it management

Der Motor für Innovation
November/Dezember 2025

INKLUSIVE 48 SEITEN
it security



DIE WORKPLACE REVOLUTION

Vom Drucker zur digitalen Transformation

Michael Raberger, Ricoh Deutschland GmbH

THOUGHT LEADERSHIP

AB SEITE 16
Natuvion

Aagon
Treiber updaten ohne WSUS
ab Seite 20

AI-AGENTS UND AI-BUDDYS

Vom Blackbox-Risiko zum digitalen Assistenten

FINANCE SPEZIAL

Cognitive Operations, E-Invoicings & Agentic AI

www.it-daily.net

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

Aagon

DriveLock

easy by conrizon

Impossible Cloud

Panasonic CONNECT TOUGHBOOK

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



JAHRESENDSPURT

LIEBE LESERINNEN UND LESER,

ja, es ist bereits wieder November und wie jedes Jahr um diese Zeit, konzentriert sich alles auf zwei große Themen: Oh nein! Weihnachten steht an, was tun, was schenken oder wohin flüchten? Das zweite Thema? Ganz klar, die Planung für das kommende Jahr. Bei uns im Verlag ist die Themen- und Terminplanung zum Glück schon durch, wobei das nicht heißt, dass das Thema damit beendet ist. Aber grundsätzlich existiert schon einmal ein Rahmen.

In vielen Unternehmen stehen zusätzlich die Budgetplanung und die strategische Weichenstellung an. Die Entscheidungen, die IT-Verantwortliche jetzt treffen, bestimmen nicht nur, welche Projekte 2026 realisiert werden sollten – sie definieren auch, wie abhängig oder unabhängig Unternehmen in den kommenden Jahren agieren können.

Digitale Souveränität ist längst kein politisches Schlagwort mehr, sondern eine wirtschaftliche Notwendigkeit. Das hat die Störung der Amazon Web Services Mitte Oktober gezeigt: wenn eine der weltgrößten Cloud-Plattformen ausfällt, geht plötzlich nicht mehr viel – unabhängig davon, wie gut die eigene IT aufgestellt ist. Die Frage ist nicht mehr, ob Unternehmen sich mit Vendor Lock-ins, Datenhoheit und technologischer Autonomie auseinandersetzen müssen, sondern wie schnell. Wer heute Budgets für Cloud-Infrastrukturen, KI-Plattformen oder ERP-Systeme vergibt, sollte genau prüfen: Welche Abhängigkeiten schaffe ich damit? Mehr zu diesem Thema, aber auch jede Menge Informationen zum Thema Storage, KI und Finanzen lesen Sie in dieser Ausgabe.

Herzlichst



Carina Mitzschke | Redakteurin it management & it security





INHALT

COVERSTORY

10 **Die Workplace Revolution**
Vom Drucker zur digitalen Transformation

THOUGHT LEADERSHIP

16 **HCM-Transformation**
Expertise und Tools sind entscheidend

18 **Erfolgreich auf SAP HCM für S/4HANA**
Gelungene Zusammenarbeit mit Natuvion

IT MANAGEMENT

20 **Wenn WSUS an seine Grenzen stößt**
Betriebssystem und Treiber updaten ohne WSUS

22 **DNA Data Storage**
Revolution der Langzeitarchivierung und ihre Herausforderungen für die IT-Sicherheit

26 **Object Storage ohne Umwege**
Was der Verzicht auf Tiering bringt

28 **Speichermedien im Umbruch**
Die Zukunft von Daten und Datenspeichern in Zeiten des Quantencomputings

32 **Vom Blackbox-Risiko zum digitalen Assistenten**
Wie AI-Agents und AI-Buddys kontrollierbar bleiben

36 **Mit künstlicher Intelligenz die Zukunft gestalten**
KI, Content & Sicherheit im Fokus

38 **ERP meets KI**
Bundesministerium fördert Entwicklung einer On-Premises-KI-Plattform

40 **Transformationen und Datenmigrationen im SAP-Umfeld**
Agilität als Schlüsselfaktor

42 **So viel KI war noch nie**
STARFACE 10 stellt die Weichen auf Zukunft

44 **Zwischen Laser und Latenz**
Warum eine intelligent zusammengeschaltete Weltraumwirtschaft so wertvoll für die Menschheit ist

Farblich hervorgehobene Artikel sind von der Redaktion als besonders lesenswert empfohlen

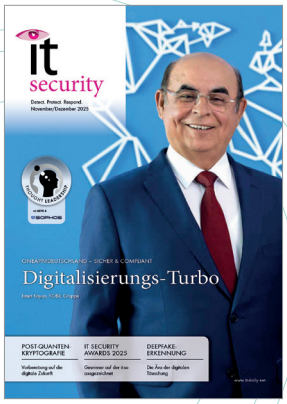




46 **Innovativ statt oversized**
Wie Monitoring wieder bezahlbar wird

48 **Der Weg zur AI-getriebenen und zukunftssicheren IT**
Warum ganzheitliche Transformation mehr ist als Plattform-Migration

50 **AI Factory**
Ein Fließband für KI-Use-Cases



Inklusive 48 Seiten it security

FINANCE SPEZIAL

56 **Grundregeln des E-Invoicings**
Effizientere und transparentere Rechnungsprozesse

58 **Agentic AI im Finanzbereich**
Vom Burger zum Sternemenü

60 **E-Invoicing: Mit dem richtigen Set-up, Fehler vermeiden**
Auf Automatik und Weitblick setzen

62 **Cognitive Operations in der Finanzbranche**
Wie Europa die Industrialisierung kognitiver Workloads anführen kann

65 **DORA und Threat Intelligence**
Von der Vorschrift zur praktischen Resilienz



GUT ZU WISSEN

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

DIGITALE SOUVERÄNITÄT BIS 2030?

ENTSCHEIDER ZWEIFELN

Bis 2030 soll Europa in zentralen Bereichen der Digitalisierung eigenständiger, resilienter und unabhängig sein. Das wird unter dem Begriff „digitale Dekade 2030" zusammengefasst. Doch die Bereitschaft vieler Unternehmen, auf souveräne Lösungen zu setzen, ist nur begrenzt vorhanden. Das zeigt auch die Wire-Umfrage.

Souveränität gibt es nicht zum Nulltarif

Führungskräfte in Europa sind sich der prekären Lage somit bewusst. Warum also setzen sie weiter auf US-Tools?

Zum einen kommt Widerstand aus den eigenen Reihen. Mitarbeiter sind vertraut mit bekannten Tools wie Microsoft Teams oder Zoom und wollen daran festhalten. Datenschutzrisiken sind für 63,2 Prozent der Befragten kein Argument, die bekannten Anwendungen aufzugeben.

Hinzu kommt die technische Abhängigkeit. Die meisten IT-Landschaften werden von US-Software-Suiten dominiert. Für mehr als die Hälfte der Entscheider (57,9 Prozent) ist die Integration souveräner Plattformen in US-dominierte IT-Landschaften daher ein fast unüberwindbares Hindernis.

Wenn Führungskräfte die Notwendigkeit erkennen und handeln wollen, wissen sie oft nicht, welche souveränen Tools auf dem Markt sind. Außerhalb von bestimmten politischen Kreisen werden souveräne Anbieter immer noch als Nischenlösungen angesehen. 36,8 Prozent der Befragten gibt an, schlicht nicht genug Informationen über europäische Tools zu haben, um entscheiden zu können.

Zu guter Letzt stecken die meisten Unternehmen in langfristigen Verträgen mit ihren Dienstleistern und nutzen deren proprietäre Formate auf allen Unternehmensebenen. Mehr als ein Viertel der Entscheider (26,3 Prozent) betont, dass ein Wechsel deshalb keine reine IT-Entscheidung sei, sondern eine, die das gesamte Unternehmen betrifft und politische wie monetäre Folgen mit sich ziehen kann.

Angesichts dieser Hürden überrascht es kaum, dass nur 15,8 Prozent der Befragten glauben, dass Europa bis 2030 echte digitale Souveränität erreichen kann.

„Compliance-Theater": Hemmnis statt Motor

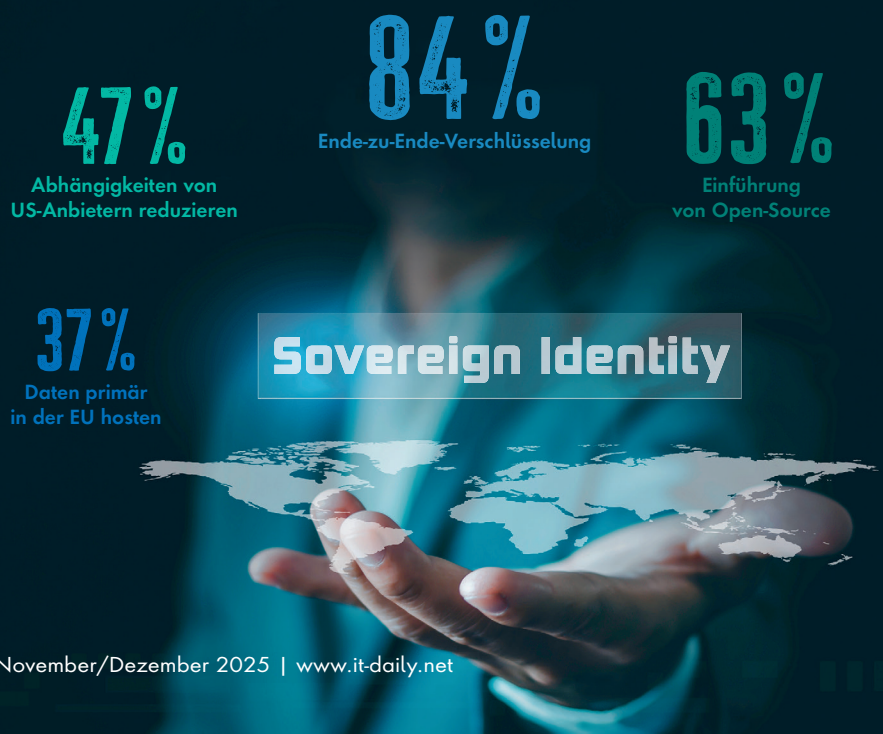
Die EU versucht gegenzusteuern und Unternehmen mit Regulierungen und gesetzlichen Rahmenwerken zu mehr Souveränität zu motivieren. NIS2, DORA, und DSGVO legen zwar eine wichtige Grundlage für mehr Datenschutz und erfordern eine strengere Berichterstattung. Die Einhaltung kommt jedoch mehr einem „Compliance-Theater" gleich, bei dem Unternehmen zwar nach außen hin die Regularien einhalten, aber mit minimalem Einsatz, der kaum Auswirkungen auf die Widerstandsfähigkeit und Unabhängigkeit von Systemen und Anbietern hat.

Die Hoheit über eigene Daten zu behalten, nimmt angesichts der geopolitischen Spannungen an Relevanz zu. Daten-Leaks und Cyberangriffe können Unternehmen und ihre Reputation stark schädigen. Führungskräfte sollten deshalb auf organisatorischer Ebene selbst Weichen stellen, indem sie das Bewusstsein für souveräne Lösungen unter Entscheidern schärfen und Anreize zum Experimentieren schaffen.

www.wire.com

WIE GEHT ECHTE DIGITALE SOUVERÄNITÄT?

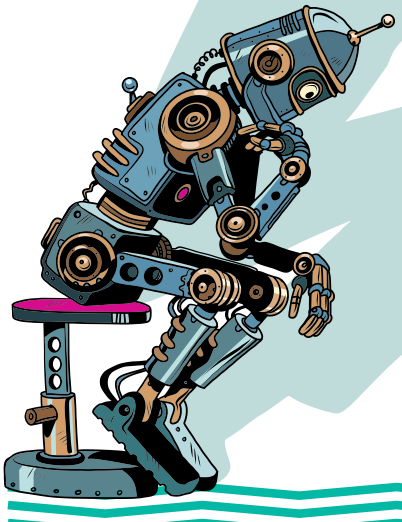
Wo müssten die Prioritäten liegen?



Schatten-KI verhindern

6 TIPPS FÜR SICHERE KI-ANWENDUNGEN

Künstliche Intelligenz ist ein echter Gamechanger – sie ermöglicht Unternehmen neue Services, besseres Kundenverständnis, erhöht die Effizienz, beschleunigt Prozesse und pusht so die Wettbewerbsfähigkeit. Ohne Sicherheit, Kontrolle und klare Regeln geht das allerdings nicht, denn wie jedes andere Werkzeug muss KI mit Verstand eingesetzt werden. Ziellos damit herumzufuchteln, bringt vor allem Ärger. Ein solches Ärgernis ist die so genannte Schatten-KI oder Shadow AI. Darunter versteht man die vom Unternehmen nicht genehmigte – oft dem Unternehmen nicht einmal bekannte – Nutzung von KI-Tools durch Mitarbeiter, bei der nicht selten sensible Informationen, etwa zu Produkten, Firmen-Interna oder sogar Kundendaten, arglos in KI-Lösungen eingegeben werden.



KI-Technologien zukunftssicher etablieren – so geht's!

#1 KI-Einsatz strategisch planen
#2 Mitarbeiter praxisnah schulen
#3 Datensicherheit gewährleisten
#4 Regulatorische Anforderungen zuverlässig einhalten
#5 Zugriffskontrolle gewährleisten
#6 Transparenz & Nachvollziehbarkeit sichern

Gemeinsam den Einstieg schaffen

Ob für Auswertungen, Zusammenfassungen, Präsentationen, Assistenz und vieles mehr: Generative KI verändert den Unternehmensalltag und verbessert Arbeitsschritte. Doch sensible Kundendaten und Interna dürfen nicht unkontrolliert an fremde KI-Modelle übergeben werden. Dennoch wollen und sollen Mitarbeiter KI einfach nutzen und kennenlernen. Das ist möglich, wenn Unternehmen ein paar Punkte beachten und Schritt für Schritt in die KI-Nutzung einsteigen.

www.vier.ai

Webinar

IT-Ausgaben im Griff: Der richtige Toolmix für Observability

Tools strategisch planen.
Langfristig Kosten sparen.
IT-Monitoring optimieren.

USU

Jetzt kostenlos anmelden
Live dabei sein oder
die Aufzeichnung flexibel
On-Demand abrufen.



DATENKLAU IN UNTERNEHMEN

KI- UND QUANTENRISIKEN LEGEN LÜCKEN OFFEN

Die Anforderungen an die Cybersicherheit in deutschen Unternehmen steigen rapide. Das zeigt die aktuelle PwC-Studie „Global Digital Trust Insights 2026", für die Geschäfts- und Technologieverantwortliche aus rund 3.900 Unternehmen weltweit – darunter 262 aus Deutschland – befragt wurden.

Reaktionen auf geopolitische Risiken
Insbesondere die geopolitischen Krisen führen zu einer Verschärfung der Cyberrisiken. Staatliche Akteure und komplexe Angriffsszenarien zwingen Unternehmen dazu, ihre Cyberstrategie zu überdenken. Besonders auffällig: Organisationen in Deutschland setzen dabei zunehmend auf Diversifizierung. 55 Prozent wollen ihr Cyber-Risikomanagement ausbauen, 40 Prozent denken über einen Wechsel des Standorts kritischer Infrastruktur nach. 42 Prozent planen Anpassungen bei Handels- und Betriebspolitik, jeweils 35 Prozent erwägen eine Verlagerung von Geschäftsaktivitäten oder den Wechsel des Sicherheitsanbieters – letzteres deutlich häufiger als international (26 %).

Wie wichtig solche Maßnahmen sind, unterstreichen die Ergebnisse der PwC-Studie: Rund neun von zehn deutschen Unternehmen (89 %) wurden in den vergangenen drei Jahren Opfer von Datendiebstahl oder -missbrauch. Damit liegt Deutschland über dem internationalen Durchschnitt (82 %).

Cyberabwehr unter Druck
In deutschen Unternehmen gibt es bei neuartigen Cyberrisiken deutliche Unsicherheiten, die über das weltweite Niveau hinausgehen: 32 Prozent fühlen sich unzureichend auf Angriffe mithilfe von Quantencomputing vorbereitet (global: 26 %). Auch Attacken auf vernetzte Produkte und Geräte (30 %), cloud-bezogene Risiken (28 %), Datenschutzverletzungen durch Dritte (28 %), Social Engineering (23 %), Kompromittierung der Software-Lieferkette (20 %) und Ransomware (18 %) bereiten deutschen Unternehmen große Sorgen.

Der anhaltende Mangel an Cybertalenten verschärft die Situation zusätzlich. Mehr als die Hälfte der deutschen Befragten (54 %) setzt daher auf KI- und Machine-Learning-Tools, um offene Stellen zu kompensieren.

Künstliche Intelligenz als Chance und Risiko
Die Rolle der Künstlichen Intelligenz wächst – allerdings nicht ohne Risiken. Bereits im vergangenen Jahr berichteten 67 Prozent der Sicherheitsverantwortlichen, dass generative KI die Angriffsfläche für Cyberangriffe deutlich vergrößert hat – dieser Wert bleibt aktuell unverändert. Als besonders kritisch betrachten sie in diesem Zusammenhang KI-basierte Malware (53 %), Angriffe auf die Lieferkette (51 %) und Deepfakes (41 %). Als Hindernisse für den KI-Einsatz sehen die Befragten mangelndes Wissen (44 %), unklare Verantwortlichkeiten (41 %) und fehlende Budgetpriorität (38 %). Dennoch will ein Viertel der deutschen Befragten gezielt agentische KI zur Strategie- und Geschäftsentwicklung einsetzen – mehr als im internationalen Vergleich (19 %).

Quantencomputing
Die Studie beleuchtet erstmals auch die Risiken durch Quantencomputing. Während die Unternehmen beim Einsatz von KI bereits wichtige Schritte gehen, gibt es hier großen Nachholbedarf. So hat mehr als die Hälfte der deutschen Befragten (51 %) noch nicht begonnen, quantenresistente Maßnahmen umzusetzen. Nur 20 Prozent implementieren bereits konkrete Lösungen. Die größten Hürden sind fehlendes Know-how und geringe Ressourcen (46 %), mangelnde technische Expertise (42 %) und Defizite bei Verschlüsselung und Anonymisierung (32 %).

www.pwc.com

Neue Karrierewege?

„INCOME STACKING“ STATT FESTANSTELLUNG

Ein schwächelnder Arbeitsmarkt und Veränderungen bei der Einstellung von Berufseinsteigern führen dazu, dass sich die Gen Z zunehmend von traditionellen Karrierewegen abwendet und stattdessen auf mehrere Einkommensquellen setzt: ein Trend, der als „Income Stacking“ bekannt ist. Ziel ist es, finanzielle Sicherheit in unsicheren Zeiten zu erreichen, wie aus der von Fiverr veröffentlichten Next Gen of Work-Umfrage hervorgeht.

52 Prozent der befragten deutschen Mitglieder der Generation Z und Gen Alpha halten mehrere Einkommensquellen für unerlässlich, um finanziell abgesichert zu sein. Angesichts der wachsenden wirtschaftlichen Unsicherheit verspüren viele junge Berufstätige Panik und Misstrauen gegenüber traditionellen Festanstellungen mit nur einer Gehaltsquelle. Infolgedessen wenden sie sich zunehmend Nebenjobs und nicht-traditionellen Beschäftigungsformen zu. 40 Prozent sind bereits freiberuflich tätig oder planen, sich durch Freiberuflichkeit ein zusätzliches Einkommen zu sichern. 60 Prozent glauben, dass traditionelle Beschäftigungsverhältnisse in Zukunft überholt sein werden.

Zukunftssorgen

Analog zum Konzept der Money Dysmorphia, bei der eine Person ihren finanziellen Status verzerrt wahrnimmt und sich finanziell ärmer oder schlechter gestellt fühlt, als es der Realität entspricht, bildet die Studie auch die finanziellen Sorgen der Gen Z rund um ihre berufliche Zukunft ab. Ob steigende Mieten, Studienkredite oder sogenannter „performance pressure“ in sozialen Medien, für 44 Prozent ist die größte berufliche Angst, nicht genug Geld zum Leben zu verdienen. Rund ein Viertel fürchtet wiederum, in einem Beruf zu landen, der sie nicht erfüllt.

de.fiverr.com



NEXT GEN OF WORK

Die jährliche Umfrage, durchgeführt in Zusammenarbeit mit Censuswide, befragte über 1.000 Personen der Generation Z und Generation Alpha in Deutschland und 12.000 Personen weltweit zur Zukunft der Arbeit. Sie zeigt auf, wie sich junge und kommende Generationen an die sich verändernden wirtschaftlichen Rahmenbedingungen anpassen.

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



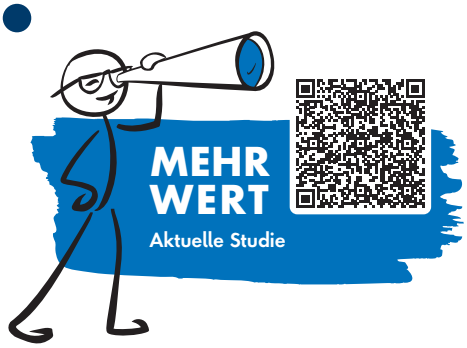
Die Workplace Revolution

VOM DRUCKER ZUR DIGITALEN TRANSFORMATION

Seit 2022 führt Michael Raberger Ricoh Deutschland durch einen strategischen Wandel. Das Unternehmen positioniert sich heute als Anbieter umfassender Workplace-Lösungen. Im Interview spricht er mit Carina Mitzschke, Redakteurin it management, über aktuelle Markttrends, erklärt die wachsende Nachfrage nach hybriden Arbeitsmodellen und beschreibt, wie sich traditionelle Office-Technologien zu Bausteinen digitaler Transformationsstrategien entwickeln.

Carina Mitzschke: *Herr Raberger, Sie sind nun seit drei Jahren CEO von Ricoh Deutschland. Welche strukturellen Veränderungen haben Sie in dieser Zeit vorangetrieben, um das Unternehmen zukunftsfähig aufzustellen?*

Michael Raberger: Ricoh Deutschland ist heute ein anderes Unternehmen als noch vor zehn Jahren, als wir den Transformationsprozess zur Digital Service Company aktiv gestartet haben. Neben unserem Printgeschäft haben wir in den letzten Jahren die Bereiche Workplace Experience und Prozessautomatisierung konsequent erweitert. Heute sind wir einer der führenden Anbieter für AV-UCC und Managed Workplace Services, der Bereich Process Automation Software ist 2024 um gut 30 Prozent gewachsen und dieser Wachstumstrend führt sich auch in diesem Jahr fort. Unser MPS-Angebot zählt zu den besten am Markt, und wir haben das branchenweit breiteste Portfolio zur Geschäftsoptimierung. Ganz wichtig sind unsere Mitarbeitenden: Sie prägen die moderne Organisations- und Innovationskultur bei Ricoh, intern wie extern. Das ist das Fundament für nachhaltigen Geschäftserfolg, Resilienz und Wachstum.



Carina Mitzschke: *Wie haben sich die Anforderungen Ihrer Kunden an digitale Arbeitsplatzlösungen in den letzten drei Jahren konkret verändert und welche Arbeitnehmeransprüche sollten Unternehmen berücksichtigen?*

Michael Raberger: Beim Digital Mindset der Führungskräfte hat sich in den letzten Jahren spürbar etwas bewegt. Der Wille zur Digitalisierung ist vielerorts vorhanden - allerdings bremsen die gesamtwirtschaftlichen Rahmenbedingungen und eine häufig fehlende Transformationsstrategie die Umsetzung. Aktuell erleben wir hier Bewegung: Investitionsanreize in die Modernisierung veralteter Infrastruktur, der Handlungsdruck beim Fachkräftemangel sowie die Ansprüche von Mitarbeitenden an Hybrid Work und moderne Arbeitsumgebung fördern das Investitionsklima für IT, Office und Prozessautomatisierung.

