it management

Der Motor für Innovation
Juli/August 2025

INKLUSIVE 48 SEITEN
it security

TRANSFORMATIONSSTUDIE 2025

Zielerreichung deutlich verbessert

Patric Dahse, Natuvion

THOUGHT LEADERSHIP

DSAG SPEZIAL

Generative KI, S/4HANA, Cloud-ERP-System, SAP BDC, SAP EWM und SAP DM

SPOT AN FÜR STARKE IT-LÖSUNGEN

it spotlight

by it-daily.net

Die besten IT-Lösungen | Die innovativsten Anbieter | Alles auf einen Blick!

UNSERE PREMIUMANBIETER

DriveLock

Aagon

Hier könnte Ihr Logo platziert sein!
Jetzt buchen.

Ihre Ansprechpartner:

Kerstin Fraenzke
Head of Media Consulting
Tel. +49 8104 6494 19
fraenzke@it-verlag.de

Karen Reetz-Resch
Media Consulting
Tel. +49 8121 9775 94
reetz@it-verlag.de

Marion Mann
Media Consulting
Tel. +49 152 363 412 55
mann@it-verlag.de

it-daily.net/it-spotlight

DAS GROSSE IT-DILEMMA

LIEBE LESERINNEN UND LESER,

Das Motto des DSAG-Jahreskongresses „The Art of Balance. Alles eine Frage der Ballons?" in Bremen trifft den Nerv der Zeit weit über die SAP-Welt hinaus. Bei meinem letzten Besuch eines anderen SAP-Events wurde mir bewusst, wie sehr die dort diskutierten Dilemmata das gesamte IT-Management prägen.

SAPs Vision einer integrierten Business Suite in der Cloud spiegelt einen branchenweiten Trend wider: Hyperscaler und Softwareanbieter drängen mit ambitionierten Cloud-First-Strategien vorwärts. Die Balance zwischen bestehenden Investitionen und dem Druck zur digitalen Transformation – diese Herausforderung kennt jeder CIO, unabhängig vom ERP-System.

Wie ein IT-Leiter eines mittelständischen Unternehmens treffend bemerkte: „Wir sollen alle gleichzeitig KI-Pioniere, Cloud-Experten und Compliance-Hüter sein. Aber am Ende des Tages müssen die Systeme noch laufen." Diese Aussage fasst das Dilemma des IT-Managements prägnant zusammen.

Das Sicherheitsthema durchzieht dabei alle IT-Entscheidungen. Cloud, KI und Security müssen gemeinsam gedacht werden. Eine Erkenntnis, die über SAP hinaus für jede IT-Architektur gilt. Das Geheimnis liegt vielleicht darin, nicht alle Ballons gleichzeitig steigen zu lassen, sondern zu entscheiden, welche davon wirklich zum Geschäftserfolg beitragen.

Herzlichst,

Lars Becker | Redakteur

INHALT

Farblich hervorgehobene Artikel sind von der Redaktion als besonders lesenswert empfohlen

Inklusive 48 Seiten
it security

GUT ZU WISSEN

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

TECHNISCHE SCHULDEN

FAKTEN, DIE CIOs UND DBAs KENNEN SOLLTEN

In vielen Organisationen wurde das Datenbankdesign zu einer Zeit entwickelt, als Skalierbarkeit, Automatisierung und agile Entwicklungsmethoden noch keine zentrale Rolle spielten. Heute stehen Datenbankadministratoren (DBAs), IT-Architekten und CIOs vor der Herausforderung, ihre Systeme nicht nur leistungsfähig und sicher zu betreiben, sondern sie gleichzeitig auch so flexibel zu gestalten, dass Innovationen möglich sind. Technische Schulden stehen dieser Aufgabe im Weg.

Was bedeutet „technische Schulden" im Kontext von Datenbanken?

Technische Schulden entstehen, wenn IT-Teams bei der Entwicklung oder Wartung einer Datenbank bewusst oder unbewusst Abstriche bei Qualität und Nachhaltigkeit machen – etwa zugunsten kürzerer Projektlaufzeiten oder schneller Releases. Anstatt saubere, skalierbare und dokumentierte Lösungen umzusetzen, entstehen pragmatische Zwischenlösungen, die kurzfristig helfen, aber langfristig Wartungsaufwand, Komplexität und Fehleranfälligkeit erhöhen.

Warum entstehen technische Schulden?

Eine zentrale Rolle spielt Zeitdruck: Wenn neue Features schnell verfügbar sein müssen, werden Datenbankänderungen oft hastig und ohne Rücksicht auf die langfristigen Folgen für das Management umgesetzt. Hinzu kommt, dass die Datenbankentwicklung in vielen Unternehmen nicht oder nur unzureichend in moderne DevOps-Prozesse eingebunden ist. Während Applikationscode längst versioniert, getestet und automatisiert bereitgestellt wird, erfolgen Datenbankanpassungen vielerorts noch manuell – außerhalb kontrollierter Pipelines und ohne strukturierte Qualitätssicherung.

Welche Folgen haben technische Schulden für Unternehmen?

Zunächst leidet die Performance: Überladene Schemata, ineffiziente Abfragen oder fehlerhafte Indizes verursachen längere Ladezeiten und höheren Ressourcenverbrauch. Auch die Fehleranfälligkeit steigt: Nicht getestete Änderungen oder intransparente Strukturen können dazu führen, dass ganze Systeme instabil werden oder ausfallen. Besonders teuer wird es, wenn technische Schulden Innovationen blockieren – etwa bei der Einführung neuer Anwendungen, der Anbindung externer Systeme oder der Migration in Cloud-Architekturen.

Welche Maßnahmen helfen gegen technische Schulden?

Um technische Schulden zu vermeiden oder gezielt zu tilgen, ist ein strukturierter Ansatz erforderlich. Im Zentrum steht dabei ein Datenbankmanagement nach modernen DevOps-Praktiken. Dazu zählt die automatisierte Versionierung von Datenbankschemata, mit der sich Änderungen rückverfolgbar dokumentieren lassen. Ergänzt wird dies durch automatisierte Testverfahren, die auch bei kleinen Änderungen sicherstellen, dass keine unerwünschten Nebeneffekte auftreten. Moderne Tools helfen, Änderungen vorab zu analysieren und transparent zu kommunizieren – insbesondere zwischen Entwicklern und DBAs.

www.red-gate.com/de/

Cloud Report 2025

WIRTSCHAFT RUFT NACH EINER DEUTSCHEN CLOUD

In der deutschen Wirtschaft wächst die Sorge vor einer zu hohen Abhängigkeit von Cloud-Diensten aus dem Ausland. Fast zwei Drittel (62 Prozent) der Unternehmen in Deutschland würden ohne Cloud-Dienste stillstehen. Zugleich halten mehr als drei Viertel (78 Prozent) Deutschland für zu abhängig von US-Cloud-Anbietern, 82 Prozent wünschen sich große Cloud-Anbieter, sogenannte Hyperscaler, aus Deutschland oder Europa, die es mit den außereuropäischen Marktführern aufnehmen können. Und jedes zweite Unternehmen (50 Prozent), das Cloud-Computing nutzt, sieht sich aufgrund der Politik der neuen US-Regierung gezwungen, die eigene Cloud-Strategie zu überdenken.

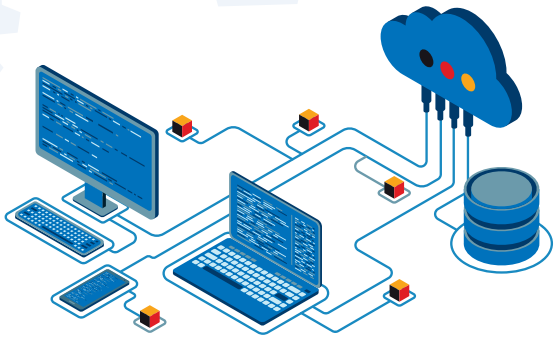
Das sind Ergebnisse des „Cloud Report 2025", den der Digitalverband Bitkom im Juni veröffentlicht hat, und für den 604 Unternehmen ab 20 Beschäftigten in Deutschland befragt wurden.

Für praktisch alle Unternehmen, die Cloud-Dienste nutzen oder dies in Betracht ziehen (97 Prozent), spielt ein vertrauenswürdiges Herkunftsland des Cloud-Anbieters bei der Auswahl eine Rolle. Für 67 Prozent ist es sogar eine zwingende Voraussetzung, 2024 war das nur für 58 Prozent der Fall. Alle (100 Prozent) würden einen Anbieter aus Deutschland bevorzugen, dahinter folgt mit 61 Prozent ein Anbieter aus der EU. Die USA liegen mit 6 Prozent gleichauf mit Großbritannien auf Platz 6, noch hinter den europäischen Nicht-EU-Staaten (14 Prozent), Japan (12 Prozent) und Indien (8 Prozent).

Leistungsfähige Cloud

Allerdings muss ein Cloud-Dienst, der Daten ausschließlich in Deutschland und vor ausländischem Zugriff geschützt verarbeitet, konkurrenzfähig sein. Nur 12 Prozent würden ein solches Angebot nutzen, wenn man länger als bei internationalen Wettbewerbern auf neue Funktionen warten muss. Für 8 Prozent wäre es akzeptabel, wenn nicht alle Funktionen von internationalen Anbietern vorhanden sind, 7 Prozent wären bereit, etwa 10 bis 20 Prozent mehr zu bezahlen und 6 Prozent würden Abstriche bei der Bedienbarkeit oder dem Service hinnehmen. Zwei Drittel (65 Prozent) würden allerdings keine dieser Nachteile akzeptieren.

www.bitkom.org



Einen Schritt Voraus

Modernes IT Financial Management mit USU

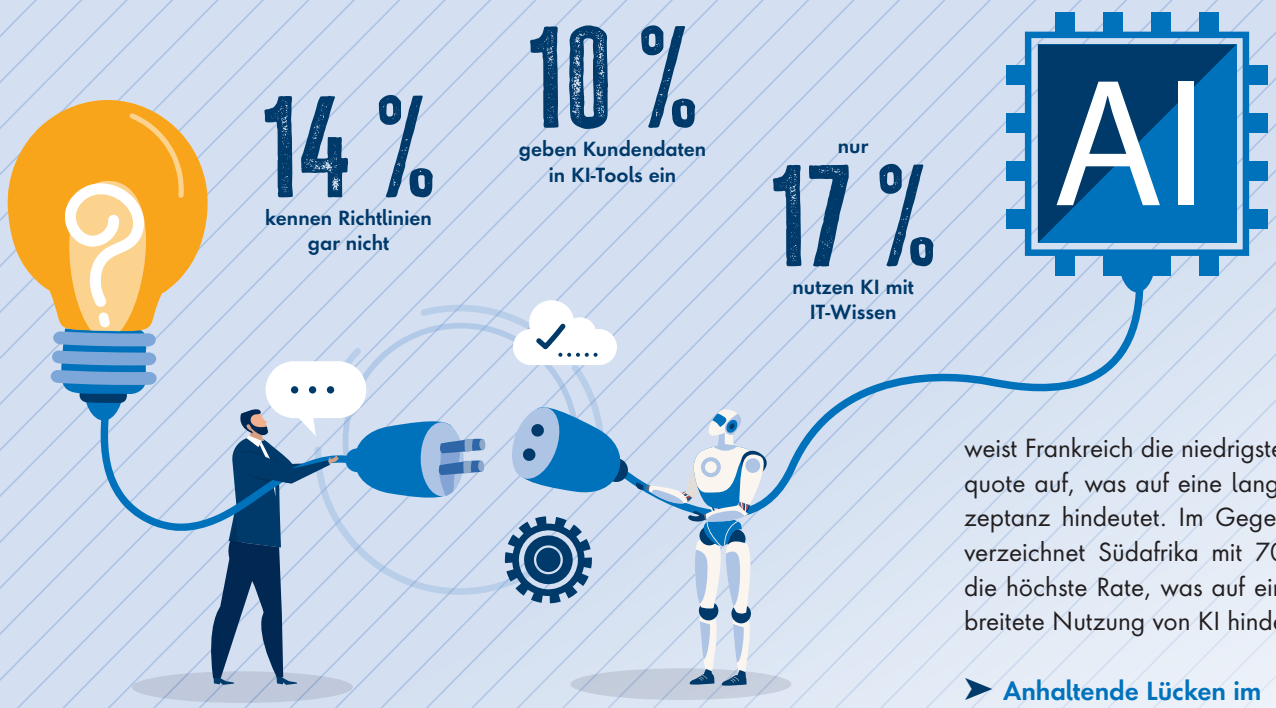
USU

360° Perspektive
auf Ihre Services

Abbildung verschiedenster
Kostenmodelle

Transformation in Richtung
FinOps & TBM

Lernen Sie USU IT Financial Management kennen:



KÜNSTLICHE INTELLIGENZ

ZWISCHEN NUTZUNG UND SICHERHEITSBEWUSSTSEIN

KnowBe4 hat neue Umfrageergebnisse veröffentlicht, die eine gravierende KI-Governance-Lücke aufzeigen. Die aktuelle Umfrage unter Arbeitnehmern in Deutschland, Südafrika, den Niederlanden, Frankreich, Großbritannien und den USA zeigt, dass eine große Mehrheit der Arbeitnehmer bereits mit Tools der Künstlichen Intelligenz (KI) arbeitet, aber nur ein geringer Prozentsatz die offiziellen Unternehmensrichtlinien für deren Nutzung kennt.

Im Durchschnitt setzen 60,2 Prozent der Mitarbeiter KI-Tools am Arbeitsplatz ein. Im Gegensatz dazu kennen nur 18,5 Prozent die Richtlinien ihres Unternehmens für deren Einsatz. Diese signifikante Lücke deutet darauf hin, dass die überwiegende Mehrheit der KI-Aktivitäten in Unternehmen ohne Anleitung oder Aufsicht stattfindet. Jeder zehnte Mitarbeiter (10 Prozent) gab zu, Kundendaten in ein KI-Tool eingegeben zu haben, um eine Arbeitsaufgabe zu erledigen.

Weitere Erkenntnisse

➤ **Unterschiedliche KI-Akzeptanzraten:**
Der weltweite Durchschnitt der Arbeitnehmer, die KI am Arbeitsplatz nutzen, liegt bei 60,2 Prozent. Die Akzeptanzraten variieren jedoch je nach Region. Mit nur 54,2 Prozent der Arbeitnehmer, die angaben, KI-Tools bei der Arbeit zu nutzen, weist Frankreich die niedrigste Annahmequote auf, was auf eine langsamere Akzeptanz hindeutet. Im Gegensatz dazu verzeichnet Südafrika mit 70,1 Prozent die höchste Rate, was auf eine weit verbreitete Nutzung von KI hindeutet.

➤ **Anhaltende Lücken im Bewusstsein für die Politik:**
Im Durchschnitt gaben 14,4 Prozent der Arbeitnehmer an, die KI-Richtlinien ihres Unternehmens nicht zu kennen. Besonders auffällig ist dieser Mangel an Bewusstsein in den Niederlanden (16,1 Prozent) und im Vereinigten Königreich (15,8 Prozent), was auf einen Bedarf an verbesserten Kommunikations- und Schulungsstrategien hinweist.

➤ **Die sanktionierte KI-Nutzung hinkt hinterher:**
Nur durchschnittlich 17 Prozent der Mitarbeitenden nutzen KI bei der Arbeit mit dem Wissen ihres IT-/Sicherheitsteams. Diese Zahl ist in Südafrika mit 23,6 Prozent zwar am höchsten, bleibt aber insgesamt niedrig. Dies deutet darauf hin, dass Unternehmen proaktiv genehmigte KI-Lösungen bereitstellen und fördern müssen.

Die Studie unterstreicht, wie wichtig es für Unternehmen ist, diese Kluft zwischen Bewusstsein und Nutzung zu überbrücken. Dazu ist es erforderlich, nicht nur Richtlinien festzulegen, sondern diese auch aktiv zu kommunizieren. Außerdem müssen umfassende Schulungen zur ethischen und sicheren Nutzung von KI angeboten und bewährte, benutzerfreundliche KI-Tools bereitgestellt werden, um die erheblichen Risiken einer unkontrollierten KI-Nutzung zu mindern.

www.knowbe4.com

Thema Arbeitsort

WENN CHEFS UND MITARBEITENDE ANEINANDER VORBEIREDEN

Während in Deutschland über flexiblere gesetzliche Arbeitszeitmodelle gestritten wird, spielt sich der eigentliche Konflikt woanders ab: beim Arbeitsort. Die neue Talent Trends-Studie der Personalberatung PageGroup zeigt deutlich, dass sich die Vorstellungen von Mitarbeitenden und Führungskräften stark unterscheiden.

Ein Drittel der Unternehmen zwingen ihre Mitarbeitenden inzwischen wieder häufiger zurück an den Schreibtisch im Firmengebäude. Der Anstoß kommt dabei meist von oben: Denn 37 Prozent der Führungskräfte sind überzeugt, dass im Büro effizienter gearbeitet wird. Nur 19 Prozent glauben an die höhere Produktivität im Homeoffice.

Auffällig: Rund ein Drittel der Mitarbeitenden sieht gar keinen Unterschied zwischen Büro und Heimarbeit in Bezug auf die Leistung. Der Großteil zieht dennoch die Arbeit in den eigenen vier Wänden vor – nicht zuletzt wegen der besseren Vereinbarkeit von Beruf und Privatleben.

Die weltweite Studie, für die in Deutschland 2.500 Personen befragt wurden, zeigt: Unternehmen, die weiterhin auf Kontrolle und Präsenz setzen, laufen Gefahr, den Anschluss zu verlieren. Die Zukunft der Arbeit liegt nicht in starren Regeln, sondern in einem Umfeld, das genügend Flexibilität für die individuellen Lebensumstände bietet. Karriere und Status verlieren an Relevanz, wichtiger sind heute Transparenz, Sicherheit und Stabilität.

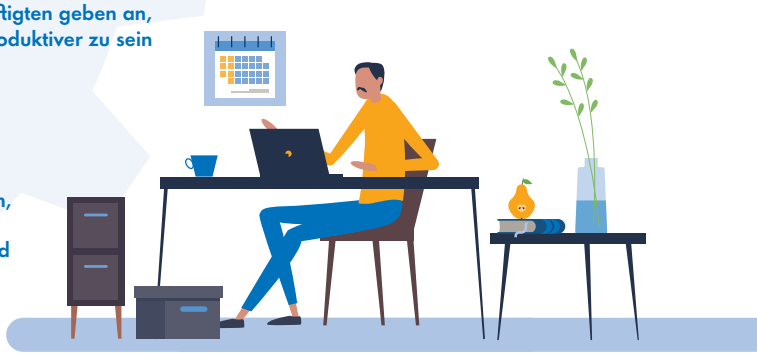
Die Frage bleibt, ob Führungsetagen bereit sind, neue Wege zu gehen, um die Produktivität ihrer Teams nachhaltig zu fördern. Denn Unternehmen stehen nun vor der Herausforderung, den Wandel aktiv zu gestalten, um ihren Beschäftigten ein vertrauensvolles Arbeitsumfeld zu schaffen.

www.page.com

EINE KLARE VERTRAUENSLÜCKE

38 %
der Beschäftigten geben an, zuhause produktiver zu sein

19 %
der Arbeitgeber glauben, dass Mitarbeitende zuhause produktiver sind als im Büro



WANDEL**ERP**ROBT
DIE SOFTWARE ZUR TRANSFORMATION. KONZIPIERT FÜR LOSGRÖSSE 1+
ams-erp.com
ams ERP

MOBILE SYSTEME

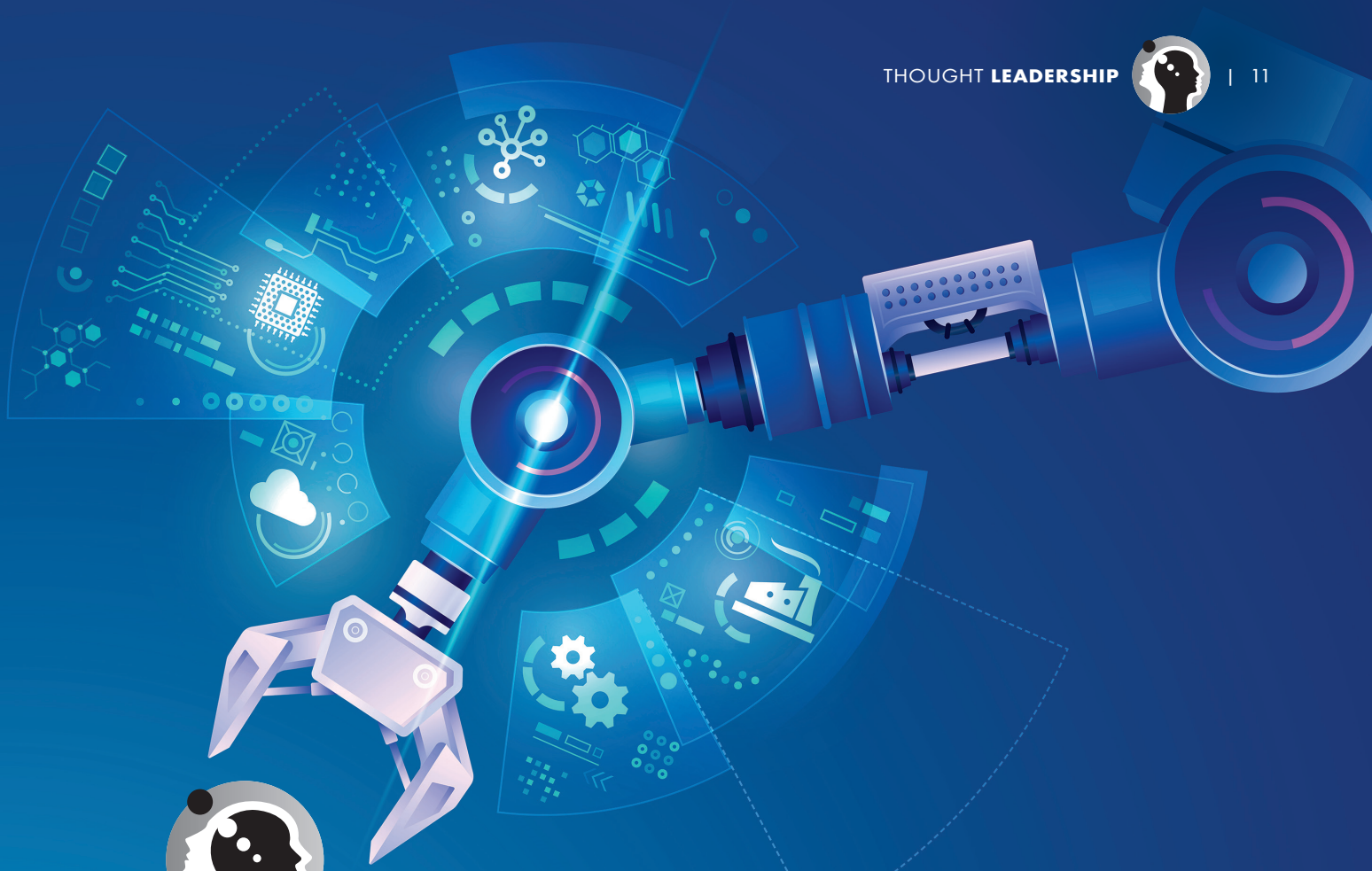
KONZEPTION, ENTWICKLUNG UND BETRIEB

Mobile Systeme
Konzeption, Entwicklung und Betrieb;
Florian Bliesch,
Carl Hanser Verlag GmbH & Co.KG; 06-2025

„Mobile Systeme – Konzeption, Entwicklung und Betrieb" ist ein umfassendes Grundlagenwerk, das fundiertes Wissen über mobile Technologien, deren Entwicklung und praktischen Einsatz vermittelt. Es erklärt die technischen Grundlagen ebenso wie fortgeschrittene Anwendungsbereiche und deckt den gesamten Lebenszyklus mobiler Systeme ab. Dabei geht es um Themen wie User Experience Design, Entwicklungsstrategien, Application Management, Green IT, XR-Technologien, Mobile Security und Zukunftsthemen wie das Mobile Metaverse. Das Ziel ist es, Studierende der Informatik, Wirtschaftsinformatik und Medieninformatik sowie IT-Manager:innen mit den Besonderheiten, Chancen und Herausforderungen mobiler Ökosysteme vertraut zu machen. Sie sollen lernen, wie man mobile Technologien gezielt und nachhaltig einsetzt. Das Buch bereitet sie auf die Umsetzung innovativer mobiler Projekte in verschiedenen Branchen vor.

Aus dem Inhalt:

- Mobile Systeme
- Mobile Geräte
- Mobile User Experience
- Mobile Security
- Mobile KI
- Mobile Business
- Green IT und Green Coding



TRANSFORMATION, UEM & DLP

Wurden Unternehmen früher hauptsächlich durch das Service-Ende älterer Systeme zur Transformation gedrängt, handelt es sich heute hauptsächlich um strategische Entscheidungen. Die größten Herausforderungen liegen nach wie vor in der Analyse bestehender IT-Landschaften und Datenbestände.

Gleichzeitig führt die Verschiebung hin zu Remote Work und mobilen Geräten zu neuen Problemen. Heterogene IT-Infrastrukturen sollen effizient verwaltet werden, was häufig zu fragmentierten Verwaltungsstrukturen führt. IT-Administratoren müssen oft zwischen verschiedenen Konsolen wechseln, Sicherheits- und Compliance-Berichte liegen verstreut und Änderungen werden nicht automatisch zwischen den Systemen synchronisiert.

Das nächste Problem zeigt sich darin, dass sensible Daten durch hybride und globale Netzwerke wandern. Diese Entwicklung macht traditionelle Data-Loss-Prevention-Ansätze obsolet und erfordert neue, ganzheitliche Sicherheitsstrategien, die plattformübergreifend funktionieren.

Die IT steht vor einem dreifachen Wandel bei Transformation, Verwaltung und Sicherheit.

Transformationsstudie 2025

ZIELERREICHUNG DEUTLICH VERBESSERT

Zum vierten Mal in Folge hat Natuvion gemeinsam mit NTT Data Business Solutions eine internationale IT-Transformationsstudie durchgeführt. Befragt wurden leitende Personen in Unternehmen und in 14 Ländern zu ihren Erfahrungen und Einschätzungen bei großen Transformationsprojekten. Zu den Ergebnissen der aktuellen Studie spricht Ulrich Parthier, Publisher it management, mit Patric Dahse, CEO und Mitbegründer des Transformationsspezialisten Natuvion.

Ulrich Parthier: *Herr Dahse, was ist das wichtigste Argument, die jährliche Studie nun zum vierten Mal zu wiederholen?*

Patric Dahse: Es hat sich während der letzten Jahre sehr viel geändert und das wollen wir verstehen. Unternehmen, die heute eine Transformation durchlaufen, sind besser vorbereitet und wissen, was sie von einer Transformation erwarten. Noch vor wenigen Jahren waren viele Unternehmen vom Service-Ende älterer SAP-Versionen getrieben und sind eher einer technischen Notwendigkeit gefolgt. Heute ist die Transformation eine strategische Entscheidung und Manager wollen aus dem hohen Einsatz von Ressourcen und Budgets klare Business-Vorteile ziehen.

Eine Transformation muss einen Wettbewerbsvorteil schaffen. Grundlage dafür ist eine solide Datenstrategie, denn hier passieren die meisten Fehler, die zu Budget- und Zeitüberschreitungen oder im schlimmsten Fall zum Verfehlen von Transformationszielen führen. Genau hier setzt unsere Transformationsstudie an und hilft mit den Erfahrungen anderer Unternehmen, Best Practices zu entwickeln, um den maximalen Benefit aus einer IT-Transformation zu schöpfen.

Ulrich Parthier: *Lassen Sie uns über die Ergebnisse der Studie sprechen. Haben sich denn die Gründe für eine Transformation im Vergleich zu den Studien der letzten Jahre verändert?*

Patric Dahse: Ja, die Gründe haben sich signifikant geändert. In den vergangenen Jahren waren Unternehmen teils noch mit den Folgen von Corona, mit der Inflation oder mit anderen operativen Themen beschäftigt und setzten die Ziele entsprechend anders. Jetzt priorisieren Unternehmen wieder mehr Zukunftsthemen und folgen deutlich mehr den großen Trends der Informationstechnologie. Dieses Jahr hat die Einführung neuer Technologien wie Künstliche Intelligenz (KI) mit fast 57 Prozent die oberste Priorität. Ich finde es ist ein großer Schritt von eher traditionellen Prioritäten, wie der Optimierung der Organisation oder der Kostenreduktion, hin zur Stärkung von Zukunftsthemen.

Ulrich Parthier: *Die letzten Studien haben gezeigt, dass Unternehmen schon in der Planung schwerwiegende Fehler begehen. Ist das nach wie vor so?*

Patric Dahse: Eine IT-Transformation in großem Ausmaß muss gut geplant werden. Das beginnt bei der Zeitplanung, geht über die Budgetplanung und reicht bis zur gewünschten Ergebnisdefinition. Gerade was den Zeitfaktor angeht sehen wir, dass die Unternehmen voneinander und auch durch Studien wie unsere lernen, dass derartige Projekte nicht mal schnell umgesetzt werden können. Beispielsweise sehen wir einen Anstieg um 6 Prozent bei den Unternehmen, die mehr als ein Jahr für die Transformation vorgesehen haben – heute sind es 64 Prozent. Mit mehr als zwei Jahren planen jetzt 22,7 Prozent - 2024 waren es nur 18,9 Prozent. Der vielleicht wichtigste Unterschied zur Vorjahresstudie ist, dass der Anteil derer, die meinen, eine Transformation in weniger als 6 Monaten durchführen zu können, von 16,9 Prozent um rund die Hälfte auf 8,3 Prozent zusammengeschrumpft ist.

? **Ulrich Parthier:** *Zeit ist aber nicht der einzige Stolperstein einer Transformation, oder?*

Patric Dahse: Richtig. Neben einer realistischen Zeiteinschätzung für das Projekt ist auf jeden Fall auch das Wissen über die existierenden Systeme von entscheidender Bedeutung. Wenig überraschend liegt die größte Herausforderung mit 38,6 Prozent in der Analyse der bestehenden IT-Landschaft und Daten. Das war schon 2024 einer der größten Stolpersteine. Im Vergleich zu den Vorjahresstudien hat dieser Wert sogar nochmals mit 12 Prozent Abstand zur zweitgrößten Herausforderung zugelegt.

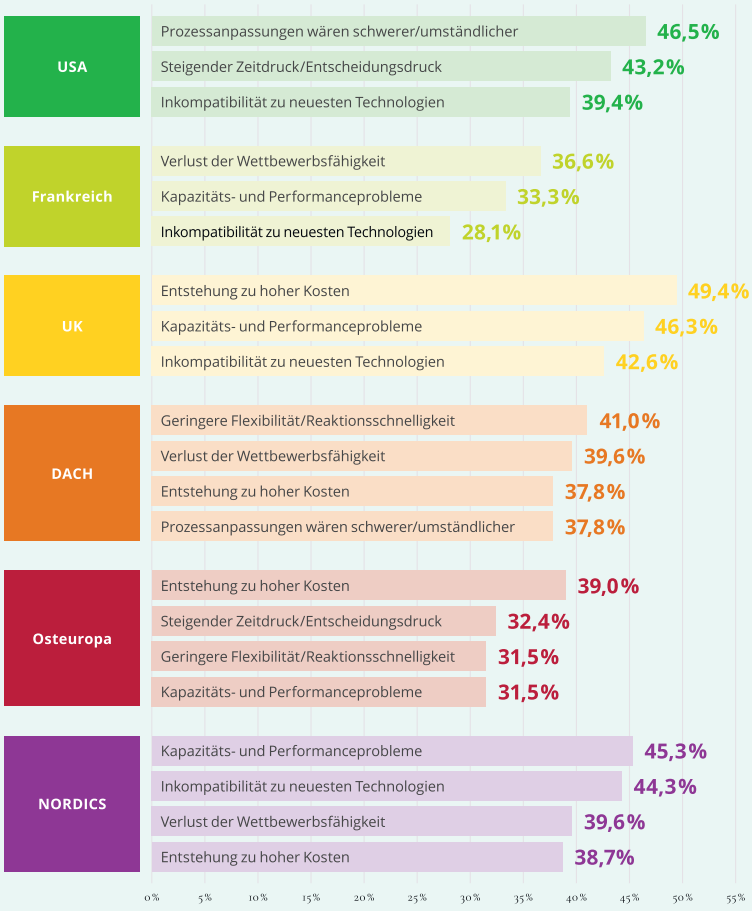
Auf Rang zwei sehen wir in der aktuellen Studie die Komplexität des Gesamtprojekts, was teilweise auch mit dem Alter der zu transformierenden Systeme zu tun hat. Über 42 Prozent der Altsysteme sind sechs bis zehn Jahre alt, 37 Prozent waren älter als 10 Jahre und etwa 11 Prozent waren sogar älter als 16 Jahre. In solch langen Zeiträumen ist viel Eigenentwicklung passiert und es wurden Datenbestände aufgebaut, die oft schlecht dokumentiert sind oder aus heutiger rechtlicher Sicht nicht existieren dürften.

Diese Ergebnisse deuten darauf hin, dass sich Unternehmen zunehmend mehr darüber bewusst sind, dass die umfassende Analyse der Datenbestände das Fundament jeder Transformation bildet. Um daran nicht zu scheitern, ist es ratsam, frühzeitig Experten an Bord zu holen.

? **Ulrich Parthier:** *Lassen Sie uns über die Durchführung der Transformation sprechen. Wie gehen die Unternehmen mit ihren Daten um? Alles mitnehmen, ausmisten oder von vorne anfangen?*

Patric Dahse: Die Umstellung auf ein neues System erfordert die Wahl der optimalen Transformationsstrategie. Essenziell ist dabei das Wissen um die Vor- und Nachteile der Migrationsmethoden Brownfield, Greenfield, Selective Data Transition oder einer Kombination aus Brown- und Greenfield mit der selektiven Datentransformation. In der aktuellen Studie wählten 30,2 Prozent aller Befragten die Brownfield-Methode, 25 Prozent gingen den Weg des Neuanfangs mit Greenfield. Der überwiegende Anteil (45 Prozent) will nur Teile des Systems mitnehmen oder zurücklassen. Das ist fast der gleiche Wert wie schon 2024. Die rein selektive Datenmigration wählten 25,8 Prozent der Studienteilnehmer. Eine Kombination aus selektiver Datenmigration mit dem Brownfield- oder Greenfield-Ansatz durchliefen 19,1 Prozent.

WAS WÄRE PASSIERT, WENN SIE DIE TRANSFORMATION NICHT DURCHGEFÜHRT HÄTTEN? (nach Regionen)



Ulrich Parthier: *Was genau bedeutet das für eine Transformation?*

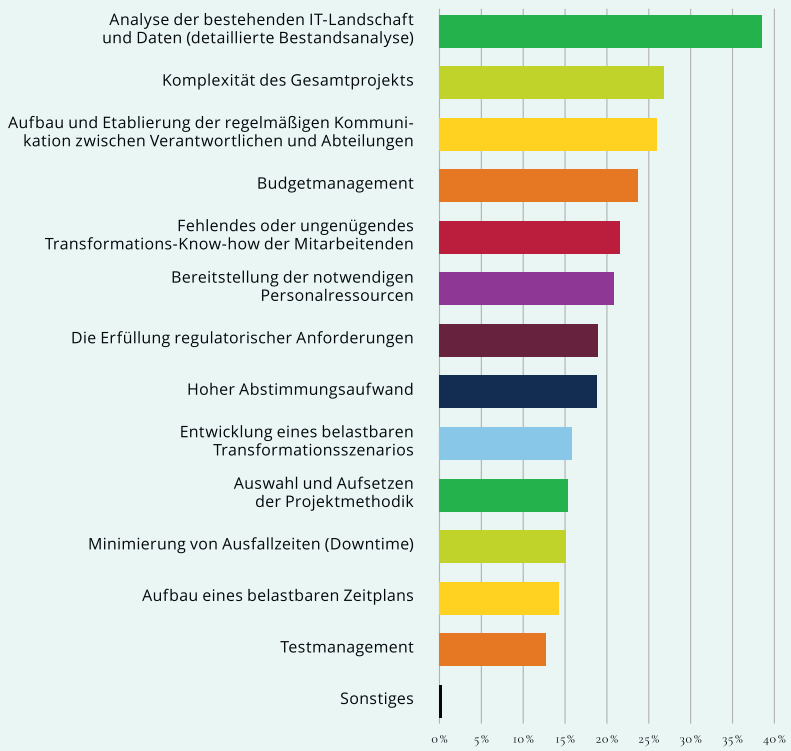
Patric Dahse: Aus der täglichen Praxis wissen wir, dass die wenigsten Transformationsprojekte vollständig neu auf der grünen Wiese starten. 75 Prozent aller befragten Unternehmen nehmen Teile oder alle Daten mit in ihr neues System. 45 Prozent entscheiden sich für eine umfangreiche Analyse und nehmen als Ergebnis nur Teile ihrer bestehenden Daten und Prozesse mit.

Interessant ist in diesem Zusammenhang das Alter des zu migrierenden Systems und die gewählte Migrationsmethode. Je jünger das System ist, desto beliebter ist der Weg über den Brownfield-Ansatz. Das ist nachvollziehbar, denn bei Systemen, die erst vor wenigen Jahren erneuert wurden, sind die Datenqualität und Prozesse bereits bereinigt und überarbeitet. Hier erscheint die Übernahme aller Prozesse und Daten der einfachste und schnellste Weg ins neue System. Allerdings ist die Gefahr groß, dass bei dieser Methode zugunsten der einfacheren Transformation das Potenzial möglicher Innovationen auf der Strecke bleibt.

EINE UMFANGREICHE IT-TRANSFORMATION MUSS VON ANFANG AN GUT GEPLANT WERDEN.

Patric Dahse, CEO, Natuvion GmbH, www.natuvion.com

WAS WAREN IHRE GRÖSSTEN HERAUSFORDERUNGEN BEI DER PLANUNG?



Ulrich Parthier: *Lassen Sie uns über die Ziele reden. Haben die Erfahrungen und vielleicht auch die Studie zu besseren Ergebnissen geführt?*

Patric Dahse: Der Gradmesser der Zielerreichung hängt interessanterweise davon ab, wen man fragt. Über die Grundgesamtheit hinweg gesehen, erreichten die befragten Unternehmen zu knapp 69,4 Prozent ihre Ziele. Letztes Jahr waren es nur 56,6 Prozent. In der aktuellen Studie berichten 29,4 Prozent, ihre Ziele nur teilweise und 1,2 Prozent gar nicht erreicht zu haben – im Gegensatz zu 39,2 und 3,7 Prozent in der letztjährigen Studie. Von daher kann man sagen, dass sich die Ergebnisse für die Unternehmen signifikant verbessert haben.

Betrachtet man nur die Vorstände und Geschäftsführer, so behaupten diese mit 76,8 Prozent deutlich häufiger, alle Ziele erreicht zu haben. Umgekehrt beurteilen die Abteilungsleiter mit 72,5 Prozent und Teamleiter mit 56 Prozent die Ergebnisse deutlich weniger euphorisch.

Interessant ist auch der Vergleich zwischen den Regionen. Mit 75 Prozent bestätigen die Amerikaner am häufigsten, dass sie die Ziele der Transformation erreicht haben. DACH, UK und die Nordics schneiden mit jeweils über 70 Prozent ebenfalls recht gut ab. Unterdurchschnittlich schneiden Osteuropa mit 62 Prozent und Frankreich mit 59,6 Prozent ab.

Bemerkenswert ist zudem, dass der Anteil derjenigen, die alle ihre Transformationsziele erreicht haben, in den letzten vier Erhebungen stetig angewachsen ist. Von 2022 mit 51 Prozent zur aktuellen Studie mit 69,4 Prozent.

Ulrich Parthier: *Was bedeutet das im Kontext mit der Vorbereitung und Durchführung einer Transformation?*

Patric Dahse: Zum einen ist auffällig, dass diejenigen, die die Analyse und eine fundierte Bestandserfassung als erfolgskritischen Teil ihrer Transformation höher

ÜBER DIE TRANSFORMATIONSSTUDIE 2025

Im Rahmen der Transformationsstudie 2025 wurden 909 Manager mittelständischer und großer Unternehmen von einem Marktforschungsunternehmen ausgewählt und anonym in den Ländern Deutschland, Österreich, Schweiz, Großbritannien und Frankreich, Schweden, Dänemark, Norwegen, Finnland, Polen, Ungarn, Slowakei und USA befragt. Alle Befragten gaben an, ein Transformationsprojekt entweder aktuell durchzuführen oder innerhalb der letzten zwei Jahre abgeschlossen zu haben.

Mehr als 75 Prozent der Befragten arbeiten in Unternehmen mit mehr als 1.000 Mitarbeitern, fast 20 Prozent aller Umfrageteilnehmer sind IT-Entscheider von Unternehmen mit mehr als 10.000 Mitarbeitern. Die Befragung wurde im Februar/März 2025 durchgeführt.

beurteilt haben, auch öfter angeben, alle ihre Ziele erreicht zu haben. Dies verdeutlicht die Wichtigkeit einer soliden, fundierten und umfassenden Vorbereitung.

Zweitens ist interessant, dass diejenigen die ihre Transformationsziele vollständig erreicht haben, zu 36 Prozent ihre Transformation per Brownfield-Verfahren umgesetzt haben. Allerdings erhöht das die Gefahr, dass Innovationen durch die Transformation auf der Strecke bleiben, was dem ausgeprägten Wunsch für die Einführung neuer Technologien wie Künstliche Intelligenz widerspricht.

Ulrich Parthier: *Was ist mit den Budgets. Haben die Erfahrungen und vielleicht auch die Studie zu besseren Ergebnissen geführt?*

Patric Dahse: An dieser Stelle sehen wir aufgrund der neuesten Studienergebnisse noch großen Handlungsbedarf. Über 82 Prozent gaben an, dass sie ihr geplantes Budget nicht einhalten konnten. Davon haben 56,5 Prozent ihr Budget, um mindestens 10 Prozent überschritten. Um 20 Prozent oder mehr haben 30 Prozent der Befragten ihr Budget überzogen. Das ist insgesamt etwas weniger als in der letzten Stichprobe von 2024, aber es ist nach wie vor viel zu hoch.

Ulrich Parthier: *Was ist somit Ihr Fazit der diesjährigen Studie?*

Patric Dahse: Über die Jahre hinweg werden IT- und Datentransformationen geplanter und strukturierter. Das ist gut so, denn künftig wird es aufgrund kürzerer Softwarezyklen viel mehr Transformationen geben. Unternehmen benötigen daher eine Plattform, mit der sie ihre Daten unkompliziert, schnell und vor allem mit höherer Qualität auf andere Systeme umziehen können. Genau da setzt unsere zentrale Plattform, die Natuvion Data Conversion Suite (DCS), an, mit der KI-gestützt die Transformationszeit um mindestens 30 Prozent verkürzt werden kann. Wo ist der Zusammenhang? Die Erkenntnisse unserer Studien fließen natürlich auch in unsere Transformationsplattform ein.

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

Fragmentierte IT-Verwaltung im Griff

EINE ÜBERGREIFENDE MANAGEMENT-PLATTFORM FÜR ALLE GERÄTE

In den heute üblichen gemischten IT-Infrastrukturen aus mobilen Geräten, Windows-PCs und Servern fahren IT-Abteilungen besser, die alles über eine einheitliche Plattform verwalten. Wie das geht, zeigt das Beispiel eines mittelständischen Medizingeräteherstellers.

Auch wenn einige – auch große – Unternehmen ihre Beschäftigten mittlerweile wieder mehr ins Büro binden wollen: Den Megatrend der heutigen Arbeitswelt „Remote Work" wird dies nicht aufhalten. Von überall her auf Dokumente zugreifen oder an Besprechungen teilnehmen erfordert leistungsfähige mobile Geräte – sie zu managen eine spezielle Software wie die cloud-basierte Endgeräteverwaltung Microsoft Intune. Praktisch und vor allem kostenlos, denn sie ist bereits im Microsoft 365 E3 Enterprise-Lizenzpaket enthalten.

DAS NEBENEINANDERHER ZWEIER VERWALTUNGSLÖSUNGEN BEDEUTET IMMER, ZWISCHEN MEHREREN KONSOLEN SWITCHEN ZU MÜSSEN.

Sebastian Weber, Chief Evangelist, Aagon GmbH, www.aagon.com

Für Silke Färbinger, IT-Leiterin eines mittelständischen Medizintechnikherstellers, war es deshalb keine Frage, auf Intune zu setzen. „Uns war schon bewusst, dass wir damit eine Doppelstruktur aufbauen", so die 38jährige. Denn um die stationären IT-Desktops und -Assets zu verwalten, ist bereits seit einigen Jahren eine Unified-Endpoint-Management (UEM)-Plattform im Einsatz, die ACMP Suite von Aagon.

Umständlicher Wechsel zwischen mehreren Konsolen

Das Nebeneinanderher zweier Verwaltungslösungen bedeutet immer, zwischen mehreren Konsolen switchen zu müssen: Intune, ACMP, Entra ID (Azure AD) und das lokale Active Directory (AD). Das erschwert IT-Admins die Übersicht, denn Sicherheits- und Compliance-Berichte liegen verstreut über verschiedene Tools.

„Zu diesem Transparenzproblem gesellt sich die Tatsache, dass Änderungen an einem System – etwa die Benutzerverwaltung in Entra ID – nicht automatisch von der Nachbarlösung übernommen werden, oder wenn, dann oft nur verzögert", berichtet Silke Färbinger. „Eines Morgens habe ich zum Beispiel bemerkt, dass ein Windows-Update auf mehreren Clients nicht durchgeführt wurde. Intune meldete, dass die Geräte compliant sind, doch ACMP zeigte fehlende Patches. Wir mussten manuell nacharbeiten – ein ineffizienter Prozess, der sich durch eine einheitliche Verwaltung vermeiden ließe."

Funktionsausfall bei Netzausfall

Das Handling oder die mangelnde Kommunikation sind nur die eine Seite. Hinzu kommen handfeste funktionale Handicaps, die jede Lösung mitbringt – eben, weil sie speziell auf ihren ureigenen Verwendungszweck konzipiert ist: Intune deckt zwar Mobile Device Management und einige Endpoint-Management-Funktionen ab, Server aber werden nur mit zusätzlichen Tools unterstützt. SNMP-Geräte bleiben gleich ganz außen vor – es sei denn, man investiert in weitere kostenpflichtige Add-ons.

Bei der Bereitstellung von Anwendungen über Intune verharren immer wieder einige Geräte im Status „waiting on install status" – und dies über 24 Stunden hinweg. Immer wieder kam es in dem Unternehmen zudem vor, dass die Attack Surface Reduction (ASR)-Regel „Block Credential Stealing from the Windows local security authority subsystem" die Installation von Microsoft 365-Anwendungen beeinträchtigte. Es führte dazu, dass Installationen bei zwei Prozent stoppten, sowohl bei Bereitstellungen über Intune als auch bei manuellen Installationen. Cloud-Dienste benötigen außerdem Internet; bei einem Netzausfall sind bestimmte Verwaltungsfunktionen nicht verfügbar.

Demgegenüber läuft das On-Premises-UEM-System auf den eigenen Servern des Medizintechnikherstellers. Es beinhaltet spezialisierte Agenten für eine umfassende Kontrolle, und die Datenhoheit verbleibt im Unternehmen. Allerdings sind Investitionen in Hardware und Lizenzen notwendig. Und der – auch für Silke Färbinger – bedeutendste Pain Point: die nur eingeschränkte Unterstützung mobiler Endgeräte, die sich in einer zunehmend mobilen Arbeitswelt inzwischen als Nachteil erweist. „Diese unterschiedlichen Funktionalitäten muss man seiner Geschäftsführung erst einmal vermitteln" sagt sie. „Sonst denkt diese, man könne das teure UEM-System im Grunde sparen und gleich alles mit dem bereits bezahlten Intune erledigen."

Die Ankündigung, dass ACMP-Hersteller Aagon seiner Software künftig ein eigenes Intune-Management-Modul hinzufügen würde, ließ die IT-Leiterin daher aufhorchen. „Das würde bedeuten, dass wir hybride Infrastrukturen einheitlich verwal-

ten und die Daten jeweils aus dem führenden System importieren können."

Übergreifende Management-Plattform für alle Geräte

Aagon hatte Intune bereits vor längerem mittels eines Connectors in seine Konsole integriert und damit den Weg Richtung hybrid beschritten. Die jetzt – vom Medizingerätehersteller genutzte – Intune-Integration geht darüber noch einmal weit hinaus. Wird die Konsole der Plattform geöffnet, hat man darin alles im Blick: Windows-Clients, Server, Tablets, Android-Smartphones und iPhones vereint in einer Oberfläche – eine übergreifende Management-Plattform für alle Geräte, inklusive Mobile Device Management.

Basierend auf den Daten aus Intune können App-Zuweisungen klar und intuitiv dargestellt werden. Entra ID wird mit ACMP abgestimmt, so dass ein durchgängiges Benutzer- und Geräte-Management gewährleistet wird. „Mit dieser hybriden Lösung können wir kritische Systeme auch ohne Internetverbindung sicher betreiben", freut sich Martin Fröbel, IT-Admin des mittelständischen Unternehmens. „Und auch Sicherheit im Client Management ist jetzt kein großer Aufwand mehr. Da alles zentral verwaltet ist, bildet das UEM-System jede Lücke, jeden Bericht und jeden Patch ab – eine Sorge weniger!"

