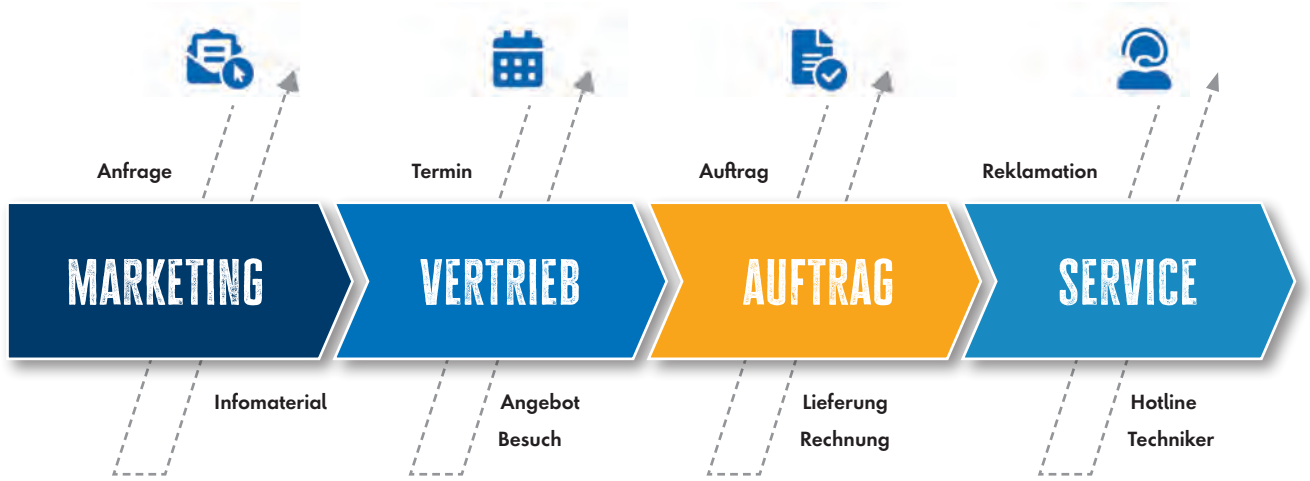


Bild 2: Zeitstrahl des Kundenlebenszykluses

derten Qualitätsindikatoren eine Organisationsstruktur aufzubauen, die schnell, einfach und effizient reagieren kann. Am Ende muss das neue Kundenversprechen in dem Unternehmen verankert und durch standardisierte Prozesse unterstützt werden.

#1 Fokus auf die Kunden

Früher nutzten Unternehmen – aufgrund ihrer archaischen IT – häufig das One-Face-to-the-Customer-Prinzip. Dabei handelt es sich um eine Organisationsform, bei der jeder Kunde individuell von einem zugeordneten Mitarbeiter betreut wird. Zeitweilig liebten alle Beteiligten die persönliche Betreuung, aber am Ende war die Kommunikation intransparent, langsam und teuer.

Heute nutzen Kunden verschiedenste Kontaktpunkte zum Unternehmen und die vielfältigsten Medien. Die Digitalisierung verstärkt den Effekt, da der Kunde sowohl analog (E-Mail, Telefon, Besuch, Teams) als auch digital (Kunden- Händler-, Serviceportal) kommuniziert. Die Vielfalt der Interaktionen ist gestiegen und es gilt, sie systemisch zu orchestrieren.

Nur mit einer modernen IT-Infrastruktur und entsprechenden Prozessen haben Mitarbeiter im Kundenkontakt die Möglichkeit, alle relevanten Informationen zum jeweiligen Kunden und seinen Vorgängen in einer 360-Grad-Sicht zu erkennen. Der Kundenbetreuer kann jederzeit und von überall den Datensatz zum Kunden öffnen, neue Vorgänge anlegen oder offene Vorgänge bearbeiten. Um den Kunden professionell zu betreuen, werden gezielt Kundenkontaktpunkte geschaffen, die seinem Anliegen bestmöglich entsprechen (Beratung, Auftrag, Störung).

Für die Planung der CRM-Strategie bedeutet dies, dass Kundenbeziehungen in verschiedenen Perspektiven durchleuchtet werden sollten. Als Erstes zeichnen wir den Kundenlebenszyklus anhand einer typischen Anfrage oder eines Auftrags. Danach untersuchen wir die besonderen Bedürfnisse für Neu-, Bestands- und Potenzialkunden. Letztlich braucht es eine Einteilung der möglichen Vertriebsinstrumente nach Kundenwert.

#2 Kundenlebenszyklus zeichnen

Setzen sich Mitarbeiter aus den kundennahen Bereichen (Marketing, Vertrieb, Service etc.) zusammen, entsteht die 360°-Kundenbeziehung. Der Lebenszyklus beginnt beim ersten Kontakt, der Beratung, führt über das Angebot und den Auftrag bis hin zu Serviceleistungen wie Installation, Schulung sowie Reparatur nach dem Kauf. Jeder Mitarbeiter bringt seinen Teil der Kundenbeziehung ein und hilft uns, den Kundenlebenszyklus zu vervollständigen. Es entsteht ein Zeitstrahl, der die gesamte Interaktion mit dem Kunden darstellt.

Nun gilt es, die Interaktion an jedem einzelnen Kontaktpunkt gezielt zu hinterfragen. Die Methode heißt „Walk in the Shoes of your Customer". Dabei ist es erforderlich, die Perspektiven der Kunden einzunehmen, ihre Situationen und Erwartungen zu analysieren und auch die Prozesse zu durchleuchten. Zu den Prozessen auf Kundenseite zählen zum Beispiel die Lieferantensuche, die Informationsbeschaffung, die Kaufentscheidung oder die Auswirkung einer Störung.

Ist der Kundenlebenszyklus gezeichnet, sind die Kundenkontaktpunkte definiert und die Interaktionen bekannt, werden die dahinterliegenden Arbeitsplätze betrachtet. Interessant ist hier die Performance in Bezug auf Qualität, Reaktionszeit und Aufwand. Durch die Arbeitsplatzanalyse bekommt der Berater einen guten Einblick in die gelebten Prozesse, die Fähigkeiten der Mitarbeiter und die Unterstützung

durch die IT-Systeme. An jedem Kundenkontaktpunkt beurteilt der Kunde bewusst oder unbewusst die erbrachte Leistung. Aus der Summe der einzelnen Interaktionen entsteht die Gesamtzufriedenheit.

Jeder Kontaktpunkt ist wichtig, denn ein negatives Erlebnis erzählt der Kunde zehnmal und ein positives dreimal weiter. In den meisten CRM-Strategien geht es vorrangig darum, eine durchgängig professionelle Leistung zu etablieren, anstatt ein ausgefallenes Kundenerlebnis (Customer Experience) zu kreieren.

#3 Kundenversprechen formulieren

Durch die Analyse werden Schwachstellen aufgedeckt, welche durch Zahlen verifiziert werden können. Eine schlechte Website senkt die Neukundenquote, eine schlechte Beratung oder minderwertige Angebote reduzieren die Auftragsquote und ein Ersatzteil, welches nicht lieferbar ist, vermindert die Wiederkaufquote. Alles hängt miteinander zusammen und der Kundenlebenszyklus hilft, die Schwachstellen gezielt zu adressieren.

Jetzt kommt der spannende Teil, denn es geht darum, für Kunden an den wichtigen Interaktionspunkten ein Versprechen zu formulieren: Wir wollen im Web leicht zu finden sein und die Kunden einfach, aber umfassend informieren. Wir wollen unsere Angebote aufwerten, damit Kunden sie verstehen. Wir bieten allen einen 24-h-Ersatzteilservice.

Die Methode zur Definition der Kundenversprechen wird unter dem Motto „Pain und Gain" charakterisiert. Es geht darum, den Kunden eine Qual zu nehmen oder eine geforderte Stärke nochmals auszubauen. Kundenversprechen können ebenfalls Leistungen beschreiben, die heute noch nicht verfügbar sind, zum Beispiel Werksführungen, Referenzbesuche, Schulungen etc.

Zusätzlich versehen wir bei der Entwicklung der Kundenversprechen unsere Leitaussagen mit einer Nutzenargumentation. Das hilft der internen Kommunikation und motiviert uns in unserem Handeln. Natürlich werden alle Kundenversprechen geprüft, korrigiert und verbessert. Nach einem Realitätscheck beginnt die Priorisierung nach Aufwand und Wirkung.

#4 Maßnahmen umsetzen

Die Umsetzung der CRM-Strategie ist ein fortlaufender Prozess. Aus der Priorisierung des Verbesserungspotenzials können jetzt dezidierte Projekte mit Auftrag, Zeithorizont und Ressourcen initiiert werden, welche zum Ziel haben, die Kundenbeziehung sukzessive zu verbessern. Einige Projekte werden den Ausbau der IT-Infrastruktur zur Folge haben und bedeuten größeren Aufwand.

Der unternehmerische Erfolg stellt sich ein, wenn Prozesse, Mitarbeiter, Führung und die IT aufeinander abgestimmt sind. Die Prozesse müssen einfacher, flexibler und effizienter werden und eine kontinuierlich hohe Qualität bei jeder Interaktion sicherstellen.

DIE CRM-STRATEGIE WIRKT IN ZWEI RICHTUNGEN: SIE HEBT DIE QUALITÄT FÜR DEN KUNDEN UND SENKT DIE KOSTEN DURCH PRÄZISION.

Stephan Bauriedel, Unternehmensberatung Stephan Bauriedel, www.erfolg-mit-crm.de

Das Management bleibt ein Ankerpunkt in jeder CRM-Strategie. Es ist erforderlich, die neue Qualität vorzuleben und einzufordern. Führungskräfte können von ihren Mitarbeitern Freundlichkeit und professionelle Kundenbetreuung nur erwarten, wenn die Unternehmenskultur Eigeninitiative durch Empowerment unterstützt.

Das technologische Fundament für CRM ist eine moderne IT-Infrastruktur. Die kundennahen Prozesse entlang des Kundenlebenszyklus benötigen einen durchgängigen Workflow. Hierfür braucht es die Integration der Systeme und eine klare Datenhaltung.

CRM zahlt sich aus

Die erste Wahl für den Kunden zu sein, ist die treibende Kraft bei der Entwicklung der kundenfokussierten Strategie. Gleichzeitig steigert CRM die Performance des Unternehmens durch mehr Leads, mehr Opportunities und mehr Aufträge.

Die neue Qualität verbessert zeitgleich die interne Kommunikation. Mit der Reduktion auf das Wesentliche steigen die Prozessqualität und -geschwindigkeit. Es gibt weitaus weniger manuelle Tätigkeiten, doppelte Eingaben, unstrukturierte Daten und somit weniger Fehler. Das Resultat ist ein enormer Zeitgewinn, welcher für neue und bestehende Kundenbeziehungen genutzt werden kann.

Die CRM-Strategie wirkt in zwei Richtungen: Sie hebt die Qualität für den Kunden und senkt die Kosten durch Präzision. Die Investitionen in die Prozessqualität, Mitarbeiter und Führungskräfte sowie den Ausbau der IT-Infrastruktur zahlen sich mittelfristig aus und stärken langfristig die Position im Markt.

Stephan Bauriedel

it management

AUSGABE 01-02/2024
ERSCHEINT
AM 18. JANUAR 2024

UNSERE THEMEN

Unified Communication
Herausforderung Office 4.0
SAP-Partnerlösungen

it security

AUSGABE 01-02/2024
ERSCHEINT
AM 18. JANUAR 2024

UNSERE THEMEN

Security Awareness
Zero Trust
Cybersecurity

WIR WOLLEN IHR FEEDBACK

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

INSERENTENVERZEICHNIS

it management

ZOI TechCon GmbH (Teaser)	U1
ITW Verlag GmbH	U2
ams.Solution AG	7
USU Software AG	9
Asseco Solutions GmbH (Advertorial)	17
T-Systems International GmbH	25
FNT GmbH	29
it verlag GmbH	33, 61, U4
Mesago Messe Frankfurt GmbH	53
E3/B4B Media	U3

it security

macmon secure GmbH (Teaser)	U1
Tehtris (Teaser)	U1
it verlag GmbH	U2, U4
CONTECHNET Deutschland GmbH	11
HiScout GmbH	17
Nevis Security AG (Advertorial)	21
NCP engineering GmbH (Advertorial)	25
Qualys (Advertorial)	29

IMPRESSUM

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

Chefredaktion: Silvia Parthier (-26)

Redaktion: Carina Mitzschke (nur per Mail erreichbar)

Redaktionsassistenz und Sonderdrucke: Eva Neff (-15)

Autoren: Daria Batrakova, Stephan Bauriedel, Martin Besemann, Sven-Anwar Bibi, Philipp von der Brüggen, Gilles Chêne, Jakob Freund, Stefan Heizmann, Sridhar Iyengar, Michaela Lackner, Frank Laschet, Carina Mitzschke, Adrian Müller, Silvia Parthier, Ulrich Parthier, Kristin Pitz, Daniel Pott, Christian Quandt, Dr. Fridtjof Schucht, Amadeus Thomas, Dr. Joachim Weber

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

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

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

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

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

Anzeigenpreise: Es gilt die Anzeigenpreisliste Nr. 31.
Preisliste gültig ab 1. Oktober 2023.

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

Online Campaign Manager:
Roxana Grabenhofer, 08104-6494-21, grabenhofer@it-verlag.de

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

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

Erscheinungsweise: 6 x pro Jahr

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

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

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


Steampunk
und BTP Summit 2024
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

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

it security

Detect. Protect. Respond.
November/Dezember 2023

THOUGHT LEADERSHIP

AB **SEITE 7**

SOPHOS

macmon intelligent einfach

Zero Trust Network Access

ab Seite 12

TEHTRIS
FACE THE UNPREDICTABLE

Risiken und Chancen der IT-Security

ab Seite 14

KOMPLEXE CYBERSICHERHEIT

Schlüsselrolle Automatisierung?

Andrè Schindler, NinjaOne

EDR/XDR & ANTI-VIRENSOFTWARE

Was ist der Unterschied?

SICHERHEIT IM MITTELSTAND

Drei Schlüsselerkenntnisse

UNIFIED ENDPOINT MANAGEMENT

Aus dem Schatten ins Licht

”Unternehmen denken nach, Thought Leader denken voraus!”

THOUGHT LEADERSHIP

Mehr Infos dazu im Printmagazin

itsecurity

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

Inhalt

COVERSTORY

4 **Komplexe Cybersicherheit**
Schlüsselrolle Automatisierung?

THOUGHT LEADERSHIP

7 **Wie Cybersicherheit moderne Arbeitswelten unterstützt**
Managed Services für moderne Unternehmen

IT SECURITY

12 **Zero Trust Network Access**
OT-Netzwerke verstärkt im Fokus von Kriminellen

14 **Künstliche Intelligenz**
Risiko und Chance der IT-Security-Strategie der Zukunft

16 **MDR-Services als Gebot der Stunde**
Proaktivität als Ass im Ärmel der Gefahrenabwehr

18 **Besser Vor- als Nachsorge**
Mit Incident Response Unternehmen wappnen

22 **Was Software „Made in Europe" besonders sicher macht**
Security und Datenschutz sind Milliardenfragen

26 **Üben ist das A und O**
Notfallübungen stärken die Unternehmensresilienz

30 **EDR/XDR und Antivirensoftware**
Was ist der Unterschied?

32 **Unified Endpoint Management**
Aus dem Schatten ins Licht

33 **Wissen, was geht**
Threat Intelligence für eine proaktive Gefahrenabwehr

34 **IT-Sicherheit im Mittelstand**
Drei Schlüsselerkenntnisse für den Schutzes Ihres Unternehmens

36 **Sicherheit in der Industrie**
Optimierte IT-Notfallplanung

37 **Knox Native**
Sicherheit und Kontrolle über kryptografische Schlüssel

38 **it security AWARDS 2023**
Gewinner im Rahmen der „it-sa 2023" ausgezeichnet

43 **IT-Sicherheitstrends 2024**
Von Auditierung bis Zero Trust

44 **Fernwartung im industriellen Umfeld**
So lassen sich IT- und OT-Systeme verwalten

Komplexe Cybersicherheit

SCHLÜSSELROLLE AUTOMATISIERUNG?

Die Arbeitswelt hat sich in den letzten Jahren gewandelt und diese Veränderungen haben die Notwendigkeit für eine verstärkte Cybersicherheit in Unternehmen deutlich gemacht. Die treibende Kraft heißt Digitalisierung. Die digitale Transformation von Unternehmen, der Trend zum Arbeiten aus der Ferne und die zunehmende Abhängigkeit von Cloud-Services haben die Tür für neue Cyberbedrohungen weit aufgestoßen. Wie man diese Herausforderungen meistert, darüber sprach wir mit André Schindler, General Manager EMEA bei NinjaOne.

it security: *Herr Schindler, wie hat sich das Thema Sicherheit in den letzten Jahren verändert?*

André Schindler: Früher war Cybersicherheit hauptsächlich darauf ausgerichtet, die firmeneigene Infrastruktur und Netzwerke zu schützen. Das Unternehmensnetzwerk bildete einen soliden Sicherheitsperimeter und Endgeräte waren weniger kritisch. Mit dem Aufkommen von hybriden Arbeitsmodellen, dezentralen Netzwerken und der Nutzung verschiedener Devices hat sich diese Situation verändert: Die Umstellung auf Remote-Arbeit und der Einsatz cloudbasierter Dienste bedingen einen neuen Blick auf das Thema Sicherheit. Cybersecurity-Strategien müssen nun eine verteilte Belegschaft, eine Vielzahl von Endpunkten und ein komplexes Netzwerk von Cloud-Services berücksichtigen.

Cyberangriffe und Datenlecks mit hoher Medienpräsenz haben eindrucksvoll gezeigt, wie verheerend unzureichende Sicherheitsstrategien sein können: Im Jahr 2022 stieg die Anzahl der Ransomware-Angriffe um alarmierende 41 Prozent und die Identifizierung und Behebung solcher Attacken dauerte im Durchschnitt 49 Tage länger als bei anderen Sicherheitsverletzungen. Täglich ereignen sich durchschnittlich 2.200 sicherheitsrelevante Vorfälle und die durch Cyberkriminalität verursachten Kosten sind innerhalb eines Jahres um 10 Prozent gestiegen. Angesichts dieser alarmierenden Fakten haben Führungskräfte und Vorstände erkannt, dass Cyberbedrohungen ein erhebliches Business-Risiko darstellen.

it security: *Wie reagieren Ihrer Erfahrung nach IT-Verantwortliche auf diese Bedrohungslage?*

André Schindler: Die Veränderungen haben zu verstärkten Investitionen in das Thema Security geführt, die in Sicherheitstrainings, Phishing-Tests und Schulungen zur Sensibilisierung der Mitarbeiter fließen. Denn Cybersicherheit ist nicht mehr nur die Aufgabe spezialisierter Fachkräfte, sondern die Verantwortung jedes Einzelnen. Doch auch das Management muss dieses Thema ganz oben auf der eigenen Agenda positionieren. Ein wesentlicher Baustein einer wirksamen Security-Strategie ist definitiv die Absicherung sämtlicher Geräte. Um Risiken in der sich wandelnden Arbeitswelt zu minimieren, müssen Chief Information Security Officers (CISOs) vor allem die Endpunktsicherheit zuverlässig gewährleisten.

> EIN EFFEKTIVES PATCH MANAGEMENT IST UNERLÄSSLICH, UM SOFTWARE UND SYSTEME STETS AUF DEM NEUESTEN STAND UND SICHER ZU HALTEN.
>
> **André Schindler,**
> **General Manager EMEA, NinjaOne, www.ninjaone.de**

it security: *Wie sieht effektives Endpoint Management in der Praxis aus?*

André Schindler: Zunächst brauchen die Verantwortlichen echte Transparenz und eine zentrale Verwaltung. Die Fähigkeit, alle Endpunkte im Netzwerk genau zu überwachen, ist eine Grundvoraussetzung, um potenzielle Bedrohungen schnell zu erkennen und darauf zu reagieren. Eine zentrale Verwaltung ermöglicht eine effiziente Überwachung, Konfiguration und Fehlerbehebung von Geräten über eine einheitliche Schnittstelle.

Außerdem ist ein effektives Patch Management unerlässlich, um Software und Systeme stets auf dem neuesten Stand und sicher zu halten.

Des weiteren geht es um die Absicherung der Endpunkte: Die Konfiguration der Endgeräte muss so erfolgen, dass die Angriffsfläche minimiert wird. Dies können IT-Teams erreichen, indem sie unnötige Dienste deaktivieren und strenge Zugriffskontrollen durchsetzen. Eine erfolgreiche Endpunktverwaltung sollte außerdem effizient und skalierbar sein, sodass Unternehmen eine steigende Anzahl von Geräten und Benutzern unterstützen können, ohne die Komplexität oder Arbeitsbelastung zu erhöhen. Automatisierung spielt eine Schlüsselrolle bei der Zeit- und Ressourceneinsparung. Sie ermöglicht es IT-Teams, Routineaufgaben wie das Patchen, die Bereitstellung von Software und die Gerätekonfiguration an Systeme abzugeben. Dadurch steigt die Effizienz und die Endpunkte bleiben stets auf dem neuesten Stand.

Last but not least braucht jedes Unternehmen eine umfassende Backup-Strategie, um kritische Daten zu schützen und eine schnelle Wiederherstellung im Falle von Cyberangriffen oder Datenlecks zu ermöglichen.

it security: *Automatisierung ist ein gutes Stichwort. Warum wird sie zunehmend sicherheitsrelevant?*

André Schindler: Ein Blick auf die wachsende Anzahl an Geräten in Unternehmen macht schnell deutlich, dass effektive Endpoint Security nicht manuell gelingen kann. Die einzige Lösung, die den Herausforderungen der Praxis standhält, ist Automatisierung. Insbesondere die Automatisierung von Patch-Scans, -Genehmigungen und -Berichterstattung bietet erhebliche Vorteile: Automatisierte Tools können die gesamte IT-Infrastruktur schnell und präzise auf fehlende Patches und Schwachstellen überprüfen. Diese Effizienz gewährleistet, dass mögliche Einfallstore für Angreifer schnell geschlossen werden, um das Risiko von Bedrohungen zu minimieren. Außerdem beseitigt Automatisierung das Risiko menschlicher Fehler oder Versäumnisse, das in manuellen Prozessen nicht zu unterschätzen ist. Durch die Automatisierung von patchbezogenen Aufgaben können IT-Teams erhebliche Zeitersparnisse erzielen und ihre frei gewordenen Ressourcen für strategische Aufgaben wie die Entwicklung von Sicherheitsrichtlinien oder das Erkennen neuer Bedrohungen nutzen. Automatisierte Berichterstattungen liefern detaillierte Informationen zur Patch-Compliance und zum Status von Schwachstellen. Diese Informationen sind für Compliance-Audits von unschätzbarem Wert und ermöglichen es Unternehmen, die Einhaltung von Vorschriften aufrechtzuerhalten und transparent zu dokumentieren.

it security: *Welche anderen IT-Aufgaben können von Automatisierung profitieren?*

André Schindler: Seit der Pandemie beobachten wir immer häufiger Schwierigkeiten, die Softwareverteilung über Geräte in der Domain und im Home Office zu standardisieren. VPN-Verbindungen sind nicht für jedes Unternehmen praktikabel. Automatisierung und lückenloses Monitoring helfen dabei, das Ticketaufkommen zu reduzieren, was den IT-Support spürbar entlastet.

Zudem können Unternehmen durch die Vereinheitlichung des IT-Managements konsistente und robuste Sicherheitsmaßnahmen in ihrer gesamten IT-Infrastruktur implementieren, Schwachstellen reduzieren und ihre Gesamtsicherheitslage nachhaltig verbessern. Ein leistungsfähiger IT-Support für Mitarbeiter im Home Office ist außerdem ein nicht zu unterschätzendes Instrument zur Mitarbeiterbindung. In Zeiten des Fachkräftemangels ist es für Unternehmen ratsam, gut auf die hybride Arbeitswelt eingestellt zu sein, auch um als Arbeitgeber für Fachkräfte attraktiv zu bleiben. Doch um die Sicherheit standortunabhängiger Arbeitsplätze zu gewährleisten, ist ein besonders effektives IT Management unerlässlich. Sich dem Trend der Remote-Arbeit aus Sicherheitsgründen zu verschließen, kann negative Folgen haben.