Das gilt für alle Regionen in Deutschland, für den Mittelstand, Behörden und Großkonzerne gleichermaßen. Unsere aktuelle Ricoh-Studie untermauert das: 44 Prozent der Unternehmen planen eine Modernisierung in eine attraktivere Büroausstattung, jeder vierte Angestellte vermisst bessere Technik im Büro, um dadurch mehr Zeit für andere, strategisch wichtige Aufgaben zu haben.

Wir bieten für diese steigende Nachfrage passgenaue Lösungen: von Einsparungen für Unternehmen durch optimierte Managed Print Services über skalierbare Cloudlösungen im Dokumentenmanagement bis hin zum Einsatz von KI zur Automatisierung digitaler Prozesse. Mit Ricoh IDX unterstützen wir Unternehmen außerdem bei der Umsetzung gesetzlicher Vorgaben wie der E-Rechnung. Auch hybride Arbeitsumgebungen und skalierbare „Workplace as a Service"-Lösungen sind ein großes Investitionsthema. Nicht zuletzt spielt auch das Thema Nachhaltigkeit eine zentrale Rolle – ein Bereich, in

dem Ricoh seit Jahren Maßstäbe setzt.

Carina Mitzschke: *Der Begriff „New Work" hat sich stark gewandelt. Wie definieren Sie heute modernes Arbeiten?*

Michael Raberger: Für Ricoh steht im Mittelpunkt aller Lösungen die Bereitstellung und Integration eines digitalen Arbeitsplatzes, der Menschen miteinander vernetzt, Agilität fördert und das Potenzial eines Unternehmens freisetzt. Für mich ist der Arbeitsplatz mehr als nur ein physischer Raum, er ist ein Ort der Zusammenarbeit, Innovation und Produktivität. Smarte Technologie ermöglicht cloudbasierte Kollaboration und optimierte Prozesse, um Arbeitsabläufe effizienter und produktiver zu gestalten. Die Rückkehr ins Büro ist ein unternehmerisches Ziel, das viele Arbeitgeber ganz vorn auf ihre Agenda setzen – dafür braucht es eine optimale Employee Experience, die Interaktion und Fokus bei der Arbeit sinnvoll vereint.

Carina Mitzschke: *Welche technologischen Hürden mussten Ihre Kunden beim Übergang zu hybriden Arbeitsmodellen überwinden – und welche Rolle spielte dabei die IT-Infrastruktur? Wie adressiert das Ricoh-Portfolio strukturelle IT-Barrieren konkret?*

Michael Raberger: Die Hürden sind bekannt: Fragmentierte IT-Systeme sind in vielen Unternehmen historisch gewachsen. Insellösungen und rein lokale (On-Premises-)Systeme schränken die Flexibilität beim Daten- und Anwendungszugriff erheblich ein. Darüber hinaus spielen Sicherheitsbedenken und Compliance-Richtlinien an hybrides Arbeiten eine zentrale Rolle. Wir adressieren genau das: Unterstützung bei der strukturierten Cloud-Migration, Implementierung spezifischer Compliance-Lösungen, sicherer Collaboration-Tools sowie Remote Device Management und Support.

Carina Mitzschke: *Welche Punkte sind für IT-Entscheider bei der Arbeitsplatzoptimierung am wertvollsten und warum?*

Michael Raberger: Es geht in erster Linie darum, Effizienz, Sicherheit und Mitarbeiterzufriedenheit sicherzustellen – und das im Kontext hybrider Arbeitswelten. Ricoh leistet hier einen konkreten Beitrag: durch Managed Print Services, die digitale Entlastung von Fachkräften, den Einsatz langlebiger Technologien zur Reduzierung des CO -Footprints und durch moderne, skalierbare Arbeitsplatzkonzepte. Büroräumlichkeiten sind heute häufig nur noch halb so groß, dafür aber doppelt so ansprechend – und damit ein echter Faktor für Arbeitgeberattraktivität und Produktivität.

Carina Mitzschke: *Ricoh bezeichnet Multifunktionsdrucker als „ersten Schritt zur digitalen Transformation". Welche konkreten Digitalisierungsstrategien entwickeln IT-Entscheider ausgehend von dieser Basis-Infrastruktur? Wie unterstützen beispielsweise KI-optimierte Digitalisierungsprozesse IT-Abteilungen dabei, ihre Dokumentenmanagement-Strategien zu skalieren?*

> FÜR RICOH STEHT IM MITTELPUNKT ALLER LÖSUNGEN DIE BEREITSTELLUNG UND INTEGRATION EINES DIGITALEN ARBEITSPLATZES, DER MENSCHEN MITEINANDER VERNETZT, AGILITÄT FÖRDERT UND DAS POTENZIAL EINES UNTERNEHMENS FREISETZT.
>
> **Michael Raberger, CEO, Ricoh Deutschland GmbH, www.ricoh.de**



Michael Raberger: Für viele Unternehmen und Behörden ist die Digitalisierung papierbasierter Prozesse der erste Schritt zur Automatisierung. Moderne Multifunktionsdrucker (MFPs) werden zu zentralen Schnittstellen digitaler Strategien – sie integrieren Cloud-Dienste wie Microsoft 365, DMS-/ECM-Systeme wie DocuWare oder SharePoint und unterstützen dank KI das Predictive Management sowie den Aufbau digitaler Akten, automatisiertes Routing und Freigabeprozesse. Ein spannendes Beispiel ist unsere neueste MFP-Generation, die jetzt in Deutschland gelauncht wurde und und Bürodigitalisierung so einfach wie nie zuvor macht. Dieses System ist das erste seiner Art, das anstelle eines herkömmlichen Dokumenteneinzugs mit einem vollwertigen Hochleistungs-Scanner ausgestattet ist: Verschiedene Formate von sehr dünnem Papier bis Plastikkarte können gleichzeitig digital erfasst, klassifiziert und archiviert werden. Das ermöglicht eine völlig neue Qualität bei der Digitalisierung.

? **Carina Mitzschke:** *Mit der Ricoh-Tochter DataVision setzen Sie in Bezug auf Hybrid Work neue Maßstäbe. Welche Synergien schaffen Sie für eine ganzheitliche Workplace-Transformation?*

Michael Raberger: Das Know-how von DataVision bei Collaboration, AV-Lösungen und digitalen Konferenzraumkonzepten ist ein Kernstück für moderne Büroumgebungen und Hybrid Work. Stichwort Employee Experience: Mitarbeitende sollten von überall eine einheitliche Nutzererfahrung erleben. Interaktive Displays, mobile Apps und die Integration von Meeting-Workflows steigern die Mitarbeiterbindung und fördern produktive, vernetzte Teams.

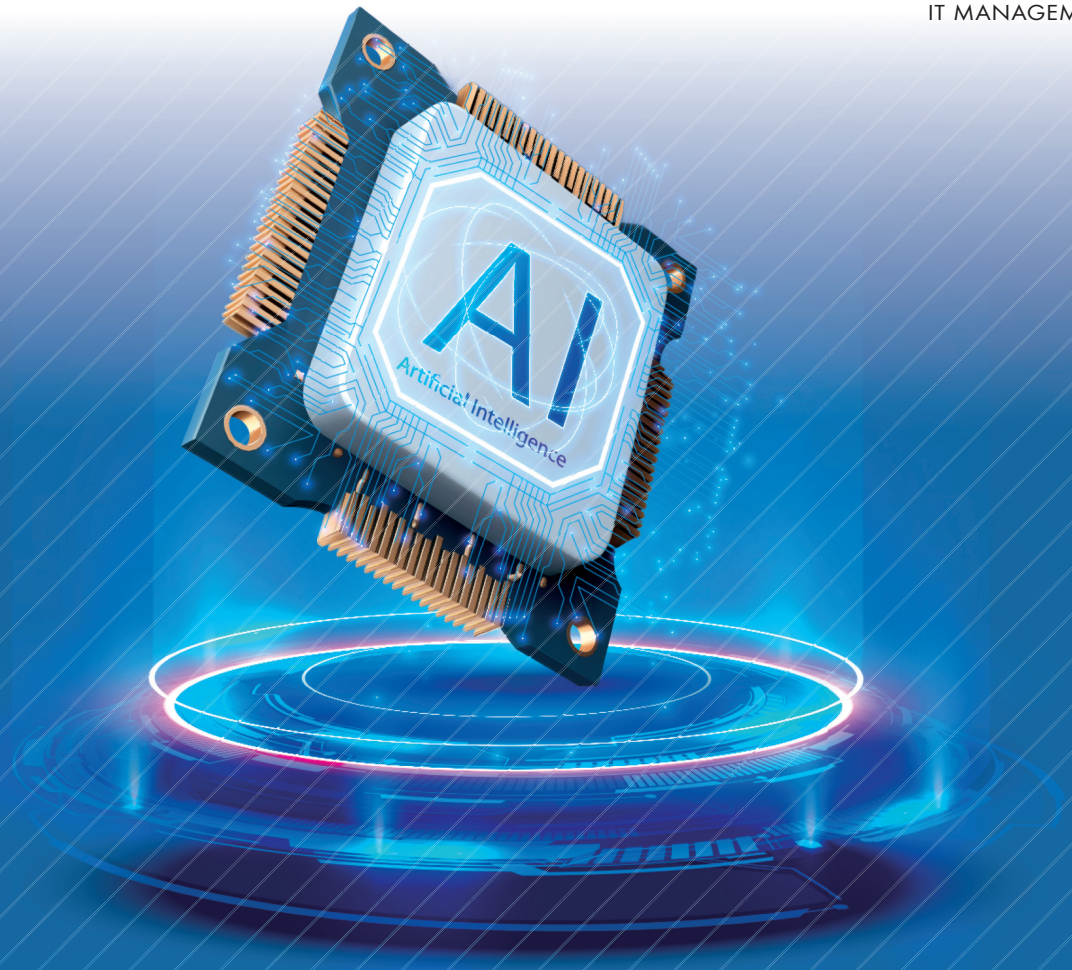
Gleichzeitig entwickeln wir unsere Plattform Ricoh Spaces kontinuierlich weiter - hin zu einer umfassenden Lösung für Arbeitsplatzmanagement, Prozessautomatisierung und smarter Vernetzung.

? **Carina Mitzschke:** *Ein Blick in die Zukunft: Welche Technologie-Trends sehen Sie als nächste Disruption für die Workplace-Experience?*

Michael Raberger: Ich glaube, die nächste Disruption wird nicht durch Technologie allein geprägt sein, sondern durch menschenzentrierte, intelligente Anwendungen im Arbeitsalltag. Virtuelle Meetings werden noch immersiver werden und so noch mehr persönliche Nähe für Kollaboration und Kreativität schaffen. Automatisierungsprozesse, die Workflows auch mit Hilfe von KI eigenständig initiieren, steuern und optimieren, werden die Office-Arbeit noch produktiver und effizienter werden lassen. Der Arbeitsplatz der Zukunft wird adaptiv, KI-gestützt, nachhaltig und sicherheitszentriert sein – und wir setzen darauf, unsere Kunden nicht nur technisch, sondern strategisch vorzubereiten.

! **Carina Mitzschke:** *Herr Raberger, wir danken für dieses Gespräch.*





KÜNSTLICHE INTELLIGENZ FÜR ALLTAG UND BERUF

FÜR ALLE, DIE KI NICHT NUR VERSTEHEN, SONDERN SINNVOLL NUTZEN WOLLEN

Die Künstliche Intelligenz verändert unsere Welt in rasantem Tempo – im privaten Alltag ebenso wie im Berufsleben. Dieses Buch bietet eine umfassende Einführung in die transformative Kraft der KI und zeigt, wie sie Lebensqualität, Produktivität und Entscheidungsprozesse neu definiert. Gleichzeitig beleuchtet es kritisch die ethischen, gesellschaftlichen und technologischen Herausforderungen, die mit dieser Entwicklung einhergehen.

Ob im Management, im Ingenieurwesen oder im täglichen Leben – anhand zahlreicher praxisnaher Beispiele und fundierter Analysen erhalten Leserinnen und Leser einen vielschichtigen Einblick in die Wirkweise und Auswirkungen moderner KI-Systeme. Beschrieben werden u. a. private bzw. berufliche Anwendungen wie Spracherkennung, Finanzprognosen, maschinelles Sehen, medizinische Diagnosesysteme und Mensch-Maschine-Interaktionen. Ethische Herausforderungen und Fairnessprobleme werden aufgezeigt, um eine Vertrauenskrise zu vermeiden.

Dieses Buch ist nicht nur ein informativer Leitfaden, sondern auch ein Denkanstoß: Es lädt dazu ein, die Rolle der KI in einer global vernetzten Welt zu hinterfragen, neue Kompetenzprofile zu entdecken und sich aktiv an der Gestaltung einer fairen, inklusiven und nachhaltigen Technologiezukunft zu beteiligen.



Künstliche Intelligenz für Alltag und Beruf;
Günter Hofbauer, Ruimei Zhou;
Carl Hanser Verlag GmbH & Co. KG;
09-2025



HYBRIDE UEM-STRATEGIE MIT ACMP INTUNE MANAGEMENT

MEHR FLEXIBILITÄT, SICHERHEIT UND KONTROLLE BEI DER VERWALTUNG VON ENDGERÄTEN

Die Verwaltung von Endgeräten in Unternehmen hat sich in den letzten Jahren stark weiterentwickelt. Das Spektrum der Clients reicht heute weit über klassische Desktops hinaus. Mobile Betriebssysteme wie iOS und Android müssen einbezogen werden, und eine verteilte Infrastruktur aus Homeoffice und Inhouse-Arbeitsplätzen entzieht die Gesamtheit der Endgeräte dem direkten physischen Zugriff. Hinzu kommen wachsende Sicherheitsbedrohungen. Ransomware-Angriffe nehmen jährlich zu – inzwischen gibt es ein regelrechtes Ransomware-as-a-Services Geschäftsfeld.

Mit gleichbleibender Personalstärke müssen Administrationsabteilungen Systeme aktuell halten und auf Schwachstellen reagieren. Sie müssen den Datenschutz im Auge behalten, ISO-Normen und gesetzliche Regularien wie etwa NIS2 und DORA erfüllen und dafür zusätzliche Dokumentationen erstellen und Vorkehrungen treffen.

Die Aagon Client Management Platform (ACMP) bietet durch die Kombination mit Microsoft Intune dafür die ideale Lösung: ein hybrides Unified Endpoint Management (UEM) für 100 Prozent Transparenz, Kontrolle und Sicherheit bei der Geräteverwaltung.



WHITEPAPER DOWNLOAD

Das Whitepaper umfasst 9 Seiten und steht kostenlos zum Download bereit.

www.it-daily.net/download

TRANSFORMATIONS-STRATEGIEN

THOUGHT LEADERSHIP

Die Migration von SAP ERP HCM auf S/4HANA wird für Unternehmen zur Pflichtaufgabe, da ältere Systeme bis 2027 bzw. 2030 eingestellt werden. Neben der technischen Umstellung stehen Organisationen vor Herausforderungen wie der Bereinigung von Altdaten, der Auswahl der passenden Migrationsmethode und dem Umgang mit sensiblen Personaldaten.

Doch welche Migrationsmethode ist die richtige? Welche Vorbereitungen sind notwendig? Wie lassen sich Risiken durch Altdaten, individualisierte Bestandssysteme und sensible Personaldaten minimieren? Und welche Rolle spielen Datenqualität, spezialisierte Tools und Expertenwissen für den Projekterfolg?





HCM-Transformation

EXPERTISE UND TOOLS SIND ENTSCHEIDEND

Gelegentlich müssen Unternehmen Altsysteme modernisieren. Bei SAP HCM für S/4HANA sollte dieser Schritt allerdings mit einer durchdachten Planung, einer Qualitätssteigerung der Daten und mit dem Einsatz KI-gestützter Transformations-Tools einhergehen.

Personalmanagementsysteme erfordern eine Transformation auf moderne Plattformen, wenn die Verwaltbarkeit verbessert, die Automation erhöht oder das Ende des System-Lebenszyklus erreicht wurde. Die Einführung von SAP HCM für S/4HANA (H4S4) ist ein solcher Fall. Die im Oktober 2022 eingeführte HCM-HANA-Version bietet Unternehmen vielfältige Möglichkeiten zur Verbesserung der HCM-Funktionalität und der Betriebsabläufe. Allerdings ist die neue Plattform keine Nice-to-Have-Option. Sie gehört zur Strategie von SAP, alle alten Systeme auf die neue Plattform zu migrieren. Unternehmen, die für ihre HCM-Systeme bis dato noch kein Transformationsprojekt angestoßen haben, geraten unter Zeitdruck. Denn ältere SAP ERP-Lösungen wie SAP ERP HCM werden bis 2027 bzw. 2030 eingestellt.

Housekeeping erhöht die Erfolgsaussichten

Die IT-Transformation eines HCM-Systems ist keine Aufgabe, die nebenher erledigt werden kann. Dabei stellt das Personalmanagement und dessen IT-Transformation besondere Herausforderungen an die IT- und Transformationsteams. Dazu gehört beispielsweise die hoch sensible Geheimhaltung der Personalinformationen, wie Gehälter und Zahlungen. Eine weitere oft auftretende Herausforderung ist das Alter, der hohe Individualisierungsgrad der Bestandssysteme und die große Menge an Altdaten.

Der Erfolg einer HCM IT-Transformation hängt maßgeblich von der Qualität der Datenbasis ab. Daher müssen die Daten noch vor der eigentlichen Transformation aufgeräumt und in Ordnung gebracht werden (Data-Housekeeping). Dieser Schritt ist entscheidend für den gesamten Erfolg. In der Natuvion Transformationsstudie 2025 gaben 31 Prozent der Befragten an, ihre Ziele nicht oder nicht vollständig erreicht zu haben. Enttäuschungen bezüglich der Zielerreichung kommen meist von einer ungenügenden Vorbereitung. Werden die Daten nicht konsequent im Vorfeld der Transformation analysiert und optimiert, ist das Erreichen der Ziele grundsätzlich schwieriger.

Grundsätzliche Überlegung zur Transformationsmethode

Das Standardvorgehen von SAP bei einer IT-Transformation ist die sogenannte Conversion oder Brownfield-Methode. Dabei werden alle Einstellungen, Daten und Entwicklungen (so S/4HANA-kompatibel) in die „Neue Welt" übernommen. Im Wesentlichen erfolgt hierfür ein Upgrade auf SAP S/4HANA 2022 und im Nach-

MEHR WERT
Natuvion Transformationsstudie 2025

MEHR WERT
SAP HCM für S/4HANA

gang die Aktivierung der SAP S/4HANA-Version des SAP HCM. Dieses Verfahren funktioniert prinzipiell, belässt allerdings „alles beim Alten". Damit sind die Vorteile, die aus einer IT-Transformation gezogen werden könnten, weit weniger wahrscheinlich als bei anderen Migrationsmethoden.

Alternativ bieten sich neben der Brownfield-Methode weitaus gewinnversprechendere Möglichkeiten an. Die hiermit verbundenen Chancen beinhalten sowohl die Restandardisierung und das Redesign der Anwendung als auch eine Reduzierung der vorhandenen Daten. Die Nutzung dieser Chancen ist mit einer kompletten Neueinführung – der sogenannten Greenfield-Methode – und insbesondere mit einer teilweisen Neuausrichtung – der sogenannten Selective Data Transition (SDT) – möglich.

Fünf Gründe für die Selective Data Transition

Es gibt fünf Gründe, weshalb Unternehmen bei ihrer HCM-Transformation auf die Selective Data Transition setzen sollten:

#1 Eine selektive Transition kann den Wechsel beschleunigen.

#2 Das Verfahren reduziert das Projektrisiko im Vergleich zu einer Neuimplementierung.

#3 Die Auswirkungen auf die laufenden Prozesse und die IT-Organisation sind gering.

#4 Historische Systemausprägungen, Datenstrukturen und Datenbestände können bereinigt und reduziert werden.

#5 Veränderungen der IT-Landschaft wie Systemkonsolidierungen oder Prozessauslagerungen in Cloud-Lösungen können in einem Schritt erfolgen.

Experten und spezielle Tools machen den Unterschied

Das Gelingen einer IT-Transformation von großen HCM-Umgebungen ist maßgeblich von den nötigen Software-Tools und von erfahrenen Transformationsexperten abhängig. An dieser Stelle kommen hoch spezialisierte Unternehmen ins Spiel, die mit sehr viel Expertise und mit passenden Tools maßgeblich zum Erfolg der IT-Transformation beitragen. Natuvion hat diese Expertise und verfügt mit seiner Data Conversion Suite (DCS) über eine voll integrierte Plattform, die alle Bereiche in allen Phasen einer IT-Transformation unter einem Dach unterstützt. Mit der Funktionsvielfalt lassen sich Transformationsprojekte skalieren und an den Lebenszyklus einer IT-Transformation anpassen – von der Analyse und Selektion über die Datenbereinigung bis zum finalen Load und einer möglichen Stilllegung nicht verwendeter Daten. Durch den gezielten Einsatz von KI werden viele Migrationsaufgaben automatisiert und damit einhergehend eine durchgängig hohe Qualität in der Transformation erreicht. Das Ergebnis ist eine sichere, nachhaltigere, kostengünstigere und vor allem schnellere Transformation auf IT-Plattformen wie SAP HCM für S/4HANA (H4S4).

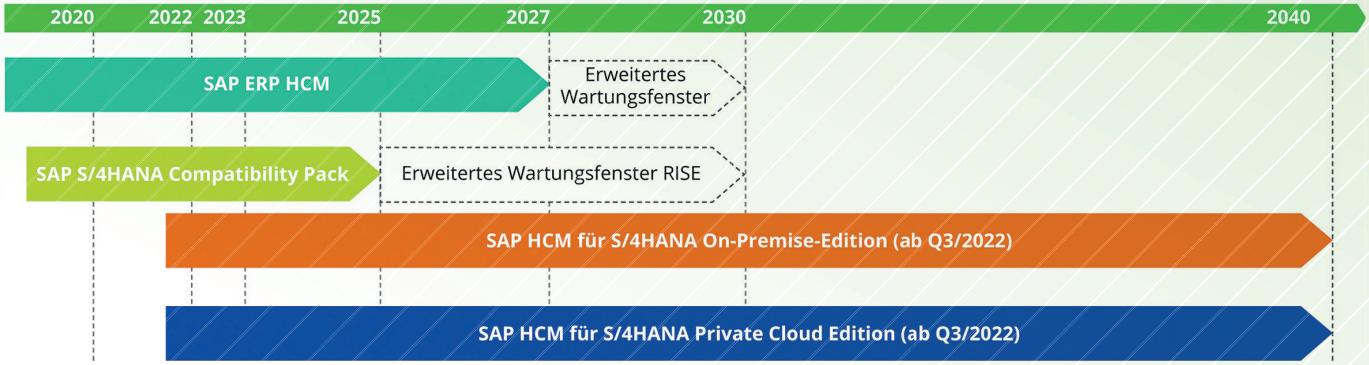
Niels Northe



DAS GELINGEN EINER IT-TRANSFORMATION VON GROSSEN HCM-UMGEBUNGEN IST MASSGEBLICH VON DEN NÖTIGEN SOFTWARE-TOOLS UND VON ERFAHRENEN TRANSFORMATIONSEXPERTEN ABHÄNGIG.

Niels Northe, Natuvion GmbH, Head of HCM-Transformation, www.natuvion.com

ROADMAP ZU H4S4



Erfolgreich auf SAP HCM für S/4HANA

DIE STADTWERKE MÜNCHEN SETZTEN BEI IHRER H4S4 TRANSFORMATION AUF DIE ZUSAMMENARBEIT MIT NATUVION

Von SAP ERP HCM auf SAP HCM für S/4HANA (H4S4) ohne spürbaren Verlust der bisherigen und mit Einführung neuer S/4-spezifischer Funktionen. Diese Aufgabe hatten sich die Stadtwerke München (SWM) zum Ziel gesetzt. Für die zeitgerechte Umsetzung holte sich das kommunale Versorgungsunternehmen Unterstützung von den Natuvion HCM-Experten.