Sicherheitszonen individuell konfigurieren

Isolierte Systeme nämlich sind nicht nur ineffizient, sondern auch riskant. Die Kombination aus Intune für Mobile Device Management und ACMP für erweiterte Steuerung und Sicherheitsmanagement schließt diese Lücke. Dass mit dem lokal betriebenen UEM, anders als bei einer Cloud-Lösung, sensible Informationen innerhalb der eigenen Infrastruktur verbleiben, ist insbesondere für deutsche Mittelständler wichtig. Zudem können mit einer (mandantenfähigen) UEM-Lösung im eigenen Haus Sicherheitszonen individueller konfiguriert werden als bei einem Cloud-System „von der Stange".

Gleichzeitig ist der rechtliche Aufwand geringer. Datenverarbeitungsverträge mit Dienstleistern müssen nicht aufwändig verhandelt werden beziehungsweise sie beschränken sich auf die eigentliche Geschäftsbeziehung – und eben nicht auf Firmen- oder Kundendaten.

Durchgängige Workflows für alle Geräte und Server

Dass Aagon sich des Themas Mobile Device Management angenommen und mit Intune auch noch die meistverbreitete Cloud-Lösung in seine Konsole integriert hat, hält Silke Färbinger für einen besonders cleveren Schachzug. „Ein UEM mit keiner oder nur eingeschränkter Unterstützung mobiler Endgeräte ist heute einfach unvollständig. Man braucht dann eine zweite Lösung, und das Nebeneinander mehrerer Plattformen macht die Arbeit für Admins immer unübersichtlich." Mehr Effizienz, Transparenz und Sicherheit sowie durchgängige Workflows für alle Geräte und Server haben sie und ihr Team jetzt mit dem neuen Hybrid-UEM von Aagon, dank des Moduls ACMP Intune Management.

Sebastian Weber

MEHR WERT
Hybrides UEM

Data Loss Prevention neu gedacht

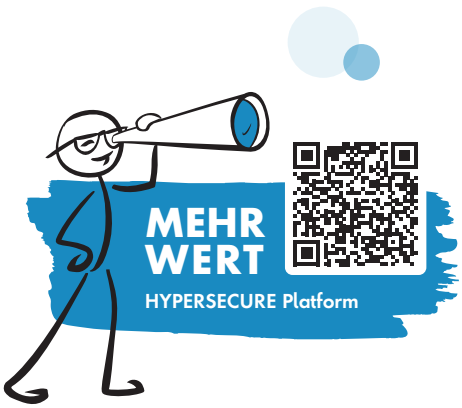
WARUM DER SCHUTZ SENSIBLER DATEN NEUE LÖSUNGEN BRAUCHT

Moderne Arbeitsumgebungen erstrecken sich heute über lokale, mobile und Cloud-Infrastrukturen und sensible Informationen wandern blitzschnell durch hybride und globale Netzwerke. Der Verlust von Daten und Datenschutzverletzungen haben dabei nicht nur enorme finanzielle und rechtliche Folgen, sondern erschüttern auch nachhaltig das Vertrauen von Kunden und Partnern.

Diese Realität verlangt nach einer Data-Loss-Prevention (DLP), die diese Entwicklungen berücksichtigt; eine DLP, die sich als integraler Bestandteil einer Zero-Trust-Strategie versteht – ganzheitlich, plattformübergreifend und zukunftsfähig.

Die neue Welt der Endpoints und Perimeter

Traditionell als Arbeitsplatzrechner definiert, sind Endpoints heute viel mehr: von lokalen Geräten zu virtuellen Maschinen über Container, Cloud-Speicher bis hin zu Web-Anwendungen. Für diese Vielfalt müssen Sicherheitsmechanismen greifen, die Daten in all ihren Lebensphasen schützen – sei es „at rest", „in motion" oder „in use" – unabhängig davon, wo die Daten erhoben, gespeichert oder verarbeitet werden.



ENDPOINT PROTECTION MUSS MEHR SEIN ALS NUR EIN SCHUTZWALL.

Andreas Fuchs, Director Product Management & Strategic Platform Partnerships, DriveLock SE, www.drivelock.com

Daten befinden sich nicht mehr nur auf lokalen Servern – sie wandern durch hybride Infrastrukturen, private Endgeräte, Cloud-Speicher und mobile Anwendungen. Damit existiert der traditionelle Perimeter nicht mehr und verliert an Bedeutung. Wir müssen mit der Tatsache leben, dass Endpoints immer und von überall her Angriffen ausgesetzt sein können. Endpoint Protection muss also mehr sein als nur ein Schutzwall. Sie muss sicherstellen, dass jeder digitale Eintrittspunkt, von physischen Geräten bis hin zu komplexen virtuellen Umgebungen, streng gesichert ist. Lösungen wie die von DriveLock setzen frühzeitig in der Sicherheitskette an und überwachen und regulieren die Anwendungskontrolle, überprüfen das Verhalten zugelassener Software und erzwingen eine umfassende Verschlüsselung. Sie gewährleisten, dass Unternehmen potenzielle Bedrohungen identifizieren und abwehren, bevor diese eine Chance haben, Schaden anzurichten.

Von DLP zu Cloud-DLP: Schutz im mehrdimensionalen Datenraum

Die Sicherheit endet aber nicht am physischen Endpoint. In der cloudbasierten Arbeitswelt müssen auch Daten, die über Plattformen wie Microsoft 365, SharePoint, OneDrive, Google Workspace oder AWS verarbeitet und gespeichert werden, wirksam vor unbefugtem Zugriff geschützt werden.

Eine Cloud-Data-Loss-Prevention integriert sich nahtlos in diese Dienste, scannt gespeicherte Inhalte automatisiert, erkennt sensible Daten auf Basis vordefinierter Klassifizierungen, verschlüsselt sie gezielt und setzt unternehmensweite Sicherheitsrichtlinien durch.

Im Falle potenzieller Risiken werden Administratoren umgehend benachrichtigt, sodass alle datenschutzrelevanten Vorgänge lückenlos nachvollzogen und bei Bedarf regulatorisch belegt werden können.

Transparenz, Zugriffskontrolle und „Least Privilege"

Mit der Verlagerung von Daten in die Cloud wird die Kontrolle über geteilte Informationen zu einer zentralen sicher-

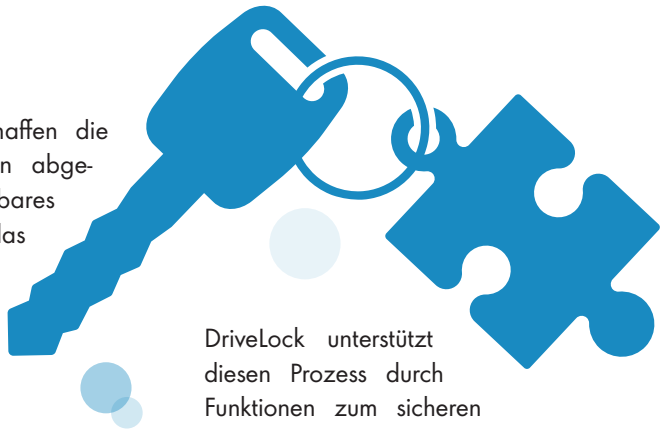
heitsrelevanten Aufgabe. Ohne klare Übersicht kann keine wirksame Absicherung erfolgen. Unternehmen müssen nachvollziehen können, welche Daten mit welchen internen oder externen Stellen geteilt wurden und in welcher Form. Erst diese Transparenz ermöglicht es, das Sicherheitsprinzip des „Least Privilege“

- also den minimal notwendigen Zugriff
- effektiv umzusetzen.

DriveLock stellt mit seiner HYPERSECURE Platform gezielt Funktionen bereit, um den Zugriff auf sensible Inhalte kontrollierbar und dokumentierbar zu gestalten. Dazu zählen:

- die Visualisierung sämtlicher geteilten Inhalte,
- die Möglichkeit zur Anpassung bestehender Rechteverteilungen,
- die Protokollierung von Zugriffen auf personenbezogene Daten (PII),
- sowie die Integration in ein differenziertes Rollen- und Rechtekonzept.

Diese Maßnahmen schaffen die Grundlage für ein fein abgestimmtes und überprüfbares Zugriffsmanagement, das den Anforderungen moderner Compliance- und Datenschutzrichtlinien gerecht wird.



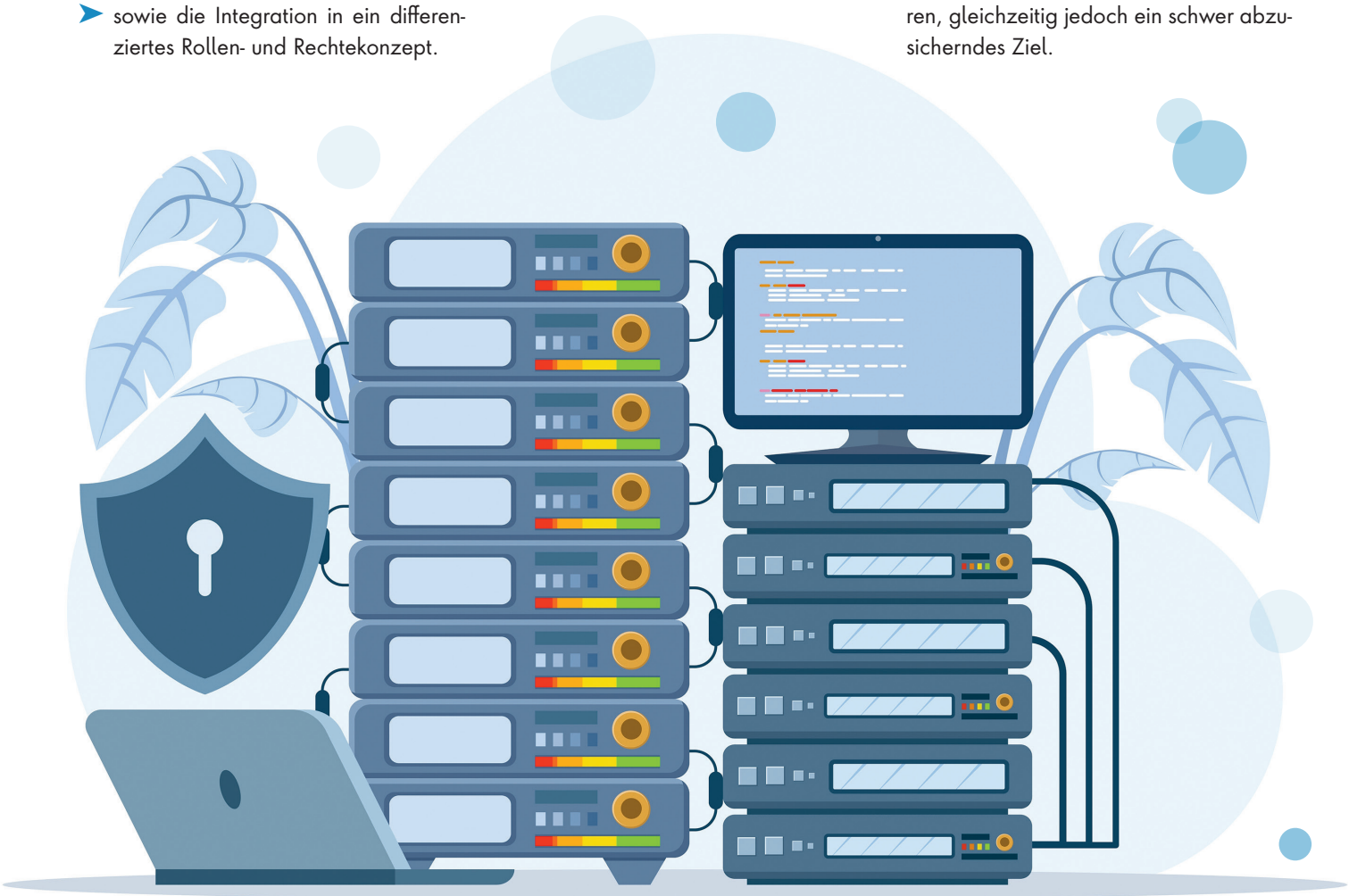
Sicheres Löschen und dokumentierter Datenschutz

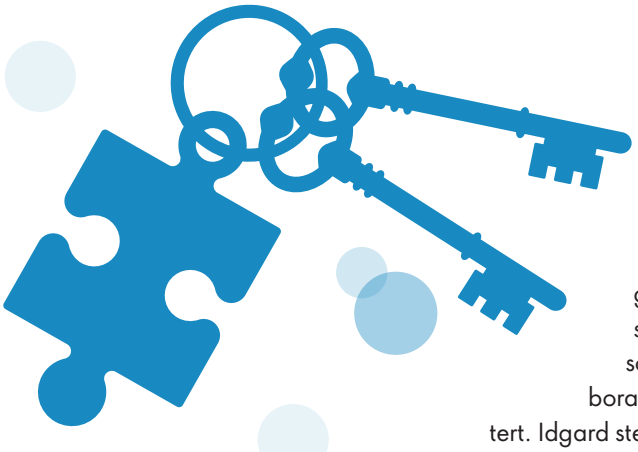
Datenschutz endet nicht mit dem Speichern oder Teilen von Informationen – auch das sichere und nachweisbare Löschen von Daten ist ein wesentlicher Bestandteil regulatorischer und technischer Sicherheitsanforderungen. Insbesondere im Kontext der DSGVO, etwa im Rahmen des Art. 17 („Recht auf Vergessenwerden“), ist ein vollständiges und revisionssicheres Entfernen sensibler Daten über verschiedene Speichermedien hinweg zwingend erforderlich.

DriveLock unterstützt diesen Prozess durch Funktionen zum sicheren Löschen auf USB-Sticks, Festplatten und in der Cloud, wobei alle Vorgänge auditkonform dokumentiert werden zum Beispiel im Rahmen von Offboarding-Prozessen.

Die Welt der Workloads – neue Herausforderungen für DLP

Workloads sind die neuen digitalen Arbeitslasten - Dienste und Anwendungen, die in Clustern, Containern und virtuellen Maschinen ausgeführt werden. Sie kommunizieren über APIs, lassen sich dynamisch skalieren und ermöglichen ein Höchstmaß an Flexibilität – ideale Voraussetzungen für moderne IT-Architekturen, gleichzeitig jedoch ein schwer abzusicherndes Ziel.





Denn Workloads sind häufig kurzlebig, automatisiert erzeugt und über verschiedene Plattformen verteilt. Herkömmliche DLP-Lösungen, die auf feste Endgeräte fokussiert sind, stoßen hier an ihre Grenzen. Umso wichtiger ist es, Sicherheitsstrategien zu entwickeln, die diesem dynamischen Umfeld gerecht werden.

Die HYPERSECURE Plattform von DriveLock erkennt Schwachstellen innerhalb solcher Workload-Umgebungen, überwacht deren Verhalten in Echtzeit und erlaubt ausschließlich die Ausführung verifizierter Images – ein Ansatz, der funktional einem Allow-Listing entspricht. Auf diese Weise lassen sich Sicherheitsvorfälle proaktiv verhindern, bevor sie sich ausbreiten oder kritische Daten gefährden.

Mit der Akquise von idgard und seinen Lösungen für sicheres File Sharing hat DriveLock sein Portfolio um eine Lösung für den geschützten Austausch sensibler Informationen insbesondere in Cloud- und Kollaborationsumgebungen erweitert. Idgard stellt geschützte Datenräume zur Verfügung, die mit vollständiger Protokollierung und individuell steuerbarer Verschlüsselung ausgestattet sind.

Diese Funktionen stärken nicht nur die Datenhoheit innerhalb digitaler Prozesse, sondern ermöglichen auch eine präzise Nachvollziehbarkeit sämtlicher Zugriffe und Veränderungen, wie sie für Audits, Compliance-Prüfungen oder regulatorische Anforderungen erforderlich ist.

Idgard ist damit eine essenzielle Ergänzung zur Endpoint Protection von DriveLock: Gemeinsam entsteht eine durchgängige Sicherheitskette, die sich über alle Phasen des Datenlebenszyklus erstreckt – von der lokalen Verarbeitung über den sicheren Austausch bis hin zur revisionssicheren Löschung. Während DriveLock den Schutz auf Endpoint-Ebene gewährleistet, sichert idgard den vertraulichen Austausch und die strukturierte Verwaltung sensibler Daten in der Cloud.

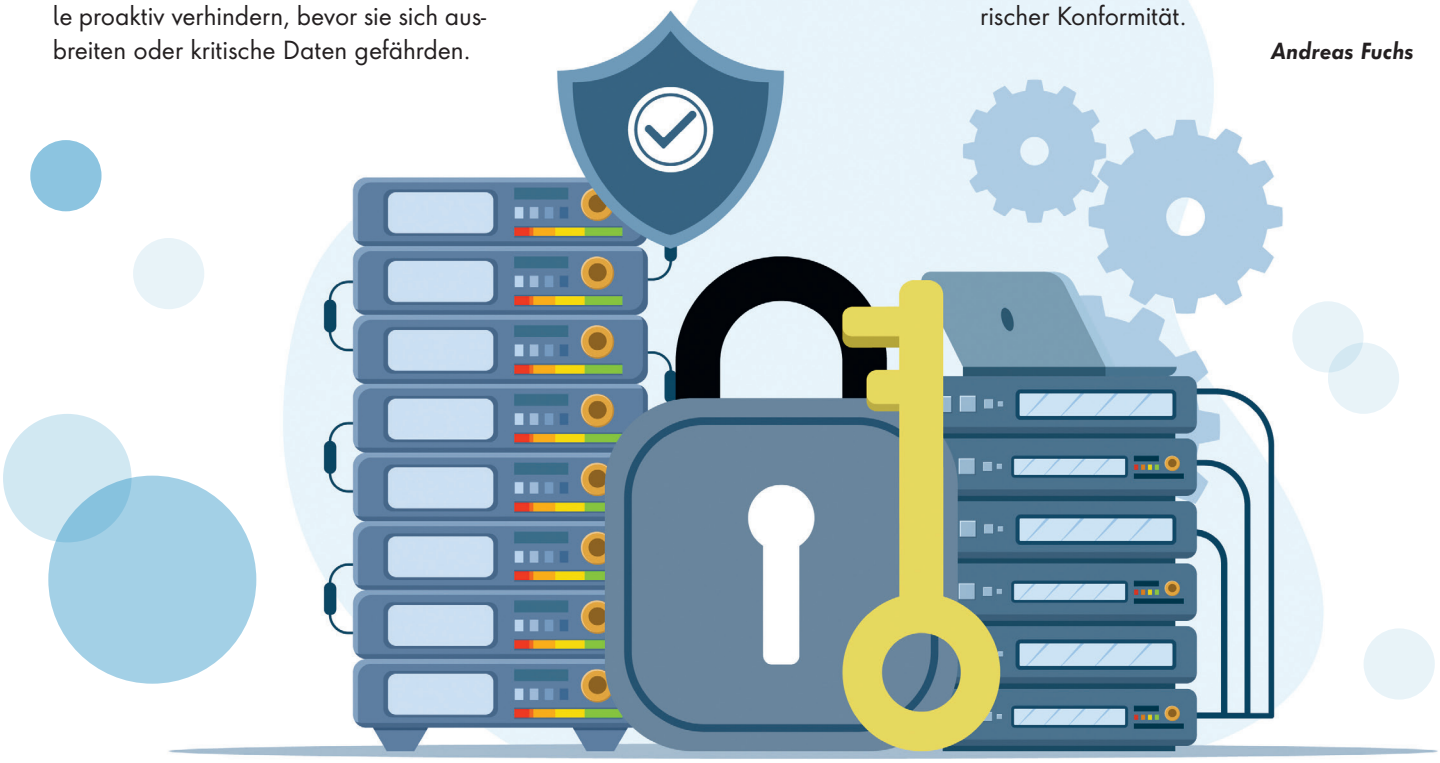
Diese Kombination ermöglicht Unternehmen, die wachsende Komplexität hybrider IT-Landschaften souverän zu bewältigen, ohne dabei Abstriche bei Mobilität, Effizienz oder Datenschutz machen zu müssen.

Fazit: Zwei starke Partner für ganzheitliche Datensicherheit

Unternehmen und Organisationen benötigen eine leistungsfähige und integrierte Sicherheitslösung, die den Anforderungen moderner, hybrider Arbeitsumgebungen gerecht wird und sensible Daten entlang ihres gesamten Lebenszyklus – von der Entstehung über die Nutzung bis zur sicheren Löschung – schützt.

Dieser vernetzte Ansatz eröffnet nicht nur eine tiefgreifende Schutzwirkung gegen Datenverluste und Sicherheitsvorfälle, sondern unterstützt auch die Umsetzung ganzheitlicher Sicherheitskonzepte wie Zero Trust und Least Privilege und verbindet technologische Effizienz mit regulatorischer Konformität.

Andreas Fuchs



OFFICE 2024 UND MICROSOFT 365

DAS PRAXISBUCH

Dieses praktische Handbuch unterstützt Sie dabei, Office 2024 bzw. Microsoft 365 auf dem PC, Notebook oder Tablet gekonnt anzuwenden. Ob im Büro, Studium, in der Ausbildung, für private Anlässe oder Ihren Verein, konkrete Fallbeispiele und leicht nachvollziehbare Praxislösungen helfen Ihnen dabei, Ihre Office-Projekte umzusetzen. So finden Sie sich rasch in Word, Excel, PowerPoint und Outlook zurecht, erstellen Dokumente, Tabellen und Präsentationen und nutzen die neuen KI-Funktionen in Copilot. Mit diesem umfassenden Nachschlagewerk sind Sie für den Office-Alltag gut gerüstet.

Office 2024 und Microsoft 365
Das Praxisbuch;
Wolfram Gieseke,
Markt + Technik Verlag GmbH; 05-2025

Aus dem Inhalt:

- Office 2024: Neuerungen und erste Schritte
- Cloud, Dateiformate und Co.: wichtige Office-Grundfunktionen
- KI-Funktionen in Office 2024 und Microsoft 365 - Mit Word ansprechende Dokumente gestalten
- Excel – Daten übersichtlich aufbereiten und überzeugend präsentieren
- Mit PowerPoint beeindruckende Präsentationen erstellen
- Mit Outlook mailen und organisieren
- Nahtlose Zusammenarbeit zwischen den Office-Programmen
- Hilfreiche Tastenkombinationen

noris network

Ihr Partner für **sichere IT im Finanzwesen**

- Zertifizierte Rechenzentren in Deutschland bis **TÜViT-TSI-Level-4**
- Georedundanz: Nürnberg – München in 2 Millisekunden
- Umfassendes Portfolio von Colocation bis Cloud-Services
- Kompetente Unterstützung durch unsere IT-Security-Experten bei der Umsetzung Ihrer Sicherheitsauflagen: **MaRisk, BAIT, VAIT, ZAIT, NIS2, DORA, IT-SiG 2.0 und FISG**
- Ausgefeilte SIEM-Systeme und eigenes SOC für die Bearbeitung und Dokumentation Ihrer Security-Events

Jetzt informieren

KÜNSTLICHE NEURONALE NETZE

DIE WELT DER GENERATIVEN KI VERSTEHEN

Dieses Lehrbuch bietet eine verständliche Einführung in die Welt der neuronalen Netze, die für ein breites Publikum zugänglich ist. Es erklärt grundlegende Algorithmen und Verfahren, die neuronale Netze antreiben, ohne tiefere mathematische Vorkenntnisse oder Programmiererfahrung vorauszusetzen.

Die Leser lernen, wie einfache neuronale Netzwerke aufgebaut, trainiert und getestet werden. Darauf aufbauend werden fortgeschrittene Themen wie Autoencoder, autoregressive Modelle, Faltungsnetzwerke und Diffusionsmodelle erläutert. Zahlreiche praktische Beispiele und leicht nachvollziehbare Erklärungen machen das Werk zu einem praxisnahen Lehrbuch für alle, die sich in dieses zukunftsweisende Thema einarbeiten möchten.

Online finden Sie Zusatzmaterial in Form von interaktiven Anwendungen sowie Codebeispielen.

Künstliche neuronale Netze – Die Welt der generativen KI verstehen; Daniel Scholz; Carl Hanser Verlag GmbH & Co.KG; 05-2025

DSAG SPEZIAL

Unternehmen, aber besonders SAP-Anwenderunternehmen, stehen vor einem Wendepunkt ihrer digitalen Transformation. Die Herausforderung: die Balance zwischen technologischen Innovationen und praktischen Geschäftsanforderungen halten.

Während die Produktion durch intelligente Vernetzung von Lager- und Fertigungsprozessen effizienter wird, transformiert generative KI klassische Finanz-und Buchhaltungsprozesse. Selbstlernende Systeme übernehmen zunehmend regelbasierte Tätigkeiten und ermöglichen intelligente Workflow-Unterstützung. Die Sicherheit bleibt dabei ein zentraler Erfolgsfaktor.

Der DSAG-Jahreskongress 2025 thematisiert all diese zentralen Herausforderungen moderner IT-Strategien und bietet Verantwortlichen die Gelegenheit, die Balance zwischen Innovationen und Pragmatismus zu reflektieren und praxiserprobte Lösungsansätze für ihre eigenen Transformationsvorhaben zu entwickeln.

Wie Generative KI die Buchhaltung transformiert

VON DER DATENVERARBEITUNG ZUR INTELLIGENTEN ENTSCHEIDUNGSHILFE

Auch vor der Finanzwelt macht der technologische Wandel nicht halt, sondern schreitet unaufhaltsam voran. Insbesondere die Möglichkeiten der Künstlichen Intelligenz (KI) haben das Potenzial, klassische Prozesse der Rechnungsverarbeitung und Buchhaltung neu zu definieren. Was einst manuelle, regelbasierte Arbeit war, wird zunehmend von lernenden Systemen übernommen – präziser, schneller und intelligenter. Der nächste Evolutionsschritt in dieser Entwicklung: der Einsatz generativer KI (GenAI).

Von OCR zu intelligenten KI-Systemen

Traditionell beruhte die digitale Rechnungsverarbeitung auf optischer Zeichenerkennung (OCR) und regelbasierten Workflows. Doch diese Ansätze stoßen zunehmend an Grenzen – etwa bei unstrukturierten Daten, wechselnden Formaten oder unternehmensspezifischen Anforderungen. Moderne KI-Systeme, insbesondere generative Modelle, ermöglichen hingegen eine semantische Analyse von Dokumenten. Sie verstehen Inhalte im Kontext, erkennen Zusammenhänge zwischen Positionen, Zahlungszielen und Bestellreferenzen – und reichern Daten auf dieser Basis intelligent an.

Durch diese kontextuelle Interpretation können Rechnungen nicht nur schneller verarbeitet, sondern auch qualitativ hochwertiger erfasst werden. Fehleranfällige manuelle Zuordnungen werden durch algorithmisch gestützte Vorschläge unterstützt – etwa bei der Buchung auf Kostenstellen, Sachkonten oder Buchungskreise.

Selbstlernende Kontierung

Ein Kernproblem vieler Buchhaltungslösungen ist die korrekte Kontierung eingehender Rechnungen. Klassische Systeme nutzen starre Regeln, die pflegeintensiv und fehleranfällig sind. Generative KI hingegen arbeitet probabilistisch: Sie analysiert vergangene Buchungsvorgänge, lernt aus Interaktionen mit Nutzern und schlägt automatisch plausible Kontierungen vor – angepasst an den spezifischen Kontext eines Unternehmens.

Der besondere Vorteil: Die Systeme benötigen kein separates Nachtrainieren. Sie lernen kontinuierlich und verbessern ihre Vorschläge anhand der tatsächlichen Korrekturen durch die Anwender. So entsteht ein dynamischer, sich selbst optimierender Buchungsprozess.

Intelligente Workflow-Unterstützung

Ein bislang unterschätztes Einsatzfeld von KI in der Finanzabwicklung ist die auto-

matische Ermittlung zuständiger Personen für Prüf- und Freigabeprozesse. Anstatt feste Regeln für jede Organisationseinheit zu pflegen, erkennen KI-Systeme anhand von Strukturen, Historie und Workload, welche Mitarbeiter oder Abteilungen für eine Rechnung zuständig sein könnten. Dies reduziert den Verwaltungsaufwand deutlich und beschleunigt Freigabeprozesse erheblich.

Anomalieerkennung und Risikoprävention

Neben der Effizienzsteigerung rückt zunehmend auch das Thema Sicherheit in den Fokus. KI-basierte Systeme können durch Mustererkennung und historische Analysen Abweichungen und potenzielle Unregelmäßigkeiten erkennen, bevor sie kritisch werden. Dazu gehören zum Beispiel doppelte Zahlungen, unplausible Beträge oder verdächtige Lieferantenkonstellationen.

Insbesondere im Hinblick auf Compliance-Vorgaben und Fraud Detection bietet GenAI ein enormes Potenzial: Statt stichprobenartiger Prüfungen kann eine durchgängige Überwachung sämtlicher Belege erfolgen – rund um die Uhr, lernfähig und in Echtzeit.

Der unsichtbare Assistent im Hintergrund

Ein häufiges Missverständnis besteht in der Annahme, KI müsse als separates Tool eingeführt werden. Moderne Anwendungen lassen sich jedoch nahtlos in bestehende ERP-Systeme integrieren. Die KI agiert dabei im Hintergrund – als „intelligente Assistenz", die bestehende Prozesse ergänzt und optimiert, ohne sie vollständig zu ersetzen.

Für Mitarbeitende bedeutet dies eine neue Qualität in der täglichen Arbeit: weniger wiederholende Tätigkeiten, mehr Entscheidungsspielräume und bessere Informationsgrundlagen für strategische Maßnahmen.

Warum KI wichtiger bleibt denn je

Mit dem bevorstehenden verpflichtenden Einsatz von E-Rechnungen in Deutschland rückt die Frage nach der Notwendigkeit zusätzlicher Technologien in den Fokus. Tatsächlich liefern strukturierte Formate wie XRechnung oder ZUGFeRD bereits viele relevante Daten – jedoch längst nicht alle. Unternehmensspezifische Informationen, Kontextwissen oder historische Abgleiche bleiben weiterhin außerhalb dieser Standards.

KI wird daher auch in einer E-Rechnungswelt eine zentrale Rolle spielen: als Ergänzung zur strukturierten Datenerfassung, zur intelligenten Anreicherung und zur kontinuierlichen Qualitätskontrolle.

Ausblick: Der Weg zur „Autonomous Finance"

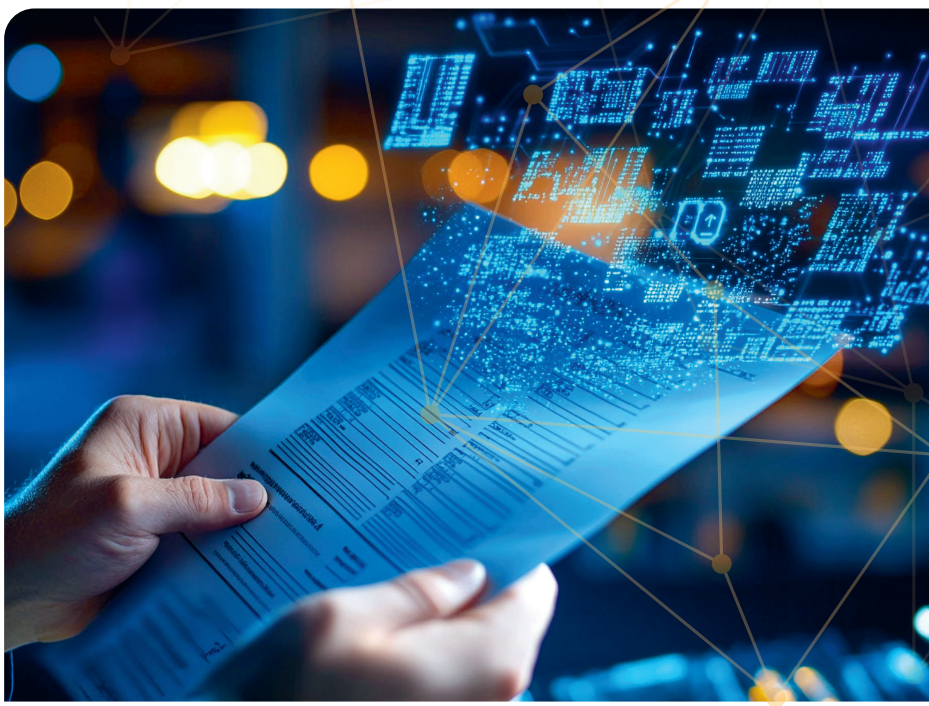
Das langfristige Ziel dieser Entwicklung ist die weitgehende Automatisierung finanzieller Kernprozesse – hin zu einem Zustand, den man als „Autonomous Finance" bezeichnen kann. In dieser Vision übernehmen KI-Systeme nicht nur Routineaufgaben, sondern entwickeln sich zu Entscheidungsunterstützern: Sie priorisieren Zahlungsströme, schlagen Optimierungen vor und erkennen Risiken frühzeitig.

UNTERNEHMEN, DIE HEUTE IN KI-SYSTEME INVESTIEREN, SCHAFFEN SICH NICHT NUR EFFIZIENZVORTEILE, SONDERN POSITIONIEREN SICH STRATEGISCH FÜR DIE DIGITALE ZUKUNFT.

Dina Ziems,
Senior Lead Marketing,
xSuite Group GmbH,
www.xsuite.com

Unternehmen, die heute in diese Technologien investieren, schaffen sich nicht nur Effizienzvorteile, sondern positionieren sich strategisch für die digitale Zukunft. Generative KI wird dabei zu einem der entscheidenden Enabler.

Dina Ziems



Enterprise Architektur

ZWISCHEN POTENZIAL UND REALITÄT

SAP LeanIX veröffentlichte die Ergebnisse der SAP LeanIX EA Insights 2025, basierend auf einer Online-Befragung von 360 Enterprise Architekten. Es zeigt sich, dass in 64 Prozent der Unternehmen in den letzten zwei Jahren die Investitionen in EA zugenommen haben.

Gleichzeitig gaben die Befragten an, dass EA in den Firmen in erster Linie als administrative und steuernde Funktion wahrgenommen wird. Das mag daran liegen, dass die Erstellung eines zuverlässigen Inventars von Applikationen und IT-Ressourcen sowie die Etablierung eines Governance-Frameworks ganz oben auf der Prioritätenliste der EA-Teams stehen.

Wahrnehmungsproblem trotz steigender Relevanz

Nur 14 Prozent der befragten EA-Experten fühlen sich als vollwertige Business-Partner anerkannt. Stattdessen dominiert die Sicht auf EA als administrative IT-Funktion. Besonders alarmierend: 29 Prozent berichten, dass die meisten Kollegen nicht einmal wissen, dass ein EA-Team existiert – selbst in 21 Prozent der Unternehmen mit mindestens dreijähriger EA-Praxis.

Fragmentierte IT-Landschaften als größte Herausforderung

73 Prozent der Enterprise Architekten identifizieren fragmentierte IT-Umgebungen als Hauptproblem. Entsprechend steht die Erstellung eines zuverlässigen Applikations- und IT-Ressourcen-Inventars mit 66 Prozent Zustimmung ganz oben auf der Prioritätenliste für 2025. Dahinter folgen die Etablierung eines EA-Governance-Rahmenwerks (85 Prozent bewerten dies als hoch- oder mittelpriorig) und Kosteneinsparungen durch Applikationsrationalisierung (65 Prozent).

Governance-Lücke bremst Entscheidungen

Obwohl 91 Prozent der Befragten transparente Architektur-Entscheidungsprozesse als wichtig erachten, haben nur 40 Prozent der Unternehmen solche etabliert. Die Folge: In 51 Prozent der Organisationen dauern Architektur-Entscheidungen einen Monat oder länger. Unternehmen mit umfassenden Governance-Maßnahmen treffen hingegen deutlich schnellere Entscheidungen.

MEHR WERT
SAP LeanIX EA Insights 2025

Besonders problematisch: Nur 15 Prozent der Architecture Review Boards binden das Business ein, obwohl 64 Prozent dies als wichtig bewerten. 81 Prozent dieser Gremien bestehen ausschließlich aus IT-Personal.

KI-Einführung: Chance mit Risiken

Während die Wirtschaft KI-Euphorie zeigt, mahnen Enterprise Architekten zur Vorsicht. Nur 27 Prozent unterstützen einen „AI-first"-Ansatz. 68 Prozent sehen KI aufgrund von Problemen bei Erklärbarkeit, Verzerrung und Datenschutz als besonders behandlungsbedürftig an.

Empfehlungen für die Praxis

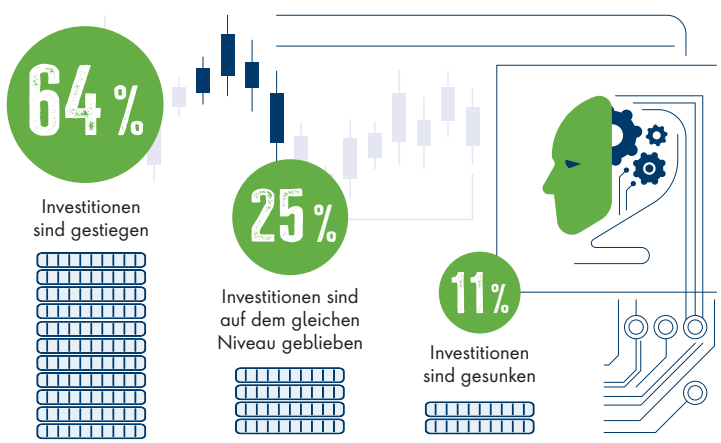
Die Studie identifiziert drei Erfolgsfaktoren:

- **Kommunikation** – A-Aktivitäten müssen als strategische Enabler statt als administrative Hürden dargestellt werden.
- **Konsequenz** – als wichtig erkannte Governance-Maßnahmen müssen konsequent umgesetzt werden.
- **Kollaboration** – das Business muss aktiv in EA-Prozesse eingebunden werden.

Enterprise Architekten, die diese Prinzipien befolgen und ihre scheinbar administrativen Aufgaben als Grundlage strategischer Geschäftsziele kommunizieren, können ihre Rolle als unverzichtbare Business-Partner festigen und das volle Potenzial der EA ausschöpfen.

www.leanix.net/de/

HAT IHR UNTERNEHMEN IN DEN LETZTEN BEIDEN JAHREN MEHR ODER WENIGER IN DIE EA-PRAXIS INVESTIERT?



SAP EWM und SAP DM im Doppelpack

WIE INTELLIGENTE VERZAHNUNG VON LAGER UND PRODUKTION GELINGT

Mit rund 1,8 Milliarden Euro Umsatz gehört ElringKlinger zu den führenden Anbietern von Systemlösungen und Komponenten für Elektromobilität, Leichtbau sowie Dichtungs- und Abschirmtechnik. Um auch in Zukunft die Mobilität mitzugestalten, schärft der Konzern mit seiner Transformationsstrategie SHAPE30 sein Profil und hat fünf Erfolgsfaktoren herausgebildet. Einer dieser Erfolgsfaktoren ist eine umfangreiche digitale Transformation, die auch eine ausgefeilte Intralogistik und moderne Produktionsprozesse beinhaltet. Dafür kombiniert das Unternehmen seit 2025 SAP Extended Warehouse Management (SAP EWM) und SAP Digital Manufacturing (SAP DM) für intelligente und ganzheitliche Logistik- und Produktionsprozesse.

Logistik und Produktion vernetzen für die digitale Fabrik

Bereits einzeln bewertet bieten SAP DM und SAP EWM Vorteile: So verwendet ElringKlinger SAP DM beispielsweise, um wichtige Anlagen und Maschinen auf dem Shopfloor an ein einheitliches System anzubinden, die Auslastung datenbasiert zu optimieren und Fehlerquoten zu verringern. Über Terminals stellt das Unternehmen den Werkerinnen und Werkern zudem leicht bedienbare digitale Dashboards zur Verfügung, die alle Informationen für den anstehenden Fertigungsschritt bereitstellen.

Für die Lager- und Logistikprozesse im Werk setzt der global aufgestellte Technologiekonzern auf SAP EWM. Damit verschafft sich das Unternehmen u.a. einen optimalen Überblick über die aktuellen Lagerbestände und kann Bestandsveränderungen automatisiert fortschreiben. Das trägt dazu bei, eine frühzeitige Beschaffung sicherzustellen und Engpässe zu vermeiden.

Den größten Nutzen entfalten SAP DM und SAP EWM vor allem dann, wenn beide Lösungen strategisch integriert und abgestimmt eingesetzt werden. ElringKlinger setzt hier richtungsweisende Maßstäbe – und entwickelte gemeinsam mit der Management- und IT-Beratung MHP entsprechende Prozesse für Intralogistik und Produktion.

FERTIGUNG UND INTRALOGISTIK PRÄSENTIEREN SICH MODERNER, TRANSPARENTER UND KONSEQUENT KUNDENZENTRIERT.

Marc Neher, Senior Manager SAP Production & Logistics (SPL), MHP Management- und IT-Beratung GmbH, www.mhp.com

Systemübergreifende End-to-End-Prozesse

Der wichtigste Effekt der neuen Prozesse: Wenn die Werkerinnen und Werker mit ihrem Fertigungsschritt beginnen, können sie via Dashboard alle benötigten Komponenten digital im Lager anfordern. In SAP DM entsteht dabei eine Bereitstellungsanforderung, die das System automatisch an SAP EWM übermittelt. Die Mitarbeitenden in der Intralogistik bestätigen den Auftrag und stellen die angeforderten Komponenten rechtzeitig am richtigen Ort und in der erforderlichen Menge für die Produktion bereit.

Kommt es während der Fertigung zu Ausschuss, wird auch dies in SAP DM erfasst. Anschließend können die Shopfloor-Mitarbeitenden Ersatzkomponenten schnell erneut anfordern. So entsteht ein reibungsloser End-to-End-Prozess zwischen Lager und Produktion, der eine zügige Bereitstellung sicherstellt und eine einfache, bereichsübergreifende Abstimmung sowie hocheffiziente Fertigung ermöglicht.

Durchgängige Traceability und moderne Intralogistik

Mit der Einführung von SAP EWM und SAP DM hat ElringKlinger seine fertigungsnahen Logistik- und Produktionsprozesse erfolgreich digitalisiert und stärker miteinander vernetzt. Dadurch lässt sich der Weg eines Produkts im Fertigungsprozess jederzeit lückenlos nachvollziehen – selbst höchste Anforderungen an die Traceability werden zuverlässig erfüllt. Insgesamt präsentieren sich Fertigung und Intralogistik dadurch effektiver, transparenter und konsequent kundenzentriert.

Marc Neher

MHP
A PORSCHE COMPANY

S/4HANA-Implementierung in der Automobilindustrie

GLOBALE PROZESSE MODERNISIEREN

Automobilzulieferer stehen unter Druck durch Trendwenden oder Marktturbulenzen, Lieferkettenkrisen, Rohstoffmangel und hohe Investitionen in E-Mobilität/autonomes Fahren. Digitalisierung (KI, Blockchain, Automatisierung) senkt Kosten und treibt Innovation. Daher ersetzt der Automotive-Spezialist VOSS sein SAP ECC 6.0 durch S/4HANA für agile Prozesse, Effizienz und datengetriebene Erkenntnisse. Beim Umstieg entschied sich VOSS für einen Crossfield-Ansatz (Greenfield im Finance und Brownfield in der Logistik) mit CONSILIO.

Finance ist ein entscheidender Treiber

Mittel- bis langfristig wollten die Automotive-Spezialisten ihr „Global Finance"-Programm und somit die Digitale Transformation des Finanzwesens und des Controllings vorantreiben. Denn: Digitale Technologien verhelfen dem Finanzwesen zu einer neuen Rolle im Unternehmen. Sie brechen althergebrachte Arbeitsprozesse auf, fördern den Wandel von Mitarbeitern und helfen bei der Differenzierung von Marktbegleitern durch neue Erkenntnisse bei der digitalen Finanz-Transformation. Das Konzept „Global Finance" setzt damit die Leitplanken für Themen wie Logistik oder BI-Konzept beim Wechsel auf S/4HANA.

Optimalen Partner gefunden

Als Partner für dieses Projekt haben sich die Nordrhein-Westfalen Unterstützung bei den SAP-Spezialisten von CONSILIO aus München geholt, die über eine tiefgreifende Expertise in der Automobil-Branche verfügen. „Das war eines der besten Projekte, das ich in meinem Leben in der IT realisiert habe. Maximale Komplexität, trotzdem in Time, in Scope und in Budget", resümiert Sacha Dannewitz, VP IT & Digitalization bei VOSS Automotive.

Das Vorgehen im Detail

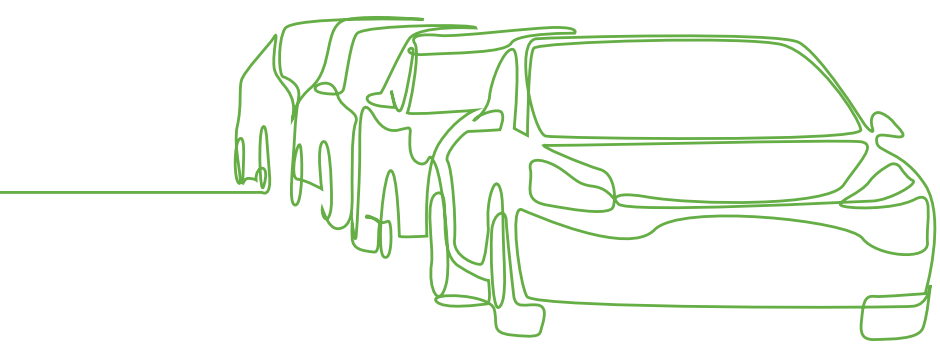
Innerhalb des „Global Finance"-Rahmens von VOSS Automotive arbeiteten die SAP-Spezialisten von CONSILIO zusammen mit den Spezialisten von VOSS in der Explore-Phase das Konzept für die Implementierung aus, das in der Realisierungsphase umgesetzt werden sollte. Die Grundlage dafür bildeten die SAP Best Practices bei der Standardisierung und Harmonisierung sowie der Automatisierung von Geschäftsprozessen im Finance und Controlling. Unterstützung für das globale Projekt holte sich CONSILIO bei Partnern wie Deloitte und SNP. In Workshops wurden dabei die Anforderungen an eine Global-Finance-Lösung definiert, ein Abgleich (FIT/GAP) mit den SAP Best Practices durchgeführt und parallel dazu die Tasks für die Realisierungsphase erarbeitet.

Fokus auf Logistik-Prozessen

Für die Bereiche Warehouse Management und Integrated Business Planning (IBP) zeigten die SAP-Spezialisten bereits während der Explore-Phase transparent darauf hin, welche Vorteile und welchen Nutzen VOSS aus den SAP-Lösungen ziehen kann.

Ein Redesign der Finance- und Controlling-Lösung mit der Einführung von SAP S/4HANA betrifft auch immer die logistischen Prozesse, weshalb die Anpassung der Organisationseinheiten im Finance und Controlling erforderlich ist – das liegt vor allem an der sehr engen Integration der logistischen Prozesse im Finance und Controlling. So lassen sich manche Ziele im Finance und Controlling nur durch eine Anpassung der logistischen Prozesse erreichen. Beispiel: Die Vereinheitlichung der Kontenpläne oder auch Umstellungen erfordern zwingend Anpassungen in den logistischen Prozessen bei Wareneingangs- und Warenausgangsbuchungen, weshalb in diesem Zusammenhang auch ein intensiver Test der logistischen Prozesse obligatorisch ist.

Für viele andere End-to-End-Prozesse (ebenfalls logistische Prozesse) erfolgt kein umfassendes Prozess-Redesign, jedoch identifizierte CONSILIO im Rahmen der Explore-Phase durch einen Prozesscheck die so genannten „Low Han-



EINE IMPLEMENTIERUNG ÜBER MEHRERE PHASEN HINWEG HÄTTE BEDEUTET, MEHRERE ERP-SYSTEME ÜBER VIELE JAHRE PARALLEL HALTEN, PFLEGEN UND UNTERHALTEN ZU MÜSSEN.

Ivo Konecny,
Partner im Bereich FICO,
CONSILIO GmbH,
www.consilio-gmbh.de

ging Fruits" (Quick-Wins) und erfasste sie in einem Backlog. VOSS Automotive hatte dadurch die Möglichkeit, am Ende der Explore-Phase zu entscheiden, welche Quick-Wins im Rahmen der Realize-Phase oder gegebenenfalls zu einem späteren Zeitpunkt ebenfalls umgesetzt werden sollen. Dazu gehörte zum Beispiel PP/DS, das während des Projektes bereits im Vorfeld ausgerollt und mit dem Go-live an den Standorten implementiert wurde.

Historische Daten bleiben erhalten

Die Migration historischer Daten ist bei der S/4HANA-Transformation essenziell. CONSILIO nutzt mit Partner SNP die Crystal Bridge Software. Bei Datenproblemen wird objektbasierte Stammdatenmigration mit automatisiertem Qualitäts- und Integritätsscreening kombiniert. VOSS setzt für Custom Code Conversion das SAP-Tool SmartShift ein.

Erfolgreiches Projektmanagement ist entscheidend. CONSILIO empfiehlt für den SAP-Umstieg die SAP-Activate-Methodologie, strukturiert in sechs Phasen: Discover, Prepare, Explore, Realize, Deploy, Run. Innerhalb dieser Phasen erfüllen die verschiedenen Streams (Arbeitsteams) die ihnen zugewiesenen Aufgaben.