Und zu guter Letzt können IT-Teams die Konsolidierung von IT-Management-Workflows dazu nutzen, ihre bestehenden Ressourcen optimal einzusetzen. Je mehr Routineaufgaben in der Systemadministration automatisiert werden können, desto mehr Zeit bleibt für kritische Aufgaben in der Informationssicherheit.

it security: *Herr Schindler, wir danken für dieses Gespräch.*

MANAGED SERVICES

Den Übergang in eine hybride Arbeitswelt haben viele Unternehmen noch nicht wirklich gemeistert. Nicht nur die komplexere IT-Infrastruktur, da immer mehr Geschäftsprozesse und Daten online abgewickelt werden, auch rechtliche und sicherheitsrelevante Fragen stellen Unternehmen vor Herausforderungen.
Cybersicherheit spielt eine entscheidende Rolle bei der Unterstützung moderner Arbeitswelten, indem sie Unternehmen vor den vielfältigen Bedrohungen schützt, die mit der Nutzung von digitalen Plattformen und Diensten einhergehen.
Managed Services nehmen dabei eine wichtige Position ein, da sie Unternehmen professionelle Unterstützung bieten, um die Herausforderungen der Cybersicherheit zu bewältigen und eine robuste Sicherheitsstruktur aufzubauen.

Wie Cybersicherheit moderne Arbeitswelten unterstützt

MANAGED SERVICES IM BEREICH IT-SICHERHEIT SCHAFFEN AGILITÄT UND SIND KATALYSATOR SOWIE TRIEBKRAFT FÜR MODERNE, FORTSCHRITTLICHE UND VERANTWORTUNGSVOLLE UNTERNEHMEN

Der Übergang in eine hybride Arbeitswelt mit einer immer schneller wachsenden Anzahl verbundener Geräte und mobiler Mitarbeiter stellt Unternehmen vor beträchtliche Herausforderungen. Gründe dafür sind sich zunehmend auflösende Netzwerkgrenzen, hauptsächlich verursacht durch verteilte Organisationsstrukturen und den Datenfernzugriff. Dem entgegen stehen immer raffiniertere Angriffstaktiken der Cyberkriminellen, insbesondere mit Ransomware. Diese gegensätzliche Konstellation hat gravierende Auswirkungen: In der State of Cybersecurity 2023 Studie von Sophos glauben 56 Prozent der in Deutschland befragten Teilnehmer, dass die Cybergefahren

CHEFSACHE IT SECURITY?

IT-Abteilung: | **Um die IT Security kümmert sich hauptsächlich:** | **Dienstleister:**

39,8 % Deutschland

37,7 % Österreich

43,1 % Schweiz

33,8 % Deutschland

32,1 % Österreich

27,5 % Schweiz

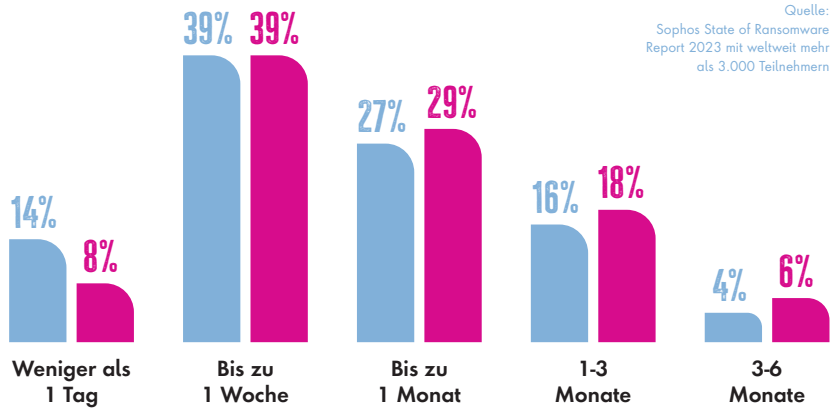
zu fortgeschritten sind, um sie allein bewältigen zu können. Als Folge ist der Bedarf an Cybersecurity as a Service (CSaaS) mit skalierbaren, zentral fernverwalteten und agilen Lösungen enorm und wird zusätzlich durch den eklatanten Fachkräftemangel angefeuert.

Realität und Verantwortung

Es ist fast schon an der Tagesordnung, dass über eine gefährliche Sicherheitslücke oder über einen Cybersicherheitsvorfall berichtet wird. Doch ist die Bedrohungslage vielleicht weniger spektakulär als berichtet wird? Oder wird vielleicht nur über die Spitze eines gewaltigen Eisbergs berichtet? Ergebnisse aus aktuellen Studien sprechen eine klare Sprache: Die Masse der Ereignisse bleibt tatsächlich im Verborgenen, denn worüber öffentlich berichtet wird, sind meist nur prominente Vorfälle, die keinesfalls die Gesamtheit darstellen. Im aktuellen State of Ransomware-Report von Sophos wurden weltweit rund 3000 Unternehmen unterschiedlicher Größen und aus unterschiedlichen Branchen, darunter 500 aus der DACH-Region, nach Ransomware-Angriffen und den Folgen befragt. 61 Prozent der in DACH befragten Unternehmen bestätigen, dass sie mit Ransomware angegriffen wurden. Und obwohl das bereits weit über die Hälfte der befragten Unternehmen ist, kann bei der Raffinesse der Cyberkriminellen davon ausgegangen werden, dass ein zusätzlicher Prozentsatz die Angriffe gar nicht bemerkt hat – was abermals die Eisbergtheorie untermauert. Betroffen sind alle Unternehmen und es gibt in einzelnen Marktsegmenten dabei kaum Ausreißer, die stärker oder geringer betroffen sind. Lediglich die IT-, Technologie- und Telekommunikationsbrache sowie die Produktion schaffen es mit 50 Prozent beziehungsweise 56 Prozent deutlich unter den Schnitt. Überdurchschnittlich häufig betroffen sind hingegen Regierungsbehörden mit 70 Prozent sowie der Bildungssektor mit fast 80 Prozent.

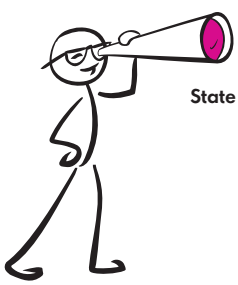
Angesichts der hohen Gefahrenpotenziale stellt sich die Frage, wer dafür verantwortlich ist, die Situation zu verbessern. Denn Ransomware-Angriffe können verheerende Auswirkungen für Unternehmen haben. Neben der Bezahlung der Lösegeldsummen, was 42 Prozent der Unternehmen in DACH für die Freigabe der verschlüsselten Daten tatsächlich tun, bringen vor allem die Folgeschäden durch Betriebs- und Produktionsausfälle die Unternehmen existenziell in Bedrängnis. 27 Prozent derer, die von Ransomware betroffen waren, bestätigen Summen von 500.000 bis 1 Million US-Dollar an Gesamtschaden, 15 Prozent berichten sogar von 1 bis 5 Million US-Dollar – ganz zu schweigen von der Zeit, die es benötigt, um die Systeme wiederherzustellen.

ZEITAUFWAND ZUR WIEDERHERSTELLUNG DES NORMALEN GESCHÄFTSBETRIEBS NACH EINER RANSOMWARE-ATTACKE



Quelle: Sophos State of Ransomware Report 2023 mit weltweit mehr als 3.000 Teilnehmern

Dieser wirtschaftliche Schaden legt nahe, das die Verantwortung nicht nur in der IT-Abteilung liegen darf. In einer weiteren Studie von Sophos wird allerdings klar, dass das Thema Cybersicherheit zwar auf der Agenda der Unternehmensführungen angekommen ist. Bei der Frage, wie eng die Umsetzung des Themas tatsächlich mit den Führungsetagen verknüpft ist, zeigen sich jedoch deutliche Unterschiede zwischen der Bewertung des IT-Sicherheitsbewusstseins der Chefetagen und der tatsächlichen operativen Verantwortung: Letztere liegt laut der Befragung der Führungskräfte bei den IT-Teams, obwohl sich die Chefs selbst mit über 80 Prozent ein hohes Sicherheitsbewusstsein attestieren. Bei nur rund 16 Prozent ist IT-Security tatsächlich Chefsache. Gleichsam hegt die Chefetage dennoch berechtigte Sorge um die wirtschaftlichen Auswirkungen und die Reputation des Unternehmens im Falle eines Cyberangriffs. Dies zeigt deutlich, dass das Thema Cybersicherheit noch zu wenig wirkungsvoll in der Unterneh-



PLUS

State of Cybersecurity 2023

mensstrategie verankert ist. Die hoffnungsvolle Nachricht: Knapp ein Drittel der Chefs setzt bei der Umsetzung der IT-Security nicht nur auf das interne IT-Team, sondern ergänzend auch auf IT-Dienstleister.

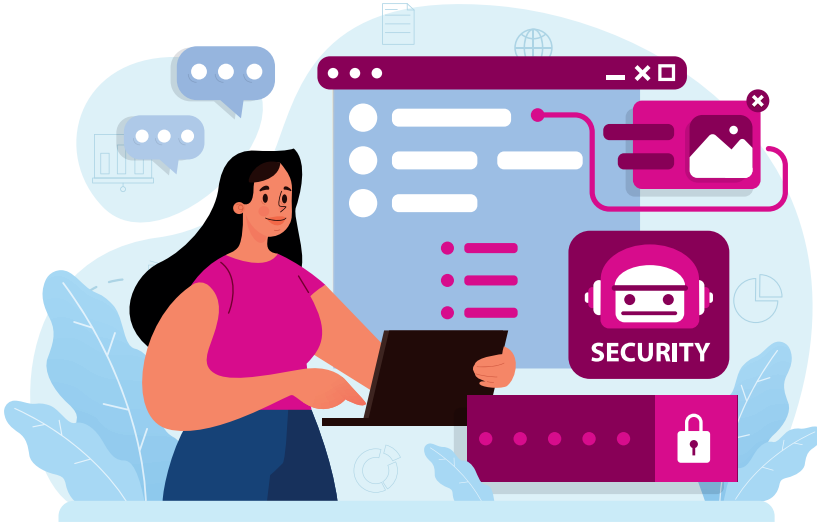
Es geht darum, Cyberangriffe so früh wie möglich zu entdecken

Als Antwort auf die sich verschärfende Bedrohungslage in Verbindung mit einer hybriden Arbeitswelt starten viele Unternehmen konzertierte Anstrengungen, um ihre Abwehrmaßnahmen zu stärken. Dabei wird aktuell ein dringend nötiger Paradigmenwechsel durchlaufen, durch den das Ziel einer Cybersicherheitsstrategie im Vergleich zu früheren Jahren deutlich verlagert wird: Es geht nicht mehr primär darum, Bedrohungen nach dem Entdecken unschädlich zu machen. Das neue Hauptziel besteht darin, Bedrohungen wesentlich früher zu identifizieren und wenn möglich gleich am Anfang der Angriffskette zu stoppen – idealerweise bevor der Angreifer überhaupt umfänglich in Unternehmenssysteme eindringt. Die Schwierigkeit besteht darin, die ersten Signale eines potenziellen Angriffs zu erkennen. Laut der State of Cybersecurity 2023 Studie von Sophos sehen 59 Prozent der in Deutschland Befragten genau darin noch ein Problem.

Hierfür gibt es bereits Lösungsansätze. Mittlerweile sind speziell ausgebildete und international vernetzte Experten durch gezielte Bedrohungssuche und mit Hilfe von Künstlicher Intelligenz in der Lage, Lücken oder Schwachstellen frühzeitig zu identifizieren und zu schließen, bevor ein Angreifer sie ausnutzen kann. Durch die zentrale Steuerung dieser Abwehrmaßnahmen erreichen Unternehmen den optimalen Schutz – auch für hybride Arbeitsmodelle, egal ob im Büro, Zuhause oder unterwegs.

So bekannt das Problem, so aufwändig und schwierig ist allerdings die Umsetzung, da die Implementierung eines umfassenden Cybersicherheits-Ökosystems zwei maßgebliche Komponenten benötigt: die vernetzte und intelligente Kontrolle aller Endgeräte, Server und Netzwerke sowie die Unterstützung durch erfahrene Cybersicherheitsexperten, die aus Kosten- und Verfügbarkeitsgründen nur die wenigsten Organisationen intern vorhalten können.

Dass diese Grundpfeiler für eine moderne Cybersicherheitsstrategie oftmals noch nicht implementiert sind, ist besorgniserregend. Denn laut der Sophos-Umfrage „State of Cybersecurity in Business" empfinden 93 Prozent der Unternehmen bereits die Durchführung klassischer Sicherheitsmaßnahmen als Herausforderung. Darüber hinaus sagen über die Hälfte der Befragten IT-Verantwortlichen, dass Cyberbedrohungen mittlerweile zu weit fortgeschritten sind, um sie als Unternehmen alleine bewältigen zu können – eine ernüchternde Realität.



Wie Unternehmen von Cybersecurity as a Service profitieren können

Die Lösung im Falle einer ungenügenden Cybersicherheit bietet sich in Form eines Cybersecurity-as-a-Service-Modells (CSaaS) an. Bei diesem Modell können drei entscheidende Säulen der Cybersicherheit miteinander vereint werden: die Nutzung eines intelligent vernetzten und integrierten Cybersicherheitsökosystems, der Betrieb und die Überwachung der Cybersicherheit durch einen spezialisierten Dienstleister und die Einbindung menschlicher Expertise in das Threat Hunting und in die Reaktion auf Risiken und Vorfälle.

Der CSaaS-Ansatz punktet in vier entscheidenden Bereichen:

#1 Konzentration auf das Wesentliche

Durch die Auslagerung oder Erweiterung der Cybersicherheit auf einen Managed Detection and Response (MDR)-Dienst erhalten Unternehmen die Möglichkeit, Sicherheitsvorgänge je nach Bedarf zu skalieren. Dadurch können sich IT-Verantwortliche auf organisatorische Prioritäten konzentrieren und strategischer vorgehen, um ihr Unternehmen vor ständig wachsenden und sich ändernden Bedrohungen zu schützen. Mehr Konzentration auf strategische und wichtige Arbeit in der IT-Abteilung wünschen sich 55 Prozent der Befragten in der State of Cybersecurity 2023 Studie.

#2 Umgehung des Fachkräftemangels

Umfragen unter IT-Führungskräften haben ergeben, dass der Mangel an inter-

nen Fähigkeiten oder Fachwissen im Bereich Cybersicherheit heute als eines der drei größten Sicherheitsrisiken angesehen wird. Das ist einer der Gründe, weshalb laut der Sophos Studie nur noch 4 Prozent der in Deutschland Befragten Cybersicherheit rein intern behandeln. Denn MDR-Anbieter können diese Lücke schließen, da sie in der Lage sind kurzfristig und rund um die Uhr Hunderte von Fachkräften bereitstellen zu können – darunter Analysten, Forscher, Bedrohungsjäger und Datenwissenschaftler.

#3 Bestmögliche Nutzung bestehender Investitionen

Unternehmen befürchten oft, dass ein MDR-Anbieter automatisch ihre bestehende Infrastruktur umstrukturiert oder sogar ersetzt. Dies ist jedoch oftmals nicht der Fall. Moderne MDR-Services nutzen Telemetriedaten bestehender Tools, um die Erkennung und Untersuchung von Bedrohungen zu beschleunigen. Darüber hinaus entlastet ein MDR-Service die Mitarbeiter, sodass diese Projekte vorantreiben können, die andernfalls möglicherweise ins Stocken geraten wären.

#4 Bessere Cybersicherheit und TCO durch MDR

Insbesondere für kleinere und mittelständische Unternehmen ist es aus Kostengründen kaum möglich, in ausgewiesene Security-Spezialisten zu investieren. Dennoch muss der Cybersicherheitsbetrieb 24/7 aktiv sein, inklusive Forschung, Forensik und Reaktion. Dafür wären je nach Unternehmensgröße mindestens zwei dieser Experten nötig, um diese Position während Tag- und Nachtschichten, Urlauben, Krankheitstagen oder Schulungen etc. durchgängig zu besetzen. Da ein MSP seine Experten wesentlich effizienter über alle Kunden hinweg einsetzen kann, ist die Total Cost of Ownership (TCO) für die meisten Unternehmen mit einem MSP auch aus wirtschaftlicher Sicht die weitaus bessere Wahl.

Fazit

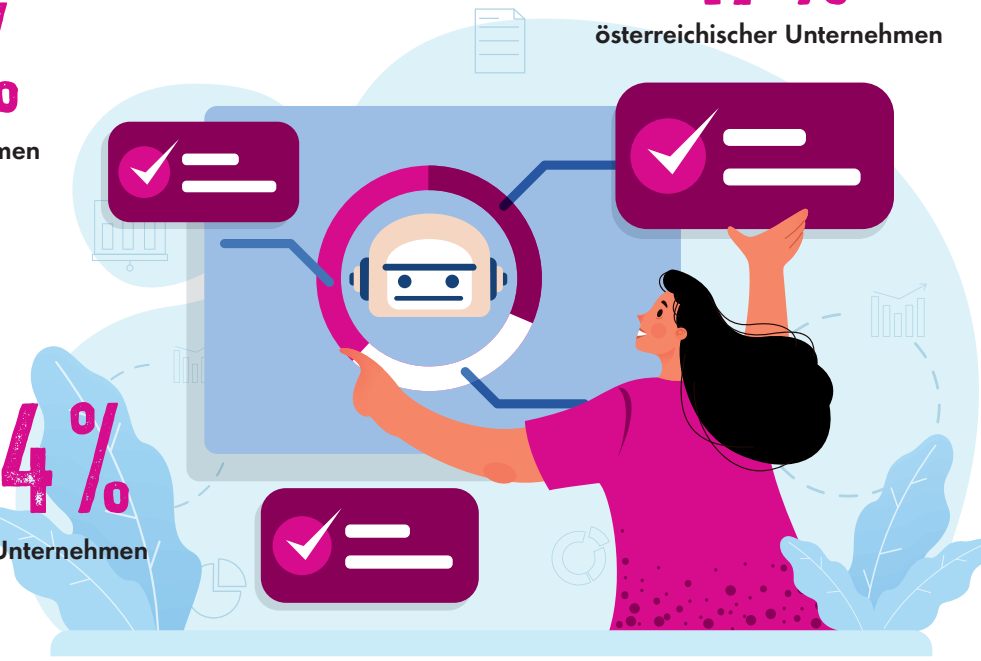
Der effizienteste Schutz vor Cyberattacken ist ein integriertes und intelligentes Cybersicherheitsökosystem, gepaart mit Künstlicher Intelligenz und menschlicher Security-Expertise in Form von MDR-Services. Damit sorgen Unternehmen nicht nur für die entscheidende Reduzierung des Cyberrisikos, sondern auch für das Erreichen einer Agilität, die eine zukunftsorientierte Gestaltung des Business und der Arbeitswelten möglich macht.

Michael Veit

NUR BEI EINEM GERINGEN TEIL DER UNTERNEHMEN IST IT SECURITY CHEFSACHE!

15,7 %
schweizer Unternehmen

17 %
österreichischer Unternehmen



16,4 %
deutscher Unternehmen

CYBERSECURITY IM MITTELSTAND

VERÄNDERTE BEDROHUNGSLAGE BIRGT GROSSE GEFAHREN

In den vergangenen Jahren wurde viel über IT-Sicherheit gesprochen. So viel, dass jedes Unternehmen eigentlich eine übergreifende IT-Security-Strategie aufweisen müsste. Schließlich ist nicht von der Hand zu weisen, dass sich Cyberkriminelle die durch die Digitalisierung gestiegenen Möglichkeiten für Cyberangriffe zu eigen machen. Denn in den vergangenen Jahren ist die Anzahl und die Schwere von Cyberangriffen kontinuierlich gestiegen.

Dabei sind nicht nur große Unternehmen von Cyberangriffen betroffen, kleine und mittelgroße Unternehmen sind gleichermaßen bedroht. Großunternehmen verfügen im Gegensatz zum Mittelstand über deutlich mehr Ressourcen und Know-how zur Abwehr von Cyberattacken. Knappere Budgets und weniger personelle Kapazitäten, um das eigene Unternehmen auf sich verändernde Bedrohungslagen anzupassen, setzen kleine und mittlere Unternehmen einem enormen Gefahrenpotenzial aus.

Bereits im Jahr 2019 wurden im Rahmen der Studie „IT-Sicherheit im Mittelstand" kleine und mittlere Unternehmen zu ihrem Umgang mit IT-Sicherheit befragt. In dieser Neuauflage betrachten wir, was sich in den vergangenen vier Jahren, speziell auch durch den Digitalisierungsbeschleuniger „Corona", in Sachen IT-Sicherheit im Mittelstand verändert hat.

WHITEPAPER DOWNLOAD

Das Whitepaper umfasst 19 Seiten und steht kostenlos zum Download bereit: **www.it-daily.net/download**

Zero Trust Network Access

OT-NETZWERKE VERSTÄRKT IM FOKUS VON KRIMINELLEN

Bereits 2018 zeigte eine Umfrage von statista zur Entwicklung der OT-Cybersecurity-Bedrohungen in Industrieunternehmen eine hohe Besorgnis unter den Verantwortlichen in Deutschland: Demnach gaben 35 Prozent der Befragten an, dass sich im vergangenen Jahr die Anzahl der OT-spezifischen Cybersecurity-Bedrohungen in ihrem Unternehmen erhöht hat.

Eine weitere Studie im Jahr 2020 ergab, dass 98 Prozent der Befragten angaben, dass das Ausmaß der digitalen Risiken für ihren Betrieb in den letzten drei Jahren zugenommen hatte. Die Umfrage unter 200 leitenden Cybersicherheits-Verantwortlichen ergab außerdem, dass 70 Prozent der Befragten ihre Prozesse oder Best Practices geändert hatten, um den beschleunigten Trend zur vernetzten Produktion zu berücksichtigen.

Angetrieben durch die Pandemie und in der Hoffnung, immer effizienter und kostengünstiger zu werden, sehen sich die Unternehmen gezwungen, ihre Prozesse zu digitalisieren. Dies hat zur Folge, dass ehemals abgeschottete Industrieumgebungen heute dem Internet ausgesetzt sind.

OT-Netze nicht mehr isoliert

Die meisten der heute existierenden OT-Netze wurden in den frühen 90er Jahren entworfen. Die Sicherheit eines OT-Netzes beruht auf der Design-Philosophie der Isolation - einer vollständigen Trennung von anderen Netzen. Diese Technik gewährleistete den Standardschutz eines OT-Netzes, unabhängig vom Vormarsch der IT-bezogenen Bedrohungen. Die OT-Netze wurden oft durch strenge Protokolle an ihren jeweiligen Standorten geschützt, wodurch die meisten Bedrohungen ausgeschlossen werden konnten. Die jahrzehntealten OT-Netze erfordern eine kontinuierliche Wartung und die Installation von Upgrades, was in der Praxis nicht immer erfolgt.

Ursachen für die gestiegene Vulnerabilität von Unternehmen ist der breitere Einsatz von Betriebstechnologien, die die Zahl der Anwendungsfälle erhöht, die Schutz erfordern. Die verschwimmenden Grenzen zwischen IT, OT und IoT erhöhen den Bedarf an integrierten, kooperativen Cybersicherheitsstrategien.