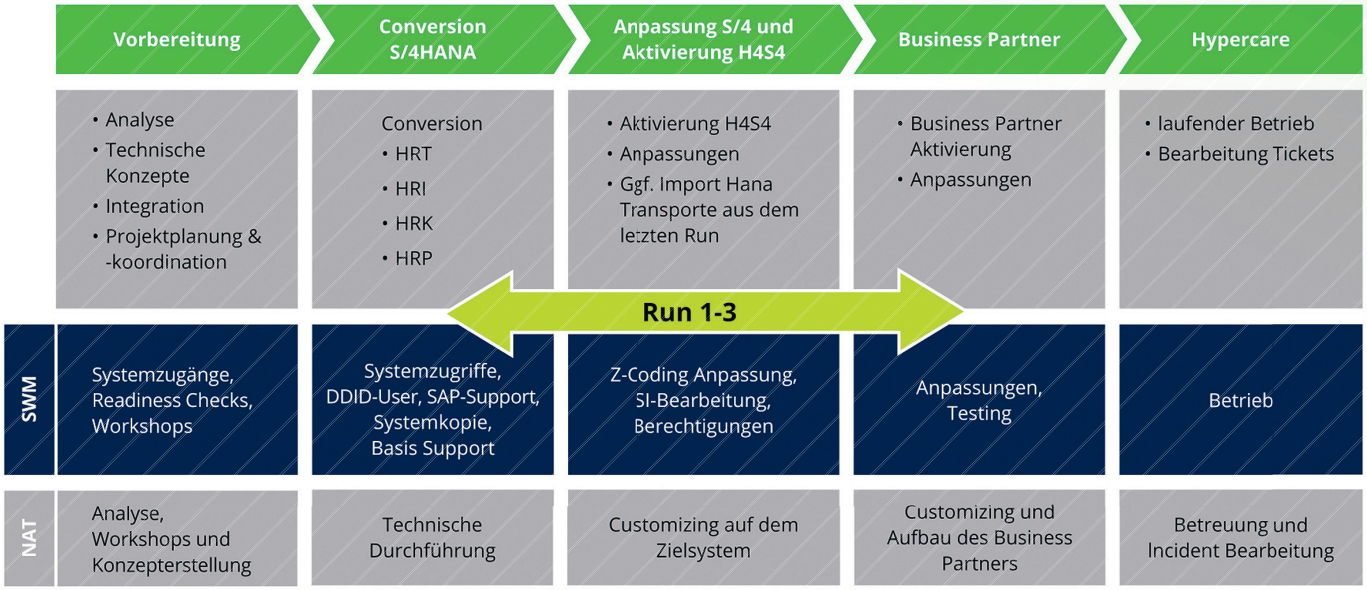
Um die Zukunftsfähigkeit ihres SAP HCM-Systems zu sichern, entschieden sich die Stadtwerke München für das Upgrade auf SAP S/4HANA. Die Herausforderung: Das bisherige HCM- System war komplex und bestand aus zahlreichen Eigenentwicklungen. Um die Kompatibilität dieser hatte sich die SWM überwiegend selbst gekümmert. Gleichzeitig erfordern die neu etablierten Konzepte von SAP S/4HANA aber Anpassungen in der bisherigen Systemlandschaft. Zum Beispiel die Einführung des SAP Employee Business Partner Modells oder die Angleichung von Custom Code an die HANA-Datenbank. Und auch FI-relevante Veränderungen ziehen Anpassungen bei den Auszahlungsprozessen im HCM-System nach sich.

Mit dem Ziel den Systemwechsel möglichst ohne Funktionsverluste zu bewältigen, setzte die SWM auf eine H4S4 Brownfield-Migration. Da es bei dem Münchner Versorgungsunternehmen intern jedoch nur wenig Vorabkenntnisse oder Erfahrung zu diesem Thema gab, wurde das Projekt ausgeschrieben. Natuvion überzeugte dabei als Partner, insbesondere dank der bereits guten fachlichen und technischen Zusammenarbeit in einem parallel laufenden ILM-Projekt. Zentrale Aufgabe von Natuvion war neben der Migrationsunterstützung auch der Know-how Transfer, damit die SWM von Beginn an in der Lage war, möglichst viel Fachwissen intern aufzubauen und viele Aufgaben selbst zu übernehmen.

Grundstein für den Migrationserfolg: Saubere Projektplanung

Als im Dezember 2023 der Startschuss für das Migrationsvorhaben fiel, stand

GRUNDSÄTZLICHER VERLAUF EINER H4S4-MIGRATION





die Vorbereitung im Fokus. Allen voran die System- und Datenanalyse. Mithilfe des SAP Readiness Checks und der Simplification Items verschaffte sich das Projektteam einen umfassenden Überblick über das bestehende HCM-System und die darin enthaltenen Daten und Prozesse. Mit dem ATC (ABAP Test Cockpit) Check wurden außerdem die Eigenentwicklungen geprüft und festgelegt, welche Code-Anpassungen für S/4HANA nötig sind. Diese Analysen waren die Grundlage für alle weiteren Schritte. In gemeinsamen Workshops stimmten sich Natuvion und die SWM zum besten technischen Vorgehen ab und erarbeiteten ein detailliertes Conversion-Konzept sowie einen Cutover-Plan. Dann konnte die Umstellung starten.

In 4 Schritten zum laufenden H4S4-Betrieb

Mithilfe einer Systemkopie überführte Natuvion im ersten Schritt das bestehende SAP ERP mit den Systemen HRT (Sandbox), HRI, HRK und HRP der HCM-Systemlandschaft technisch auf SAP S/4HANA. Anschließend wurde auf dem Zielsystem SAP HCM für SAP S/4HANA aktiviert und an die individuellen Anforderungen angepasst. Dazu zählte auch die Umstellung der zentralen Schnittstellenkommunikation auf Filegate sowie Anpassungen bei der Fiori Launchpad Benutzeroberfläche und der Hausbankenpflege. Der dritte Schritt umfasste die Einrichtung des „Mitarbeitergeschäftspartners" (Employee Business Partner), der für eine erfolgreiche H4S4 Migration zwingend erforderlich ist. Außerdem standen in diesem Schritt noch weitere notwendige Anpassungen im Fokus, um eine reibungslose Umstellung sicherzustellen. Abschließend erfolgten umfangreiche technische und funktionale Tests, bevor das System erfolgreich in den Produktivbetrieb überführt werden konnte.

Weichen für HXM erfolgreich gelegt

Der anvisierte Go-live des Projekts bis Ende August 2024 wurde erfolgreich eingehalten. In insgesamt nur 9 Monaten konnte das SAP ERP HCM auf S/4HANA umgestellt werden – unter Beibehaltung aller bisherigen Funktionen des Tagegeschäfts und der erfolgreichen Einführung S/4-spezifischer Funktionen wie dem Employee Business Partner. Grund für diesen erfolgreichen Projektverlauf war nicht zuletzt die hervorragende Zusammenarbeit zwischen SWM und Natuvion. Mithilfe eines übersichtlichen Jira Boards, themenbezogenen Jour Fixes sowie kurzfristigen Statusberichten via Microsoft Teams stellte man sicher, dass alle Projektbeteiligten jederzeit auf dem Laufenden waren und Probleme auch kurzfristig geklärt werden konnten. Da die SWM ihr System außerdem sehr gut kannte, konnte sie unter der Anleitung von Natuvion auch vieles selbst umsetzen. Der IT-Projektleiter von SWM, Stefan Brandstätter, zeigt sich mit dem Ergebnis sehr zufrieden: „Natuvion war für uns in jeder Hinsicht ein super Sparringspartner, nicht nur was die Projektbegleitung, sondern auch den internen Wissensaufbau und die schnelle Lösung von Fehlern anging. So konnten wir unseren Go-live-Termin problemlos halten und sind jetzt in einer guten Ausgangslage für das Thema HXM und den weiteren Weg in die Cloud."

Niels Northe
www.natuvion.com



Wenn WSUS an seine Grenzen stößt

BETRIEBSSYSTEM UND TREIBER UPDATEN OHNE WSUS

IT-Abteilungen stehen vor der täglichen Herausforderung, Windows-Betriebssysteme, Treiber und Microsoft 365-Updates zuverlässig zu verteilen. Besonders WSUS stößt dabei regelmäßig an seine Grenzen. Das Ergebnis: fehleranfällige Prozesse, langwierige Freigabeschleifen und im schlimmsten Fall instabile Client-Systeme. Sebastian Weber, Chief Evangelist beim UEM-Spezialisten Aagon, stellt im Interview vor, welche Alternative Aagon hier zu bieten hat.

it management: *Herr Weber, das Jahr 2026 gilt IT-technisch als besonders kritisch für nahezu alle Unternehmen. Was steht uns da bevor?*

Sebastian Weber: Microsoft hat angekündigt, dass die bisher genutzten Root- und Key-Exchange-Zertifikate aus dem Jahr 2011 auslaufen. Ab Juni beziehungsweise Oktober 2026 werden Geräte ohne die neuen KEK- und DB-Zertifikate Probleme bekommen. Das kann von fehlschlagenden Boot-Vorgängen über nicht mehr installierbare Updates bis hin zu als „nicht vertrauenswürdig" eingestuften digitalen Signaturen reichen. Für Unternehmen bedeutet das potenziell einen produktionsweiten Stillstand. Gerade regulierte Branchen riskieren damit de facto einen Produktionsstopp. Es ist also nicht nur ein technisches, sondern auch ein Compliance-Thema, das man frühzeitig angehen muss.

MEHR WERT
Complete Aagon Windows Update Management (CAWUM)

it management: *Microsoft empfiehlt, für diese Updates auf die eigene Update-Infrastruktur zu setzen. Warum sehen Sie das anders?*

Sebastian Weber: Microsoft sähe es am liebsten, die Verwaltung von Windows-Updates selbst zu übernehmen. Den dafür traditionell verwendeten WSUS stellen wir schon seit längerem unser ACMP Modul Complete Aagon Windows Update Management (CAWUM) als durchgängige Lösung gegenüber. Damit lassen sich Windows-, Office 365-, Treiber- sowie Firmware-Updates so koordinieren, dass die Systeme gleichzeitig sicher, kompatibel und betriebsbereit bleiben. Eine proaktive, zentral gesteuerte Update-Strategie reduziert die operative Komplexität, verbessert die Cyber-Resilienz und stellt sicher, dass kritische Infrastrukturen auch nach Ablauf der alten Secure-Boot-Zertifikate ohne Unterbrechung weiterarbeiten. Wir sehen jeden Tag bei Kunden, dass eine eigenständige Strategie für Updates mehr Kontrolle und Verlässlichkeit bedeutet.

it management: *Die Secure-Boot-Zertifikate als Paradebeispiel für die Notwendigkeit, Windows-Updates proaktiv und zentral zu managen. Worin unterscheidet sich CAWUM konkret von WSUS?*

Sebastian Weber: WSUS war lange das Standardwerkzeug für Windows-Updates. Allerdings stößt es immer häufiger an seine Grenzen – sei es bei der Bandbreite, der Steuerung einzelner Clients oder beim Freigabeprozess. CAWUM übernimmt diese Funktion, aber auf einer moderneren, granulareren Basis. Wir liefern den Clients nicht mehr das komplette Gigabyte-Update-Paket, sondern nur die tatsächlich benötigten Patches. Das spart Bandbreite, beschleunigt Installationen und erhöht gleichzeitig die Transparenz. Und wir können mehrere Update-Ringe,

Testphasen und unterschiedliche Repositories definieren, ohne komplizierte Zusatz-Tools.

it management: *Was bedeutet das für die operative Sicherheit?*

Sebastian Weber: Sicherheit entsteht durch Aktualität. Ungepatchte Systeme sind nachweislich eine der Hauptursachen für Ransomware-Angriffe und Datenlecks. CAWUM erlaubt eine proaktive Update-Strategie – inklusive Testsystemen, Freigaberingen und klar definierten Prozessen. Das reduziert operative Komplexität, erhöht die Cyber-Resilienz und sichert langfristig Compliance mit NIS-2, ISO 27001 und branchenspezifischen Standards. Gerade im Zusammenspiel mit strengen Audits ist es wichtig, Updates nicht nur einzuspielen, sondern auch revisionssicher zu dokumentieren.

it management: *Viele Administratoren fürchten Störungen im laufenden Betrieb, wenn sie Updates schneller ausrollen. Wie adressiert CAWUM diesen Punkt?*

Sebastian Weber: Wir setzen auf planbare und transparente Update-Prozesse. Updates lassen sich zuerst in Testumgebungen einspielen, dann kontrolliert in Freigaberingen ausrollen. Administratoren können definieren, welche Patches auf welchen File-Repositories liegen sollen und in welchen Sprachen. All das senkt das Risiko instabiler Clients und reduziert Freigabeschleifen drastisch. Außerdem sind unsere Rollback-Optionen klar definiert: Falls ein Patch unvorhergesehen Probleme macht, lässt sich sehr schnell der vorherige Zustand wiederherstellen.

it management: *WSUS wird spätestens nach dem Laufzeitende von Windows Server 2025 keine Zukunft mehr haben. Wie stellen Sie sicher, dass Unternehmen nicht ins Leere laufen?*

Sebastian Weber: Wir unterstützen Kunden bereits heute dabei, den Umstieg zu vollziehen. CAWUM ist so konzipiert, dass es nahtlos die Aufgaben von WSUS übernimmt – ohne dass Microsofts Cloud-Dienste eingebunden werden müssen. Das ist besonders für Unternehmen mit hohen Compliance-Anforderungen interessant. Gleichzeitig bleibt man tagesaktuell gegenüber neuen Bedrohungen, weil CAWUM wie ein synchronisierter WSUS arbeitet – nur mit deutlich mehr Steuerungsmöglichkeiten. Durch die enge Verzahnung mit anderen ACMP Modulen lassen sich Inventarisierung, Lizenzmanagement oder Endpoint Security nahtlos integrieren.



SICHERHEIT ENTSTEHT DURCH AKTUALITÄT. UNGEPATCHTE SYSTEME SIND NACHWEISLICH EINE DER HAUPTURSACHEN FÜR RANSOMWARE-ANGRIFFE UND DATENLECKS.

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

it management: *Neben Betriebssystem-Updates spielt auch das Treibermanagement eine wichtige Rolle. Welche Herausforderungen sehen Sie hier?*

Sebastian Weber: Treiber sind ein klassisches Einfallstor für Angreifer. Je älter ein Treiber, desto höher das Risiko. Microsoft hat die Treiberfunktion von WSUS bereits Ende April 2025 abgekündigt, und viele Unternehmen stehen damit ohne automatisierten Prozess da. Treiber und Firmware müssen aber genauso aktuell gehalten werden wie Windows selbst. Hinzu kommt: Treiber haben oft unmittelbaren Einfluss auf Stabilität und Performance. Ein veralteter oder fehlerhafter Treiber kann ganze Systeme lahmlegen.

it management: *Wie hilft CAWUM konkret bei der Treiberaktualisierung?*

Sebastian Weber: Wir binden Treiberkataloge von Drittanbietern – beginnend mit Lenovo, Dell und HP – direkt in CAWUM ein. Damit können Administratoren Treiber genauso granular auswählen und testen wie Windows-Updates. Nur die tatsächlich benötigten Dateien werden geladen, was den Speicherbedarf minimiert und Netzwerke entlastet. Mit bekannten Test- und Freigabeprozessen sowie ausführlichen Reports lässt sich lückenlos dokumentieren, dass die Infrastruktur sicher und konform ist. In Zukunft wollen wir auch weitere Hersteller ergänzen und so eine nahezu vollständige Abdeckung erreichen.

it management: *Sie betonen also grundsätzlich die Dringlichkeit, mit der Unternehmen ihr Patch- und Treibermanagement modernisieren müssen.*

Sebastian Weber: Das Auslaufen der Secure-Boot-Zertifikate ab 2026 und die Abkündigung von WSUS zeigen das nur zu deutlich. CAWUM ersetzt nicht nur WSUS, sondern schafft eine zukunftssichere, zentrale und planbare Plattform für Betriebssystem-, Office- und Treiber-Updates – und damit die Grundlage für nachhaltige Cyber-Resilienz und Compliance. Unternehmen können so ihre Update-Prozesse konsolidieren, Kosten sparen und ihre IT-Teams von Routinearbeiten entlasten.

it management: *Herr Weber, vielen Dank für das Gespräch.*



DNA Data Storage

REVOLUTION DER LANGZEITARCHIVIERUNG UND IHRE HERAUSFORDERUNGEN FÜR DIE IT-SICHERHEIT

Die weltweite Datenmenge verdoppelt sich alle zwei Jahre, doch unsere Speichertechnologien stoßen an ihre Grenzen. DNA Data Storage könnte die Lösung sein – bringt jedoch völlig neue IT-Sicherheitsrisiken mit sich, die von Bio-Cyber-Angriffen bis zur Bedrohung durch Quantencomputing reichen.

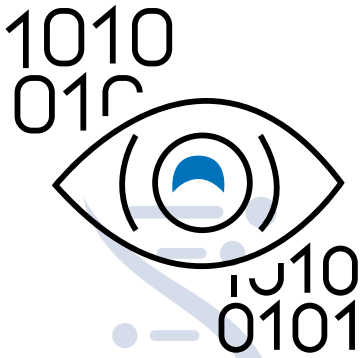
Das Datenzeitalter braucht eine Revolution

Die weltweite Datenmenge explodiert exponentiell und erreicht bereits heute mehr als 175 Zettabyte. Unsere bewährten Speichermethoden – Festplatten, SSDs und Magnetbänder – sind jedoch anfällig, energiehungrig und haben eine begrenzte Lebensdauer von wenigen Jahren bis Jahrzehnten. Eine revolutionäre Lösung für dieses Problem liegt buchstäblich in der Natur selbst: DNA Data Storage.

Diese bahnbrechende Technologie kodiert digitale Informationen in die Grundbausteine des Lebens und verspricht, die gesamte Datenmenge des Internets in einem Objekt von der Größe eines Zuckerwürfels für Tausende von Jahren zu bewahren. Diese Aussage ist etwas vereinfacht und bezieht sich auf die theoretische Kapazität, visualisiert sie aber gut. In der Praxis sind aktuell noch keine derartigen Speicherdichten erreicht worden. Doch wie jede transformative Technologie bringt sie neue Herausforderungen mit sich. Besonders kritisch sind die völlig neuartigen Risiken für die IT-Sicherheit und die Frage, wie Quantencomputing und Künstliche Intelligenz diese Probleme lösen können.

Was ist DNA Data Storage?

Das Grundprinzip der DNA-Speicherung ist so elegant wie genial. Digitale Daten



bestehen aus einer Abfolge von Nullen und Einsen (Bits). Das Erbgut aller Lebewesen, die DNA, besteht aus vier chemischen Basen: Adenin (A), Thymin (T), Cytosin (C) und Guanin (G).

Beim DNA Data Storage wird der Binärcode systematisch in einen DNA-Code übersetzt. Ein bewährtes Schema ordnet beispielsweise 00→A, 01→T, 10→C und 11→G zu. Aus der Binärsequenz 00110101 würde somit die DNA-Sequenz ATCG entstehen. Anschließend wird die entsprechende DNA-Sequenz mithilfe spezieller DNA-Synthesizer physisch im Labor hergestellt.

Das Auslesen erfolgt durch DNA-Sequenzierung – dieselbe Technologie, die auch in der Genomforschung verwendet wird. Dabei wird die Basenabfolge entschlüsselt und wieder in den ursprünglichen Binärcode zurückverwandelt.

Die dunkle Seite der Revolution

Während DNA-Speicher die Antwort auf das globale Kapazitätsproblem sein könnten, schaffen sie eine völlig neue Angriffsfläche. Die IT-Sicherheit muss sich erstmals mit Bio-Cyber-Bedrohungen auseinandersetzen – einer gefährlichen Verschmelzung biologischer und digitaler Risiken.

Im Gegensatz zu herkömmlichen Speichermedien ist DNA mikroskopisch klein und praktisch unsichtbar. Der Diebstahl einer winzigen, kaum sichtbaren DNA-Probe könnte zum Verlust von Petabytes hochsensibler Daten führen. Traditionelle physische Sicherheitsmaßnahmen für Rechenzentren greifen hier nicht mehr.

Bio-Cyber-Angriffe

Noch bedrohlicher ist die Möglichkeit manipulierter DNA-Sequenzen. Forscher der University of Washington demonstrierten bereits 2017, wie bösartige DNA-Sequenzen beim Auslesevorgang gezielt Schwachstellen in der Sequenzier-Software ausnutzen können. Diese „Schad-DNA" löst beim Dekodierungscomputer klassische Pufferüberlauf-Angriffe aus – ein Cyber-Angriff mit biologischem Einfallstor. Allerdings: es handelte sich um ein sehr spezifisches Laborsetting. In der Praxis müssten viele Voraussetzungen erfüllt sein, damit so ein Angriff funktioniert.

Ein Angreifer könnte theoretisch:

- Schadcode in DNA-Sequenzen verstecken
- Sequenziersoftware kompromittieren
- Ganze Computernetzwerke über „infizierte" DNA-Proben angreifen

Böswillige Akteure könnten versuchen, gespeicherte DNA durch chemische oder enzymatische Verfahren zu verändern. Im Gegensatz zu digitalen Medien, die sich durch Kopien sichern lassen, ist jede DNA-Probe physisch einzigartig und ihre Manipulation potenziell irreversibel.

Die Quantenbedrohung

Die größte langfristige Herausforderung für DNA-Speicher ist paradoxerweise ih-

re größte Stärke: die Langlebigkeit. Quantencomputer bedrohen die Grundfesten unserer heutigen Verschlüsselung fundamental.

Algorithmen wie RSA und elliptische Kurven-Kryptografie, die heute unsere digitale Sicherheit gewährleisten, basieren auf mathematischen Problemen, die für klassische Computer praktisch unlösbar sind. Quantencomputer mit Algorithmen wie Shor's Algorithmus könnten diese Verschlüsselung jedoch in absehbarer Zeit mühelos brechen.

Für DNA Data Storage entsteht dadurch ein kritisches Zeitparadox: Sensible Daten, die heute mit aktuellen Standards verschlüsselt in DNA gespeichert werden, könnten schon in 10-15 Jahren von leistungsstarken Quantencomputern rückwirkend entschlüsselt werden. Bei der Dynamik im Bereich KI und Quantencomputing ist eher von einer noch früheren Zeitspanne auszugehen. Die jahrhundertelange Haltbarkeit der DNA wird dann zur Achillesferse.