Umstellung in einem Rutsch

Wenn international aktive Unternehmen wie VOSS Automotive auf S/4HANA umsteigen, stehen ihnen zwei Methoden zur Verfügung: der klassische Rollout-Ansatz (Step-by-Step) und der Big-Bang-Ansatz (In-one-Step). Beide Methoden haben ihre Vor- und Nachteile. Der Automobilist hat sich für den Umstieg auf S/4HANA in einem Big-Bang entschieden – also der Umstellung des vollständigen Systems auf ein einheitliches System inklusive Finance und Controlling für die gesamte Gruppe. „Eine Implementierung über mehrere Phasen hinweg, nicht in einem Rutsch über mehrere Länder, hätte bedeutet, mehrere ERP-Systeme über viele Jahre parallel halten, pflegen und unterhalten zu müssen und das in den verschiedenen Ländern. Das hätte sich sehr negativ auf die Effizienz und die Kosten ausgewirkt", erklärt Ivo Konecny, Partner im Bereich FICO bei CONSILIO. Mit einer Downtime von nur vier Tagen – inklusive Wochenende – ging VOSS weltweit wieder Online beziehungsweise nahm zu 100 Prozent die Produktion wieder auf.

DAS WAR EINES DER BESTEN PROJEKTE, DAS ICH IN MEINEM LEBEN IN DER IT REALISIERT HABE.

Sacha Dannewitz,
VP IT & Digitalization,
VOSS Automotive,
www.voss.net

VOSS und CONSILIO realisierten erfolgreich eine globale S/4HANA-Transformation als Crossfield-Projekt: Greenfield im Finance-Bereich kombiniert mit Brownfield in der Logistik. Der Big-Bang-Go-live über alle Standorte (China – Europa – Mexiko) gelang mit nur vier Tagen Downstime. 140 Mitarbeiter (davon 50 CONSILIO-Consultants) sicherten in zwei Jahren die effiziente Umsetzung.

Ivo Konecny

Quelle: VOSS

FÜHREN MIT ALPHA INTELLIGENCE

STARTKLAR FÜR DIE ARBEITSWELT DER ZUKUNFT

In ihrem neuen Buch stellt Barbara Liebermeister einen innovativen, integrativen Führungsansatz vor, der Führungskräfte befähigt, auch in einer Welt, die sich in einer fundamentalen Transformation befindet, die gewünschte Wirkung zu entfalten.

Führen mit Alpha Intelligence
- Startklar für die Arbeitswelt der Zukunft; Barbara Liebermeister; Haufe, 05-2025

Höchste Zeit, Führung in die Hand zu nehmen – und das nicht nur als Führungskraft, sondern auch als Mensch. Barbara Liebermeister verbindet neueste neurowissenschaftliche Erkenntnisse mit den aktuellen Veränderungen im Management und hat den Begriff der Alpha Intelligence geprägt.

Dabei handelt es sich um einen tiefgreifenden Ansatz, der Führungskräften hilft, ihre Rolle in einer postpandemischen, hybriden Arbeitswelt zu meistern. Das Ergebnis jahrelanger Forschung zeigt sich in fünf zentralen Sphären der Alpha Intelligence, in denen Führungskräfte ihre besonderen Stärken entwickeln und eine hohe Strahlkraft in ihrem Umfeld entfalten können. Die vorgestellten Praxisfälle bieten inspirierende Beispiele für eine zukunftsweisende Führung.

Das neue 208-seitige Buch knüpft an die Tatsache an, dass sich Führung zunehmend in einem Umfeld vollzieht, das sich rasant verändert – als Stichworte seien hier nur die Begriffe KI und neue Weltordnung genannt. Unser „altes" Gehirn hingegen hält noch an überholten (Denk-) Strukturen fest und versucht in „chaotischen" Situationen und Konstellationen zumindest noch die Illusion von Kontrolle aufrechtzuerhalten auch im Bereich Management und Führung.

Und dies, obwohl wir seit Jahren spüren: Die digitale Transformation, permanente Unsicherheit und stets unberechenbarer werdenden Märkte (oder die „Zeitenwende", wie wir oft verallgemeinernd sagen) erfordern eine neue Form der Führung und neue Kompetenzen bei den Führungskräften (ganz gleich, in welchen Bereichen sie tätig sind – sei es in der Wirtschaft, der Politik usw.).

xSuite
It's simple. It's digital.

Game Changer für Ihre Finanzprozesse

Künstliche Intelligenz

- Schnellere, genauere, sichere Rechnungsverarbeitung
- Automatische Vorschläge für Sachkonto, Kostenstelle, Innenauftrag, Bearbeiterfindung
- Dynamische Fraud Protection

xSuite powered by AI

SAP Certified
for clean core with SAP S/4HANA Cloud

info@xsuite.com

www.xsuite.com

SAP Business Data Cloud: Mehr als ein Hype?

BDC ALS STRATEGISCHES ELEMENT IM DATENMANAGEMENT

Stellen Sie sich vor, Ihr Unternehmen hätte einen zentralen Ort für alle Daten – strukturiert und unstrukturiert, aus SAP- wie Non-SAP-Systemen, integriert, qualifiziert und bereit für KI-Anwendungen in Echtzeit. Genau das verspricht die SAP Business Data Cloud (BDC). Doch ist sie wirklich der erhoffte Game Changer oder nur ein weiterer Name im SAP-Universum? Die valantic SAP Studie 2025 liefert dazu spannende Erkenntnisse.

Das Ende der Datensilos

Datenstrategie ist nicht mehr optional, sondern sie ist der Schlüssel zur Zukunftsfähigkeit moderner Unternehmen. Denn wer generative KI produktiv und wertstiftend einsetzen will, braucht eine konsolidierte Datenbasis. Genau hier setzt die BDC an: Statt verteilte Datenstrukturen bietet sie einen durchgängigen, semantisch einheitlichen Datenlayer, der über Systemgrenzen hinweg funktioniert. SAP BW, Datasphere & Co. waren erste Schritte in diese Richtung. Die BDC zieht nun diese Linie weiter und vereint strukturierte sowie unstrukturierte Daten auf einer Plattform.

DIE SAP BUSINESS DATA CLOUD IST MEHR ALS EIN NEUES LABEL. SIE IST DIE ANTWORT AUF DIE GRÖSSTEN HERAUSFORDERUNGEN MODERNER DATENARCHITEKTUREN.

Timo Rüb, Head of Innovation, valantic, www.valantic.com

Was die BDC besonders macht

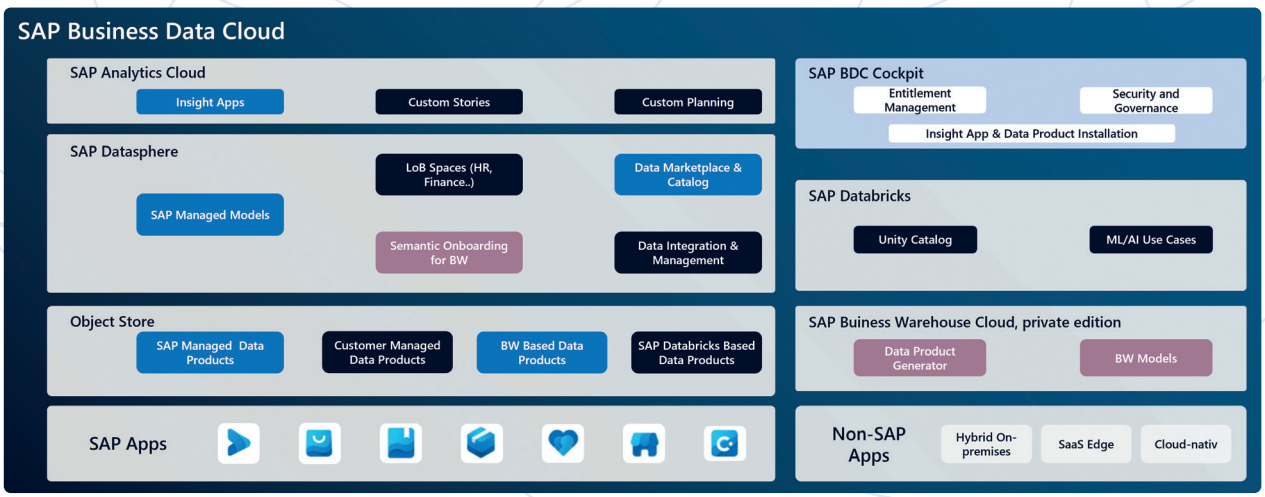
Mit der SAP Business Data Cloud bündelt SAP erstmals zentrale Datenfunktionen in einer offenen Plattform: Datenintegration, -modellierung und -katalogisierung (Datasphere), Speicherung (Object Store), Analyse, Planung und BI (SAP Analytics Cloud) und Steuerung (BDC Cockpit) greifen ineinander. Neu ist nicht nur die Kombination, sondern vor allem der Anspruch: Über alle Quellen hinweg entsteht ein harmonisiertes, semantisches Datenmodell.

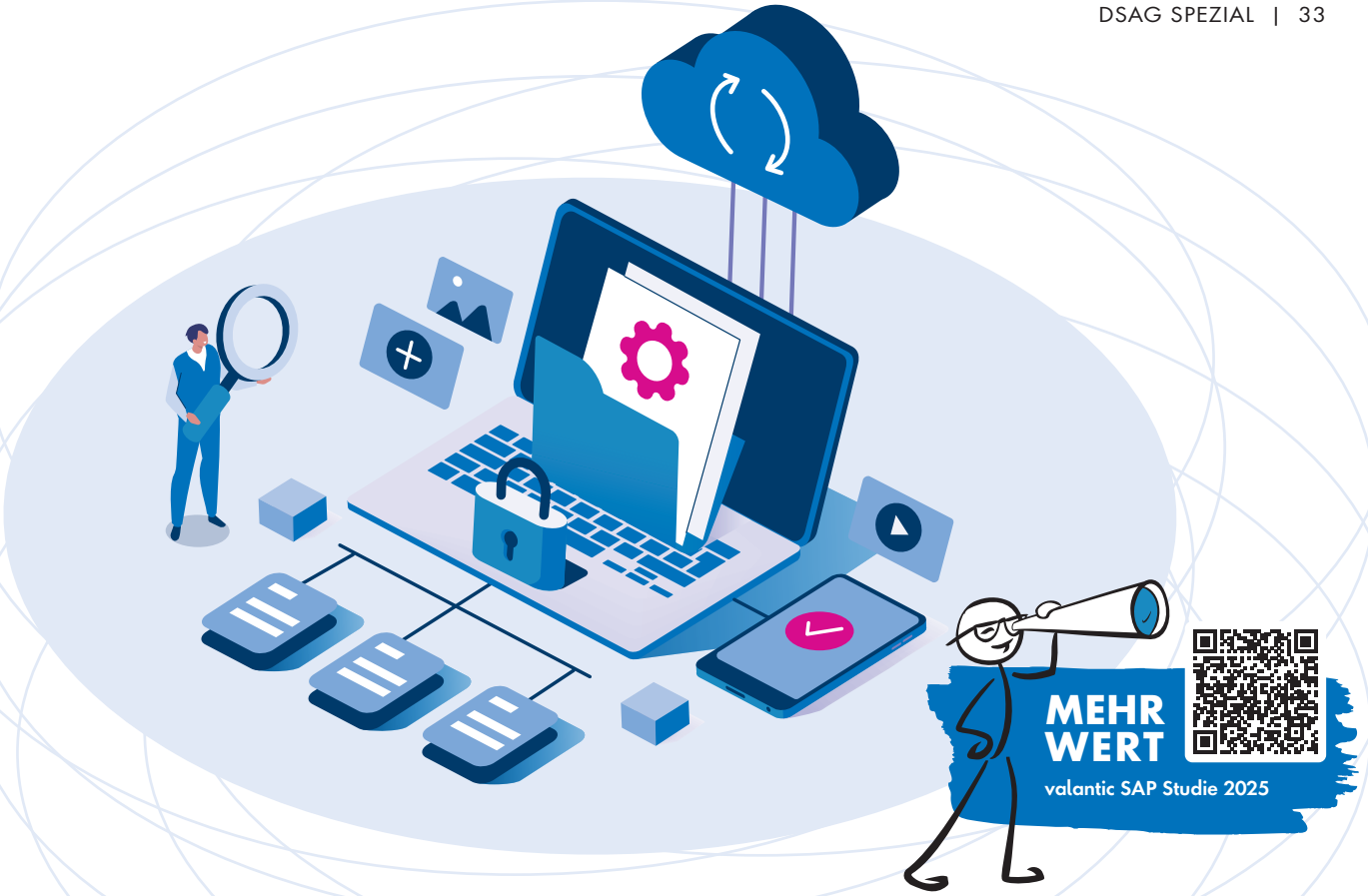
Marktstart mit Signalwirkung

Die BDC trifft offensichtlich einen Nerv. Laut der SAP Studie 2025 sehen 54 Prozent der Unternehmen in der DACH-Region die BDC bereits heute als festen Bestandteil ihrer zukünftigen Datenarchitektur. Besonders ausgeprägt ist das Interesse in der Automobilindustrie (80 %) und der diskreten Fertigung (59 %).

Bemerkenswert: Obwohl SAP die Business Data Cloud erst Anfang 2025 offi-

SAP BUSINESS AI





ziell als strategische Datenplattform positioniert hat, kennen 94 Prozent der befragten Unternehmen die BDC bereits. Ein deutliches Zeichen dafür, wie stark das Thema im Markt resoniert.

Datenstrategie als KI-Enabler

Ein wesentlicher Treiber für die Marktrelevanz der BDC ist der zunehmende Einsatz generativer KI in Unternehmen. Laut der Studie nutzten 2024 lediglich sieben Prozent der Unternehmen KI integral in ihren Geschäftsprozessen – 2025 sind es bereits 29 Prozent. Weitere 51 Prozent haben erste Anwendungen im Einsatz.

Diese Dynamik erhöht den Handlungsdruck auf IT-Entscheider, ihre Datenarchitektur grundlegend zu überdenken. Denn klar ist: Wer generative KI ernsthaft nutzen will, braucht eine durchdachte Datenarchitektur. 49 Prozent der Befragten sehen in der BDC genau die Chance, das Potenzial generativer KI endlich produktiv zu nutzen.

Wettbewerb & Investitionsschutz: Die zwei großen Herausforderungen

Trotz hoher Zustimmung gibt es Hürden: Unternehmen haben in den letzten Jahren in SAP Datasphere, BW/4HANA oder alternative Plattformen wie Snowflake investiert. 40 Prozent der Befragten nutzen heute bereits vergleichbare Lösungen anderer Anbieter.

SAP muss deshalb zweierlei leisten: Erstens eine klare Differenzierung gegenüber der Konkurrenz, zweitens einen pragmatischen Migrationspfad für Bestandskunden.

Ein Blick nach vorn: Die Vision hinter der BDC

Was heute entsteht, ist der Grundstein für eine neue Datenlogik: Künftig könnten SAP-Services und SAP-Produkte ohne den bisherigen Datentransfer zwischen verschiedenen Systemen auskommen. Stattdessen greifen sie direkt auf eine gemeinsame Persistenzschicht zu. Dadurch entfällt das Verschieben von Daten, da sie von Anfang an genau dort bereitgestellt werden, wo sie benötigt werden. Diese Idee bringt klare Vorteile: weniger Redundanzen, geringerer Speicherbedarf, einfachere Integration und ein deutlich reduzierter Datenfußabdruck. Gerade in Zeiten wachsender regulatorischer Anforderungen und steigender Nachhaltigkeitserwartungen wird dieser Architekturansatz immer relevanter.

Fazit: Mehr als nur ein Hype!

Die SAP BDC ist mehr als ein neues Label. Sie ist die Antwort auf die größten Herausforderungen moderner Datenarchitekturen wie fragmentierte Datensilos, Intransparenz und fehlende KI-Readiness. Sie bietet nicht nur Technik, sondern ein strategisches Architekturversprechen.

Für IT-Entscheider heißt das: Wer generative KI nicht nur testen, sondern produktiv einsetzen will, sollte sich mit der BDC beschäftigen. Sie bindet bestehende Systeme ein, schafft neue Freiheitsgrade für Datenzugriff und -nutzung und legt damit die Grundlage für echte Wertschöpfung im KI-Zeitalter.

Timo Rüb

DSAG-JAHRESKONGRESS

Unsere valantic Experten stehen Ihnen auf dem DSAG-Jahreskongress vom 16. bis 18. September 2025 in Bremen gerne für Fragen und persönliche Beratung zur Verfügung.

Die Themen Cloud, Künstliche Intelligenz und Security spielen beim diesjährigen DSAG-Jahreskongress eine zentrale Rolle.

Quelle: DSAG

DSAG-Jahreskongress 2025

THE ART OF BALANCE. ALLES EINE FRAGE DER BALLONS?

Der DSAG-Jahreskongress 2025 vom 16. bis 18. September in Bremen steht unter dem Motto „The Art of Balance. Alles eine Frage der Ballons?". Die Kunst der Balance besteht darin, in einem von Unsicherheit geprägten Umfeld ambitionierte Innovationen mit den realen Bedürfnissen der Anwenderunternehmen in Einklang zu bringen. Zu der Veranstaltung werden über 5.500 Teilnehmende erwartet.

SAP richtet sich konsequent neu aus und hat mit der neuen Business Suite ein ganzheitliches Zielbild für zukünftige SAP- und IT-Architekturen in der Cloud vorgegeben. Der Weg in die Cloud ist richtig, aber anspruchsvoll. Individuelle Anpassungen, bestehende Investitionen und regulatorische Vorgaben sind Ballast, den Unternehmen und Organisationen mit sich führen. Hinzu kommen die ständigen Veränderungen in einem immer komplexeren, dynamischeren und von Unsicherheit geprägten Umfeld. SAP gibt die Richtung in dieser Gemengelage vor, doch ist der Auftrieb stark genug, um alle auf die Reise mitzunehmen? Die richtige Strategie ermöglicht den Fortschritt, ohne die Praxisrealität zu vernachlässigen. So entstehen Stabilität und Sicherheit, die es braucht, um in der Cloud-Welt anzukommen. Der Zuspruch für die S/4HANA-Cloud-Strategie steigt, aber das Tempo von SAP ist nicht für alle Unternehmen und Organisationen realistisch. Hier bedarf es noch besserer Handlungsspielräume, etwa im Hinblick auf die eigene strategische Roadmap.

Lösungen müssen zusammenspielen

Die neue Business Suite kann ihr ganzes Potenzial nur dann in der Cloud entfalten, wenn Lösungen wie SAP Cloud ERP, SAP Business AI und die SAP Business Data Cloud (BDC) auf der SAP Business Technology Platform (BTP) zusammenspielen. Dies setzt eine entsprechende Adoption der Lösungen durch Unternehmen bzw. Organisationen voraus. Diesen Adoptionsprozess muss SAP noch stärker unterstützen. Der Weg in die neue SAP-Welt beginnt für viele Unternehmen immer noch mit SAP ERP On-Premises oder der alten SAP Business Suite.

Künstliche Intelligenz kann unterstützen

Unterstützung auf dem Weg in die Cloud kann Künstliche Intelligenz (KI) bieten, auch wenn KI aus Sicht der DSAG nicht zwingend auf die Cloud angewiesen ist. Sie bietet aber viele Vorteile, um die Entwicklung und den Einsatz von KI zu erleichtern. Beispielsweise durch die Skalierbarkeit von Ressourcen und den Zugriff auf große Datenmengen. Der Zugang zu KI muss, unabhängig von der Größe eines Unternehmens oder einer Organisation sowie von Cloud-Verträgen möglich sein.

Sicherheit hat hohe Relevanz

Sowohl bei den Cloud-Lösungen als auch im Bereich KI ist die Sicherheit ein zentraler Faktor. Müssen doch sowohl die Cloud-Infrastruktur als auch KI-Anwendungen vor Angriffen geschützt werden. Hier müssen hohe Standards für Datenschutz und Datensicherheit entwickelt und eingehalten werden, da KI-Systeme oft große Mengen an Daten verarbeiten. SAP ist sich der Bedeutung von Cyber-Sicherheit bewusst und bietet entsprechende Lösungen an, um Unternehmen und Organisationen zu unterstützen. Aber auch diese sind in der Pflicht, sich intensiver mit diesem Thema auseinanderzusetzen. Letztlich müssen die Themen Cloud, Künstliche Intelligenz und Security bei der Reise in die neue SAP-Cloud-Welt gemeinsam gedacht und entsprechend umgesetzt werden. Der DSAG-Jahreskongress 2025 bietet den Rahmen für die entsprechenden Überlegungen, um die Kunst der Balance zwischen den drei zentralen Themen angeregt zu diskutieren und Wege in die Cloud aufzuzeigen.

www.dsag.de/jahreskongress

IT-SICHERHEITSMANAGEMENT

DAS UMFASSENDE PRAXIS-HANDBUCH

IT-Sicherheitsmanagement – Das umfassende Praxis-Handbuch; Thomas W. Harich; mitp Verlags GmbH & Co.KG; 10-2025

Daten werden in Public Clouds verlagert und dort verarbeitet, auf Mobiltelefonen gespeichert, über Chat-Apps geteilt oder im Rahmen von Industrie 4.0 in einer Größenordnung erfasst, die bislang kaum denkbar war. IT-Security-Manager müssen die entsprechenden Maßnahmen nicht nur an diese Veränderungen anpassen, sondern auch an die EU-Datenschutz-Grundverordnung, das IT-Sicherheitsgesetz, die Anforderungen von Kunden oder das China Cybersecurity Law.

Dieser Praxisleitfaden wird Ihnen dabei helfen, sich in der riesigen Menge an Einzelthemen und Aufgaben, mit denen sich IT-Security-Manager auseinandersetzen müssen, zurechtzufinden und den richtigen Weg zu wählen, um mit all diesen Anforderungen umzugehen.

Typische Fragestellungen und Antworten für den Berufsalltag

Jedes Kapitel beschreibt ausführlich jeweils einen Bereich der IT-Security. Die notwendigen theoretischen Grundlagen wechseln sich dabei ab mit Tipps aus der Praxis für die Praxis, mit für den Berufsalltag typischen Fragestellungen, vielen konkreten Beispielen und hilfreichen Checklisten. Alle Teilgebiete werden abschließend in einem Kapitel zusammengeführt, das die Einführung und Weiterentwicklung eines IT-Sicherheitsmanagements auf Basis der ISO-27000-Normen-Familie unter Beachtung der datenschutzrechtlichen Bestimmungen der EU-DSGVO behandelt.

Logistics Experts Hours:
SAP EWM
Online-Event
u.a. mit Projekt-Insights von
GROZ-BECKERT®
8. Juli 2025
9:00 - 11:30 Uhr
Zur kostenfreien Anmeldung
CONSILIO
DIE VORAUSDENKER.
DIE PROZESSOPTIMIERER.
DIE LÖSUNGSENTWICKLER.
SAP Gold Partner
Einsteinring 22 | D-85609 Aschheim
T +49 89 9605750 | www.consilio-gmbh.de

Der sichere Weg zum Cloud-ERP-System

KOSTEN UND RISIKEN BEI DER SAP-TRANSITION

Um auf wettbewerbsintensiven und internationalen Märkten zu bestehen, benötigen Unternehmen flexible und durchgängig digitale Geschäftsprozesse. Als Voraussetzung dafür gelten moderne, cloudbasierte ERP-Systeme wie SAP S/4HANA. Allerdings sind insbesondere mittelständische Unternehmen unsicher, wenn sie Kosten und Projektlaufzeiten kalkulieren möchten. Das Komplettpaket GROW with SAP minimiert typische Unsicherheitsfaktoren einer Transition und kann Unternehmen unterstützen.

EIN SOLIDES FUNDAMENT

MHP begleitet seit vielen Jahren erfolgreich SAP-Projekte. Dabei steht besonders im Vordergrund, die Transition zu SAP S/4HANA für Kunden so umfassend und einfach wie möglich zu gestalten. Neben SAP-Transitionen ist ein weiterer Arbeitsschwerpunkt die Erweiterung von GROW um zusätzliche SAP Cloud-Lösungen: So kombinieren bereits heute einige unserer Kunden SAP S/4HANA in der Public Cloud Edition mit SAP Digital Manufacturing (SAP DM) und schaffen damit ein solides Fundament für moderne, datenbasierte Fertigungsprozesse.

GROW with SAP verspricht einen einfachen Einstieg in die SAP-Cloudwelt und besteht im Kern aus drei Bausteinen. Erstens: SAP S/4HANA Public Cloud und SAP Business Technology Platform (SAP BTP). Die SAP S/4HANA Public Cloud Edition ist dabei weitgehend standardisiert, vorkonfiguriert, schnell einsatzbereit und deckt alle zentralen Funktionsbereiche eines Unternehmens ab. Zweitens: Services für eine schnelle ERP-Implementierung. Besonders hervorzuheben ist hier SAP Activate – ein Framework für eine vereinfachte SAP S/4HANA-Implementierung, bei der Anwender ihre neuen Prozesse anhand hinterlegter Best-Practice-Szenarien definieren. Dritter GROW-Baustein: Lernangebote zur Nutzung der SAP-Lösungen. Unternehmen und User können das Wissen der SAP-Community sowie die umfassende Lernplattform SAP Learning verwenden.

Diese Vorteile bietet GROW with SAP

GROW ermöglicht einen schnellen, einfachen und vergleichsweise kostengünstigen Zugang zu einem zukunftsfähigen und einfach zu skalierenden Cloud-ERP-System. Durch die in der Public Cloud Edition hinterlegten Best-Practice-Szenarien profitieren sie von SAPs gebündeltem Prozess- und Branchenwissen. Über die SAP Business Technology Plattform bleiben Unternehmen flexibel für neue Herausforderungen: Die Innovationsplattform stellt zahlreiche Technologien und Services bereit für den Aufbau einer komplexen Systemarchitektur. Dazu gehört beispielsweise ein einfaches API-Management zu Drittsystemen, systemübergreifende Datenspeicher und KI-basierte Analysetools.

Für SAP-Einsteiger kommt der Vorteil hinzu, dass die Implementierungs- und Migrationstools bei GROW vor allem auf den Greenfield-Ansatz ausgelegt sind. Das erleichtert und beschleunigt die Transition und senkt die Einstiegshürden. Dazu passt auch das spezifische Bezahl- und Betreibermodell: Das GROW-Paket führt zu planbaren Kosten, während die von

SAP gewartete Public Cloud hohe Sicherheitsstandards garantiert, für einen unterbrechungsfreien Betrieb sorgt und unternehmensinterne IT-Ressourcen entlastet.

Die Transition beginnt: Sechs Schritte bis zum Go-live

Über das Framework SAP Activate werden die neuen Anwender bereits während des Projekts intensiv eingebunden, können das neue System in Demosystemen kennenlernen und mitgestalten. Auf diese Weise wird der S/4-Nutzen früh erkennbar und die Risiken sinken. Eine Transition verläuft typischerweise in sechs Phasen.

#1 **Discover:** Das Unternehmen sucht nach einer passenden ERP-Lösung und nach einem SAP-Partner, um diese zu implementieren.

#2 **repare:** Der SAP-Partner und der Kunde legen die Verantwortlichkeiten für das Projekt fest und erstellen einen ersten Projektplan, der die wesentlichen Anforderungen berücksichtigt.

#3 **Explore:** Partner und Kunde definieren in „Fit-to-Standard"-Workshops gemeinsam die künftigen Geschäftsprozesse.

#4 **Realize:** Neben der Umsetzung der Explore-Ergebnisse werden die Daten des Altsystems in das neue System migriert.

#5 **Deploy:** Go-live und Cut-over, also Produktivsetzung des neuen Systems und Übergang.

#6 **Run:** Die Transition ist erfolgreich beendet, der SAP-Partner steht weiter für Fragen, Anpassungen und Korrekturen bereit.

Antonio Cavalieri

GROW BIETET EINEN SCHNELLEN, EINFACHEN UND VERGLEICHSWEISE KOSTENGÜNSTIGEN ZUGANG ZU EINEM ZUKUNFTSFÄHIGEN UND EINFACH ZU SKALIERENDEN CLOUD-ERP-SYSTEM.

Antonio Cavalieri,
Associated Partner, MHP Management- und IT-Beratung GmbH,
www.mhp.com

STAMMDATEN-SERVICES

UNTERSTÜTZUNG FÜR DIE S/4HANA-MIGRATION

simus systems hat seine Dienstleistungen im Bereich der Stammdatenaufbereitung für SAP S/4HANA ausgebaut. Das Portfolio umfasst nun neben Materialstammdaten auch die Bereiche SAP Business Partner, Materials, Equipments und Technical Objects. Diese Erweiterung zielt darauf ab, Migrationsprojekte zu vereinfachen.

SAP S/4HANA zeichnet sich durch eine stärkere Integration von Stammdaten in Geschäftsprozesse, Reporting-Funktionen und Benutzeroberflächen aus. Die Plattform basiert auf einem zentralisierten Datenmodell, das Echtzeitverarbeitung, Automatisierung und Datenanalyse ermöglicht. Diese Architektur stellt erhöhte Anforderungen an die Qualität der Stammdaten, insbesondere bei den Kernobjekten wie Geschäftspartnern, Materialien, Equipments und Technical Objects.

Externe Unterstützung essenziell

Mit ausgereiften Methoden, Werkzeugen und Erfahrungen übernimmt der Dienstleister im Vorfeld einer Migration die gesamte Datenaufbereitung für diese Zielstruktur nach den Vorgaben des Kunden. Nach immer feineren Regeln werden die Daten sortiert, angereichert und in einer Ergebnisdatenbank abgelegt. Die Ergebnisse lassen sich filtern und betrachten, um eventuelle Fehler, Dubletten oder Ungenauigkeiten aufzufinden. In Workshops mit den betroffenen Fachabteilungen des Kunden werden die Ergebnisse überprüft und beurteilt. Änderungen werden jedoch nicht über einzelne Datensätze, sondern über das Regelwerk korrigiert. Die freigegebenen Daten können mitsamt neuer Struktur jederzeit mit einer flexiblen Schnittstelle von simus systems in das neue System übertragen werden.

www.simus-systems.com

Process Engine und digitales Logbuch

ALLE PROJEKTINFORMATIONEN ZENTRAL BÜNDELN

Bei der Gestaltung transparenter Unternehmensabläufe ergänzen sich bei dem Kunststoffspezialisten Reinert-Ritz GmbH zwei zentrale Komponenten: Das Anfang 2023 implementierte ERP-System ams.erp sorgt für die durchgängige Datenbasis, während das nahtlos integrierte Collaboration-Tool ams.taskmanager die Prozessbeteiligten über die reinen ERP-Zahlen hinaus mit sämtlichen Zusatz- und Zwischeninformationen versorgt, die für die Abwicklung der Projekte relevant sind. Diese Informationen, die zuvor mündlich, per Mail und in Papiermappen abteilungsweise weitergegeben wurden, stehen nun zentral zur Verfügung. Damit übernimmt die Collaboration-Software die Rolle eines digitalen Logbuchs, das stets den Überblick über den aktuellen Status der Erledigung aller Aufgaben und Vorgänge liefert.

Dem Prozessverantwortlichen bei Reinert-Ritz, Niklas Pietruschka, war klar, dass im Rahmen der Auftrags- oder Projektabwicklung jede Menge Informationen anfallen, die abteilungsübergreifend ausgetauscht werden müssen. Dies können kundenindividuelle Absprachen zu den Produkten sein, es kann die Verpackungs- und Versandkonditionen betreffen oder auch die Abwicklung von Reklamationen. Für die Übermittlung dieser Informationen hält er ERP-Systeme generell nicht für prädestiniert, weil sie notwendigerweise einer vorab definierten Logik folgen, die angrenzende oder sich spontan ergebende Aspekte außer Acht lassen müsse. Am nützlichsten sei diese logische Abfolge in der Fertigung, wo das ERP-System über die Stücklisten und die Arbeitspläne das alleinige Kommando übernehme. An vielen anderen Stellen hingegen sei vielfach ein Eingreifen erforderlich, zumindest aber die Aufnahme weiterführender Auskünfte.

Einbindung sämtlicher Zwischeninformationen

Für die strukturierte Einbindung dieser Zusatz- und Zwischeninformationen in den Gesamtprozess kommt die Collaboration-Software ams.taskmanager zum Einsatz, über die sich unternehmensweite alle typischen Dokumentations- und Freigabeprozesse sowie auch Änderungs- und Service-Anfragen von Kunden digital verwalten lassen. Der Hauptnutzen liegt darin, den Bearbeitungsstatus der jeweiligen Aufgaben und Anfragen vom Eingang bis zu ihrer Erledigung an zentraler Stelle bereitzustellen. Dies sorgt für Nachvollziehbarkeit und digitale Prozesssicherheit, die bei eher formloser Kommunikation per Telefon, Mail oder Arbeitsmappe nicht möglich ist.

An ams.erp ist das frei konfigurierbare Software-Modul über eine Standardschnittstelle angebunden, so dass beide Systeme jederzeit miteinander korrespondieren. Das Zusammenspiel erfolgt über Referenzen: Sobald im ERP eine Angebotsnummer existiert, wird eine Referenz im entsprechenden Task hinterlegt. ams.taskmanager öffnet sich als Website und zeigt die Referenzen ins ERP-System an. Klickt nun eine bearbeitende Person auf eine Referenz, wird sie ins ERP-System weitergeleitet und weiß von vornherein, auf welches Angebot oder welchen Kunden sich der jeweilige Task bezieht.

Der Nutzen der Collaboration-Software liegt vor allem darin, Prozessengpässe aufzudecken, wenn Aufgaben nicht erledigt werden konnten oder Entscheidungen nicht getroffen wurden. Früher wurden solche Problemstellungen im Rahmen von Koordinationsrunden aufzudecken versucht, heute erfolgt die Analyse anhand der in der Task-Software gesammelten Informationen.

Die Notwendigkeit von Transparenz und die Erkenntnis, dass in einem durchgängigen Prozess alle relevanten Informationen zentral verknüpft und jederzeit verfügbar sein müssen, sieht Niklas Pietruschka im deutschen Mittelstand als noch unterrepräsentiert an. Dabei biete die Task-Software sogar die Option für die Umsetzung der von der DIN EN ISO 9001:2015-11 geforderten Prozessorientierung.

Guido Piech | www.ams-erp.com

IT-STRATGIEN IN DEUTSCHEN KMU

ZWISCHEN ANSPRUCH UND OPERATIVER REALITÄT

Auf den ersten Blick weisen kleine und mittlere Unternehmen (KMU) in Deutschland im internationalen Vergleich eine hohe IT-Service-Management (ITSM)-Reife auf. Jedes fünfte KMU hierzulande verfügt laut eigener Aussage über ein voll ausgereiftes, proaktives ITSM-Framework. Weitere 56 Prozent beschreiben ihre Prozesse als gut strukturiert. Zudem sehen 53 Prozent ITSM als strategische Möglichkeit, sowohl Effizienz als auch Geschäftserfolg zu steigern. Das zeigt der neue globale Benchmark-Report „The State of SMB IT for 2026", für den EasyVista und die OTRS AG über 1.000 Führungs- und IT-Fachkräfte in elf Ländern befragt haben.

Doch diese strategische Ambition trifft auf eine operative Realität, die häufig nicht mithalten kann. Derzeit nutzen 43 Prozent einfache Ticketsysteme anstelle integrierter ITSM-Lösungen – deutlich mehr als im globalen Schnitt (28 Prozent). Weitere zehn Prozent verwalten IT-Service-Anfragen vollständig manuell.

Deutsche KMU setzen zu oft auf fragmentierte Systeme

Auch im Hinblick auf das für ein proaktives ITSM wichtige IT Asset Management (ITAM) klafft eine Lücke zwischen Anspruch und Realität. Fast zwei Drittel (63 Prozent) nutzen nur einfache ITAM-Tools oder gar Tabellenblätter, um ihre IT Assets zu verwalten.

Bei der Integration von ITAM, Monitoring und ITSM besteht noch größerer Nachholbedarf. Fast drei Viertel (71 Prozent) arbeiten aktuell mit manuellen Methoden oder Tabellenblättern, um ITSM- und ITAM-Prozesse zu integrieren. Nur vier von zehn geben an, eine vollständige Integration ihrer Monitoring-Tools mit ihrem ITSM- oder Ticketingsystem erreicht zu haben.

https://info.otrs.com

MEHR WERT
The State of SMB IT for 2026

Vorarbeit für intelligente ERP-Prozesse

OHNE SCHIENEN KEIN KI-ZUG

GEFRAGT SIND NEUE, PROZESSORIENTIERTE ANSÄTZE.

Ralf Bachthaler, Mitglied des Vorstands, Asseco Solutions, www.applus-erp.de

Mit GenAI-basierter Agententechnologie geht bald der „ICE" unter den Automatisierungsvehikeln in die Serienreife. Doch so wie ein Hochgeschwindigkeitszug stabile Trassen braucht, benötigt auch KI ein robustes Prozess-Schienennetz.

Damit KI sinnvoll genutzt werden kann, müssen Unternehmen ihre Datenhaltung in Ordnung bringen. Sauber strukturierte Daten spielen eine entscheidende Rolle für den KI-Erfolg. Mindestens ebenso wichtig ist jedoch strukturiertes Wissen um Prozessabläufe. Denn ihr wahres Potenzial entfaltet generative künstliche Intelligenz bei der Bearbeitung von Kernprozessen. Erhält sie jedoch keine Möglichkeiten, die konkreten Einzelschritte zur Bearbeitung einer Aufgabe zu erlernen, können entsprechende Szenarien kaum über den Konzeptstatus hinauskommen.

Gesucht: Die Streckenkarte für Geschäftsprozesse

In der täglichen Praxis sind Prozessabläufe nur selten digital – etwa im ERP-System – hinterlegt. Das echte Prozesswissen? Sitzt meist im Kopf der Anwender. Sie sind es, die sich ihren Weg durch komplexe ERP-Masken bahnen, bei Bedarf ihren Prozess unterbrechen, um auf Rückmeldung von Kollegen zu warten, oder fehlende Informationen von Hand in anderen Systemen recherchieren und nachtragen.

Eine Arbeitsweise, mit der menschliche User in der Regel zurechtkommen. Mit entsprechenden Schulungen und Erfahrung finden sie selbstständig ihren Weg durch die verschiedenen Ansichten und Masken des ERP-Systems. Ein KI-Agent hingegen „tickt" völlig anders. Er benötigt sehr klare Anweisungen, welche Einzelschritte der Reihe nach etwa zur Bearbeitung eines neuen Auftrags vonnöten sind. Ein Prinzip, das sich auch außerhalb der ERP-Welt widerspiegelt: Ein schienengebundenes Fahrzeug zu steuern, ist für eine KI deutlich einfacher als ein Auto. Die Freiheitsgrade im Straßenverkehr machen den Prozess schlicht ungleich komplexer und weniger berechenbar.

Bild: Adobe Stock | Echt&Kreativ

Um sich auf die bevorstehende KI-Zukunft vorzubereiten, gilt für Unternehmen: Bestehende Prozesse analysieren und dokumentieren, um dann auf diese Weise ein stabiles „Schienennetz" ihrer täglichen Abläufe zu erhalten. Die zentralen Kernprozesse darin können im Anschluss zu „Hochgeschwindigkeitstrassen" ausgebaut werden, auf denen hochgradig automatisierte KI-Agenten auf möglichst direktem Weg und ohne unerwartete Hindernisse an ihr Ziel gelangen können.

Neue Wege in der ERP-Welt

Damit Unternehmen ihr Prozessschienennetz digital hinterlegen können, müssen ERP-Lösungen ihre datenzentrierte Ausrichtung überdenken. Gefragt sind neue, prozessorientierte Ansätze. Diese müssen die spezifischen Abläufe eines Unternehmens in einer Sprache abbilden, die KI verstehen kann. Besonders gut geeignet ist hier etwa die Prozesssprache „Business Process Model and Notation" (BPMN).

Eine solche digitale Prozessabbildung lohnt sich auch jenseits ihrer Vorteile für die KI-Nutzung: Durch sie erhalten ERP-Systeme die Möglichkeit, Anwender Schritt für Schritt durch die erforderlichen Abläufe zu führen. Gerade in Zeiten des anhaltenden Fachkräftemangels lässt sich so die Prozessgeschwindigkeit deutlich erhöhen. Mitarbeitende werden entlastet, während die Gesamteffizienz des Unternehmens steigt.

Ralf Bachthaler

DIE KI IM DIENSTE DER IT-SICHERHEIT

VERTRAUEN, SICHERHEIT UND GOVERNANCE

Künstliche Intelligenz ist ein Dauerthema, das kein Unternehmen mehr ignorieren sollte. Egal in welchen Bereich man schaut: Cloud Computing, Datenbanken, Digitale Transformation oder Cybersecurity – die KI ist allgegenwärtig, aber sie steht erst am Anfang.

Ein großer Bereich, in dem KI nicht nur unterstützend sein, sondern auch zum Risiko werden kann, sind die Sicherheitsstrategien der Unternehmen. Sie kann genutzt werden, um den Schutzschild zu stärken, sie wird vermehrt aber auch von Angreifern verwendet.

Unser neues eBook zeigt, wie moderne Unternehmen ihre Abwehrkräfte wirklich stärken.

Entdecken Sie, wie verschiedene Ansätze ineinandergreifen – und warum jetzt der richtige Zeitpunkt ist, Ihre Sicherheitsstrategie neu zu denken!

Aus dem Inhalt:

- KI-gestützte Nutzerprofilierung
- Cyber Security Divide
- Mehrwert mit AI Mesch
- Responsible AI
- Zero Trust
- Sicherheit fürs KI-Zeitalter

eBook Download

Das eBoook umfasst 36 Seiten und steht kostenlos zum Download bereit.
www.it-daily.net/download

THE ART OF BALANCE

ALLES EINE FRAGE
DER BALLONS?

DSAG

DSAG-Jahreskongress 2025

16. - 18. September 2025
Messe Bremen

Der strategische Blindspot beim KI-Einsatz

WARUM UNTERNEHMEN JETZT HANDELN MÜSSEN

WER KI GESTALTEN WILL, BRAUCHT MEHR ALS TECHNOLOGIE. ES BRAUCHT EINE KLARE STRATEGIE, STARKE STRUKTUREN UND DEN MUT ZUR VERÄNDERUNG.

Marco Heid, Principal, Head of Content & Collaboration, Campana & Schott, www.campana-schott.com

Künstliche Intelligenz (KI) verändert die Arbeitswelt rasant. Seit der Veröffentlichung von ChatGPT Ende 2022 hat sich generative KI (GenAI) von einer technischen Neuerung zu einem festen Bestandteil vieler Geschäftsprozesse entwickelt. Unternehmen setzen sie nicht nur zur Effizienzsteigerung, sondern zunehmend auch für datenbasierte Entscheidungen, automatisierte Abläufe und kürzere Innovationszyklen ein. KI mausert sich vom Hype zur Grundlagentechnologie für Organisationen.

Laut aktueller Social Collaboration Studie von der TU Darmstadt und Campana & Schott nutzen knapp 50 Prozent der Unternehmen im DACH-Raum GenAI. Führende Stimmen aus der Wirtschaft nehmen die Zukunft ins Visier. Marc Benioff, CEO von Salesforce, bringt es auf den Punkt: „Wir bewegen uns auf eine Welt zu, in der Menschen und KI-Agenten gemeinsam geführt und gesteuert werden." Unternehmen müssen sich jetzt darauf vorbereiten, dass diese Zusammenarbeit Realität wird. Es ergeben sich fünf Handlungsfelder, die es für Organisationen zu bespielen gilt:

KÜNSTLICHE INTELLIGENZ WIRD ZUM TEIL DER TEAMARBEIT. FÜHRUNG BEDEUTET, MENSCHEN UND KI GEZIELT ZUSAMMENZUBRINGEN.

Sven Hausen, Associate Partner, Transformation of Work, Campana & Schott, www.campana-schott.com

Handlungsfeld #1: Strategie
Erste Anwendungen sind produktiv, das Wissen wächst. Jetzt gilt es, aus Insellösungen tragfähige Strukturen zu entwickeln. Unternehmen müssen GenAI nicht nur technisch beherrschen, sondern strategisch einordnen, organisatorisch absichern und kulturell verankern. Datenschutz, Governance und ethische Fragen sind durch klare Verantwortlichkeiten, technische Leitplanken und etablierte Plattformstandards lösbar.

Gleichzeitig verändert sich die Perspektive. KI wird nicht mehr als Experiment betrachtet, sondern als Mittel, um strategische Unternehmensziele zu erreichen. In erfolgreichen Unternehmen übernehmen Fachbereiche Verantwortung, treiben Führungskräfte die Umsetzung und zeigen viele Mitarbeitende Bereitschaft zur Veränderung. Wer jetzt zögert, verliert nicht nur technologisch den Anschluss, sondern auch kulturell und strukturell.

MEHR WERT
Social Collaboration Studie

Unternehmen, die KI strategisch einsetzen, denken über Einzelanwendungen hinaus und integrieren KI als Transformationswerkzeug.

Handlungsfeld #2: Organisation
Immer mehr Unternehmen etablieren unternehmensweite KI-Programme mit klaren Zielbildern. Governance-Modelle, festgelegte KPIs und ein koordinierter Aufbau helfen, Einzelinitiativen zu bündeln und strategisch weiterzuentwickeln. Zentrale Einheiten wie KI-Teams oder ein Center of Excellence definieren Standards, sammeln Erfahrungen und unterstützen andere Bereiche bei der Umsetzung.

Parallel entstehen in den Fachbereichen dezentrale Verantwortlichkeiten, um Anwendungsfälle schnell zu identifizieren und umzusetzen. Damit KI im Arbeitsalltag wirksam wird, braucht es das Zusammenspiel aus zentralen Leitlinien, technischer Absicherung und Freiraum für unternehmerisches Handeln.

Handlungsfeld #3: Technologie
Parallel zur organisatorischen Verankerung schreitet auch die technologische Entwicklung voran. Eine der dynamischs-

ten Entwicklungen im Umfeld generativer KI ist Agentic AI. Anders als bisherige GenAI-Anwendungen, die auf direkte Nutzereingaben reagieren, agieren KI-Agenten zunehmend eigenständig. Sie kombinieren Daten aus verschiedenen Quellen, treffen vorbereitende Entscheidungen, koordinieren Prozesse und interagieren mit anderen Systemen. Dadurch eröffnen sich Potenziale für intelligente, automatisierte Abläufe über Abteilungsgrenzen hinweg.

Vernetzte Agenten gehen einen Schritt weiter. Sie sind in bestehende Systemlandschaften integriert, kommunizieren untereinander und reagieren flexibel auf Veränderungen. Starre Schnittstellen werden überflüssig. Stattdessen entstehen dynamische Abläufe, die sich kontextbezogen anpassen und kontinuierlich optimieren lassen. Das macht die Systemintegration schneller, flexibler und wirtschaftlicher.

Agentic AI steht für eine neue Stufe der Automatisierung. Unternehmen können auf bestehenden Plattformen aufbauen, erste Projekte realisieren und die Basis für eine skalierbare, vernetzte Prozesslandschaft schaffen.

Handlungsfeld #4: Kompetenz

Trotz wachsender technischer Autonomie bleiben die Menschen im Zentrum. Sie entscheiden, wie und wofür KI eingesetzt wird und müssen entsprechend befähigt werden. Sie steuern Prozesse, interpretieren Ergebnisse und treffen Entscheidungen. Damit verändern sich die Anforderungen an Kompetenzen und Rollen.

Im Vordergrund steht nicht technisches Spezialwissen, sondern die Fähigkeit, KI sicher in den Arbeitsalltag zu integrieren, Ergebnisse einzuordnen und souverän damit umzugehen. Neue Rollen entstehen dort, wo Unternehmen den KI-Einsatz aktiv gestalten – etwa als Prompt Engineer, Agent Designer oder KI-Trainer. Gleichzeitig werden übergreifende Fähigkeiten wichtiger, etwa digitale Urteilskraft, systemisches Denken und die Bereitschaft, Verantwortung im Zusammenspiel mit automatisierten Systemen zu übernehmen.

Viele Organisationen investieren daher in Programme, die an den konkreten Aufgaben der Mitarbeitenden anknüpfen. Sie vermitteln technisches Grundlagenwissen, fördern prozessbezogenes Denken und stärken eine Lernkultur, in der der bewusste Umgang mit KI als Schlüsselkompetenz verstanden wird.

Handlungsfeld #5: Kultur

Der zunehmende Einsatz von GenAI und Agentic AI verändert Prozesse, aber auch die Struktur von Organisationen. Arbeitsweisen werden agiler, Entscheidungen basieren stärker auf Daten, und klassische Hierarchien verlieren an Bedeutung. An ihre Stelle treten flexiblere Netzwerke, in denen Menschen und KI-Agenten gemeinsam agieren. Fachbereiche, Rollen und Technologien rücken enger zusammen.

Führung bedeutet in diesem Umfeld mehr als Koordination. Sie schafft Orientierung, fördert Vertrauen und ermöglicht Veränderung. Wer diesen Wandel aktiv gestaltet, entwickelt eine Organisation, die anpassungsfähig bleibt und Innovation aus sich heraus ermöglicht.