Übersicht und Kontrolle aller Netzwerkkomponenten

Das Erkennen eines Komponentenfehlers in einer Produktionsanlage kann einige Minuten, Stunden oder sogar Tage dauern. Diese ungeplante Ausfallzeit kann den Betriebsablauf und die Geschäftstätigkeit des Unternehmens stark beeinträchtigen. Ohne zentralen Überblick über das gesamte OT-Netzwerk ist es unmöglich in Echtzeit zu erkennen, welche Geräte dem Netzwerk hinzugefügt werden oder es verlassen. Bis man das Vorhandensein eines fremden Geräts im Netzwerk bemerkt, ist es oft zu spät. Zu diesem Zeitpunkt kann

ein Angreifer bereits enormen Schaden anrichten, denn das OT-Netz muss zu jeder Zeit betriebsbereit sein. Der Angreifer kann über bekannte und nicht gepatchte Sicherheitslücken, Systeme von Drittanbietern oder schlecht verwaltete OT-Geräte in das System eindringen. Das Netzwerk sollte ständig überwacht werden, um jegliche Eindringversuche zu erkennen. Sicherheitslösungen für industrielle Netzwerke umfassen eine breite Palette von Produkten zum Schutz von Anlagen, Netzwerken und Endpunkten.

Industrielle Netzwerksicherheit

Die Implementierung von Asset-Identifizierung, Protokollierung, Network Access Control (NAC), Security Information and Event Management (SIEM) und eine sinnvolle Netzwerksegmentierung ist geboten. Die Überwachung jedes Geräts in einem OT-Netzwerk ist für die sichere Trennung zwischen Netzsegmenten (Perimeter) unerlässlich.

Dazu Christian Bücker, Business Director, macmon secure: „Wenn OT-Systeme vernetzt sind und Fernzugriffe möglich sind, ist eine Netzwerkzugangskontrolle (Network Access Control) unabdingbar, um die Sicherheit zu gewährleisten. Nutzer und Endgeräte müssen authentifiziert und autorisiert werden. Um die Komplexität des OT-Netzes sichtbar zu machen benötigt man eine vollständige Netzwerkübersicht. Damit der Ausfall einer Maschine nicht den kompletten Betrieb beeinflusst, sollten virtuelle Teilabschnitte mithilfe von Netzwerksegmentierung gebildet werden (VLAN-Management)."

OT-Sicherheitslösungen sollten Übersicht und Kontrolle über jedes Gerät im OT-Netzwerk über einen einzigen Bildschirm ermöglichen. Zu den Geräten können technische Workstations, Programmable Logic Controlers (PLCs), Human Maschine Interfaces (HMIs) und andere Industrial Control Systems (ICS) gehören. Da die Geräte und Komponenten in OT-Netzwerken von verschiedenen Herstellern stammen, sollte man deshalb auch auf die Herstellerunabhängigkeit einer OT-Sicherheits-Lösung achten, zum Schutz von Anlagen, Netzwerken und Endpunkten.

Kritische Infrastrukturen unter Beschuss

Die Energie-, Versorgungs- und Transportsektoren sind sowohl für die Wirtschaft als auch für die nationale Sicherheit von entscheidender Bedeutung und veranlassen Regierungen dazu, neue Vorschriften einzuführen und die bestehenden zu aktualisieren und weiterzuentwickeln.

Industrieunternehmen und Betreiber kritischer Infrastrukturen geraten zunehmend ins Visier von Cyber-Kriminellen. Mittlerweile sind die Angreifer nicht nur daran interessiert, Geld durch Erpressung zu verdienen, sondern haben in immer mehr Fällen auch die Absicht, OT-Netzwerksysteme empfindlich zu stören.

Neue Sicherheitsstrategien sind notwendig

Neue Geschäftsprozesse sorgen für höhere Leistung und niedrigere Kosten in der gesamten Industrielandschaft. Unternehmen nutzen neue Entwicklungen in den Bereichen Cloud Computing, Künstliche Intelligenz (KI), IoT, Edge-Lösungen und digitale Zwillinge, um zum einen Ressourcen-Engpässe und Optimierungsmöglichkeiten zu ermitteln. Die Vorteile der Digitalisierung können groß sein, aber Unternehmen müssen sich auch mit den erhöhten Risiken schwerer, kostspieliger Cybervorfälle auseinandersetzen.

Herkömmliche industrielle IT- und OT-Sicherheitsprogramme sind nicht dafür ausgelegt, all diese neuen Herausforderungen zu bewältigen. Digitalisierte Unternehmen benötigen Zero Trust Sicherheitsstrategien, die die Sicherheit für jedes Gerät, jede Anwendung, jedes System und jedes Netzwerk im Unternehmen überwachen, steuern und koordinieren, unabhängig davon, wo es sich befindet.

WENN OT-SYSTEME VERNETZT SIND UND FERNZUGRIFFE MÖGLICH SIND, IST EINE NETZWERK-ZUGANGSKONTROLLE (NETWORK ACCESS CONTROL) UNABDINGBAR, UM DIE SICHERHEIT ZU GEWÄHRLEISTEN.

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

Christian Bücker fasst zusammen: „Die Trennung der Cybersicherheitsbemühungen nach Technologien ist kein nachhaltiger Ansatz mehr. Unternehmen müssen neue integrierte Strategien entwickeln, die IT-, OT- und IoT-Sicherheitsbemühungen kombinieren und die Nutzung aller Cybersicherheits-Ressourcen des Unternehmens maximieren. Die Entwicklung einer umfassenden Sicherheitsstrategie, die sich mit den aktuellen und aufkommenden Risiken der Digitalisierung befasst, war noch nie so dringend wie heute. Deshalb verfolgen wir die Zero Trust Network Access Philosophie."

Sabine Kuch

Künstliche Intelligenz

RISIKO UND CHANCE DER IT-SECURITY-STRATEGIE DER ZUKUNFT

Alle Unternehmen haben ein gemeinsames Anliegen: die Gewährleistung der Cybersicherheit in ihrem Betrieb. Vom kleinsten Unternehmen bis zum multinationalen Konzern mit kritischen Infrastrukturen können sie zur Zielscheibe von Cyberkriminellen werden. Sie machen keine Unterschiede und werden immer versuchen so viel Schaden wie möglich anzurichten.

Eine der Hauptbedrohungen ist Ransomware, die Daten verschlüsseln kann, um deren Nutzung zu verhindern und Lösegeld zu erpressen. Die zweite große Bedrohung ist die Ausnutzung von Software-Schwachstellen. Aber es gibt noch mehr. DDoS-Angriffe, Imitationen von Personen und Marken (Phishing), Kryptowährungsbetrug oder Supply-Chain-Attacks erweitern die Liste. Hinzu kommen Insider-Bedrohungen, fahrlässige Mitarbeiterentscheidungen und Insider-Vorfälle.

Ein technologischer Fortschritt, der dabei von den Kriminellen ausgenutzt wird, ist die künstliche Intelligenz (KI), deren Nutzung durch Lösungen wie Chatbots, erweiterte Sprachmodelle und generative KI, immer einfacher wird. Angreifer nutzen diese beispielsweise, um ihre eigene Malware zu entwickeln, verbessern und zu verbreiten.

Mit XDR-Technologie zum Erfolg

Dass Cyberbedrohungen immer raffinierter werden, ist Realität und stellt herkömmliche Antivirenlösungen vor unlösbare Herausforderungen. Unternehmen können sich nicht mehr auf bekannte Maßnahmen verlassen, neue Technologien sind nötig, um Erkennung und Abwehr von Cyberattacken in Echtzeit durchzuführen.

Die eXtended Detection and Response (XDR)-Technologie erfüllt diese Anforderungen. Ihr erweiterter Erkennungs- und Reaktionsansatz bietet eine größere Abdeckung durch Zusammenführung mehrerer Lösungen in einer Plattform. Dank des Informationsaustauschs der zwischen den Produkten aufgebaut wird, können Vorfälle mit einem mehrschichtigen Konzept angegangen werden.

Um mit der sich ständig verändernden Umgebung Schritt halten zu können, brauchen die Sicherheitsteams in Unternehmen jede erdenkliche Hilfe. Informationen zu zentralisieren und eine ganzheitliche Sicht zu konfigurieren ist hierbei am besten geeignet, um die Analyse zu erleichtern und blinde Flecken zu vermeiden.

Eine der Grundlagen, auf denen Erkennungs- und Reaktionstools aufgebaut sind, ist EDR (Endpoint Detection and Response). Ein EDR geht von Verhaltensmustern aus und identifiziert Anomalien, wenn es Telemetrie- und Geräteleistungsdaten sammelt und sie korreliert. Es greift mit tiefgreifenden Analysen und Untersuchungen ein, um Abhilfe zu schaffen. Dieser Endpunktschutz ermöglicht es in einer kompliziert gewordenen Welt in den grundlegenden Sicherheitstools vorhandene Lücken zu schließen.

Nur so können Cyberkriminelle in Schach gehalten werden. Es gibt Malware-Muster, die für jedes erdenkliche Szenario entwickelt wurden, ein Cyberangriff kann jederzeit erfolgen und in wenigen Minuten abgeschlossen sein. Daher ist es wichtig, dass man die Möglichkeit

ANGREIFER NUTZEN KÜNSTLICHE INTELLIGENZ, UM IHRE EIGENE MALWARE ZU ENTWICKELN UND ZU VERBREITEN.

Olaf Müller-Haberland, Head of Sales and Services DACH, Tehtris, www.tehtris.eu

hat, sofort einzugreifen. Eine hyperautomatisierte Lösung, die Angriffe in Echtzeit abwehrt, ohne dass ein Mensch eingreifen muss, ist die ideale Lösung für Unternehmen. Proaktivität und Reaktivität sind hierbei entscheidend.

Optimierter Schutz mit KI

Die Bedrohungen ändern sich ständig mit dem Ziel die bestehenden Schutzbarrieren zu durchbrechen. Cybersecurity ist ein dynamisches Thema: In der Vergangenheit kämpften Unternehmen gegen von Einzelpersonen entwickelte Malware für die signaturbasierte Angriffserkennung ausreichend war, heute sind die Angriffe fortschrittlicher, gezielter - und nutzen künstliche Intelligenz. Mehr denn je muss der Schutz optimiert und sich von der langsamen manuellen Analyse verabschiedet werden

Eine Lösung, die das gesamte Unternehmensnetz einschließlich der mobilen Endgeräte überwacht, muss in der Lage sein, Anomalien zuverlässig zu erkennen, zu qualifizieren und so schnell wie möglich zu unterbinden. Hier kommt die künstliche Intelligenz in ihrer positivsten Facette ins Spiel, denn sie bringt Handlungsschnelligkeit in die IT-Sicherheit. Sie trifft die Entscheidung, potenzielle Bedrohungen abzuwehren, bevor es zu spät ist und Auswirkungen auf die Finanzen und den Ruf des Unternehmens hat. Ein erfolgreicher Angriff führt oft zu Problemen und wird im Extremfall sogar zum Existenzrisiko des Unternehmens selbst. Unternehmen können und sollten sich mit denselben Waffen zur Wehr setzen, die böswilligen Akteuren zur Verfügung stehen. KI stützt sich auf Big Data, um ihre Aktionen zu steuern, in einer Geschwindigkeit, die durch Analysten nicht erreichbar ist. Die Vielfalt der Geräte, Systeme und Umgebungen erfordert heute eine Lösung, die sich mit der Entwicklung der Cyber-Bedrohungen weiterentwickelt.

Abwehrfähigkeiten fördern

Banken, Versicherungen, Bildungseinrichtungen, der Energiesektor, Gesundheitseinrichtungen... in allen Branchen besteht die Gefahr, in die Netze der Hacker zu geraten. Um eine digitale Katastrophe zu verhindern, ist es ratsam, die Sichtbarkeit zu verbessern und die Abwehrfähigkeit zu fördern, nicht nur die Erkennung. Dies wird durch die Integration von verschiedensten Sicherheitstools in eine einzige Plattform erreicht. In noch stärkerem Maße mit einer einheitlichen Konsole, die alle Module zusammenführt und miteinander verknüpft. So wird IT-Security Spezialisten eine 360-Grad-Sicht ermöglicht.

Der Innovationsgrad im Bereich der KI ermöglicht es die Cybersicherheit zu stärken. Die TEHTRIS XDR-Plattform erfüllt die heutigen Geschäftsanforderungen an Transparenz, Einfachheit und wirksamen Schutz durch ihren Ansatz der automatischen Neutralisierung von Cyberangriffen in Echtzeit und ohne menschliches Zutun. Das Unternehmen ist sowohl für die Herausforderungen der Gegenwart als auch für die der Zukunft gerüstet. Die Lösung besteht aus verschiedenen Sicherheitsmodulen, darunter EDR, MTD, SIEM, NTA, DR (Honeypots) oder DNS-Firewall. Alle diese Komponenten sind miteinander verbunden und werden von der CYBERIA-KI-Engine gesteuert, die die Suche nach Schwachstellen in großen, verteilten Infrastrukturen durch die Erkennung von Anomalien vereinfacht. Das integrierte SOAR ermöglicht intelligente Sensorinteraktionen und das Blockieren von Bedrohungen. Da es sich um eine offene Plattform handelt, bietet sie native Interoperabilität mit verschiedensten Produkten auf dem Markt. Das Ergebnis ist eine 360°-Sicherheit.

Fazit

Das unaufhaltsame Wachstum der Cyberkriminalität rund um den Globus ist eine große Herausforderung. TEHTRIS hat die Antwort darauf. Mit dem Wissen, wie man ihr begegnet, Bedrohungen erkennt, analysiert und abwehrt. Die Tools werden innerhalb einer einzigen Plattform orchestriert, um einen globalen Überblick über die Unternehmenssysteme, eine optimierte Zusammenarbeit zwischen professionellen Teams und eine umfassende Reaktionsfähigkeit zu ermöglichen. Die Lösung ist datenfreundlich. Und es setzt künstliche Intelligenz für die Cybersicherheit ein – denn wenn es die Angreifer machen, sollten IT-Security Experten nicht davor zurückschrecken.

Olaf Müller-Haberland

MDR-Services als Gebot der Stunde

PROAKTIVITÄT ALS ASS IM ÄRMEL DER GEFAHRENABWEHR

ANGESICHTS DER KOMPLEXITÄT AKTUELLER ANGRIFFSSZENARIEN WIRD EIN VORAUSSCHAUENDES AGIEREN IM ZUGE DER UMSETZUNG EINER EFFEKTIVEN IT-STRATEGIE ZUR PFLICHT.

Michael Haas,
Regional Vice President Central Europe,
WatchGuard Technologies GmbH,
www.watchguard.de

Von einem Security Operations Center (SOC) geht entscheidender Mehrwert aus und gerade kleinen und mittelständischen Unternehmen bieten sich dank moderner MDR-Services (Managed Detection and Response) immer mehr Möglichkeiten, Gefahren schneller zu erkennen und entsprechend abzuwehren.

Angesichts der Komplexität aktueller Angriffsszenarien wird ein vorausschauendes Agieren im Zuge der Umsetzung einer effektiven IT-Strategie zur Pflicht. Genau hier kommen SOC ins Spiel, die auf die konsequente Überwachung und Analyse der Bedrohungslandschaft ausgelegt sind. Im Hinblick auf die Vorgehensweise fallen dabei immer wieder die Begriffe IoC (Indicators of Compromise) und IoA (Indicators of Attack). Aber was ist der Unterschied in der jeweiligen Ausrichtung? Die folgende Betrachtung hilft bei der Einordnung.

IoC (Indicators of Compromise)
IoC-basierte Analysen erkennen die Gegenwart einer Bedrohung auf einem Computer, wenn dieser bereits kompromittiert wurde. Das bedeutet: IoC werden verwendet, um ein Sicherheitsproblem zu diagnostizieren, das gerade innerhalb des Unternehmens aufgetreten ist. Sie zeigen an, dass eine Sicherheitsgefährdung stattgefunden hat oder in Kürze bevorstand.

Ziel ist die Identifikation von Dateien oder Ereignissen, die zuvor als bösartig eingestuft wurden – wie beispielsweise Phishing-Mails, Malware-Dateien, IP-Adressen, die im Zusammenhang mit Cyberkriminalität stehen, oder riskante Verzeichniseinträge. IoC sind für Unternehmen immer dann nützlich, wenn es darum geht, den Schaden nach oder während einer Kompromittierung zu analysieren – und entsprechend zu reagieren, um Schlimmeres zu verhindern. Zugleich können aufgedeckte Lücken geschlossen werden, damit sich ähnliche Szenarien in Zukunft nicht wiederholen.

IoA (Indicators of Attack)
Die Suche nach IoA folgt einer anderen Philosophie, hierbei ist deutlich mehr Proaktivität im Spiel: Aufgabe ist es, die Kompromittierung anhand verdächtiger Aktivitäten vorherzusehen. Mit anderen Worten: IoA wirken nicht erst, wenn der Angriff bereits stattgefunden hat, sondern zum Zeitpunkt der Attacke oder bereits davor.

Sie machen auf jeden Angriffsversuch aufmerksam – unabhängig davon, welche Methode zur Umgehung des Sicherheitssystems des Unternehmens angewendet wurde. Das heißt, IoA erkennen selbst Angriffsschritte, für die keine Malware erforderlich ist, wie bei Living-off-the-Land-Techniken.

Gefahren rechtzeitig erkennen
Für den Schutz einer Organisation sind grundsätzlich beide Konzepte notwendig, wobei der proaktive IoA-Ansatz im Hinblick auf die Vermeidung von Sicherheitsvorfällen einen klaren Schritt weitergeht. Insofern liefern MDR-Anbieter (Managed Detection and Response) wertvolle Unterstützung. Ihre Dienste sind hochgradig proaktiv ausgerichtet. Das Gesamtpaket umfasst dabei nicht nur effektive Technologie auf Basis von Künstlicher Intelligenz und Maschinellem Lernen, sondern auch Cybersicherheitsexperten sowie gut definierte und routinierte Prozesse, die massiv zum Schutz von Unternehmen gegenüber fortschrittlichen Bedrohungen beitragen. Damit ist das SOC-Konzept bei Weitem nicht mehr nur Konzernen vorbehalten, die über die nötige Manpower verfügen und hohe IT-Budgets zur Verfügung haben. Immer mehr Service-Angebote richten sich gerade an KMUs. Und diese sind gut damit beraten, dem Thema Managed Detection and Response einen genaueren Blick zu schenken. Denn die besten Karten bei der Absicherung hat derjenige, der die Gefahren erkennt, bevor das Eis dünn wird.

Michael Haas

Kampf gegen Cyberkriminalität

MARKT FÜR IT-SICHERHEIT WÄCHST

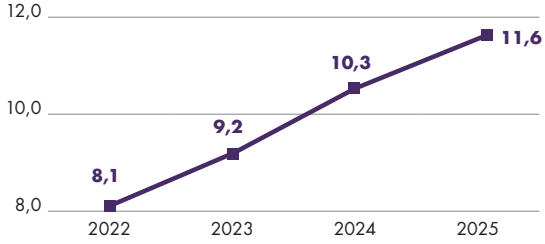
Die deutsche Wirtschaft wappnet sich für den Kampf gegen Cyberkriminalität. Erstmals werden hierzulande für IT-Sicherheit mehr als 9 Milliarden Euro ausgeben – Tendenz weiter steigend. Das teilte der Digitalverband Bitkom bei der Eröffnung der IT-Sicherheitsmesse „it-sa" in Nürnberg mit. Im laufenden Jahr klettern die Ausgaben für IT-Sicherheit um 13 Prozent auf 9,2 Milliarden Euro. Im kommenden Jahr wird ein erneuter Anstieg um rund 13 Prozent auf 10,3 Milliarden Euro erwartet. „Es ist ein gutes Signal, dass die Unternehmen ihre Ausgaben für IT-Sicherheit hochfahren. Jedes Unternehmen kann Opfer von Cyberangriffen werden. Aber auch jedes Unternehmen kann sich schützen – und sollte das auch tun", sagt Bitkom-Hauptvorstand Udo Littke. „Zuletzt ist deutschen Unternehmen durch Sabotage, Spionage und Datendiebstahl ein jährlicher Schaden von 206 Milliarden Euro entstanden, davon 148 Milliarden Euro durch Cyberattacken. Die Angreifer werden immer professioneller und gehen arbeitsteilig vor, dabei sind die Grenzen zwischen organisierter Kriminalität und staatlich gesteuerten Akteuren fließend."

Den größten Anteil an den Aufwendungen haben Ausgaben für IT-Sicherheitssoftware mit rund 4,3 Milliarden Euro (plus 18 Prozent). Knapp dahinter liegen Aufwendungen für Dienstleistungen rund um IT-Sicherheit, die um 12 Prozent auf 4,0 Milliarden Euro zulegen. Unverändert weitere knapp 0,9 Milliarden entfallen auf IT-Sicherheits-Hardware. „IT-Sicherheit muss für alle Unternehmen eine Daueraufgabe sein und ganz oben im Management verankert werden," so Littke.

www.bitkom.org

MARKT FÜR IT-SICHERHEIT WÄCHST

Ausgaben für IT Sicherheit in Deutschland (in Mrd. Euro)



bitkom

Besser Vor- als Nachsorge

WIE INCIDENT RESPONSE UNTERNEHMEN FÜR CYBER-ANGRIFFE WAPPNET

„Incident-Response-Pläne? Nützen uns nichts, sind zu teuer und verschwenden die Zeit meiner Mitarbeiter!". Diese Ansicht vertreten 41 Prozent der IT-Verantwortlichen in Deutschland, wie eine aktuelle Kaspersky-Studie zum Thema „Incident Response zur Prävention" [1] zeigt. Da überrascht es nicht, dass nur jedes fünfte Unternehmen über Pläne für Incident-Response verfügt.

Klar ist: Ohne gezielte und kontinuierliche Vorbereitung auf IT-Sicherheitsvorfälle riskieren Unternehmen im Akutfall folgenschwere Konsequenzen – wirtschaftlicher, finanzieller und nicht zuletzt imagetechnischer Natur. Mitunter kann auch ihre Existenz auf dem Spiel stehen, denn Cyberversicherungen, die zumindest die gröbsten Kosten abdecken, bilden bei Unternehmen in Deutschland eher die Ausnahme (bei 30,5 Prozent). Allein im vergangenen Jahr entstand laut Bitkom ein Schaden von insgesamt rund 203 Milliarden Euro durch Cyberangriffe auf deutsche Unternehmen [2].

INCIDENT-RESPONSE-PROZESSE SIND BEI WEITEM KEIN NETTES BEIWERK, SONDERN EIN MUST-HAVE.

Kai Schuricht,
Lead Incident Response Specialist,
Kaspersky, www.kaspersky.de

UNTERSTÜTZUNG BEI DER VORFALLREAKTION

Kaspersky setzt als Cybersicherheitsanbieter sein gesamtes Wissen für die Etablierung einer robusten Cyberabwehr und Vorfallreaktionskapazität von Unternehmen ein.

- Die Kaspersky Incident Response Services [3] bewahren Unternehmen vor Cyberangriffen und ihren schwerwiegenden Folgen.
- Wie können interne Teams auf Cyberattacken richtig reagieren und schädliche Aktionen analysieren? Das Kaspersky Security Training [4] vertieft ihre Kenntnisse in den Bereichen Forensik und Incident Response. Außerdem werden Trainings zur Malware-Analyse und Reverse Engineering angeboten.
- Bei einem Sicherheitsvorfall unterstützt Kaspersky Unternehmen bei der aktiven Reaktion auf Angriffe und kann den gesamten Zyklus der Vorfalluntersuchung abdecken.

Basisschutz? Hälfte der Unternehmen in Deutschland ist vulnerabel
Grundsätzlich scheint es in den von Kaspersky befragten Unternehmen bereits am Basisschutz zu hapern. Demnach:

- fehlt in jedem dritten (35,5 Prozent) Unternehmen in Deutschland eine Passwort-Richtlinie.
- erstellen nur 58 Prozent von ihnen Backups.
- hat sich die wichtige Sicherheitsmaßnahme einer Multi-Faktor-Authentifizierung bis dato nur bei knapp mehr als der Hälfte (54 Prozent) etabliert.

Das Fehlen regelmäßiger Datensicherungen, kombiniert mit unzureichendem Passwort- und Zugangsschutz für Anwendungen sowie ungeschulten Mitarbeitern, machen es Unternehmen potenziellen Angreifern einfach, in das eigene Unternehmensnetzwerk einzudringen. Haben Cyberkriminelle erst mal eine Lücke im Netzwerk ausgemacht, können sie auf kritische Systeme und Tools oder sensible Informationen wie Kundendaten, Zahlungsinformationen oder Geschäftsgeheimnisse zugreifen.