Post-Quanten-Kryptografie als Rettungsanker

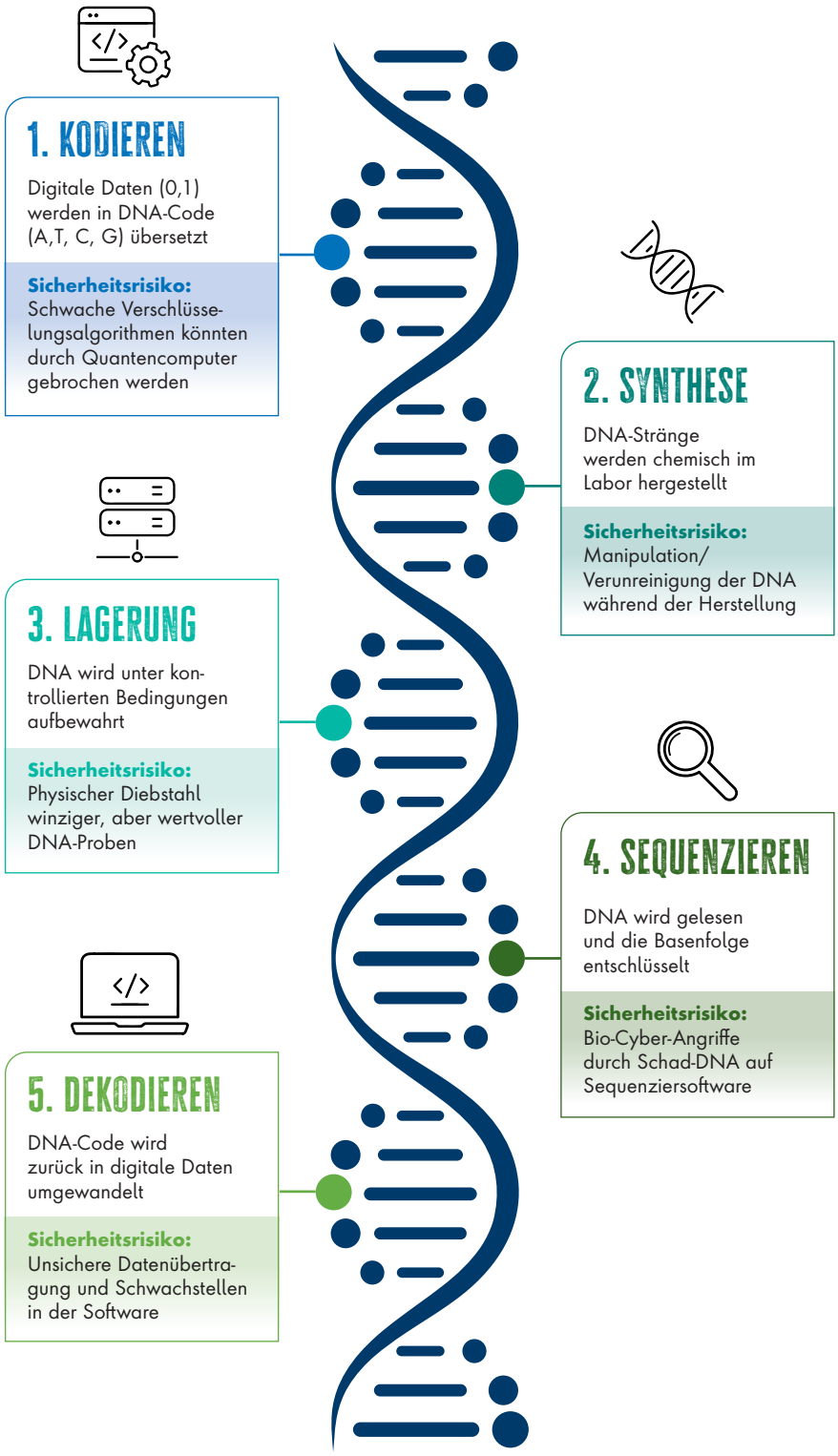
Die Lösung heißt Post-Quanten-Kryptografie (PQC). Dabei handelt es sich um neue Verschlüsselungsalgorithmen, die auch gegen Angriffe von Quantencomputern resistent sind. Das US-amerikanische National Institute of Standards and Technology (NIST) hat bereits erste Standards verabschiedet.

Für DNA Data Storage ist die frühzeitige Integration von PQC überlebenswichtig. Nur so können Daten, die heute archiviert werden, auch in einer post-quantischen Zukunft sicher bleiben.

Ironischerweise sind ausgerechnet die Technologien, die neue Bedrohungen schaffen, auch Teil der Lösung. Künstliche Intelligenz spielt bereits heute eine entscheidende Rolle dabei, DNA Data Storage sicherer und effizienter zu machen.

VOM BIT ZUR BASE: DER DNA-SPEICHERKREISLAUF UND SEINE SICHERHEITSRISIKEN

Jeder Schritt des DNA Data Storage Prozesses bringt spezifische IT-Sicherheitsherausforderungen mit sich



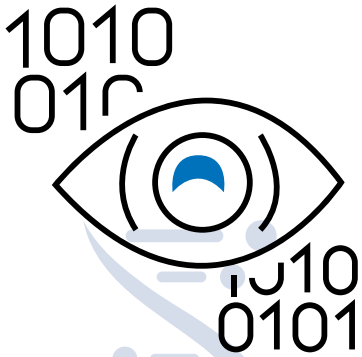
Der Beitrag der Künstlichen Intelligenz

Intelligente Kodierung: KI-Algorithmen entwickeln effizientere Kodierungsverfahren, die weniger fehleranfällig sind und die Synthesekosten reduzieren.

Erweiterte Fehlerkorrektur: Machine-Learning-Modelle erkennen und korrigieren Sequenzierfehler mit einer Präzision, die klassische Algorithmen übertrifft.

Optimierte Synthese: KI kann vorhersagen, welche DNA-Sequenzen besonders stabil und kostengünstig herzustellen sind.

Virtuelle Experimente: Millionen von Simulationen identifizieren optimale Parameter, bevor teure Laborexperimente durchgeführt werden.



Langfristig könnte Quantencomputing selbst zur Lösung beitragen:

- Optimierung der Speicherdichte durch Lösung komplexer kombinatorischer Probleme
- Beschleunigte DNA-Assemblierung bei der Rekonstruktion großer Datensätze
- Molekulare Simulation für verbesserte Syntheseverfahren

Technologieführer und Marktentwicklung

Das DNA-Speicher-Ökosystem besteht aus spezialisierten Akteuren, die jeweils unterschiedliche Aspekte der Technologie vorantreiben:

#1 Spezialisierte Biotech-Unternehmen:

Twist Bioscience: Marktführer in der DNA-Synthese und bevorzugter Partner der meisten Forschungsprojekte

Catalog: Pionier eines einzigartigen Ansatzes mit vorgefertigten DNA-Bibliotheken

Iridia: Entwickelt ganzheitliche Systeme mit verbesserter Stabilität

#2 Technologie-Konzerne:

Microsoft Research: Aktivster Player mit spektakulären Proof-of-Concepts und Plänen für Azure-Integration

Western Digital: Traditioneller Speicherhersteller mit strategischem Interesse an der Zukunft

#3 Standardisierung:

DNA Data Storage Alliance: Gegründet von führenden Unternehmen zur Entwicklung gemeinsamer Standards

Der Weg zur Marktreife

Experten schätzen, dass DNA-Speicher in 10-15 Jahren wirtschaftlich mit herkömmlichen Archivierungslösungen konkurrieren könnten. Die ersten Anwendungen werden voraussichtlich in Nischenbereichen erfolgen.

Unternehmensarchivierung: Für selten genutzte, aber rechtlich wichtige Daten

Wissenschaftliche Langzeitspeicherung: Für Forschungsdaten und historische Archive

Cold Storage in Rechenzentren: Als energieeffiziente Alternative für Backup-Systeme

Weitsicht als Schlüssel zum sicheren DNA-Archiv

DNA Data Storage repräsentiert mehr als nur eine neue Speichertechnologie – es ist ein fundamentaler Paradigmenwechsel. Die Technologie zwingt uns, IT-Sicherheit als disziplinübergreifende Aufgabe zu begreifen, die Informatik, Biologie und Quantenphysik miteinander verbindet.

Die Herausforderungen sind beträchtlich: von physischen Bio-Cyber-Angriffen bis zur quantencomputing-bedingten Entschlüsselung historischer Archive. Doch die Werkzeuge zur Bewältigung dieser Risiken sind bereits im Entstehen. Durch die frühzeitige Integration von Post-Quanten-Verschlüsselung, die Absicherung der Software-Pipelines und den strategischen Einsatz von KI kann das immense Potenzial der DNA als ultimativer Speicher sicher und verantwortungsvoll genutzt werden.

Die Zukunft der Datenspeicherung wird in Basenpaaren geschrieben – und ihre Sicherheit muss heute mitgedacht werden.

Ulrich Parthier

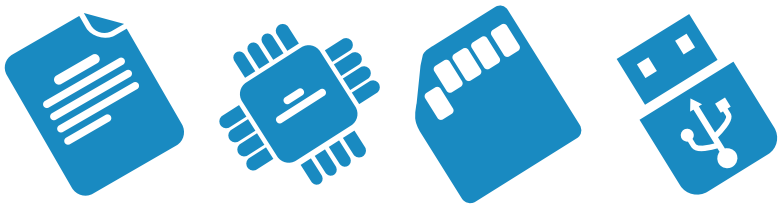
DIE UNSCHLAGBAREN VORTEILE DER DNA-SEQUENZIERUNG

Extreme Datendichte: Ein Gramm DNA kann theoretisch bis zu 215 Petabyte an Daten speichern – genug, um die gesamte digitale Welt von heute aufzunehmen.

Außergewöhnliche Langlebigkeit: Unter optimalen Bedingungen (kühl, trocken, dunkel) bleibt DNA Jahrtausende stabil, während herkömmliche Speichermedien regelmäßig ersetzt werden müssen.

Absolute Energieeffizienz: Einmal synthetisiert, benötigt DNA-Speicher keinerlei Energie für die Aufbewahrung. Allerdings sind die Synthese und Sequenzierung das Gegenteil, nämlich sehr energieintensiv.

Zukunftssicherheit: Solange es Leben auf der Erde gibt, wird die Technologie zum Lesen von DNA verfügbar sein.



Plattformunabhängige Archivierung

6 WICHTIGE ASPEKTE FÜR DIE WORM-ARCHIVIERUNG

Die Archivierung ist für die meisten Unternehmen Pflicht und je nach gesetzlichen Vorgaben müssen viele Daten langfristig aufbewahrt werden. Dazugehören Finanzdaten, Jahresanschlüsse, Verträge oder beispielsweise Patientendaten mit besonders langen Archivierungszeiträumen. Aufgrund des enormen Datenwachstums und zunehmend strenger Regulatorik setzen Organisationen jeglicher Größe und Branche auf digitale Archivlösungen – in der Hoffnung, dass die Daten trotz des schnellen technologischen Fortschritts auch in 15 oder mehr Jahren noch revisionssicher zur Verfügung stehen und lesbar sind. Lange Zeit hatten sich Tape oder optische Speichermedien wie CD oder DVD bewährt. Doch mit dem Preisverfall und der leistungsfähigkeit der Festplatte rücken traditionelle Speichermedien in den Hintergrund und das Software-WORM (Write Once Read Many) macht die Platte zum idealen Datenträger.

Sechs Aspekte einer modernen WORM-Archivierung

Eine moderne WORM-Software-Archivlösung sollte technische Vorteile bieten und gleichzeitig die speziellen Anforderungen und gesetzlichen Vorschiften unterschiedlicher Branchen erfüllen. Bei der Wahl einer Lösung gilt es sechs wichtige Punkte zu beachten:

#1 Die WORM-Archiv-Software muss über Schnittstellen unabhängig von anderen Anwendungen funktionieren. Damit ist gewährleistet, dass bei der Änderung einer Kernapplikation, beispielsweise einer Personaldatenbank, kein Wechsel der Archiv-Software nötig ist.

#2 Die WORM-Archiv-Software sollte Hardware-unabhängig sein. Dies erlaubt es den IT-Verantwortlichen, sowohl Server- als auch Speichersysteme unabhängig und ohne zusätzliche Kosten für das Archiv zu modernisieren.

#3 Die WORM-Lösung muss sich nahtlos in die bestehende IT-Infrastruktur integrieren. Für sämtliche Anforderungen und Anwendungen wie Systemmanagement, Backup, Virenscanner, Accounting- oder Virtualisierungssoftware sollte kein Anpassungsaufwand entstehen.

#4 Der Volumenausbau der Datenarchive muss von der WORM-Software-Lösung bis hin zu sehr großen Archiven unterstützt werden. Der schnelle Anstieg an Datenvolumina in Archiven darf die Systemverantwortlichen nicht zwingen, aufgrund von Leistungsbeschränkungen schon bald nach neuen Lösungen suchen zu müssen.

#5 Die WORM-Software-Lösung muss nicht nur allgemeingültige Anforderungen, beispielsweise Revisionssicherheit oder GoBD, erfüllen, sondern idealerweise weitere Zertifizierungen und Testate von offiziellen Prüforganisationen aufweisen, welche Unternehmen oder Organisationen mit sensiblen Datenbeständen branchenspezifisch und zusätzlich absichern.

#6 Eine moderne WORM-Archivsoftware muss die Datenvernichtung automatisiert und selbstständig ermöglichen. Je nach Konfiguration der Software können einzelne Datensätze oder ganze Daten-Pools nach einer festgelegten Zeitspanne – automatisch oder wahlweise manuell unwiderruflich gelöscht werden.

Fazit

Die Datenarchivierung in Unternehmen und Organisationen sollte möglichst wenig zusätzlichen Administrationsaufwand erfordern. Ein hoher Automatisierungslevel, wie es beispielsweise mit FileLock von GRAU DATA erreicht werden kann, sorgt für eine deutliche Entlastung über viele Jahre hinweg. Gleichzeitig werden die allgemeinen und branchenspezifischen Vorschriften der Revisionssicherheit eingehalten. Damit liegt die Zukunft des Archivs in einer plattformunabhängigen und schlanken WORM-Software-Lösung, die trotz stetigem Datenzuwachs und IT-Modernisierungen langfristig einsetzbar sind.

Kai Hambrecht



EINE MODERNE WORM-SOFTWARE-ARCHIVLÖSUNG SOLLTE TECHNISCHE VORTEILE BIETEN UND GLEICHZEITIG DIE SPEZIELLEN ANFORDERUNGEN UND GESETZLICHEN VORSCHIFTEN UNTERSCHIEDLICHER BRANCHEN ERFÜLLEN.

Kai Hambrecht,
Leiter Service und Support,
GRAU DATA, www.graudata.com



Quelle: iStock

Object Storage ohne Umwege

WAS DER VERZICHT AUF TIERING BRINGT

Cloud Object Storage gehört seit Jahren zu den Standardbausteinen moderner IT-Infrastrukturen. Die meisten Unternehmen orientieren sich am etablierten S3-Modell, das Amazon Mitte der 2000er geprägt hat. Dieses Modell sieht eine klare Trennung verschiedener Speicherklassen vor: häufig genutzte Daten liegen im schnellen Zugriff, selten genutzte Inhalte werden in günstigere, langsamere Tiers verschoben. Lifecycle-Regeln sorgen dafür, dass Objekte nach einem definierten Zeitraum automatisch verschoben werden. Dazu kommen Zugriffsrechte und Policies, die einen differenzierten Umgang mit Daten ermöglichen sollen.

Auf dem Papier wirkt dieser Ansatz logisch. Er verbindet Performance mit Kostenersparnis, indem er Daten nach ihrer Nutzungshäufigkeit aufteilt. Doch im Alltag zeigt sich: Die Theorie ist oft nur eingeschränkt praxistauglich. IT-Teams kämpfen mit komplexen Regeln, schwer kalkulierbaren Kosten und unerwarteten Verzögerungen im Betrieb.

Warum Tiering eingeführt wurde – und warum es heute Probleme schafft

Tiering hatte lange Zeit eine klare Berechtigung. Speicher war teuer, und die Auslagerung seltener Daten in günstigere Klassen versprach Einsparungen. Mit dem massiven Preisverfall für Storage und den gestiegenen Anforderungen an Datenverfügbarkeit kippt diese Rechnung jedoch zunehmend.

Ein Beispiel: Viele Unternehmen definieren Lifecycle-Regeln nach dem Prinzip „nach 30 Tagen ohne Zugriff ins Archiv verschieben". Das funktioniert, solange die Daten tatsächlich nicht mehr benötigt werden. Sobald aber ein Analyse-Tool, ein Reporting-Prozess oder eine Compliance-Anfrage auf alte Daten zugreift, werden diese Regeln zum Hindernis. Daten liegen im Archiv, müssen zeitaufwendig zurückgespielt werden und verursachen Kosten, die im Vorfeld kaum einplanbar sind.

Besonders problematisch ist das bei Archiven wie Glacier oder Deep Archive. Hier dauert ein Restore nicht selten mehrere Stunden. Gleichzeitig entstehen Gebühren, die schnell ein Vielfaches der ursprünglichen Speicherkosten ausmachen. Für Anwendungen, die sofortige Antworten erwarten, bedeutet das: Timeouts, Fehlermeldungen und abgebrochene Workflows. In produktionsnahen oder zeitkritischen Szenarien kann das gravierende Folgen haben – von Verzögerungen bis hin zu Geschäftsausfällen.

Ein weiterer Nachteil des Tierings ist seine mangelnde Transparenz. Unterneh-

men kalkulieren oft mit den reinen Speicherkosten und übersehen dabei Abrufgebühren, Mindesthaltedauer oder Egress-Kosten. Diese „versteckten" Posten schlagen jedoch genau dann zu, wenn Daten kurzfristig benötigt werden.

Ein Beispiel aus der Praxis: Ein Unternehmen lagert ältere Kundendaten in eine Cold-Klasse aus. Monate später wird im Rahmen einer Revision auf diese Daten zugegriffen. Der Restore dauert Stunden, verursacht zusätzliche Abrufgebühren und blockiert parallel laufende Prozesse. Das IT-Team sieht sich plötzlich mit Budgetüberschreitungen und unzufriedenen Fachbereichen konfrontiert – obwohl die ursprüngliche Speicherstrategie eigentlich Kosten senken sollte.

Always-Hot statt Klassenlogik

Immer mehr IT-Verantwortliche stellen deshalb die Grundannahme des Tierings infrage. Statt Daten nach Nutzungshäufigkeit in unterschiedliche Speicherklassen zu verschieben, setzen sie auf Architekturen, die alle Objekte jederzeit im direkten Zugriff halten. Der Vorteil liegt auf der Hand: Es gibt keine Restore-Prozesse, keine Wartezeiten und keine unvorhersehbaren Zusatzkosten. Alle Daten stehen permanent zur Verfügung, unabhängig davon, wie oft sie tatsächlich genutzt werden. Für Unternehmen bringt das mehr Planbarkeit. Ob Backups, langfristige Archive oder Analysen mit wechselnden Zugriffsmustern – die Performance bleibt konsistent, und die Kosten lassen sich klar kalkulieren. Komplexe Lifecycle-Regeln entfallen, was den Betrieb deutlich vereinfacht.

Ein Speicher, der Daten jederzeit verfügbar macht, braucht zugleich eine robuste Zugriffskontrolle. Klassische S3-Mechanismen mit Bucket Policies und ACLs bieten zwar Flexibilität, erweisen sich aber bei vielen Buckets und komplexen Organisationen oft als unübersichtlich. Moderne Systeme setzen daher auf identitätsbasierte Zugriffskontrolle (IAM). Rechte werden granular pro Nutzer oder Objekt vergeben, und Aktionen wie Lesen, Schreiben oder Löschen sind klar definierbar. Gerade in Multi-Tenant-Umgebungen sorgt das für Übersicht und Sicherheit.

Neben der Backend-Logik spielt die Bedienoberfläche eine entscheidende Rolle. IT-Teams benötigen eine zentrale Konsole, in der sie Rechte, Rollen und Freigaben steuern können, ohne tief in API-Dokumentationen einzutauchen. Dazu gehören auch temporäre Freigaben über presigned URLs, Monitoring- und Logging-Funktionen sowie die Möglichkeit, Migrationen effizient zu verwalten. Eine gute Oberfläche ist damit nicht nur Komfort, sondern Voraussetzung für reibungslose Abläufe.



DIE WAHL DER SPEICHERARCHITEKTUR IST MEHR ALS EINE KOSTENFRAGE.

Lennart Rother,
Director Partner Solutions & Growth,
Impossible Cloud,
www.impossiblecloud.com

Rechtliche und regulatorische Anforderungen

Parallel zu den technischen Fragen sind die rechtlichen Rahmenbedingungen ein weiterer Treiber für neue Speicherstrategien. Unternehmen wollen ihre Daten nicht nur performant, sondern auch rechtskonform verwalten. DSGVO-Konformität, europäische Datensouveränität und Schutz vor extraterritorialen Gesetzen wie dem US CLOUD Act sind zentrale Kriterien bei der Auswahl von Speicherlösungen.

Hinzu kommen branchenspezifische Vorgaben. Banken und Versicherer müssen strenge Audit- und Aufbewahrungspflichten erfüllen, produzierende Unternehmen achten auf Nachvollziehbarkeit und Lieferketten-Sicherheit, im Gesundheitswesen geht es um Vertraulichkeit und Zugriffsrechte. Ein Object Storage, der Verschlüsselung, Mandantenfähigkeit und standardisierte APIs bereitstellt, ist hier mehr als ein technisches Detail, er ist eine Grundvoraussetzung für die Compliance.

Speicher als Teil der Resilienz-Strategie

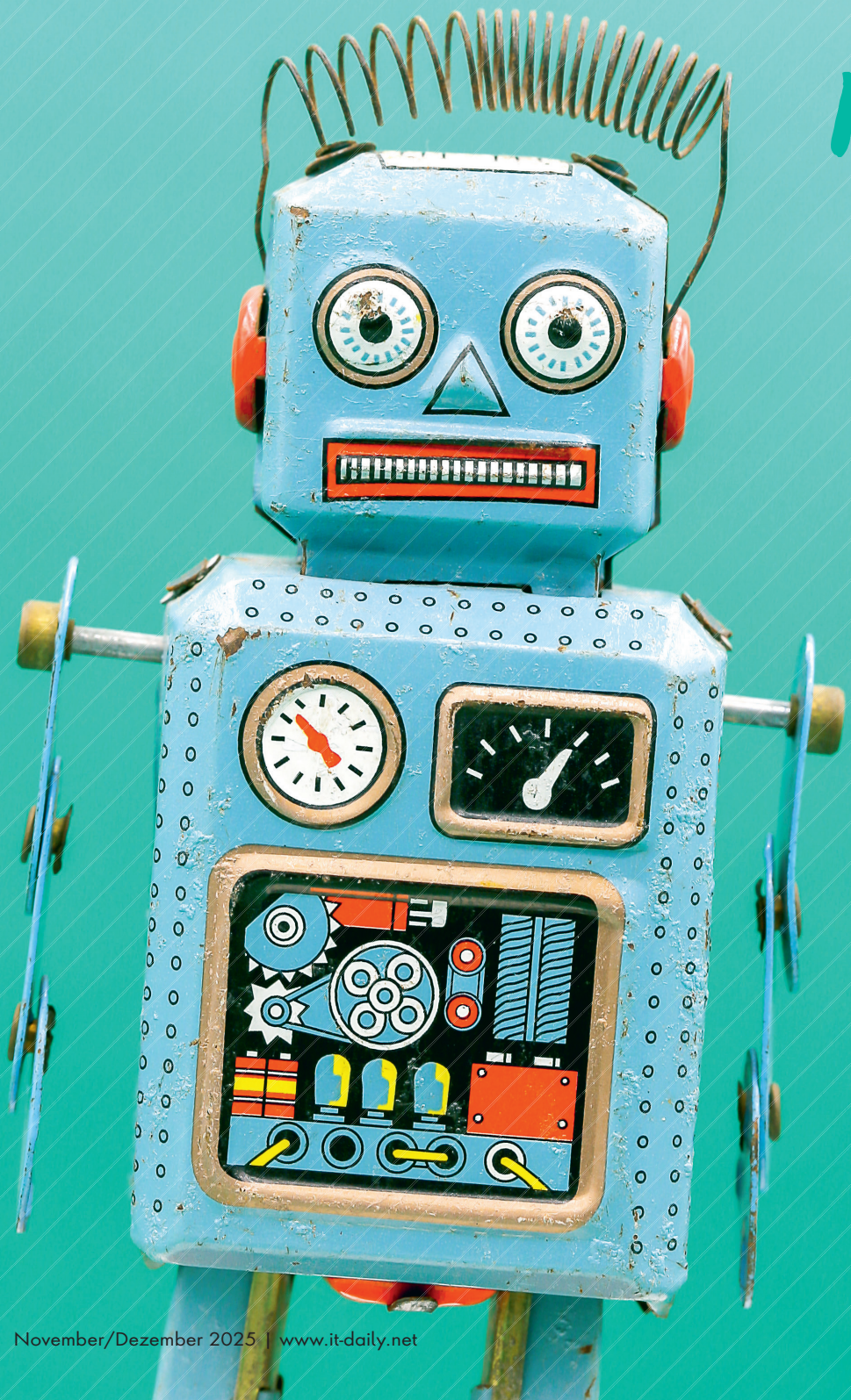
Der Blick nach vorn zeigt: Datenmengen wachsen weiter exponentiell, gleichzeitig steigen die Anforderungen an Verfügbarkeit und Sicherheit. Unternehmen können es sich immer weniger leisten, Daten erst wiederherstellen zu müssen oder in unübersichtlichen Speicherklassen zu verlieren.