Fazit: Gestaltungskompetenz entscheidet

Die Voraussetzungen für den produktiven Einsatz von KI waren nie besser. Technologien sind verfügbar, Plattformen etabliert, erste Erfahrungen vorhanden. Jetzt kommt es darauf an, KI gezielt in die Organisation zu integrieren – technisch, strukturell und kulturell.

Dafür braucht es entschlossenes Handeln auf fünf Ebenen:

#1 Strategie:
KI-Initiativen müssen ein klares Ziel verfolgen und in die Gesamtstrategie eingebettet sein.

#2 Organisation:
Rollen, Prozesse und Governance-Strukturen sollten abgestimmt und zukunftsfähig aufgesetzt werden.

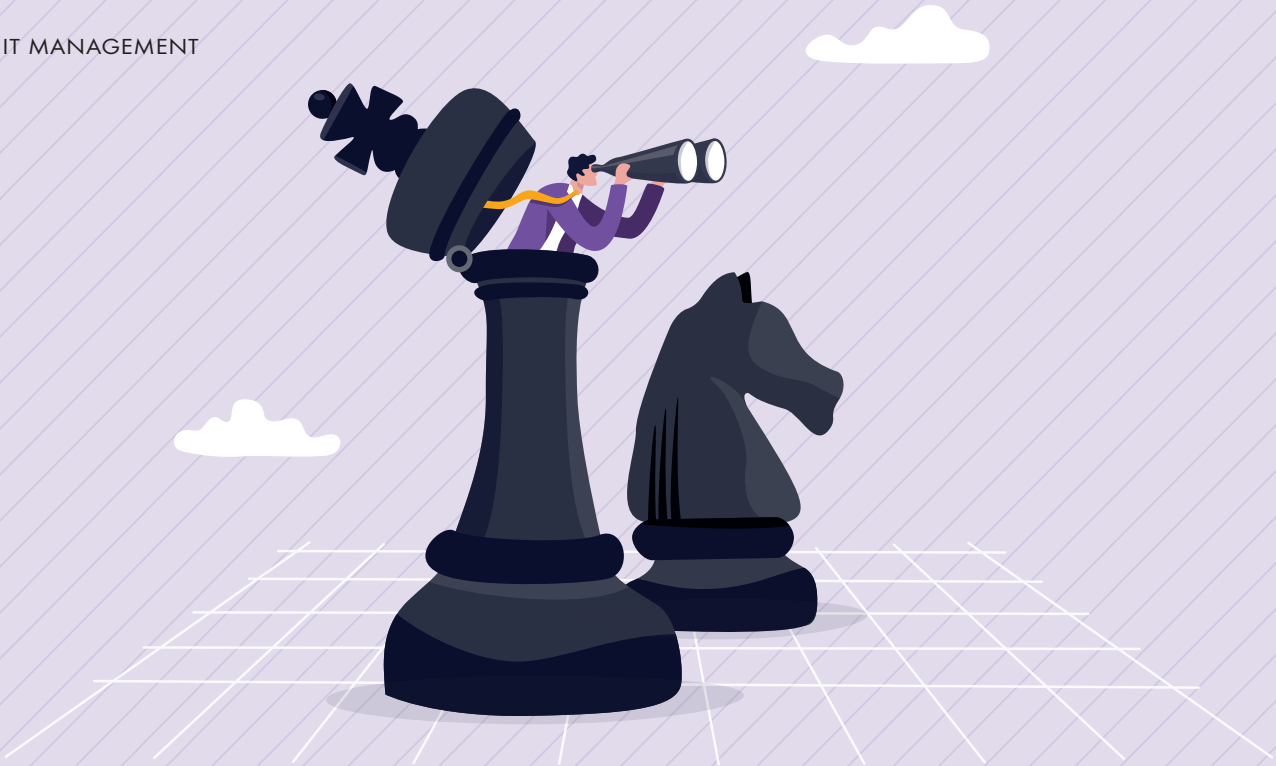
#3 Technologie:
Die schnellen technologischen Weiterentwicklungen von GenAI sollten als Chance verstanden und genutzt werden.

#4 Kompetenzen:
Mitarbeitende benötigen neue Fähigkeiten im Umgang mit KI im Alltag und in der Gestaltung von Lösungen.

#5 Kultur:
Der offene und verantwortungsvolle Umgang mit KI muss Teil der Zusammenarbeit werden.

Wer den Wandel nicht nur beobachtet, sondern aktiv gestaltet, schafft technologische Fortschritte und entwickelt eine Organisation, die kontinuierlich dazulernt, Wandel aktiv formt und wettbewerbsfähig bleibt.

Sven Hausen, Marco Heid



KI als Gamechanger im Finanzbereich

WAS IT-MANAGER WISSEN SOLLTEN

Die rasanten Fortschritte im Bereich der Künstlichen Intelligenz (KI) verändern nahezu alle Unternehmensbereiche – besonders aber das Finanzwesen. Innovative IT-Manager sollten dieses Momentum nutzen und die technologische Basis für eine erfolgreiche Transformation der Finance & Accounting-Abteilung legen und sich damit als strategischer, impulsgebender Partner der Geschäftsführung positionieren. Laut einer internationalen Umfrage, die Censuswide im Auftrag von BlackLine unter Führungskräften und Finanzexperten durchgeführt hat, versprechen sich 35 Prozent der Führungskräfte erhebliche Produktivitätsgewinne durch den Einsatz von KI im Finanzbereich. Weitere 31 Prozent erwarten verlässlichere und konsistentere Finanzdaten. Das darf als klarer Hinweis darauf gesehen werden, dass KI weit mehr ist als nur Automatisierung: KI schafft die Grundlage für bessere Analysen, präzisere Prognosen und fundiertere Entscheidungen.

Insbesondere die CFOs scheinen besonders optimistisch zu sein: 40 Prozent sehen in KI eine Unterstützung bei der strategischen Entscheidungsfindung, was zugleich die wachsende Erwartungshaltung gegenüber den IT-Abteilungen verdeutlicht; sie soll die entsprechenden Lösungen bereitstellen, damit der Finanzbereich bestmöglich performen kann.

Herausforderungen: Implementierung und Know-how

Trotz der positiven Erwartungen bestehen nach wie vor erhebliche Hürden bei der Umsetzung. Rund ein Viertel der Befragten äußert Bedenken hinsichtlich der effektiven Implementierung von KI. Fehlendes internes Know-how (24 %) sowie Unsicherheiten über die künftige Entwick-

ÜBER DIE UMFRAGE

Im Rahmen der Umfrage wurden von Censuswide in sieben Märkten (USA, Kanada, Großbritannien, Frankreich, Deutschland, Australien und Singapur) 653 Vorstände und Geschäftsführer sowie 684 F&A-Fachleute aus Unternehmen mit den folgenden Mindestjahresumsätzen befragt: USA: 150 Mio. USD; Kanada: 50 Mio. CAD; UK: 50 Mio. GBP; Frankreich: 50 Mio. EURO; Deutschland: 50 Mio. EURO; Australien: 20 Mio. AUD; Singapur: 20 Mio. SGD. Die Umfrage wurde im Oktober 2024 durchgeführt.

MEHR WERT
Future CFO

lung der Finanzfunktion (25 %) erschweren die praktische Umsetzung. Für IT-Manager bedeutet das: Sie müssen nicht nur Systeme bereitstellen, sondern auch dafür sorgen, dass KI verantwortungsvoll, sicher und unternehmensspezifisch implementiert wird.

Verhaltener Optimismus in Deutschland

In Deutschland zeigt sich ein differenziertes Bild. 40 Prozent der deutschen CFOs sind optimistisch, was die zukünftige Rolle von KI im Finanzbereich angeht. Allerdings sehen nur 20 Prozent konkrete Produktivitätsgewinne, und ebenso viele geben an, die Auswirkungen von KI noch nicht einschätzen zu können. Diese Zurückhaltung eröffnet IT-Verantwortlichen die Chance, durch transparente Pilotprojekte, gezielte Schulungen und eine engere Zusammenarbeit mit der Finanzabteilung Vertrauen in neue Technologien aufzubauen.

IT-Manager stehen heute nicht mehr nur für Stabilität und Sicherheit der Systeme. Sie sind Enabler für Innovation – insbesondere, wenn es um den Einsatz von KI im Finanzbereich geht. Das bedeutet: Sie sollten frühzeitig in KI-Initiativen eingebunden sein, die strategische Ausrichtung mitgestalten und die Integration neuer Technologien so gestalten, dass sie den fachlichen Anforderungen gerecht werden.

Fazit

KI ist mehr als ein Trend – sie ist der nächste Evolutionsschritt in der Finanztransformation. Für IT-Manager ergibt sich daraus die Chance, eine zentrale Rolle im Unternehmen einzunehmen: als Vermittler zwischen Technologie und Business, als Partner des CFO und als Treiber einer resilienten, datengestützten Finanzorganisation.

Ralph Weiss

KI IST MEHR ALS EIN TREND – SIE IST DER NÄCHSTE EVOLUTIONSSCHRITT IN DER FINANZTRANSFORMATION.

Ralph Weiss, Geo VP Central Europe, BlackLine, www.blackline.com

ZEIT IST GELD, ICH SPAR MIR BEIDES.

Die Business Platinum Card mit GetMyInvoices automatisiert die Belegsuche und spart Zeit – für mehr Fokus im Business.

Jetzt Angebot sichern.

amex.de/gmi

Es gelten Bedingungen.

Drei Stufen zum KI-Erfolg

KI-PROJEKTE STRATEGISCH ANGEHEN

Künstliche Intelligenz unkoordiniert und unkontrolliert einzusetzen, kann Risiken mit sich bringen – übermäßige Vorsicht hingegen ihren Nutzen deutlich schmälern. Einen sinnvollen Mittelweg zu finden, stellt aktuell eine zentrale Herausforderung für Unternehmen und ihren KI-Erfolg dar. Der Schlüssel dazu liegt in einer strukturierten und durchdachten Planung. Drei zentrale Schritte haben sich dazu in der Praxis bewährt.

In der medialen Berichterstattung ist KI weiterhin das Top-Thema, Mitbewerber berichten von beeindruckenden Szenarien, Experten warnen davor, abgehängt zu werden. Unternehmen sehen sich einem steigenden Druck gegenüber, der sie mitunter überhastet in die KI-Welt starten lässt – ohne die Technologie selbst, ihre Grenzen und Risiken wirklich zu verstehen. Die Folge: Viele KI-Projekte kommen nicht über den Konzeptstatus hinaus.

Wichtiger als eine schnelle KI-Einführung ist eine durchdachte KI-Einführung, um tatsächlich und langfristig von den Vorteilen der intelligenten Technologie zu profitieren. In der Praxis hat sich hierfür ein Ansatz aus drei Phasen bewährt: Grundlegender Wissenserwerb, Aktivierung von Potenzialen sowie nachhaltige Umsetzung.

#1 Kenne die Technologie – und kenne dich selbst

Zu Beginn einer jeden KI-Implementierung sollten sich Verantwortliche unbe-

Quelle: „Adobe Stock – Echt&Kreativ – #1354032239"

dingt ein generelles Verständnis davon aneignen, wie KI aus technischer Sicht funktioniert. Generative KI etwa erstellt ihre Antworten, indem sie – basierend auf der Frage – immer wieder das am wahrscheinlichsten folgende Wort an die bereits erstellte Textpassage anreiht. Ein echtes Verständnis des Inhalts ist damit nicht verbunden. Wer den Blick hinter die Kulissen wirft, kann Chancen und Grenzen besser einschätzen.

Neben der Technologie selbst ist auch der Status quo im eigenen Unternehmen für den KI-Erfolg entscheidend. Welche Kompetenzen sind intern vorhanden? Wie gut eignet sich der Datenfundus für eine KI-Nutzung? Wie positiv oder negativ sind die Mitarbeitenden generell gegenüber KI eingestellt? Durch eine Analyse der „KI-Readiness" lassen sich insbesondere potenzielle Hürden frühzeitig erkennen.

#2 Der Nutzen steht im Zentrum

In einer darauffolgenden Experimentierphase werden konkrete, für das Unternehmen sinnvolle KI-Szenarien identifiziert und evaluiert. Durch die Entwicklung von Prototypen wird das Nutzenpotenzial erlebbar. Gleichzeitig können Unternehmen damit eine realistische Erwartungshaltung setzen. Entscheidend ist, dass hinter jedem Use Case ein klar umrissenes, messbares Ziel steht.

Bei der Identifizierung von Einstiegsszenarien kann die Frage helfen: „In welchen Bereichen sind wir mit spezifischen Herausforderungen konfrontiert, für die KI bereits heute Lösungen bietet?" Der Hauptfokus sollte zunächst auf Bereichen liegen, in denen Mitarbeitende durch immer wiederkehrende Aufgaben Zeit verlieren, und die gleichzeitig klar umrissene, idealerweise gut strukturierte Datenquellen nutzen.

WICHTIGER ALS EINE SCHNELLE KI-EINFÜHRUNG IST EINE DURCHDACHTE KI-EINFÜHRUNG, UM TATSÄCHLICH UND LANGFRISTIG VON DEN VORTEILEN DER INTELLIGENTEN TECHNOLOGIE ZU PROFITIEREN.

Anže Mis,
Data Analytics & AI Director,
BE-terna Group,
www.be-terna.com/de

#3 Nachhaltig implementieren

Erst im letzten Schritt erfolgt auf Basis der gewonnenen Erkenntnisse die Implementierung der KI-Technologie. Damit verbunden ist auch die Definition interner Richtlinien für den Gebrauch, die geltende rechtliche Vorgaben miteinbeziehen. Insbesondere hierzu empfiehlt es sich, einen externen Spezialisten hinzuzuziehen, der die aktuellen Vorgaben kennt und fundiert beraten kann.

Generell sollten Unternehmen immer dafür sorgen, interne Kapazitäten für die Betreuung und Weiterentwicklung der KI-Projekte aufzubauen. Eine entsprechende Inhouse-Kompetenz, die bei Fragen unterstützt und künftige Entwicklungen im Blick behält, ist einer der zentralen Schlüssel für einen nachhaltigen und kontrollierten KI-Einsatz.

Anže Mis

HOCHSCHULE SCHMALKALDEN
UNIVERSITY OF APPLIED SCIENCES
FERNSTUDIUM

"Weil PERSÖNLICHE BETREUUNG hier großgeschrieben wird."

BACHELOR
WIRTSCHAFTSINFORMATIK UND DIGITALE TRANSFORMATION
BERUFSBEGLEITEND
INFORMATIK UND IT-MANAGEMENT
MASTER

- Persönliche Betreuung, KEINE anonyme Hochschule
- Exklusive Präsenzphasen, KEINE aufgezeichneten Vorlesungen
- Modulweise Prüfungen, KEINE Prüfungswochen am Semesterende
- Erfolgreicher Studienabschluss, KEINE hohe Abbruchquote

Jetzt Kontakt aufnehmen!
0 36 83 / 6 88 - 17 40 oder - 17 46
info@hsm-fernstudium.de
www.hsm-fernstudium.de
HSM Fernstudium

Die Zukunft der Geschäftsentscheidungen

WARUM KI-AGENTEN MEHR KÖNNEN ALS KLASSISCHE RPA

Laut Gartner wird 2028 jede dritte Geschäftsentscheidung halbautonom oder autonom mit Unterstützung von KI-Agenten getroffen.

Eine oft gestellt Frage in diesem Zusammenhang ist die wie sich KI-Agenten von RPA unterscheiden? Nun, KI-Agenten (Künstliche Intelligenz) und RPA (Robotic Process Automation) sind beides Technologien, die Aufgaben automatisieren, aber sie unterscheiden sich in ihrer Funktionsweise und den Arten von Prozessen, die sie abdecken können.

Funktionsweise

Die Unterschiede erläutert Ulrich Parthier im Folgenden: RPA automatisiert standardisierte, regelbasierte Prozesse, die wiederholbar sind. RPA-Roboter führen genau definierte Aufgaben aus, wie das Ausfüllen von Formularen, das Kopieren von Daten zwischen Systemen oder das Senden von E-Mails. Diese Roboter folgen strengen Regeln und müssen weder „Verständnis" noch „Intelligenz" haben, um ihre Arbeit zu tun.

FLEXIBEL & ANPASSUNGSFÄHIG

KI-Agenten hingegen nutzen fortgeschrittene Techniken wie maschinelles Lernen, natürliche Sprachverarbeitung und kognitive Fähigkeiten, um zu lernen, zu interpretieren und Entscheidungen zu treffen. Sie können unstrukturierte Daten verarbeiten, aus Erfahrung lernen und sich an neue Situationen anpassen. Ein KI-Agent könnte beispielsweise in der Lage sein, eine E-Mail zu verstehen und basierend auf dem Kontext eine Antwort zu generieren oder ein komplexes Problem zu lösen.

Komplexität

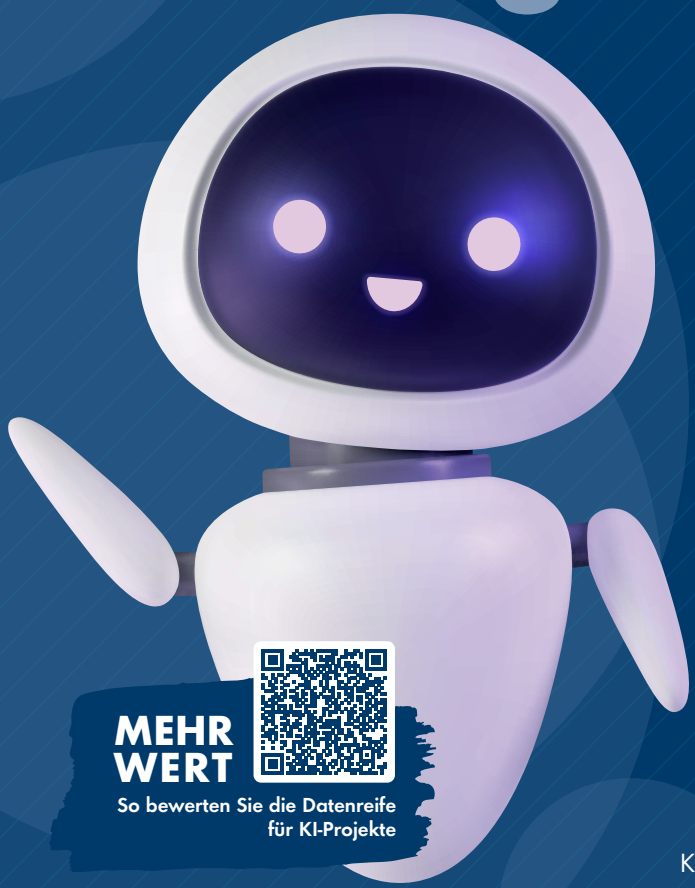
Das zweite Unterscheidungsmerkmal ist das der Komplexität. RPA ist ideal für einfache, repetitive Aufgaben, die keine Entscheidungsfindung oder komplexes Problemlösen erfordern. Es wird oft für Prozesse verwendet, die auf festen Regeln basieren, wie etwa das Übertragen von Daten zwischen Anwendungen oder das Ausführen von Transaktionen in Software.

Das Einsatzgebiet für KI-Agenten ist für komplexere Aufgaben gedacht, die mehr Intelligenz und Anpassungsfähigkeit erfordern. Sie sind in der Lage, aus Daten zu lernen, Muster zu erkennen und auch mit unstrukturierten Daten wie Text oder Sprache zu arbeiten.

Anwendungsfälle

Bei RPA sind Datenextraktion und -eingabe, die Automatisierung von Rechnungs- und Bestellprozessen, die Berichtserstellung und Datenabgleich sowie IT-Support-Aufgaben primäre Aufgaben.

KI-Agenten eignen sich hervorragend für Chatbots und virtuelle Assistenten, die in natürlicher Sprache kommunizieren, Empfehlungssysteme (wie bei Netflix oder Amazon), die Diagnose von



MEHR WERT
So bewerten Sie die Datenreife für KI-Projekte

Problemen oder Fehlern in komplexen Systemen oder die Analyse von großen Datenmengen und Vorhersage von Trends.

Flexibilität und Anpassungsfähigkeit
Das ist das letzte größere Unterscheidungsmerkmal. RPA funktioniert nur dann effektiv, wenn der Prozess klar und unverändert ist. Wenn sich der Prozess ändert, muss der RPA-Roboter entsprechend angepasst werden.

Die KI-Agenten sind wesentlich flexibler und können sich an neue und unbekannte Situationen anpassen, da sie aus Erfahrungen und Daten lernen.

Ergebnis
RPA eignet sich damit eher für die Automatisierung von Routineaufgaben mit klaren Regeln und wiederholbaren Abläufen, während KI-Agenten komplexe, datenintensive und anpassungsfähige Aufgaben übernehmen können, die ein gewisses Maß an „Verstehen" und „Lernen" erfordern. In vielen modernen Automatisierungsprojekten werden beide Technologien oft kombiniert, um die Stärken beider auszunutzen, fasst it management-Herausgeber Ulrich Parthier den ersten Teil „Wie sich KI-Agenten von RPA unterscheiden" zusammen.

Fehlertoleranzen
Desweiteren hat sich Gartner mit den Fragen „Wie werden Fehlertoleranzen programmatisch genutzt?" und „Welche Herausforderungen und Risiken bringen KI-Agenten mit sich?", beschäftigt.

In der Praxis wird davon ausgegangen, dass Fehler dynamisch korrigiert werden können, indem adaptive Workflows verwendet werden, die Fehler automatisch erkennen und korrigieren.

Herausforderungen und Risiken
Neben den Chancen bringen KI-Agenten auch eine Reihe von Herausforderungen mit sich. Agentische KI wird fortschrittliche Cyberangriffe fördern, die zu „intelligenter Malware" führen.

Das kontinuierliche Wachstum der agentenbasierten KI wird auch ernsthafte Bedenken hinsichtlich der Governance für Unternehmen aufwerfen, da Sie versuchen, eine Technologie zu kontrollieren, die autonom arbeitet. Orchestrierung und Governance erfordern fortschrittliche Tools und strenge Leitplanken.

Agentische KI trifft Entscheidungen auf der Grundlage ihrer Analyse der Daten des jeweiligen Unternehmens und erstellt auf dieser Basis Pläne. Von dort aus wird sie nach diesen Plänen handeln.

Dies kann gefährlich werden, es sei denn, Unternehmen investieren in die Fähigkeiten, Praktiken und Technologien, um vertrauenswürdige KI-Agenten bereitzustellen. Ein weiteres Problem entsteht dadurch, dass die Daten des Unternehmens von schlechter Qualität sein können. Eine schlechte Datenqualität und -architektur hemmt die Entwicklung von KI-Agenten.

Anushree Verma, Ulrich Parthier

WO CHANCEN SIND, FINDEN SICH AUCH RISIKEN. NEBEN DEN CHANCEN BRINGEN KI-AGENTEN NATÜRLICH AUCH EINE REIHE VON HERAUSFORDERUNGEN MIT SICH.

Anushree Verma,
Sr Director Analyst, Gartner Inc.,
www.gartner.de

Aus dem Alltag einer IT-Abteilung

OPERATIV AM ANSCHLAG, STRATEGISCH BLOCKIERT

Wer für die IT eines Unternehmens verantwortlich ist, den quälen die Lizenzbestimmungen von Microsoft. Sie werfen Fragen auf, die inhouse kaum jemand verlässlich beantworten kann. Doch: Microsoft-Lizenz-Wissen aufzubauen – und zu halten – kostet Zeit und personelle Ressourcen. Und so kämpfen viele Abteilungen mit undurchsichtigen Lizenzmodellen, wechselnden Bestimmungen, dem Versuch, ihre Software irgendwie zu managen – und der diffusen Sorge vor dem Audit.

Operativ am Anschlag, strategisch blockiert

Ähnlich sah es auch im Alltag von Helmut Fetsch aus, IT-Leiter einer Großen Kreisstadt in Bayern. „Wie viele Office-Lizenzen haben wir eigentlich? Reichen die? Was ist wem zugeordnet?", waren wiederkehrende Fragen. Um auf Nummer sicher zu gehen, wurden immer ein paar mehr angeschafft als es User gab. Administrativ an sich gut organisiert, aber gefangen in einem Lizenzsystem ohne System, hangelte man sich von Jahr zu Jahr. Für mehr blieb einfach keine Zeit.

Doch der Druck steigt und wer Ordnung, Klarheit, eine Strategie will, kann sich nicht ewig auf Excel-Listen stützen und vor bösen Überraschungen fürchten.

Eine bayerische Gemeinde wird zur Blaupause

Deshalb beschloss die Kreisstadt vor zwei Jahren, ihre 250 PCs rechtskonform und wirtschaftlich neu aufzusetzen. Man schrieb gebrauchte Software aus und der Microsoft Solutions Partner VENDOSOFT erhielt den Zuschlag. Helmut Fetsch und sein Team bekamen Joyce Studier zur Seite gestellt. Und statt einfach nur zu liefern, stellte sie die richtigen Fragen: Wie arbeiten Sie? Was braucht die Stadt wirklich? Welche Altverträge existieren? Wo sind die Lizenznachweise? Was ist in Zukunft geplant? Joyce Studier analysierte, sortierte, strukturierte. Das Ergebnis war ein strategischer Lizenzplan, revisionssi-

KLARHEIT STATT LIZENZCHAOS – UND DABEI NOCH GESPART

DAS ZIEL:

- 250 PC-Arbeitsplätze rechtssicher und wirtschaftlich lizenzieren
- optimale Hybridstruktur aus Microsoft Cloud und on-prem
- Lizenzmanagement modernisieren, Unterlizenzierung vermeiden
- Adobe & Microsoft-Lösungen ohne Mietmodell

DIE LÖSUNG:

- Office 2021, Windows Server 2022 / 2025 + Remote Desktop + CALs + Adobe: lokal, datenschutzkonform, langlebig, auditsicher
- M365 für Schulen und externe Partner
- Elektronisches Lizenzarchiv statt Inventarlisten
- Rückverkauf alter Lizenzen – automatisch verrechnet
- 52.000 Euro Einsparung durch gebrauchte Software

MEHR WERT
Casestudy

WER LOKALE INSTALLATIONEN UND CLOUD KLUG KOMBINIERT, SPART GELD, BEHÄLT DIE KONTROLLE – UND SCHAFFT EINE IT, DIE OPERATIV UND STRATEGISCH LANGFRISTIG TRÄGT.

Joyce Studier, Microsoft-Beraterin, VENDOSOFT GmbH, www.vendosoft.de

cher dokumentiert in einem elektronischen Archiv. Seitdem ist Microsoft hier keine Baustelle mehr – sondern Best Practice.

Frei machen vom Cloud-Zwang

Anfang dieses Jahres wagte die Kreisstadt dann den Schritt in die Cloud. Der führte dank Joyce Studier nicht blindlinks zu Cloud-only. Um ständig steigende Abo-Kosten und den Verlust der Datenhoheit zu vermeiden, schlug sie eine hybride Lösung vor, die so auch für Unternehmen funktioniert: Office 2021 (gebraucht) als lokal installierte Version. Weil man damit unabhängig bleibt, stabile Systeme gewährleistet – und aktuell besonders viel Geld spart. Windows Server 2022 und 2025 ersetzten ältere Installationen. Damit alles medienbruchfrei funktioniert, kommt Microsoft 365 punktuell zum Einsatz.

Klarheit statt Lizenzchaos

Und das rechnet sich: Über 52.000 Euro Einsparung brachte VENDOSOFT der Gemeinde – durch den intelligenten Einsatz gebrauchter Software. Die hybride Strategie zeigt, dass Digitalisierung nicht in Abhängigkeit führen muss. Wer lokale Installationen und Cloud klug kombiniert, spart Geld, behält die Kontrolle – und schafft eine IT, die operativ und strategisch langfristig trägt.

www.vendosoft.de

CONSILIO

DIE VORAUSDENKER.
DIE PROZESSOPTIMIERER.
DIE LÖSUNGSENTWICKLER.

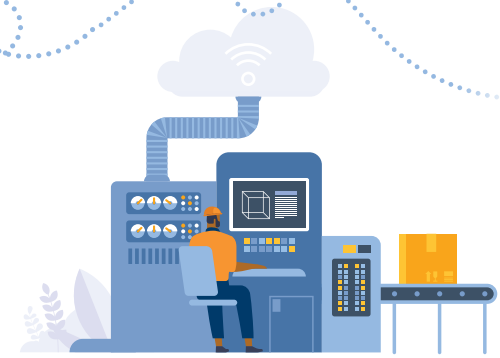
SAP Gold Partner

Erfahren Sie mehr zu unserem Webinarangebot

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

Smart Factory

FÜNF SCHLÜSSELTECHNOLOGIEN FÜR MAXIMALE EFFIZIENZ



Das Konzept der vernetzten, autonomen und flexiblen Smart Factory steht schon seit Jahren im Mittelpunkt der industriellen Transformation. Dabei treiben immer neue Entwicklungen die Umsetzung dieses Konzepts weiter voran. Dell Technologies erläutert fünf aktuelle Trends, die die Industriebranche in der nächsten Zeit prägen werden:

#1 Ultrahochauflösende Kameras

Maschinen werden mit immer mehr Sensorik zur Datenerfassung ausgestattet. Dazu zählen insbesondere Kameras mit Auflösungen von bis zu 8K, die die notwendige Bildqualität für Analysen mit Machine-Learning- und Deep-Learning-Modellen liefern können. Diese Analysen wiederum ermöglichen Anwendungen wie die Qualitätskontrolle direkt in der laufenden Produktion oder die intelligente Echtzeit-Steuerung von Roboterarmen.

#2 KI-Copiloten

Zur Ausstattung von Maschinen zählen auch immer häufiger KI-Copiloten. Sie basieren auf generativer KI und ermöglichen es, Maschinen per natürlicher Sprache zu steuern, oft sogar direkt per Stimme und ohne Texteingaben. Mit diesen Copiloten kann das Personal die immer komplexeren Maschinen besser beherrschen und effizienter bedienen und hat zudem die Hände frei für andere Aufgaben.

#3 Adaptive Maschinen

Mit Hilfe von Künstlicher Intelligenz lernen Maschinen, ihre Leistung zu verbessern und sich an Veränderungen ihrer Umgebung oder ihrer Aufgaben anzupassen. Das Lernen erfolgt dabei entweder durch menschliches Feedback während der laufenden Produktionsprozesse, komplett autonom durch die Analyse von Daten oder durch eine Kombination aus beidem.

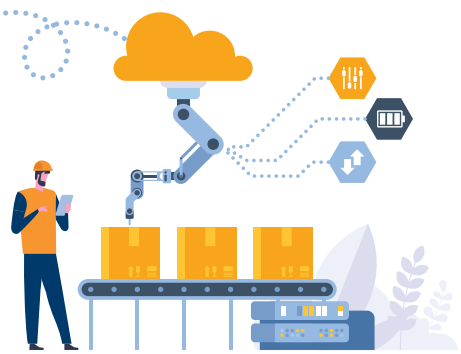
#4 Absicherung der OT

Die Daten, die Unternehmen bei der Produktion mit ihren Maschinen erzeugen, enthalten meist den Schlüssel für ihre Differenzierung vom Wettbewerb. Das erfordert eine umfassende Absicherung der Operational Technology (OT). Dabei benötigt die Branche auch Wege zum sicheren Datenaustausch. Die Produktionsdaten ihrer Kunden können es den Maschinenherstellern beispielsweise ermöglichen, ihre Anlagen kontinuierlich zu verbessern.

#5 Virtualisierung von PLCs

Hersteller virtualisieren zunehmend die speicherprogrammierbaren Steuerungen (Programmable Logic Controllers, PLCs) ihrer Maschinen. Sie bilden die Funktionen der Steuerungen in Software ab, die auf Standard-Servern ausgeführt werden kann. Das ermöglicht es ihnen, Hardware-Ressourcen besser auszunutzen und Sicherheits- sowie funktionelle Updates schneller auszurollen und damit agiler auf neue Anforderungen zu reagieren.

www.delltechnologies.com



WORM-Technologie

DAUERBRENNER FÜR DATENSICHERHEIT UND COMPLIANCE

EIN VORTEIL MODERNER SOFTWARE-WORM-SYSTEME LIEGT IN IHRER UNABHÄNGIGKEIT VON HARDWARE-HERSTELLERN UND DER EXISTIERENDEN SPEICHER-INFRASTRUKTUR.

Kai Hambrecht, Leiter Service & Support, Grau Data GmbH, www.graudata.com

Die WORM-Technologie („Write Once Read Many") ist ein Dauerbrenner in der IT-Welt. Seit den 1980er-Jahren schützt sie Daten vor Veränderungen – ein Prinzip, das im Zeitalter wachsender gesetzlicher Anforderungen an Datensicherheit aktueller ist denn je.

Unveränderbare Speicherung

WORM bezeichnet ein Speicherkonzept, bei dem Daten nach dem Schreiben nur noch lesbar sind, aber nicht mehr verändert oder gelöscht werden können. Früher geschah das physikalisch – etwa auf CDs, DVDs oder speziellen Magnetbändern. Heute wird diese Schutzfunktion meist softwarebasiert realisiert: In einer dedizierten Softwareschicht, in die nicht eingegriffen werden kann, wird das Schreiben und Lesen von Daten auf der Festplatte oder im Speichernetzwerk organisiert und überwacht. Zugelassen sind lediglich Schreibvorgänge für neue Dateien und das Lesen existierender Daten. Alle anderen Operationen, wie ein Verändern oder erneutes Schreiben in existierende Dateien, werden unterbunden.

Beispielhaft dafür ist die Lösung FileLock von GRAU DATA: Sie nutzt eine besonders geschützte Partition auf der Festplatte. Auch wenn ein Nutzer über externe Tools Zugriff zu erlangen versucht – die Schutzfunktion bleibt aktiv. Eine zusätzlich transparente Verschlüsselung der Daten bietet eine erweiterte Sicherheit. Damit sind die Daten nicht nur gegen Veränderung oder das Überschreiben geschützt, sondern auch gegen den unbemerkte Manipulationen. Denn nur ein System, auf dem das Software-WORM installiert und der Verschlüsselungs-Code aktiviert ist, kann die Daten lesen.

Mehr Revisionssicherheit

Die Pflicht zur Datensicherheit betrifft sehr viele Unternehmen und es geht darum, einer Überprüfung standzuhalten. Richtlinien wie etwa nach GoBD, SEC, BAO, GeBÜV der FDA sowie Teile der DSGVO beschreiben genau, welche Daten schützenswert sind und auch wie lange diese aufbewahrt werden müssen – eine technische Anleitung geben diese Vorgaben allerdings nicht, das bleibt jedem einzelnen Unternehmen überlassen. Um die Revisionssicherheit zu erreichen profitieren Unternehmen jeder Größe von einer WORM-Archivierung: Ob große Konzerne oder kleine Betriebe – ein Software-WORM sorgt für einfache Revisionssicherheit. Mit der WORM-Archivierung können Unternehmen ihre Compliance und die gesetzlichen Vorgaben sicherstellen und Richtlinien wie GoBD, DSGVO, SEC oder GeBÜV mit einer nachweisbaren, unveränderbaren Datenaufbewahrung erfüllen.

Zukunftssicher trotz technologischem Wandel

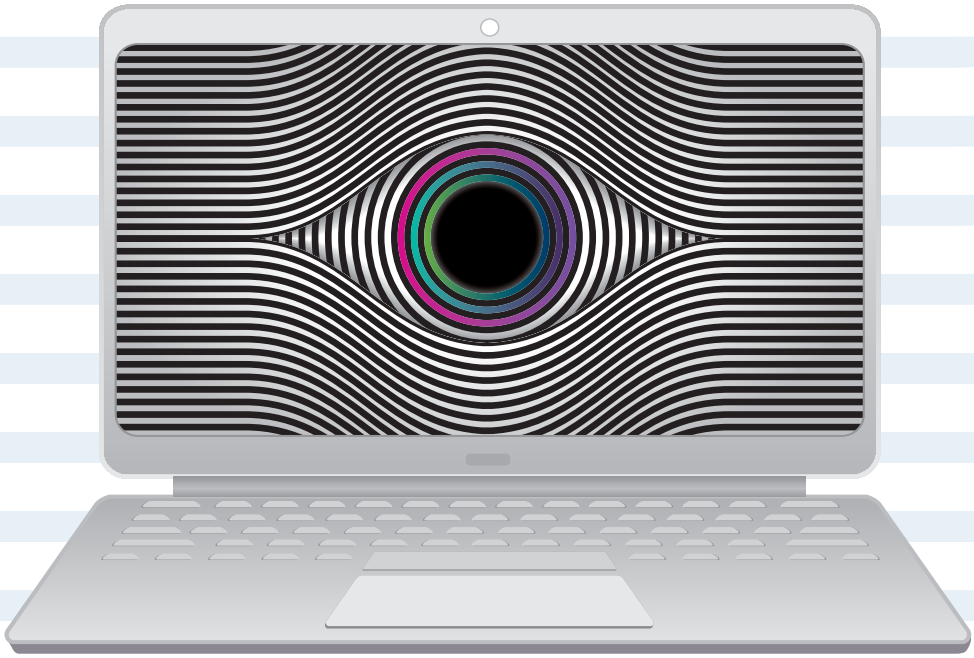
Ein Vorteil moderner Software-WORM-Systeme liegt in ihrer Unabhängigkeit von Hardwareherstellern und der existierenden Speicherinfrastruktur – ein Pluspunkt für jede langfristige Archivstrategie.

Sie lassen sich für beliebige Speicherinfrastrukturen einsetzen, völlig unabhängig davon, ob es das Festplattenmodell oder den Speicherhersteller in zehn, zwanzig oder dreißig Jahren noch gibt. Niemand kann heute sagen, welche Speichermodelle oder Speicherinfrastrukturen langfristig Bestand haben, dafür sind die Innovationszyklen der Speicherhersteller viel zu schnell und unberechenbar. Sicher ist aber eines: Das herstellerunabhängige Software-Worm kann sehr einfach von einem Speichertechnologieschritt zum nächsten völlig unproblematisch mitgenommen werden.

Fazit

Trotz technologischer Umwälzungen bleibt WORM ein fester Bestandteil zukunftsfähiger IT-Strategien. Insbesondere bei der revisionssicheren Langzeitarchivierung ist sie auch Jahrzehnte nach ihrer Erfindung unverzichtbar – und aktueller denn je.

Kai Hambrecht



Schatten-IT, Schatten-KI und das SaaS-Chaos

WIE UNTERNEHMEN DIE KONTROLLE ZURÜCKGEWINNEN

Als Marc, IT-Leiter eines international tätigen Unternehmens, in einem internen Ticketsystem auf die Nachricht „Ich kann mich nicht mehr in mein Projektmanagement-Tool einloggen" stieß, hielt er das zunächst für einen Routinefall. Doch die Situation nahm eine unerwartete Wendung: Die betroffene Abteilung arbeitete mit Asana – einer Software, die von der zentralen IT nie freigegeben oder verwaltet worden war.

Weitere Nachforschungen offenbarten das ganze Ausmaß: Über 50 verschiedene SaaS-Anwendungen waren im Unternehmen im Einsatz – viele davon parallel, redundant oder ohne Wissen der IT. Offiziell verwaltet wurden nur rund 20.

Dieses Beispiel ist kein Einzelfall. Immer mehr Unternehmen stehen vor ähnlichen Herausforderungen. Die dezentrale Nutzung von Cloud-Diensten nimmt zu – oft schneller, als IT und Governance-Strukturen darauf reagieren können. Das Ergebnis: steigende Kosten, Sicherheitslücken, ineffiziente Prozesse und wachsende Schatten-IT. Mit dem Einzug generativer KI-Tools entsteht zusätzlich ein neuer blinder Fleck: Schatten-KI, also der ungenehmigte Einsatz von KI-Diensten wie ChatGPT, Midjourney oder Copilot in Fachabteilungen, verschärft die Lage weiter.

Eine Reihe von aktuellen Studien zeigt die Dringlichkeit des Problems:

➤ 30 Prozent der SaaS-Ausgaben sind verschwendet (Gartner). Bei jährlichen SaaS-Kosten von 1 Million Euro bedeutet das eine Verschwendung von 300.000 Euro.

➤ 86 Prozent der Unternehmen nutzen generative KI-Technologien (Cohesity), oft ohne Wissen der IT. 54 Prozent der deutschen Wissensarbeiter verwenden inoffizielle KI-Tools (Software AG), was erhebliche Sicherheits- und Compliance-Risiken birgt.

➤ 71 SaaS-Anwendungen nutzen Unternehmen durchschnittlich, 32 Prozent mehr als 2021, über die Hälfte davon ohne Genehmigung (Productiv).

8.700 US-Dollar betragen die jährlichen SaaS-Ausgaben pro Mitarbeitenden. Davon sind 30 Prozent ungenutzt oder doppelt – eine Verschwendung von 2.600 US-Dollar pro Person, bei 1.000 Mitarbeitenden summiert sich das auf 2,6 Millionen Dollar jährlich (Torii).

4.500 Stunden für manuelle On- und Offboarding-Prozesse in einem Unternehmen mit 1.000 Mitarbeitenden (Okta). Bei einem IT-Stundensatz von 60 € entstehen

Kosten von 270.000 € jährlich, zusätzlich zu Sicherheitsrisiken und Fehleranfälligkeit.

Wichtige KPIs für ein effektives SaaS-Management

Ein effektives SaaS-Management ist essenziell für Unternehmen, um Kosten zu optimieren, IT-Prozesse zu automatisieren und die IT-Sicherheit zu gewährleisten. SaaS-Management-Tools bieten hierfür umfangreiche Funktionen wie automatisierte Lizenzverwaltung, Zugriffsmanagement, Nutzungsanalysen und Compliance-Kontrollen. Durch den Einsatz solcher Tools können relevante Kennzahlen gezielt verbessert werden, wodurch sich sowohl wirtschaftliche als auch sicherheitstechnische Vorteile ergeben., zum Beispiel:

➤ **Lizenznutzungseffizienz:** Sie zeigt, wie viele der bezahlten SaaS-Lizenzen tatsächlich genutzt werden. In vielen Unternehmen entstehen hier erhebliche Ineffizienzen, da Lizenzen oft überflüssig, doppelt vergeben oder nach dem Austritt von Mitarbeitenden nicht deaktiviert werden. SaaS-Management-Tools optimieren diesen Bereich durch automatisierte Lizenzüberwachung, die über API-Integrationen die tatsächliche Nutzung analysiert und ungenutzte Lizenzen identifiziert. Rollenbasierte Lizenzzuweisungen ermöglichen eine präzisere Vergabe, während automatische Deprovisionierung sicherstellt, dass Lizenzen bei Austritten oder Rollenwechseln umgehend gesperrt oder zurückgegeben werden.

➤ **SaaS-Kosten pro Mitarbeitendem:** Diese Kennzahl liefert Einblicke in die Kostenstruktur pro Nutzer und hilft, redundante oder ineffiziente Software-Ausgaben zu identifizieren. SaaS-Management-Tools schaffen hier Transparenz, indem sie über zentrale Dashboards alle SaaS-Ausgaben je Nutzer, Team oder Abteilung aggregieren. So lassen sich Abweichungen erkennen und die Rentabilität einzelner Anwendungen bewerten. Eine optimierte Vertragsverwaltung sorgt dafür, dass Abonnementkosten effizient gesteuert und überdimensionierte Lizenzmodelle vermieden werden. Maschinelles Lernen unterstützt zudem die automatische Lizenz-Zuordnung auf Basis der tatsächlichen Nutzung – und reduziert so Überlizenzierung.

➤ **Schatten-IT-Reduzierung:** Dabei geht es um die Nutzung nicht genehmigter oder unbekannter SaaS-Anwendungen innerhalb eines Unternehmens. Diese unkontrollierte Nutzung führt zu Compliance-Risiken, Sicherheitslücken und unnötigen Mehrkosten. SaaS-Management-Tools bieten eine automatische SaaS-Erkennung, indem sie sich mit Identity-Management-Systemen wie Okta oder Azure AD integrieren und auf Basis von Single Sign-On- und Netzwerk-Logs unautorisierte Anwendungen identifizieren. Zudem ermöglichen Whitelisting- und Blacklisting-Funktionalitäten die zentrale Festlegung erlaubter Anwendungen, während Alerting-Mechanismen Nutzer proaktiv über Schatten-IT warnen und ihnen alternative, genehmigte Lösungen anbieten.

➤ **Effizientes On- und Offboarding:** Die Dauer, die benötigt wird, um neue Teammitglieder mit den notwendigen SaaS-Tools auszustatten oder scheidende Mitarbeitende vollständig zu deprovisionieren, hat direkten Einfluss auf die Produktivität und IT-Sicherheit. Durch automatisiertes User-Provisioning über SCIM-Schnittstellen können SaaS-Management-Tools eine nahtlose Integration in bestehende Identity-Management-Plattformen gewährleisten. Workflows für die Rechteverwaltung sorgen dafür, dass Mitarbeitenden automatisch nur die für ihre Rolle notwendigen Berechtigungen zugewiesen werden, während durch eine nahtlose HR-Integration sichergestellt wird, dass ausgeschiedene Mitarbeitende sofort aus allen Systemen entfernt werden. Dadurch sinkt nicht nur das Risiko unautorisierter Zugriffe, sondern auch der manuelle Aufwand für die IT-Abteilung.

DER EINSATZ EINES SAAS-MANAGEMENT-TOOLS SENKT KOSTEN, AUTOMATISIERT IT-PROZESSE UND VERBESSERT DIE SICHERHEITSLAGE.

Dr. Thomas Gerick,
Berater, USU GmbH, www.usu.com

➤ **Reduzierung von IT-Support-Tickets:** Ein Großteil der Tickets im SaaS-Umfeld resultiert aus Passwort-Rücksetzungen, Zugriffsproblemen oder Unklarheiten bezüglich der Lizenzvergabe. Durch den Einsatz von Self-Service-Portalen erhalten Mitarbeitende die Möglichkeit, eigenständig neue SaaS-Tools zu beantragen oder Zugangsprobleme zu lösen, wodurch der IT-Support entlastet wird. Zusätzlich reduziert eine zentralisierte Authentifizierung über Single Sign-On (SSO) das Risiko vergessener Zugangsdaten erheblich. KI-gestützte Support-Automatisierung oder automatisierte Workflows, ermöglicht es, häufige Supportfälle wie Lizenzanfragen oder Rollenwechsel ohne manuelle IT-Eingriffe zu lösen.

Der Einsatz eines SaaS-Management-Tools senkt Kosten, automatisiert IT-Prozesse und verbessert die Sicherheitslage. Durch die Optimierung zentraler Kennzahlen wie Lizenznutzung, SaaS-Kosten pro Mitarbeitenden, Schatten-IT-Anteil und On-/Offboarding-Zeiten werden Einsparpotenziale realisiert und die IT transparenter und effizienter. Eine vollständige Automatisierung kann sich bereits nach wenigen Monaten amortisieren. Langfristig profitieren Unternehmen von höherer IT-Produktivität, besserer Compliance und optimierten Kostenstrukturen.

Dr. Thomas Gerick

Smarte Einführung der E-Rechnung

TIPPS, TRICKS UND EINE CHECKLISTE FÜR IT-ENTSCHEIDER

Anfang 2025 wurde in Deutschland im B2B-Bereich die E-Rechnungspflicht eingeführt. Den rechtlichen Background bildet das Wachstumschancengesetz, in dem die Bundesregierung definiert, was sie unter einer elektronischen Rechnung versteht. Demnach handelt es sich um eine Rechnung, die in einem strukturierten elektronischen Format ausgestellt, übermittelt und empfangen wird und eine elektronische Verarbeitung ermöglicht. Das strukturierte elektronische Format muss der europäischen Norm für die elektronische Rechnungsstellung und der Liste der entsprechenden Syntaxen gemäß RL 2014/55/EU entsprechen (und damit der CEN-Norm EN 16931).

Die Einführung des neuen Rechnungsformats wirft in den Unternehmen zahlreiche Fragen auf. Beispielsweise, welche Prozesse von der Regelung betroffen sind und welche technischen Anforderungen erfüllt werden müssen. Außerdem handelt es sich um eine schrittweise Einführung, sodass noch nicht alle Unternehmen E-rechnungspflichtig sind. Ziel ist es, dass die Unternehmen ausreichend Zeit zur Anpassung ihrer Systeme und Prozesse haben. Unterschieden wird bei den Übergangsfristen zwischen dem Versenden und Empfangen von E-Rechnungen.

Übergangsfristen sollen die Einführung erleichtern

Seit dem 1. Januar 2025 müssen alle Unternehmen und Behörden ausnahmslos in der Lage sein, E-Rechnungen zu empfangen und zu verarbeiten. Konkret bedeutet das, sie müssen den XML-Datensatz einer E-Rechnung zur Weiterverarbeitung visualisieren und archivieren können – optimalerweise innerhalb eines ERP-Systems. Der Versand von Papierrechnungen und elektronischen Rechnungsformaten (PDF, EDI), die nicht EN 16931 konform sind, ist bis Ende 2026 zulässig. Ab dem 1. Januar 2027 ist die

DREI HERAUSFORDERUNGEN BEI DER UMSETZUNG DER E-RECHNUNGSPFLICHT

Optimale Datenqualität: Für die elektronische Rechnungsstellung ist eine hohe Datenqualität von zentraler Bedeutung. Unternehmen sollten darauf achten, dass ihre Daten präzise, vollständig und konsistent vorliegen. Automatisierte Validierungsprozesse können dabei hilfreich sein.