Kritischer Faktor Zeit
Im Fall der Fälle sind Unternehmen im Vorteil, wenn sie einen klaren Maßnahmenplan aus der Schublade ziehen können – Stichwort Incident-Response-Plan und -Playbook. Je schneller Unternehmen auf den Vorfall reagieren, ihn eingrenzen und den Zugriff auf kritische Systeme und Daten abschneiden kann, desto mehr können die Konsequenzen eines Angriffs eingedämmt werden. Al-

lerdings dauert die Entdeckung in den meisten Fällen deutlich länger, als viele IT-Entscheider in Unternehmen wahrhaben wollen: 41,5 Prozent von ihnen sind zuversichtlich, dass ihr Sicherheitsteam einen kritischen Vorfall innerhalb von wenigen Minuten identifiziert. Allerdings zeigen Zahlen, dass wenn der ursprüngliche Zugriff auf das eigene Netzwerk nicht entdeckt wurde (was nicht selten vorkommt), meist mit einem ganzen Jahr bis zur Identifizierung gerechnet werden muss. Sehr viel Zeit, in der Cyberkriminelle mit gestohlenen Daten und kompromittierten Netzwerken Schaden anrichten können. Unternehmen müssen also ihre Vorfallentdeckungskapazitäten auf ein sehr hohes Niveau bringen.

Wie man Incident Response richtig etabliert

Incident-Response-Prozesse sind also bei weitem kein nettes Beiwerk, sondern ein Must-Have. Im Notfall sorgen sie dafür, dass Unternehmen schnell und effizient reagieren können. Denn die Methoden von Cyberkriminellen werden immer ausgeklügelter und schwerer zu enttarnen. Ihre Vorgehensweisen sind so zahlreich wie variabel: Spear-Phishing, Ransomware, DDoS-Attacken, Spyware, generische Malware und mehr.

Doch wie werden IR-Prozesse etabliert? Was sollte ein guter IR-Plan beziehungsweise ein IR-Playbook enthalten? Wird ein Unternehmen angegriffen, steht es vor zwei großen Herausforderungen: Einerseits gilt es den Schaden zu minimieren, andererseits so schnell wie möglich zum normalen Arbeitsablauf zurückzukehren. An dieser Stelle kommt Incident Response ins Spiel. Sie ermöglicht eine effiziente Reaktion auf den Sicherheitsvorfall (Vorfallreaktion), aber liefert darüber hinaus auch ein detailliertes Bild des Vorfalls. IR deckt den gesamten Untersuchungs- und Reaktionszyklus ab: von der frühen Reaktion auf Vorfälle und der Sammlung von Beweismitteln bis hin zur Identifizierung zusätzlicher Spuren von Hackerangriffen und der Erstellung eines Plans zur Angriffsabwehr.

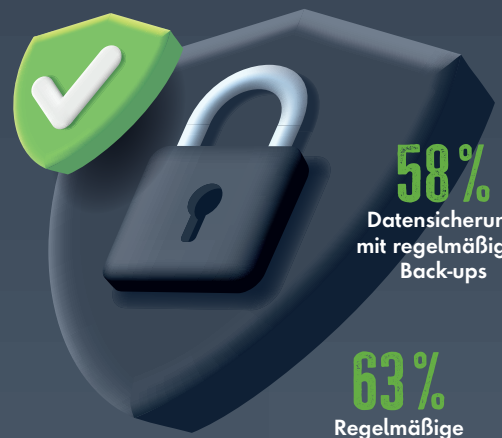
Unternehmen sollten in den folgenden Phasen die passenden Antworten parat haben:

- **Vorbereitung:** Incident Response sollte nicht nur als proaktive Reaktion auf einen Sicherheitsvorfall verstanden werden, sondern auch als präventive Maßnahme. Unternehmen bereiten sich allgemein auf den Ernstfall vor. Dazu gehören neben Incident-Response-Plänen und Playbooks auch Tabletop Exercises oder das Abschließen einer dedizierten Cyberversicherung.
- **Erkennung:** In dieser Phase wird ein Vorfall als solcher identifiziert und gemeldet sowie die ersten Informationen zum Vorfall gesammelt.
- **Schadensbegrenzung:** Basierend auf den vorhandenen Informationen wird der Vorfall eingedämmt, damit dieser sich nicht weiter im Unternehmensnetzwerk ausbreiten kann.
- **Beseitigung:** Mit der Schadensbegrenzung geht die Beseitigung des Angriffs einher. Vorhandene Schaddateien werden von den infizierten Geräten entfernt, diese Systeme mit weiteren Sicherheitsmaßnahmen gehärtet, Updates eingespielt und vorhandene Sicherheitslücken geschlossen.
- **Wiederherstellung:** In dieser Phase werden die Systeme wiederhergestellt, nachdem diese beispielsweise von der Infrastruktur getrennt wurden. Backups werden wieder eingespielt.
- **Lessons Learned:** Nach dem Angriff ist vor dem Angriff. Nach einem Vorfall werden alle unternommenen Schritte durchgegangen und rückblickend analysiert.

Kai Schuricht

Quellen:
[1] https://kas.pr/ir-report_de
[2] https://www.bitkom.org/Presse/Presseinformation/Wirtschaftsschutz-2022
[3] https://www.kaspersky.de/enterprise-security/incident-response
[4] https://www.kaspersky.de/enterprise-security/cyber-security-training

ZUR VORBEUGUNG VON CYBERSICHERHEITSVORFÄLLEN HABEN WIR FOLGENDE MASSNAHMEN IM UNTERNEHMEN IMPLEMENTIERT (AUSZUG):



65 %
Einrichtung und Kontrolle einer Kennwort-/ Passwortrichtlinie

55 %
Anti-Phishing-Software im Einsatz

54 %
Multi-Faktor-Authentifizierung implementiert

58 %
Datensicherung mit regelmäßigen Back-ups

63 %
Regelmäßige Mitarbeiterschulungen zu Cybersicherheitsthemen

Cyberabwehr

INVESTITIONEN IN GENERATIVE KI NEHMEN ZU

Deutsche Unternehmen wollen 2024 zunehmend in ihre Cyber-Security-Fähigkeiten investieren. Das ist eine zentrale Erkenntnis aus der jüngsten Ausgabe der jährlich erscheinenden globalen „Digital Trust Insights"-Studie. PwC hat für die Neuauflage der Untersuchung weltweit 3.876 Organisationen zu verschiedenen Aspekten der Cybersicherheit befragt. 84 Prozent der befragten Unternehmen aus Deutschland wollen ihr Budget für den Bereich um mindestens 5 Prozent erhöhen (global: 79 %). Eine Kürzung des Budgets planen hingegen nur 4 Prozent – im Vorjahr waren es noch 24 Prozent. Generative KI nimmt im Zuge der Investitionen eine wichtige Rolle ein: In Deutschland planen in den nächsten zwölf Monaten 75 Prozent der Befragten GenAI-Tools für die Cyberabwehr einzusetzen (global: 69 %).

Zunehmende Regulierung

Neben den erhöhten geopolitischen Risiken spielt auch die dynamische Regulierungslandschaft eine wichtige Rolle für den Anstieg der Cyber-Security-Budgets. So sieht beispielsweise die NIS-2-Richtlinie vor, dass Führungskräfte persönlich für die wirksame Beaufsichtigung von Cyber-Security-Risiken haftbar gemacht werden können. 84 Prozent der deutschen Unternehmen erwarten in diesem Zusammenhang erhöhte Compliance-Kosten (global: 75 %). Im Finanzsektor erfordert die DORA-Verordnung (Digital Operational Resilience Act) von Führungskräften ebenfalls eine höhere Aufmerksamkeit für digitale Risiken.

Finanzielle Schäden nehmen zu

Dem wachsenden Bewusstsein für die IT-Sicherheit im eigenen Unternehmen gehen vielerorts Sicherheitsvorfälle mit empfindlichen, finanziellen Schäden voraus. So sind in den letzten drei Jahren bereits bei 70 Prozent der befragten Unternehmen in Deutschland Kosten zwischen 100.000 und 20 Millionen US-Dollar entstanden.

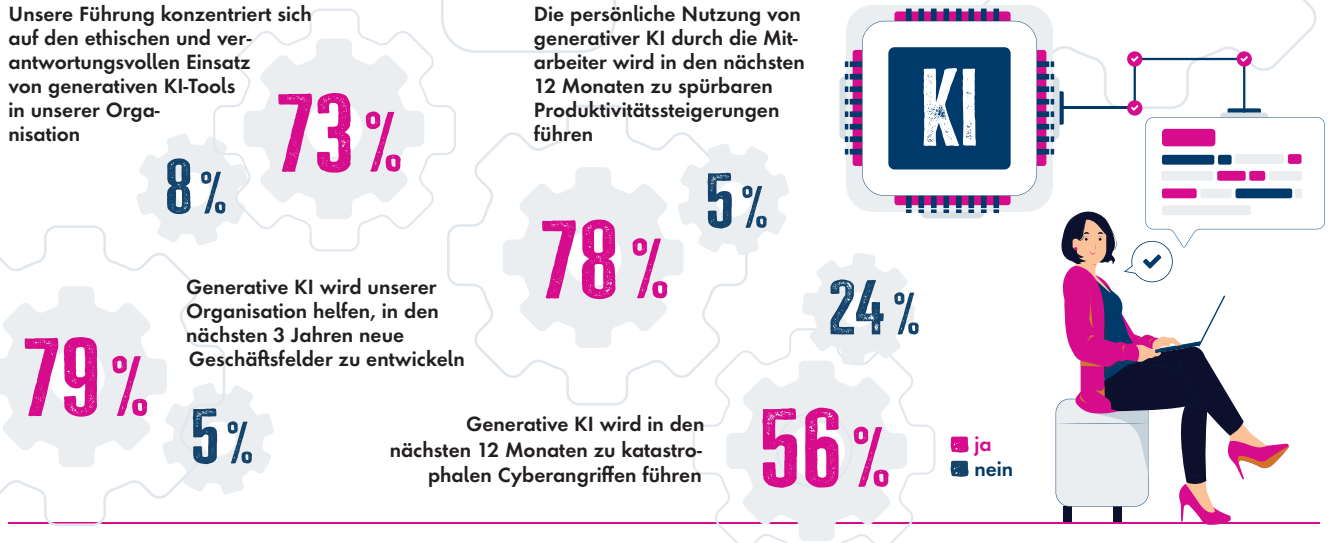
Um solche Schäden zu vermeiden und Cyber Security zu vereinfachen, setzen immer mehr Unternehmen auf integrierte Cyber-Technologie-Plattformen. 49 Prozent in Deutschland nutzen bereits vorrangig entsprechende Technologien, weitere 43 Prozent planen diesen Schritt in den nächsten zwei Jahren.

Cloud-Infrastrukturen

Cyberrisiken in Zusammenhang mit Cloud-Infrastrukturen bleiben sowohl global (47 %) als auch in Deutschland (52 %) die größte Sorge der Unternehmen. Darüber hinaus beurteilen 29 Prozent der Befragten in Deutschland auch die Kompromittierung ihrer Software-Lieferketten als ernstzunehmendes Risiko (global: 25 %). Weitere 24 Prozent fürchten Angriffe über Zero-Day-Schwachstellen (global: 17 %). Der Risikowahrnehmung entsprechend plant ein Drittel (33 %) der Unternehmen sowohl in Deutschland als auch weltweit, vermehrt in ihre Cloud Security zu investieren. Investitionen in die Anwendungssicherheit sowie die OT Security sind ebenfalls in vielen deutschen Unternehmen ein wichtiges Thema (41 % bzw. 36 %).

www.pwc.com

INWIEWEIT STIMMEN SIE DEN FOLGENDEN AUSSAGEN ÜBER GENERATIVE KI ZU ODER NICHT ZU?



Customer Identity and Access Management

DIE SCHLÜSSELTECHNOLOGIE FÜR OPTIMIERTE CYBERSICHERHEIT UND BENUTZERERFAHRUNG

Das Bundeslagebild Cybercrime 2022 des Bundeskriminalamts (BKA) zeigt, dass die Zahl der Cybercrime-Vorfälle weiterhin hoch ist. Im vergangenen Jahr registrierte die zuständige Behörde 136.865 Fälle von Cyberattacken. Doch das ist nur die Spitze des Eisbergs, denn das BKA schätzt das Dunkelfeld auf bis zu 90 Prozent. Umgerechnet bedeutet dies, dass nur jeder zehnte Fall tatsächlich angezeigt wird. Das Haupteinfallstor für Schadsoftware ist nach wie vor das Phishing. Um die Cybersicherheit zu erhöhen und Daten umfassend zu schützen, ist ein Customer Identity and Access Management (CIAM) unerlässlich. Gleichzeitig erwarten die Nutzer aber auch einen einfachen und nahtlosen Onboarding- und Login-Prozess. CIAM vereint beides, wie die Sicherheitsspezialisten der Nevis Security AG erklären.

CIAM unterstützt Unternehmen auch bei der Implementierung von robusten Sicherheitsrichtlinien, um sicherzustellen, dass sensible Informationen nicht in unbefugte Hände gelangen. Der Schutz sensibler Daten vor Verstößen und Angriffen von Cyberkriminellen ist entscheidend, um die Anforderungen der verschiedenen Datenschutzgesetze zu erfüllen. Darüber hinaus ermöglicht eine Single Source of Truth (SSoT), das heißt eine einzige zuverlässige und konsolidierte Datenquelle, Unternehmen wertvolle Einblicke in das Verhalten und die Interessen ihrer Kunden, denen sie außerdem ein hervorragendes Kundenerlebnis bietet.

Ein erfolgreiches Kundenerlebnis erfordert ein harmonisches Zusammenspiel von Sicherheit und Benutzerfreundlichkeit. Der Zugang zu persönlichen Nutzerdaten ermöglicht es Unternehmen, maßgeschneiderte und relevante Nutzererfahrungen anzubieten. Kunden sind jedoch nur dann bereit, ihre persönlichen Daten preiszugeben, wenn dies auf einer soliden Grundlage von Vertrauen und Sicherheit geschieht. Ein verbessertes Kundenerlebnis darf daher nicht auf Kosten der Sicherheit gehen und umgekehrt. Genau hier setzt CIAM an.

Risikominimierung im Fokus

CIAM basiert auf den Säulen Sicherheit, Skalierbarkeit, Compliance und Kundenzufriedenheit. Durch die Integration von CIAM-Lösungen in Kunden-Self-Service-Systeme, Zahlungsabwicklung, Auftragsverfolgung, Retourenmanagement und andere Bereiche können Unternehmen die Risiken minimieren, die mit schwachen oder wiederverwendeten Passwörtern verbunden sind.

EIN VERBESSERTES KUNDENERLEBNIS DARF NICHT AUF KOSTEN DER SICHERHEIT GEHEN UND UMGEKEHRT. GENAU HIER SETZT CIAM AN.

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

CIAM-Lösungen optimieren die Verwaltung digitaler Identitäten (Benutzer und ihre Daten) und Zugriffsrechte (Zuweisung von Zugriffsrechten auf bestimmte Daten/Informationen für bestimmte Benutzer), die von einem Unternehmen (oder einem externen Cloud-Anbieter) gesammelt und gespeichert werden. Digitale Identitäten ermöglichen den Kunden einen einfachen und sicheren Zugang zu ihren persönlichen Konten und Informationen und verschaffen Unternehmen die Möglichkeit, eine einzigartige und personalisierte Benutzererfahrung zu verwirklichen.

Um Cyberkriminellen das Handwerk zu legen, ist es wichtig, eine Lösung zu implementieren, die ihnen das Einfallstor verschließt. Zugleich dürfen die Sicherheitsmaßnahmen aber nicht zulasten des Kundenerlebnisses gehen. Mit einem CIAM-System sind Sie auf der sicheren Seite.

Stephan Schweizer

nevis®

Was Software „Made in Europe" besonders sicher macht

SECURITY UND DATENSCHUTZ SIND MILLIARDENFRAGEN

Open Source-Lösung oder etablierter Anbieter aus den USA? Oft sind es diese beiden Alternativen, die bei der Auswahl einer Software-Plattform für Digitalisierungsprojekte zu Beginn in den Raum gestellt werden. Beides hat seine Vor- und Nachteile, denkt man beispielsweise an Datenschutz, Nutzerkomfort oder Update-Sicherheit. Eine dritte, gleichwertige, wenn nicht sogar bessere Alternative wird häufig aber vergessen: Software „Made in Europe". Besonders bei Videokonferenzen sind deren Vorteile enorm.

Amerikanische Software?

Aus Nutzersicht ist Software amerikanischer Anbieter praktisch. Fast jeder kennt sie und ist mit der Bedienung vertraut. Die marktführenden Anbieter haben dazu beigetragen, gewisse Standards ihrer eigenen Produkte zu etablieren. Aus Unternehmenssicht gestaltet sich die Sache weniger einfach. Grundsätzlich ist jedes Unternehmen daran interessiert, durch gut funktionierende und bekannte Tools für hohe Produktivität zu sorgen. Spätestens seit der EU-Datenschutzgrundverordnung (DSGVO) aber sind Fragen des Datenschutzes für die Auswahl von Software immer relevanter. In Kombination mit der US-Rechtslage wirft der Einsatz amerikanischer Produkte komplexe Fragen auf. Der Patriot Act etwa verpflichtet US-amerikanische IT-Unternehmen, Methoden zur Datenerfassung oder Backdoors einzubauen, die zum Zweck der nationalen Sicherheit von US-Behörden genutzt werden können. Allein das kann mit Blick auf den Datenschutz zum Problem werden, natürlich können diese Schnittstellen aber auch als Angriffspunkt für Cyberkriminelle dienen.

Auch der US-amerikanische Cloud Act erlaubt es den amerikanischen Behörden, die Herausgabe von Daten über elektronische Kommunikation zu erzwingen. Dies ist mit der DSGVO logischerweise schwer vereinbar.

Open Source: Souveränität auf Kosten von Sicherheit?

Aus solchen Überlegungen heraus und zudem um nicht von einzelnen großen IT-Konzernen abhängig zu sein, überlegen viele Unternehmen, auf Open Source Software zu setzen. Auch Staat und Behörden sind an vielen Stellen an einer „souveränen Lösung" interessiert.

EINE SORGFÄLTIGE SUCHE BEI DER AUSWAHL VON SOFTWARE IST EINE INVESTITION, DIE UNTERNEHMEN IM ZWEIFELSFALL MILLIONEN SPART.

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

Dennoch ist Open Source nicht frei von Bedenken. Besonders problematisch ist häufig die Frage der Sicherheit. Es ist einfacher, eine Bank auszurauben, wenn man die Baupläne kennt. Im Fall von Open Source sind die Baupläne per Definition frei verfügbar, mit Vor- und Nachteilen für beide Seiten. Angreifer können sie lesen, um Schwachstellen zu finden, die Developer-Community kann sie nutzen, um sie zu schließen. Der Mehrzahl an Open Source-Projekten fehlt es aber an klaren Commitments und Roadmaps hinsichtlich Bugfixes und regelmäßigen Updates. Unternehmen können es sich nicht leisten, auf „Best Effort"-Lösungen zu setzen, denn die Anzahl an Cyberangriffen wächst und wächst. Die langfristige Versorgung mit Sicherheitsupdates ist ein absolutes Muss.

Auch mit unabhängigen und staatlichen Sicherheits-Zertifizierungen hat Open Source ein Problem: Meist gibt es keine, da Open-Source-Projekte weder TOE (Target of Evaluation) noch ST (Security Target) definieren, die von einer anerkannten Behörde getestet werden können. Somit haben Nutzer solcher Software keine Bescheinigung, dass diese gängige Sicherheitsstandards gewährleistet.

Im Hinblick auf Open Source ist auch der Cyber Resilience Act (CRA) von Bedeutung, den die EU initiiert hat. Dieser soll die Benutzer von Hard- und Software besser schützen. Anbieter müssten demnach für den gesamten Lebenszyklus und alle Verwendungen ihrer Software Sicherheitsupdates zur Verfügung stellen und bestimmte Richtlinien erfül-

Tixeo steht für maximale Sicherheit Made in Europe und Nutzerkomfort.

len. Für Open Source ist dies ein Problem, denn diese soll nur dann vom CRA ausgeschlossen sein, wenn sie für nichtkommerzielle Verwendung genutzt wird.

Die Vorteile von Software „Made in Europe"

Der dritte Weg, neben den beiden bisher diskutierten, ist Software „Made in Europe". Entgegen dem gängigen Vorurteil ist diese mindestens so leistungsfähig wie die Pendants amerikanischer Anbieter. Besonders bei Datenschutz und DSGVO-Komptabilität hat europäische Software meist deutliche Vorteile, da das Thema bei den Anbietern oft schon länger und präsenter im Bewusstsein ist. Und durch Hosting in Europe entfällt außerdem die Gefahr, dass Daten durch den Cloud Act an amerikanische Behörden gehen.

Auch hinsichtlich Cybersecurity lohnt sich der Blick auf europäische Anbieter. Sie erhalten ihre Sicherheitszertifikate von lokalen Behörden und nach lokalen Standards. Dies stellt sicher, dass die verwendete Software den nationalen Anforderungen und der Gesetzeslage entspricht.

Milliardenschäden durch Spionage

Besonders bei Videokonferenzen sind Security und Datenschutz Kernfragen. In der Bitkom-Studie zum Wirtschaftsschutz 2023 geben 80 Prozent der Unternehmen an, dass sie von Spionage oder Diebstahl betroffen oder wahrscheinlich betroffen waren. 61 Prozent berichten, dass Kommunikation via Messenger oder E-Mail ausgespäht wurde. Der deutschen Wirtschaft entstehen durch Cyberangriffe jährlich Schäden über 200 Milliarden Euro. Der Schutz der digitalen Kommunikation verdient oberste Priorität.

Der beste Weg dabei sind Anbieter wie Tixeo, die die einzige Videokonferenz-Technologie, die für ihre Ende-zu-Ende-Verschlüsselung von der ANSSI (Nationale Agentur für Computer- und Netzsicherheit Frankreichs) nach CSPN zertifiziert wurde, entwickelt haben.

Anders als bei vielen Anbietern sind bei Tixeo auch Konferenzen mit mehreren Teilnehmern durchgängig End-to-End verschlüsselt. Viele Videokonferenzlösungen geben an, eine End-to-End-Verschlüsselung zu bieten, verschlüsseln allerdings lediglich die Datenströme zwischen dem Benutzer und dem Kommunikationsserver. Sprich eine End-to-End-Verschlüsselung ist nur bei zwei Teilnehmern gegeben. Bei Tixeo dagegen werden Verschlüsselungsschlüssel mit der Konferenz erstellt und ausschließlich zwischen den Teilnehmern ausgetauscht. Es ist unmöglich, den Kommunikationsstrom zu entschlüsseln. Die End-to-End-Verschlüsselung ist eine der wirksamsten Maßnahmen zur Abwehr von Cyberangriffen. Damit ist sie der Grundpfeiler von Videokonferenzen, die eine vollständige Vertraulichkeit der Kommunikation gewährleisten können. Zudem werden mittels einer Multi-Cloud-Strategie alle Datenströme aus Meetings an verschiedenen Orten in Europa bei C5 zertifizierten Rechenzentren gehostet. Es besteht keine Verbindung zu Servern außerhalb Europas. Dadurch unterliegt der Anbieter keiner außereuropäischen Gesetzgebung, die die Vertraulichkeit der ausgetauschten Daten gefährdet.

Aus gutem Grund setzen Unternehmen und Organisationen aus sensiblen Zweigen wie Pharma, Rüstung, Behörden oder kritische Infrastruktur auf Anbieter wie Tixeo, die sich voll und ganz der Datensicherheit verschrieben haben. „Made in Europe" ist in diesem Fall die bessere Alternative zu Open Source oder gängigen amerikanischen Anbietern.