Always-Hot-Ansätze passen daher in eine breitere Strategie: Sie sind ein Baustein für resiliente IT-Architekturen, die Ausfälle vermeiden, Kosten planbar halten und regulatorische Vorgaben einhalten. Statt Speicher in komplexe Klassen zu unterteilen, rückt das Prinzip in den Vordergrund, dass jede Information jederzeit verfügbar sein muss – egal, ob für den täglichen Betrieb, für Audits oder für unvorhersehbare Analysen.

Das klassische Tiering-Modell stößt in der Praxis immer häufiger an seine Grenzen. Seine Komplexität, die Abhängigkeit von Regeln und die schwer kalkulierbaren Kosten machen es für viele Unternehmen unattraktiv. Speicherlösungen, die Daten dauerhaft verfügbar halten, reduzieren diese Risiken und schaffen mehr Transparenz. Für IT-Entscheider gilt daher: Die Wahl der Speicherarchitektur ist mehr als eine Kostenfrage. Wer auf direkte Verfügbarkeit, klare Zugriffskontrollen und rechtskonforme Infrastruktur setzt, schafft die Grundlage für eine zukunftssichere IT.

Lennart Rother

Welches Speicher-Medium für Morgen?



Speichermedien im Umbruch

DIE ZUKUNFT VON DATEN UND DATENSPEICHERN IN ZEITEN DES QUANTENCOMPUTINGS

Die Frage, ob Quantencomputer mit unseren heutigen Speichermedien kompatibel sein werden oder ob gänzlich neue Technologien nötig sind, führt direkt in das Herz der zukünftigen IT-Infrastruktur. Die Antwort ist differenziert: Ja, aber nur teilweise.

Quantencomputer Kompatibilität

Man muss grundsätzlich zwischen zwei Arten von Daten unterscheiden. Zum einen sind das die konventionellen Daten, also die Eingabeprobleme für den Quantencomputer (wie eine komplexe Simulationsaufgabe) und die Ergebnisse, die er liefert. Für diese Daten werden auch in Zukunft bewährte Speichermedien wie SSDs, Festplatten und Cloud-Speicher die erste Wahl bleiben. Der Quantenprozessor (QPU) selbst wird über klassische Steuerrechner mit diesen Speichern verbunden sein. In diesem Sinne besteht Kompatibilität.

Zum anderen geht es um die Quantenzustände selbst - die Qubits. Ihre fragile quantenmechanische Natur (Superposition, Verschränkung) ist die eigentliche Information während der Berechnung. Diese Zustände können nicht auf einer herkömmlichen Festplatte gespeichert werden, da jede Wechselwirkung mit der Umwelt sie sofort zerstören würde (Dekohärenz). Für die kurzlebige Speicherung und Manipulation von Quanteninformationen sind daher die Qubits selbst oder spezielle Quantenspeicher notwendig.

Holografie und DNA-Speicher

Die indirekten Folgen des Quantencomputings - etwa die Generierung extrem großer und komplexer Simulationsdatensätze - sowie die Vision eines Quanteninternets werden jedoch sehr wohl neue Speichertechnologien erfordern. Hier rücken holografische Speicher und DNA-Datenspeicher in den Fokus, auch wenn ihre Rolle eine andere ist.

Holografische Speicher, die Daten in lichtempfindlichen Materialien mit hoher Dichte und parallelem Zugriff speichern, könnten sich als ideale Lösung erweisen, um die gewaltigen konventionellen Datensätze, die Quantencomputer analysieren sollen, schnell bereitzustellen. Aktuell gibt es noch technische Herausforderungen wie die Materialstabilität und die Kosten. Für die Speicherung von Quanteninformationen sind sie jedoch ungeeignet.

Ähnlich verhält es sich mit DNA-Datenspeichern. Ihre unschlagbaren Vorteile sind die extrem hohe Datendichte und die Haltbarkeit über Jahrtausende. Das macht sie zum perfekten Medium für die Langzeitarchivierung bahnbrechender, aber statischer Ergebnisse von Quantensimulationen für die Nachwelt. Aufgrund



Kernaussage: Quantencomputer ersetzen keine Festplatten – sie erforn eine erweiterte Speicherhierarchie mit neuen Technologien für Quantenstände.

ÜBERSICHT:
SPEICHERMEDIEN IM KONTEXT DES QUANTENCOMPUTINGS

Technologie	Rolle & Anwendung	Eignung für Quanten-information	Zeitrahmen/ Reife
SSDs, HDDs, Cloud	**Steuerung & konventionelle Daten:** Verwaltung von Ein-/Ausgabe daten, Steuerung des Quanten prozessors (QPU) über klassische Rechner.	**Nein**	Gegenwart & Zukunft (Etabliert, bleibt unver-zichtbar)
Holografische Speicher	**Hochperformante Daten-speicherung:** Schneller Zugriff auf große, konven-tionelle Datensätze (z.B. für Simula-tionsreferenzdaten).	**Nein**	Zukunft (Mögliche Alternative für Big-Data-Szenarien)
DNA-Datenspeicher	**Langzeitarchivierung:** Extrem platzsparende und dauer-hafte Speicherung von kalten, kon-ventionellen Daten (z.B. Ergebnis-sen von Quantensimulationen).	**Nein**	Zukunft (Für Archive, zu langsam für operativen Einsatz)
Quantenspeicher (Quantum Memories)	**Handhabung von Quantenzuständen:** Kurzzeitiges „Einfrieren“ und Übertragen von Qubit-Zuständen, essentiell für ein Quanteninternet (Quantenrepeater).	**Ja (Primärzweck)**	Forschung & Zukunft (Kritische Schlüsseltech-nologie in Entwicklung)
Fehlertolerante Quantencomputer	**Dynamische Quanteninformations-Speicherung:** Der Quantencomputer selbst dient als Speicher, indem er Qubits durch Fehlerkorrektur aktiv stabilisiert.	**Ja (Primärzweck)**	Langefristige Zukunft (Ziel der aktuellen Forschung)

der sehr langsamen Schreib- und Lesezeiten scheidet DNA-Speicher für den operativen Einsatz jedoch aus.

Die Datenvorbereitung für Quantencomputer

Ein weiterer wichtiger Punkt ist die Geschwindigkeit der Datenvorbereitung. Bevor ein Quantencomputer rechnen kann, müssen oft immense klassische Datenmengen aufbereitet und in ein für ihn verarbeitbares Format transformiert werden.

Hier könnten speichernahe Compute-Technologien oder extrem schnelle NVMe-Speicher eine entscheidende Rolle spielen, um diesen Engpass zu vermeiden und den Quantenprozessor optimal auszulasten. Speichernahe Compute-Technologie wird auch als „Processing-in-Memory (PIM)" oder „Near-Data Computing" bezeichnet.

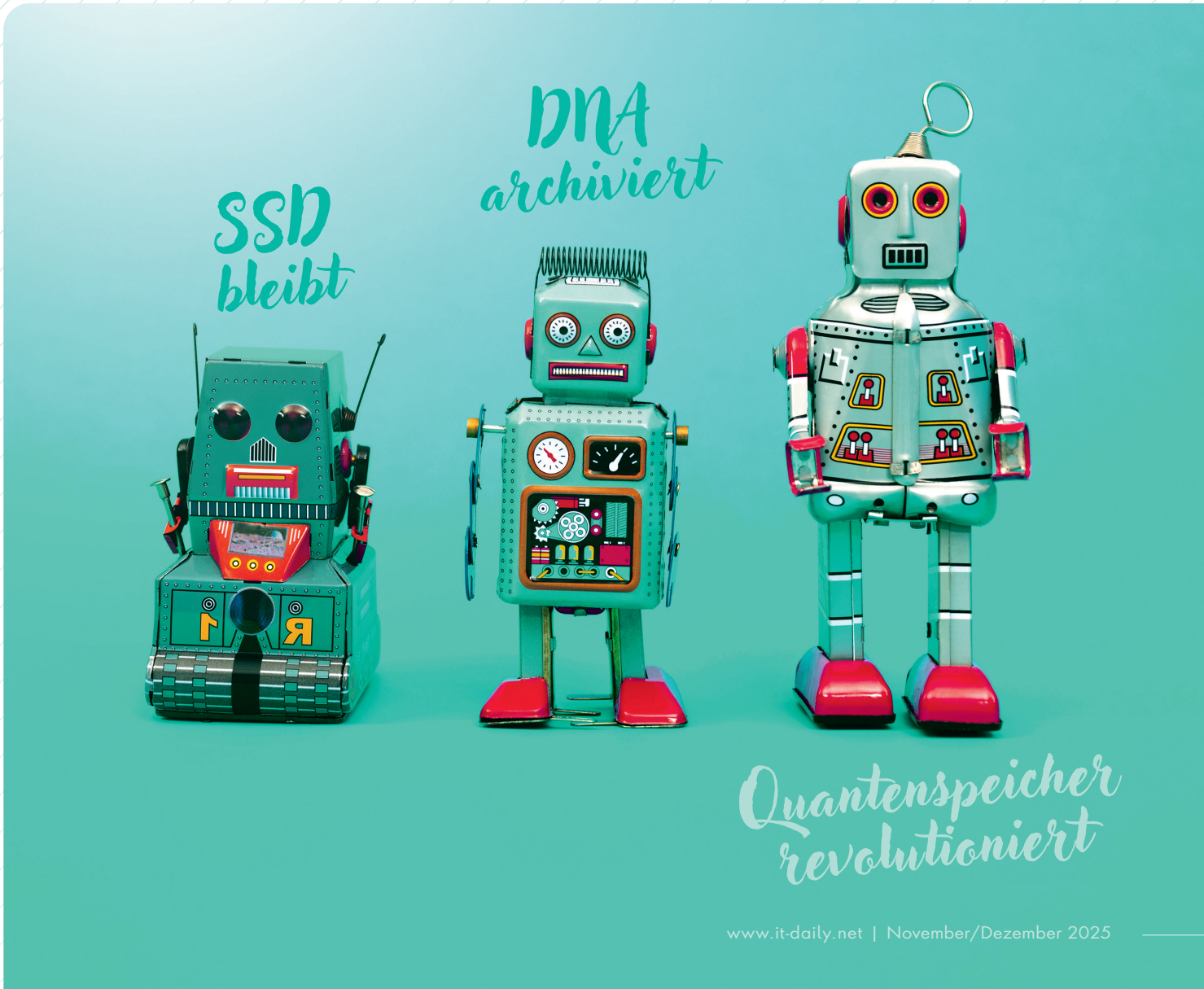
Quantenspeicher der Zukunft

Die wirkliche Revolution für die Speicherung von Quanteninformationen spielt sich in einem ganz anderen Bereich ab. Der beste „Speicher" für Qubits ist letztlich ein fehlertoleranter Quantencomputer selbst, der durch fortlaufende Fehlerkorrektur die Quantenzustände stabil hält. Für die Übertragung von Quanteninformationen über Distanzen, etwa in einem Quanteninternet, sind zudem Quantenspeicher (Quantum Memories) unverzichtbar. Diese physikalischen Systeme - wie Ionenfallen oder Fehlstellenzentren in Diamanten - können Quantenzustände kurzzeitig „einfrieren" und wieder auslesen und fungieren so als eine Art Quanten-Repeater.

Fazit: Speichermedien im Zeitalter des Quantencomputings

Zusammenfassend lässt sich also sagen: Quantencomputer werden die Festplatte im heimischen PC nicht ersetzen. Sie agieren als spezialisierte Beschleuniger in einem klassischen Rechenumfeld. Während holografische Speicher und DNA-Archivierung Antworten auf das generelle, durch Hochleistungsrechnen befeuerte Datenwachstum geben, liegt die eigentliche Speicherrevolution in der Entwicklung von Technologien, die Quantenzustände selbst zu manipulieren und zu übertragen vermögen.

Ulrich Parthier



Vom Blackbox-Risiko zum digitalen Assistenten

WIE AI-AGENTS UND AI-BUDDYS KONTROLLIERBAR BLEIBEN

Die Herausforderungen und Sorgen, die mit der Zunahme von KI-Technologien einhergehen, sind vielseitig. Sie reichen von Datenschutzbedenken und ethischen Vorbehalten bis hin zur Angst vor einem Kontrollverlust. Dergleichen ist nicht neu. Schon früher wurden disruptive Technologien mit anfänglicher Skepsis und Unsicherheiten betrachtet, bevor sie ihren Siegeszug antraten. Ähnliches gilt auch für KI. Da hilft nur Aufklärung, etwa darüber, welche KI-Modelle es gibt und wo sie sich am wirkungsvollsten einsetzen lassen.

Ein konkretes Einsatzszenario für KI ist beispielsweise der elektronische Datenaustausch (EDI), der viele Unternehmen vor Herausforderungen stellt – personell wie finanziell. Wer diese Situation zum Anlass nimmt, sich mit dem Thema KI auseinanderzusetzen und mutig genug ist, auf diese Technologie zu setzen, profitiert in doppelter Hinsicht. Zum einen lernt er die Chancen und Risiken der Technologie kennen, zum anderen sammelt er Erfahrung darüber, wie man sich KI bestmöglich zunutze machen kann.



DIE FRAGE FÜR UNTERNEHMEN SOLLTE NICHT MEHR LAUTEN, OB SIE KI EINSETZEN, SONDERN WANN UND IN WELCHEN BEREICHEN SIE DEN GRÖSSTEN MEHRWERT ERZIELEN KANN.

Lumir Boureanu, Geschäftsführer, compacer GmbH, www.compacer.com

Was unterscheidet einen AI-Buddy von einem AI-Agent?

Die Begrifflichkeiten rund um das Thema Künstliche Intelligenz (KI) befinden sich derzeit in einem dynamischen Wandel. Dennoch hat sich der Begriff AI-Agent zunehmend etabliert. Dabei handelt es sich um autonome Softwareprogramme, die auf Basis von Daten, entsprechendem Kontext und mittels Large Language Models (LLM) Entscheidungen treffen und zielgerichtet handeln, um definierte Ziele zu erreichen. Man kann also sagen, dass ein AI-Agent aktions- und systemorientiert vorgeht. In Unternehmen sind KI-Agenten digitale Mitspieler, die dabei helfen, Prozesse zu automatisieren, Entscheidungen zu optimieren und Ressourcen effizienter zu nutzen. Ihre Einsatzmöglichkeiten reichen von operativen Aufgaben bis hin zur strategischen Unterstützung.

Im Gegensatz dazu steht der AI-Buddy – ein Konzept, das ebenso in der digitalen Transformation von Unternehmen an Bedeutung gewinnt. AI-Buddys basieren meist auf LLM-Technologie, veredelt durch Expertenwissen, und sind darauf ausgelegt, Wissen bereitzustellen und im kommunikativen Austausch mit den Anwendern zu agieren. Sie unterstützen bei Aufgaben wie Informationsbeschaffung, Textverarbeitung oder Organisation, ohne dabei eigenständig zu handeln. Die Funktionsweise eines AI-Buddys ist also ausschließlich wissensorientiert.

Beide Systeme haben somit jeweils spezifische Einsatzbereiche und Mehrwerte, die sich – je nach Bedarfsfall – auch kombinieren lassen. Gerade in digitalen Geschäftsprozessen kann die Kombination aus aktionsorientierten Agenten und wissensorientierten Buddys neue Effizienzpotenziale erschließen.

Die Zukunft: KI-gesteuerter elektronischer Datenaustausch

Ein spezifisches Anwendungsfeld, sowohl für AI-Agents als auch AI-Buddys, ist EDI. Hier kann die Integration von KI das gesamte EDI-Ecosystem auf das nächste Level heben. Unternehmen, die beim elektronischen Datenaustausch auf KI setzen, verschaffen sich damit nicht nur ganz pragmatische Vorteile, sondern auf lange Sicht vor allem strategische. Warum? Weil KI dazu in der Lage ist, aus einem starren Dokumentenaustauschsystem eine intelligente Business-Plattform zu entwickeln.

Wie funktioniert das? Indem KI die Automatisierung komplexer Prozesse unterstützt und Systeme in die Lage versetzt, sich selbst zu optimieren – sprich, sie stößt einen weitgehend autonomen Verbesserungsprozess an, sodass sich die Verantwortlichen auf andere Aufgaben konzentrieren können.

Chancen der Modernisierung und Erfolgsfaktoren für KI

Mit dem Einsatz von AI-Agenten eröffnen sich Unternehmen vielfältige Potenziale. Gleichzeitig bietet die Auseinandersetzung mit technischen, ethischen und orga-



nisatorischen Fragen – wie etwa der Einhaltung von Datenschutzrichtlinien oder dem Schutz sensibler Geschäftsdaten – die Möglichkeit, robuste und zukunftssichere Lösungen zu entwickeln.

Ein wichtiger Aspekt bei der Einführung von KI ist darüber hinaus die Datenqualität. Fakt ist: Damit KI bestmöglich „performen" kann, benötigt sie hochwertige Daten, denn inkonsistente Daten führen zu Fehlern. Diese Datenqualität ist vielfach bei älteren EDI-Systemen problematisch, da diese zwar über viele, aber oft unvollständige Daten verfügen, sodass KI nur unzureichend – schlimmstenfalls fehlerhaft – wirken kann.

Auch vor Compliance-Richtlinien kann sich KI nicht drücken. Das bedeutet, dass die von KI gesteuerten Prozesse den gleichen Branchenvorschriften und Standards unterliegen wie die der Anwender. Das macht die Einführung und Nutzung von KI vor allem für stark regulierte Branchen oder KRITIS-Organisationen überaus anspruchsvoll.

Doch damit nicht genug. Insbesondere die Akzeptanz derer, deren Arbeit durch den Einsatz von KI betroffen ist, spielt eine wichtige Rolle im Hinblick auf den Erfolg der KI-Einführung. Gerade wenn Mitarbeiter Angst haben, wegen KI ihren Arbeitsplatz zu verlieren oder wenn sie sich sträuben, vertraute Arbeitsabläufe zu hinterfragen, ist es ratsam, diese Menschen frühzeitig einzubinden und aufzuklären. Nur so kann sichergestellt werden, dass die Einführung erfolgreich ist und nicht am Widerstand der Belegschaft scheitert.

WELCHE VORTEILE BIETEN AI-AGENTEN UNTERNEHMEN?

Automatisierung und Effizienz: AI-Agenten übernehmen Routineaufgaben wie Anomalie-Erkennung, Berichte oder E-Mail-Bearbeitung. Mitarbeitende können sich so stärker auf strategische Tätigkeiten konzentrieren.

Datenanalyse und Entscheidungsunterstützung: Sie erkennen Muster in großen Datenmengen, geben Empfehlungen und ermöglichen fundierte Echtzeitentscheidungen.

Skalierbarkeit: AI-Agenten passen sich flexibel an neue Anforderungen und Arbeitslasten an – auch bei Wachstum oder Spitzenzeiten ohne Qualitätsverlust.

Kostenoptimierung: Automatisierung und geringere Fehlerquoten senken Kosten, etwa in der Rechnungsverarbeitung oder Logistik.

Herausforderungen beim Einsatz von AI-Agenten

Technische Integration: Die Einbindung in bestehende IT-Landschaften ist komplex. Veraltete Systeme, inkompatible Schnittstellen und mangelhafte Datenqualität können den Rollout erschweren.

Datenqualität: Die Leistung hängt von hochwertigen Daten ab. Fehlerhafte Informationen führen zu Fehlentscheidungen.

Governance: Autonome Entscheidungen werfen Haftungsfragen auf, weshalb klare Zuständigkeiten und Governance-Strukturen unverzichtbar sind.

Akzeptanz und Change-Management: AI-Agenten verändern Prozesse und Rollen. Ohne Einbindung und Schulung der Mitarbeitenden drohen Widerstände.



Investition in Zukunftstechnologie: KI als strategischer Erfolgsfaktor

Die Einführung moderner KI-Technologie erfordert zu Beginn eine gezielte Investition – etwa in leistungsfähige Hardware, ausreichende Speicherkapazitäten, die Implementierung geeigneter KI-Module sowie den Aufbau von internem Know-how. Für kleinere Unternehmen kann dies zunächst eine Herausforderung darstellen.

Doch diese Investitionen sind strategisch sinnvoll: KI gilt als Schlüsseltechnologie der digitalen Zukunft. Sie eröffnet neue Möglichkeiten zur Effizienzsteigerung, zur Automatisierung von Prozessen und zur Entwicklung innovativer Geschäftsmodelle. Daher sollte die Frage für Unternehmen nicht mehr lauten, ob sie KI einsetzen, sondern wann und in welchen Bereichen sie den größten Mehrwert erzielen kann. Mit einem klaren Fahrplan lässt sich der Einstieg in die KI-Welt nachhaltig und wirtschaftlich gestalten.

Praxisbeispiel: Prozesse mit KI verschlanken und beschleunigen

Um erste Erfahrungen zu sammeln und einschätzen zu können, wie wirkungsvoll KI für ein Unternehmen sein kann, bietet sich der elektronische Datenaustausch (EDI) an. Hier lassen sich beispielsweise durch eine Kombination des AI-Agents und des AI-Buddys von compacer unterschiedliche Verbesserungen erzielen. Ein AI-Agent erkennt automatisch eine fehlerhafte Bestellnummer, während der AI-Buddy dem zuständigen Mitarbeiter sofort die Historie des Kunden anzeigt und eine Korrektur vorschlägt. So hat sich bereits gezeigt, dass KI-gesteuertes EDI nicht nur bis zu 90 Prozent der Prozesse automatisiert, sondern auch spürbare, intelligente Optimierungen ermöglicht, etwa die aussagekräftige, vielschichtige und schnelle Durchführung von Echtzeitanalysen. Darüber hinaus sorgen adaptive Standards, die sich fortwährend an Veränderungen anpassen, für messbare Mehrwerte.

Lumir Boureanu

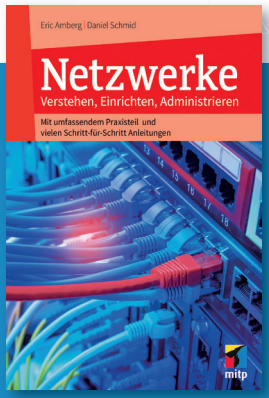
NETZWERKE

VERSTEHEN, EINRICHTEN, ADMINISTRIEREN

Netzwerk-Know-how ist in nahezu allen IT-Berufen unerlässlich – dieser praxisorientierte Leitfaden vermittelt es fundiert, verständlich und mit starkem Praxisbezug. Er richtet sich an angehende Netzwerkadministratoren, IT-Fachkräfte und technisch versierte Power-User.

Sie lernen wichtige Hardware-Komponenten und die komplette TCP/IP-Protokollfamilie kennen – von IPv4 und IPv6 über ICMP, ARP, TCP und UDP bis hin zu DNS, DHCP und gängigen Anwendungsprotokollen. Anhand nachvollziehbarer Schritt-für-Schritt-Anleitungen setzen Sie ein vollständiges Netzwerk in einer virtuellen Umgebung um. Sie konfigurieren IP-Adressen, Switches und Router (z.B. mit Cisco-Geräten), richten Active Directory ein und implementieren zentrale Netzwerkdienste. Ein eigenes Kapitel zur Fehlersuche zeigt Ihnen bewährte Tools und Methoden für effektives Troubleshooting.