Sicherstellung der Rechtskonformität: Unternehmen sollten sich mit den rechtlichen Anforderungen und Standards vertraut machen und diese in ihre internen Abläufe integrieren. Fachkundige Unterstützung und regelmäßige Compliance-Kontrollen sorgen für zusätzliche Sicherheit.

Effektive Kommunikation fördern: Die Einführung fester Kommunikationswege und eine effiziente Gestaltung des Informations- und Datenaustauschs sind unerlässlich. Elektronische Austauschformate und standardisierte Protokolle unterstützen diesen Prozess.

E-RECHNUNG = §§ (EN 16931)

- ✔ Peppol BIS Billing
- ✔ X-Rechnung
- ✔ ZUGFeRD (hybride PDF)

SONSTIGE E-RECHNUNG

- ➜ EDIFACT
- ➜ VDA4906
- ➜ IDoc Invoice05
- ➜ UNIDOC
- ➜ csv
- ➜ JSON

Ausstellung von E-Rechnungen im B2B-Bereich verpflichtend. Ab diesem Zeitpunkt müssen alle Unternehmen E-Rechnungen an ihre Geschäftspartner ausstellen. Formate, die nicht EN 16931-konform sind, dürfen nur dann versendet werden, wenn der jeweilige Empfängers ausdrücklich zustimmt. Da Rechnungssender zukünftig in der Lage sein müssen, sowohl den XML-Datensatz als auch die Originalrechnung zu visualisieren, empfiehlt es sich, frühzeitig ein elektronisches Rechnungsprogramm in die eigenen Prozesse zu integrieren oder auf eine dedizierte Visualisierungslösung zu setzen.

Diese Voraussetzungen muss eine E-Rechnung erfüllen

Technisch basiert die E-Rechnung in Deutschland primär auf dem XRechnung-Standard, einer XML-basierten Syntax. Zugelassen sind die EU-Norm-konformen Varianten Cross Industry Invoice (CII) und Universal Business Language (UBL). Ein wichtiges E-Rechnungsformat, das dem XRechnung-Standard entspricht, ist ZUGFeRD (Zentraler User Guide des Forums elektronische Rechnung Deutschlands). Dieses hybride Format hat den Vorteil, dass es sowohl menschen- als auch maschinenlesbare Rechnungsdaten in einem Dokument speichert. Das ZUGFeRD-Format kann in verschiedenen Geschäftsszenarien (B2B, B2G, B2C) sowohl in Unternehmen als auch Behörden verwendet werden.

Ausnahmen von der E-Rechnungspflicht

Um die Einführung der elektronischen Rechnung möglichst pragmatisch zu gestalten, hat der Staat Unternehmen, die im Jahr 2026 einen Jahresumsatz von maximal 800.000 € haben, von der Pflicht des E-Rechnungsversandes vorerst ausgenommen. Für sie gilt eine Übergangsfrist bis Dezember 2027. Bestimmte Rechnungsarten sind sogar vollständig von der E-Rechnungspflicht befreit: Rechnungen unter 250 €, Fahrausweise und Rechnungen an Verbraucher sowie Bereiche, in denen der Austausch von Papierrechnungen gesetzlich vorgeschrieben ist.

E-Rechnungen einführen

Wie aber lässt sich der Rechnungsstellungsprozess konkret auf das E-Rechnungsformat umstellen? Zunächst ist eine gründliche Status-Quo-Analyse erforderlich. Zuerst sollten die Versandwege der Rechnungen, die verwendeten Formate sowie die Versandhäufigkeit untersucht werden, um daraus den konkreten Handlungsbedarf abzuleiten. Dann gilt es, relevante Systeme und Schnittstellen zu identifizieren, die für den EU-Norm -konformen Rechnungsaustausch oder -eingang berücksichtigt werden müssen. Außerdem muss geklärt werden, welche zusätzlichen Daten innerhalb der E-Rechnung noch benötigt werden, um der EN 16931-Norm vollständig zu entsprechen. All diese Informationen erleichtern die Integration der elektronischen Rechnungsstellung in die FiBu-, das ERP- oder Archiv- und Dokumentenmanagement.

Wichtig: Neben dem korrekten Auslesen und Erkennen der strukturierten Daten aus einer E-Rechnung spielt auch das Decodieren aus XML und das vorgangsbezogene Speichern eine zentrale Rolle. Geklärt werden muss auch, ob bereits eine EN 16931-kompatible Version des Buchhaltungs-/ ERP-Systems vorliegt und inwieweit diese die Rahmenbedingungen des Unternehmens und der Branche erfüllt. Darüber hinaus gilt es zu prüfen, ob die EN 16931-konformen Codes korrekt in das Zielsystem übertragen werden und die Kreditorenbuchhaltung darauf zugreifen und mit den Daten arbeiten kann. Schließlich sollte man kontrollieren, ob der Inhalt einer E-Rechnung EN 16931-konform angelegt ist.

Interaktive Checkliste hilft bei Einführung

compacer hat eine Checkliste veröffentlicht, die konkrete Tipps und Schritte umfasst, die Unternehmen helfen, sich EN 16931-ready aufzustellen. Unterschieden werden drei Phasen der Umstellung. Zunächst geht es um ein möglichst vollständiges Bild der Ausgangssituation, für welches die Checkliste einen Leitfaden bietet. Dann rückt die Systemlandschaft in den Fokus und es geht darum zu ermitteln, welche Daten wo vorhanden sind und ob beziehungsweise wie diese miteinander verknüpft sind.

Schlussendlich stehen die Inhalte und deren aufgeführte Reihenfolge im Fokus, die in einer E-Rechnung in einer gesetzlich vorgeschriebenen Formatierung enthalten sein müssen, um der EN 16931-Norm zu entsprechen.

Die Checkliste ist damit Orientierungshilfe und Leitfaden zugleich. Sie umfasst nicht nur alle innerhalb eines Unternehmens von der Umstellung betroffenen Bereiche, sondern bietet auch Zusatzinformationen und Tipps. Wer sich nicht nur rechtzeitig auf eine Digitalisierung seines Rechnungsstellungsprozesses vorbereiten möchte, sondern auch das volle Potenzial der Umstellung ausschöpfen will, für den ist die EN-16931-Norm- ready Checkliste ein optimaler Ausgangspunkt.

Dirk Auberlen | www.compacer.com

CHECKLISTE

Die Checkliste steht zum kostenlosen Download bereit.

Was gute IT-Leadership heute ausmacht

ZWISCHEN TECHNOLOGIE-EXPERTISE UND SOZIALEN KOMPETENZEN

Führungskräfte in der IT stehen unter Druck. Sie sollen nicht nur den technologischen Wandel im eigenen Unternehmen anführen, was starke bereichsübergreifende Führungsqualitäten erfordert, sondern auch fortlaufend ihre Teams und deren Fähigkeiten in einem sich ständig ändernden Umfeld ausbauen. Dabei zählt technologisches Know-how ohne Frage zu den zentralen Kompetenzen – insbesondere in einer Arbeitswelt, die immer mehr von generativer und agentischer KI beeinflusst wird. Doch gelten heute auch Power Skills wie analytisches Denken, Empathie, aktives Zuhören, kreatives Denken und Neugier als zentrale Führungsqualitäten. Laut des aktuellen Future of Jobs Reports des World Economic Forums machen Power Skills wie diese den größten Anteil der zehn wichtigsten Kernkompetenzen aus. Im Vergleich mit dem Report 2023 haben Führung und sozialer Einfluss, Belastbarkeit, Flexibilität und Agilität sowie KI und Big Data am stärksten an Bedeutung gewonnen.

Welche Kompetenzen CIOs und IT-Teams jetzt brauchen

Gute CIOs verbinden technische Expertise mit emotionaler Intelligenz und Führungsqualitäten. Sie verstehen, wie Technologie zu besseren Geschäftsergebnissen führen kann, und bringen Compliance-Anforderungen mit den Unternehmenszielen in Einklang. Mehr noch: Sie positionieren die IT als bedeutenden Teil der Geschäftsstrategie. Dabei muss ihr Fokus darauf liegen, ein Gleichgewicht zwischen der Optimierung von Abläufen und dem Anführen der Transformation herzustellen.

Power Skills helfen CIOs, ein vertrauensvolles Verhältnis zu ihren Teams und der Führungsebene aufzubauen. Diese Fähigkeiten sind entscheidend, damit sie effektiv mit anderen Führungskräften kommunizieren und zusammenarbeiten, ihre Teams leiten und ausbauen und Innovationen im Unternehmen vorantreiben können. Die effektivsten Tech-Leader nutzen ihr technisches Wissen, um die IT auf dem Laufenden zu halten – und setzen gleichzeitig ihre Neugier, Empathie und Führungsstärke dazu ein, um ihre Teams durch den Wandel zu leiten.

Wenn alle Teammitglieder über gute Power Skills verfügen, ist es wahrscheinlicher, dass sie die Perspektiven der anderen verstehen und respektieren, auf gemeinsame Ziele hinarbeiten und sich gegenseitig bei Herausforderungen unterstützen. Auf die-

POWER SKILLS – DIE NEUEN KERNKOMPETENZEN

Analytisches Denken
Komplexe Probleme strukturiert analysieren und datenbasierte Entscheidungen treffen

Empathie
Teams verstehen, motivieren und durch Veränderungen führen

Aktives Zuhören
Effektive Kommunikation und Aufbau vertrauensvoller Beziehungen

se Weise entsteht eine positive und produktive Teamkultur, in der sich alle wertgeschätzt fühlen und motiviert sind, ihr Bestes zu geben.

Wie IT-Teams zukunftsfähig bleiben

Durch ihren Einfluss in der Organisation und ihre Wachstumsmentalität prägen CIOs und IT-Führungskräfte sowohl die Innovationsfähigkeit als auch die gesamte Unternehmenskultur. Führungskräfte, die echte Neugier zeigen, nach dem „Warum" fragen, wenn sie eine neue Initiative oder ein neues Projekt starten, und ihre Bemühungen mit strategischen Geschäftsergebnissen verbinden, stellen sicher, dass ihre Maßnahmen auf die Prioritäten des Unternehmens abgestimmt sind. Damit erfüllen sie auch eine Vorbildfunktion und zeigen, wie wichtig bereichsübergreifende Zusammenarbeit und ein Fokus auf qualitative Ergebnisse statt Output sind. Denn nicht nur unser Arbeitsumfeld hat sich verändert – bei Skillsoft arbeiten wir zum Beispiel remote first –, dank wachsender Möglichkeiten durch Cloud-Technologien, datengesteuerte Entscheidungsprozesse und KI werden vereinzelte Silos aufgebrochen und starke teamübergreifende Partnerschaften führen schneller zu Ergebnissen. Darüber hinaus verlagert sich die Rolle der IT-Abteilung von direkter Kontrolle über alle technologiebezogenen Aktivitäten hin zu einer starken Governance.

NUR MIT FÄHIGKEITEN WIE EMPATHIE UND NEUGIER KANN ES CIOS UND IT-FÜHRUNGSKRÄFTEN GELINGEN, ZUKUNFTSFÄHIGE TEAMS AUFZUBAUEN.

Orla Daly, CIO, Skillsoft, www.skillsoft.com

Es gibt heute viel mehr funktionsübergreifende Teams, die sich aus verschiedenen Abteilungen zusammensetzen und alte Strukturen aufbrechen. Wenn die Barrieren beseitigt sind, können Projekte zügiger voranschreiten. Das setzt kreative Energie frei, motiviert zum Experimentieren und fördert neue Ideen, die die Organisation voranbringen.

Natürlich geschieht eine solche Veränderung nicht über Nacht. Mitarbeitende wie Führungskräfte brauchen dafür nicht nur den nötigen Freiraum, sondern auch gezielte Fort- und Weiterbildungen, um die eigenen Kompetenzen auszubauen und den kulturellen Wandel anzunehmen. Dank aufstrebender Technologien wie agentischer KI gibt es heute zunehmend personalisierte Lernangebote, die auf die individuellen Fähigkeiten und Ziele der Teammitglieder einzahlen. Aber auch Formate wie Hackathons sind sinnvoll, da sie verschiedene Teams für die Lösung eines Problems zusammenbringen und aufzeigen, wie sie zukünftig zusammenarbeiten könnten.

Mentorship: CIOs als Wegbereiter für den IT-Nachwuchs

Es ist wichtig, dass CIOs ihren Teams und Mentees eine gemeinsame Mission vermitteln, die ihnen Klarheit, Orientierung und Sinn gibt und aufzeigt, was es bedeutet, in unserer technologischen Welt eine IT-Führungskraft zu sein. Eine klare Vision und operative Rahmenbedingungen dienen als Anker für die Teammitglieder und erinnern daran, auf welche Ziele sie ihre Energie konzentrieren sollten. Das erleichtert es auch, Investitionen innerhalb einer Organisation aufeinander abzustimmen und Prioritäten zu setzen –

Kreatives Denken
Innovative Lösungsansätze entwickeln und Transformationen vorantreiben

Neugier
Nach dem „Warum" fragen und kontinuierliches Lernen fördern

Führung & Einfluss
Teams inspirieren und bereichsübergreifend zusammenarbeiten

insbesondere dann, wenn konkurrierende Interessen aufeinandertreffen. Auf dem hart umkämpften IT-Arbeitsmarkt von heute kann dies von Vorteil sein und dazu beitragen, einen vielseitigeren Talentpool aufzubauen, das Engagement zu stärken und die Bindung an das Unternehmen zu fördern.

Aus diesen Gründen sind Mentoring und die Entwicklung von Power Skills für IT-Teams und -Führungskräfte von großer Bedeutung. Dies ist allerdings nur möglich, wenn Fähigkeiten wie Kommunikation, aktives Zuhören und Empathie richtig verstanden und angewandt werden. Dann schaffen CIOs gleichzeitig eine Grundlage für ein offenes Miteinander, Vertrauen und Awareness für die Gesundheit der Mitarbeitenden – und können dazu beitragen, Teams zu vereinen und Stressfaktoren in der Zusammenarbeit zu reduzieren.

Fazit: IT-Führungskräfte brauchen einen klaren Kompass

Um im Job erfolgreich zu sein, müssen sich CIOs auf das Wesentliche konzentrieren: eine starke operative Disziplin, die qualitative Ergebnisse über Output stellt, robuste und sichere technologische Grundlagen, die Verwaltung von Budgets und die Fähigkeit, den geschäftlichen Anforderungen einen Schritt voraus zu sein und gleichzeitig das Tempo für die Einführung neuer Technologien im Unternehmen vorzugeben. Aktuell stehen viele CIOs vor der Herausforderung, den Einsatz von KI in ihrem Unternehmen voranzutreiben und ihre Teams entsprechend vorzubereiten und mitzunehmen. Dabei geht es nie nur um das Erlernen und Implementieren neuer Tools, sondern auch

um innerbetriebliche Strukturen, Zuständigkeiten und Zusammenarbeit.

Technisches Können allein genügt nicht mehr. Nur mit Fähigkeiten wie Empathie und Neugier kann es CIOs und IT-Führungskräften gelingen, zukunftsfähige Teams aufzubauen. Indem sie ihre Power Skills erkennen und einsetzen, erfüllen sie ihre Rolle als Führungskraft, die neben der Verantwortung für die IT und die Verwaltung von Systemen auch beinhaltet, das Unternehmen durch den Wandel zu führen, um das Geschäft zu transformieren.

Orla Daly

Cyber-Risiken

FÜHRUNGSKRÄFTE SIND SICH ZU SICHER

Beazley veröffentlichte seinen aktuellen Risk & Resilience Report Spotlight: Tech Transformation & Cyber-Risiken 2025.

In Deutschland nennen 30 Prozent der Führungskräfte Cyber-Risiken als ihre größte Bedrohung – 2024 waren es noch 28 Prozent. Doch während das Bewusstsein wächst, fühlen sich 87 Prozent besser darauf vorbereit, gegenüber 81 Prozent im Jahr 2024. Das könnte auf ein falsches Sicherheitsgefühl deuten, denn vielen Unternehmen mangelt es immer noch an der erforderlichen Wachsamkeit.

Auch das Thema der künstlichen Intelligenz wird immer präsenter: 77 Prozent der befragten Führungskräfte sind der Meinung, dass sich KI in diesem Jahr positiv auf ihr Geschäft auswirken wird. Außerdem rechnen 68 Prozent damit, dass KI in den nächsten 18 Monaten Arbeitsplätze in ihren Unternehmen ersetzen werde. Damit einhergehend nimmt auch die Sorge rund um das Thema Datenschutz und IP-Risiken zu (IP für Intellectual Property – dt. geistiges Eigentum). Während die technologische Obsoleszenz letztes Jahr noch 27 Prozent beschäftigte, sinkt die Sorge darüber dieses Jahr auf 23 Prozent.

Cyber-Risiken rücken stärker in den Fokus

Auch Ransomware ist nach wie vor ein zentrales Problem, das jetzt durch KI verstärkt und beschleunigt wird – mit höherer Wirkung. Gleichzeitig ist Hacktivismus auf dem Vormarsch, bei dem Aktivisten in Systeme eindringen, um Geschäftsprozesse zu stören oder den Ruf zu schädigen. Eine Bedrohung für Unternehmen, die zwischen ideologischen Fronten stehen.

www.Beazley.com

MEHR WERT

Spotlight: Tech Transformation & Cyber-Risiken 2025

Die Zukunft des Asset- und Instandhaltungsmanagements

WIE NEUE TECHNOLOGIEN DIE GEBÄUDEVERWALTUNG UND -INSTANDHALTUNG REVOLUTIONIEREN

Die Facility Management-Branche durchlebt derzeit einen fundamentalen Wandel. Digitale Technologien und innovative Lösungsansätze heben die Gebäudeverwaltung und -instandhaltung auf ein neues Level. Welche Entwicklungen diesen Transformationsprozess vorantreiben und wie Unternehmen davon profitieren können, verdeutlicht der folgende Fachbeitrag.

Die Arbeitsweisen sowie die Erwartungen an Arbeitsplätze haben sich in den vergangenen Jahren fundamental gewandelt. Niedrige Gebäudeauslastungen sind heute keine Seltenheit mehr. Viele Unternehmen würden ihre Belegschaft zwar gerne wieder öfter vor Ort begrüßen, erzwingen lässt sich dies in Zeiten eines hart umkämpften Wettbewerbs um Fachkräfte jedoch nicht mehr. Stattdessen gilt eine ansprechende, gesunde und sichere Arbeitsumgebung als entscheidender Faktor für höhere Belegungsraten.

Die Facility Management-Branche steht also vor der Herausforderung, das Asset- und Instandhaltungsmanagement mithilfe digitaler Lösungen strategisch zu verbessern und dadurch für positive Gebäudeerlebnisse zu sorgen. Neben dem Beherrschen moderner Technologien wie KI, Digitale Zwillinge, Wärmepumpen, Mikronetze, Solarenergie und dem Internet der Dinge (IoT) sind auch proaktive und vorbeugende Instandhaltungsstrategien unerlässlich. Doch woher kommt dieser Wandel hin zu digitalen Lösungen eigentlich?

Die Gründe für den Wandel

Digitale Lösungen haben große Auswirkungen auf das Erlebnis unserer bebauten Umwelt und werden zunehmend nicht nur akzeptiert, sondern sogar erwartet. Den Betreibern und Nutzern von Gebäuden bietet die Digitalisierung die Möglichkeit, auf umfangreiche Anlageninformationen zuzugreifen, sie zu überwachen und zu verfolgen – um dadurch die Erwartungen an die Gebäudeerlebnisse zu erfüllen.

Auch der demografische Wandel mit einer alternden Belegschaft im Bereich der Gebäudeinstandhaltung trägt zur digitalen Transformation bei. Denn ein möglichst digitales Arbeitsumfeld hilft dabei, die dringend notwendigen jungen Talente anzuziehen und schneller einzuarbeiten. Parallel dazu haben die COVID-19-Pandemie sowie die Verbreitung von KI-Tools als Beschleunigungs-Booster für die Adaption neuer Technologien gewirkt.

Dies erhöht jedoch gleichzeitig auch den Druck auf Instandhaltungsteams, da Kunden in einer digitaleren Gesellschaft höhere Servicequalitätsstandards erwarten – wie etwa Lösungen für die prädiktive Wartung oder Benutzer-Self-Services, um die Reaktionsfähigkeit und Geräteverfügbarkeit zu verbessern.

Der Ausgangspunkt bestimmt die Strategie

Bevor die künftige Strategie oder gar der Einsatz spezifischer Technologien diskutiert wird, sollten Unternehmen zunächst ihre Situation verstehen und den aktuellen Reifegrad ihres Asset- und Instandhaltungsmanagements ermitteln. Dieser lässt sich in fünf verschiedenen Phasen kategorisieren:

DIGITALE LÖSUNGEN HABEN GROSSE AUSWIRKUNGEN AUF DAS ERLEBNIS UNSERER BEBAUTEN UMWELT UND WERDEN ZUNEHMEND NICHT NUR AKZEPTIERT, SONDERN SOGAR ERWARTET.

Daniel Negro,
Sales Director, Planon,
www.planonsoftware.com

#1 Reaktive Instandhaltung

#2 Geplante Instandhaltung

#3 Proaktive Instandhaltung

#4 Datengesteuerte Instandhaltung

#5 Zielbasierte Instandhaltung

Der aktuelle Reifegrad ist ein entscheidender Faktor für Investitionsentscheidungen, da er bestimmt, welche kommenden Modernisierungsschritte auf Basis der bestehenden technologischen Infrastruktur sinnvoll und umsetzbar sind.

Schlüsselbereiche zur Verbesserung der Instandhaltung

Im Umfeld der Gebäudeinstandhaltung stechen derzeit vier Bereiche heraus, die erhebliches Potenzial haben, die Zukunft der Branche mitzugestalten. Dazu gehört der Einsatz von IoT-, Mobile First- und Digital Twin-Lösungen, die dabei unterstützen, umfassende Anlagendaten zu erfassen, diese ortsunabhängig abzurufen und sogar automatisierte, datenbasierte Aktionen und Prozesse einzuleiten. Vor allem die ersten beiden Reifegradphasen werden erheblich von Investitionen in diesen Technologiebereich profitieren.

Mit der Aggregation und Nutzung umfangreicher Daten ist bereits ein bedeutender Schritt zu einem effizienteren Asset- und Instandhaltungsmanagement getan. Mit steigender Datenmenge werden die manuelle Auswertung und Nutzung der Daten jedoch immer aufwändiger. Der Einsatz von KI- und Datenanalyse-Tools, von der insbesondere die fortgeschrittenen Reifegrade profitieren, unterstützt bei der fundierten Entscheidungsfindung für Anlageninvestitionen und entlastet Instandhaltungstechniker auf vielfältige Weise.

Die prädiktive und präskriptive Instandhaltung beschreiben fortschrittliche Wartungsstrategien, die mithilfe von KI und Datenanalysen Anlagenprobleme vorhersagen und gezielte Maßnahmen vorschlagen, um diesen vorzubeugen. Dieser State-of-the-Art-Ansatz sorgt für deutliche Reduzierungen von Wartungskosten, Anlagenausfällen und Stillstandszeiten und ist das Mittel der Wahl in Branchen mit hohen Ansprüchen an die Geschäftskontinuität – wie etwa in Healthcare, Hightech oder Telekommunikation.

Aufgrund der gesamtgesellschaftlichen Bedeutung und zunehmender regulatorischen Vorgaben gehören die Themen Energie und Nachhaltigkeit über alle Reifegrade hinweg ebenfalls zu den Schlüsselbereichen in der FM-Branche. Da zwischen der Energieeffizienz und

der effektiven Instandhaltung mechanischer Gebäudesysteme ein wichtiger Zusammenhang besteht, sollte die Nachhaltigkeitsperspektive bei Investitionen in das Asset- und Instandhaltungsmanagement stets eine Rolle spielen.

Drei Tipps für smarte Investitionen

Die Liste der digitalen Lösungen in der Gebäudeinstandhaltung umfasst unzählige Technologien und Anbieter. Doch welche Lösungen adressieren die Instandhaltungsziele am besten? Für die Formulierung der richtigen Technologiestrategie und sinnvolle Investitionen sollten Unternehmen drei wichtige Aspekte beachten:

Identifikation und Priorisierung von Instandhaltungszielen: Mithilfe einer Balanced Scorecard, die sowohl die finanzielle Perspektive als auch Auswirkungen auf Kunden, interne Prozesse sowie Lernen, Entwicklung und Wachstum vereint, lassen sich verschiedene Lösungen anhand klarer Kennzahlen vergleichen. So ermitteln Strategieteams diejenigen Instandhaltungslösungen, die zur individuellen Zielsetzung passen und den Unternehmensanforderungen entsprechen.

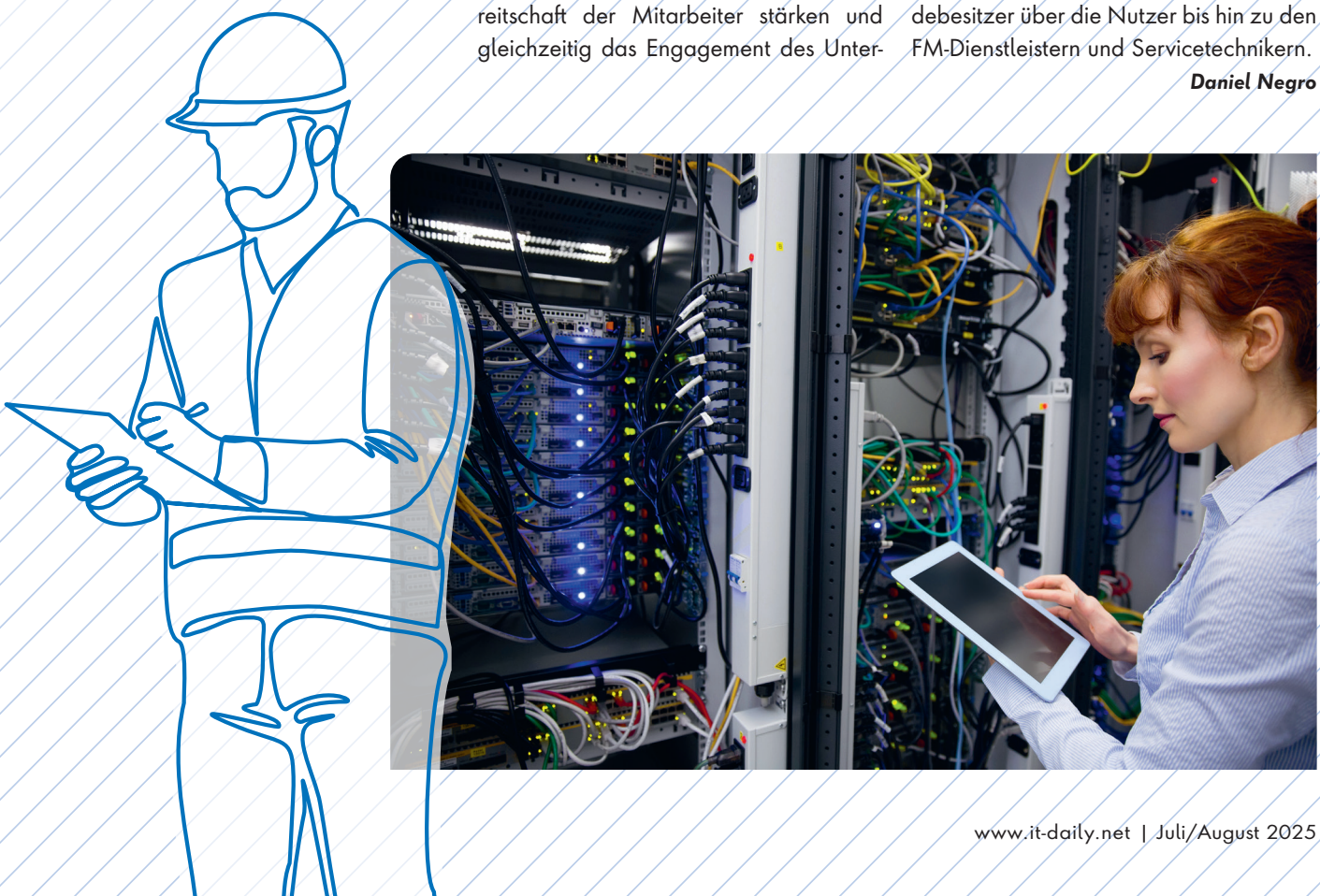
Technologieintegration: Isolierte Systeme bedeuten für Instandhaltungsteams einen enormen Mehraufwand und können dazu führen, dass die anvisierten Effizienzsteigerungen verpasst sowie Instandhaltungsanforderungen nicht erfüllt werden. Der Technologie-Stack entfaltet nur dann sein volles Potenzial, wenn die verschiedenen Lösungen sich nahtlos miteinander integrieren lassen.

Benutzerakzeptanz: Obwohl die Technologie die Instandhaltungstechniker nicht ersetzt, sondern auf vielfältige Weise unterstützt, ist die Sorge, dass dies geschehen könnte, weit verbreitet. Unternehmen sollten daher die Benutzerakzeptanz proaktiv angehen und dem Personal aufzeigen, dass sowohl die Serviceteams als auch der Instandhaltungsdienstleister und der Gebäudenutzer von der Technologie profitieren. Investitionen in Mitarbeiterschulungen verringern darüber hinaus die Mitarbeiterfluktuation, indem sie das Selbstvertrauen und die Arbeitsbereitschaft der Mitarbeiter stärken und gleichzeitig das Engagement des Unternehmens für die berufliche Weiterbildung demonstrieren.

Fazit

Der grundlegende Wandel durch die voranschreitende Digitalisierung stellt die Facility Management-Branche vor komplexe und wegweisende Weichenstellungen. Umso wichtiger ist eine strategische und analytische Herangehensweise, um die passenden Asset- und Instandhaltungstechnologien auszuwählen. Dazu bedarf es einer klaren Definition der eigenen Geschäftsziele und der Bewertung von Technologieauswirkungen auf das Kerngeschäft. Neben der klassischen Kosten-Nutzen-Abwägung hängt der Erfolg digitaler Lösungen auch ganz erheblich vom menschlichen Faktor ab – denn Menschen wünschen sich am Arbeitsplatz die gleichen digitalen Annehmlichkeiten wie in ihrem Privatleben und müssen Technologie als unterstützenden Faktor wahrnehmen. Sind diese Herausforderungen jedoch erst einmal überwunden, sorgen fortschrittliche digitale Lösungen für einen enormen Effizienzgewinn und ermöglichen umfangreiche Wettbewerbsvorteile für alle Beteiligten – vom Gebäudebesitzer über die Nutzer bis hin zu den FM-Dienstleistern und Servicetechnikern.

Daniel Negro



Besser flottmachen als wegwerfen

MIT AUSRANGIERTER HARDWARE KOSTEN UND CO_2 REDUZIEREN

Wir müssen Rohstoffe sparen – und deshalb die Kreislaufwirtschaft vorantreiben. Das ist vereinfacht gesagt eine der wesentlichen Vorgaben der neuen EU-Initiative Clean Industrial Deal. Besonders in gebrauchter IT-Hardware bleiben Rohstoffe bis heute millionenfach ungenutzt. Eine Chance für Unternehmen jeder Größenordnung.

Der Name der EU-Initiative ist neu, doch man sollte sich nicht täuschen lassen. Denn auch mit dem Clean Industrial Deal stehen Unternehmen in der Pflicht, ihre CO_2-Emissionen weiter zu verringern. Das angepeilte Ziel geht allerdings über reinen Umweltschutz hinaus: Mit der Initiative soll die europäische Wirtschaft wettbewerbsfähiger und krisensicherer werden. Sprich, wirtschaftlich und politisch unabhängiger von internationalen Rohstoffhändlern, globalen Lieferketten und den Regierungen anderer Länder. Die Mittel dazu lauten Dekarbonisierung, Ressourceneffizienz und Kreislauffähigkeit.

Keine leichte Aufgabe, besonders im Bereich IT-Hardware. Denn ohne Zweifel wird der Einsatz von KI den millionenfachen Verbrauch an Servern, PCs, Laptops oder Tablets zukünftig in noch größere Höhen treiben. In diesen Geräten stecken tonnenweise Ressourcen. Die aber großenteils schon nach zwei bis drei Jahren brachliegen, wenn die Modelle durch leistungsfähigere Neuware ersetzt werden. Diesen bequemen Austausch zu durchbrechen und in ein Kreislaufmodell zu überführen, ist eine Herausforderung. Aber eine, die sich Unternehmen stellen müssen, wenn sie handlungsfähig bleiben wollen. Denn im Schlepptau des EU-

Verkaufen Unternehmen ihre gebrauchte IT-Hardware für ein nachhaltiges Remarketing, sorgen zertifizierte IT-Dienstleister wie AfB social & green IT für garantierte Sicherheit. (Quelle: AfB Group)

Deals werden konkrete Maßnahmen zum Beschaffungswesen und Vergaberecht folgen, um die europäische Wirtschaft durch Dekarbonisierung und Materialkreisläufe zu unterstützen.

Herausforderung IT – viele Rohstoffe, kurze Nutzungsdauer

Erkennbar ist bereits, dass neben dem Kriterium „Made in Europe" weitere Nachhaltigkeits- und Resilienzkriterien in das öffentliche und private Beschaffungswesen sowie in die Vergabe öffentlicher Aufträge integriert werden sollen. Darüber hinaus plant die EU, den Einkauf von Rohstoffen für eine bessere Verhandlungsposition zu bündeln und insbesondere schwer zu beschaffende Rohstoffe mehr zu recyceln. Bis 2030 soll fast ein Viertel aller Stoffe kreislauffähig sein. Gerade bei IT-Geräten gestaltet sich das allerdings sehr aufwendig. Denn in der Regel besteht selbst ein Smartphone aus mehr als einem Dutzend verschiedener Metalle, darunter die sogenannten Seltenen Erden. Alle in kleinen bis winzigen Mengen, kaum voneinander zu trennen, und ein Großteil davon nur unter intransparenten oder zumindest klimaschädlichen Umständen zu beschaffen. Unter diesen Aspekten ist die kurze Nutzungsdauer der Geräte besonders schmerzhaft.

Refurbishing, Remarketing und Recycling

Mit dem Verkauf ihrer gebrauchten IT zur Wiederaufbereitung können Großkonzerne ebenso wie Mittelständler aktiv gegensteuern. Denn IT-Remarketing verlängert die Lebensdauer der Geräte deutlich, das Recycling der nicht verwertbaren Hardware-Komponenten fördert außerdem die Materialkreisläufe. Ein professioneller, zertifizierter Partner ist allerdings – zur eigenen unternehmerischen Sicherheit – unabdingbar, wenn man bedenkt, welche Arbeitsschritte zum IT-Refurbishing, Remarketing und Recycling gehören.

Eins der ersten und wichtigsten Kriterien im Refurbishing- und Remarketing-Prozess ist die Datensicherheit. Die gebrauchte Hardware muss absolut zugriffsicher zum Verwerter transportiert und dort DSGVO-konform vollständig gelöscht oder nicht löschbare Datenträger vernichtet werden. Das betrifft im Übrigen auch Drucker oder andere Hardware, bei der die integrierte Datenspeicherung nicht sofort offensichtlich ist.

Nach dem Löschen werden die Geräte technisch geprüft, gereinigt und defekte oder veraltete Komponenten ausgetauscht. Ist der Refurbisher von Microsoft autorisiert, wird zusätzlich eine Microsoft-Lizenz auf das Gerät aufgespielt. Danach entspricht die Hardware technisch fast einem Neuprodukt und kann in den Wiederverkauf gehen. Meist über Online-Plattformen mit entsprechender Versandlogistik im Hintergrund, aber auch in speziellen Stores mit geschultem Verkaufspersonal vor Ort.

Sind Geräte oder Komponenten für das IT-Remarketing nicht mehr geeignet, bietet sich im letzten Schritt ein zertifiziertes Recycling an. Dafür müssen alle Teile akribisch zerlegt, die enthaltenen Wertstoffe umweltschonend voneinander getrennt und fachgerecht für die Wiederverwertung aufbereitet werden.

Garantierte Sicherheit nur bei zertifizierten IT-Unternehmen

Die Komplexität dieser Prozesse bringt diverse Stolperfallen mit sich. Angefangen vom Datenschutz bei Transport und Löschvorgang über den Umweltschutz beim Refurbishing und Recycling bis zum Klimabeitrag durch das Remarketing. Eine durchgängige Transparenz zu allen verkauften Geräten, hundertprozentige Datensicherheit, gesetzeskonformes Recycling sowie fundierte Nachweise zu ihren CO_2-Einsparungen bekommen Unternehmen deshalb nur bei zertifizierten IT-Anbietern.

Zum Beispiel bei AfB social & green IT. Einer von wenigen autorisierten Microsoft-Refurbishern in Deutschland. TÜV-geprüft und ISO-zertifiziert im Qualitätsmanagement (ISO 9001), Umweltmanagement (ISO 14001) sowie im Informationssicherheitsmanagement (ISO/IEC 27001), außerdem staatlich anerkannter Entsorgungsfachbetrieb. Seinen Partnerunternehmen stellt AfB wissenschaftlich fundierte Wirkungsurkunden über das Refurbishing aus, mit detaillierten Zahlen zu den abgegebenen Geräten, eingesparten CO_2-Emissionen, Rohstoffen, Wasser, Energie und weiteren Fakten.

Damit liefert der IT-Dienstleister Konzernen, Großfirmen und mittelständischen Betrieben, die eine nachhaltige Lösung für ihre gebrauchte Hardware suchen, sämtliche Voraussetzungen. „Die Zusammenarbeit zwischen Siemens und AfB ist ein Gewinn für beide Unternehmen", sagt auch Hanna Hennig, CIO von Siemens. „Wir haben einen verlässlichen, sozial engagierten Partner für unsere ausrangierte IT-Hardware gefunden, dessen Prozesse hinsichtlich Datensicherheit auf höchstem Niveau sind. Wir übernehmen Verantwortung für die Umwelt durch Abfallreduzierung und Recycling. Durch die Partnerschaft erhalten Menschen mit Beeinträchtigung eine sinnvolle und nachhaltige Beschäftigung bei AfB." Die Partnerschaft zwischen Siemens und AfB besteht seit über zehn Jahren.

Doppelte Nachhaltigkeit

Warum Unternehmen wie Siemens durch eine Partnerschaft mit AfB gleich doppelt profitieren, erschließt sich aber erst auf den zweiten Blick: Die AfB gGmbH ist ein Inklusionsunternehmen. Das heißt, sie agiert frei am Markt, während ihre Belegschaft knapp zur Hälfte aus Menschen mit Behinderungen besteht. AfB-Partner sammeln im Bereich Nachhaltige Beschaffung sowohl Pluspunkte in Bezug auf Umwelt und Klima als auch für ihre soziale Nachhaltigkeit. Als erster Refurbisher überhaupt hat AfB diese soziale Wirkung extern untersuchen und wissenschaftlich bestätigen lassen. Die Effekte der Inklusion werden den Partnerunternehmen ebenfalls in ihren individuell ausgestellten Wirkungsurkunden nachgewiesen.

www.afb-group.de

UNSERE THEMEN

it management

Fokusthema: IT Service Management

Schwerpunktthemen: Data Center, Digitalisierung, Managed Services, Smart Office Solutions

Die Ausgabe 09/10 2025 erscheint am 12. September 2025

UNSERE THEMEN

it security

Spezialthema: IT-SA Spezial

Cybersecurity: Die Cybersecurity-Landschaft wandelt sich permanent – und wir wandeln uns mit. Statt starrer Themenplanung folgen wir dem Puls der Security-Welt und bleiben so immer aktuell.

WIR WOLLEN IHR FEEDBACK

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

INSERENTENVERZEICHNIS

it management

it security

IMPRESSUM

Herausgeber: Ulrich Parthier (08104-6494-14)

Geschäftsführer: Ulrich Parthier, Vasiliki Miridakis

Chefredaktion: Silvia Parthier (-26)

Redaktion: Carina Mitzschke (nur per Mail erreichbar)

Redaktionsassistenz und Sonderdrucke: Eva Neff (-15)

Autoren: Dirk Auberlen, Ralf Bachthaler, Lars Becker, Antonio Cavalieri, Orla Daly, Andreas Fuchs, Dr. Thomas Gerick, Kai Hambrecht, Sven Hausen, Marco Heid, Timo Rüb, Ivo Konecny, Anže Mis, Carina Mitzschke, Daniel Negro, Marc Neher, Silvia Parthier, Ulrich Parthier, Guido Piech, Joyce Studier, Anushree Verma, Sebastian Weber, Ralph Weiss, Dina Ziems

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. 32.
Preisliste gültig ab 1. Oktober 2024.

Mediaberatung & Content Marketing-Lösungen
it management | it security | it daily.net:
Kerstin Fraenzke, 08104-6494-19, fraenzke@it-verlag.de
Karen Reetz-Resch, Home Office: 08121-9775-94, reetz@it-verlag.de
Marion Mann, +49 152-3634 1255, mann@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.

JETZT DEN NÄCHSTEN
KARRIERESCHRITT GEHEN
– MIT DER **JOBBÖRSE** VON

it-daily.net

JETZT
ENTDECKEN!

itsa

HOME OF IT SECURITY

Jetzt mehr erfahren!

7. – 9. Oktober 2025
Nürnberg, Germany
itsa365.de/itsa-expo-besuchen

NÜRNBERG MESSE

it security

Detect. Protect. Respond.
Juli/August 2025

THOUGHT LEADERSHIP

AB SEITE 8

SOPHOS

CYBERSICHERHEIT

Real Security for the Real World

Michael Haas, WatchGuard Technologies GmbH

Haben Sie etwa eine Ausgabe der itmanagement und itsecurity

verpasst?

...mit einem Abo wäre das nicht passiert.

Trends von heute und morgen sowie Fachartikel und Analysen renommierter Branchenexperten: Die Fachmagazine IT Management und IT Security bieten einen fundierten Einblick in verschiedene Bereiche der Enterprise IT.

ZUM ABO

it-daily.net/leser-service

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

Inhalt

COVERSTORY

THOUGHT LEADERSHIP

IT SECURITY

Real Security for the Real World

MIT LEISTUNGSSTARKEM SCHUTZ DEN TATSÄCHLICHEN ANFORDERUNGEN BEGEGNEN

Cybersicherheit zählt heute zu den größten Herausforderungen für Unternehmen aller Größen – angesichts wachsender Bedrohungen, regulatorischer Vorgaben und technischer Komplexität. Was können Anwender gegen die Bedrohungen tun? Michael Haas, Vice President Central Europe bei WatchGuard, im Gespräch mit Ulrich Parthier, Publisher it security.

Ulrich Parthier: *Immer neue Angriffsvektoren, komplexe Tools, Zeit- und Personalmangel – was raten Sie Anwendern im Umgang mit dieser zunehmenden Komplexität?*

Michael Haas: Der wichtigste Rat ist wohl: Ruhe bewahren. Es geht darum, die Situation für das eigene Unternehmen objektiv zu analysieren und dann entsprechend individuell zu priorisieren. Die Basics sollten in jedem Fall stehen. Dabei ist es gerade im KMU-Umfeld entscheidend, den Herausforderungen möglichst einfache und praktikable Lösungen entgegenzusetzen, die den Bedürfnissen der Anwender entsprechen. Genau hier treffen wir unter dem Motto „Real Security for the Real World" einen wichtigen Nerv.

Ulrich Parthier: *Was verbirgt sich dahinter konkret?*

Michael Haas: Wie schon angesprochen, muss das Sicherheitskonzept den tatsächlichen Bedarf des jeweiligen Unternehmens adäquat abbilden. Die größten Schwachstellen und Nöte können sich von Organisation zu Organisation unterscheiden. Wir sehen unsere Aufgabe als Hersteller nicht darin, Anwendern „fancy" Produkte zu verkaufen, sondern wollen Lösungen bieten, die die tatsächlichen Anforderungen abdecken. Gerade in Zeiten von Kaufzurückhaltung ist ein solcher Ansatz wichtig. Es kommt dabei auf Präzision und Leistungsstärke an, mit Konzentration auf das Wesentliche. Überflüssige Technologien braucht keiner. Die Lösungen müssen sich dem täglichen Betrieb anpassen und nicht umgekehrt – insbesondere im Mittelstand. Zudem geht es um Nähe und persönliche Ansprechpartner. Wir und unsere Partner sind da, wenn es drauf ankommt.

Ulrich Parthier: *Im Markt sprießen gleichzeitig konsequent neue Produkte wie Pilze aus dem Boden. Wie bewerten Sie diese Entwicklung?*

Michael Haas: Ich bin immer wieder begeistert vom Ideenreichtum der zahlreichen Startups, die mit neuen Konzepten vorstoßen. Technologisch ist das meist „cutting edge", aber leider handelt es sich bei den Lösungen in der Regel um Silos, die nur mit großem Aufwand implementiert und gewartet werden können. Kleinere und mittlere Unternehmen sind kaum in der Lage, diesen Aufwand in Kauf und Betrieb zu stemmen, für sie zählt vielmehr Zeit- und Kostenersparnis. Hier punkten Plattform-Lösungen, die auf maximale Integration ausgelegt sind und dadurch nicht zuletzt das Fundament für gezielte Managed Services liefern. So lässt sich jederzeit sicherstellen, dass Security-Funktionen nicht oversized sind. WatchGuard bietet gemeinsam mit den Partnern ein flexibles Portfolio – von klein bis groß. Im Idealfall muss sich der Kunde um gar nichts kümmern, die MSPs übernehmen die Integration und zentrale Verwaltung. Damit kann sich der Anwender voll und ganz auf seinen Betrieb konzentrieren und gewiss sein, dass seine Geschäftswerte rund um die Uhr abgesichert sind.

Ulrich Parthier: *Welche Cyberbedrohungen bereiten Ihnen derzeit die größten Sorgen? Zero Trust, KI und Deepfakes sind drei Themenaspekte, die man immer wieder im Zusammenhang mit Bedrohungsszenarien hört. Was raten Sie den Anwendern?*

Michael Haas: Leider ist der Mensch nach wie vor die größte Schwachstelle und daher gilt es mehr denn je, in Security Awareness und Schulungen zu investieren. Zero Trust liefert in dem Zusammenhang einen wichtigen techni-

ALS PIONIER BEIM UTM-KONZEPT HABEN WIR DIE ZUSAMMENFÜHRUNG UND OPTIMALE KONFIGURATION VIELFÄLTIGER SICHERHEITSFUNKTIONALITÄT QUASI IN DER DNA.

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

schen Ansatz, um die Sicherheit zu generalisieren und damit in jeder Umgebung auf höchstem Niveau zu halten. Nichtsdestotrotz müssen wir Menschen als Anwender wachsam sein und bleiben. Die Bedrohungslage entwickelt sich rasend schnell weiter und sollte daher konsequent beobachtet werden. Neue Angriffstrends, Technologien, aber auch Plattformen müssen immer wieder kritisch hinterfragt werden. Das bedeutet ein stetiges Abwägen, was nützlich ist und was nicht, was dabei hilft, Zeit und Ressourcen zu sparen oder diese unnötig auffrisst.

? **Ulrich Parthier:** *Wo sehen Sie die größten Cybersecurity-Herausforderungen der nächsten zwei Jahre?*

Michael Haas: Das Stichwort KI ist bereits gefallen, hieran finden Angreifer zunehmend mehr Gefallen, aber auch Ransomware und Datenlecks werden uns weiterhin zu schaffen machen. Im Zuge von Cloud-Konzepten und Remote-Arbeit stößt der klassische Perimeterschutz an klare Grenzen, insofern werden SASE-Lösungen im Mittelstand ebenfalls immer bedeutsamer. Vor diesem Hintergrund macht mir etwas anderes aber viel mehr Sorgen: In Zeiten von kleinen Budgets wird häufig bei vermeintlich nicht-produktiven Systemen eingespart, was leider auch oft das Thema IT-Security betrifft. Angesichts der steigenden Anforderungen kann dies einigen Unternehmen schwer auf die Füße fallen.

? **Ulrich Parthier:** *Wie lässt sich diese Lücke schließen und welche Rolle spielt dabei KI in den Reihen der Verteidigung?*

Michael Haas: Durch KI werden gerade auch Managed Services immer weiter aufgewertet. Zugleich können diese zu Kosten angeboten werden, die nicht mehr jenseits der Realität von KMU liegen. Bei WatchGuard setzen wir bereits seit vielen Jahren auf KI-Technologie, die dabei unterstützt, Abwehrmaßnahmen schnell und effizient umzusetzen. Gerade im SOC spielt die künstliche Intelligenz klare Stärken aus, von denen Unternehmen im Zuge von Dienstleistungsmodellen maximal profitieren.

? **Ulrich Parthier:** *Das klingt, als wären für Sie Managed Security Services der Königsweg für den Mittelstand?*

Michael Haas: Aus meiner Sicht ist es sogar der einzige Weg für den Mittelstand. Der Siegeszug von KI – sowohl auf der Angreifer- als auch der Abwehrseite – ist dabei ein perfekter Aufhänger. Dieses Thema hat vor zwei Jahren in diesem Umfang noch gar nicht existiert. Und das passiert immer wieder: Neue Technologien kommen hinzu und der einzelne IT-Leiter oder ein kleines Team auf Unternehmensseite ist gar nicht in der Lage, damit konsequent Schritt zu halten. Genau an diesem Punkt schaffen Managed Service Provider überzeugenden Mehrwert, indem sie – nicht zuletzt vor dem Hintergrund neuer gesetzlicher Bestimmungen wie NIS2 oder DORA – am Puls der Zeit bleiben und den Schutz dank ganz anderer, professioneller Möglichkeiten aufrechterhalten, und zwar rund um die Uhr. Exakt dafür ist die WatchGuard Unified Security Platform konzipiert.