Eine sorgfältige Suche bei der Auswahl von Software ist eine Investition, die Unternehmen im Zweifelsfall Millionen spart. Der Schutz von Nutzern und Daten ist wichtig wie nie, gerade bei der Kommunikation.

Valentin Boussin

BYE, BYE, RANSOMWARE!

RANSOMWARE VERSTEHEN UND BEKÄMPFEN

Natürlich ist es immer besser, wenn man sein Hab und Gut aktiv verteidigt. Aber auch ein Plan B und C muss her, wenn der Worst Case doch eintritt. Wenn hier die Lösungen nicht greifen, dann bedarf es eines weiteren Plans.

Zum Minimum an Verteidigung gehören sicherlich regelmäßige Patches, Schwachstellenscanner sowie Firewall und EDR-Lösungen. Mittlerweile zählen auch Backupsysteme dazu. Dabei sollte man darauf achten, dass es unterschiedliche Backupsysteme sind, die auch physikalisch von den Servern getrennt sind.

Ein regelmäßiges Training der Mitarbeiter wird helfen, das Risiko von Phishing-Attacken weiter zu senken. Und: mittlerweile gibt es zusätzlich viele Ransomware-Module in EDR-Lösungen, die man nutzen sollte. Software zum Aufspüren von Anomalien und eine Netzwerksegmentierung sind weitere Gebote der Stunde.

Sicherheit hat oberste Priorität, und in der heutigen digitalen Ära ist der Schutz vor Ransomware-Angriffen von entscheidender Bedeutung. Unser brandneues eBook behandelt das wichtige Thema: „Ransomware verstehen und bekämpfen". In diesem umfassenden Leitfaden bieten wir Ihnen Einblicke, bewährte Praktiken und Strategien, um Ihr Unternehmen vor den verheerenden Auswirkungen von Ransomware zu schützen.

Das eBook umfasst 60 Seiten und steht kostenlos zum Download bereit: **www.it-daily.net**

RANSOMWARE 2023 – INHALT

- Cyberstorage: Schutz vor Ransomware-Angriffen
- Der Ransomware-Notfallplan
- Strategie: Auf Ransomware-Angriffe vorbereiten
- Zehn Ransomware-Tools: Ein Blick auf die Bedrohungslandschaft
- Wie moderne Backup Anwendungen Ransomwareschutz bieten
- Neu: Zero-Day-Ransomware-Schutz

Moderner Remote Access

WARUM AUCH NEUESTE CLOUD-INFRASTRUKTUREN VON VPN-INTEGRATION PROFITIEREN

Cyberangriffe verursachen so hohe Schäden wie noch nie zuvor – voraussichtlich 206 Milliarden Euro im Jahr 2023. Unternehmen setzen daher auf immer fortschrittlichere, cloudbasierte Security-Ansätze wie Zero Trust. Doch auch diese können noch optimiert werden – durch die Kombination mit einer zeitgemäßen, modernen VPN-Lösung. Wie dies in der Praxis aussieht, lesen Sie im Folgenden.

VPN mit Zero-Trust-Ansatz

Immer häufiger hört man in der IT-Security-Welt Begriffe wie „Zero Trust", „SD-WAN", „SASE" oder „SSO durch SAML". Dahinter verbergen sich aktuelle Cloud-Konzepte, -Technologien und -Standards, die den immer gerissener werdenden Cyberkriminellen die Stirn bieten sollen. Bei Zero Trust wird dafür der Zugriff der Nutzer nach dem „Least privilege"-Prinzip reglementiert. Wer für bestimmte Anwendungen nicht berechtigt ist, erhält auch keinen Zugriff. Auf diese Weise bieten Unternehmen potenziellen Eindringlingen wenig Angriffsfläche. Wenn sich ein Angreifer Zugang auf den Rechner eines Nutzers verschafft, hat er nur Zugriff auf die wenigen Daten, die dem jeweiligen Nutzer zur Verfügung stehen. Der IT-Admin kann den kompromittierten Bereich gezielt abkapseln und bereinigen.

Um diesen Security-Ansatz umzusetzen, benötigt man allerdings auch entsprechende Software-Produkte. Hier kommt modernes VPN ins Spiel: Fortschrittliche, softwarebasierte VPN-Lösungen wie die Secure Enterprise Produkte von NCP funktionieren bereits seit Jahren nach dem gleichen Prinzip. Per zentraler Management-Komponente wie dem NCP Secure Enterprise Management (SEM) definieren Administratoren alle Zugriffsrechte ihrer Nutzer mit wenig Zeitaufwand – und zwar nicht nur für Cloud-Applikationen, sondern IP-basiert für den gesicherten Netzwerkbereich.

MEHR WERT

Weitere Informationen zu modernem Remote Access von NCP finden Sie unter:
www.ncp-e.com/de/loesungen/cloud-vpn

Kompatibilität und Usability

Ein weiterer Vorteil moderner VPN-Lösungen: hohe Kompatibilität! Produkte wie die NCP Secure Enterprise Solution sind zu 100 Prozent softwarebasiert und können dadurch sowohl On Premises als auch im Rechenzentrum bei Managed (Security) Service Providern zum Einsatz kommen. Diese Funktionsweise macht die NCP-VPN-Produkte cloudfähig, wodurch sie lückenlos in SASE-, SSE-, Zero-Trust- und SD-WAN-Konzepte integriert werden können.

Hinzu kommt die „Usability" für Endanwender. Die Lösung muss unkompliziert im Hintergrund laufen und einfach zu bedienen sein. Bei den Enterprise-VPN-Produkten von NCP ist genau das der Fall. Das Zauberwort heißt: One-Click-Solution. Nach dem Start des Rechners muss der Mitarbeiter nur seine Anmeldeinformationen und gegebenenfalls einen zweiten Faktor eingeben - fertig. Damit startet der IP-basierte Netzzugriff über den Tunnel und parallel die nach Applikationen definierten Zugriffe im VPN-Bypass per Split-Tunneling.

Währenddessen profitieren auch IT-Administratoren von hohem Bedienkomfort. Dies äußert sich in der Praxis vor allem durch die Möglichkeit des zentralen Managements. Mit wenigen Mausklicks werden Nutzer in Benutzergruppen eingeteilt, Updates ausgerollt oder Firewall- und Zugriffsrichtlinien verteilt – entweder an einzelne Nutzer, bestimmte Abteilungen oder die gesamte Organisation. Umständliches und zeitraubendes Management einzelner Accounts entfällt damit vollständig, während IT-Admins mehrere hundert oder tausend Nutzer mit möglichst wenig Zeitaufwand administrieren können.

www.ncp-e.com

Üben ist das A und O

EFFEKTIVE NOTFALLÜBUNGEN STÄRKEN DIE UNTERNEHMENSRESILIENZ

Bild: alphaspirit – Stock.adobe.com

Betriebsunterbrechungen ereignen sich unerwartet und können Unternehmen schwer treffen. Um solche Situationen zu bewältigen, ist eine erprobte Krisenführung essenziell. Unternehmen sollten sich daher intensiv mit Notfällen und Krisenszenarien auseinandersetzen und ihr Notfall- und Krisenmanagement regelmäßig überprüfen. Viele Unternehmen besitzen zwar Notfallpläne, diese werden jedoch oft mangelhaft auf Umsetzung und Optimierung geprüft. Hier setzen Notfallübungen an. Die Durchführung solcher Übungen ist entscheidend, um die Wirksamkeit von Notfallabläufen und -maßnahmen zu überprüfen und zu verbessern.

Herausforderungen und Lösungen

Wie wichtig regelmäßiges Üben ist zeigt ein Praxisbeispiel aus dem Gesundheitswesen: Bei einer Notfallübung für einen Stromausfall in einem Krankenhaus trat tatsächlich ein Stromausfall auf. Im Verlauf der Übung versagte auch noch die Backup-Stromversorgung. Dies gefährdete Patientenleben und erschütterte das Vertrauen in das Krankenhaus. Durch regelmäßiges Üben hätte diese Schwachstelle des Notfallplanes rechtzeitig aufgedeckt werden können.

Die besten Übungen sind an realen Bedrohungs- und Krisenszenarien orientiert und bergen oft allerlei Überraschungsmomente bei der Durchführung. Solch umfangreiche Übungen tragen nicht nur dazu bei, Ängste und Unsicherheiten bei den Teilnehmern abzubauen, sondern decken in der Regel Schwachstellen in der Notfallplanung auf. Auch in der teamübergreifenden Kommunikation, an die in der Übung meist weniger gedacht wird.

Je umfangreicher die Übung ist, desto wichtiger ist die sorgfältige Planung und Vorbereitung.

Wichtige Vorbereitungsschritte für eine erfolgreiche Notfallübung sind:

- Identifikation von Notfallszenarien: Potenzielle Bedrohungen und Notfallsituationen müssen identifiziert, beschrieben und basierend auf Relevanz und Wahrscheinlichkeit für die Übung ausgewählt werden.
- Berücksichtigung von Vorgaben: Je nach Regulierung oder Zertifizierung können bestimmte Übungsarten erforderlich sein.
- Jahresplanung: Jedes Ausfall- und Bedrohungsszenario sollte mit entsprechenden Übungen jedes Jahr geübt werden, um Audit-Anforderungen zu erfüllen.
- Klare Ziele setzen: Die Ziele jeder Übung, wie Testen von IT-Hot-Standby oder Evakuierung, müssen klar definiert werden.
- Übungskonzept erstellen: Ein detailliertes Konzept beschreibt alle Übungsschritte und berücksichtigt Abhängigkeiten und Aufwände.
- Aktionsplan und Drehbuch: Ein Plan mit Details zu Datum, Zeit, Beteiligten, Rollen und Verantwortlichkeiten wird erstellt.
- Sicherheitsvorkehrungen prüfen: Sicherheitsmaßnahmen im Unternehmen werden überprüft und an Standards angepasst.
- Übung durchführen: Die Übung wird gemäß Plan durchgeführt, unter Einbeziehung aller relevanten Aspekte.
- Auswertung und Feedback: Die Übung wird bewertet, Ergebnisse analysiert, Verbesserungspotenzial

identifiziert und erforderliche Maßnahmen geplant.

Optimierung durch BCM-Tools

Business Continuity Management (BCM)-Tools wie HiScout erleichtern die Vorbereitung und Durchführung von Notfallübungen. Sie bilden nicht nur den gesamten Prozess des Business Continuity Managements ab – von der Business-Impact-Analyse (BIA) über die Geschäftsfortführungsplanung bis hin zur Notfallvorsorge und Notfallbewältigung. Diese Tools bieten Dokumentation, Vorgangsmanagement und Rückverfolgbarkeit von Maßnahmen. Erkenntnisse, Handlungsempfehlungen und Maßnahmen aus absolvierten Übungen können ebenso darin festgehalten werden wie deren Umsetzungspflege und -nachweise. Gute Tools spiegeln die erreichten und durch die Übung verifizierten Wiederherstellungszeiten von zum Beispiel IT-Services in den Soll-Ist-Vergleich zurück und können dadurch kontinuierliche Verbesserungen identifizieren und aufzeigen.

Fazit

Notfallübungen sind entscheidend, um Unternehmen widerstandsfähiger zu machen und im Ernstfall effizient handeln zu können. Die Herausforderungen reichen von fehlender Vorbereitung bis zu mangelnder Koordination. Die sorgfältige Planung und Durchführung von Übungen ist entscheidend für die Unternehmensresilienz. Die Einbeziehung eines geeigneten BCM-Tools, erleichtert nicht nur die Übungsplanung sondern unterstützt den kontinuierlichen Verbesserungsprozess und macht diesen auch sichtbar.

Silke Menzel

NOTFALLÜBUNGEN SIND ENTSCHEIDEND, UM UNTERNEHMEN WIDERSTANDSFÄHIGER ZU MACHEN UND IM ERNSTFALL EFFIZIENT HANDELN ZU KÖNNEN.

Silke Menzel, Projektmanagement, HiScout GmbH, www.hiscout.com

AUTHENTIFIZIERUNG

VERBRAUCHER FORDERN PASSWORTALTERNATIVEN

Die Befragung von mehr als 10.000 Verbrauchern im Rahmen des Online-Authentifizierungsbarometers der FIDO Alliance hat ergeben, dass die manuelle Eingabe von Passwörtern ohne zusätzliche Sicherheitsmaßnahmen mit rund vier Anwendungen pro Tag die am häufigsten genutzte Authentifizierungsmethode ist. Dazu zählt der Zugriff auf Arbeitscomputer und -konten (37 %), die Verwendung von Streaming-Diensten (25 %), sozialen Medien (26 %) und Smart-Home-Geräten (17 %).

Und das, obwohl Verbraucher sichere Login-Optionen bevorzugen: Bei der Frage ihrer persönlichen Präferenz und der höchsten Sicherheit haben die meisten Befragten die biometrische Authentifizierung angegeben. Finanzdienstleistungen sind jedoch der einzige Bereich, in dem die Verbraucher biometrische Verfahren (33 %) tatsächlich häufiger nutzen als Passwörter (31 %).

Passwörter als Haupthindernis

Aufgrund veralteter Authentifizierungsmethoden haben 59 Prozent der Befragten in den letzten 60 Tagen den Zugriff auf einen Onlinedienst abgebrochen, 43 Prozent einen Kauf. Die Häufigkeit stieg im Vergleich zum Vorjahr um 15 Prozent auf rund viermal pro Monat und Person. 70 Prozent der Verbraucher mussten zudem in den letzten zwei Monaten ihre Passwörter zurücksetzen, weil sie diese vergessen hatten.

„Das Interesse der Verbraucher an sichereren Authentifizierungsmethoden wächst. Sie unterstreichen jedoch auch, dass das Potenzial der passwortlosen Authentifizierung noch nicht ausgeschöpft ist, denn Verbraucher sind oftmals nach wie vor auf weniger sichere Methoden angewiesen", so Andrew Shikiar, Executive Director und CMO der FIDO Alliance.

www.fidoalliance.org

Multifaktor Authentifizierung

SCHWACHSTELLEN ERKENNEN

Seit der flächendeckenden Einführung von Multifaktor-Authentifizierungsprodukten in einer Reihe von Unternehmen und IT-Produkten sowie Portalen häufen sich die Vorfälle, bei denen die Maßnahmen umgangen werden. Angreifer haben sich mittlerweile darauf spezialisiert, mit mehreren Authentifizierungsstufen umzugehen. Es ist zunehmend üblich, dass Angreifer QR-Codes oder Bilder verwenden, um Opfer in die Irre zu führen. In den Betreffzeilen von Phishing-E-Mails wird oft der Name bekannter Marken oder Unternehmen missbraucht, um die Aufmerksamkeit zu erregen.

Folgende Methoden sind mittlerweile verbreitet:

- Bilder anstelle von Text
- QR-Codes anstelle von infizierten Links und Anhängen
- Zufallsgenerierung von „Absender"-Namen und E-Mail sowie Verschlüsselung mit SHA-256
- Manipulation von Betreffzeilen zur Verfälschung von Authentifizierungsdaten (SPF, DKIM, ...)

Auf diese oder ähnliche Art überlisten Angreifer vorhandene Filter und andere technische Schutzmaßnahmen, sodass Phishing-E-Mails im Posteingang der Mitarbeiter landen.

Im September hatte der Anbieter von Identitäts- und Authentifizierungsmanagement Okta vor Social-Engineering-Angriffen gewarnt, die die Mehrfaktor Authentifizierung umgehen. Diese Angriffe zielen auf IT-Mitarbeiter ab und versuchen, Administratorrechte zu erlangen, um Unternehmensnetzwerke zu infiltrieren und zu übernehmen.

Mehrere Unternehmen in den USA waren von wiederholten Social Engineering-Angriffen auf IT-Service-Desk-Mitarbeiter betroffen. Bei diesen Angriffen versuchten die Angreifer, die Mitarbeiter des Service-Desks dazu zu bringen, alle Mehrfaktor-Authentifizierungsfaktoren (MFA), die von hoch privilegierten Benutzern eingerichtet wurden, zurückzusetzen. Nachdem die hoch privilegierten Okta-Superadministrator-Konten kompromittiert waren, scheinen die Angreifer diese Situation auszunutzen, um legitime Identitätsföderationsfunktionen zu missbrauchen. Dadurch konnten sie sich innerhalb der infiltrierten Organisation als berechtigte Benutzer ausgeben.

Sensibilisierung schützt

Nach Angaben des MFA-Anbieters verfügten die Angreifer bereits über einige Informationen über die Zielorganisationen, bevor sie die IT-Mitarbeiter kontaktierten. Es scheint, dass sie entweder im Besitz von Passwörtern für privilegierte Benutzerkonten sind oder die Fähigkeit besitzen, den Authentifizierungsfluss über das Active Directory zu beeinflussen. Dies tun sie, bevor sie den IT-Service-Desk einer Zielorganisation kontaktieren und das Zurücksetzen sämtlicher MFA-Faktoren des Zielkontos anfordern. Bei den betroffenen Unternehmen hatten sie es speziell auf Nutzer mit Superadministrator-Rechten abgesehen. Darüber hinaus gaben sie sich außerdem mit einer gefälschten App als ein anderer Identitätsmanagement-Anbieter aus.

Eine wirksame Methode, um das eigene Unternehmen trotz kompromittierter MFA zu schützen, sind Schulungen zur Sensibilisierung für Sicherheitsfragen. Mitarbeiter aus allen Abteilungen können dadurch lernen, Social-Engineering-Taktiken zu erkennen und sich vor zielgerichteten Angriffen auf ihre Konten, sei es per E-Mail, in Teams-Chats oder in sozialen Medien, zu schützen.

Dr. Martin Krämer | www.knowbe4.de

Software-Schwachstellen

FÜNF WEGE, UM BEI DER BEHEBUNG VON SICHERHEITSPROBLEMEN EINEN VORSPRUNG ZU HABEN

Die Behebung von potenziellen Software-Schwachstellen ist eine der besten Möglichkeiten, Angriffe zu verhindern. Viele der IT-Probleme, sind bekannte Software-Schwachstellen - in der diesjährigen Top 20-Liste des Qualys Security Vulnerability Research gehören zu den fünf häufigsten Exploits ein Problem mit der Privilege Escalation im Zerologon-Protokoll, Probleme mit Remotecodeausführung (RCE) in MS Office und Wordpad aus dem Jahr 2017 und sogar ein RCE mit Microsoft Windows Common Controls aus dem Jahr 2012. Diese Probleme wurden 2023 von Bedrohungsakteuren ins Visier genommen.

Warum sind diese Probleme Jahre nach der Veröffentlichung von Patches noch immer da? Auch wenn Abhilfemaßnahmen bekannt sind, stehen andere Dinge im Weg. Deshalb ist es ist wichtig, die Prozesse rund um die Fehlerbehebung zu verbessern:

#1 Überprüfen Sie Ihre Systemimages und Vorlagen

Um die Verwaltung Ihrer IT-Systeme zu erleichtern, verfügen Teams über eine Reihe von Basis-Images, die sie verwenden. Diese Images können die Bereitstellung neuer Endpunkte oder Cloud-Server erleichtern; für Anwendungen, die in Containern in Cloud-Umgebungen ausgeführt werden, sind diese Images als Teil Ihrer Bereitstellungspipeline unerlässlich. Diese Images müssen auch aktuell gehalten werden, da sie sonst alte Schwachstellen in ihre Umgebungen einbringen können.

#2 Automatisieren Sie Ihre Patching-Prozesse für weniger kritische Anwendungen

Ihre Assets bestehen aus Software und Diensten - einige davon sind für den Betrieb Ihres Unternehmens von Bedeutung, andere weniger. Bei den Anwendungen mit geringem Risiko sollte die Bereitstellung von Updates automatisiert werden. Durch die automatisierte Bereitstellung von Patches werden Aktualisierungen von Drittanbietern von der Liste gestrichen, so dass mehr Zeit für das Testen von Patches für kritischen Anwendungen bleibt.

#3 Überprüfen Sie die Genauigkeit bei der Anzahl der Schwachstellen

In einem Unternehmen gab es eine Liste von Sicherheitslücken, die immer gleichblieb, egal wie viele Updates bereitgestellt wurden. Die Experten fanden heraus und waren überrascht: die Liste der Schwachstellen war nicht korrekt. Dafür gibt es mehrere Gründe – zum Beispiel kann es virtualisierte Desktop-Umgebungen geben, die immer neu gebootet werden und bei denen nicht die neuesten Updates installiert sind. Oder es gibt stillgelegte Anlagen, die mitgezählt werden.

#4 Überprüfen Sie, was das Problem verursacht

Die Anzahl der Schwachstellen hängt davon ab, welche Software Sie einsetzen. Wichtig ist zu wissen, welche Schwachstellen vorliegen und ob die Software auf den Geräten noch benötigt wird, etwa veraltete Browser-Versionen, die auf den Geräten installiert waren. Diese Browser waren auf Servern installiert, auf denen die Software nicht benötigt wurde. Durch die Deinstallation wurde die Zahl der Installationen verringert.

#5 Sicherstellen, dass Aktualisierungen abgeschlossen werden

Der Abschluss einer Patch-Bereitstellung ist umfangreicher als das Ausrollen eines Updates. Um den Prozess zu beenden, muss das Systems oft neu gestartet werden. Dies ist problematisch, wenn die Anwendung geschäftskritisch ist. So kann es schwierig sein, ein Neustart durchzusetzen. Ein Blick auf die möglichen Auswirkungen kann helfen, das Risiko zu beheben, anstatt mit unsicheren Systemen weiterzuarbeiten. Durch die Kombination dieser Schritte können Sie die Effektivität und Effizienz Ihrer Patching- und Abhilfemaßnahmen verbessern.

Karl Alderton

Qualys.

EDR/XDR und Antivirensoftware

WAS IST DER UNTERSCHIED?

Begriffe wie „NGAV" („Next-Generation Antivirus"), „EPP" („Endpoint Protection Platform") und „EDR" („Endpoint Detection and Response") gewinnen immer mehr an Bedeutung. Doch wie unterscheiden sich diese Technologien von herkömmlichen Antivirenprogrammen? Sind letztere überhaupt noch erforderlich?

Fast ein Jahrzehnt nach dem angekündigten Ende traditioneller Antivirenprogramme stehen selbige bei der breiten Öffentlichkeit nach wie vor hoch im Kurs. Erstmals im Jahr 1987 von der Firma IBM als Antwort auf das Computervirus „Brain" entwickelt, wurde der Begriff Antivirus im Laufe der Jahre durch viel Werbung populär und bildete in der Vorstellung der breiten Öffentlichkeit den einzigen Schutz vor Computerviren.

EINE XDR-PLATTFORM BIETET EINEN GESAMTÜBERBLICK ALS KORRELATIONSPLATTFORM UND TRÄGT DAZU BEI, DAS RISIKO ZU MINDERN, AUF VORFÄLLE ZU REAGIEREN UND SIE ZU BEHEBEN.

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

Ähnlich wie ein Impfstoff verfügt ein Antivirenprogramm über eine Signaturdatenbank, mit der es Computerviren anhand deren Signaturen (Fingerabdrücke) erkennen kann. Das bedeutet aber, dass das Virus zunächst bekannt sein soll, bevor man seine Signatur identifizieren (und den Schädling bekämpfen) kann. Die zweite und wichtigste Einschränkung ist das Aufkommen des Polymorphismus, einer Technologie zur Erzeugung von mehreren Schadsoftwares, die zwar jeweils über eine einzigartige digitale Signatur verfügen, deren Infektionsmethode und Auswirkungen jedoch gleich sind. Diese Einschränkung wird umso prägnanter, da laut dem Institut AV-TEST fast 4 Millionen neue Malware-Programme pro Monat entwickelt werden. Darüber hinaus nutzen Cyberkriminelle zunehmend blinde Flecken in den Erkennungsalgorithmen aus, etwa bei Angriffen ohne Dateien („fileless malware"). Das Ergebnis: Ausschließlich auf Signaturen beruhende Erkennungsmechanismen lassen die Mehrheit der Malware durch und müssen unbedingt durch andere Sicherheitstechnologien ergänzt werden.