Auf diese Weise erfahren Sie, wie moderne Netzwerke konzipiert, implementiert, abgesichert und langfristig betrieben werden und lernen bewährte Best Practices zur Segmentierung, zum Einsatz von Firewalls und zur Einrichtung von VPNs kennen – praxisnah und direkt umsetzbar.



Netzwerke – Verstehen, Einrichten, Administrieren

Eric Amberg, Daniel Schmid; mitp Verlags GmbH & Co.KG; 10-2025

e3mag.com

Information und Bildungsarbeit von und für die SAP-Community



E3 ist die Antwort.

Was war die Frage?

Jetzt 3 Monate kostenlos testen!

Erhalten Sie Zugang zur Welt der SAP-Community:

✓ Exklusive Interviews, Markttrends und Hintergründe
✓ Online und als hochwertiges Print-Magazin
✓ Läuft automatisch aus – völlig unverbindlich

Jetzt mit Promocode: itv25
e3mag.com/de/abo/e3

© ra2 studio, Shutterstock.com

SAP® ist eine eingetragene Marke der SAP SE in Deutschland und in den anderen Ländern weltweit.

e3mag.com

Mit künstlicher Intelligenz die Zukunft gestalten

KI, CONTENT & SICHERHEIT IM FOKUS

Wir erleben aktuell eine Zäsur. Künstliche Intelligenz übernimmt schon heute nicht nur Routineaufgaben, sondern verändert von Grund auf, wie Inhalte erstellt, verarbeitet und genutzt werden. Mittlerweile nutzen in Deutschland bereits 37 Prozent der Unternehmen KI, so eine Studie von IW Köln[1]. Diese Entwicklung eröffnet enorme Chancen, bringt aber auch immer mehr Risiken mit sich.

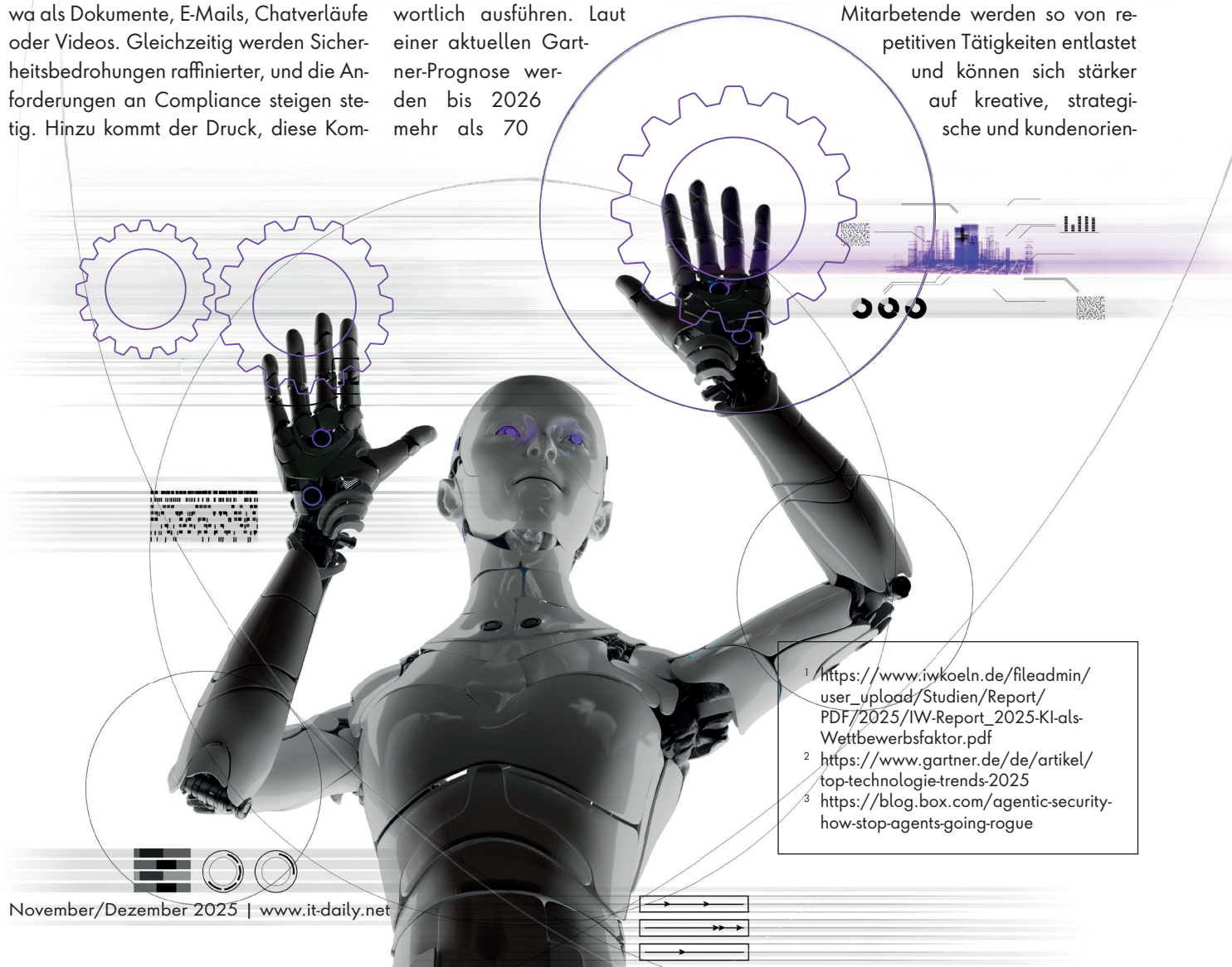
Die Menge an Content explodiert und rund 90 Prozent aller Unternehmensdaten liegen heute unstrukturiert[2] vor – etwa als Dokumente, E-Mails, Chatverläufe oder Videos. Gleichzeitig werden Sicherheitsbedrohungen raffinierter, und die Anforderungen an Compliance steigen stetig. Hinzu kommt der Druck, diese Komplexität in Echtzeit zu managen. Das stellt Unternehmen vor die Aufgabe, ihre Strategien neu auszurichten. Es entscheidet nicht allein die Wahl der Technologie, sondern die Fähigkeit, Vertrauen bei Mitarbeitenden, Kunden und Partnern aufzubauen.

KI Agenten als neue Akteure in Workflows

Immer häufiger agieren sie wie eigenständige Teammitglieder, die Aufgaben steuern, Entscheidungen vorbereiten und ganze Prozesse eigenverantwortlich ausführen. Laut einer aktuellen Gartner-Prognose werden bis 2026 mehr als 70 Prozent der Unternehmen KI-Agenten in zentrale Geschäftsprozesse, von Kundenservice und IT-Support bis hin zu Sicherheits- und Compliance-Workflows, integriert haben[3].

In der Praxis reicht dieses Spektrum von einfachen Assistenten, die Standardanfragen bearbeiten, bis hin zu Agentensystemen, die komplette Workflows planen und ausführen. Unternehmen, die hier bereits erste Schritte gegangen sind, berichten von erheblichen Effizienzgewinnen.

Mitarbetende werden so von repetitiven Tätigkeiten entlastet und können sich stärker auf kreative, strategische und kundenorien-



[1] https://www.iwkoeln.de/fileadmin/user_upload/Studien/Report/PDF/2025/IW-Report_2025-KI-als-Wettbewerbsfaktor.pdf
[2] https://www.gartner.de/de/artikel/top-technologie-trends-2025
[3] https://blog.box.com/agentic-security-how-stop-agents-going-rogue



tierte Aufgaben konzentrieren. Damit verschiebt sich das Verhältnis zwischen Mensch und Maschine und Organisationen müssen herausfinden, wie sie diese neue Arbeitsteilung aktiv gestalten, beispielsweise durch klare Rollenbilder, neue Verantwortlichkeiten und gezielte Qualifizierung.

Sicherheit neu denken

Traditionelle Sicherheitsmechanismen sind auf das Reagieren nach einem Angriff ausgelegt. Doch Cyberbedrohungen bewegen sich in maschineller Geschwindigkeit. Ein reines Hinterherlaufen reicht nicht aus. Sicherheit muss als selbstlernender, vorausschauender Prozess verstanden werden.

Neue Technologien zeigen, wie das aussehen kann:

Automatische Klassifizierung sensibler Inhalte: KI erkennt und schützt kritische Daten ohne manuelle Eingriffe.

Proaktive Bedrohungsanalysen in Echtzeit: Anomalien und Angriffsmuster werden identifiziert, bevor sie Schaden anrichten.

Früherkennung von Ransomware-Aktivitäten: Angriffe können gestoppt werden, noch bevor Verschlüsselungen beginnen.

Auf diese oder ähnliche Weise fungiert KI wie ein zusätzliches Teammitglied, das neue Kompetenzen mit einbringt.

Auch jenseits der Sicherheit bietet Automatisierung großes Potenzial. KI-Agenten übernehmen Routineaufgaben, beschleunigen Abläufe und verbessern Entscheidungen. Das steigert Produktivität und senkt Risiken. Zusammenarbeit wird zunehmend hybrid – Mensch und Maschine agieren gemeinsam und dafür sind Vertrauen, klare Prozesse und eine offene Innovationskultur entscheidend.

Unternehmen müssen zukunftssicher handeln

KI verändert nicht nur Prozesse, sondern auch die Anforderungen an Sicherheit und Governance. Um den Wandel erfolgreich zu gestalten, braucht es eine ganzheitliche Strategie, die Verantwortung und Innovation verbindet.

1. Strategien regelmäßig evaluieren

Sicherheits- und Content-Strategien müssen dynamisch bleiben. Authorization Checks sorgen dafür, dass KI-Agenten nur auf Inhalte zugreifen, für die sie berechtigt sind – ein wichtiger Schutz vor Datenexposition und Compliance-Verstößen.

2. Governance mit Human-in-the-Loop

Mit wachsender Autonomie steigt das Risiko unbeabsichtigter Aktionen. Tool Guardrails und Human-in-the-Loop-Workflows schaffen hier Kontrolle und Transparenz: Kritische Entscheidungen werden geprüft, bevor sie umgesetzt werden.

3. Teams befähigen

Mitarbeitende müssen verstehen, wie KI sicher und verantwortungsvoll eingesetzt wird. Schulungen und klare Richtlinien fördern Vertrauen und machen KI zu einem verlässlichen, kontrollierten Partner im täglichen Arbeiten.

Ausblick: Intelligenter Content wird Standard

Die Zukunft liegt in Inhalten, die nicht mehr passiv gespeichert werden, sondern sich selbst aktiv organisieren. Dokumente, Verträge oder multimediale Dateien können sich selbst klassifizieren, mit Schutzmechanismen versehen und im richtigen Kontext nutzbar machen. Anstatt dass Mitarbeitende Zeit für das Durchsuchen von Datensilos verschwenden, stehen die relevanten Informationen jederzeit zur Verfügung: sicher, aktuell und vollständig.

Für Unternehmen wird Content damit vom Kostenfaktor zum Werttreiber. Daten, die bisher brachlagen, lassen sich in Echtzeit analysieren und für strategische Entscheidungen nutzen. Compliance wird nicht mehr als Hürde erlebt, sondern als integrierter Bestandteil der Wertschöpfungskette. Gleichzeitig sinkt das Risiko menschlicher Fehler, weil Sicherheitsmechanismen automatisch greifen.

Die entscheidende Frage lautet daher nicht mehr, ob Unternehmen KI einsetzen, sondern auf welche Weise. Erfolgreich werden die Organisationen sein, die Technologie mit Verantwortung verbinden. Das sind diejenigen, die Sicherheit und Governance nicht als Gegenspieler von Innovation sehen, sondern als Grundlage für nachhaltiges Wachstum. Wer Vertrauen, Kreativität und Effizienz in Einklang bringt, wird im Wettbewerb deutlich im Vorteil sein und Content in einen Erfolgsfaktor verwandeln.

Michael Pietsch



DIE ZUKUNFT LIEGT IN INHALTEN, DIE NICHT MEHR PASSIV GESPEICHERT WERDEN, SONDERN SICH SELBST AKTIV ORGANISIEREN.

Michael Pietsch, Vice President DACH & Eastern Europe, Box, www.box.com



ERP meets KI

BUNDESMINISTERIUM FÖRDERT ENTWICKLUNG EINER ON-PREMISES-KI-PLATTFORM

Fertigungsunternehmen der Einzel-, Auftrags- und Variantenfertigung sind verpflichtet, hochsensible Daten – Konstruktionsdetails, Preiskalkulationen, personenbezogene Informationen und Vertragsinhalte – vor unerwünschtem Datentransfer zu schützen. Die Verwendung öffentlicher Large Language Models wie ChatGPT stellt ein erhebliches Compliance- und Sicherheitsrisiko dar, da diese Daten in unkontrollierte externe Systeme fließen können.

Dieses Szenario möchte der ERP-Anbieter ams.Solution verhindern, indem er seinen Kunden die sichere und datenschutzkonforme Nutzung von „Künstlicher Intelligenz (KI)" auf jeweils bei den Anwenderunternehmen lokal installierten Plattformen ermöglicht.

Bereits seit vier Jahren arbeiten die Spezialisten des Softwarehauses intensiv an der Bereitstellung einer adaptiven On-Premises-RAG-Architektur für die kontextsensitive Analyse von Daten, die aus der Branchenstandardsoftware ams.erp stammen. Für die Realisierung dieses im Vergleich zur simplen Einbindung cloudbasierter KI-Plattformen technisch anspruchsvolleren Verfahrens wurde ein eigenes Experten-Team gegründet. Das große Potenzial und die übergeordnete Relevanz dieses KI-Modells für den gesamten ERP-Markt wurde kürzlich dadurch verdeutlicht, dass das Bundesministerium für Forschung, Technologie und Raumfahrt die Entwicklungsarbeit unterstützt und entsprechende Forschungsgelder bereitstellt.

Sichere KI für den Mittelstand

Der Leiter des KI-Projekts bei ams.Solution, André Finken, beschreibt die Bereitstellung einer lokal installierbaren KI-Plattform ohne jegliche Online-Anbindung zur direkten Kommunikation mit dem ERP-System als Alleinstellungsmerkmal im Markt. Die Entwicklung der Architektur, die die semantische Suche innerhalb der betriebswirtschaftlichen Standardsoftware ams.erp ermöglicht, setzt laut seiner Aussage das Verständnis komplexer KI-Zusammenhänge voraus. Dadurch habe das Projekt etwas mehr Zeit beansprucht, als wenn lediglich die hinreichend bekannten Cloud-Dienste eingebunden worden wären. Auf der anderen Seite seien die marktführenden Anwenderunternehmen aus dem Mittelstand, die aus Sicherheitsgründen größtenteils immer schon On-Premises-ERP-Installationen bevorzugten, weiterhin deutlich besser gegen den unbemerkten Abfluss ihrer digitalen Informationen ins Web geschützt. „Um die Datensouveränität unserer Kunden zu gewährleisten, haben wir nicht bloß die hinlänglich bekannten Cloud-Komponenten zusammengesteckt. Vielmehr haben wir gemeinsam mit unserem Partner AI/UI eine leistungsfähige und sichere KI-Umgebung geschaffen, die den Usern die vollständig selbstbestimmte Kontrolle über die Nutzung, Verarbeitung und Speicherung der eigenen Daten gibt", bringt es der Projektverantwortliche auf den Punkt.

Lokale KI-Installationen erfüllen Datenschutzregularien

Dies ist in Augen des Experten nicht nur reiner Selbstschutz, sondern wird auch mit Blick auf die Gesetzgebung höchste Relevanz erlangen. Im Rahmen des EU AI Act wurde bereits im Februar 2025 das Verbot bestimmter KI-Systeme in Kraft gesetzt. Seit August 2025 müssen zudem nationale Behörden benannt sein, die die Umsetzung der gesetzlichen Vorgaben überprüfen. Denn spätestens ab August

2026 wird es vollständige Compliance-Pflichten geben.

In diese Richtung zielt auch das Bundesforschungsministerium in seiner Begründung für die Bewilligung der Fördergelder. Das Kriterium der technologischen Neuartigkeit sei vor allem in Bezug auf den Schutz unternehmenskritischer Informationen erfüllt. Der Aufbau einer On-Premises-Lösung zur KI-basierten Aufbereitung von Daten aus einer Enterprise-Resource-Planning (ERP)-Plattform sei deshalb ein Novum, weil für diesen Anwendungszweck bislang häufig Cloud-API-basierte Large-Language-Model (LLM)-Dienste verwendet wurden, bei denen Kundendaten das lokale Rechenzentrum während der Verarbeitung verlassen. Dies stellt auch in den Augen der wissenschaftlichen Gutachter ein Problem für den Datenschutz dar. Weiter heißt es, dass das Produkt einer On-Premises-Lösung für LLM-Dienste im hauseigenen ams.erp-System den derzeitigen Stand der Technik übertreffe.

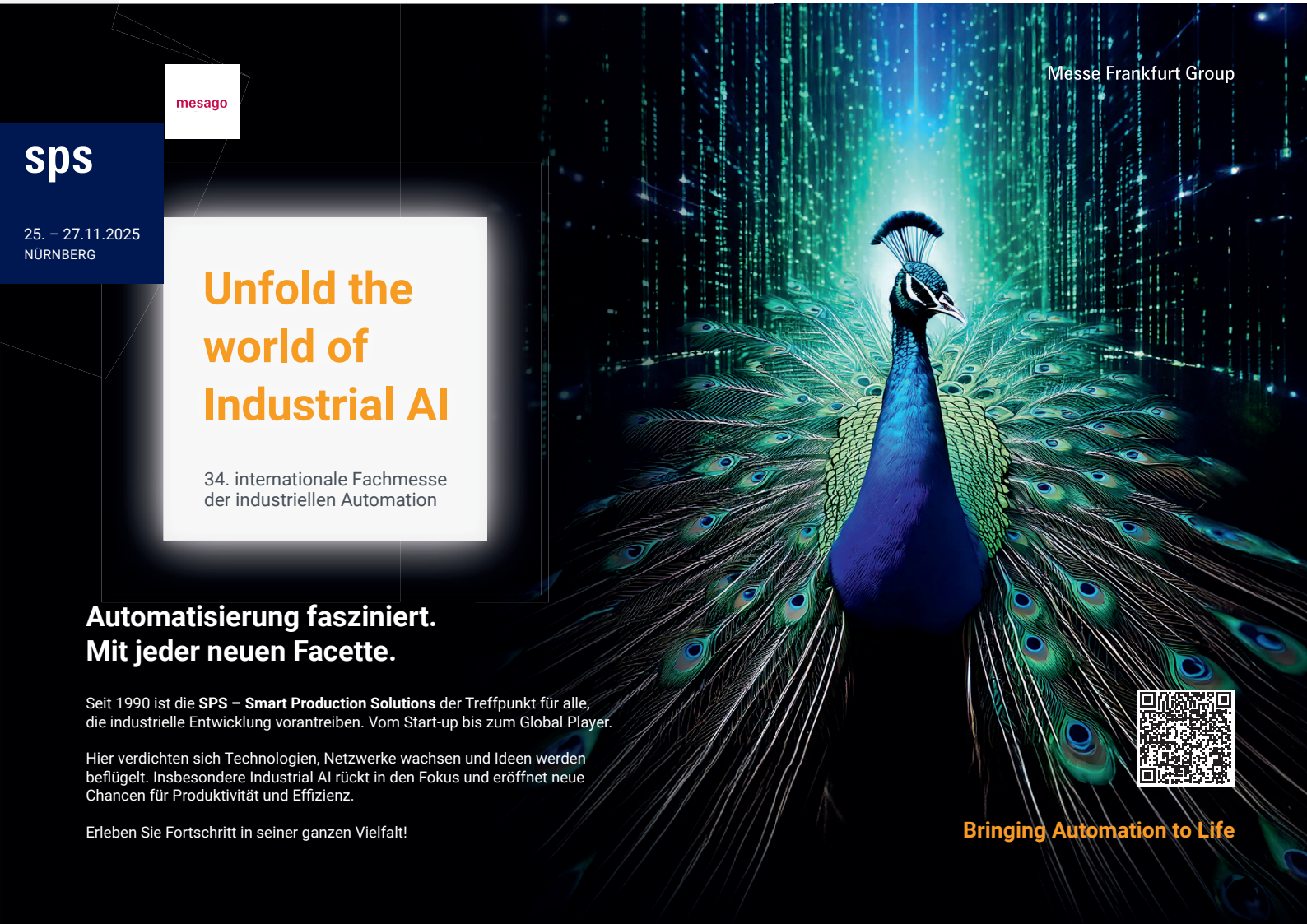
Für Nikas Schröder, Vorstand Entwicklung bei ams.Solution, ist diese Argumentation die Bestätigung dafür, in Sachen KI auf das richtige Pferd gesetzt zu haben: „Viele unserer Kunden haben sich in den letzten Jahren aus gutem Grund für ams.erp und den Aufbau lokaler IT-Architekturen entschieden. Warum sollte diese Risikobewertung nun in Bezug auf die Einbindung von KI auf einmal eine andere sein?“ In seinen Gesprächen mit vielen ams-Kunden wurde ihm zuletzt immer wieder bescheinigt, dass der Sicherheitsaspekt mehr denn je ganz oben auf der Agenda der Verantwortlichen von Unternehmen aus dem Umfeld der Losgröße 1+ steht.

www.ams-erp.com



UM DIE DATENSOUVERÄNITÄT UNSERER KUNDEN ZU GEWÄHRLEISTEN, HABEN WIR GEMEINSAM MIT UNSEREM PARTNER AI/UI EINE LEISTUNGSFÄHIGE UND SICHERE KI-UMGEBUNG GESCHAFFEN.

André Finken, Head of AI, ams.Solution AG, www.ams-erp.com





Transformationen und Datenmigrationen im SAP-Umfeld

ZWISCHEN LEGACY UND CLOUD: AGILITÄT ALS SCHLÜSSELFAKTOR

Unternehmen stehen heute vor einem nie dagewesenen Tempo der Veränderung. Fusionen, Carve-outs, Systemkonsolidierungen und Cloud-Migrationen sind längst keine punktuellen Projekte mehr – sie gehören zum kontinuierlichen Geschäft. SAP-ERP-Systeme, die zentrale Finanz-, Personal- und Lieferkettenprozesse steuern, bilden dabei das Rückgrat zahlreicher Geschäftsmodelle. Ihre Komplexität, jahrzehntelang gewachsene Anpassungen und die enge Verzahnung von Stammdaten, Bewegungsdaten und Workflows machen jede Transformation zu einer anspruchsvollen Aufgabe. Fehlende Transparenz, unzureichende Planung oder manuelle Datenprozesse können Geschäftsunterbrechungen, Compliance-Risiken oder Dateninkonsistenzen verursachen.



Die Dimensionen erfolgreicher SAP-Transformationen

Die technische Dimension solcher Transformationen erfordert präzise Analyse, Automatisierung und Softwaregestützte Umsetzung. Moderne Plattformen ermöglichen es, SAP-Landschaften vollständig zu erfassen, Abhängigkeiten zwischen Modulen, Prozessen und Daten zu erkennen und Transformationsszenarien zu simulieren. So lassen sich Risiken frühzeitig erkennen, Migrationen beschleunigen und Ressourcen effizient einsetzen. Zentral ist dabei die selektive Datenmigration: Nicht alle historischen Daten sind für den zukünftigen Betrieb relevant. Durch die Bewertung nach Qualität, Volumen, Governance und Nutzung können Unternehmen nur die notwendigen Informationen übertragen, Redundanzen vermeiden und die Downtime minimieren. Hybride Migrationsansätze erlauben zudem, bestehende Strukturen mit neuen Zielsystemen flexibel zu kombinieren, um sowohl Innovation als auch Stabilität zu gewährleisten.