? **Ulrich Parthier:** *Diese verspricht höhere Effizienz und Skalierbarkeit – welche technologischen Innovationen stecken konkret dahinter?*

Michael Haas: Als Pionier beim UTM-Konzept haben wir die Zusammenführung und optimale Konfiguration vielfältiger Sicherheitsfunktionalität quasi in der DNA. Unsere Plattformstrategie geht darüber weit hinaus und erstreckt sich über zahlreiche Bereiche – vom Perimeterschutz über Endpoint Security und sicheres WLAN bis hin zur Authentifizierung. Hinzu kommen die weitreichenden MDR- und XDR-Möglichkeiten. Durch das stringente Zusammenwirken und die Korrelation der auf der Plattform zusammenfließenden Daten ergibt sich zum einen ein stichhaltiges Lagebild und volle Übersicht. Gleichzeitig sorgt die Integration von Machine Learning und KI für bestmögliche Unterstützung der Prozesse. All diese Leistungen lassen sich optimal in flexible und leicht zugängliche Managed Services packen, die exakt auf die Bedürfnisse mittelständischer Unternehmen abzielen und mit neuen Anforderungen mitwachsen können. Die Absicherung hybrider Infrastrukturen bereitet damit beispielsweise schon heute keine Probleme. Dies unterstreicht exakt unsere Zielstellung „Real Security for the Real World" und macht uns für immer mehr Unternehmen und Managed Service Provider zum idealen Partner, wenn es darum geht, Wirtschaftlichkeit und Leistungsstärke bei der Gefahrenabwehr unter einen Hut zu bekommen.

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

Das Methodensystem für Projekte

FINDEN SIE DIE PASSENDE METHODE FÜR IHR PROJEKTMANAGEMENT

Wir wünschen uns alle einen Werkzeugkasten, mit dem wir unsere Projekte erfolgreicher gestalten können. Die Autoren Christian Botta und Bernhard Schloß haben daher ihre eigenen Trainings ausgewertet und ein System mit 132 Projektmanagement-Methoden entwickelt. Die grafische Übersicht erinnert an das Periodensystem aus der Chemie und soll eine Orientierung im Methodendschungel geben.

Jede einzelne Methode, jedes Werkzeug und jedes Framework wird beschrieben und nach den Kriterien Aufwand, Schwierigkeit und Wirksamkeit bewertet. Zusätzlich gibt es noch Tipps und Tricks für den optimalen Einsatz sowie Hinweise auf verwandte Methoden.

Mit dem Methodensystem für Projekte finden Sie genau das passende Tool für Ihr Projekt!

Aus dem Inhalt:

- Willkommen im Dschungel der Projektmanagement- Methoden
- Planung & Steuerung
- Team & Umwelt
- Anforderungen
- Qualität & Risiko
- Projektmanagement-Konzepte
- Libraries & Frameworks
- Modelle
- Methoden-Finder

Das Methodensystem für Projekte – Finden Sie die passende Methode für Ihr Projektmanagement; Bernhard Schloß, Christian Botta; Carl Hanser Verlag GmbH & Co.KG; 06-2025

CYBERCRIME ALS GESCHÄFTSMODELL

Die moderne Cyberkriminalität hat sich zu einem hochprofessionalisierten Geschäftszweig entwickelt, der weit über spontane Einzelaktionen hinausgeht. Diese neue Generation von Cyberkriminellen operiert mit klaren Unternehmensstrukturen, Marketingstrategien und einem ausgeprägten Geschäftsverständnis. Sie nutzen legale Infrastrukturen für illegale Zwecke und verwischen dabei bewusst die Grenzen zwischen kriminellen Aktivitäten und regulären Geschäftstätigkeiten.

Für IT-Sicherheitsverantwortliche bedeutet diese Entwicklung einen fundamentalen Paradigmenwechsel: Der Schutz vor Cyberbedrohungen erfordert nicht nur technische, sondern auch wirtschaftliche Expertise, um die komplexen Strukturen dieser professionalisierten Schattenökonomie erfolgreich zu bekämpfen.

Vom Kriminellen zum Kaufmann

WIE CYBERGANGSTER DENKEN, INVESTIEREN UND EXPANDIEREN

Moderne Cyberkriminelle lassen die Grenze zwischen digitaler Kriminalität und klassischer Geschäftstätigkeit zunehmend verschwimmen. Auf Basis einschlägiger Forendiskussionen, Dienstleistungsangebote und realwirtschaftlicher Spuren hat das Team von Sophos X-Ops verfolgt, wie die Bedrohungsakteure von der Monetarisierung über die Geldwäsche bis zur Reinvestition wirtschaftlich agieren. Die digitalen Täter beweisen dabei eine hohe kaufmännische Raffinesse.

Wer steckt dahinter? Täterbilder der neuen Schattenökonomie

Die untersuchten Daten deuten auf eine heterogene, aber hochgradig ökonomisierte Szene hin. Viele geben sich als Freelancer, Entwickler, Projektmanager oder Marketingexperten aus. Einige betreiben reale Firmen – teils zur Geldwäsche, teils als Teilzeitgeschäft. Die Cybergangster agieren geografisch verteilt, arbeitsteilig, rollenbasiert und mit klarer Aufgabenteilung (Entwicklung, operativer Bereich, Vertrieb). Das Selbstverständnis ist dabei oft das eines Geschäftsmanns, nicht eines Kriminellen. Viele orientieren sich an Start-up-Ideen – nur ohne ethische oder regulatorische Grenzen.

Professionalisierung als Geschäftsmodell

In den einschlägigen Foren findet sich eine beachtliche Bandbreite an Aktivitäten – von der Entwicklung und Vermarktung neuer Malware-Tools über DDoS-as-a-Service-Angebote bis hin zu strategischer Investitionsberatung unter Kriminellen selbst. Geld, das aus Betrug oder Erpressung stammt, wird oft reinvestiert. So schreibt ein Nutzer etwa: „Investiere es in das Business, das dir das Geld gebracht hat. Ist doch logisch."

BEI KRIMINELLEN ÖKOSYSTEMEN HANDELT ES SICH NICHT UM CHAOTISCHE PARALLELWELTEN, SONDERN UM PROFESSIONELL STRUKTURIERTE, GLOBAL VERNETZTE SYSTEME.

Michael Veit, Security Evangelist, Sophos, www.sophos.com

Vier zentrale Geschäftsmodelle lassen sich identifizieren:

1. Digitale Geschäftsmodelle im Cybercrime
2. Umwandlung und Nutzung realer Gewinne
3. Investitionen in halblegale Graubereiche
4. Reinvestition in illegale Geschäfte

#1 Digitale Geschäftsmodelle

E-Commerce und Dienstleitung, Skalierbarkeit und Automatisierung, Markenbildung und Partnerprogramm

Die Cybercrime-Ökonomie ist hochgradig strukturiert, arbeitsteilig und auf Wachstum ausgelegt. Wo früher spontane Einzelaktionen dominierten, finden sich heute skalierbare Geschäftsmodelle mit Support, Wiederverwendbarkeit und klarer Nutzerzentrierung.

Angriffswerkzeuge wie Stealer, Phishing-Kits oder Botnet-Frameworks werden als Malware-as-a-Service (MaaS) in abonnementbasierten Modellen angeboten. Kunden erhalten nicht nur fertige Tools, sondern auch Dashboards mit Echtzeit-Statistiken – inklusive Geodaten, Infektionsraten und Umsatzmetriken.

Ein Forennutzer bringt es auf den Punkt: „Wer nicht misst, kann nicht wachsen."

Viele Gruppen orientieren sich am klassischen E-Commerce: Helpdesks, Ticket-Systeme und sogar Live-Chats für Erpressungsopfer gehören zur Grundausstattung. Technische Dokumentationen, Schritt-für-Schritt-Zahlungsanleitungen und FAQ-Bereiche sorgen für niedrigere Abbruchraten. Rabatte, Countdown-Timer und Gütesiegel wirken als psychologische Trigger.

Ein anderer Beitrag merkt an: „Conversions erhöhen sich um 30 Prozent, wenn du zeigst, dass du erreichbar bist."

Die Szene denkt in KPIs, Branding und User Experience – wie legale Tech-Start-ups, nur im kriminellen Kontext. Vertrauenssiegel, „Partnerprogramme" und Kundenbewertungen dienen zur Differenzierung. Manche Gruppen nutzen Corporate Design, eigene Logos und Social-Media-artige Kanäle zur Imagepflege. Selbst Empfehlungsmarketing und Reputationsbewertungen sind etabliert.

#2 Umwandlung und Nutzung realer Gewinne

Mixer, Mules, Luxus und Haustiere: Geldwäsche und Investitionen mit Bedacht

Cybercrime endet nicht mit dem digitalen Diebstahl, im Gegenteil, er beginnt oft erst dort. Die Konvertierung von Kryptowährungen in reale Vermögenswerte erfordert durchdachte Strategien zur Anonymisierung und Legitimierung.

Krypto-Mixer, Tumbler und Prepaid-Karten dienen zur Verschleierung von Transaktionen. Täter greifen aber auch auf regulierte Plattformen wie Binance oder PayPal zurück – häufig über gefälschte oder gemietete Identitäten. Geldkuriere („Mules") und Briefkastenfirmen übernehmen die finale Distribution. In einigen Fällen entwickeln Gruppen sogar eigene Tools zur Geldwäsche, um externe Abhängigkeiten zu vermeiden.

Die Gewinne werden häufig in langlebige, transportable Güter überführt: Uhren, Autos, Technik oder Designerstücke dienen als Wertspeicher. Auch Immobilieninvestitionen – vor allem in Russland, Südostasien oder auf dem Balkan – sind gängige Praxis, meist über Strohleute oder Offshore-Konstrukte. Sogar NFT(Non-Fungible Token)-Kunst – also digitale Kunstwerke, auf der Blockchain als nicht austauschbare Eigentumszertifikate gesichert – sowie teure Rassehunde tauchen in Diskussionen als Kapitalanlage auf.

Auch hier finden sich Logos, CI-konforme Oberflächen sowie Ratings, „Trust-Levels" und Kundenbewertungen, und es existieren Empfehlungsprogramme und Partnermodelle.

Viele Täter zeigen sich dabei erstaunlich diszipliniert: Statt dekadenter Ausgaben setzen sie auf unauffälligen Konsum und langfristige Wertstabilität.

#3 Investitionen in halblegale Graubereiche

Expansion in die Grauzone, Legalisierung durch Nebel

Brisant ist die zunehmende Verlagerung in halb-legale Geschäftsmodelle. Hier reinvestieren Täter ihre Gewinne in Aktivitäten, die auf den ersten Blick legal erscheinen, tatsächlich aber aus dem Schatten finanziert werden – und für Ermittlungsbehörden schwer greifbar sind. Dazu zählen der Handel mit Spionagesoftware, etwa über vorgeschobene Pentesting-Firmen, der Betrieb von Webcam-Studios und pornografischen Plattformen, teils mit ausbeuterischen Strukturen, sowie der Verkauf von Traffic, SEO-Diensten und Affiliate-Klicks. Auch Online-Glücksspiel, P2P-Wetten auf Blockchain-Basis, Pharmahandel ohne Zulassung und sogenannte Residency-for-Crypto-Programme fallen in dieses Spektrum.

Diese Formen der wirtschaftlichen Schattenintegration nutzen bewusst juristische Nebelfelder, Offshore-Jurisdiktionen, regulierte Dienstleister (wie Zahlungsabwickler oder Domainanbieter) und verschachtelte Firmenkonstruktionen, um das kriminelle Fundament zu verschleiern. So entsteht ein Ökosystem, das zunehmend professionell, arbeitsteilig und regulatorisch entkoppelt operiert. Die Trennung zwischen digitalem Verbrechen und realwirtschaftlicher Nutzung löst sich damit weiter auf.

#4 Reinvestition in illegale Geschäfte

Illegale Geschäfte mit System: Betrug, Bestechung, Sexarbeit, Fälschungen, Drogen

Cyberkriminelle sprechen in den Foren offen von ihren „schwarzen Projekten" – also Geschäftsmodellen, die illegal, halblegal oder bewusst schwer zu verfolgen sind. Dabei reicht das Spektrum von digitalen Betrugsmaschen bis hin zu Geschäftsmodellen mit realem Fußabdruck in der physischen Welt.

Der klassische Betrug umfasst etwa Rückerstattungstricks bei bekannten Online-Händlern, Fake-Anzeigen auf Plattformen wie Avito oder die Erstellung synthetischer Identitäten mithilfe sogenannter CPNs (Credit Privacy Numbers). Auch Pyramidenspiele mit angeblich lukrativen Renditen auf Basis von Kryptowährungen (etwa USDT) werden aktiv beworben. Der Bereich Fälschungen reicht von nachgemachtem Gold bis hin zu vermeintlich antiken Artefakten, die über private Kanäle vertrieben werden sollen.

Darüber hinaus dokumentieren die Foren strukturelle Vorhaben: Escort-Agenturen mit geplanten Bestechungsmaßnahmen, Bordellkonzepte mit „hoher Rendite" oder Cannabisplantagen, die detailliert in Businessplänen inklusive Break-Even-Kalkulation vorgestellt werden. Parallel dazu werden Anleitungen zur Steuerhinterziehung oder Geldwäsche geteilt, darunter auch Hinweise, wie etwa in Kanada, wo angebliche Einnahmen aus Sexarbeit zur Legalisierung illegaler Gelder dienen könnten. Diskutiert wird auch der gezielte Einsatz geleakter Unternehmensdaten für Insiderhandel, etwa durch das Platzieren von Put-Optionen vor einem Ransomware-Angriff.

Verstörend sind zudem Berichte über Falschgeld in hoher Druckqualität oder sogar über den Einsatz von Scopolamin („Wahrheitsserum") zur Einschüchterung und Ausraubung von Opfern.

Die kriminelle Logik hinter dem Business

Was alle beschriebenen Aktivitäten eint, ist eine grundlegend unternehmerische Logik. In Diskussionen geht es um Zielgruppen, Kostenoptimierung, Risikominimierung, Expansion – genau wie in der legalen Startup-Welt. Selbst „Exit-Strategien" werden erörtert, etwa durch den Wechsel in vermeintlich legale Geschäftsfelder oder durch die Einrichtung komplexer Geldwäschestrukturen. Eine nüchterne Stimme aus einem Forum bringt es auf den Punkt:

„Cybercrime ist ein Markt. Wer schlau investiert, gewinnt."

Cybercrime verstehen heißt Wirtschaft verstehen

Die Analyse krimineller Ökosysteme offenbart daher ein überraschend klares Bild: Es handelt sich nicht um chaotische Parallelwelten, sondern um professionell strukturierte, global vernetzte Systeme. Cybercrime funktioniert nach ökonomischen Prinzipien – mit skalierbaren Geschäftsmodellen, KPI-orientierter Steuerung und wachstumsgetriebenem Denken. Die Täter agieren dabei nicht außerhalb des Systems, sondern nutzen legale Infrastrukturen – Finanzdienste, Hosting, Social Media – auf eine Weise, für die sie nie gedacht waren, die aber umso wirkungsvoller ist.

Für Sicherheitsverantwortliche und Ermittlungsbehörden ergibt sich daraus ein Paradigmenwechsel: Threat Intelligence muss um wirtschaftliche Perspektiven erweitert werden – etwa durch Analysen zur Wertschöpfungskette krimineller Gruppen oder zur Kapitalverwendung. Strafverfolgung und Compliance sollten enger verzahnt agieren, um regulatorische Schlupflöcher systematisch zu schließen. Und nicht zuletzt gilt: Technischer Schutz allein greift zu kurz, wenn sich Täter zunehmend im Schatten legaler Infrastrukturen bewegen. Denn auch, wenn ein Unternehmen legal erscheint, können dahinter einzelne Bedrohungsakteure oder ganze Gruppen stecken – die mit dem legal verdienten Geld erneut Cybercrime begehen.

Michael Veit

KI IN DER CYBERSECURITY: HYPE ODER ALLHEILMITTEL?

SO SETZEN SIE KI OPTIMAL UND SICHER ZUR STÄRKUNG IHRER CYBERABWEHR EIN

Das Thema KI erfährt in der Cybersicherheit aktuell viel Aufmerksamkeit. Unternehmen werden mit verlockenden Versprechungen einer KI-gestützten Transformation der Cybersecurity geradezu bombardiert: mehr Schutz, niedrigere Kosten, ein geringerer Bedarf an Fachkräften. Gleichzeitig wird davor gewarnt, dass KI eine völlig neue Ära von Cyberangriffen einläuten wird.

Dieser Leitfaden soll Unternehmen dabei helfen, den Hype und die Missverständnisse rund um KI in der Cybersicherheit besser einzuschätzen. Sie erfahren, was KI leistet (und was nicht), um die Cyberabwehr in Unternehmen zu optimieren, und welche Risiken KI für Cybersicherheit und Betriebsabläufe mit sich bringt. Dazu erhalten Sie Tipps, wie Sie mögliche Gefahren minimieren und so die Vorteile von KI sicher nutzen können, um sowohl Ihren Cyberschutz als auch Ihren Return on Investment zu verbessern.

Zudem liefert der Guide Einblicke in die Praxis: Wie sieht die KI-Nutzung in der Realität aus? Welche Erwartungen und Bedenken bestehen? Die Erkenntnisse hierzu beruhen auf den Ergebnissen einer unabhängigen, Ende 2024 durchgeführten Befragung von 400 IT-/Cybersecurity-Entscheidern. Diese direkten Erfahrungsberichte bieten eine wertvolle Orientierungshilfe für Unternehmen, die über Einsatzmöglichkeiten von KI nachdenken.

WHITEPAPER DOWNLOAD

Das Whitepaper umfasst 14 Seiten und steht kostenlos zum Downloadbereit.

www.it-daily.net/download

IT-SICHERHEIT HEUTE UND MORGEN

ZWISCHEN NEUEN BEDROHUNGEN UND ALTEN INSELLÖSUNGEN

Die digitale Transformation verändert nicht nur die Arbeitsweise von Unternehmen grundlegend, sondern treibt auch die Entwicklung neuer Technologien voran. Gleichzeitig eröffnet sie jedoch eine Fülle an Schwachstellen, die Cyberkriminelle gezielt ausnutzen. Mit der Zunahme von Cloud-Lösungen, Remote-Arbeitsmodellen und einer immer komplexeren IT-Infrastruktur sehen sich Unternehmen mit einer eskalierenden Bedrohungslage konfrontiert. Gleichzeitig reagiert die Gesetzgebung hierauf mit einer erschöpfenden Anzahl an Regularien. Gemeinsam facht diese Entwicklung die dringende Notwendigkeit an, Sicherheitsstrategien zu überdenken und neu auszurichten.

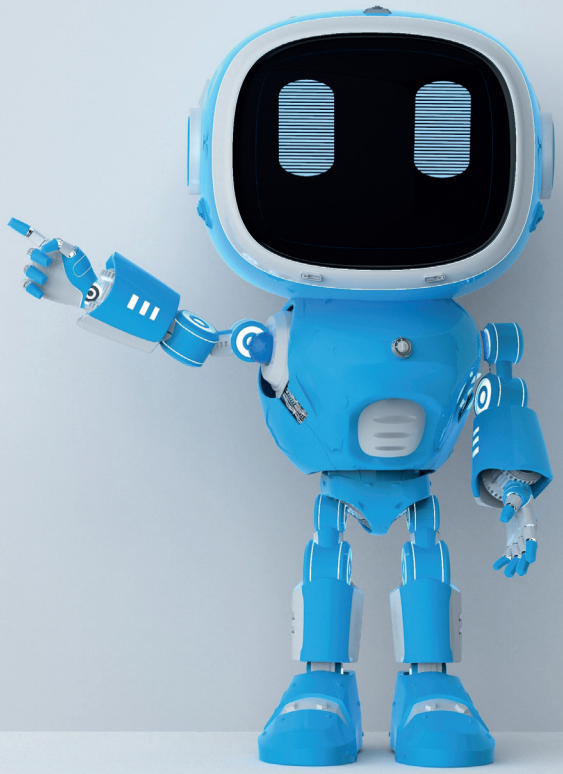
Die folgende Studie beschäftigt sich daher mit folgenden Fragestellungen:

- Welche Maßnahmen gehören zu einer effektiven IT-Sicherheitsstrategie?
- Wie sollten Sie Budgets planen und priorisieren?

Im Fokus stehen integrierte Plattformlösungen, die als Antwort auf die Herausforderungen isolierter Security-Tools gelten.

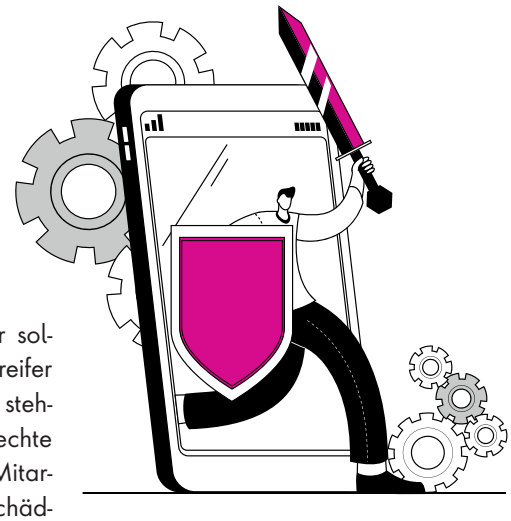
STUDIEN DOWNLOAD

Die Studie umfasst 13 Seiten und steht kostenlos zum Download bereit.
www.it-daily.net/download



Einfallstor Smartphone

SO SCHÜTZEN UNTERNEHMEN DIE KOMMUNIKATION



Ob ein Videocall per Smartphone oder eine schnelle Chatnachricht an eine wichtige Kundin: Immer mehr Unternehmen in Deutschland setzen bei der Zusammenarbeit auf digitale Prozesse per Smartphone und Tablet. Das ist ein Ergebnis des Digital Office Index 2024 des Digitalverbands Bitkom. Doch der Einsatz der mobilen Geräte birgt auch Gefahren. Denn durch ausgefeilte Betrugsmethoden wie Phishing-Nachrichten oder Cyberangriffe attackieren Hacker gezielt Unternehmen, um wertvolle Daten zu entwenden oder Lösegelder zu erpressen. Ein erhöhtes Risiko besteht für Unternehmen etwa dann, wenn Mitarbeitende unbeabsichtigt im Smartphone-Browser eine Webseite mit betrügerischen Inhalten aufrufen. Über solche Einfallstore können die Angreifer sensible Daten manipulieren und stehlen. Aber auch durch täuschend echte Phishing-Mails oder -SMS sollen Mitarbeitende dazu verleitet werden, schädliche Links zu öffnen oder vertrauliche Informationen preiszugeben.

Mehr Cyberangriffe auf kleine und mittlere Unternehmen

Wie akut die Gefahr eines wirtschaftlichen Schadens durch einen Cyberangriff ist, zeigt die Bitkom-Studie „Wirtschaftsschutz 2024". Laut der Untersuchung waren im vergangenen Jahr 74 Prozent der befragten Unternehmen von Datendiebstahl betroffen. Der Gesamtschaden in Deutschland durch Cybercrime betrug 178,6 Milliarden Euro – eine Steigerung um mehr als 20 Prozent im Vergleich zu 2023. Der aktuelle Lagebericht zur IT-Sicherheit in Deutschland des Bundesamtes für Sicherheit in der Informationstechnik (BSI) warnt zudem, dass vor allem kleine und mittelständische Unternehmen (KMU) anfällig für Angriffe sind, da sie häufig nicht über entsprechende Sicherheitslösungen verfügen.

Cybersicherheit als kostenlose Kernleistung

Eine neue Lösung der Telekom unterstützt Unternehmen jetzt dabei, sicher im Mobilfunknetz unterwegs zu sein. Denn die Mobilfunktarife der Telekom für Geschäftskunden enthalten die kostenlos integrierte Sicherheitsoption Security OnNet Basic. Das Security-Feature ist direkt im Mobilfunknetz der Telekom verankert und erkennt Bedrohungen im mobilen Internet. Es blockiert den Zugang zu betrügerischen Webseiten durch das unbeabsichtigte Anklicken von Phishing-Links, unterbindet Cyberattacken durch mit Malware infizierte, ferngesteuerte Bots und verhindert den Zugriff auf unzureichend gesicherte Webseiten.

Die Tarife sorgen dafür, dass Kunden keine zusätzliche, kostenpflichtige App herunterladen müssen, um ihre mobile Kommunikation zu schützen. Darüber hinaus haben die Betriebe auch keinen Mehraufwand bei der Verwaltung der Security-Option.

Roaming-Angebot und Partnerkarten

Je nach Tarif erhalten Unternehmen pro Nutzer entweder 30 GB, 50 GB oder unbegrenztes Datenvolumen im 5G-Mobilfunknetz der Telekom. In allen Business Mobiltarifen ist das Roaming in der EU, dem Vereinigten Königreich und der Schweiz inbegriffen. Neben einer Hauptkarte haben Betriebe die Möglichkeit, weitere Businesscards für bis zu sechs Teammitglieder zu ordern und sparen dabei bis zu 70 Prozent der Kosten.

https://telekom.de

ALLE VORTEILE AUF EINEN BLICK

Keine Extrakosten: Security OnNet Basic ist kostenlos in allen neuen Tarifen enthalten und schützt vor Bedrohungen im Mobilfunknetz der Telekom.
Direkter Schutz: Ohne zusätzliche App, unmittelbar im Telekom Mobilfunknetz integriert.
Datenvolumen: Tarife bieten 30 GB (S), 50 GB (M) oder unbegrenztes Datenvolumen (L und XL) im 5G-Netz.
Roaming: EU, UK und Schweiz inklusive, weltweit 1 GB Welcome Pass für 48 Stunden.
Partnerkarten: Bestellung von bis zu sechs zusätzlichen Businesscards möglich. Kostenersparnis ab der zweiten Karte.

MEHR WERT
Handytarife für Geschäftskunden

Datensicherheit in Microsoft 365

SENSIBLE DATEN HABEN IM TEAMS-CHAT NICHTS VERLOREN

Microsoft 365 ist aus vielen Unternehmen nicht mehr wegzudenken. Für vertrauliche Informationen birgt die Anwendungs-Suite aus der Cloud aber zahlreiche Risiken. Mit einem Cloud Access Security Broker können Unternehmen für umfassende Datensicherheit sorgen.

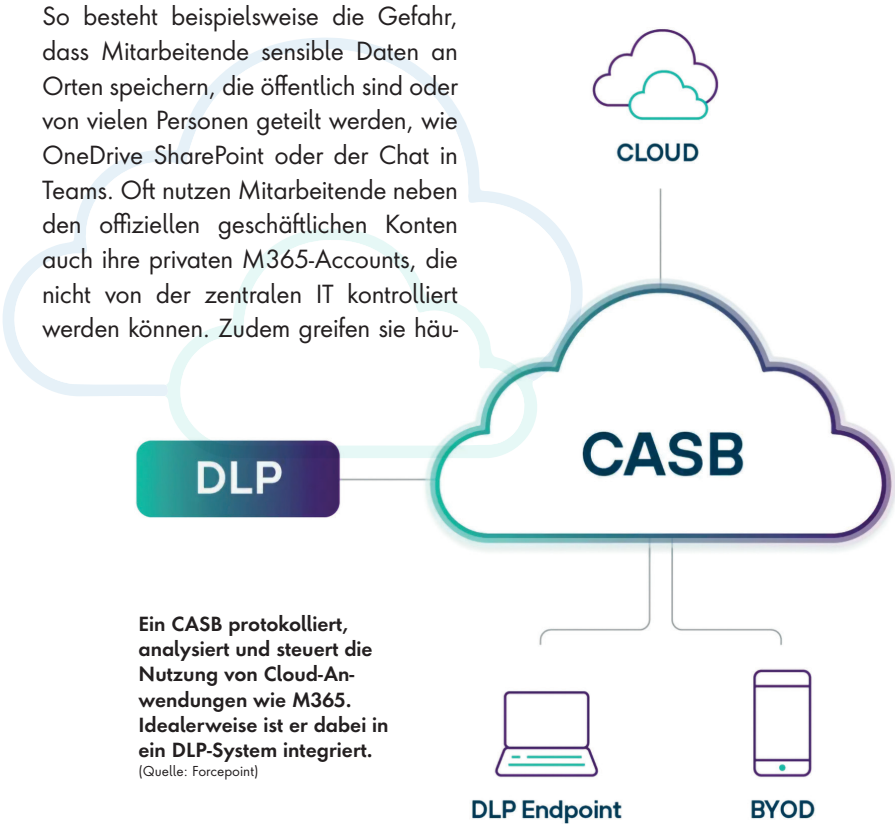
Microsoft 365 (M365) ist heute der Quasi-Standard für digitale Arbeitsumgebungen. Die cloudbasierte Suite mit ihren Produktivitäts- und Kollaborations-Anwendungen ist aus vielen Unternehmen nicht mehr wegzudenken. IT-Security-Teams stellt M365 aber vor große Herausforderungen, denn es birgt zahlreiche Risiken für Datensicherheit und Compliance.

So besteht beispielsweise die Gefahr, dass Mitarbeitende sensible Daten an Orten speichern, die öffentlich sind oder von vielen Personen geteilt werden, wie OneDrive SharePoint oder der Chat in Teams. Oft nutzen Mitarbeitende neben den offiziellen geschäftlichen Konten auch ihre privaten M365-Accounts, die nicht von der zentralen IT kontrolliert werden können. Zudem greifen sie häufig von ungemanagten BYOD-Geräten aus auf M365 zu und laden sogar Daten auf diese Geräte herunter.

Ein ähnliches Problem besteht bei externen Parteien wie Zulieferern, Partnern und Dienstleistern. Die Endgeräte, mit denen sie sich verbinden, werden ebenfalls nicht von der Haus-eigenen IT verwaltet. Nicht zuletzt gibt es natürlich auch das Risiko, dass böswillige Akteure Kontrolle über Unternehmenskonten in M365 erlangen und sensible Daten exfiltrieren oder Daten löschen, verschlüsseln und manipulieren.

Ein CASB überwacht, steuert und sichert die Zugriffe

Diese Herausforderungen können IT-Security-Teams mithilfe eines Cloud Access Security Broker (CASB) meistern. Ein solches Tool wird zwischen M365 und die Endnutzer geschaltet, um den Zugriff auf die Anwendungen der Suite zu überwachen, zu steuern und abzusichern. Diese Zwischenschaltung erfolgt auf drei unterschiedlichen Wegen: per API-Integration, Forward Proxy und Reverse Proxy.



Ein CASB protokolliert, analysiert und steuert die Nutzung von Cloud-Anwendungen wie M365. Idealerweise ist er dabei in ein DLP-System integriert.
(Quelle: Forcepoint)

Bei der API-Integration dockt der CASB über ein Application Programming Interface direkt an M365 an und erhält über diese Schnittstelle Informationen über die verbundenen Anwender und ihr Verhalten. Zur Analyse des Datenverkehrs zwischen M365 und den Endnutzern werden zudem zentrale Gateways eingebunden. Ein Forward Proxy überwacht und steuert dabei den Zugriff von Endgeräten auf M365 und nutzt dazu Software-Agenten, die auf den Devices installiert sind. Ein Reverse Proxy wiederum kontrolliert den Traffic in Richtung der Endgeräte, wofür er keine Software-Agenten benötigt.

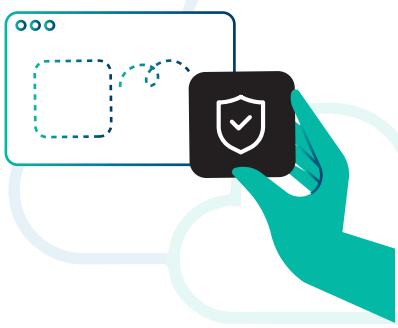
Ruhende Daten und Datenübertragungen schützen

Ein moderner CASB kombiniert alle drei Methoden (API, Forward Proxy, Reverse Proxy) und ermöglicht damit um-

fassende Datensicherheit in M365. IT-Security-Teams können:

• **Ruhende Daten schützen:** Teams erhalten Transparenz über die Daten, die in M365 gespeichert sind und können Maßnahmen für den Schutz sensibler Informationen ergreifen. Sie haben die Möglichkeit, alle ruhenden Daten zu scannen und dabei vertrauliche Informationen zu identifizieren und Freigaben in SharePoint oder OneDrive zu entdecken, die gegen die Sicherheitsrichtlinien des Unternehmens verstoßen. Identifiziert der CASB offengelegte sensible Informationen schützt er sie automatisiert durch Verschlüsselung oder Verschiebung in Quarantäne. Darüber hinaus erkennt der CASB auch verdächtiges Nutzungsverhalten wie ungewöhnlich viele Downloads oder die Anmeldung eines Nutzers aus einem Land, aus dem er sich bisher noch nie angemeldet hatte. In solchen Fällen setzt er automatisch Warnmeldungen ab.

• **Datenübertragungen absichern:** Um die Exfiltration sensibler Daten über Outlook, SharePoint, OneDrive und Teams zu verhindern, führt ein CASB in Echtzeit DLP-Inspektionen (Data Loss Prevention) durch und ergreift, wenn erforderlich, Schutzmaßnahmen. Er blockiert beispielsweise die Übertragung von Daten an SharePoint oder maskiert in Echtzeit Informationen in Teams-Chats. Beim Herunterladen von Dateien verschlüsselt er sie mithilfe eines Digital Right Managements (DRM) und stellt damit sicher, dass sie nicht auf unautorisierten Geräten entschlüsselt werden können. Dadurch schützt er sensible Informationen auch in nachgelagerten Offline-Szenarien. Unberechtigte Personen können sie nicht öffnen, kopieren und drucken.



EIN MODERNER CASB KOMBINIERT API, FORWARD PROXY, REVERSE PROXY UND ERMÖGLICHT DAMIT UMFASSENDE DATENSICHERHEIT IN M365.

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

• **Ungemanagte Geräte einbinden:** Ein CASB bietet auch zahlreiche Features, um Zugriffe von Endgeräten abzusichern, die nicht von der Haus-eigenen IT verwaltet werden. So erkennt und blockiert er beispielsweise verdächtige Aktivitäten wie wiederholte Anmeldeversuche. Außerdem bewertet er kontinuierlich den Sicherheitsstatus der Endgeräte und prüft beispielsweise, ob ihr Betriebssystem auf einem aktuellen Stand ist oder ob auf ihnen eine Anti-Malware-Software ausgeführt wird. Zudem haben Administratoren die Möglichkeit, Uploads zu und Downloads von M365 auf ungemanagte Geräte zu unterbinden. Damit ermöglicht der CASB sichere Zugriffe mit den BYOD-Geräten von Mitarbeitenden und den Devices von Partnern oder Dienstleistern.

• **Schadsoftware abwehren:** Ein guter CASB bringt integrierte Anti-Malware-Engines mit, um Dateien, die in M365 hochgeladen werden, auf Schadsoftware zu untersuchen und Dateien, die dort gespeichert sind, zu scannen. Durch die Integration von Drittanbieterlösungen ermöglicht er außerdem erweiterten Anti-Malware-Support und unterstützt die Erkennung von Zero-Day-Bedrohungen durch Sandboxing. Für den Austausch von Bedrohungsinformationen ist er zudem nahtlos in gängige SIEM-Lösungen wie Splunk und IBM QRadar integrierbar und kann über REST-APIs Daten in SIEM- und SOAR-Lösungen exportieren.

Ganzheitliche Datensicherheit

Wenn Unternehmen ein DLP-System für die Datensicherheit in ihren lokalen Umgebungen im Einsatz haben, sollte der CASB möglichst eng mit diesem System integriert sein. Dann können die Unternehmen ihre lokalen DLP-Vorgaben mit nur wenigen Klicks auf die M365-Anwendungen ausweiten. Sämtliche Richtlinien, Richtlinienvorlagen und Datenklassifizierer sind dann ohne aufwändige Migrationen sofort im CASB verfügbar. Einheitliche Richtlinien über On-Premises und M365 hinweg reduzieren zudem Lücken im Schutzniveau und minimieren das Risiko von Fehlkonfigurationen. Dadurch gewährleistet die DLP-CASB-Integration eine ganzheitliche Datensicherheit über beide Welten hinweg.

Fabian Glöser

IDENTITY & ACCESS MANAGEMENT

VON STATISCHEN ZU DYNAMISCHEN SICHERHEITSMODELLEN

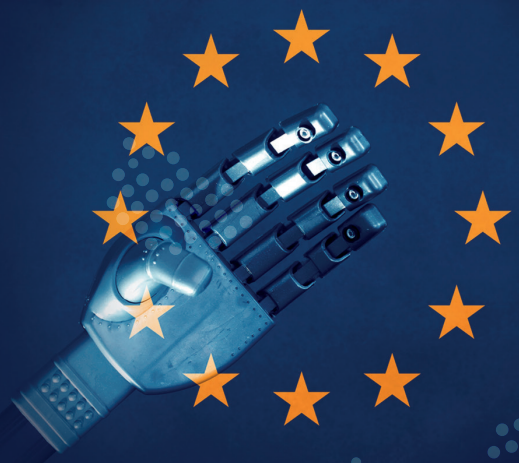
Für 2025 zeichnet sich eine fundamentale Neuausrichtung des IAM-Bereichs ab. Der Fokus verschiebt sich von statischen zu dynamischen Sicherheitsmodellen, die kontinuierliche Überwachung und Anpassung ermöglichen. Organisationen müssen ihre IAM-Strategien entsprechend anpassen, um mit dieser Entwicklung Schritt zu halten.

Die Integration von KI, Zero-Trust-Architekturen und passwortloser Authentifizierung wird nicht mehr optional, sondern notwendig sein, um den steigenden Sicherheitsanforderungen gerecht zu werden. Besonders die Verbindung von IAM mit Cybersecurity-Disziplinen und die Einbindung neuer Technologien wie GenAI werden die Entwicklung in den kommenden Jahren prägen.

Unser neues eBook liefert praktische Insights für ein zukunftsfähiges Identity & Access Management.

Wir zeigen, wie Unternehmen ihre IT-Sicherheit zukunftssicher gestalten, denn das moderne Identitäts- und Zugriffsmanagement (IAM) muss sich den wachsenden Bedrohungen anpassen.

Das eBook umfasst 38 Seiten und steht kostenlos zum Download bereit.
www.it-daily.net/download



Digitale Souveränität

WARUM DER EU AI ACT JETZT WICHTIG IST

Die künstliche Intelligenz erlebt derzeit einen beispiellosen Aufstieg. Plötzlich schreibt KI Texte, generiert Bilder oder analysiert komplexe Daten – für uns alle erstaunlich leicht zugänglich. Doch während viele die Vorteile nutzen möchten, offenbart sich gleichzeitig eine geopolitische Dimension: Die Abhängigkeit von internationalen Tech-Konzernen und deren Ausrichtung nach den Interessen ihrer Heimatländer.

Geopolitische Herausforderungen bei KI-Nutzung

Schon früher gerieten US-Technologiekonzerne häufig unter Druck der Regierung in Loyalitätskonflikte. Für europäische Unternehmen stellt sich daher die Frage: Wer hat tatsächlich Kontrolle über die eigenen Daten, wenn diese durch KI-Systeme verarbeitet werden?

Die Veränderung der weltweiten politischen Landschaft lässt die europäische KI-Regulierung in neuem Licht erscheinen. Was vielfach als „typisch europäische Überregulierung" kritisiert wurde, erhält plötzlich den Charakter eines strategischen Schutzwalls.

Der amerikanische „Move fast and break things"-Ansatz kollidiert mit dem europäischen Vorsorgeprinzip. Der EU AI Act stellt klare Regeln für KI-Systeme auf und klassifiziert sie nach ihrem Risikoniveau. Damit schafft er einen verbindlichen Rahmen, der die Interessen der Nutzer schützt und für Hersteller Rechtssicherheit erhöht.

EU AI Act als Wettbewerbsvorteil

Für Unternehmen bedeutet die Compliance mit dem EU AI Act nicht nur eine rechtliche Notwendigkeit, sondern ein Differenzierungsmerkmal im Wettbewerb. Die Einhaltung europäischer Datenschutzstandards wird zum Qualitätsmerkmal.

IN ZEITEN WACHSENDER GEOPOLITISCHER SPANNUNGEN GEWINNT DER EU AI ACT AN BEDEUTUNG FÜR DIGITALE SOUVERÄNITÄT UND VERBRAUCHERSCHUTZ.

Sebastian von Bomhard, Vorstand, SpaceNet AG, www.space.net

Bedenken hinsichtlich technologischer Abhängigkeit verstärken den Wert datenschutzkonformer europäischer Alternativen. Während internationale Tech-Giganten ihre Dienste an die Anforderungen ausländischer Regierungen anpassen müssen, behalten Unternehmen mit europäischen Technologie-Anbietern die volle Kontrolle über ihre Daten.

Der EU AI Act bietet die Chance, europäische Werte in die KI-Entwicklung zu integrieren und gleichzeitig Innovation zu fördern. Die Regulierung könnte langfristig zum Vorteil werden, da sie Vertrauen stärkt und die Akzeptanz von KI-Lösungen erhöht.

Kosten und Nutzen im Überblick

Die Implementierung wird für Unternehmen mit Mehraufwand verbunden sein. Die Kosten für Compliance-Maßnahmen können jedoch gegen die langfristigen Vorteile abgewogen werden:

- Erhöhtes Vertrauen der Nutzer
- Rechtssicherheit für Entwickler
- Reduzierung von Haftungsrisiken
- Strategischer Vorteil im geopolitischen Kontext

Was zunächst als Wettbewerbsnachteil erscheint, entpuppt sich im aktuellen geopolitischen Kontext als strategischer Vorteil. Der EU AI Act ist ein Baustein europäischer digitaler Souveränität.

In einer Zeit, in der Vertrauen in Technologieanbieter fundamentale Bedeutung erlangt, bietet die konsequente Umsetzung europäischer Standards einen Wettbewerbsvorteil, der weit über reine Compliance hinausgeht. Für Kunden bedeutet dies die Gewissheit, dass ihre Daten nicht zum Spielball fremder Interessen werden.

Sebastian von Bomhard

SpaceNet

IT und OT wachsen zusammen

NIS2 VERÄNDERT SECURITY-STRATEGIEN IN UNTERNEHMEN

In einer zunehmend geopolitisch angespannten Welt wächst der Druck auf Unternehmen und staatliche Einrichtungen, ihre digitalen Infrastrukturen resilient und souverän abzusichern. Wer IT-Security heute strategisch denkt, setzt auf integrierte Schutzkonzepte, geprüfte Infrastruktur und Partner, die Sicherheit nicht nur technisch, sondern als Vertrauensversprechen verstehen.

Die Bedrohungslage für Unternehmen hat sich in den vergangenen Jahren dramatisch verschärft. Sie ist geprägt von hoher Dynamik, wachsender Komplexität und systemischer Tiefe. Gleichzeitig verändert sich die Motivation hinter den Attacken auf IT-Infrastrukturen: Zielten Angriffe in der Vergangenheit primär auf den finanziellen Gewinn ab, so stehen heute vermehrt auch politische und geopolitische Beweggründe im Vordergrund. Staatlich unterstützte Cyberangriffe, hochentwickelte Advanced Persistent Threats (APTs), gezielte Attacken auf kritische Lieferketten und Einrichtungen der kritischen Infrastruktur (KRITIS) – all das verdeutlicht, dass klassische Schutzkonzepte nicht mehr ausreichen.

NIS2 braucht strukturelle Ansätze

Mit Regelwerken wie der überarbeiteten NIS2-Richtlinie und dem Digital Operational Resilience Act (DORA) will deshalb auch die EU neue verbindliche Standards setzen, um für mehr Klarheit und Verlässlichkeit im Umgang mit digitalen Risiken zu sorgen. Konkret stellt NIS2 eine konsequente Weiterentwicklung der bisherigen NIS-Richtlinie dar. Ziel ist es, die Cybersicherheit in der EU sektorübergreifend zu stärken. In diesem Zusammenhang erweitert die überarbeitete Richtlinie nicht nur den Kreis der betroffenen Unternehmen erheblich, sondern definiert auch deutlich konkretere Anforderungen an technische und organisatorische Sicherheitsmaßnahmen. Hinzu kommen strengere Pflichten zur Meldung von Sicherheitsvorfällen, höhere Anforderungen an das Risikomanagement und eine stärkere persönliche Haftung von Unternehmensleitungen.

Für viele Organisationen bedeuten diese Tatsachen einen Paradigmenwechsel: Cybersicherheit darf spätestens jetzt nicht mehr als technische Randdisziplin behandelt, sondern muss als strategisches Element der Unternehmensführung mit klar definierten Verantwortlichkeiten verstanden werden. Die Umsetzung dieser Zielsetzungen erfordert allerdings ein Umdenken in Organisationen, nämlich, dass Cybersicherheit ganzheitlich gedacht werden muss.

KLASSISCHE GRENZEN ZWISCHEN IT UND OPERATIVEN TECHNOLOGIEN (OT) DÜRFEN NICHT LÄNGER BESTEHEN BLEIBEN.

Stefan Tiefel,
Senior Market Development Manager Security & Network, noris network AG, www.noris.de

IT und OT wachsen zusammen

In anderen Worten: Klassische Grenzen zwischen IT und operativen Technologien (OT) dürfen nicht länger bestehen bleiben. Die zunehmende Vernetzung industrieller Systeme mit der IT-Infrastruktur macht es notwendig, auch in bislang vernachlässigten Unternehmensbereichen wie der Produktion, im Gebäudemanagement oder in Versorgungseinrichtungen einheitliche Sicherheitsstandards zu etablieren. Insbesondere ältere OT-Systeme, die für lange Laufzeiten konzipiert wurden, sind häufig nicht auf heutige Bedrohungsszenarien ausgelegt.

Eine weitere typische Baustelle für das erfolgreiche Zusammenwachsen von IT und OT ist der häufig fehlende strategische Stellenwert von IT-Sicherheit im Management. Zwar steigt das Bewusstsein, dass Cyberrisiken geschäftskritisch sein können, doch fehlt es vielerorts noch an strukturellen Konsequenzen. Sicherheitsstrategien werden nicht systematisch in digitale Transformationsprojekte eingebunden, sondern häufig parallel dazu betrieben.

Cybersicherheit entfaltet ihre volle Wirkung allerdings nur dann, wenn sie als integraler Bestandteil von Innovationsprozessen verstanden wird – von der Planung über die Umsetzung bis zur Nachsorge. Und nicht zuletzt braucht es stärkere Kooperationen, über Unternehmens- und Branchengrenzen hinweg. Viele der heutigen Bedrohungen sind so komplex, dass sie nicht mehr

isoliert abgewehrt werden können. Damit wird der intensive Austausch zwischen Organisationen, Behörden, CERTs und Forschungseinrichtungen zum zentralen Bestandteil einer modernen, resilienten Sicherheitsarchitektur.

Notwendig sind darüber hinaus klare Prozesse, ein zentrales Asset-Management, Transparenz über eingesetzte Komponenten sowie automatisierte Verfahren zur Schwachstellenbewertung. Nur wer jederzeit den Überblick über seinen digitalen Bestand hat, kann Risiken realistisch einschätzen und ihnen wirksam begegnen. Um diesen regulatorischen Rahmen wirksam zu füllen, braucht es freilich mehr als technische Lösungen: ganzheitliche, strukturelle Ansätze, Transparenz, interdisziplinäre Zusammenarbeit – und ein Sicherheitsverständnis, das über reine Compliance hinausgeht und echte Resilienz zum Ziel hat.

Blinde Flecken durch Fachkräftemangel

Ein wesentliches Hindernis ist neben der Security-Governance und der Verantwortungskultur der anhaltende Mangel an qualifizierten IT-Sicherheitsfachkräften. IT-Verantwortliche sehen sich zunehmend mit der Einhaltung neuer wie bestehender regulatorischer Anforderungen konfrontiert – was in vielen Fällen die Umsetzung operativer Sicherheitsmaßnahmen erschwert.

Um dieser Herausforderung zu begegnen, setzen Unternehmen verstärkt auf externe Unterstützung bei sicherheitsrelevanten Aufgaben. Dabei kommt es jedoch entscheidend darauf an, dass zentrale Funktionen wie Angriffserkennung oder Schwachstellenmanagement eng mit dem internen Sicherheitsökosystem verzahnt bleiben. Andernfalls drohen systemische „blinde Flecken", in denen Bedrohungen unerkannt bleiben können.

Sicherheit im ganzheitlichen Kontext

Diese Risiken steigen zusätzlich mit der zunehmenden Verlagerung von Anwendungen und Workloads in hybride und Multi-Cloud-Umgebungen. Denn: So flexibel diese Modelle auch sind – sie erschweren eine konsistente Umsetzung von Sicherheitsrichtlinien über Systemgrenzen hinweg. Besonders herausfordernd ist dies bei verteilten Systemen außerhalb automatisierter Patch-Prozesse, die ohne gezielte Sicherheitsstrategien potenzielle Einfallstore darstellen können.