Die Raffinesse von Cyberangriffen reicht sogar so weit, dass AV-Programme selbst zur Zielscheibe werden. Auf der Konferenz Black Hat Europe im Dezember 2022 enthüllte ein Sicherheitsforscher beispielsweise eine neue Schwachstelle, die mehrere Antivirenprogramme betraf. Diese ermöglicht es, Antivirensoftware zu kapern und sie dazu zu bringen, legitime Dateien zu löschen. Was kann man also tun, wenn das wichtigste Schutzinstrument seine Funktion nicht mehr erfüllt?

Der Einzug der Verhaltenserkennung

Um auf diese Bedrohung zu reagieren, mussten die Hersteller von Cybersicherheitslösungen umdenken und von der Suche nach Fingerabdrücken zur heuristischen Analyse auf der Grundlage des Malwareverhaltens wechseln. Unter dem Namen „Next Gen Antivirus" oder NGAV bildeten diese neuartigen Antivirenprogramme die Grundlage für das spätere Konzept der EPP („Endpoint Protection Platform"). EPP-Lösungen waren eine erste Antwort auf Polymorphismus und dateilose Angriffe, indem sie neue Funktionen wie Speicherüberwachung, Verhaltensanalyse oder die Überprüfung von Kompromittierungsindikatoren (IoCs) integrierten. Trotzdem schlüpften heimtückische Cyberangriffe weiterhin durch die Maschen des Sicherheitsnetzes. So tauchten im Jahr 2013 ETDR-Lösungen („Endpoint Threat Detection & Response") zur Incident-Response und Investigation auf. Ab 2015 wurde das Akronym ETDR durch EDR für „Endpoint Detection & Response" ersetzt.

Die Besonderheit des neuen Ansatzes liegt in der Fähigkeit, unbekannte Bedro-

hungen zu erkennen und in Echtzeit halb autonom darauf zu reagieren: Wenn eine Bedrohung erkannt wird, blockiert die EDR-Lösung die Ausführung des Programms im Vorfeld manchmal via Quarantäne. Sie unterstützt also Einsatzteams dabei, eine weitere Ausbreitung der Infektion zu verhindern und Nachforschungen anzustellen. EDR- und EPP-Lösungen sind dabei komplementär: Wenn man eine Parallele zur physischen Sicherheit eines Unternehmens ziehen möchte, so sind EDR-Lösungen die Überwachungskameras. Mit ihnen kann man sehen, ob etwa eine Person in Ihr Firmengelände eindringt. Aber um den Eindringling schon am Eingang abzuwehren, benötigt man einen Wachmann vor Ort, das ist dann ein EPP.

Der Bedarf an Antivirenprogramme besteht aber nach wie vor. Sie stellen eine erste Sicherheitsebene dar: Selbst wenn sie nicht gegen alle Cyberangriffe wirksam sind, bieten sie dennoch einen ersten Schutz vor weniger raffinierten Angriffen, sorgen für die Verringerung, gar Vermeidung von False Positives und verbrauchen geringe Ressourcen auf dem Computer. Eine erste Sicherheitsebene allein reicht jedoch nicht aus. Demnach werden in Unternehmen des Öfteren auf demselben Computer mehrere Sicherheitslösungen installiert. Eine Kombination, die sich aber nicht immer gut verträgt. Einige Konstellationen können zu Konflikten führen, wodurch Cyberkriminellen eine weitere Tür geöffnet wird.

NDR, XDR, MDR

Trotz der versprochenen Autonomie solcher Lösungen müssen diese Tools von Experten betreut werden, wie die Entwicklung von Angeboten für Managed EDR oder Mini-SOCs zeigt. Neben der Verbesserung der Erkennung müssen Tools zum Endpunktschutz unbedingt auch über die Fähigkeit verfügen, Vorfälle zu erkennen und darauf zu reagieren. Und da es immer mehr Sammelstellen für Vorfälle gibt, müssen SOC-Analysten Zugriff auf alle Netzwerk- und Infrastrukturgeräte haben. So analysieren NDR-Lösungen („Network Detection and Response") die TCP/IP-Pakete, die über das Netzwerk versendet werden, um verdächtige Aktivitäten zu erkennen, während XDR-Plattformen („eXtended Detection and Response") dazu dienen sollen, alle internen und externen IT-Assets zusammenzuführen. Eine XDR-Plattform bietet diesen Gesamtüberblick als Korrelationsplattform und trägt dazu bei, das Risiko zu mindern, auf Vorfälle zu reagieren und sie zu beheben. Unabhängig von Tools und Technologien sollte man sich allerdings stets vor Augen halten, dass Analysten weiterhin eine zentrale Rolle spielen und dass keine Technologie allein sensible IT-Systeme oder Daten schützen kann.

In einer Studie der Organisation Survey Risk Alliance gaben nur 12 Prozent der Fachleute für Cybersicherheit an, dass sie bis 2022 eine XDR-Lösung in ihrer Organisation eingeführt hatten. Die übrigen 78 Prozent sagten, dass sie die Einführung in den nächsten 24 Monaten planten. Die Nachfrage nach Sicherheitsfachleuten, die sich auf die Erkennung von und die Reaktion auf Vorfälle spezialisiert haben, dürfte folglich in den nächsten Jahren weiter steigen. Diese Fähigkeiten werden dringend benötigt, um mit der ständigen Weiterentwicklung cyberkrimineller Vorgehensweisen Schritt zu halten, und ihre Dienste werden für Unternehmen wahrscheinlich leichter zugänglich sein, wenn sie Managed EDR oder Mini-SOCs nutzen.

Uwe Gries

Unified Endpoint Management

AUS DEM SCHATTEN INS LICHT

Private USB-Sticks, Notebooks und Smartphones mit Firmen-E-Mail-Zugang ohne Freigabe – sie sind nur der sichtbare Teil der sogenannten Schatten-IT, dem Graus jeder IT-Abteilung. Hinzu kommen Softwareprogramme, die ohne nachzufragen installiert wurden. Dahinter steckt nicht unbedingt böser Wille. Vielmehr geht es oft nur darum, tatsächliche (oder vermeintliche) Mängel der zentralen Informationssysteme zu umgehen, um effizienter arbeiten zu können oder eigene Bedürfnisse zu erfüllen.

So oder so: Nicht genehmigte Soft-, Hardware oder andere IT-Ressourcen bleiben ein Problem, denn den Vorteilen stehen vielfältige Nachteile, ja sogar erhebliche Risiken für das Unternehmen gegenüber: Nicht lizenzierte Programme ziehen nicht nur Strafzahlungen nach sich. Dadurch, dass keine Updates aufgespielt werden, öffnen sich auch schnell Sicherheitslücken. Programme aus fragwürdigen Quellen enthalten unter Umständen Schadsoftware oder laden solche nach. Private USB-Sticks werden zudem oft von Viren befallen, die sich dann im gesamten Firmennetz ausbreiten. Und da sie in der Regel nicht verschlüsselt sind, droht Datenverlust, wenn sie verloren gehen.

IT-Ressourcen überwachen...

Unternehmen sollten Richtlinien und Prozesse zur Genehmigung und Überwachung von IT-Ressourcen einführen. Die IT-Abteilung muss zudem stets ein Ohr an den Beschäftigten haben, um deren Bedürfnisse mit Sicherheit und Compliance in Einklang zu bringen. Schulungen und Sensibilisierungsmaßnahmen tragen dazu bei, das Bewusstsein für die Risiken von Schatten-IT zu schärfen.

Vor allem sollte jede IT-Abteilung die hauseigene Infrastruktur regelmäßig überprüfen, um potenzielle Schatten-IT-Systeme zu identifizieren und zu kontrollieren. Eine Lösung für Unified Endpoint Management (UEM) stellt dafür das notwendige Instrumentarium bereit.

MEHR WERT

Kostenlose Testversion
www.aagon.com/testversion

... durch Sensibilisierung und Technologie

Aagon ermöglicht schon mit dem Kernmodul seiner ACMP Suite eine vollständige Inventarisierung aller Hard- und Software und ihre zentrale Einbindung in eine Management Console. Dafür installiert die Software einen Agenten auf jedem Client. Die Client-Software hält die Kommunikation zwischen lokalem Rechner und ACMP Server aufrecht, liefert in frei definierbaren Intervallen Inventardaten an den Server und nimmt in der anderen Richtung Aufträge entgegen. Bereits nach wenigen Augenblicken stehen über 150 Hardware-Daten und sämtliche Details der Windows-Installation auf dem Server zur Verfügung. Regelmäßige Reports sorgen dafür, dass Änderungen sofort auffallen.

Ein weiteres Modul für das Asset Management inventarisiert alle Anlage- und Sachgüter im Unternehmen, fasst sie in logische Gruppen zusammen und ordnet Standort, Besitzer und Status einander zu. Unter- oder Überlizenzierung erkennen IT-Abteilungen mithilfe eines speziellen Lizenzmanagement-Moduls. Entscheidungen über Nachkaufen oder Deinstallieren sind damit schnell getroffen.

Das ACMP Bitlocker Management der UEM-Lösung schützt gegen unautorisierte USB-Sticks. Mit diesem Modul ergänzt Aagon den Microsoft BitLocker um Funktionen zur zentralen Verwaltung der Festplattenverschlüsselungen. Es erlaubt Statusabfragen von Schlüsselschutzvorrichtungen und gibt einen Überblick über BitLocker-fähige Clients. Im Verbund mit weiteren Modulen der UEM-Plattform für automatisches Patchen von Third Party Software mit qualitätsgesicherten Paketen und Desktop Automation über Client Commands führen Unternehmen ihre bisherige Schatten-IT damit ans helle Tageslicht.

www.aagon.com

Wissen, was geht

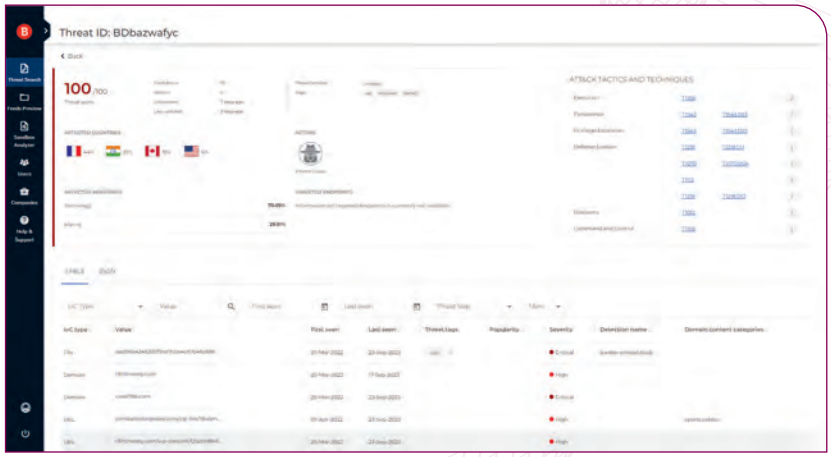
THREAT INTELLIGENCE FÜR EINE PROAKTIVE GEFAHRENABWEHR

IT-Sicherheitsverantwortliche brauchen aktuelle Informationen über die Sicherheitslage, um Unternehmen proaktiv schützen zu können. Mit Threat Intelligence können sie dies wirksam erreichen – egal ob in Eigenregie oder durch den beauftragten Dienstleister wie etwa ein MSSP.

Zu einer umfassenden IT-Sicherheitsstrategie gehören zahlreiche Abwehrtechnologien: Endpunktschutz, Firewalls verschiedenster Ausprägung, Intrusion Detection & Prevention, VPNs, Web-Proxies, Mails-Security-Gateways, Zugangskontrollen oder Schwachstellen-Erkennung bis hin zum Management all dieser Sicherheitslösungen. Ebenso wichtig sind die damit verbundenen Prozesse wie das Patch-Management, Reaktionen auf Vorfälle, Desaster-Recovery oder Forensik – um nur einige zu nennen. Wie komplex diese Einzelbausteine einer Defensive auch sind – sie lassen sich nur mit relevanten Echtzeit-Informationen zur aktuellen Gefahrenlage bestmöglich betreiben. Threat Intelligence ermöglicht eine schnelle und präzise Beurteilung der individuellen Bedrohung, kann aktuelle Gefahren vorhersehen, abwehren oder deren Effekte auf das Netzwerk abschwächen. Von den umfangreichen Erkenntnissen und Informationen einer Threat-Intelligence-Lösung profitieren sowohl große Unternehmen mit eigenem Security Operation Center, Anbieter von Managed Security Services (MSSP) oder auch kleinere Unternehmen, die auf ein externes verwaltetes SOC bzw. einen Managed Detection and Response-Dienst (MDR) zugreifen.

Ein Emotet-Threat-Profil in Bitdefender Threat Intelligence.

Quelle: Bitdefender



Informationen als Basis für die Defensive

Threat Intelligence basiert auf Telemetriedaten von weltweit hunderten Millionen von aktiven Endpunkten. Zu dieser Telemetrie gehören nicht nur physikalische Endpunkte, sondern auch erweiterte Cloud-Instanzen oder IoT-Systeme. Diese unterschiedlichen Quellen liefern Details über beobachtetes Verhalten, schreiben cyberkriminelle Angriffe den richtigen Urhebern zu und verorten die Effekte eines Angriffs in MITRE. Informationen zur geographischen Verbreitung und zu von den Angreifern bevorzugten Plattformen zeigen zudem auf, wie wahrscheinlich ein Angriff auf das jeweilige eigene Unternehmen ist.

Nur wenn aktuelle Informationen in einen aussagekräftigen Kontext gestellt und mit dem Verhalten eines Bedrohungsmusters korreliert werden, lassen sich potenzielle Angriffe frühestmöglich erkennen. Auf Grundlage der vielen Informationen erstellen Experten Risikoprofile etwa für Ransomware-Attacken gegen Behörden: Daten über die Herkunft stattfindender Angriffe und die Art der Informationen, auf die Hacker zielen, liefern die Argumente, strengere Zugriffsregeln in der betroffenen Region und für die jeweiligen Informationen oder Systeme zu begründen und durchzusetzen.

Threat Intelligence unterstützt die Prävention komplexer Angriffe, wie etwa mehrstufige Attacken auf Zero-Day-Schwachstellen. Diese werden oft erst nach längerer Zeit bekannt, obwohl die betreffende Lücke schon seit Erscheinen der jeweiligen Software existiert. Unter Umständen haben Hacker bereits unauffällig Daten exfiltriert oder manipuliert.

Von der Reaktion zur Prävention

Der kontinuierliche Informationsfluss durch Telemetriedaten liefert in Echtzeit eine stets aktuelle Datenbasis zur aktiven Gefahrenlage. Aus Kontextinformationen zur Bedrohung in Bezug auf die IT des Unternehmens leiten Abwehrexperten dann ein für jedes Unternehmen in jeder Branche relevantes und aktuelles Risikoprofil ab. Der IT-Sicherheitsdienstleister oder die interne IT können präventiv die Abwehr steuern, ohne sich mit False Positives aufzuhalten.

Jörg von der Heydt | www.bitdefender.de

IT-Sicherheit im Mittelstand

DREI SCHLÜSSELERKENNTNISSE FÜR DEN SCHUTZ IHRES UNTERNEHMENS

Cyberangriffe sind nicht nur ein Problem für große Konzerne. Kleine und mittelständische Unternehmen (KMU) sind genauso gefährdet, verfügen jedoch oft über begrenzte Ressourcen und Fachwissen, um sich effektiv zu schützen. Wie steht es um die IT-Sicherheit im Mittelstand? Wie können KMU ihr Unternehmen trotz begrenzter Budgets und Personal schützen? Eine aktuelle Neuauflage der Studie „IT-Sicherheit im Mittelstand", die erstmals 2019 durchgeführt wurde, beleuchtet diese Fragen und zeigt drei entscheidende Erkenntnisse, die Unternehmen berücksichtigen sollten.

Erkenntnis 1:

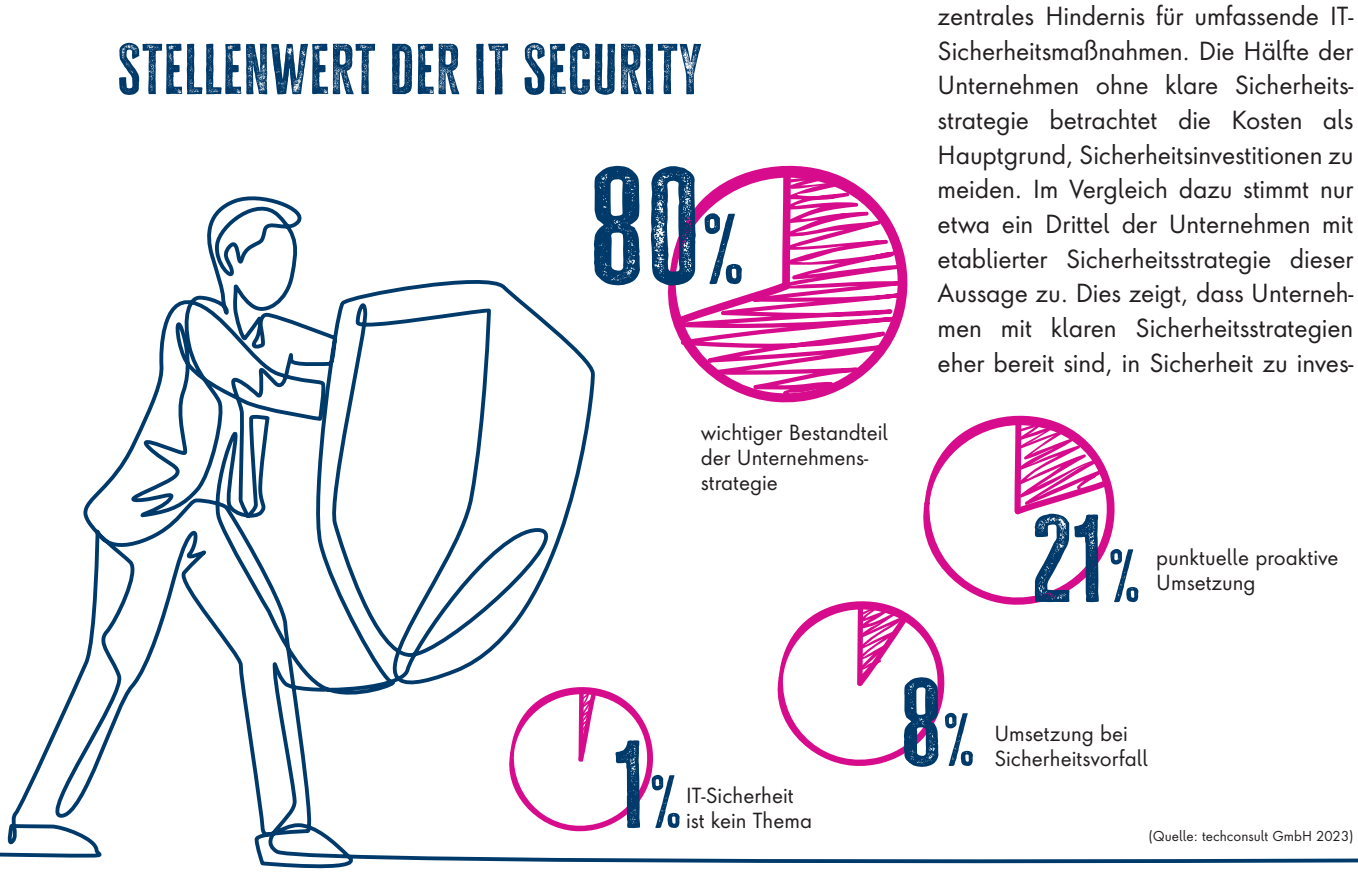
Wandel im Blick auf IT-Sicherheit

Die Studie offenbart einen grundlegenden Wandel in der Wahrnehmung von IT-Sicherheit im Mittelstand. Vor vier Jahren betrachteten lediglich 55 Prozent der befragten Unternehmen IT-Sicherheit als wichtigen Bestandteil ihrer Geschäftsstrategie. Heute sind es bereits 70 Prozent. Dieser Anstieg zeigt, dass die Bedeutung von IT-Sicherheit erkannt wird und vermehrt in die strategische Planung einfließt. Dennoch gibt es Raum für Verbesserungen: 21 Prozent der Befragten setzen Sicherheitsmaßnahmen nur sporadisch und ohne klare Strategie um, während weitere 8 Prozent erst nach einem Sicherheitsvorfall reagieren. Dies betont die Notwendigkeit einer konsequenten Umsetzung von Sicherheitsmaßnahmen.

Erkenntnis 2:

Kosten und Zeit als Barrieren für IT-Sicherheit

Die wahrgenommenen Kosten sind ein zentrales Hindernis für umfassende IT-Sicherheitsmaßnahmen. Die Hälfte der Unternehmen ohne klare Sicherheitsstrategie betrachtet die Kosten als Hauptgrund, Sicherheitsinvestitionen zu meiden. Im Vergleich dazu stimmt nur etwa ein Drittel der Unternehmen mit etablierter Sicherheitsstrategie dieser Aussage zu. Dies zeigt, dass Unternehmen mit klaren Sicherheitsstrategien eher bereit sind, in Sicherheit zu inves-



tieren. Zeitmangel ist ein weiteres Hindernis: Rund 40 Prozent der Unternehmen ohne Sicherheitsstrategie geben an, nicht genug Zeit für Sicherheitsmaßnahmen zu haben. Interessanterweise gehen fast 30 Prozent dieser Unternehmen davon aus, nicht Opfer von Cyberangriffen zu werden, was jedoch ein riskanter Irrglaube ist.

Cyberangriffe können erhebliche finanzielle und nicht-monetäre Schäden verursachen. Erfolgreiche Angriffe verursachten höhere interne Kosten bei fast der Hälfte der betroffenen Unternehmen. Unternehmen ohne Sicherheitsstrategie und Notfallpläne waren besonders anfällig für einen Anstieg interner Kosten im Fall eines Angriffs. Zusätzlich gingen 31 Prozent der von Cyberkriminalität betroffenen Unternehmen unternehmenskritische Informationen verloren, insbesondere durch Ransomware-Angriffe. Datenlecks können zudem zu Bußgeldern aufgrund von Datenschutzverletzungen führen und das Kundenvertrauen beeinträchtigen. Die Investition in IT-Sicherheit ist daher unverzichtbar.

Erkenntnis 3:

Mittelstand vertraut weiterhin nur auf Security-Klassiker

Die Studie zeigt, dass E-Mail-Sicherheit, Antiviren-Software und Firewalls nach wie vor die zentralen Sicherheitsvorkehrungen im Mittelstand sind. Diese etablierten Security-Klassiker bilden die Grundlage für die Mehrheit der Unternehmen. Unternehmen mit einer etablierten Sicherheitsstrategie setzen zudem auf weitergehende Sicherheitslösungen. Eine wichtige und richtige Entscheidung. Angesichts der zunehmenden Raffinesse von Cyberangriffen und Veränderungen in der Unternehmensstruktur, wie der Einführung von Cloud-Infrastrukturen und Remote-Arbeit, ist eine Anpassung der Sicherheitsmaßnahmen unerlässlich. Unternehmen sollten ihre Sicherheitsstrategien überdenken und die Bedeutung mehrschichtiger Sicherheitsmaßnahmen erkennen, um sich effektiver vor Cyberbedrohungen zu schützen.

www.drivelock.com

Netzwerksicherheit

VIER BLIND SPOTS, DIE SIE AUF DEM SCHIRM HABEN SOLLTEN

Sogenannte Blind Spots oder auch „blinde Flecken" im Netzwerk treiben den meisten deutschen IT- und Security-Entscheidern die Schweißperlen auf die Stirn – laut einer aktuellen Hybrid-Cloud-Studie von Gigamon sind das 52 Prozent.

Die folgenden vier Blind Spots zählen zu den kritischsten und unter Cyber-Kriminellen beliebtesten Schwachstellen von Unternehmensnetzwerken. IT- und Sicherheitsteams sollten diese kennen und aufdecken bevor sie zu gefährlichen Sicherheitsrisiken werden.