Global tätige Unternehmen sehen sich zusätzlich mit regulatorischen und Compliance-Herausforderungen konfrontiert. Daten müssen über Ländergrenzen hinweg den Datenschutzanforderungen, branchenspezifischen Vorgaben und internationalen Standards entsprechen. Transparenz, Revisionssicherheit und kontinuierliches Monitoring sind dabei unverzichtbar. Softwaregestützte Lösungen bieten nicht nur technische Sicherheit, sondern auch eine nachvollziehbare Dokumentation für Audits und regulatorische Prüfungen.

Die strategische Dimension von Transformationen geht über Technik hinaus. Anpassungsfähige SAP-Landschaften sind Enabler für Business Agility: Sie ermöglichen es, Geschäftsbereiche dynamisch zu verschieben, ineffiziente Prozesse aufzulösen und Ressourcen gezielt neu zu verteilen. Cloud-Migrationen, harmonisierte Datenstrukturen und automatisierte Prozesse schaffen die Grundlage, Entscheidungen schnell, fundiert und global abzustimmen. Unternehmen, die diese Flexibilität nutzen, können Kapital effizient einsetzen, Wettbewerbsvorteile sichern und neue Geschäftschancen schneller realisieren.

Künstliche Intelligenz und moderne Analytik erweitern diese Möglichkeiten. KI-Systeme können Datenbestände prüfen, Abhängigkeiten analysieren und Transformationen simulieren, bevor die operative Umsetzung beginnt. Dadurch lassen sich Engpässe und Optimierungspotenziale erkennen, Projektzyklen verkürzen und die Qualität der Datenbasis erhöhen. In Verbindung mit Cloud-Infrastrukturen entsteht eine flexible, skalierbare Plattform, die kontinuierliche Anpassungen erlaubt und die Geschwindigkeit von Transformationsprojekten erheblich steigert.

Transformationen sind heute kein einmaliges Unterfangen mehr, sondern fortlaufende Prozesse. Unternehmen, die ihre Systemarchitektur vorausschauend gestalten, können nicht nur auf Marktveränderungen reagieren, sondern auch Daten als strategisches Asset nutzen. Automatisierte Migrationsprozesse, kontinuierliche Datenvalidierung und integrierte Governance sorgen dafür, dass Transformationsprojekte nicht nur effizient umgesetzt werden, sondern auch zukunftssicher bleiben.



Globale Perspektiven zeigen zudem, dass harmonisierte SAP-Landschaften die Grundlage für eine internationale Skalierung bilden. Einheitliche Prozesse und Datenstrukturen erlauben es, Märkte schneller zu erschließen, Compliance über Regionen hinweg sicherzustellen und Geschäftsmodelle flexibel anzupassen. Dies gilt nicht nur für Fusionen oder Carve-outs, sondern ebenso für die Migration in Public Clouds oder die Integration neuer Unternehmensbereiche.

Zusammenspiel von Exzellenz und Agilität

Ein global tätiges Pharmaunternehmen hat innerhalb von 18 Monaten ein SAP-ECC-System mit über 85 Terabyte Daten selektiv auf SAP S/4HANA migriert – bei minimaler Downtime und deutlicher Reduktion technischer Altlasten. Auch ein großer Energieversorger konnte über 500 Gesellschaften und zahlreiche SAP-Systeme in eine einheitliche, harmonisierte S/4HANA-Landschaft überführen. Durch systematische Analyse von Abhängigkeiten und schrittweises Vorgehen wurden Risiken minimiert und die Transformation kontrolliert umgesetzt. Ein weiteres Beispiel liefert ein internationaler Einzelhändler, der im Zuge einer strategischen Neuausrichtung Geschäftseinheiten ausgliedern und seine SAP-Systeme trennen musste – auch hier gelang eine präzise, selektive Datenmigration innerhalb eines engen Zeitrahmens.

Diese Fälle verdeutlichen: Unternehmen, die auf Automatisierung, Transparenz und selektive Migration setzen, sichern sich Effizienz und Stabilität und legen zugleich die Grundlage für eine fortlaufende, zukunftssichere Transformation.

Wer jetzt handelt, gestaltet die Zukunft

Die Zukunft von SAP-Transformationen liegt in der Kombination aus technischer Exzellenz, globaler Perspektive und strategischer Agilität. Unternehmen, die diesen Dreiklang beherrschen, können ihre IT-Landschaften kontinuierlich optimieren, Risiken minimieren und gleichzeitig den Wert ihrer Daten und Prozesse für nachhaltige Wertschöpfung steigern. Business Agility wird damit zum zentralen Erfolgsfaktor: Wer flexibel auf Veränderungen reagiert und gleichzeitig präzise, sichere und automatisierte Transformationen umsetzt, schafft die Voraussetzungen, um im globalen Wettbewerb erfolgreich zu sein.

Unternehmen, die Transformation weiterhin als einmaliges Projekt begreifen, laufen Gefahr, ihre technologische und organisatorische Handlungsfähigkeit zu verlieren. Veraltete Systeme, unklare Datenstrukturen und fehlende Agilität führen zu langen Reaktionszeiten, ineffizienten Prozessen und wachsender Abhängigkeit von Einzelanpassungen. Im globalen Wettbewerb bedeutet das: Innovationshemmung statt Wachstum. Dagegen positionieren sich Organisationen, die heute in kontinuierliche Transformation und agile Arbeitsweisen investieren, als Gestalter ihres Wandels. Sie schaffen Strukturen, die Veränderung nicht nur ermöglichen, sondern beschleunigen – und entwickeln ein Mindset, das Transformation als dauerhaften Erfolgsfaktor versteht. Diese Unternehmen sind in der Lage, neue Technologien, regulatorische Anforderungen und Marktveränderungen schnell zu integrieren – und damit auch in Zukunft widerstandsfähig, skalierbar und wettbewerbsfähig zu bleiben.



Paola Krauss
www.snpgroup.com

So viel KI war noch nie

STARFACE 10 STELLT DIE WEICHEN AUF ZUKUNFT

Ende September lud die STARFACE-Gruppe ihre Community zur jährlichen Partnerkonferenz in den Europa-Park Rust – und die Resonanz war beeindruckend: Über 700 Fachhändler, Systemintegratoren und Technologiepartner folgten der Einladung, um sich aus erster Hand über die Roadmap von STARFACE und estos zu informieren und zu erfahren, wie es nach der Übernahme durch die britische Gamma Group weitergeht. Die Karlsruher nutzten die große Bühne, um zu zeigen, warum sie seit Jahren als Innovationstreiber im deutschen UCC-Markt gelten. Mit Version 10 ihrer Kommunikationsplattform präsentierten sie ein Release, das dank praxisnaher KI-Funktionen zum echten Gamechanger werden könnte – und dem Channel neue Chancen für lukratives Solution Selling eröffnet.

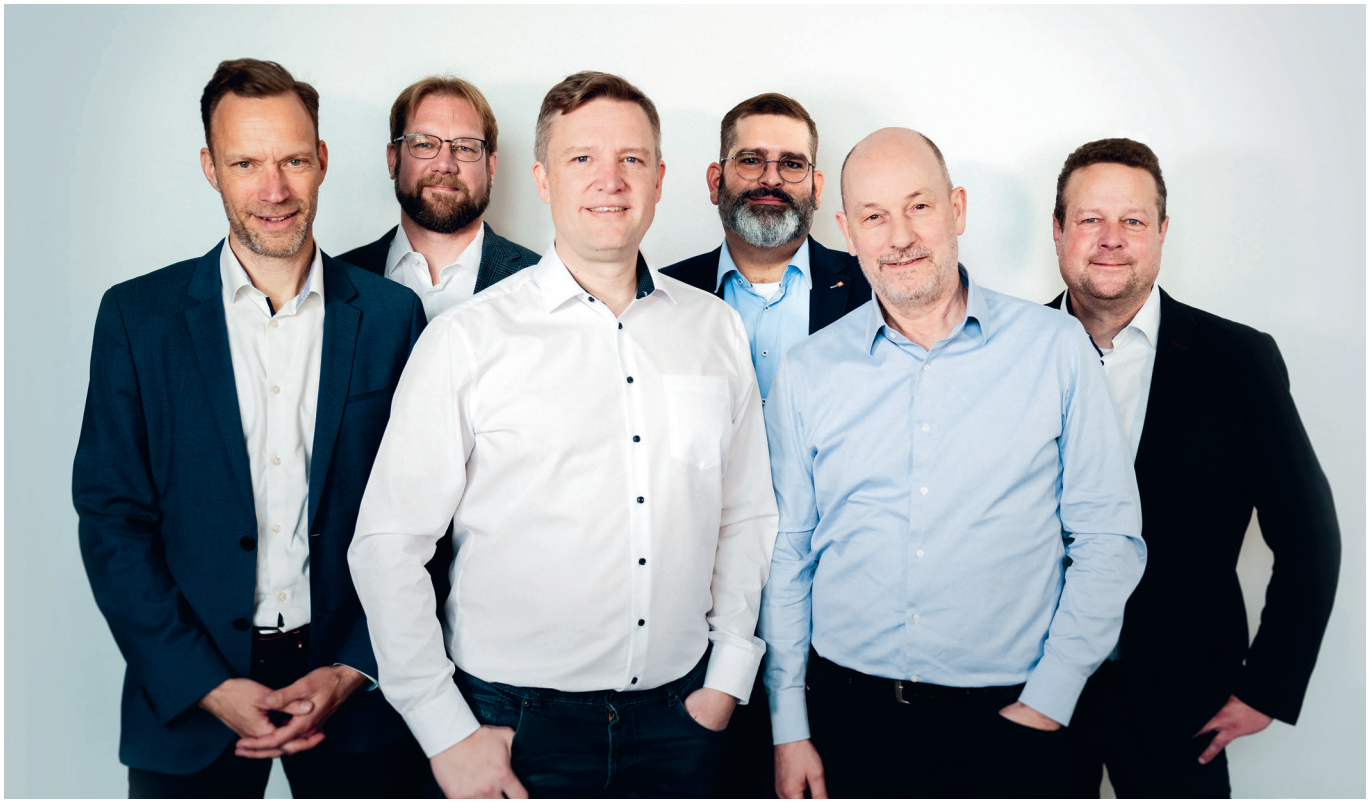
KI als Schlüsseltechnologie – aber mit Augenmaß

Künstliche Intelligenz ist das Thema der Stunde – doch viele Unternehmen tun sich schwer, aus der Technologie echten Nutzen zu ziehen oder sie wirtschaftlich zu verwerten. Auch für STARFACE war der Weg in die KI-Welt kein Selbstläufer. Was die Karlsruher in Rust zeigten, dokumentiert jedoch eindrucksvoll, dass sie die Weichen richtig gestellt haben.

Eine zentrale Rolle spielt dabei die neu entwickelte STARFACE 10, die ab Dezember verfügbar sein wird. Ihre modernisierte technische Basis schafft die Voraussetzung für die Integration smarter KI-Funktionen. Herzstück ist dabei der neue STARFACE Hub, eine dedizierte Cloud-Plattform, über die Anwender gezielt die gewünschten Services abrufen können. Der Hub ist bewusst anbieterneutral konzipiert, sodass sich unterschiedlichste KI-Modelle anbinden lassen.

Drei Beispiele für gelebte KI im UCC-Alltag

Wie die KI-basierte Zukunft konkret aussieht, demonstrierte STARFACE in Rust anhand dreier praxisnaher Use Cases, die ab Version 10 verfügbar sein werden:



Nach der Übernahme von STARFACE im Februar 2025 hat Gamma das Führungsteam in Deutschland reorganisiert. Florian Buzin (STARFACE CEO), vorne, leitet zusätzlich Gamma Communications Deutschland. Christoph Scheuermann (ehemals Produktmanagement STARFACE) verantwortet nun Produktmanagement, Marketing und Operations. Alexander Seyferth (ehemals estos CEO) übernimmt Sales, Customer Care und Academy. Thomas Weiß (STARFACE CTO) bleibt für Development und IT zuständig. Gerben Wijbenga koordiniert als Managing Director Europe die Aktivitäten in DACH, Benelux und Spanien. Andreas Hampel (ehemaliger HFO Telecom) leitet die Bereiche SIP und NGN.

#1 Intelligente Anrufweiterleitung (IVR):
Dank KI-gestützter Sprachanalyse erkennt das System die Anliegen der Anrufer und verbindet sie automatisch mit dem am besten qualifizierten Ansprechpartner – ganz ohne starre Menüstrukturen oder Tastendruck. Nutzer formulieren ihr Anliegen einfach in natürlicher Sprache und gelangen so schneller ans Ziel.

#2 Automatische Gesprächstranskription:
Gespräche können in Echtzeit transkribiert und automatisch in der jeweiligen Kundenakte abgelegt werden. Das erleichtert die Nachbearbeitung, spart Zeit und schafft Transparenz im Kundenkontakt.

#3 Smarter Warteschlangen-Bot
Für das STARFACE-eigene Warteschleifen-Modul iQueue wurde ein Bot entwickelt, mit dem sich individuelle Standard-Fragen konfigurieren lassen. Diese verkürzen dem Anrufer die Wartezeit und bereiten das folgende Gespräch mit dem Agenten vor, denn damit lassen sich wichtige Infos schon vorab klären (Kundennummer etc). So geht der Agent besser vorbereitet in das Gespräch mit dem Kunden.

Datenschutz bleibt oberstes Gebot
Bei aller Begeisterung für KI dürfen Datenschutz und Datensicherheit selbstverständlich nicht auf der Strecke bleiben. Die neuen KI-Funktionen sind daher alle optional – es läuft nichts automatisch im Hintergrund, und es gibt keine versteckten Datenflüsse. Der Kunde oder Partner entscheidet selbst, ob und wie er eine Funktion nutzt.

Neue Chancen für den Channel
Mit dem Go-live von STARFACE 10 erhalten Partner die Möglichkeit, die neuen KI-Funktionen aktiv in Kundenprojekten umzusetzen. Das eröffnet Spielraum für Integrationsdienstleistungen, Managed Services und Support – auch wenn die konkreten Geschäftsmodelle rund um KI noch im Entstehen sind.

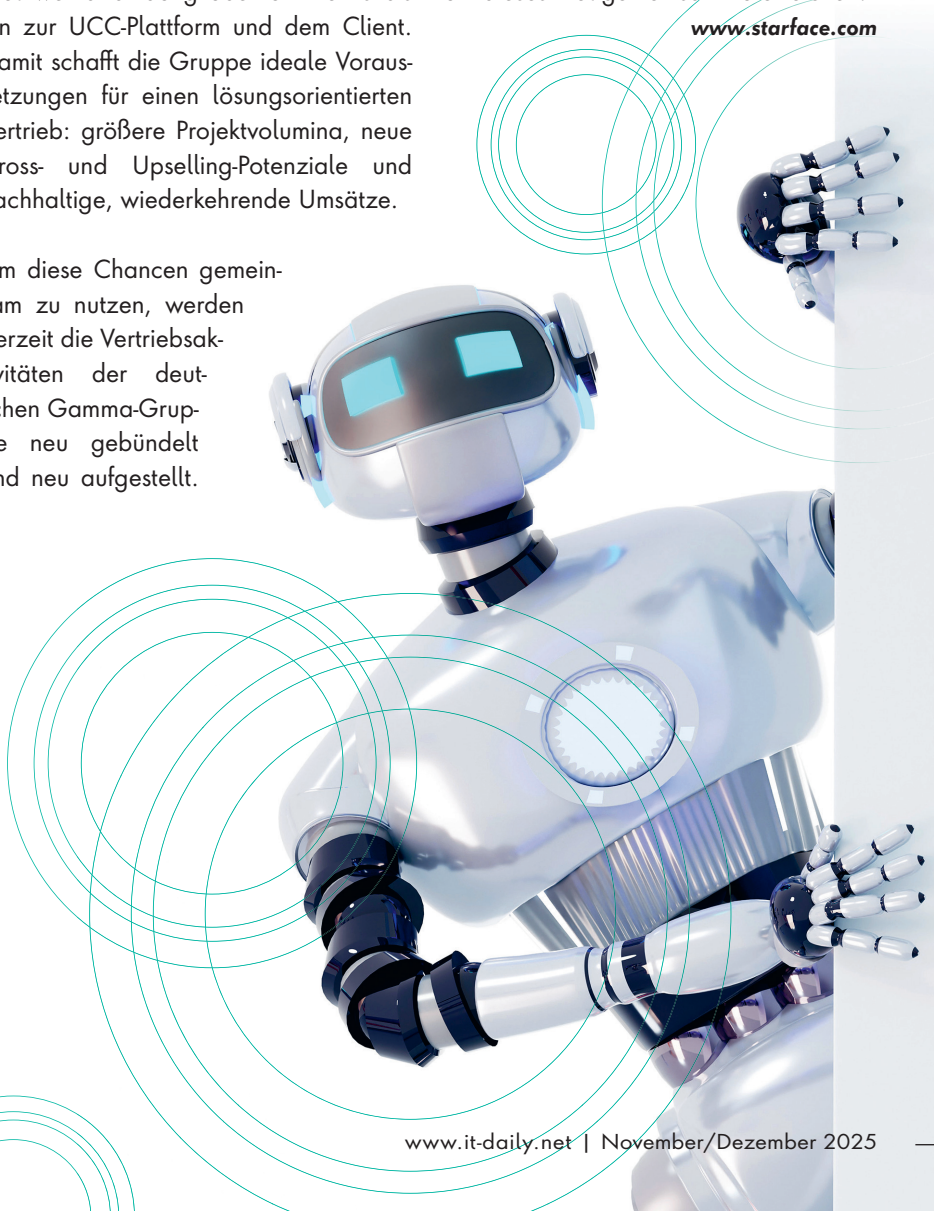
„Welche Monetarisierungsmodelle sich daraus entwickeln, wird sich erst zeigen", erklärt Florian Buzin, Geschäftsführer von STARFACE. „Es ist ein bisschen wie in der Frühphase des Internets: Das Potenzial ist offensichtlich, aber die Geschäftsmodelle müssen sich noch finden. Unsere Aufgabe sehen wir darin, die Plattform bereitzustellen – unsere Partner werden darauf aufbauen und den Mehrwert für ihre Kunden konkretisieren."

Vom Produktverkauf zum Lösungsanbieter
Die Möglichkeiten, die dem Channel dabei offenstehen, sind dank der Integration der Marken STARFACE, estos und Gamma Communications (ehemals HFO) in die Gamma-Gruppe vielfältiger denn je – denn das durchgängige Produkt- und Lösungs-Portfolio reicht heute von der Netzwerkanbindung über SIP-Trunks bis hin zur UCC-Plattform und dem Client. Damit schafft die Gruppe ideale Voraussetzungen für einen lösungsorientierten Vertrieb: größere Projektvolumina, neue Cross- und Upselling-Potenziale und nachhaltige, wiederkehrende Umsätze.

Um diese Chancen gemeinsam zu nutzen, werden derzeit die Vertriebsaktivitäten der deutschen Gamma-Gruppe neu gebündelt und neu aufgestellt. Dies soll es dem Unternehmen ermöglichen, die Partner der Gamma-Gruppe im Endkundengeschäft noch gezielter zu unterstützen und die Vermarktung integrierter Komplettlösungen voranzutreiben.

Auf Kurs Richtung Top 3
Dabei verfolgen STARFACE und die gesamte Gamma-Gruppe ambitionierte Ziele: Mittelfristig wird der Sprung in die Top 3 der deutschen Business-Telekommunikationsanbieter angestrebt. „Wir werden weder die Telekom noch Vodafone überholen", räumt STARFACE CEO Florian Buzin ein. „Aber die dritte Position ist derzeit nicht klar besetzt – und wir sind überzeugt, dass wir die Gamma-Gruppe dort erfolgreich etablieren können. Gamma hat in kurzer Zeit eine Reihe starker Marken unter einem ebenso starken Dach vereint. Das ist eine hervorragende Basis, um dieses Ziel gemeinsam zu erreichen."

www.starface.com





Zwischen Laser und Latenz

WARUM EINE INTELLIGENT ZUSAMMENGESCHALTETE WELTRAUMWIRTSCHAFT SO WERTVOLL FÜR DIE MENSCHHEIT IST

Von GPS über Mobiltelefone bis hin zu Verkehrsampeln – das Leben auf dem Boden hängt immer stärker von Technologien im Erdorbit ab. Damit Flugzeuge sicher navigieren, Autos fahren und Menschen rund um den Globus zuverlässig miteinander kommunizieren können, richten Regierungen ihren Blick immer häufiger zu den Sternen. Beispiel USA: Unter dem Dach der United States Space Force arbeiten private und öffentliche Organisationen zusammen, um die Interessen der Nation im Weltraum zu schützen. Gleiches gilt für die Europäische Union. Mit IRIS² plant der Staatenbund, 290 eigene Satelliten in die Umlaufbahn zu transportieren, um die eigene digitale Unabhängigkeit zu sichern. Nicht anders die neue Bundesregierung, die in der jüngsten Raumfahrtstrategie den Weltraum in den Fokus von Politik und Wirtschaft stellt.



Ob in den USA, Europa oder anderswo – all dies geschieht aus gutem Grund. Der Kosmos birgt milliardenschwere Chancen. Laut McKinsey und Weltwirtschaftsforum soll die weltraumbasierte Wirtschaft in den kommenden Jahren mit 9 Prozent jährlich deutlich stärker wachsen als das globale Bruttoinlandsprodukt. Von 2024 bis 2035 steigen die Umsätze von 630 Milliarden US-Dollar auf 1,8 Billionen US-Dollar – und erreichen damit eine ähnliche Größe wie die Halbleiterbranche. Was die Entwicklung antreibt, sind beispielsweise Rohstoffe wie Platin, Iridium oder Kobalt. Diese machen den extraterrestrischen Bergbau attraktiv. Gleichzeitig wird der Orbit zum Reiseziel. Mit seinem Start-up Blue Origin befördert Amazon-Gründer Jeff Bezos Touristen ins All und wieder zurück.

LEO-Satelliten verkürzen Datendurchlaufzeiten

Rohstoffe, Tourismus oder Staatsinteressen – egal, welche Ziele die Menschheit jenseits der Stratosphäre verfolgt, leistungsfähige Konnektivität ist dafür die Basis. Konnektivität, wie sie etwa LEO-Satelliten ermöglichen. Diese laufen ihren geostationären Pendants gerade technologisch den Rang ab. Wie ihnen das gelingt: Weil sie näher an der Erde kreisen, erreichen Signale ihr Ziel deutlich schneller. Der Vorteil: Dauerten Datendurchläufe bei GEO-Satelliten in hoher Umlaufbahn sonst zwischen 400 und 700 Milli-

sekunden, verkürzt sich diese Zeit im erdnahen Orbit (Low Earth Orbit, LEO) auf nur 20 bis 50 Millisekunden.

DE-CIX und DLR optimieren LEO-Datenverkehr

Vom Breitband-Internet für abgelegene Landstriche über Backhaul-Systeme für den Mobilfunk bis hin zur Edge-Konnektivität – Anwendungen wie diese machen LEO-Konstellationen möglich. Applikationen, die auf möglichst minimale Latenzen angewiesen sind. Um die Grenzen des technologisch Machbaren weiter zu verschieben, forscht DE-CIX aktuell mit dem Deutschen Zentrum für Luft- und Raumfahrt an innovativen Lösungen, um den Datenverkehr zwischen LEO-Satelliten und Bodenstationen weiter zu optimieren. Als Teil des OFELIAS-Projekts der Europäischen Weltraumorganisation zielt die Arbeit bis Juli 2026 darauf ab, Protokolle, Algorithmen und Verfahren zu entwickeln, die die Netzauslastung intelligent steuern und somit Probleme durch wetterbedingte Abschattungen reduzieren. Denn sind die Flugkörper wie im Projekt nicht per Funk, sondern über Laser verbunden, erlaubt das zwar höhere Bandbreiten und schnellere Informationsflüsse. Aber zugleich sind optische Übertragungen anfälliger für atmosphärische Störungen: Nebel, Wolken und Regen bremsen die Signale aus.