Eine Situation, in der hochsichere Rechenzentrumsarchitekturen gemeinsam mit eng integrierten, lokal oder hybrid betriebenen Security Operations zunehmend als souveräne Alternative zu internationalen Hyperscalern wahrgenommen werden – insbesondere im Hinblick auf europäische Datenschutzanforderungen und regulatorische Vorgaben. Doch IT-Sicherheit endet nicht am Rand des Rechenzentrums. Organisationen erwarten zunehmend passgenaue Sicherheitslösungen entlang ihrer gesamten Infrastruktur, von der Cloud bis zum Edge. Das umfasst die Härtung industrieller Systeme, die Integration von Zero-Trust-Architekturen und eine effektive Incident Response durch regional verankerte und reaktionsfähige Teams. Vor allem der Betrieb von Security Operations mit starker lokaler Anbindung – etwa aus Deutschland – gewinnt an strategischer Bedeutung. Nicht nur aus rechtlicher Sicht, sondern auch im Hinblick auf Vertrauen, Fachkompetenz und die Fähigkeit zur schnellen, kontextbezogenen Reaktion. Wer Cybersicherheit heute strategisch denkt, setzt auf integrierte Schutzkonzepte, transparente Prozesse und auf Partner, die Sicherheit nicht nur technisch, sondern auch organisatorisch und kulturell verstehen und leben.

Stefan Tiefel

NIS2-Referentenentwurf

KLEINE ÄNDERUNGEN MIT GROSSEN AUSWIRKUNGEN

Erneut wurde ein Referentenentwurf zum „Entwurf eines Gesetzes zur Umsetzung der NIS2-Richtlinie und zur Regelung wesentlicher Grundzüge des Informationssicherheitsmanagements in der Bundesverwaltung" vorgelegt – dieses Mal datiert auf den 2. Juni 2025, womit sich der Entwurfsstand in der ministeriellen Abstimmung befindet.

Und die Änderungen sind durchaus interessant, denn sie betreffen nicht nur Fragen der Zusammenarbeit zwischen BSI und BBK, sondern auch Aktualisierungen im Hinblick auf den Anwendungsbereich. Insgesamt erhalten BSI und BMI einen Befugnisaufwuchs, sollten die Änderungen wie vorgeschlagen umgesetzt werden.

Anwendungsbereich und Entlastungen für die Wirtschaft

Insbesondere im Hinblick auf den Anwendungsbereich wurde aus der Wirtschaft regelmäßig kritisiert, dass vor allem auch Nebentätigkeiten durch die zahlenmäßige Berücksichtigung der Gesamt-Konzerninfrastruktur in den Anwendungsbereich von NIS2 fallen – mit der Folge erheblicher wirtschaftlicher Belastungen. Nun wird im Entwurf der Vorschlag gemacht, solche Geschäftstätigkeiten unberücksichtigt bleiben zu lassen, die im Hinblick auf die gesamte Geschäftstätigkeit der Einrichtung vernachlässigbar sind. Damit soll im Einzelfall vermieden werden, dass eine nur geringfügige Nebentätigkeit zu einer unverhältnismäßigen Identifizierung als wichtige oder besonders wichtige Einrichtung führt.

Darüber hinaus gibt es auch im Bereich der Bundesverwaltung mehrere Neuerungen, insbesondere betreffend die Vorgaben zur Cybersicherheit und die Rolle des BSI. So wird einerseits die behördenübergreifende Unterstützerrolle ausgebaut, ebenso wird der begrüßenswerte Hinweis aufgenommen, dass der IT-Grundschutz für die Einrichtungen der Bundesverwaltung mittelbar Gesetzesrang erhält. Dass Cybersecurity auch im Bund fach- und ressortübergreifendes Thema ist, wird insbesondere deutlich durch die Erweiterung der Rolle der Informationssicherheitsbeauftragten, denen ebenso die Aufgabe zukommt, die Geheimschutzbeauftragten zu unterstützen und zu beraten. Insgesamt kommt dem BMI in dem Entwurf eine deutlich herausgehobene fachliche Stellung zu.

ZWAR WIRD WIE ZU ERWARTEN WIEDER NUR AN EINZELNEN STELLSCHRAUBEN GEDREHT, WENN DIE ÄNDERUNGEN ABER WIE VORGESCHLAGEN KOMMEN, SIND DIE AUSWIRKUNGEN NICHT UNERHEBLICH.

Prof. Dr. Dennis-Kenji Kipker, cyberintelligence.institute, www.cyberintelligence.institute

Neuordnung der Behördenzuständigkeiten

Doch auch im Zusammenspiel zwischen den einzelnen Fachbehörden werden Änderungen angestrebt – so unter anderem im Hinblick auf das Verhältnis BSI und BNetzA für die IT-Sicherheit im Anlagen- und Netzbetrieb. So wird eine Konsolidierung der bisherigen Zuständigkeiten von BNetzA und BSI im Hinblick auf konventionelle und digitale Dienstleister im Sektor Energie vorgeschlagen. Hintergrund: Die Aufsicht über KRITIS-Betreiber im Sektor Strom hinsichtlich der Einhaltung von Cybersicherheitsmaßnahmen oblag bislang hauptsächlich der BNetzA. Ausgenommen waren lediglich „Anlagen oder Systeme zur Steuerung/Bündelung elektrischer Leistung" (etwa virtuelle Kraftwerke), für die die Aufsicht beim BSI lag. Die abstrakten Cybersicherheitsvorgaben des EnWG wurden dabei durch Sicherheitskataloge der BNetzA – im Benehmen mit dem BSI – konkretisiert.

Über die nunmehr vorgesehene Einvernehmensregelung soll das BSI größeren Einfluss auf die IT-Sicherheitsanforderungen im Sektor Energie erhalten. Das BSI soll dadurch in die Lage versetzt werden, ein einheitliches Sicherheitsniveau über alle KRITIS-Sektoren hinweg sicherzustellen. Dadurch dürfte das BSI in seiner Rolle als zentrale Cybersicherheitsbehörde nicht unerheblich gestärkt werden – zumal es ebenso für die zukünftige nationale Umsetzung des EU Cyber Resilience Act (CRA) mandatiert wird.

Last but not least werden Änderungen bei der Ermächtigung zum Erlass von Rechtsverordnungen vorgeschlagen. Durch ebenjene Rechtsverordnungen wird die Anwendung des BSIG schon jetzt konkretisiert – so unter anderem auch im Hinblick auf den Anwendungsbereich mit der BSI-KritisV. Für letztgenannte wird das Festlegungsverfahren deutlich verändert, indem nach dem Entwurf nun keine Anhörung von Wissenschaftsvertretern, der betroffenen Betreiber und der betroffenen Wirtschaftsverbände erforderlich ist. Eine ganz ähnliche Einschränkung findet sich in der Bestimmung von Vorgaben, wann ein erheblicher Sicherheitsvorfall vorliegt – auch hier sollen künftig die Wirtschaftsverbände und die Wissenschaft ausgeschlossen werden.

Fazit

Zwar wird wie zu erwarten wieder nur an einzelnen Stellschrauben gedreht, wenn die Änderungen aber wie vorgeschlagen kommen, sind die Auswirkungen nicht unerheblich. Dies betrifft sowohl den Bereich der Public Private Partnerships, die interbehördliche Zusammenarbeit in der Cybersicherheit, die Stärkung der Cybersicherheit in der Bundesverwaltung, die Erleichterungen im Anwendungsbereich sowie daneben die Rolle des BMI und vor allem des BSI, das teils über die Befugnisse von NIS2 hinausgehend eine weitere deutliche Stärkung erfährt.

Prof. Dr. Dennis-Kenji Kipker

Cyberrisiken: Handeln statt Hoffen

10 ANZEICHEN, DASS IHR VULNERABILITY MANAGEMENT STRUKTURELLE LÜCKEN AUFWEIST

VULNERABILITY MANAGEMENT IST MEHR ALS EIN SCAN, ES IST EINE DISZIPLIN.

Patrick Schäfers,
Head of Security Projects,
Arvato Systems,
www.arvato-systems.de

Cyberangriffe sind längst kein Ausnahmefall mehr – sie gehören zum Alltag nahezu jeder Branche. Viele Unternehmen sind überzeugt, in Sachen IT-Security gut aufgestellt zu sein. Doch wenn der Ernstfall eintritt, zeigt sich oft: Die eigentlichen Schwachstellen liegen nicht in fehlender Technologie, sondern in nicht gelebten Prozessen. Aktuelle Studien zeigen: Es dauert im Schnitt 137 Tage, bis eine bekannte Schwachstelle geschlossen wird. Angreifer hingegen benötigen im Zweifel nur 5 Tage für eine erfolgreiche Ausnutzung. Wer auf Einzelmaßnahmen oder Tools ohne durchgängige Abläufe setzt, riskiert mehr als Sicherheitslücken: Reputationsverluste, Betriebsunterbrechungen und regulatorische Konsequenzen sind reale Folgen.

Die folgenden zehn Indikatoren zeigen, wo im Schwachstellenmanagement besonders häufig strukturelle Defizite auftreten, und was Unternehmen tun können, um sie zu beheben. Besonders wichtig dabei: Die Rolle des Vulnerability Managers – nicht als Tool-Anwender, sondern als gestaltende Instanz im Spannungsfeld von Technik, Governance und Umsetzung.

#1 Schwachstellen bleiben monatelang unbearbeitet.

Wenn Schwachstellen über längere Zeit bestehen bleiben, obwohl sie bekannt sind, fehlt häufig ein klar strukturierter Prozess zur Bewertung und Behebung. Solche „Langläufer" entstehen durch mangelnde Priorisierung, fehlende Verantwortlichkeiten oder unzureichende Tool-Integration. Ein zentrales Vulnerability Management mit automatisierter Bewertung, verbindlichen Fristen und Nachverfolgung schafft hier Abhilfe – vorausgesetzt, es wird prozessual verankert und aktiv gesteuert.

#2 Serverprozesse sind nicht auf Effizienz und Sicherheit ausgelegt.

Server sind das Rückgrat der IT, doch viele Prozesse dort sind historisch gewachsen und schlecht synchronisiert. Das erhöht die Wahrscheinlichkeit von Fehlkonfigurationen und verzögert die Reaktion auf Schwachstellen. Wer regelmäßige Reviews zu Systemhärtung, Rechtevergabe und Patch-Routinen durchführt, schafft nicht nur mehr Sicherheit, sondern auch mehr Stabilität – und reduziert die operative Last langfristig.

#3 Das Patchmanagement weist systematische Lücken auf.

Patchmanagement ist kein technisches Thema, sondern ein organisatorisches. Immer wieder scheitert es daran, dass Systeme nicht vollständig eingebunden, Zuständigkeiten unklar oder Prozesse zu langwierig sind. Es braucht automatisierte Patchprozesse mit regelmäßiger Berichterstattung, sauberer Dokumentation und klaren Regeln für Ausnahmen. Hier wird sichtbar: Ein funktionierender Prozess entsteht nicht durch das Tool allein – sondern durch klare Verantwortung und Governance.

#4 Die Systeminventarisierung ist unvollständig.

Nur was bekannt ist, lässt sich schützen. Ohne vollständige und aktuelle Übersicht über Assets, Applikationen und Endpoints bleiben Risiken unerkannt. Automatisierte Lösungen zur Erfassung und Korrelation mit Schwachstellendaten sind unverzichtbar, doch auch hier gilt: Die beste Technik wirkt nur, wenn ein Prozess dahintersteht.

IT-SA 2025

Auf der diesjährigen it-sa steht Arvato Systems den Event-Teilnehmenden innerhalb der Bitkom Security Area (Halle 7A-416) gern persönlich Rede und Antwort rund um Vulnerability Management und andere Security-Themen.

#5 Änderungen und Audits lassen sich nicht nachvollziehen.

Dokumentation ist mehr als ein Compliance-Thema – sie ist ein zentraler Bestandteil resilienter Prozesse. Ob KRITIS, NIS2, DORA oder das IT-Sicherheitsgesetz: Alle fordern lückenlose Nachweise über sicherheitsrelevante Änderungen. Wer Patch- und Assetdaten nicht strukturiert verknüpft, läuft Gefahr, im Auditfall nicht nachweisen zu können, wann welche Risiken behandelt wurden.

#6 Interne Abläufe bremsen die Schwachstellenbehebung aus.

Nicht selten liegt die Ursache für unbearbeitete Schwachstellen in der Organisation selbst: Fehlende Abstimmung zwischen Fachbereichen, manuelle Schnittstellen oder unklare Eskalationswege verzögern die Umsetzung. Ein wirksames Vulnerability Management ist immer auch Change Management – mit definierten Rollen, klaren Zuständigkeiten und regelmäßigen Prozess-Reviews.

#7 Dienstleister erhalten nicht die relevanten Informationen.

In vielen Fällen übernehmen externe Partner Aufgaben im Schwachstellenmanagement, doch ohne gezielten Informationsaustausch entstehen Verzögerungen und Missverständnisse. Wichtig ist ein rollenbasiertes Export-Management, das nur die Daten bereitstellt, die der jeweilige Dienstleister benötigt – strukturiert, aktuell und nachvollziehbar.

#8 Die Prozesse sind nicht durchgängig dokumentiert.

Ein professionelles Schwachstellenmanagement endet nicht beim Scan. Es umfasst die gesamte Kette: von der Identifikation über die Bewertung und Umsetzung bis zur Verifikation. Ohne dokumentierten End-to-End-Prozess entsteht schnell Intransparenz und Verantwortung diffundiert. Struktur ersetzt hier nicht den Menschen, aber sie gibt ihm die Werkzeuge, um wirksam zu handeln.

#9 Erfolg wird nicht gemessen.

Ohne Messbarkeit bleibt jede Verbesserung zufällig. Wer nicht weiß, wie lange eine Behebung dauert oder wie viele Schwachstellen pro Quartal geschlossen wurden, kann den eigenen Fortschritt nicht bewerten, geschweige denn steuern. Kennzahlen wie MTTR (Mean Time to Remediate), offene Schwachstellen pro System oder Schließrate pro Monat sollten in jedem Dashboard sichtbar sein.

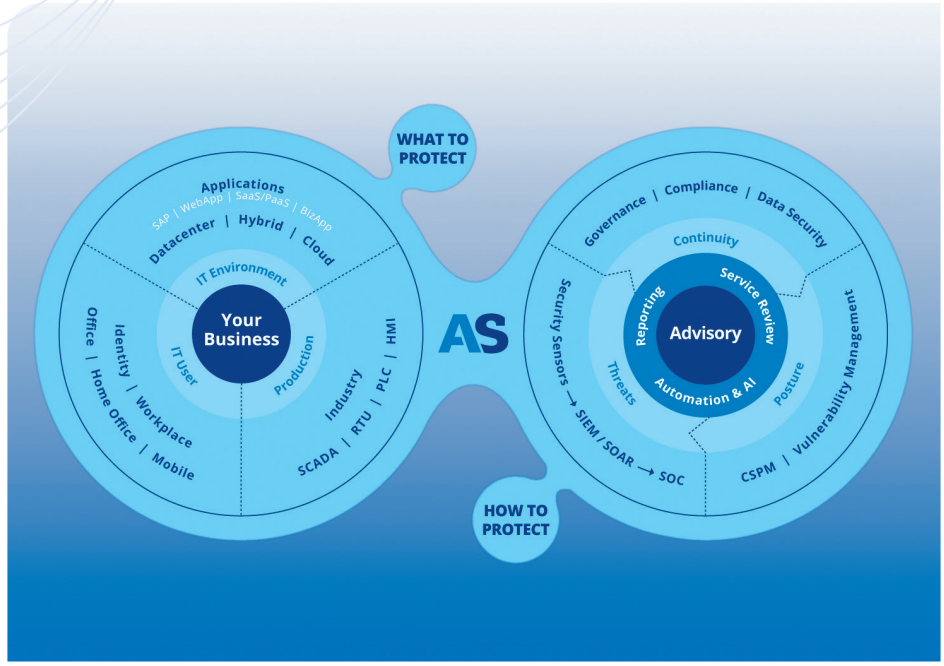
#10 Prozesse werden nicht an neue Bedrohungen angepasst.

Die Bedrohungslage entwickelt sich ständig weiter und damit auch die Anforderungen an ein dynamisches Schwachstellenmanagement. Wer seine Abläufe nicht regelmäßig überprüft und anpasst, verliert den Anschluss. Quartalsweise Reviews, die Einbindung von Zero-Day-Lagen und regulatorischen Änderungen sowie der Einsatz von externen Spezialisten zur Ergänzung interner Ressourcen sind essenziell.

Fazit: Kein Tool ersetzt ein starkes Prozessfundament.

Viele Organisationen setzen auf technische Lösungen und übersehen dabei die wichtigste Stellschraube: den Prozess. Vulnerability Management ist mehr als ein Scan, es ist eine Disziplin. Es braucht Verantwortlichkeit, strukturierte Abläufe, messbare Ergebnisse und einen Vulnerability Manager, der diese Disziplin professionell steuert. Wenn Sie sich in mehreren der Punkte wiedererkennen, ist das ein Signal, dass Handlungsbedarf besteht. Jetzt ist der richtige Zeitpunkt, Ihre Prozesse zu justieren und das Steuer zu übernehmen. Denn in der IT-Security zählt nicht, ob ein Angriff kommt – sondern, wie gut Sie vorbereitet sind.

Patrick Schäfers



UNTER CYBER-BESCHUSS

JEDER DRITTE ANGRIFF TRIFFT PRODUKTIONSUNTERNEHMEN

Das Cyber Security Team der Var Group, Yarix, hat die Cyberangriffe auf deutsche Unternehmen und Organisationen aus dem Jahr 2024 analysiert. Die Analyse führte das Yarix Cyber Threat Intelligence (Yarix CTI) Team durch.

Die größte Bedrohung

Das Yarix CTI-Team ordnete die beobachteten Angriffe im Rahmen seiner Analyse sechs Hauptkategorien zu: Die meisten (36,4 %) entfielen auf DDoS und Web-Defacement. Auch Ransomware-Angriffe waren für deutsche Unternehmen und Organisationen 2024 ein großes Problem: 27,7 Prozent der beobachteten Attacken lassen sich dieser Kategorie zuordnen. Die 2024 gegen Unternehmen in Deutschland geltend gemachten Ransomware-Angriffe machten unter den 118 analysierten Ländern 2,88 Prozent aller vom Yarix CTI-Team erfassten Ereignisse dieser Art aus. Damit war Deutschland 2024 unter den Top 5-Ländern, die am stärksten von Ransomware-Ereignissen betroffenen waren.

Im Fokus von Ransomware-Attacken

Ransomware-Angriffe betrafen mit Abstand am stärksten die Fertigungsindustrie (30,2 %). Dahinter folgen Consulting (11,8 %), IT (8,1 %) und das Baugewerbe (8,1 %).

Mit Ransomware-Angriffen hatten zudem vor allem kleine Unternehmen mit 11 bis 100 Mitarbeitenden (55,2 %) zu kämpfen. An zweiter Stelle folgen mittlere Unternehmen mit 101 bis 500 Mitarbeitenden (25,0 %), an dritter Stelle „Enterprise"-Unternehmen mit mehr als 1001 Mitarbeitenden (11,1 %).

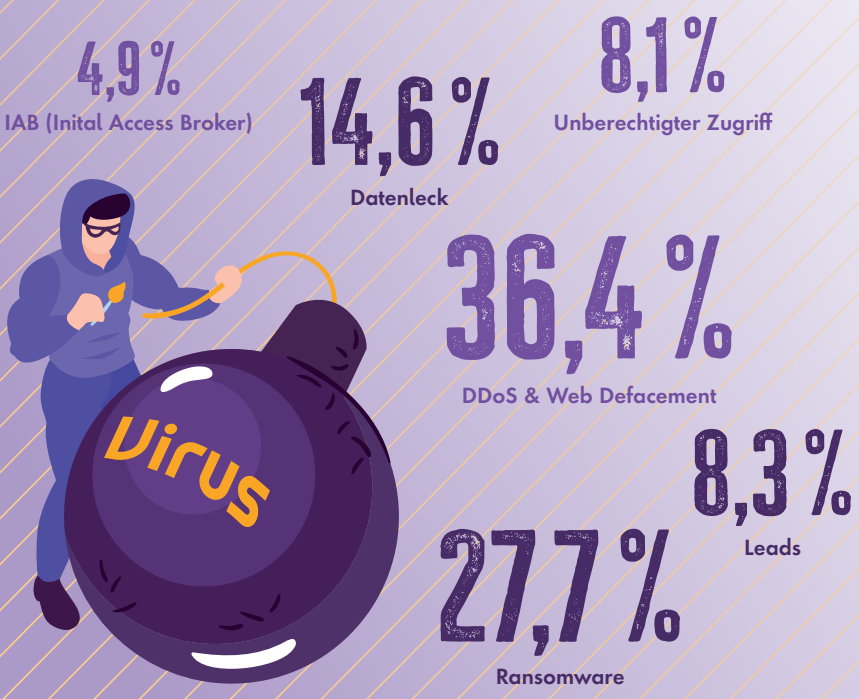
Spitze der Cyberangriffe im November und Dezember

Mit Blick auf die Zeitachse der im Jahresverlauf insgesamt registrierten Angriffe stellte das YCTI-Team eine schwankende Verteilung der beobachteten Bedrohungen über die meisten Monate des Jahres mit einer deutlichen Spitze im November und Dezember 2024 fest. DDoS- und Web-Defacement-Angriffe konzentrierten sich auf bestimmte Monate, die mit außenpolitischen Initiativen der deutschen Regierung im geopolitischen Kontext des Jahres 2024 korrespondieren. Dazu zählen beispielsweise die Unterstützung für die Ukraine und Israel. Darüber hinaus wurden auch während wichtiger innenpolitischer Ereignisse und Proteste, etwa den Protesten der deutschen Landwirte im Januar, Spitzenwerte bei solchen Angriffen verzeichnet.

Ein weiterer Grund für den Anstieg am Ende des Jahres ist die umsatzstarke Phase von Einzelhandel und E-Commerce vor Weihnachten.

www.vargroup.de

ANGRIFFE NACH BEDROHUNGSKATEGORIE



MEHR WERT

Länderbericht zur Cyberbedrohungslandschaft: Deutschland

Wenn Firewalls nicht mehr reichen

DATA-CENTRIC SECURITY ALS ENTSCHEIDENDER FAKTOR

Klassische Sicherheitsarchitekturen mit Fokus auf Perimeter-Verteidigung wie Firewalls stoßen angesichts komplexer Cyberbedrohungen an ihre Grenzen. Effektiver Schutz erfordert ein Umdenken hin zu Data-Centric Security (DCS) – einem Paradigma, das den Schutz der Daten selbst in den Mittelpunkt stellt.

Steigender Schutzbedarf für sensible Daten

Mit zunehmender Digitalisierung sind Daten zur unverzichtbaren Ressource geworden. Dies weckt auch kriminelle Interessen, da sich mit Daten bekanntlich Gewinne erzielen lassen. Cyberkriminelle setzen hier insbesondere auf Datendiebstahl. Der Schlüssel zu maximalem Profit liegt dabei nachweislich in der Jagd auf geistigem Eigentum, Kunden-, Lieferanten-, Finanz- oder Gesundheitsdaten. Diese sensiblen Daten müssen deshalb auch besonderen Schutz erfahren – auch dann, wenn der Perimeter der eigenen IT-Infrastruktur bereits überwunden wurde. Gleichzeitig nehmen Bedrohungsakteure auch solche Daten jenseits des Perimeters ins Visier, die bereits umfassend in Cloud-Diensten, auf mobilen oder IoT-Geräten mit unterschiedlichem Schutzniveau gespeichert und verarbeitet werden. An dieser Stelle setzt DCS an, indem es den Schutz nicht an der Infrastruktur, sondern unmittelbar an den Daten selbst verankert. Ein zentraler Baustein dabei ist der konsequente Einsatz kryptografischer Verfahren, mit denen schützenswerte Daten über ihren gesamten Lebenszyklus hinweg verschlüsselt werden. Dies stellt sicher, dass sensible Daten auch im Falle einer erfolgreichen Kompromittierung für Unbefugte nutzlos bleiben.

Risiken durch Insider-Bedrohungen entgegnen

Darüber hinaus ist es ein weit verbreiteter Irrglaube, dass sensible Daten, auch wenn sie ausschließlich in der eigenen IT-Infrastruktur verarbeitet und gespeichert werden, sicher sind – selbst bei der leistungsfähigsten und bestkonfigurierten Firewall. Denn das Risiko durch Insider ist omnipräsent, auch wenn sich diese Bedrohung aufgrund einer hohen Dunkelziffer oft nicht beziffern lässt. Dabei handelt es sich um aktuelle oder ehemalige Mitarbeitende, Geschäftspartner oder externe Projektverantwortliche. Besonders in Behörden oder Unternehmen, in denen Mitarbeitende mehrere Abteilungen durchlaufen oder Dienstleister eingebunden sind, entstehen dadurch erhöhte Sicherheitsrisiken. Mit DCS erfahren schützenswerte Daten über die Verschlüsselung hinaus eine feingranulare und kontextbasierte Zugriffskontrolle. Berechtigungen richten sich somit nicht nur nach klassischen Rollen, sondern auch nach dynamischen Attributen wie Standort, Tageszeit oder Gerät. Damit lassen sich Zugriffsrechte präzise an die tatsächlichen Anforderungen anpassen und unautorisierte Zugriffe, egal ob ungewollt oder böswillig, wirksam minimieren.

Daten schützen: beim Übertragen, Speichern und Nutzen

An dieser Stelle wird deutlich, dass sich Cyberangriffe auf wertvolle Daten weder von außen noch von innen vollständig verhindern lassen. Sensible Daten befinden sich zudem längst außerhalb der eigenen, sichergeglaubten IT-Infrastruktur und erfordern daher auch dort angemessenen Schutz. Umso wichtiger ist es, im Ernstfall die Auswirkungen so gering wie möglich zu halten. Ein datengetriebener Ansatz gewährleistet diesen Schutz in einer dezentralen und hochgradig vernetzten Welt – unabhängig vom Speicherort, Übertragungsweg oder der Nutzung. Wer also einen nachhaltigen Schutz für seine sensitiven Daten anstrebt, kommt an DCS nicht vorbei.

www.infodas.de

UNTERNEHMEN VERMUTEN KÜNSTLICHE INTELLIGENZ HINTER ANGRIFFEN IN DEN LETZTEN ZWÖLF MONATEN.
(Deutschland)

67 %
Ja

29 %
Nein

4 %
Nicht sicher

Cybersecurity – Bedrohungen, Sorgen und Herausforderungen

BITDEFENDER-STUDIE DECKT ALARMIERENDE DISKREPANZEN AUF

Die Cybersecurity-Landschaft in Unternehmen zeigt beunruhigende Entwicklungen: Mehr als die Hälfte der IT- und Sicherheitsexperten wird unter Druck gesetzt, Sicherheitsverletzungen zu vertuschen. Dies ergab der aktuelle Cybersecurity Assessment Report 2025 von Bitdefender, für den über 1.200 Fachkräfte aus Unternehmen mit mindestens 500 Mitarbeitern in sechs Ländern befragt wurden.

Schweigen über Sicherheitsvorfälle
Alarmierend: 57,6 Prozent der befragten IT- und Sicherheitsexperten gaben an, aufgefordert worden zu sein, eine Sicherheitsverletzung vertraulich zu behandeln, obwohl sie der Meinung waren, dass diese den Behörden gemeldet werden sollte. Gegenüber 2023 entspricht dies einem Anstieg von 38 Prozent. Regional führt Singapur mit 75,7 Prozent, gefolgt von den USA mit 73,8 Prozent. Deutschland liegt mit 48,4 Prozent im unteren Mittelfeld. Die häufigsten Sicherheitsverletzungen in Deutschland waren Cloud-Sicherheitsvorfälle (43 %), Ransomware (36 %) und unautorisierter Datenzugriff (30 %).

Angriffsfläche reduzieren hat höchste Priorität
Zwei Drittel der Fachleute (67,7 %) betonten, wie wichtig es ist, die Angriffs-

fläche zu verringern, indem sie unnötige Tools oder Anwendungen deaktivieren. Diese Prioritätensetzung deckt sich mit Bitdefender-Untersuchungen, die zeigen, dass 84 Prozent der größeren Angriffe mit bereits vorhandenen legitimen Tools erfolgen – sogenannte Living-Off-the-Land-Taktiken (LOTL-Taktiken). Als am stärksten gefährdete Infrastrukturen gelten Cloud-Infrastrukturen und -dienste (21,4 %), gefolgt von Netzwerken (18,6 %) und Endpunkten (16,8 %).

Führungskräfte überschätzen Cybersecurity-Readiness

Während 45 Prozent der Führungskräfte auf der C-Ebene sagen, dass sie „sehr zuversichtlich" sind, was den Umgang mit Cyber-Risiken angeht, stimmen nur 19 % der Manager der mittleren Ebene zu. Diese Diskrepanz erstreckt sich auch auf die Prioritäten: 41 % der C-Level-Führungskräfte geben an, dass die Einführung von KI-Tools für sie an erster Stelle steht, während 35 % der Manager der mittleren Ebene der Stärkung der Cloud-Sicherheit und des Identitätsmanagements Priorität einräumen.

KI-Bedrohungen dominieren die Sorgen

67 Prozent aller Befragten glauben, dass KI-gesteuerte Angriffe zugenommen haben, wobei die Besorgnis in Frankreich (73,5 %), den USA (71 %), und Singapur (70 %) am größten ist. Als besorgniserregendste Bedrohungen nannten 51 Prozent KI-generierte Threats wie Deepfakes und automatisierte Malware, dicht gefolgt von Phishing und Social Engineering (44,7 %). Bemerkenswert: 63,3 Prozent glauben, ihr Unternehmen habe in den letzten zwölf Monaten einen Angriff mit KI-Elementen erlebt – in Deutschland sogar 67 Prozent. Branchenuntersuchungen (einschließlich Bitdefender-Untersuchungen) finden jedoch nach wie vor nur wenige Belege für ausgefeilte Malware, die vollständig von KI erstellt wurde - vielmehr nutzen Angreifer KI-Tools wie Chatbots, um bösartigen Code zu verfeinern oder Fehler zu beheben.

Komplexität und Fachkräftemangel belasten Teams

Die Komplexität der Tools stellt für 31 Prozent der Befragten die größte Herausforderung für ihre aktuellen Sicherheitslösungen dar. Deutschland meldet mit 41 Prozent die größten Schwierigkeiten mit der Tool-Komplexität. Die Ausweitung des Schutzes auf verschiedene Umgebungen (29 %) und der Mangel an internen Fachkräften (28 %) folgten dicht dahinter. Dies äußerte besonders Singapur (39 %) als größten Mangel.

Gleichzeitig verschärft sich das Qualifikationsdefizit: 49 Prozent berichten über eine Vergrößerung der Skills-Lücke in den letzten zwölf Monaten, wobei die USA sogar 63,5 Prozent (14 Prozentpunkte über dem Durchschnitt) den höchsten Wert aufweisen, gefolgt von Singapur (59 %) und Deutschland (51 %).

Das Burnout-Problem erreicht ebenfalls kritische Ausmaße: 49 Prozent der Fachkräfte leiden unter der ständigen Notwendigkeit, auf evolvierende Bedrohungen reagieren zu müssen. In den USA und Singapur planen 50 Prozent der Cybersecurity-Professionals einen Jobwechsel im nächsten Jahr. Paradox: 95 Prozent der Führungskräfte glauben, ihr Unternehmen manage Risiken effektiv – eine weitere Diskrepanz zur Realität der operativen Teams.

Fazit

„Unternehmen sehen sich mit wachsenden Herausforderungen und Druck konfrontiert, da sich die Angriffsfläche vergrößert und die Verteidigung schwieriger wird - von der Härtung von Umgebungen und der Optimierung von Sicherheitslösungen bis hin zur Einhaltung gesetzlicher Vorschriften und der Bindung qualifizierter Fachkräfte“, sagt Andrei Florescu, President und General Manager der Bitdefender Business Solutions Group. „Die Ergebnisse unseres Berichts machen deutlich, dass Unternehmen moderne Sicherheitsstrategien einführen müssen, die einer neuen Realität Rechnung tragen, in der Angreifer KI einsetzen, um Schwachstellen auszunutzen, Social Engineering zu verbessern und die Geschwindigkeit von Angriffen zu beschleunigen. Effektive Cybersicherheit stoppt nicht nur Angriffe, sondern reduziert auch kontinuierlich das Risiko und sorgt für eine kontinuierliche Compliance im gesamten Unternehmen.“

Andrei Florescu

DIE ERGEBNISSE UNSERES BERICHTS MACHEN DEUTLICH, DASS UNTERNEHMEN MODERNE SICHERHEITSSTRATEGIEN EINFÜHREN MÜSSEN.

Andrei Florescu,
President und General Manager,
Bitdefender Business Solutions Group,
www.bitdefender.com

WELCHE ANGRIFFE ODER SECURITY-VORFÄLLE HABEN SIE INNERHALB DER LETZTEN 12 MONATE ERLEBT? (Deutschland)

43 %
Cloud Breach

30 %
Unautorisierten Zugriff

36 %
Ransomware

SPAM-E-MAILS

MENSCHENGEMACHT?

Wie eine aktuelle Studie der Universitäten Columbia und Chicago auf Basis der Bedrohungserkennungsdaten von Barracuda zeigt, nutzen E-Mail-Betrüger zunehmend KI-Tools, um Spam-E-Mail-Kampagnen im großen Maßstab zu erstellen und durchzuführen, anstatt zielgerichtete Angriffe durchzuführen.

Die Forscher der Universitäten analysierten einen von Barracuda bereitgestellten Datensatz von unerwünschten und schädlichen E-Mails aus dem Zeitraum von Februar 2022 bis April 2025.

„Festzustellen, ob oder wie KI bei Cyberangriffen genutzt wird, ist eine große Herausforderung, da wir nur den Angriff selbst sehen, aber nicht, wie der Angriff generiert wurde", sagt Asaf Cidon, Associate Professor of Electrical Engineering and Computer Science an der Universität Columbia. „Unsere Analyse deutet darauf hin, dass im Zeitraum bis April 2025 ein Großteil der Spam-E-Mails nicht von Menschen, sondern von KI generiert wurde. Bei komplexeren Angriffen wie BEC, bei denen Inhalte sorgfältiger auf den Kontext des potenziellen Opfers abgestimmt werden müssen, werden die meisten E-Mails nach wie vor von Menschen verfasst. Der Anteil der von KI generierten E-Mails nimmt jedoch stetig und kontinuierlich zu."

Der Ansatz der Forscher zur Erkennung von KI-Einsatz basierte auf der Annahme, dass E-Mails, die vor dem Launch von ChatGPT 2022 versendet wurden, wahrscheinlich von Menschen verfasst wurden. Auf diese Weise konnten sie eine Ausgangsbasis festlegen und Erkennungssysteme trainieren, damit diese automatisch erkennen, ob eine unerwünschte oder schädliche E-Mail mithilfe von KI generiert wurde.

Zur Abwehr von sich kontinuierlich weiterentwickelnden E-Mail-Bedrohungen empfiehlt Barracuda die Implementierung eines fortschrittlichen, mehrschichtigen und KI-gestützten E-Mail-Schutzes in Kombination mit Cybersicherheitsschulungen für Mitarbeiter, damit diese über die neuesten Cyberbedrohungen und Taktiken von Cyberangreifern informiert sind. Bitte hier noch eine Zeile anfügen, damit die Texte gleich stehen

www.barracuda.com

ERGEBNISSE BIS APRIL 2025

51 %
der Spam-E-Mails wurden von KI generiert

14 %
der Business-E-Mail-Compromise-Angriffe wurden von KI generiert

MEHR WERT
Threat Spotlight

Ganzheitliche IT-Sicherheitskonzepte

DATENSOUVERÄNITÄT UND IT-SECURITY MADE IN GERMANY ALS SCHLÜSSELFAKTOREN

Im Zuge der fortschreitenden Digitalisierung, hybrider Arbeitsmodelle und global vernetzter IT-Infrastrukturen ist ein belastbares IT-Sicherheitskonzept längst kein optionales Nice-to-have mehr, sondern das Fundament stabiler Unternehmensprozesse. Dennoch verlassen sich viele IT-Verantwortliche noch immer auf fragmentierte Sicherheitsmaßnahmen, etwa einzelne Endpoint-Lösungen oder Standard-VPNs, ohne das große Ganze im Blick zu haben. Dabei sind es genau diese ganzheitlichen Konzepte, die Resilienz gegenüber Cyberbedrohungen und regulatorische Sicherheit bieten.

Besonders deutlich wird die Notwendigkeit eines systematischen Sicherheitsansatzes im Kontext von Remote Work und standortunabhängiger Zusammenarbeit. Diese Entwicklungen erfordern nicht nur flexible, sondern auch jederzeit abgesicherte Verbindungen. Der Schutz mobiler Arbeitsplätze, der sichere Zugriff auf Unternehmensressourcen aus fremden Netzen und die lückenlose Protokollierung von Zugriffen sind zu zentralen Bestandteilen moderner Sicherheitsarchitekturen geworden.

Ein zukunftsfähiges IT-Sicherheitskonzept muss mehrere Dimensionen vereinen: technische Qualität, regulatorische Konformität, vertrauenswürdige Partnerschaften und die Wahrung der Datensouveränität. Gerade in Zeiten wachsender geopolitischer Spannungen und zunehmender Cloud-Abhängigkeit wird deutlich: Wer nicht weiß, wo seine Daten gespeichert und wie sie verarbeitet werden, verliert mittelfristig die Kontrolle über sein eigenes Sicherheitsprofil.

Typische IT-Infrastrukturen mittelständischer Unternehmen sind über die Jahre hinweg organisch gewachsen. Sicherheitslösungen wurden dementsprechend oft nur nach Bedarf implementiert. Was somit fehlt, ist die übergreifende Koordination. Das Resultat: Sicherheitslücken an den Schnittstellen, mangelnde Übersichtlichkeit und hohe Komplexität im Management. Solche Strukturen sind nicht nur ineffizient, sondern meistens auch gefährlich. Etwa wenn sich Angreifer lateral im System bewegen können oder Admins die Übersicht über Zugriffskontrollen verlieren.

Das IT-Sicherheitskonzept als Architektur

Ein modernes Sicherheitskonzept muss genau durchdacht und aus einer Hand verwaltet werden: modular, skalierbar und auf das jeweilige Geschäftsmodell zugeschnitten. Dabei geht es nicht nur um die Integration von Technologien wie VPN, Firewalls, Endpoint-Security oder Zero-Trust-Architekturen. Entscheidend ist vielmehr die Strategie dahinter: Welche Daten sind schützenswert? Wer darf worauf zugreifen und wann? Wie lassen sich diese Rechte flexibel und zentral steuern?

Unternehmen benötigen zentrale Management-Systeme, die es erlauben, Konfigurationen automatisiert und skalierbar auszurollen, Änderungen nachvollziehbar zu dokumentieren und Compliance-Anforderungen dauerhaft zu erfüllen. Hier sind Lösungen gefragt, die mit gewachsenen IT-Strukturen kompatibel sind und moderne Zero-Trust-Strategien unterstützen.

Im Zentrum stehen dabei sichere, verschlüsselte Verbindungen, etwa ein leistungsfähiges VPN-System, das orts- und geräteunabhängig funktioniert. Gerade hier kommt der Stellenwert von „IT-Security Made in Germany" zum Tragen: Unternehmen sollten sich fragen, ob sie bei einer solch sensiblen Technologie auf außereuropäische Anbieter vertrauen wollen, deren Softwarekomponenten möglicherweise rechtlich zur Kooperation mit ausländischen Behörden verpflichtet sind oder ob nicht eine Lösung aus Deutschland mit transparenten Sicherheitsstandards die bessere Wahl ist.

Datensouveränität als strategisches Ziel

Datensouveränität, also die Hoheit über die eigenen Daten, ist längst mehr als ein abstraktes Ideal. Für Unternehmen bedeutet es konkret, dass sie jederzeit nachvollziehen können, wo ihre Daten gespeichert, verarbeitet und transportiert werden. Dies betrifft nicht nur Kundendaten, sondern auch interne Kommunikations- und Steuerungsprozesse.

Souveränität bedeutet zudem, nicht von Black-Box-Systemen abhängig zu sein, deren Sicherheitslogik sich nicht offenlegen lässt. Unternehmen, die ihre IT-Sicherheitsinfrastruktur auf zertifizierte deutsche Anbieter stützen, verschaffen sich einen entscheidenden Vorteil: Sie behalten die Kontrolle über Technologie, Datenschutz und Compliance.

Gerade mit Blick auf Vorgaben wie die DSGVO oder branchenspezifische Regularien wie KRITIS wird klar: Compliance ist nur möglich, wenn Datensouveränität gegeben ist. Und diese lässt sich nur dann verlässlich erreichen, wenn auch die eingesetzten Technologien transparent, nachvollziehbar und rechtlich abgesichert sind.

Für Unternehmen im öffentlichen Sektor oder im Defense-Bereich sowie mit KRITIS-Verpflichtungen ist zudem die Einhaltung nationaler Standards von besonderer Relevanz. Zulassungen durch das Bundesamt für Sicherheit in der Informationstechnik (BSI) schaffen eine wichtige Grundlage für Vertrauen, sowohl in die eingesetzten Technologien als auch in die Prozesse des Anbieters.

Der Begriff „IT-Security Made in Germany" ist längst mehr als ein Marketing-Label. Für Anbieter bedeutet er ein klares Bekenntnis zur Entwicklung und Produktion in Deutschland, zu europäischen Datenschutzstandards und zu einem transparenten, auditierbaren Entwicklungsprozess. Die Nähe zu den Kunden, der direkte Support aus Deutschland sowie die Möglichkeit zur Integration in bestehende Infrastrukturen machen den Unterschied.

Sicherheitskonzepte neu denken

Der Weg zu einer resilienten IT-Sicherheitsarchitektur führt über Konsistenz, Kontrolle und Vertrauen. Statt sich auf Insellösungen oder kurzfristige Workarounds zu verlassen, sollten Unternehmen in langfristige, modulare Konzepte investieren, die zentrale Fragen beantworten: Wie ist meine Infrastruktur aufgebaut? Wo liegen meine Risiken? Und vor allem: Wem vertraue ich meine Sicherheitslogik an?

DER WEG ZU EINER RESILIENTEN IT-SICHERHEITSARCHITEKTUR FÜHRT ÜBER KONSISTENZ, KONTROLLE UND VERTRAUEN.

Christian Albrecht,
PR-Manager, NCP engineering GmbH,
www.ncp-e.com

Datensouveränität, transparente Prozesse und „IT-Security Made in Germany" sind dabei keine Nebenschauplätze, sondern elementare Bausteine einer erfolgreichen Sicherheitsstrategie. In Zeiten zunehmender Bedrohungen sogar oft der entscheidende Unterschied zwischen Schadensbegrenzung und echter Prävention.

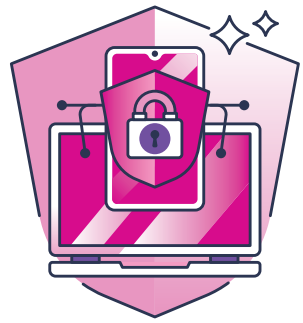
Die Kombination aus technischer Tiefe, regulatorischer Konformität und regionaler Nähe macht Lösungen wie die von NCP besonders für Unternehmen und Behörden attraktiv, die langfristige Planungssicherheit suchen – nicht nur in Bezug auf Technologie, sondern auch auf Datenschutz und rechtliche Rahmenbedingungen.

Christian Albrecht

Zero Trust Application Access

MINIMALINVASIVER ZUGRIFF OHNE VPN

In der modernen Arbeitswelt haben sich die Anforderungen an die Netzwerksicherheit grundlegend geändert. Mitarbeiter, Dienstleister und Kunden greifen vermehrt von extern und mit verschiedenen Endgeräten auf Applikationen in Unternehmensnetzwerken zu. Gleichzeitig wachsen OT und IT verstärkt zusammen, so dass auch Maschinen und Anlagen etwa in Fabriken aus dem Internet erreichbar sind. Die Vorteile liegen auf der Hand: So lassen sich die Systeme beispielsweise effizienter betreiben, da sie ohne Vor-Ort-Präsenz konfiguriert werden können. Hinzu kommt, dass Unternehmen verstärkt Cloud-Angebote nutzen – etwa, um durch den Einsatz virtualisierter Netzwerkprodukte ihre IT-Infrastruktur flexibler skalieren zu können.



Die Kehrseite: Diese Entwicklungen hebeln bisherige Perimeter-basierte Sicherheitsarchitekturen zunehmend aus. Und durch die verstärkte Exponierung sensibler Assets entstehen neue Angriffsvektoren, über die Cyberkriminelle Unternehmen attackieren können. Das wiegt schwer, da Cyberbedrohungen auch im industriellen Sektor weltweit seit Jahren massiv zunehmen. Industriespionage, Manipulation oder gar Zerstörung von Anlagen sind mögliche Folgen.

ZERO-TRUST-LÖSUNGEN KÖNNEN VOR INSIDER-BEDROHUNGEN UND KOMPROMITTIERTEN KONTEN SCHÜTZEN.

Steve Schoner, Produkt Marketing Manager, genua GmbH, www.genua.de

Die Vorteile von kombinierten IT/OT-Strukturen nicht zu nutzen, ist für viele Unternehmen jedoch keine Option. Daher stellt sich die Frage: Wie lassen sich ihre IT- und daran gekoppelte OT-Systeme bestmöglich absichern? Und gleichzeitig Möglichkeiten schaffen, Legacy-Web- und Windows-Applikationen weiter zu betreiben, spezielle Steuerungs-Anwendungen von Maschinen und Anlagen, Admin-Interfaces sowie restriktiv eingesetzte Applikationen zu erreichen und sichere temporäre Zugänge für externe User einzurichten?

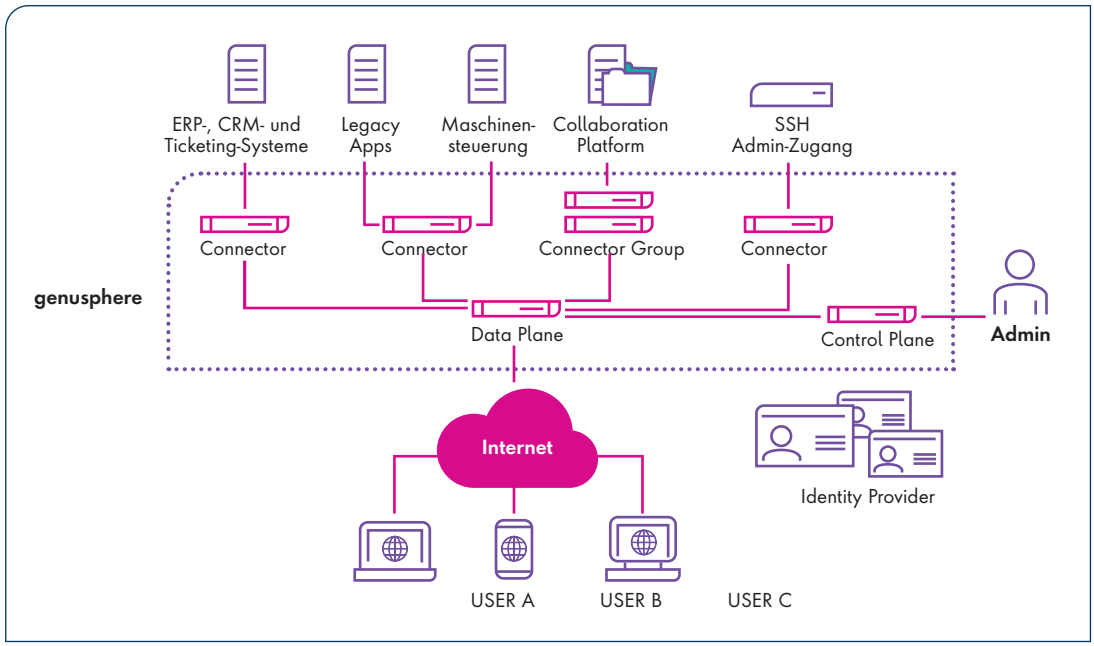
Eine Antwort lautet Zero Trust Application Access, kurz ZTAA. Der Zero-Trust-Ansatz geht grundsätzlich davon aus, dass keine Person und kein Gerät standardmäßig vertrauenswürdig sind. Stattdessen wird jeder Zugriff methodisch und wiederholt überprüft, selbst wenn der Nutzer dem System bereits bekannt ist. Zero-Trust-Lösungen lassen sich zudem so konfigurieren, dass sie für interne und externe Nutzer gleichermaßen anwendbar sind. Dadurch lässt sich ein guter Schutz auch vor Insider-Bedrohungen und kompromittierten Konten realisieren.

ZTAA agiert zudem nach dem Prinzip der minimalen Rechtevergabe. Verbindungen zwischen Usern – externen wie internen – und Anwendungen werden anhand von Identität, Rolle und Geschäftsrichtlinien (Policies) hergestellt. So erhalten Anwender abhängig von diesem Dreiklang nur Zugriff auf einzelne, für sie freigegebene Applikationen – anstatt auf weitreichende Ressourcen im Netzwerk.

Sicherer Zero-Trust-Zugriff per Webbrowser

Für die oben genannten und weitere Anwendungsfälle hat der deutsche IT-Security-Spezialist genua GmbH die hochsichere, skalierbare ZTAA-Lösung genusphere entwickelt. Das Besondere daran: genusphere benötigt anwenderseitig keine Installation einer speziellen Software, etwa eines VPN-Clients. Ein Standard-Webbrowser wie Google Chrome oder Microsoft Edge reicht, um sicher auf explizit freigegebene Ressourcen im Unternehmensnetzwerk zugreifen zu können.