Blind Spot 1: Verschlüsselter Datenverkehr

Blind Spot 2: Lateraler Datenverkehr

Blind Spot 3: Komplexität

Blind Spot 4: Shadow- und Legacy-IT

Licht ins Dunkel bringen

Lediglich 28 Prozent der deutschen IT- und Security-Entscheider haben vollumfängliche Einsicht in ihre gesamte IT-Landschaft – und zwar von den Anwendungen bis zum Netzwerk. Für Unternehmen, die die mangelhafte Sichtbarkeit bislang ignoriert haben, besteht dringender Handlungsbedarf. Sie müssen ihre Netzwerkumgebung transparenter machen, um ein umfangreiches Verständnis von ihrem Netzwerk zu erhalten – einschließlich aller Geräte, Anwendungen, User sowie Datenströme und wie sich die Daten bewegen. Erst dann können die verantwortlichen Teams jeden noch so obskuren Blind Spot aufdecken und verborgenen Sicherheitsrisiken entgegenwirken.

www.gigamon.com

Sicherheit in der Industrie

OPTIMIERTE IT-NOTFALLPLANUNG

Die steigende Komplexität der Prozesse in Industrieunternehmen, verbunden mit der Abhängigkeit von IT-Infrastrukturen, hat die Notwendigkeit von robusten Informationssicherheitsmaßnahmen in den Vordergrund gerückt. Im Angesicht der immer stärkeren Vernetzung von Maschinen und automatisierten Produktionsprozessen ist eine effektive IT-Notfallplanung unerlässlich, um möglichen Angriffen von außen vorzubeugen und im Ernstfall den Geschäftsbetrieb aufrechtzuerhalten. Die Contechnet Suite, die GRC Software für Informationssicherheit, IT-Notfallmanagement und Datenschutz, knüpft hier an.

In einer Zeit, in der Hacker zunehmend in die digitalisierten Prozesse von Unternehmen eingreifen könnten, ist die Gefahr von Manipulation, Datendiebstahl und Industriespionage allgegenwärtig. Sensible Informationen wie Firmen-, Produktions- und Kundendaten könnten in die falschen Hände gelangen, was nicht nur finanzielle Verluste, sondern auch einen erheblichen Imageschaden nach sich ziehen könnte.

Qualität und Erfahrung aus Deutschland

Die HELDELE GmbH, ein führender Dienstleister im Bereich Elektro- und Kommunikationstechnik, hat erkannt, dass eine umfassende IT-Notfallplanung entscheidend ist, um diesen Bedrohungen zu begegnen. ISO/IEC 27001 zertifiziert und stetig auf der Suche nach Verbesserungen im Bereich Informationssicherheit, hat das Unternehmen INDART Professional, eine Softwarelösung der CONTECHNET Deutschland GmbH, als Eckpfeiler für ihre IT-Notfallplanung ausgewählt.

„Durch den Einsatz von INDART Professional haben wir eine zentrale Lösung gefunden, die unsere IT-Notfallplanung strukturiert abbildet und uns in der Vorbereitung auf verschiedene Szenarien unterstützt", sagt Daniel Baron, Gruppenleiter IT Organisation der HELDELE GmbH. Die Software bietet einen klaren Umsetzungsleitfaden, der in acht Schritten fest definierte Ergebnisse liefert. Durch die Analyse kritischer Prozesse und ihrer Abhängigkeiten von der IT-Infrastruktur können praxiserprobte Wiederanlaufpläne schnell abgerufen werden, um den Geschäftsbetrieb im Ernstfall aufrechtzuerhalten.

Die Zusammenarbeit mit keepbit IT-SOLUTIONS GmbH, Business Partner der CONTECHNET Deutschland GmbH, hat es der HELDELE GmbH ermöglicht, INDART Professional nahtlos in ihre Arbeitsabläufe zu integrieren. Die Funktionen der Software, wie die strukturierte Vorgehensweise, redundanzfreie Datenhaltung und automatisierte Datenpflege, passen perfekt zu den Anforderungen eines modernen Industrieunternehmens.

Mit der Einführung der Lösung hat die HELDELE GmbH einen entscheidenden Schritt unternommen, um sich gegen die steigenden Bedrohungen aus dem Cyberraum zu wappnen. Denn in einer Zeit, in der die Abhängigkeit von der IT-Infrastruktur immer weiter zunimmt, ist eine effektive IT-Notfallplanung der Schlüssel zur Gewährleistung der Geschäftskontinuität.

www.contechnet.de

Knox Native

SICHERHEIT UND KONTROLLE ÜBER KRYPTOGRAFISCHE SCHLÜSSEL

In Kooperation mit dem Bundesamt für Sicherheit in der Informationstechnik (BSI) hat Samsung Knox Native ins Leben gerufen – ein Projekt, das mobile Kommunikation für Institutionen noch sicherer machen soll. Entstanden ist eine Lösung, die eine umfassende Verwaltung von Samsung Geräten ermöglicht.

Im Mittelpunkt steht hierbei der neue Knox Anchor – ein von Samsung entwickeltes Java Card Applet, das es ermöglicht, den Speicherort kryptografischer Schlüssel zu überwachen. Die Schlüssel werden hierfür in dem sicheren CC EAL 6+ Embedded Secure Element (eSE) gespeichert, das in Geräten von Samsung standartmäßig verbaut ist.

Als Einsatzbereiche sind vor allem Data-at-Rest-Verschlüsselungen, Data-in-Transit (VPN), Sperrbildschirmfunktionen sowie VS-NfD-Anwendungen vorgesehen. Allerdings kann der Knox Anchor auch für eigene Applikationen von Behörden oder Unternehmen verwendet werden.

Die Bestandteile des Samsung Knox Anchor

Der Knox Anchor ist das Herzstück der Kooperation zwischen Samsung und dem BSI, und wird zu einem integralen Bestandteil der Samsung Geräte. Er dient als Sicherheitsanker, zum Beispiel bei der Datenverschlüsselung, und funktioniert mit folgenden Komponenten.

#1 **Embedded Secure Element (eSE):** ein Sicherheitsmodul, das die sichere Speicherung kryptografischer Schlüssel gewährleistet und fest in Samsung Geräten verankert ist.

#2 **Nativer VPN-Client:** ein VPN-Client von Samsung Knox, der speziell für die Verwendung mit dem eSE entwickelt wurde.

#3 **Universal Credential Management (UCM):** der Dreh- und Angelpunkt für den Zugriff auf das Embedded Secure Element.

#4 **Separated App:** eine Funktion, die Applikationen und Inhalte voneinander trennt, um Sicherheit und Integrität zu gewährleisten, selbst, wenn private Applikationen auf einem Gerät vorhanden wären.

#5 **Schnittstellensammlung:** Eine eigens für dieses Projekt erweiterte Schnittstellensammlung.

Die Partnerschaft mit dem BSI

Die ausgebaute Partnerschaft von Samsung und dem BSI bietet große Vorteile für Lösungsanbieter und die Zukunft von VS-NfD. Durch die Vereinheitlichung wird es möglich, die Sicherheitsfunktionen von Samsung intensiver zu prüfen und die Evaluierung und Zulassung von VS-NfD-Lösungen schneller durchzuführen. Eine enge und langfristige Zusammenarbeit zwischen dem BSI und Samsung kann so für eine einheitlich evaluierte Plattform mit nachhaltiger Verfügbarkeit sorgen.

Wer kann Samsung Knox Anchor nutzen?

Obwohl Knox Anchor primär für die Bundesverwaltung entwickelt wurde, beansprucht das BSI diese innovative Lösung nicht exklusiv für sich.

Das Produkt kann Behörden sowie privaten Unternehmen weltweit sichere VS-NfD-Lösungen bieten und in unterschiedlichen Konfigurationen genutzt werden, um die Sicherheit und die Kontrolle über kryptografische Schlüssel zu erhöhen. Dadurch ist es nicht nur für Behörden wie etwa Geheimdienste, sondern für alle Organisationen und Unternehmen mit sehr hohen Sicherheitsstandards interessant.

In einer sich ständig weiterentwickelnden digitalen Welt, bietet die Kooperation zwischen Samsung und dem BSI eine wegweisende Lösung für die sichere Verwaltung von kryptografischen Schlüsseln und den Schutz sensibler Daten.

www.samsung.com

it security AWARDS 2023

GEWINNER IM RAHMEN DER „IT-SA 2023“ AUSGEZEICHNET

**Die Preisträger der it security Awards 2023 (v.l.n.r.):
Ulrich Parthier, it verlag GmbH; Adam Koblentz, Reveal Security; Sascha Giese, SolarWinds;
Stefan Strobel (cirosec) für Noetic und Dr. Michael Kunz, Nexis.**

DIE IT-SA WAR AUCH IN DIESEM JAHR WIEDER PLATTFORM FÜR DIE VERLEIHUNG DER IT SECURITY AWARDS. DIE PREISTRÄGER IN DEN VIER KATEGORIEN MANAGEMENT SECURITY, WEB/INTERNET SECURITY, CLOUD SECURITY SOWIE IDENTITY & ACCESS MANAGEMENT SIND NOETIC (MANAGEMENT SECURITY), REVEAL SECURITY (INTERNET/WEB SECURITY), SOLARWINDS (CLOUD SECURITY) UND NEXIS (IAM).

MANAGEMENT SECURITY

Noetic: Ständige Überwachung und kontinuierliches Management von Assets

Das Problem: Im Gegensatz zu existierenden Asset-Management-Systemen basiert die Lösung von Noetic auf einer für diesen Zweck speziell entwickelten Datenbank, die Beziehung zwischen den einzelnen Informationen abbilden kann und auf Basis dieser Beziehungen Analysen und Abfragen ermöglicht. Auch eine grafische Darstellung, in der man navigieren kann, ist möglich.

Die Lösung: Die Software von Noetic kommuniziert über zahlreiche Konnektoren mit vorhandenen IT-Security- und IT-Management-Lösungen, um Informationen über Assets zu sammeln und diese in einer eigenen Graph-Datenbank in Beziehung zu setzen. Dadurch kann man die Informationen, die in vielen Systemen verteilt und überall unvollständig sind, zusammenfassen und so die Qualität vieler IT-Prozesse verbessern.

Für das Incident Management beispielsweise benötigt man schnell und effizient Informationen über die IT, aktuelle Schwachstellen, Systeminformationen aus einer CMDB, Zuständigkeiten von Geschäftsbereichen für IT-Systeme, Data-Owner und vieles mehr. Aber auch schon im Verwundbarkeitsmanagement selbst können Informationen aus verschiedenen Quellen zusammenkommen um die Kritikalität einer Schwachstelle angemessen im Unternehmenskontext zu bewerten.

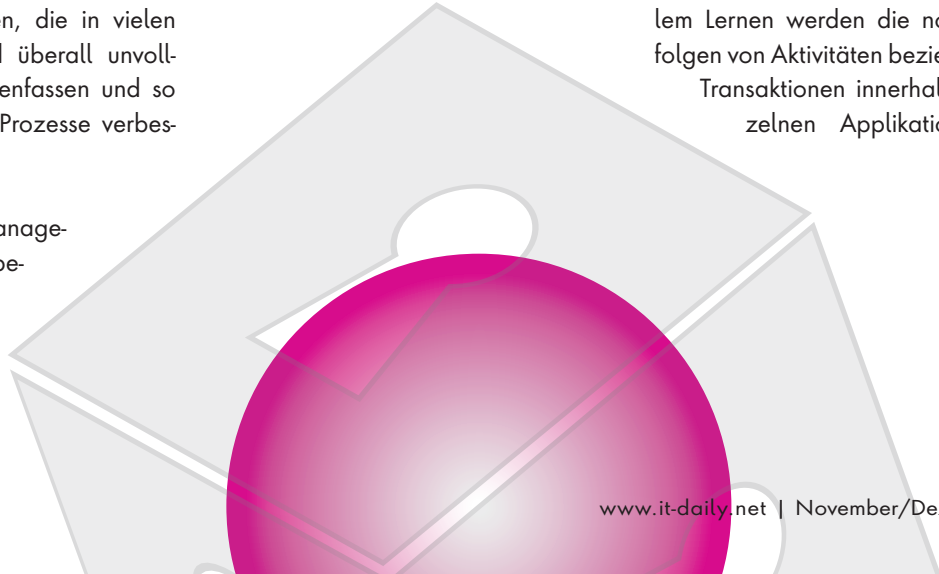
Fazit: Noetic Security unterstützt Unternehmen dabei, Sicherheitsrisiken für ihre Umgebung besser zu verstehen. Die Lösung erstellt kontinuierlich eine Übersicht aller Assets, Schwachstellen, Nutzer sowie Systeme und stellt ihre Beziehung zueinander dar. Darauf aufbauend können IT-Sicherheitsverantwortliche Risiken und entsprechenden Handlungsbedarf besser erkennen und Entscheidungen sicher treffen.

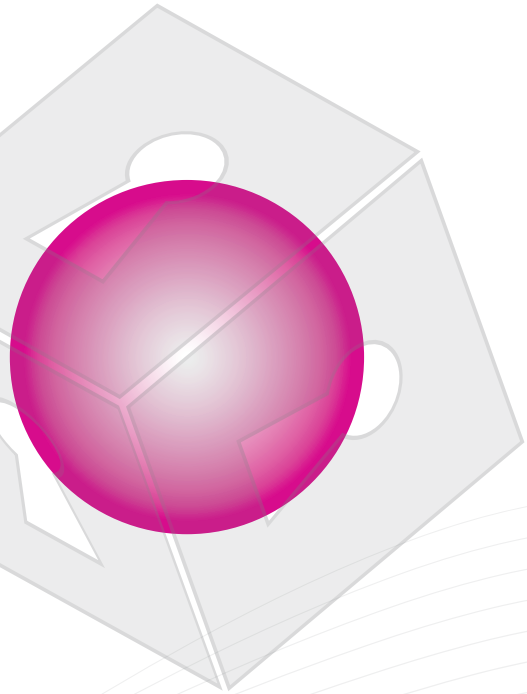
WEB/INTERNET SECURITY

RevealSecurity: Erkennung von Angriffen auf Unternehmensanwendungen

Das Problem: Bisherige Produkte zur Erkennung von Angriffen oder Kompromittierungen konzentrieren sich meist auf die Arbeitsplätze von Mitarbeitern oder den Datenverkehr im Netzwerk. Ein besonders blinder Fleck sind dabei die Business-Applikationen eines Unternehmens. Wenn die Manipulationen nicht auf Ebene des Betriebssystems, sondern in der Applikation erfolgen, musste man bisher versuchen, Use Cases zur Erkennung für jede Applikation einzeln mit Regeln in einem SIEM zu erstellen.

Die Lösung: Das Tool von RevealSecurity bietet eine Erkennung auf Basis des Wegs, den die Anwender innerhalb der Applikationen nehmen. Mit maschinellem Lernen werden die normalen Abfolgen von Aktivitäten beziehungsweise Transaktionen innerhalb jeder einzelnen Applikation gelernt.





Abweichungen davon können dann Alarme auslösen. So eröffnet die Lösung neue Optionen, um mit vertretbarem Aufwand die bisher blinden Flecken in die Erkennung von Angriffen aufzunehmen. Für weit verbreitete SaaS-Applikationen verfügt der Hersteller bereits über Konnektoren, eigene Applikationen können einfach integriert werden, indem Logs bereitgestellt werden.

Fazit: Die Lösung von RevealSecurity erlaubt es, Angreifer und Innentäter in Geschäftsanwendungen mithilfe einer sogenannten User-Journey-Analyse zu erkennen. Dabei werden Aktivitätssequenzen während der Verwendung einer Anwendung analysiert und daraus eine Zeitleiste erstellt. Mit Kontext angereichert ermöglichen diese Sequenzen, Anomalien zu erkennen. Da die Lösung selbst auch als SaaS angeboten wird, ist eine Integration mit minimalem Aufwand verbunden. Die passende Abkürzung wäre ADR für „Application Detection and Response", wobei dieser Begriff bisher nicht existiert, da es keine anderen Lösungen mit diesem Fokus gibt.

CLOUD SECURITY

SolarWinds: Next-Generation Build System

Das Problem: Die Cybersicherheitslandschaft ist ständig in Bewegung. Jeden Tag tauchen neue Bedrohungen auf, die den Bedarf an einem sichereren Softwareentwicklungsprozess verdeutlichen.

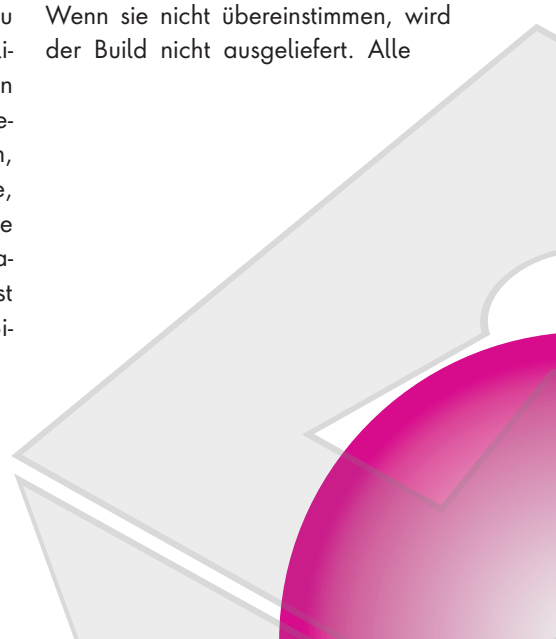
Aus diesem Grund hat SolarWinds vor kurzem sein Next-Generation Build System vorgestellt, ein transformatives Modell für die Softwareentwicklung. Das Modell ist eine Schlüsselkomponente der Secure by Design-Initiative des Unternehmens, die sich auf Menschen, Infrastruktur und Softwareentwicklung konzentriert, um die Sicherheitsinfrastruktur des Unternehmens zu verbessern.

Next-Generation Software Build ist ein Zusatz zur Standard-Agile/DevOps-Methodik, die die meisten Unternehmen verwenden. Die Cybersicherheitslandschaft unterliegt einem evolutionären Muster, bei dem neue Cyber-Bedrohungen auftauchen und im Gegenzug neue Antworten entwickelt werden, um diesen Bedrohungen zu begegnen. Das Tool ist eine zusätzliche Reihe von Prozessen, Methoden und Technologien, die Sicherheitsbedrohungen der neuesten Generation, wie etwa Angriffe auf die Lieferkette, abwehren. Der Ansatz für „Software Builds der nächsten Generation" basiert auf den Agile und DevOps Best Practices und wendet zusätzliche Sicherheitskontrollen an.

Die Lösung: Das SolarWinds Next-Generation Build System umfasst Softwareentwicklungspraktiken und -technologien, die darauf ausgelegt sind, die Integrität der Build-Umgebung durch einen „parallelen Build"-Prozess zu stärken. So wird sichergestellt, dass SolarWinds-Software in drei sicheren Umgebungen mit separaten Benutzer-Anmeldeinformationen entwickelt wird: eine Standardumgebung, eine Validierungsumgebung und eine Sicherheitsumgebung.

In der Standardumgebung wird jeder Build-Schritt aufgezeichnet, kryptografisch signiert und in einem unveränderlichen Protokoll gespeichert, so dass Auditoren den Prozess detailliert analysieren können, um etwaige Fehler oder Anomalien zu verstehen. Als Nächstes werden diese Build-Aufträge in die Validierungsumgebung verlagert, die nur einem begrenzten Kreis von DevOps-Mitarbeitern zugänglich ist. Schließlich fungiert die Sicherheitsumgebung als dritte Schicht, in der eine Vielzahl von Sicherheitsprüfungen durchgeführt werden, um das Produkt vor der Freigabe zu validieren. Diese Schritte schaffen einen vertrauenswürdigen Build-Pfad zwischen den Gedanken der Entwickler und den im Einsatz befindlichen Binärdateien.

Keine einzelne Person hat Zugang zu allen Pipelines, und die Validierungs- und Produktions-Builds werden vor der endgültigen Auslieferung verglichen. Wenn sie nicht übereinstimmen, wird der Build nicht ausgeliefert. Alle



> AUCH 2023 SEHEN WIR VIELE INNOVATIVE PRODUKTE VOR ALLEM AUS DEN USA UND ISRAEL. ABER AUCH EIN PRODUKT „MADE IN GERMANY " HAT ES DIESES JAHR AUF DAS SIEGERTREPPCHEN GESCHAFFT.
>
> **Ulrich Partier, Publlisher it management**

Entwicklungsumgebungen sind außerdem ephemer, das heißt, sie sind kurzlebig und werden jedes Mal neu erstellt, wenn ein Build abgeschlossen ist.

Fazit: Das Innovationspotenzial liegt im Bereich der Sicherheitsinfrastruktur mit einem dreistufigen transformativen Modell für die Softwareentwicklung bei der große Teile der Community als Open Source zur Verfügung gestellt werden.

IDENTITY & ACCESS MANAGEMENT

Nexis: Nexis 4 mit elektronischen Berechtigungskonzept

Das Problem: Banken und Versicherungen müssen aufgrund regulatorischer Vorgaben für alle Applikationen Berechtigungskonzepte erstellen und pflegen. Meistens werden dafür Word- und Excel-Dateien erstellt, manchmal auch Confluence Seiten eingerichtet. Das Problem ist: Diese „ungeliebten" Dokumente sind in der Regel schlecht gepflegt: Die Beschreibungen der Rollen und Rechte sind wenig aussagkräftig, Veränderungen in den Applikationen werden meistens nicht in den Berechtigungskonzepten nachgepflegt. Bei Prüfungen durch die Bankenaufsicht und/oder die interne Revision sind damit Findings vorprogrammiert.

Die Lösung: Nexis 4 wurde um die Funktionalität „elektronisches" Berechtigungskonzept erweitert. Dahinter steckt die Idee, dass viele Informationen zu den Applikationen ohnehin in Nexis 4 vorliegen, wenn der Kunde Rezertifizierungen und/oder Rollen- und Berechtigungsmanagement mit dem Produkt macht.

Idealerweise werden dabei die bestehenden und oft in standardisierter Form vorliegenden Stammdaten aus existierenden Berechtigungskonzepten übernommen und durch die von der IGA-Lösung gelieferten Daten ergänzt. Soweit Beschreibungen oder andere Metadaten zur Kritikalität, zu SoD Klassen und so weiter noch fehlen, können sie durch Workflows oder Formulare durch die Applikationsverantwortlichen ergänzt werden.

So wird auch sichergestellt, dass die Berechtigungskonzepte immer dem Ist-Zustand in den Applikationen entsprechen:

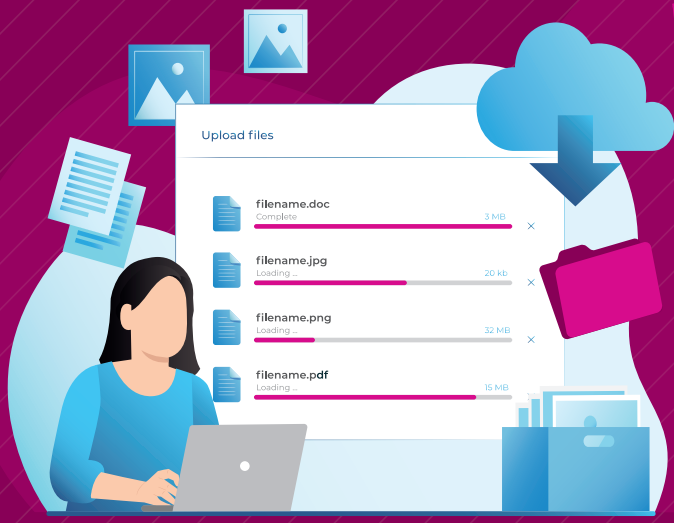
- Eine Möglichkeit ist, dass Changeprozesse direkt in Nexis 4 oder im IGA-System abgewickelt werden und damit sichergestellt wird, dass der Ist-Zustand in den Applikationen immer identisch mit dem Sollzustand ist.
- Die andere Option arbeitet mit Triggern: Immer wenn die IGA Lösung beim regelmäßigen Zielsystemabgleich eine Veränderung detektiert, zum Beispiel eine neue Berechtigung, löst das automatisch einen Prozess in Nexis 4 aus.

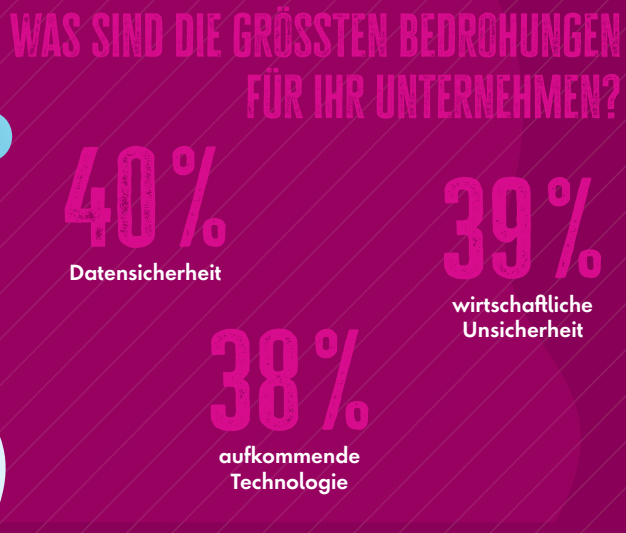
Fazit: Egal, welche Tools man für das Identitätsmanagement einsetzt oder einsetzen will: Unternehmen klagen oft über fehlende oder oberflächliche Funktionen, kostspielige Anpassungsarbeiten und vor allem über zu wenig Verständlichkeit für nicht-IT Anwender.

Nexis 4 bietet fertige Analysen, Workflows und Endanwender-Funktionen ohne teure Integrations- oder Programmierarbeiten. Eine weitere Stärke ist die Visualisierung von Daten, Strukturen und Abhängigkeiten.

Hinzu kommen als Alleinstellungsmerkmal das elektronische Berechtigungskonzept. Es gibt zu dieser automatisierten Lösung kein vergleichbares anderes Produkt auf dem Markt.

Ulrich Parthier | www.it-daily.net





Alarmierende Wissenslücken

RISIKEN FÜR UNTERNEHMEN WERDEN UNTERSCHÄTZT

Veritas Technologies veröffentlicht eine neue Studie, die zeigt, dass 26 Prozent der deutschen Befragten nicht glauben, dass ihr Unternehmen die kommenden zwölf Monate überleben wird. Die Studie „Data Risk Management: The State of the Market-Cyber to bietet Einblicke in die wichtigsten Risiken, ihre Auswirkungen und die Art und Weise, wie Unternehmen sie zu bewältigen haben.

Überraschenderweise verneinte fast die Hälfte (49 Prozent) der Umfrageteilnehmer die Frage, ob ihr Unternehmen derzeit gefährdet sei. Nachdem ihnen jedoch eine Liste individueller Risikofaktoren vorgelegt wurde, erkannten die Befragten aller Ebenen die Herausforderungen, vor denen ihre Unternehmen stehen. 99 Prozent identifizierten ein Risiko für ihre Arbeitsplätze.

Eindeutig identifizierbare Risiken

Angesichts der aktuellen makroökonomischen Situation und der täglichen Nachrichten spiegeln die Umfrageergebnisse eindeutig den Zeitgeist wider. Von einer umfassenden Liste potenzieller Gefahren nannten die Befragten Datensicherheit (40 Prozent), wirtschaftliche Unsicherheit (39 Prozent) und aufkommende Technologien wie KI (38 Prozent) als die größten Bedrohungen, mit denen ihre Unternehmen derzeit konfrontiert sind. Als schon länger bekannte Bedrohung rangiert Fachkräftemangel auf dem vierten Platz. Den fünften Platz teilen sich Risiken durch schwache Nachhaltigkeitsmaßnahmen und Risiken für die Marke. Geopolitische Instabilität fiel sogar weiter nach unten und belegte den sechsten Platz auf der Liste.

KI erweist sich für Unternehmen als zweischneidiges Schwert. In den letzten Monaten wurde in den Medien viel über Cyberkriminelle berichtet, die KI-Lösungen einsetzen, um ausgeklügelte und schwerwiegende Ransomware-Angriffe zu entwickeln. Darüber hinaus wurde ein Risikofaktor für Unternehmen identifiziert, die es versäumen, angemessene Sicherheitsvorkehrungen gegen Datenschutzverletzungen durch den Einsatz generativer KI-Tools zu treffen. Umgekehrt wird die neue Technologie als eine der vielversprechendsten Lösungen im Kampf gegen Hacker angesehen.

Weiterhin gaben 96 Prozent der Befragten zu, bereits negative Auswirkungen von Risiken erlebt zu haben, darunter Rufschädigung und finanzielle Verluste. In Bezug auf die Risiken, die ihren Unternehmen tatsächlich geschadet haben, stand Datensicherheit erneut an erster Stelle mit 45 Prozent der Befragten.

Für die große Rolle von Datensicherheitsverletzungen sprach die Anzahl der Unternehmen, die Opfer von Ransomware-Angriffen wurden. Eine bedeutende Mehrheit (78 Prozent) gab an, dass ihr Unternehmen in den vergangenen zwei Jahren mindestens einen erfolgreichen Ransomware-Angriff erlitten hat. Von denen, die einen erfolgreichen Angriff erlebt hatten, gaben 26 Prozent an, dass sie ihn nicht gemeldet hatten.

www.veritas.com

IT-Sicherheitstrends 2024

VON AUDITIERUNG BIS ZERO TRUST

Sichere Cloud-Services sind entscheidend, um die Vertraulichkeit, Integrität und Verfügbarkeit von Daten gewährleisten zu können. Zu den klassischen Technologien wie Verschlüsselung, VPN, Multi-Faktor-Authentifizierung oder L7-Firewalls kommen immer neue hinzu. Auch Cloud-Provider müssen up to date bleiben.

Das Sicherheitsmanagement beschert IT-Verantwortlichen regelmäßig Kopfzerbrechen: Immer neue Bedrohungsszenarien, Angriffsmethoden und Hiobsbotschaften über geglückte Attacken durch staatliche Organisationen auf Unternehmen machen die Cybersecurity zur Sisyphusarbeit. Das gilt für Client-Server-Topologien ebenso wie für Cloud-Umgebungen. Der Unterschied: In der Cloud verschieben sich Verantwortlichkeiten und Zuständigkeiten. Hier ist es in erster Linie der Dienstleister, der für die Sicherheit sorgen und sich dafür verbürgen muss, dass seine Technologien und Methoden dem aktuellen Stand der Cyber-Abwehr entsprechen.

EIN DAUERTHEMA FÜR IT-VERANTWORTLICHE WERDEN AUCH IM KOMMENDEN JAHR DIE ASPEKTE COMPLIANCE UND AUDITS DARSTELLEN.

Udo Kürzdörfer,
Head of Products and Marketing,
noris network AG, www.noris.de
(Quelle: noris network)

Trends für 2024

Dazu gehört neben typischen Technologien wie Verschlüsselung, VPN oder die Multi-Faktor-Authentifizierung mehr und mehr ein Zugriffsschutz mit der Bezeichnung Zero Trust Security. Dieser – relativ radikale – Sicherheitsansatz geht davon aus, dass keinerlei Vertrauensstellung in einem Netzwerk besteht, unabhängig von Benutzer oder Gerät. Jeder Zugriff wird kontinuierlich überprüft und autorisiert, um sicherzustellen, dass nur berechtigte Anwender auf bestimmte Ressourcen zugreifen können.

Aber auch der Hype um Künstliche Intelligenz (KI) und maschinelles Lernen (ML) wird in den kommenden Jahren zweifelsohne das Geschäft von IT-Dienstleistern und Rechenzentren beeinflussen. Spezielle KI- und ML-Innovationen zur Erkennung von Bedrohungen und Verbesserung von Sicherheitsanalysen unterstützen Cloud-Provider zukünftig dabei, Angriffe schneller zu identifizieren und zu bekämpfen. Beispiele dafür sind die Verhaltensanalyse und die Vorhersage von Attacken: KI und ML sind in der Lage, das normale Verhalten von Benutzern, Geräten und Netzwerken über einen längeren Zeitraum hinweg zu erlernen. Treten Abweichungen auf, schlägt das System Alarm. In Sachen Bedrohungserkennung sind diese Technologien zudem dafür einsetzbar, bekannte Muster von Malware, Viren und anderen schädlichen Aktivitäten zu erkennen, selbst wenn sie in leicht modifizierter Form auftreten. Der entscheidende Vorteil: die Erkennung von Bedrohungen, für die noch keine Signaturen vorhanden sind.

Mehr Relevanz für Compliance und Audits

Ein Dauerthema für IT-Verantwortliche werden auch im kommenden Jahr die Aspekte Compliance und Audits darstellen. Die Einhaltung von Datenschutzbestimmungen wie der DSGVO (Datenschutz-Grundverordnung) und anderer Vorschriften nimmt sogar noch an Bedeutung zu. Hier spielen weniger die Technologien als vielmehr das Know-how und die erreichten Zertifizierungen von IT-Dienstleistern und Rechenzentrumsbetreibern die entscheidende Rolle.

Unverzichtbar ist in diesem Zusammenhang neben dem Standort Deutschland die Einhaltung entsprechender Sicherheitsstandards und ein bestätigtes IT-Sicherheitsniveau durch Zertifizierungsinstanzen wie dem BSI oder TÜV. Dazu gehören ISO 27001 auf Basis von IT-Grundschutz des BSI oder der Kriterienkatalog BSI C5 (Cloud Computing Compliance Criteria Catalogue). Für besonders kritische Anforderungen im Bereich Colocation wurde TÜViT-TSI-Level-4 ins Leben gerufen: Rechenzentren, die auf TÜViT-TSI-Level-4 zertifiziert sind, erfüllen besonders strenge Anforderungen und Standards sowie Ausfallsicherheit. Erst mit diesen Zertifizierungen können Organisationen ganz sichergehen, dass der Dienstleister halten kann, was er mit seinen Technologien verspricht.

Udo Kürzdörfer

Fernwartung im industriellen Umfeld

SO LASSEN SICH IT- UND OT-SYSTEME IN DER FERTIGUNG AUS DER FERNE VERWALTEN

Das Bundesamt für Sicherheit in der Informationstechnik macht sich regelmäßig Gedanken um die Sicherheitslage von hiesigen Unternehmen und gibt dazu das IT-Grundschutz-Kompendium heraus. Seit Februar 2023 ist dort der Abschnitt „IND 3.2 – Fernwartung im industriellen Umfeld" enthalten. Dies alleine zeigt die Bedeutung dieses Themas seitens des BSI.

Sieht man sich die aktuelle – immer weiter digitalisierte - Betriebstechniklandschaft (Operational Technology; OT) genauer an, fällt vor allem eins auf: Sie weist eine enorme Heterogenität auf. Das betrifft dezentrale Infrastrukturen genauso wie die vielfältigen Steuersysteme und deren Zugriffsarten. Alleine das erfordert eine recht hohe Zahl unterschiedlicher Fernwartungszugänge. Diese werden wiederum ganz unterschiedlich realisiert, bestehen also aus einer unüberschaubaren Zahl an Hard- und Software-Komponenten.

Diese und weitere Faktoren stellen vor allem verarbeitende Unternehmen vor die Herausforderung, mithilfe der passenden Fernwartungslösung ein Höchstmaß an Sicherheit und Komfortabilität zu schaffen. Das betrifft die OT und die IT gleichermaßen. Hierfür stehen diverse Ansätze und Möglichkeiten zur Verfügung.

Unterschiede und Gemeinsamkeiten

Vergleicht man aktuelle Fernwartungssysteme ergeben sich diverse Gemeinsamkeiten, und Unterschiede. So sollten auf jeden Fall sichere Verbindungen genutzt werden. Das betrifft sowohl die infrage kommenden Protokolle wie Simple Network Management Protocol (SNMP) und Intelligent Platform Management Interface

(IPMI). Letzteres wird mehr und mehr von Redfish abgelöst, das Web-Techniken wie JSON als Datenformat HTTPS für die Datenübertragung und mehr unterstützt. Zudem gibt es unterschiedliche kryptografische Verfahren, die unter anderem auf dem AES-256-Standard basieren, mit denen Daten und Verbindungswege verschlüsselt werden. Darüber hinaus werden in OT-Infrastrukturen anstatt erprobter Standards wie TCP/IP oder IPsec immer noch proprietäre Protokolle genutzt. Das birgt unter anderem in OT-Netzwerken diverse Gefahren, wie zahlreiche Cyberattacken der Malware-Varianten Ekans, Triton und Industroyer belegen. So brachte beispielsweise Industroyer die Energieversorgung der ukrainischen Hauptstadt Kiew 2016 vollständig zum Erliegen.

OT-Fernwartung muss zudem noch weitere Funktionen bereitstellen, die bei der reinen IT-Fernwartung keine Rolle spielen, wie beispielsweise den Zugriff auf das ICS (Industrielles Steuerungssystem), um damit ein Anlaufen beziehungsweise ein Stoppen von Anlagen sicherzustellen und so Personen oder Sachschäden zu verhindern. Aber auch die Integrität der anfallenden Daten und das Beschränken der erforderlichen Kommunikationswege sollte das Fernwartungssystem bereitstellen.

Basis-Anforderungen an die Fernwartung

Für ein Mindestmaß an Sicherheit müssen Fernwartungszugänge laut BSI bestimmte Anforderungen erfüllen. Dazu gehört zum Beispiel die Auswahl der infrage kommenden Systeme, die ausschließlich von außen ferngewartet werden dürfen. Aber auch ein Minimum an benötigten Zugängen und Kommunikationswegen gehört zu den Basisanforderungen an die Fernwartung im OT- und IT-Umfeld. Ebenfalls sollte eine zuverlässige Verschlüsselung wie AES-256 zum Einsatz kommen.

DER SICHERE FERNZUGRIFF AUF IT- UND OT-SYSTEME IST NICHT NUR MIT TECHNISCHEN, SONDERN AUCH MIT ORGANISATORISCHEN ANFORDERUNGEN ENG VERKNÜPFT.

Robert Korherr, Geschäftsführer, ProSoft GmbH, www.prosoft.de

Neben diesen Basisanforderungen sollten weitere Standard-Bedingungen erfüllt werden, was die Fernwartung betrifft. Dazu zählt beispielsweise eine Ende-zu-Ende-Verschlüsselung, die auf eine möglichst geringe Zahl an Fernwartungsverbindungen angewandt wird. Aber auch allgemein gültige Richtlinien sollten definiert und beschrieben werden, mit denen sich Rollen, Zuständigkeiten und Verantwortlichkeiten definieren lassen. Hinzu kommt der Einsatz kryptografisch verschlüsselter Protokolle. Für noch mehr Sicherheit empfiehlt sich der Einsatz von sogenannten MFA-Verfahren, die häufig auf dem Einsatz von Hardware-Token basieren. Hierbei sorgt ein USB-Schlüssel beispielsweise für den kennwortlosen Zugriff auf besonders schützenswerte Anwenderkonten. Wichtig ist obendrein ein Notfallplan, der die notwendigen Schritte im Störungsfall beschreibt. Darin wird unter anderem beschrieben, wie auf einen möglichen Malware-Angriff reagiert werden soll. Hierfür werden personelle Zuständigkeiten definiert, die Art und Weise der Systemwiederherstellung, und vieles mehr.

Anforderungen bei erhöhtem Schutzbedarf

Speziell bei Betreibern von kritischen Infrastrukturen (KRITIS) - wie zum Beispiel Wasser- und Stromversorgungsunternehmen - ergibt sich aufgrund ihrer gesellschaftlichen Bedeutung ein erhöhter Schutzbedarf, woraus sich im Bezug auf das erforderliche Fernwartungssystem unter anderem folgende Aspekte ergeben:

#1 Der Funktionsumfang des OT-Fernwartungssystems sollte an die Administration von IT-Systemen angepasst werden.

#2 Es sollten möglichst nur solche Fernwartungssysteme eingesetzt werden, mit denen sich IT- und OT-Clients verwalten lassen.

#3 Redundante Kommunikationsverbindungen sollten für eine möglichst hohe Ausfallsicherheit sorgen.

Zwei Arten der Fernwartung: Software- und Hardware-basiert

Bei der Fernwartung von industriellen IT- und OT-Systemen wird in zweierlei Ansätzen unterschieden: Hardware- und Software-basiert. Beide Methoden haben ihre Vor- und Nachteile.

Die Software-basierte Fernwartung kennzeichnet sich vor allem durch den schnellen Einsatz, durch integrierte Betriebs- und Monitoring-Funktionen sowie günstige Lizenzkosten aus. Auf den ersten Blick bieten sich Online-Fernwartungslösungen an, die über eine Internetverbindung zustande kommen. Oftmals mangelhaft geschützte OT-Systeme, die über eine externe Verbindung ferngewartet werden, widersprechen sich. Abgeschlossene OT-Infrastrukturen, sollten besser mit Fernwartungssoftware verwaltet werden, die keine externen Zugänge benötigen, um zu funktionieren. Wegen dieser Risiken empfiehlt das Grundschutz-

Kompendium diese Art der Fernwartung möglichst selten einzusetzen.

Auf der anderen Seite stehen dedizierte, hardware-basierte Fernwartungslösungen zur Auswahl. Die Vor- und Nachteile liegen hierbei auf der Hand. Zum einen arbeiten diese Lösungen sehr zuverlässig und weisen einen hohen Sicherheitsgrad auf. Zum anderen sind die Anschaffungskosten recht hoch, außerdem erfordert das Einrichten geschultes Personal.

Der sichere Fernzugriff auf IT- und OT-Systeme ist nicht nur mit technischen, sondern auch mit organisatorischen Anforderungen eng verknüpft. Dazu gehört neben der bereits erwähnten Risikoanalyse ein minimales Implementieren von Fernzugriffsmöglichkeiten, exakt definierte Prozesse und Abläufe, klar geregelte Zeitfenster von Remote-Zugängen sowie das regelmäßige Verwalten und Auswerten von Protokolldaten.

Wie praktisch wäre es, wenn sich IT- und OT-Systeme mit ein und demselben Tool wie beispielsweise dem NetSupport Manager von ProSoft aus der Ferne verwalten ließen, und das mit den vom BSI geforderten Sicherheitsstandards. Damit könnte man sowohl IT-Endgeräte als auch Maschinen und Steuerungseinheiten im Fertigungsumfeld mit nur einer einzigen, zentralen Software fernwarten.

Fernwartung von IT- und OT-Systemen gleichermaßen

Das funktioniert im günstigsten Fall über sämtliche Transportmedien hinweg (also via LAN, WLAN und das Internet), und zwar auf Basis bekannter Protokolle wie TCP/IP und HTTPS. Darüber hinaus lassen sich mit solch einem Werkzeug alle verfügbaren Endgeräte gleichermaßen sowie gleichzeitig verwalten, und sich obendrein inventarisieren. So behält man jederzeit den Überblick über alle vorhandenen Gerätschaften.

Fazit

IT- und OT-Infrastrukturen können aus der Ferne gewartet und verwaltet werden - mit nur einem Tool. Das Bundesamt für Sicherheit in der Informationstechnik legt hohe Standards an, was die Sicherheitsanforderungen an die notwendigen Fernwartungslösungen im IT- und OT-Umfeld betreffen. Das schließt die zum Einsatz kommenden Hardware- und Software-Komponenten genauso ein wie die Verschlüsselungsmechanismen, die die Verbindungswege und die Daten schützen sollen. Darüber hinaus sollte penibel genau auf die Basis- und Standardanforderungen sowie auf die Bedingungen bei einem erhöhten Schutzbedarf geachtet werden. Und dies alles im Verbund mit der passenden Hardware- oder Software-Lösung, mit der sich idealerweise IT- und OT-Systeme aus der Ferne verwalten und überwachen lassen.

Robert Korherr

Das kleine Einmaleins der Security

CYBERSICHERHEIT FÜR DEN MITTELSTAND

Mittelständische Unternehmen sind bei Cyber-Kriminellen ein beliebtes Ziel, weil sie viele wertvolle Daten besitzen, aber in der Regel nicht über die gleichen Ressourcen verfügen wie große Unternehmen, um diese zu schützen. Dell Technologies stellt sie vor:

#1 **Mitarbeiter schulen:** Durch regelmäßige Schulungen können Unternehmen das Bewusstsein für Cyber-Gefahren schärfen und Best Practices im sicheren Umgang mit Daten, Anwendungen und Geräten vermitteln. Wichtig ist, dass die Schulungen keine einmalige Angelegenheit bleiben, sondern kontinuierlich stattfinden.

#2 **Auf Daten konzentrieren:** Statt sich auf den Schutz einzelner Systeme zu konzentrieren, zwischen denen die Daten hin- und herfließen, sollten Unternehmen die Daten selbst in den Mittelpunkt ihrer Sicherheitsbemühungen stellen. Das bedeutet, Daten konsequent zu verschlüsseln und genau zu kontrollieren, wer auf sie zugreift.

#3 **Komplexität reduzieren:** Lösungen, die Sicherheitsfunktionen wie Multifaktor-Authentifizierung und rollenbasierte Zugriffskontrollen von vornherein integrieren, können die Komplexität von Zero Trust reduzieren und die Einführung erheblich beschleunigen.

#4 **As-a-Service-Modelle evaluieren:** Bei knappen IT-Budgets, geringem oder fehlendem Know-how und Personal lohnt der Blick auf Managed Services. Erfahrene IT-Dienstleister übernehmen dann den Betrieb der Infrastruktur und den Schutz von Daten und Anwendungen. Abgerechnet wird verbrauchsabhängig, was eine gute Kostenkontrolle und einfache Skalierung ermöglicht.

#5 **Fortschrittliche Bedrohungen abwehren:** Um Angreifer aufzuspüren und die Analyse der Auswertungen und das Einleiten von Gegenmaßnahmen erfahrenes Personal erfordert, ist es meist am sinnvollsten, XDR als Service zu beziehen. So ist sichergestellt, dass sich Sicherheitsexperten rund um die Uhr darum kümmern, die IT-Infrastruktur zu überwachen, mögliche Bedrohungen zu untersuchen und Angriffe abzuwehren.

www.delltechnologies.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:
Karl Alderton, Valentin Boussin, Uwe Gries, Michael Haas, Jörg von der Heydt, Robert Korherr, Sabine Kuch, Udo Kürzdörfer, Silke Menzel, Carina Mitzschke, Olaf Müller-Haberland, Silvia Parthier, Ulrich Parthier, Kai Schuricht, Stephan Schweizer, Michael Veit

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

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

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

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

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

Anzeigenpreise:
Es gilt die Anzeigenpreisliste Nr. 31.
Preisliste gültig ab 1. Oktober 2023.

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

Online Campaign Manager:
Roxana Grabenhofer, 08104-6494-21,
grabenhofer@it-verlag.de

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

Erscheinungsweise: 6 x pro Jahr

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

Bankverbindung:
VRB München Land eG,
IBAN: DE90 7016 6486 0002 5237 52, BIC: GENODEF10HC

Beteiligungsverhältnisse nach § 8, Absatz 3 des Gesetzes über die Presse vom 8.10.1949: 100 % des Gesellschafterkapitals hält Ulrich Parthier, Sauerlach.

Abonnementservice: Eva Neff,
Telefon: 08104-6494 -15, E-Mail: neff@it-verlag.de

Das Abonnement ist beim Verlag mit einer dreimonatigen Kündigungsfrist zum Ende des Bezugszeitraumes kündbar. Sollte die Zeitschrift aus Gründen, die nicht vom Verlag zu vertreten sind, nicht geliefert werden können, besteht kein Anspruch auf Nachlieferung oder Erstattung vorausbezahlter Beträge.

SAVE THE DATE

IAM CONNECT 2023

Die Brücke zu neuen Geschäftsmodellen






29. November 2023 | Online via Zoom

Hier mehr erfahren

www.iamconnect.de

#IAMConnect2023

Eine Veranstaltung von itsecurity & it-daily.net