Eine Client-lose Zugriffslösung bietet für moderne Arbeitsumgebungen einige Vorteile. An erster Stelle sind hier die Unabhängigkeit von Gerät und Betriebssystem, geringer Wartungsaufwand sowie hohe Flexibilität und Skalierbarkeit zu nennen. Geringe Kosten



User und Connector bauen eine verschlüsselte Verbindung zur Data Plane auf. In der Control Plane sind die identitätsbasierten Zugriffsberechtigungen hinterlegt.

und einfache Integration sprechen ebenfalls für browserbasierte Lösungen.

genusphere baut auf Kubernetes auf – einer ursprünglich von Google entwickelten Open-Source-Plattform zum Verwalten von Container-Anwendungen. Der Container-basierte Ansatz ist von Grund auf für optimale Skalierbarkeit und Hochverfügbarkeit ausgelegt. Bei der Lösung erfolgt die Anbindung an das Zielsystem über Docker-Container, während die Verwaltung über ein zentrales Online-Administrationsportal erfolgt (siehe Grafik).

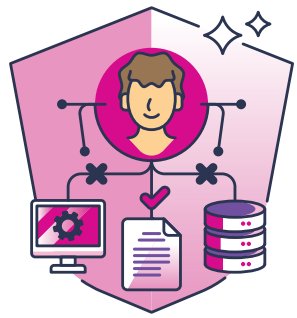
Eine Kernfunktion ist das implementierte Treffpunkt-Konzept: Nach einer vom Endgerät aus per Browser initiierten Verbindungsanfrage erfolgt der eigentliche Verbindungsaufbau von innen nach außen. So ist sichergestellt, dass für jeden Zugriff zuverlässig die definierten Zero-Trust-Regeln durchgesetzt werden.

Die Verbindungen sind grundsätzlich durchgängig mit HTTPS verschlüsselt. Fernsteuerung per RDP (Remote Desktop Protocol) oder VNC (Virtual Network Computing) sowie der Shellzugriff per SSH (Secure Shell) sind ebenfalls über Webbrowser nutzbar. Die Lösung ist mit Sicherheitsfunktionen wie Multi-Faktor-Authentisierung und Zero Trust Access Control ausgestattet.

Integration in vorhandene Sicherheitsarchitekturen

Die genua-Lösung setzt auf ein feingranulares Berechtigungsmanagement und lässt sich in vorhandene Sicherheitsarchitekturen einbinden. So unterstützt genusphere die Identity Provider Microsoft Entra ID (vormals Azure AD) und Keycloak. Single Sign On (SSO) erhöht dabei den Nutzerkomfort. Die Regeln bauen auf den Identitäten der User aus der Benutzerverwaltung auf und sind der Schlüssel zu einer hochsicheren und flexibel skalierbaren Architektur.

Ein Dashboard mit genauen Metriken bietet Administrierenden jederzeit den Überblick über Nutzung und Betrieb. Gleichzeitig können sie mithilfe zahlreicher Regeln/Policies, logischen Verknüpfungen und Sub-Policies die Zugänge dynamisch anpassen. Wichtig dabei: Nicht ausdrücklich freigegebene Ressourcen sind sicher vor unbefugten Zugriffen geschützt. Selbst kompromittierte Nutzerkonten können sich somit nicht im Netz bewegen. Die Lösung kann daher für Remote-Work-Umgebungen typische Cyberrisiken zuverlässig ausschalten.



Durch den identitätsbasierten und anwendungsspezifischen Zugriffsschutz baut genusphere eine zuverlässige Mikro-Perimeter-Sicherheit auf. Zugriffe werden revisionssicher protokolliert und sind so lückenlos nachvollziehbar. Dadurch können Systemadministratoren konsequent hochsichere Zero-Trust-Konzepte durchsetzen.

Nicht zuletzt zahlt genusphere auf die Digitale Souveränität von Unternehmen ein. Denn sie behalten die 100-prozentige Hoheit über ihre Daten. Firmen können die Lösung selbst betreiben, oder hierfür spezialisierte genua-Partner ins Boot holen. Übrigens lässt sich die ZTAA-Lösung auch mit einem VPN kombinieren – dadurch entsteht eine zusätzliche Sicherheitsebene.

Michael Eckstein | www.genua.de

Fünf Fragen vor dem Managed SOC-Wechsel

WAS IT-LEITER VOR DER ENTSCHEIDUNG KLÄREN MÜSSEN

Ein Managed Security Operations Center (Managed SOC) kombiniert modernste Sicherheitslösungen mit einem umfassenden Serviceangebot. Doch für welche Unternehmen lohnt sich der Einsatz? Wie steht es um die Themen Datenschutz und Vertrauen? Und warum verbessert ein Managed SOC die IT-Sicherheit entscheidend? Wir beantworten die wichtigsten Fragen.

#1 Welche Herausforderungen können Unternehmen mit einem Managed SOC angehen?

Die Bedrohungslage verschärft sich kontinuierlich. Viele Cyberattacken sind heute individualisiert und dateilos. Angreifer verschaffen sich häufig durch Phishing oder Sicherheitslücken in Anwendungen und Betriebssystemen Zugang zu Netzwerken.

Anschließend bleiben sie längere Zeit unentdeckt, bevor sie etwa Systeme verschlüsseln oder Daten exfiltrieren. Gleichzeitig wächst der Druck durch gesetzliche Vorgaben. Je nach Branche gelten unterschiedliche Standards: NIS2, CRA oder DORA fordern weitreichende Sicherheitsmaßnahmen – von Awareness-Programmen bis zur Endpoint-Überwachung durch ein Security Operations Center (SOC).

Viele Unternehmen möchten ihr Schutzniveau erhöhen, stoßen dabei aber auf personelle und fachliche Grenzen. IT-Sicherheit verlangt ständige Aufmerksamkeit und spezielles Know-how. Allein für den 24/7-Betrieb wären in einem mittelständischen Unternehmen etwa acht Fachkräfte nötig – eine erhebliche organisatorische und finanzielle Belastung. Ein Managed SOC ist hier oft die wirtschaftlichere Lösung.

MANAGED SOCS BIETEN ZUGANG ZU EXPERTISE, MODERNER TECHNIK UND DAUERHAFTEM MONITORING – OHNE HOHE EINSTIEGSKOSTEN.

Stefan Karpenstein,
PR-Manager, G DATA CyberDefense,
www.gdata.de

#2 Was erwarten Verantwortliche von einem Managed SOC?

Zentral ist der Schutz vor Angriffen. Bedrohungen sollen frühzeitig erkannt und unmittelbar gestoppt werden. Im Ernstfall zählt jede Minute – nicht nur bei der Erkennung, sondern auch bei der Reaktion. Aber: Wer eine durchgehende Überwachung vereinbart, muss im eigenen Unternehmen ebenfalls Ansprechpersonen rund um die Uhr benennen. Es nützt wenig, wenn um 22:00 Uhr ein Vorfall gemeldet wird, aber niemand reagiert.

Gleichzeitig erwarten Kunden eine verlässliche Betreuung. Die Zusammenarbeit mit dem Dienstleister basiert auf Vertrauen – und das muss kontinuierlich bestätigt werden. Service und Support in der Landessprache helfen dabei, Sprachbarrieren zu vermeiden und Missverständnisse in kritischen Situationen auszuschließen.

#3 Was ist bei einem Managed SOC besonders wichtig?

Aus Sicht des Dienstleisters steht der Schutz der zentralen IT-Infrastruktur und Unternehmensdaten im Mittelpunkt. Sobald ein Angriff erkannt wird, greifen Experten unmittelbar ein, um den Schaden zu minimieren.

Für Kunden bedeutet die Zusammenarbeit ein hohes Maß an Vertrauen. Sie übertragen Verantwortung an externe Partner – in der Erwartung, dass diese sorgfältig handeln. Ein intensiver Austausch über technische Abläufe, Datenhaltung und Datenschutz ist daher essenziell. Gerade öffentliche Auftraggeber ach-

ten verstärkt auf den Serverstandort, da dieser über die geltende Rechtslage entscheidet.

Ein Managed SOC ist eine komplexe Lösung, die nicht nur überwacht, sondern auch aktive Reaktion durch die Fachleute ermöglicht. Um die Leistungsfähigkeit einschätzen zu können, helfen im Vorfeld sogenannte Proof of Concepts (PoCs). Dabei handelt es sich um Testphasen mit realem Serviceeinsatz, die eine objektive Bewertung ermöglichen.

#4 Welche Rolle spielt der Datenschutz?

Für öffentliche Einrichtungen und Betreiber kritischer Infrastrukturen ist Datenschutz essenziell. Sie möchten genau wissen, welche Daten eingesehen und wo sie gespeichert werden. Viele Anbieter setzen auf ausländische Cloud-Dienste, für die keine deutsche Rechtsgrundlage gilt. Werden Daten dagegen ausschließlich in deutschen Rechenzentren verarbeitet, unterliegen sie deutschem Datenschutzrecht.

Auch bei der Datennutzung gilt: so wenig wie möglich, so viel wie nötig. Dienstleister sollten nur jene Informationen einsehen, die zur Gefahrenabwehr erforderlich sind. Wer hier transparent agiert und klare Grenzen einzieht, kann sich positiv vom Wettbewerb abheben.

#5 Für welche Unternehmen lohnt sich ein Managed SOC?

Grundsätzlich kann jedes Unternehmen Ziel eines Angriffs werden. Der Einsatz eines Managed SOCs ist daher auch für kleine Betriebe sinnvoll – etwa bei zehn bis 15 Mitarbeitenden. Viele Organisationen können eine kontinuierliche Überwachung nicht selbst stemmen. Managed SOCs bieten Zugang zu Expertise, moderner Technik und dauerhaftem Monitoring – ohne hohe Einstiegskosten. Einige Anbieter offerieren ihre Services bereits ab fünf Seats, unabhängig von der Unternehmensgröße. Unterschiede ergeben sich meist nur beim gewählten Service-Level.

Unternehmen mit verteilten oder hybriden Arbeitsmodellen profitieren besonders von zentraler Sicherheitsüberwachung – unabhängig vom Standort der Mitarbeitenden. Auch stark regulierte Branchen wie der Finanz- und Gesundheitssektor erhalten durch regelmäßige Berichte und Dokumentation wichtige Unterstützung bei der Compliance.

Stefan Karpenstein

Ransomware beginnt mit dem Login

WIE GESTOHLENE IDENTITÄTEN ZUR SYSTEMBEDROHUNG WERDEN

Ein gestohlenes Passwort kann ausreichen, um eine Ransomware-Attacke ins Rollen zu bringen. Digitale Identitäten sind für Cyberkriminelle längst wertvolle Beute. Ohne geeignete Schutzmaßnahmen bleibt das digitale Tor weit offen. Mit Customer Identity and Access Management (CIAM) lassen sich Risiken frühzeitig erkennen und gezielt absichern.

Branchenberichte zeigen: In rund drei Viertel der Fälle verschaffen sich Cyberangreifer über kompromittierte Nutzerkonten Zugriff auf sensible Systeme. Bleibt der Schutz digitaler Identitäten lückenhaft, gerät die gesamte IT-Sicherheitsarchitektur ins Wanken. CIAM schafft hier gezielte Abhilfe: Mit risikobasierter Authentifizierung, feingranularen Zugriffskontrollen und kontinuierlicher Überwachung schützt die Technologie Identitäten über den gesamten Nutzerlebenszyklus hinweg – und geht dabei weit über klassische Login-Verfahren hinaus.

Wie ungesicherte Identitäten zur Schwachstelle werden

Cyberangriffe verlaufen selten willkürlich. Meist folgen sie einem bewährten Ablauf: Mit automatisierten Tools sondieren Angreifer systematisch mögliche Schwachstellen, bevorzugt dort, wo Identitäten nicht ausreichend geschützt sind. Besonders gefährdet sind Unternehmen, die auf veraltete Authentifizierungsverfahren setzen, externen Akteuren weitreichende Rechte ohne wirksame Kontrolle einräumen oder ihre Berechtigungsprozesse nur unzureichend dokumentieren.

Nicht selten beginnt der Angriff mit gestohlenen Zugangsdaten, sei es durch Phishing, Credential Stuffing oder den Missbrauch technischer Dienstzugänge. Organisationen mit komplexen Partnernetzwerken laufen Gefahr, den Überblick über Rollen, Zugriffsrechte und Schnittstellen zu verlieren. Die Folge: kritische Sicherheitslücken. Wer solche Risiken eindämmen will, muss Identitäten und Berechtigungen entlang des gesamten digitalen Ökosystems absichern.

Zugriff ohne Risiko

In dynamischen IT-Landschaften mit zahlreichen Anwendungen, Endgeräten und Schnittstellen stoßen klassische IAM-Systeme schnell an ihre Grenzen. Ursprünglich für interne Mitarbeitende entwickelt, lassen sie sich nur schwer auf externe Zielgruppen wie Partner, Dienstleister oder Kundinnen und Kunden übertragen. Gefordert sind Lösungen, die Sicherheit und Nutzerfreundlichkeit intelligent verbinden. Genau hier setzt modernes Customer Identity and Access Management an, und zwar mit adaptiven Verfahren, die den Zugriff nicht starr, sondern situationsabhängig regeln. Wird ein Login beispielsweise von einem bekannten Gerät oder Standort aus durchgeführt, bleibt der Zugang unkompliziert. Bei Abweichungen vom üblichen Verhalten hingegen greifen automatisch zusätzliche Sicherheitsmaßnahmen.

Diese risikobasierte Authentifizierung (Risk-Based Authentication, RBA) ermöglicht es, verdächtige Zugriffe frühzeitig zu erkennen und abzuwehren – ohne legitime Nutzerinnen und Nutzer unnötig auszubremsen. So entsteht eine Sicherheitsarchitektur, die sich flexibel an das Verhalten ihrer Nutzer anpasst und aktiv mitdenkt.

Schluss mit dem Passwort – Das Login der Zukunft

Passwörter zählen nach wie vor zu den größten IT-Sicherheitsrisiken: schwer zu verwalten, leicht zu kompromittieren und ein bevorzugtes Ziel für Phishing-Angriffe. Moderne CIAM-Lösungen setzen daher auf passwortlose Authentifizierung – von biometrischen Verfahren über physische Token bis zu Authenticator-Apps mit Push-Verifizierung. Diese Technologien erhöhen die Sicherheit deutlich und verringern zugleich den Aufwand für Support und Passwortverwaltung – ein spürbarer Gewinn für alle Beteiligten:

- **Intuitive Nutzung** – Der Zugang erfolgt bequem und sicher, etwa per Biometrie oder Push-Verfahren – ganz ohne Passwörter oder Rücksetzungen.
- **Gezielte Kontrolle externer Zugriffe** – Drittparteien erhalten zeitlich begrenzte, kontextgebundene Berechtigungen, die nicht wiederverwendbar und damit deutlich schwerer zu kompromittieren sind.
- **Weniger Verwaltungsaufwand** – Weniger Passwort-Support entlastet IT-Teams, spart Ressourcen und senkt Kosten.

Zero Trust trifft CIAM

Zero Trust basiert auf dem Grundsatz „never trust, always verify". Unabhängig davon, ob er von internen oder externen Quellen stammt, wird jeder Zugriff konsequent verifiziert. CIAM-Systeme ergänzen das Zero-Trust-Prinzip dort, wo klassische IAM-Modelle nicht mehr weiterkommen: beim Identitäts- und Zugriffsmanagement für externe Zielgruppen. Sie ermöglichen eine passgenaue Authentifizierung und Autorisierung für Kunden, Partner oder Dienstleister – abgestimmt auf deren Rolle, Kontext und Sicherheitsbedarf.

CIAM-SYSTEME ERGÄNZEN DAS ZERO-TRUST-PRINZIP DORT, WO KLASSISCHE IAM-MODELLE NICHT MEHR WEITERKOMMEN.

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

Im Zusammenspiel mit Zero Trust entstehen adaptive Zugriffskonzepte, die nicht nur das Least-Privilege-Prinzip durchsetzen, sondern auch hochgradig anpassbar sind. So lassen sich auch komplexe Infrastrukturen mit verteilten Diensten, Multi-Cloud-Architekturen und häufig wechselnden Schnittstellen konsistent und sicher abbilden.

Verhalten analysieren, Angriffe verhindern

Angriffsvektoren verändern sich rasant und führen klassische Schutzmechanismen schnell ins Hintertreffen. Moderne CIAM-Plattformen setzen daher auf verhaltensbasierte Analysemodelle, die mithilfe maschinellen Lernens typische Nutzungsmuster erkennen und in Echtzeit auf Unregelmäßigkeiten reagieren. Ob auffällig viele Login-Versuche in kurzer Zeit, parallele Zugriffe aus geografisch weit entfernten Regionen oder ungewöhnliche Navigationsmuster: Solche Abweichungen vom Normalverhalten können automatisiert identifiziert und gemeldet werden – lange bevor es zu einem Sicherheitsvorfall kommt. So wird der Authentifizierungsprozess selbst zur intelligenten Verteidigungslinie im Sicherheitskonzept.

Compliance stärken, ohne Kompromisse bei der Usability

Regulatorische Anforderungen wie NIS2, DORA oder DSGVO stellen hohe Ansprüche an das Zugriffsmanagement: Jede Berechtigung muss nachvollziehbar, jede Authentifizierung lückenlos dokumentiert sein. CIAM-Lösungen ermöglichen genau das, mit zentralen Audit-Trails, dynamischen Richtlinien und granularen Rollenkonzepten. So lassen sich regulatorische Vorgaben nicht nur technisch sauber abbilden, sondern auch gegenüber Auditoren oder Geschäftspartnern eindeutig belegen, ohne die Nutzerfreundlichkeit aus dem Blick zu verlieren.

Strategisches Identitätsmanagement gegen Ransomware

Cyberangriffe mit Ransomware basieren häufig auf gestohlenen Zugangsdaten. Sie sind das unterschätzte Einfallstor in die Systeme. Wer dieses Risiko eindämmen will, kommt an einer Identitätsstrategie nicht vorbei, die Sicherheit und Nutzerfreundlichkeit vereint. CIAM-Plattformen bieten dafür ein tragfähiges Fundament: Sie steuern Zugriffsrechte differenziert, ermöglichen starke Authentifizierungsmechanismen und fügen sich reibungslos in moderne Sicherheitsarchitekturen wie Zero Trust ein. Das Ergebnis: digitale Schutzmechanismen, die mit den Anforderungen wachsen, gesetzliche Vorgaben abdecken und Ransomware-Angriffen wirksam vorbeugen – bevor überhaupt ein Schaden entsteht.

Stephan Schweizer

Cybersicherheit im Gesundheitswesen

ANSPRUCH VS. TECHNIKSTAU

Aufgrund sensibler Patientendaten, wichtiger Forschungsergebnisse und ihrer kritischen Dienstleistungen, sind Krankenhäuser und Gesundheitseinrichtungen ein attraktives Ziel für Cyberkriminelle. Jüngste Analysen zur Cybersicherheitslage im Gesundheitswesen, etwa die Studie des Hasso-Plattner-Instituts „Alarmsignal Cybersicherheit", zeichnen ein Bild einer sich zuspitzenden Bedrohungslage.

Allein in Deutschland stieg laut HPI-Studie die Zahl erfolgreicher Angriffe auf Krankenhäuser zwischen 2020 und 2024 um 74 Prozent. Auch 2025 setzt sich dieser Trend fort: Laut KonBriefing waren bereits Kliniken in Ludwigslust und Hagenow, ein Medizinprodukteanbieter (Februar), der Offenbacher Apothekerverband (April) sowie die Ärztekammer Dresden (Mai) betroffen. Cyberattacken gefährden nicht nur Finanzen und Reputation, sondern können lebenswichtige Systeme lahmlegen. Ein IT-Ausfall infolge einer Cyberattacke kann im Extremfall Leben kosten – eine schmerzhafte Realität, auch in Deutschland.

Hinzu kommt: Mit dem Start der elektronischen Patientenakte für alle gesetzlich Versicherten in Deutschland stellt sich auch die Frage nach dem Schutz der Vertraulichkeit sensibler Gesundheitsdaten mit neuer Dringlichkeit. Neben bekannten Bedrohungen wie Ransomware und Datendiebstahl gewinnen zunehmend komplexe Angriffe auf vernetzte medizinische Geräte (IoMT) sowie die Ausnutzung menschlicher Schwachstellen an Bedeutung. Dies gilt insbesondere vor dem Hintergrund verstärkter Aktivitäten staatlich unterstützter Akteure in kritischen Infrastrukturen.

Regelungen und Realität

Mit dem im Oktober 2020 verabschiedeten Krankenhauszukunftsgesetz wollte die damalige Bundesregierung finanzielle Mittel bereitstellen, um Digitalisierungsprojekte im Gesundheitswesen voranzutreiben. Dies hat in Teilen zu Verbesserungen geführt – nicht jedoch im Bereich Cybersicherheit: Noch immer sind veraltete Hard- und Software aufgrund von Zertifizierungsauflagen weit verbreitet. Die IT- und Netzinfrastruktur wird in Silos abgesichert, mit OT-Protokollen gesteuerte Gebäudemanagementsysteme sind unzureichend geschützt. Im Übrigen wird menschliches Versagen – eines der größten Einfallstore für Cyberangriffe – stark unterschätzt. Unter solchen Bedingungen ist die Anfälligkeit der Branche nahezu programmiert.

Angesichts der wachsenden Komplexität und Dynamik der Bedrohungslage ist ein umfassender, proaktiver Sicherheitsansatz unerlässlich. Dieser muss über klassische Perimeterverteidigung hinausgehen und beispielsweise eine konsequente Netzwerksegmentierung zur Begrenzung lateraler Bewegungen von Angreifern, strenge Zugriffskontrollen nach dem Zero-Trust-Prinzip, den Einsatz von VPN-Infrastrukturen und

Multi-Faktor-Authentifizierung sowie klare Sicherheitsrichtlinien im Umgang mit sensiblen Daten und veralteter Technik umfassen.

Essenziell sind obendrein Mechanismen zur frühzeitigen Erkennung (Threat-Detection) und zur schnellen Reaktion auf Sicherheitsvorfälle (Incident-Response). Angesichts der zunehmenden Vernetzung medizinischer Geräte sind auch spezifische Schutzmaßnahmen für diese Systeme erforderlich – insbesondere angesichts ihrer oftmals hohen Obsoleszenz. Und nicht zuletzt sollten kontinuierliche Schulungen und Sensibilisierungsmaßnahmen für das gesamte Personal auf der Agenda stehen.

Strategische Weichenstellungen

Ein absolut zentraler Pfeiler einer strategischen Neuausrichtung im Sinne höherer Cybersicherheit ist die konsequente Etablierung und Instandhaltung einer umfassenden Sicherheitsarchitektur. Diese muss den gesamten Lebenszyklus aller beteiligten IT-Systeme und insbesondere der hochsensiblen medizinischen Geräte von Anfang an berücksichtigen. Das bedeutet, dass das Prinzip des «Security by Design» nicht nur proklamiert, sondern bereits bei der initialen Beschaffung und Entwicklung neuer Hard- und Software kompromisslos angewendet werden muss. Dies erfordert eine beispiellos enge und vertrauensvolle Zusammenarbeit zwischen IT-Verantwortlichen, spezialisierten Medizintechnikern, dem Einkauf sowie dem klinischen Personal. Nur so kann gewährleistet werden, dass technologische Lösungen nicht nur den komplexen operativen Anforderungen gerecht werden, sondern auch den allerhöchsten Sicherheitsstandards entsprechen, ohne den Arbeitsfluss zu behindern.

Darüber hinaus muss die Resilienz der gesamten Lieferkette im Gesundheitswesen substanziell und nachweislich gestärkt werden, denn die Verwundbarkeit von Krankenhäusern erstreckt sich ebenfalls auf die Integrität und Sicherheit der Produkte und Dienstleistungen ihrer zahlreichen Zulieferer. Eine umfassende und kontinuierliche Risikobewertung der gesamten Lieferkette ist daher absolut unerlässlich. Diese Bewertung muss die detaillierte Überprüfung der Cybersicherheitsstandards von Drittanbietern, die Implementierung von Verträgen, die eindeutig definierte Sicherheitsanforderungen festlegen, sowie die Etablierung von Prozessen zur permanenten Überwachung der Lieferketten auf potenzielle Schwachstellen oder erfolgte Kompromittierungen umfassen. Hierbei spielt auch die Fähigkeit zur schnellen Reaktion auf Vorfälle bei Lieferanten eine immer größere Rolle.

Ein weiterer kritischer Erfolgsfaktor ist die kontinuierliche Investition in qualifiziertes Personal und der Aufbau einer tief verwurzelten, proaktiven Sicherheitskultur. Angesichts des eklatanten Fachkräftemangels im hochspezialisierten Segment der Cybersicherheit müssen Gesundheitseinrichtungen verstärkt in die systematische Aus- und Weiterbildung ihrer eigenen Mitarbeiter investieren. Eine proaktive Sensibilisierung für die ständig neuen Formen von Phishing-Angriffen, Social Engineering-Taktiken und den sicheren Umgang mit IT-Ressourcen kann die menschliche Fehlerquote signifikant reduzieren und die Mitarbeiter effektiv zur ersten Verteidigungslinie gegen Cyberbedrohungen ausbilden.

> DIE EINFÜHRUNG ADÄQUATER SCHUTZMASSNAHMEN UND EINES EFFEKTIVEN RISIKOMANAGEMENTS IST KÜNFTIG NICHT MEHR NUR SACHE CHRONISCH UNTERFINANZIERTER IT-ABTEILUNGEN, SONDERN PFLICHT UND PRIORITÄT AUF C-LEVEL.
>
> **Uwe Gries, Country Manager DACH, Stormshield SAS, www.stormshield.com/de**

Vom Ausnahmezustand zur strategischen Priorität

All diese Maßnahmen mögen auf den ersten Blick überfordernd erscheinen – das Ziel einer umfassenden Absicherung wirkt nahezu unerreichbar. Doch die kommende EU-NIS2-Richtlinie, die voraussichtlich Ende Oktober 2025 durch das NIS2-Umsetzungs- und Cybersicherheitsstärkungsgesetz (NIS2UmsuCG) in deutsches Recht überführt wird, verankert die Verantwortung für Cybersicherheit explizit in der Führungsebene – einschließlich der Geschäftsleitung. Damit wird Cybersicherheit zur unternehmerischen Kernaufgabe: Die Einführung adäquater Schutzmaßnahmen und eines effektiven Risikomanagements ist künftig nicht mehr nur Sache chronisch unterfinanzierter IT-Abteilungen, sondern Pflicht und Priorität auf C-Level.

Es bleibt zu hoffen, dass die NIS2-Vorgaben einen proaktiven, ganzheitlichen Sicherheitsansatz fördern, der die Resilienz der Branche gegenüber wachsenden Bedrohungen nachhaltig stärkt. Denn auf passende technische Lösungen für die Gewährleistung maximaler Absicherung und Gesetzeskonformität können das Gesundheitswesen und KRITIS allgemein jederzeit zugreifen.

Uwe Gries

Phishing als Türöffner

WIE TRADITIONELLE ANGRIFFSMETHODEN DEN WEG FÜR MODERNE KI-BASIERTE SICHERHEITSRISIKEN EBNEN

Phishing ist nach wie vor eine der hartnäckigsten und wirkungsvollsten Methoden, die Cyberkriminelle einsetzen. Allein im Jahr 2024 hat Darktrace mehr als 30,4 Millionen Phishing-Angriffe registriert. Besonders besorgniserregend ist, dass rund 70 Prozent dieser Angriffe traditionelle Sicherheitsmechanismen umgehen konnten. Während Unternehmen zunehmend auf KI setzen, um ihre Produktivität zu steigern, ist es wahrscheinlich, dass auch Angreifer KI-gestützte Werkzeuge nutzen, um ihre Angriffsmethoden zu verbessern. Laut dem „State of AI in Cybersecurity Report 2025" fürchten 93 Prozent der deutschen Firmen, dass KI-gesteuerte Cyberangriffe in den nächsten ein bis zwei Jahren erheblichen Schaden anrichten könnten. Diese Entwicklung stellt klassische Erkennungsmodelle vor Herausforderungen und macht adaptive, risikobasierte Sicherheitsstrategien notwendig, die selbst KI integrieren. Phishing dient hier als ein gutes Beispiel, um zu verstehen, wie sich Cyberbedrohungen im Zeitalter der KI verändern.

Wie Angreifer generative KI für ihre Angriffe nutzen

Phishing-Mails werden immer raffinierter: Zwar gibt es noch schlecht gemachte Nachrichten, aber Cyberkriminelle setzen zunehmend auf gezielte und kontextbezogene Kommunikation. Darktrace verzeichnete von Januar bis Februar 2023 bei tausenden E-Mail-Kunden einen Anstieg neuartiger Social-Engineering-Angriffe um 135 Prozent – zeitgleich mit der breiten Verfügbarkeit von generativen KI-Tools wie ChatGPT.

EINE ERFOLGREICHE VERTEIDIGUNGSSTRATEGIE HÖRT NICHT BEI DER E-MAIL-SICHERHEIT AUF.

Dr. Beverly McCann, Director of Product, Darktrace, www.darktrace.com

Generative KI ermöglicht es Angreifern, realistisch wirkende und skalierbare Phishing-Inhalte zu erstellen, wodurch herkömmliche Filter, die auf bekannten Angriffsmustern basieren, weniger effektiv sind. Diese Angriffe täuschen oft vor, von vertrauenswürdigen Marken zu stammen, oder setzen auf Emotionen wie Dringlichkeit oder Angst. Dabei werden auch legitime Plattformen als Angriffswerkzeuge missbraucht, sodass die Phishing-Versuche in vertrauten digitalen Umgebungen verborgen werden. Beispiele sind aktuelle Kampagnen, die sich hinter Namen wie QuickBooks, WeTransfer oder Microsoft Teams verstecken. Viele solcher Phishing-Mails versuchen, die Opfer auf Webseiten zu locken, die Zugangsdaten abgreifen und schädliche Software einschleusen.

Wie ausgeklügeltes Phishing Unternehmen täuscht

Ein anschauliches Beispiel ist „FlowerStorm", eine Phishing-as-a-Service-Plattform, die für ihre professionelle Vorgehensweise bekannt ist. Sie imitiert Microsoft-365-Anmeldeseiten, sammelt Zugangsdaten und Multi-Faktor-Authentifizierungstoken und kann sogar Angriffe „in Echtzeit" zwischen Nutzer und Dienst durchführen. Das zeigt, dass Phishing längst von opportunistischen Betrugsversuchen zu komplexen, skalierbaren Angriffssystemen geworden ist.

Solche Kampagnen sind hochprofessionell: Angreifer kopieren legitime Login-Seiten, sammeln MFA-Tokens und verzichten auf auffällige Links oder Anhänge. Das erschwert klassische, regelbasierte Erkennungssysteme. Stattdessen wird es immer wichtiger, feine Anomalien in Kommunikationsmustern, Zeitpunkten und Verhaltensweisen zu erkennen.

Zudem setzen Angreifer zunehmend darauf, unauffällig zu bleiben. Sie nutzen vertrauenswürdige Kanäle und bedienen sich legitimer Werkzeuge und Prozesse – ein Vorgehen, das als „living off the land" bekannt ist. Das macht es notwendig, Sicherheitssysteme zu entwickeln, die tiefer gehen als oberflächliche Indikatoren.

MEHR WERT
State of AI in Cybersecurity Report 2025

Wie KI eine durchgängige Bedrohungserkennung ermöglicht

Phishing ist oft nur der erste Schritt – Angreifer verfolgen meist weitergehende Ziele wie das Ausspähen von Daten oder das Bewegen innerhalb des Netzwerks. Mehrschichtige, KI-gestützte Abwehrsysteme können diese komplexen Abläufe erkennen und in Echtzeit darauf reagieren. Dafür müssen sie das gesamte digitale Umfeld – E-Mails, Netzwerkverkehr, Endgeräte, Cloud-Dienste, Nutzerverhalten und Identitätsdaten – permanent analysieren. Die besten KI-Systeme arbeiten dabei koordiniert, um komplexe Angriffsketten zu entschlüsseln, die verschiedene Bereiche betreffen.

KI unterstützt zudem Sicherheitsexperten, die oft mit einer Flut von Warnungen kämpfen. Sie hilft, falsche Alarme zu reduzieren, priorisiert Vorfälle nach Schwere und kann in manchen Fällen sogar automatisch Gegenmaßnahmen einleiten. So bleiben Analysten mehr Zeit für wirklich kritische Fälle.

Der große Vorteil von KI-basierten Systemen liegt darin, dass sie scheinbar kleine Auffälligkeiten in einen größeren Zusammenhang setzen – etwa zeitliche Unstimmigkeiten, ungewöhnliches Verhalten oder merkwürdige Zugriffe. Das schafft mehr Transparenz und ermöglicht gezieltere Reaktionen.

Praktische Umsetzung einer KI-gestützten Phishing-Abwehr

Eine erfolgreiche Verteidigungsstrategie hört nicht bei der E-Mail-Sicherheit auf. KI-Schutz sollte alle wichtigen Bereiche abdecken: Netzwerk, Endgeräte, Cloud, Identitätsmanagement und Verhaltensanalysen. Die fortschrittlichsten Systeme passen sich dabei individuell an die jeweilige digitale Umgebung an, anstatt sich nur auf vorgefertigte Regeln zu verlassen.

Ein guter Einstieg ist, KI-basierte Werkzeuge in die E-Mail-Infrastruktur zu integrieren – denn Phishing ist der häufigste Angriffsweg. Von dort aus kann die Abdeckung nach und nach auf das gesamte IT-Ökosystem ausgeweitet werden. Wichtig ist auch, die Technik mit soliden internen Abläufen und regelmäßiger Schulung der Mitarbeitenden zu kombinieren. Nur so entsteht echte Resilienz gegenüber den immer raffinierteren Bedrohungen.

Warum Prävention heute wichtiger ist als Reaktion

Es zeigt sich immer deutlicher: Proaktive Prävention ist wichtiger als reaktives Handeln. In einer von KI beschleunigten Bedrohungslandschaft entscheidet die Reaktionsgeschwindigkeit oft über den Schaden. Klassische Ansätze, die erst nach einem Vorfall eingreifen, reichen nicht mehr aus.

KI-Systeme ermöglichen eine Echtzeit-Erkennung und sofortige Gegenmaßnahmen, wodurch Verluste und rechtliche Risiken minimiert werden. Sie helfen IT-Teams, weniger „Feuerwehr" zu spielen und stattdessen strategisch zu arbeiten. Durch intelligente Automatisierung und Kontextanalysen verbessern sie die langfristige Sicherheit spürbar.

Phishing ist nur der Anfang – intelligente KI-Abwehr ist die Zukunft

Mit zunehmender Komplexität der digitalen Welt stoßen herkömmliche Sicherheitsmodelle an ihre Grenzen. Phishing zeigt, wie moderne Cyberbedrohungen funktionieren: hartnäckig, anpassungsfähig und oft unsichtbar für veraltete Tools. Um einen Schritt voraus zu bleiben, müssen Unternehmen auf KI-gestützte Sicherheitskonzepte setzen, die Bedrohungen in Echtzeit verstehen, verknüpfen und bekämpfen. In dieser Zukunft ist nicht nur die Infrastruktur entscheidend – sondern vor allem die Intelligenz dahinter.

Dr. Beverly McCann

der Cybersicherheitsexperten fühlen sich nicht auf die Realität der KI-gestützten Cyber-Bedrohungen vorbereitet

sind sich einig, dass KI-gestützte Cybersicherheitslösungen die Geschwindigkeit und Effizienz von Prävention, Erkennung, Reaktion und Wiederherstellung erheblich verbessern

Q-Day 2030

WIE UNTERNEHMEN SICH VOR QUANTENCOMPUTER-ANGRIFFEN SCHÜTZEN KÖNNEN

Quantencomputer entwickeln sich rasant und stellen eine wachsende Gefahr für klassische Verschlüsselungsmethoden wie RSA oder ECC dar. Unternehmen müssen jetzt in Post-Quantum-Kryptografie investieren, um langfristige Datensicherheit zu gewährleisten.

Doch während Technologieunternehmen ihre Quantencomputer-Systeme immer weiter verbessern, rückt der sogenannte „Q-Day" in greifbare Nähe. Dieser Tag markiert den Moment, an dem leistungsfähige Quantencomputer in den Händen böswilliger Akteure

landen und die gängigen kryptografischen Verfahren, die heute das digitale Rückgrat unserer Gesellschaft bilden, mühelos knacken können. Expertenschätzungen zufolge könnten bereits um das Jahr 2030 Quantencomputer mit kryptografischer Relevanz kommerziell verfügbar werden. Ähnlich wie bei anderen Technologien zuvor, ist auch bei Quantencomputern von wachsender Verbreitung und sinkenden Kosten auszugehen, sodass sie früher oder später auch eine Option für Kriminelle werden.

Diese Prognose basiert auf der rasanten Entwicklung von Quantenprozessoren, deren Qubit-Anzahl und Fehlerkorrektur sich stetig verbessern. Schon heute verfügen Systeme über mehr als 100 Qubits, während für das Knacken gängiger Verschlüsselungen wie RSA-2048 theoretisch etwa 4.000 fehlerkorrigierte Qubits benötigt werden – ein Wert, der im nächsten Jahrzehnt durchaus erreichbar erscheint.

Besonders beunruhigend ist die „Harvest Now, Decrypt Later"-Strategie, bei der staatliche Akteure und kriminelle Organisationen verschlüsselte Daten sammeln, um sie später mit Quantencomputern zu entschlüsseln. Dies bedroht insbesondere sensible Informationen mit langfristigem Wert, wie Geschäftsgeheimnisse, Patentinformationen oder militärische Daten. Unternehmen müssen sich daher schon jetzt die Frage stellen: Welche unserer heutigen verschlüsselten Kommunikation könnte in fünf oder zehn Jahren zum Problem werden?

Asymmetrische Kryptografie im Visier

Gefährdet ist insbesondere die asymmetrische Kryptografie, wo die Beziehung zwischen privatem und öffentlichem Schlüssel über schwer umkehrbare mathematische Operationen hergestellt wird. Mit aktueller Hardware ist es in reeller Zeit nicht möglich, aus einem öffentlichen Schlüssel auf den damit verknüpften aber geheimen privaten Schlüssel zu schließen. Die überlegene Rechenleistung der Quantenrechner könnte diese Grundlage moderner Kryptosysteme zunichte machen – mit drastischen Konsequenzen.

Asymmetrische Kryptografie ist heute allgegenwärtig – auch wenn viele Menschen sie kaum bewusst wahrnehmen. Sie bildet die Grundlage für sichere Verbindungen im Internet (HTTPS) und schützt die Kommunikation in Messenger-Diensten wie WhatsApp durch Ende-zu-Ende-Verschlüsselung. Auch digitale Nachweise, wie sie künftig in der von der EU geplanten ID-Wallet gespeichert werden sollen, basieren auf diesem Prinzip. Dabei können Inhalte mit einem öffentlichen Schlüssel überprüft werden, während nur befugte Stellen mit entsprechenden privaten Schlüsseln zur Ausstellung berechtigt sind. Ebenso

DER ÜBERGANG ZUR QUANTENRESISTENTEN KRYPTOGRAFIE IST KOMPLEX UND ZEITAUFWÄNDIG. UNTERNEHMEN SOLLTEN NICHT WARTEN, BIS DER Q-DAY DA IST – DANN IST ES ZU SPÄT.

Dr. Michael Osborne, CTO, IBM Quantum Safe, www.ibm.com/quantum

UNTERSCHIEDLICHE BEDROHUNGSWEISEN

Quantencomputer bedrohen sowohl asymmetrische als auch symmetrische Kryptografie, allerdings auf unterschiedliche Weise:

1. Asymmetrische Kryptografie (beispielsweise RSA, ECC):
Sie basiert auf schwer lösbaren mathematischen Problemen wie der Faktorisierung großer Zahlen oder dem diskreten Logarithmus. Quantencomputer können mit Shor's Algorithmus diese Probleme in polynomialer Zeit lösen, wodurch private Schlüssel aus öffentlichen berechnet werden können. Das macht diese Verfahren praktisch nutzlos, sobald leistungsfähige Quantencomputer verfügbar sind.

2. Symmetrische Kryptografie (etwa AES):
Diese Verfahren sind weniger stark betroffen, da Quantencomputer hier „nur" mit Grover's Algorithmus einen quadratischen Geschwindigkeitsschub bieten. Das bedeutet, ein 256-Bit-Schlüssel hat die effektive Sicherheit eines 128-Bit-Schlüssels – was aber immer noch als sicher gilt. Dennoch erfordert das ein Anheben der Schlüssellängen, um langfristig Sicherheit zu gewährleisten.

kommt asymmetrische Kryptografie bei qualifizierten elektronischen Signaturen zum Einsatz. Ein Angriff auf die dafür verwendeten Zertifikate könnte digitale Verträge kompromittieren, beziehungsweise wertlos machen.

Symmetrische Verschlüsselung und Quantenangriffe

Auch wenn asymmetrische Kryptografie am stärksten gefährdet ist, bleibt selbst symmetrische Verschlüsselung nicht vollständig unangetastet. Zwar erfordert das Knacken symmetrischer Verfahren wie AES durch Quantenalgorithmen (etwa Grover's Algorithmus) nur eine quadratische Geschwindigkeitssteigerung – im Vergleich zur exponentiellen bei asymmetrischen Algorithmen –, dennoch bedeutet dies, dass beispielsweise AES-128 effektiv nur noch eine Sicherheit von 64 Bit bietet. AES-256 gilt derzeit als ausreichend sicher im Post-Quantum-Zeitalter.

Post-Quantum-Kryptografie

Die gute Nachricht: Die Kryptografie ist der Bedrohung nicht schutzlos ausgeliefert. Bereits heute werden quantenresistente kryptografische Verfahren entwickelt und standardisiert. Das National Institute of Standards and Technology (NIST) hat im Juli 2022 die ersten vier quantenresistenten kryptografischen Standards ausgewählt, darunter CRYSTALS-Kyber für den Schlüsselaustausch und CRYSTALS-Dilithium für digitale Signaturen. Große Technologieunternehmen wie Google, Microsoft und IBM implementieren bereits Post-Quantum-Kryptografie (PQC) in ihre Produkte und Cloud-Dienste. Die Europäische Union fördert mit dem Projekt „OpenQKD" die Entwicklung von Quantenschlüsselverteilung (QKD), einer komplementären Technologie zur mathematikbasierten Post-Quantum-Kryptografie.

So gelingt die PQC-Migration

Unternehmen sollten jetzt handeln, um ihre Daten langfristig zu schützen. Der Umstieg beginnt mit einem umfassenden kryptografischen Inventar, bei dem alle kryptografischen Anwendungen im Unternehmen identifiziert und dokumentiert werden – von Verschlüsselungsmethoden in Netzwerkprotokollen über Authentifizierungssysteme bis hin zu digitalen Signaturverfahren. Im nächsten Schritt folgt eine Risikobewertung, bei der Unternehmen identifizieren, welche Daten auch in zehn Jahren noch sicher sein müssen und welche Systeme aufgrund langer Erneuerungszyklen zuerst migriert werden sollten.

Als Übergangsmaßnahme empfiehlt sich die hybride Kryptografie, bei der klassische und quantenresistente Verfahren parallel eingesetzt werden. Dies bietet Schutz gegen Quantenangriffe, ohne bewährte klassische Algo-

rithmen sofort aufzugeben. Bei den Unternehmen, die bereits an einer PQC-Migration arbeiten, bevorzugen die meisten (63 Prozent) diesen hybriden Ansatz, wie eine Umfrage von Utimaco unter mehr als 200 Organisationen in den USA, dem Vereinigten Königreich und Deutschland zeigt. Führende Technologieunternehmen nutzen bereits hybride TLS-Verbindungen in Testumgebungen.

PQC in der Praxis

Die Migration zu quantenresistenten Algorithmen erfordert zudem eine strukturierte Planung mit Aktualisierung der Public-Key-Infrastruktur, Einführung kryptografisch agiler Systeme und Berücksichtigung der höheren Rechenanforderungen. Unternehmen sollten darauf achten, dass Hardware-Anbieter oder Kryptografie-Dienstleister kryptoagil sind, sodass sie bei Bedarf neue, quantensichere Algorithmen auf ihre Geräte aufspielen können. Nicht zuletzt ist es wichtig, in Mitarbeiter-Know-how zu investieren, da sich der Fachkräftemangel im Bereich Quantensicherheit weiter verschärfen wird.

Quantenschlüsselverteilung (QKD)

Quantum Key Distribution (QKD), eine Methode des Schlüsselaustauschs, die sich selbst Quanteneffekte zunutze macht, möchten lediglich 12 Prozent der befragten Unternehmen als zusätzliche Sicherheitsmaßnahme implementieren. Gründe dafür könnten der Bedarf an neuer, hochspezialisierter Hardware sowie physikalische Einschränkungen der Übertragungswege sein. PQC lässt sich hingegen sehr gut in bestehende Systeme integrieren.

Regulierung für Post-Quantum-Sicherheit

Auch regulatorisch zeichnet sich Handlungsbedarf ab. Behörden wie das BSI oder die NSA fordern bereits jetzt zur Vorbereitung auf PQC auf. Die EU plant mit der eIDAS-2-Verordnung und der NIS2-Richtlinie konkrete Anforderungen an kryptografische Resilienz. Unternehmen, die frühzeitig PQC-Strategien integrieren, können regulatorische Anforderungen proaktiv erfüllen und sich rechtlich absichern.

Frühzeitige Post-Quantum-Strategie nutzen

Die Vorbereitung auf den Q-Day ist nicht nur eine technische Notwendigkeit, sondern kann auch zum Wettbewerbsvorteil werden. Unternehmen, die frühzeitig in quantenresistente Technologien investieren, können das Vertrauen ihrer Kunden stärken, regulatorische Anforderungen frühzeitig erfüllen, langfristige Datensicherheit gewährleisten und sich als Innovationsführer positionieren. Die Quantencomputer-Revolution bringt nicht nur Risiken, sondern auch Chancen. Wer jetzt handelt, wird die digitale Transformation sicher meistern – und vielleicht sogar gestärkt aus ihr hervorgehen.

Ulrich Parthier

FÜNF KONKRETE HANDLUNGS-EMPFEHLUNGEN FÜR UNTERNEHMEN:

- Kryptografisches Inventar erstellen
- Risikobewertung und Priorisierung durchführen
- Hybride Kryptografie implementieren
- Quantenresistente Infrastruktur aufbauen
- In Mitarbeiter-Know-how investieren

IMPRESSUM

Herausgeber: Ulrich Parthier (08104-6494-14)

Geschäftsführer: Ulrich Parthier, Vasiliki Miridakis

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:
Christian Albrecht, Lars Becker, Sebastian von Bomhard, Andrei Florescu, Fabian Glöser, Uwe Gries, Stefan Karpenstein, Dennis-Kenji Kipker, Dr. Beverly McCann, Carina Mitzschke, Silvia Parthier, Ulrich Parthier, Patrick Schäfers, Stephan Schweizer, Stefan Tiefel, 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. 32.
Preisliste gültig ab 1. Oktober 2024.

Mediaberatung & Content Marketing-Lösungen
it management | it security | it daily.net:
Kerstin Fraenzke, 08104-6494-19, fraenzke@it-verlag.de
Karen Reetz-Resch, Home Office: 08121-9775-94,
reetz@it-verlag.de
Marion Mann, +49 152-3634 1255, mann@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.

CYBERSICHERHEIT AM SCHEIDEWEG

GRÜNDE FÜR DAS CYBERSICHERHEITS-DILEMMA IN UNTERNEHMEN

2024 war ein Rekordjahr für Cyberangriffe. Der CrowdStrike Vorfall, der weltweit etwa 8,5 Millionen Windows Systeme zum Absturz brachte, führte zu Ausfällen in verschiedensten Branchen – vom Finanzwesen über den Flugverkehr bis hin zu Industrieunternehmen. Derartige Ausfälle sind unvermeidlich, aber wie gut sind wir darauf vorbereitet?

Unternehmen fällt es schwerer, sich von Cyberangriffen zu erholen, als sie glauben. Die durchschnittliche erwartete Wiederherstellungszeit liegt bei 5,85 Monaten. In der Praxis dauert es aber mit 7,34 Monaten knapp 25 % länger.

Um genauere Einblicke in den Umgang mit wichtigen Cybersicherheitsthemen in Unternehmen zu gewinnen und zu erfahren, in welche Richtung sich die Branche entwickelt, hat Fastly im September 2024 gemeinsam mit dem Marktforschungsunternehmen Sapio 1800 IT-Entscheider mit Einfluss auf die Cybersicherheit befragt. Dieser Bericht liefert tiefe Einblicke in die Herausforderungen, vor denen Unternehmen im Bereich Cybersicherheit stehen, und wie sie diese bewältigen wollen.

WHITEPAPER DOWNLOAD

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

Cyberkriminelle überall

da tut Hilfe not

Mehr Infos dazu im Printmagazin

itsecurity

und online auf www.it-daily.net


itsa
HOME OF
IT SECURITY
Jetzt mehr erfahren!
7. – 9. Oktober 2025
Nürnberg, Germany
itsa365.de/itsa-expo-besuchen
NÜRNBERG MESSE