Mobilfunk von der Erde für Mond und Mars

Abgeschiedene Randgebiete mit Internet und Content-Angeboten versorgen, Daten überall auf dem Planeten schneller austauschen und selbst in Flugzeugen in der Luft oder auf Schiffen im Ozean mit dem eigenen Smartphone mobil online sein: Laut Deloitte soll die LEO-Wirtschaft im Jahr 2035 rund 312 Milliarden US-Dollar wert sein. Projekte wie OFELIAS, die Himmel und Erde intelligenter zusammenschalten, liefern dafür eine erste technologische Basis. Eine Basis, die mehr und mehr zum neuen digitalen Rückgrat für die Menschheit wird, wenn sie so zu den Sternen greift, wie es andere bereits vormachen: Nokia hat auf dem Mond ein



VON RECHENZENTREN ÜBER EDGE-EINHEITEN BIS HIN ZUR CLOUD FÜR KÜNSTLICHE INTELLIGENZ (KI) – WAS HEUTE NOCH NACH SCIENCE-FICTION KLINGT, WIRD ZUNEHMEND REAL.

Ivo Ivanov,
CEO, DE-CIX, www.de-cix.net

4G/LTE-Mobilfunknetz installiert. Kommende Missionen werden das Netz nutzen, um den Erdtrabanten zu erforschen. So sollen etwa Fahrzeuge und Basen über das Nokia Lunar Surface Communications System einfacher miteinander kommunizieren und Informationen austauschen können. Ziel ist es, herauszufinden, wie zuverlässig und leistungsfähig Mobilfunk von der Erde auch auf anderen Himmelskörpern funktioniert – und das mit Blick auf kommende Marsflüge.

KI im Orbit: Die Zukunft der Weltraum-Rechenzentren

Von Rechenzentren über Edge-Einheiten bis hin zur Cloud für Künstliche Intelligenz (KI) – was heute noch nach Science-Fiction klingt, wird zunehmend real. Erste Experimente mit Satelliten zeigen, wie KI bereits im Orbit Daten analysieren kann. Künftige Weltraum-Rechenzentren lassen sich über die Sonne mit Strom versorgen und die extrem niedrigen Temperaturen im Vakuum kühlen. Die Vorteile: Deutlich geringere Betriebskosten als am Boden und neue Perspektiven für energieintensive KI-Modelle. So sieht eine Machbarkeitsstudie im Auftrag der Europäischen Union KI-Rechenzentren schon bald im Erdorbit. Bis 2050 soll 1 GW Kapazität verfügbar sein. Was das Marktpotenzial betrifft, so gehen die Autoren von Thales Alenia Space von mehreren Milliarden Euro bis 2050 aus.

Space-IX: Internetknoten für das Weltall

Ob für erdnahe Satelliten, das KI-Training in der Umlaufbahn oder den ersten Außenposten unserer Spezies auf einem fremden Himmelskörper – um eine Infrastruktur wie diese so effizient wie möglich zu verbinden, braucht es schnelles Internet zwischen Erde und Kosmos. Genauso wie Internet Exchanges (IX) die Netzwerke auf dem Boden zusammenschalten und zusammenhalten, sollen sie auch im Weltall Netze untereinander verbinden. Mit dem Space-IX bereitet sich DE-CIX auf diese Zukunft vor und baut bereits am ersten Internetknoten für den Orbit. Denn überall dort, wo Netze entstehen, wird Interconnection folgen. Die intelligente Zusammenschaltung von LEO-Satelliten ist dabei nur der erste Schritt. Der Space-IX wird die Bedürfnisse von Nutzern, Applikationen und Netzbetreibern erfüllen, die sich im Weltall untereinander und mit terrestrischen Inhalten, Clouds und Anwendungen verbinden möchten.

Der wahre Wert einer intelligent zusammengeschalteten Weltraumwirtschaft

Von Logistik und Transport über Lebensmittel bis hin zur Verteidigung – laut Weltwirtschaftsforum und McKinsey sind das einige der Branchen, die in der kommenden Dekade am stärksten vom Boom der Weltallökonomie profitieren sollen. Fest steht aber, der wahre Wert des Chancenraums zwischen den Sternen geht deutlich über den rein unternehmerischen hinaus. Klimaveränderungen überwachen, Katastrophen erkennen, Hilfseinsätze koordinieren und die soziale Teilhabe sichern: Zwar sind erste intelligent zusammengeschaltete Satelliten nur ein kleiner Schritt für die Menschen, aber ein gewaltiger Sprung für die digitale Infrastruktur, die die Menschheit auf ihrem Weg in den Kosmos braucht.

Ivo Ivanov



Innovativ statt oversized

WIE MONITORING WIEDER BEZAHLBAR WIRD

Ein System fällt aus, die Dashboards blinken rot, der Service Desk wird mit Warnungen überflutet. 153 Meldungen in wenigen Minuten – und doch keine klare Antwort. Wer ist betroffen? Wie kritisch ist die Lage? Während das Team sortiert, steigen Druck und Kosten. Die Mitarbeiter oder Kunden warten, die Budgets laufen davon.

Genau hier zeigt sich ein Grundproblem: Klassische Monitoring-Ansätze mit festen Schwellenwerten, manueller Konfiguration und isolierten Tools stoßen in dynamischen IT-Landschaften längst an ihre Grenzen. Sie liefern zwar viele Daten, aber keinen echten Kontext. Auf der anderen Seite stehen Observability-Plattformen, die jede Bewegung in der Infrastruktur erfassen. Sie versprechen Transparenz – und verursachen dabei schnell eine Kostenlawine. Denn mit jedem zusätzlichen Log und jedem Container wächst auch die volumenbasierte Abrechnung.

Das Ergebnis: Die einen Tools sehen zu wenig, die anderen zu viel. IT-Teams verlieren Zeit im Alarmchaos und Führungskräfte verlieren den Überblick über Budgets und Compliance. Es ist ein Dilemma, das viele Unternehmen kennen. Und es ist ein Dilemma, das nach Innovation verlangt.

Ein neuer Ansatz für modernes Monitoring

USU Multi Cloud Monitoring (MCM) ist eine Antwort auf genau dieses Spannungsfeld. Statt alte Tools weiterzuentwickeln, wurde die Plattform von Grund auf neu gedacht – für hybride Umgebungen, dynamische Systeme und wachsende Anforderungen an Sicherheit und Effizienz.

Die Idee ist einfach: Monitoring soll nicht mehr belasten, sondern entlasten. Statt Alarmflut gibt es klare Priorisierung. Statt unklarer Datenfülle verständliche Analysen. Statt Kostenfallen ein transparentes Modell, das auch bei Wachstum planbar bleibt.

Klarheit statt Komplexität

MCM bündelt alle relevanten Informationen in einem zentralen Dashboard – unabhängig davon, ob Systeme in der Cloud, on-Premises oder hybrid laufen. Ereignisse werden automatisch korreliert, damit nicht hunderte Warnungen entstehen, wenn in Wahrheit nur eine Ursache dahintersteckt. IT-Teams sehen sofort, welche Services betroffen sind und wie kritisch die Lage ist.

Besonderer Wert wurde dabei auf Anwenderfreundlichkeit gelegt. Denn am Ende geht es nicht um Technik-Faszinati-

MEHR WERT

Webinar: IT-Ausgaben im Griff

on, sondern um die Menschen, die jeden Tag für stabile Services sorgen müssen.

KI, die nützlich ist

Auch künstliche Intelligenz spielt eine Rolle – allerdings gezielt und nachvollziehbar. Die Plattform identifiziert automatisch die wahre Ursache eines Vorfalls, zeigt die Auswirkungen auf betroffene Services und schlägt Maßnahmen vor. Wer eine Frage hat, bekommt über ein Chat-Interface direkt eine Antwort – ohne tiefe Vorkenntnisse oder lange Schulungen. So wird KI nicht zur Black Box, sondern zu einem praktischen Werkzeug.

Innovation heißt auch volle Kostenkontrolle

Eine der größten Neuerungen steckt im Preismodell. Während viele Observability-Anbieter ihre Gebühren am Datenvolumen festmachen, geht MCM einen anderen Weg. Keine versteckten Kosten, keine bösen Überraschungen bei Lastspitzen – sondern einfache, transparente Lizenzen. Für Unternehmen bedeutet das: Budgets bleiben berechenbar, selbst wenn die IT wächst oder kurzfristig stark ausgelastet ist.

Gerade für öffentliche Verwaltungen und regulierte Branchen ist diese Klarheit ein entscheidender Vorteil. Aber auch Mittelstand und Konzerne profitieren, wenn Monitoring nicht länger ein finanzielles Risiko darstellt.

Monitoring, das Zukunft hat

USU Multi Cloud Monitoring ist damit mehr als ein weiteres Tool – es ist ein Neuanfang. Ein Bruch mit alten Mustern, bei dem Innovation nicht in mehr Komplexität mündet, sondern in Vereinfachung. Statt Datenlawine gibt es Überblick, statt Eskalationen fundierte Entscheidungen, statt unberechenbarer Kosten eine klare Linie.

Ab 2026 wird MCM verfügbar sein, schon heute lässt sich die Lösung in Demos erleben. Entwickelt wurde sie gemeinsam mit IT-Teams, die wissen, wie es ist, Verantwortung für stabile Services zu tragen.



MCM BÜNDELT ALLE RELEVANTEN INFORMATIONEN IN EINEM ZENTRALEN DASHBOARD – UNABHÄNGIG DAVON, OB SYSTEME IN DER CLOUD, ON-PREMISES ODER HYBRID LAUFEN.

Frank Laschet,
Senior Marketing Manager,
USU GmbH, www.usu.com

Wer also nicht länger zwischen starren Klassikern und überladenen Observability-Plattformen wählen möchte, findet hier eine dritte Option – ein Monitoring, das zur Realität passt und den Blick frei macht für das, was wirklich zählt: eine stabile, effiziente und zukunftsfähige IT.

Frank Laschet





Quelle: AdobeStock

Der Weg zur AI-getriebenen und zukunftssicheren IT

WARUM GANZHEITLICHE TRANSFORMATION MEHR IST ALS PLATTFORM-MIGRATION

Wer wettbewerbsfähig bleiben will, muss sich digitalisieren. So weit, so verstanden. Dennoch tun sich viele Unternehmen weiterhin schwer mit dem digitalen Wandel. Hemmnisse sind die Anforderungen an den Datenschutz, der Fachkräftemangel – insbesondere in den Bereichen Data & Analytics, IT-Security und Compliance – und fehlende zeitliche und finanzielle Ressourcen. Folglich geht es nur langsam voran mit der Transformation. Immerhin: Die Bereitschaft, zu investieren, ist vorhanden, um nicht noch weitere Marktanteile zu verlieren und ganz abgehängt zu werden.

Bei der Überlegung, in welche Bereiche diese Investitionen fließen, sollten auch Managed Services in Betracht gezogen werden. Managed Services können dazu beitragen, kosteneffizient Geschäftsprozesse zu optimieren, neue Technologien und Innovationen zu integrieren und gleichzeitig strategische Themen umzusetzen. IT-Dienstleister bieten an dieser Stelle immer häufiger partnerschaftliche Unterstützung, nicht nur operativ, sondern auch bei der Weiterentwicklung des Geschäfts.

Konkret Application Managed Services umfassen weit mehr als einen klassischen Helpdesk. Sie bieten einen Full Managed Service über die gesamte Kette hinweg: vom 1st-Level-Support (Helpdesk, Standardanfragen), über tiefere technische Analysen und Problemlösungen im 2nd-Level bis hin zur hochspezialisierten Expertise im 3rd-Level-Support.

Darüber hinaus gehören der operative Betrieb, 24/7-Monitoring sowie umfassende Cloud-Infrastruktur-Services wie Architekturplanung, Hosting, Migration und CloudOps bis hin zur SaaS-Integration dazu. Anwendungen werden dann vollständig aus der Cloud bereitgestellt und vom Dienstleister betrieben. Der Kunde muss sich weder um das Hosting noch um die Installation oder Wartung und Support kümmern. Ein wesentlicher Bestandteil ist DevOps, also die enge Verzahnung von Entwicklung und Betrieb, wodurch Anwendungen nicht nur stabil betrieben, sondern auch kontinuierlich verbessert und agil weiterentwickelt werden können.

Gleichzeitig sind Security und Compliance integraler Bestandteil eines ganzheit-

lichen AMS-Portfolios. Von Cybersecurity über Identity & Access Management bis hin zur Einhaltung regulatorischer Anforderungen.

Ein weiterer Erfolgsfaktor ist die konsequente Automatisierung, zunehmend auch mit AIOps-Ansätzen: Standardaufgaben werden automatisiert, Logs und Events KI-gestützt analysiert, Anomalien frühzeitig erkannt. So werden Qualität, Geschwindigkeit und Verfügbarkeit spürbar verbessert.

Nicht zuletzt geht es bei AMS auch um die Optimierung von Kosten und Performance, also darum, die gesamte IT-Landschaft nicht nur stabil, sondern auch effizient und zukunftssicher zu betreiben.

Auf diese Weise entsteht ein ganzheitliches Service-Modell, das IT-Abteilungen nachhaltig entlastet und gleichzeitig die Grundlage für Innovation und digitale Transformation schafft.

Von Managed Services zur IT-Modernisierung

Plattformen, Infrastruktur oder Applikationen in professionelle Hände zu geben, ist eine Möglichkeit. Die andere ist, sich Unterstützung bei der Modernisierung der IT zu holen.

Veraltete, schwer zu wartende (geschäftskritische) Legacy-Systeme sind in vielen Unternehmen weit verbreitet, oft verbunden mit historischen Daten. Sie werden den heutigen komplexen Anforderungen kaum noch gerecht und können nicht mehr ordentlich betrieben und weiterentwickelt werden. Dadurch besteht eine hohe Abhängigkeit von IT-Dienstleistern, was wiederum kostenintensiv ist. Gleichzeitig besteht die Gefahr, dass talentierte Fachkräfte das Unternehmen für eine modernere Arbeitsumgebung verlassen und ihr Wissen mitnehmen – ohne dass es vorher dokumentiert wurde.

Die Überlegung, wie die digitale Infrastruktur zukunftssicher und unabhängig gestaltet werden kann, sollte daher ganz oben auf der Agenda stehen. Moderne Systeme können die geschäftliche Flexibilität langfristig sichern, zu datenbasierten strategischen Entscheidungen in Echtzeit beitragen und eine digitale Innovationskultur fördern. Bei der Umsetzung empfiehlt es sich, zunächst die gesamte vorhandene IT-Landschaft, einschließlich der Abhängigkeiten, Schnittstellen und Prozesse sowie deren Schwachstellen und Risiken, automatisiert zu analysieren. Dabei sollten verschiedene Quellsprachen wie ABAP, Assembler, Cobol, Java und RPG untersucht werden. Dadurch kann verlorenes Wissen rekonstruiert und darauf basierend eine zielgerichtete, effiziente Modernisierungsstrategie entwickelt werden.

Das Vorgehen bewährt sich vor allem bei historisch gewachsenen Systemen, die oft schlecht oder gar nicht dokumentiert sind. Die Ergebnisse sollten anschließend mit der gesamten Organisation abgestimmt werden. Maßnahmen mit maximalem Geschäftswert und hoher Machbarkeit werden priorisiert. Auf dieser Basis werden Lösungen definiert, die schnell messbare Ergebnisse erzielen. Umfassender operativer Support stellt sicher, dass die neuen Systeme langfristig stabil laufen.



IMMER MEHR UNTERNEHMEN NEHMEN MANAGED SERVICES IN ANSPRUCH, UM RESSOURCEN FÜR DIE DIGITALE TRANSFORMATION FREIZUSETZEN.

Peter Heppt, Business Unit Lead AMS Germany, Nagarro, www.nagarro.com

Mehr als „lift and shift“

Wichtig bei der Modernisierung von Legacy-Systemen ist: Sie sollte nicht nach der „Lift-and-Shift“-Methode erfolgen, sondern ganzheitlicher durchgeführt werden. Denn sie umfasst weit mehr als nur das System: Hardware, Applikationen, Interfaces, Prozesse und die Menschen, die damit arbeiten. Für die Modernisierung stehen unterschiedliche Ansätze zur Verfügung, die je nach Ausgangslage individuell kombiniert werden können. Das kann etwa die Migration bestehender Anwendungen auf eine moderne Plattform, die Konvertierung in neue Sprachen, eine Neuentwicklung, der Ersatz durch Standardsoftware oder auch die schrittweise Weiterentwicklung bestehender Systeme sein. Eine weitere Möglichkeit besteht darin, Legacy-Systeme auf modernen Plattformen wie Linux zu emulieren. Dies reduziert vor allem die hohen Betriebskosten klassischer Legacy-Umgebungen und schafft finanzielle Spielräume, um gezielt in Modernisierung und Innovationen zu investieren. In manchen Fällen ist es sinnvoll, Anwendungen in die Wartung zu geben oder endgültig abzuschalten.

Entscheidend ist, dass die gewählte Strategie immer auf maximalen Geschäftswert und Zukunftsfähigkeit ausgerichtet ist.

Die Modernisierung bildet die Grundlage für den Einsatz von KI. Ohne modernisierte Systeme, keine Datenqualität, Schnittstellen und Flexibilität. Darauf aufbauend können Unternehmen AI-Lösungen implementieren und durch MLOps-Prozesse dauerhaft betreiben, optimieren und weiterentwickeln. In einem nächsten Schritt geht es darum, diese neuen AI-Workloads ebenfalls professionell zu managen. Stichwort ManagedAI. So schließt sich der Kreis von AMS über Modernisierung hin zu einer zukunftssicheren, AI-getriebenen Unternehmens-IT. Unternehmen, die diesen Weg konsequent gehen, schaffen nicht nur Stabilität und Effizienz, sondern sichern sich auch die notwendige Innovationskraft, um im digitalen Wettbewerb langfristig erfolgreich zu sein.

Peter Heppt

AI Factory

EIN FLIESSBAND FÜR KI-USE-CASES



EINE AI FACTORY IST MEHR ALS INFRASTRUKTUR. SIE VERANKERT KÜNSTLICHE INTELLIGENZ SICHER IM UNTERNEHMEN UND MACHT ES FIT FÜR DIE ZUKUNFT.

Bruno Maddaloni,
Solutions Architect und CTO Ambassador, Dell Technologies,
www.dell.com/de-de

Mit generativer und agentenbasierter KI hat Künstliche Intelligenz jetzt die Reife erreicht, die Unternehmen für nutzbringende Anwendungen benötigen. Die Implementierung gehen sie am besten mit einer zentralen „AI Factory" an – denn sie sorgt für Effizienz, Sicherheit und Skalierbarkeit.

Künstliche Intelligenz ist nicht neu. Doch mit dem Aufkommen von GenAI und Agentic AI erhält sie jetzt den entscheidenden Schub. Immer mehr Unternehmen möchten Künstliche Intelligenz im großen Stil nutzen und breit in ihre Geschäftsprozesse integrieren. KI wird zunehmend zu einem entscheidenden Faktor für Effizienz, Innovation und Wettbewerbsfähigkeit. Wer sie nicht einsetzt, riskiert, gegenüber Unternehmen in Rückstand zu geraten, die schneller auf Marktveränderungen reagieren und datengetriebene Chancen nutzen können. Künstliche Intelligenz ist daher nicht länger nur eine optionale Technologie, sondern ein strategisches Werkzeug, das Unternehmen an vielen Stellen helfen kann.

Von Digitalen Assistenten bis zu Coding Assistants

Zu den vielen nutzbringenden Use Cases zählen beispielsweise Digitale Assistenten, die mithilfe von Large Language Models (LLMs) in Dialogform Informationen bereitstellen und dabei helfen, Entscheidungen vorzubereiten. Solche Assistenten können im Kundenservice von Unternehmen oder im Bürgerservice von Behörden zum Einsatz kommen, aber auch intern zur Unterstützung von Mitarbeitern im Vertrieb, in der Personalabteilung oder in der IT. Durch die Einbindung von KI-Agenten, die nicht nur Antworten generieren, sondern auch aktiv prüfen, recherchieren und verifizieren, lässt sich der Wahrheitsgehalt der Aussagen von Digitalen Assistenten noch einmal deutlich erhöhen.



MIT EINER AI FACTORY SCHAFFEN UNTERNEHMEN DIE BASIS, KI EFFIZIENT, SICHER UND SKALIERBAR IN IHRE PROZESSE ZU INTEGRIEREN.

Christian Scharrer,
Enterprise Architect und CTO Ambassador, Dell Technologies,
www.dell.com/de-de

Fertigungsunternehmen können von Computer-Vision-Systemen profitieren. Mit ihnen lässt sich etwa die Qualitätskontrolle automatisieren, indem Kameras Werkstücke auf Risse, Verformungen und Montagefehler prüfen oder Produktionslinien überwachen und Abweichungen sofort erkennen. In Verbindung mit Agentic AI sind solche Systeme nicht nur in der Lage, Probleme zu identifizieren, sondern auch darauf zu reagieren – beispielsweise, indem zusätzliche Agenten andere Informationen aus dem Produktionsprozess verarbeiten und analysieren, um etwa Rückschlüsse auf mögliche Ursachen zu ziehen und Vorschläge zur Optimierung aufzubereiten. Eine Vision ist, dass sich zukünftig sogar Entscheidungen zur Korrektur komplett autonom treffen lassen. Dann werden die Produktionsabläufe mit KI nicht nur kontrolliert, sondern aktiv optimiert.

Auch bei der Softwareentwicklung kann Künstliche Intelligenz eine wichtige Rolle spielen. KI-basierte Lösungen helfen im gesamten Entwicklungsprozess. Agenten unterstützen Mitarbeiter dabei, Code schneller zu verstehen und arbeiten ihnen bei Aufgaben wie Codegenerierung, Dokumentation, Qualitätschecks, Testaufgaben und Performance-Optimierung zu. Sie erkennen Muster im Code, identifizieren potenzielle Sicherheitslücken und machen Vorschläge zur Verbesserung der Codequalität. Entwickler können Agenten in natürlicher Sprache Aufgaben stellen, etwa, Code zu ändern, Bugs zu beheben oder neue Funktionalitäten einzupflegen. Völlig autonom kann die Entwicklung derzeit noch nicht erfolgen, aber mit agentenbasierter KI lassen sich bereits recht komplexe Workflows steuern, was vor allem in umfangreichen Software-Projekten ein großer Vorteil ist.

Ein Produktionssystem für Künstliche Intelligenz aufbauen

Wegen der vielen Chancen, die KI Unternehmen eröffnet, ist der Wunsch verständlich, möglichst schnell erste Anwendungen umzusetzen zu wollen. Dabei besteht aber das Risiko, dezentrale Einzelprojekte zu schaffen, die dann in Insellösungen münden, die kostspielig und ineffizient sind, Sicherheitsrisiken bergen können und nur schlecht skalieren.

Das können Unternehmen vermeiden, indem sie die Implementierung von Künstlicher Intelligenz strategisch angehen und eine so genannte „AI Factory" aufbauen – eine IT-Plattform, die als eine Art Produktionssystem für KI fungiert, Daten, Rechenleistung und KI-Software in einer standardisierten Umgebung zusammenführt und es damit ermöglicht, neue Use Cases wie Produkte in einer Fabrik effizient herzustellen, zu testen und auszurollen. Das ermöglicht es, mit einem Anwendungsfall zu starten und schnell zu skalieren, sprich: weitere Use Cases zu implementieren.

Die Einrichtung einer solchen KI-Fabrik beginnt mit der Identifizierung und Priorisierung der Anwendungsfälle. Die entscheidenden Kriterien sind dabei Relevanz, Reichweite und Machbarkeit. Welche Prozesse generieren den größten Geschäftswert? Wo liegen ihre „Pain Points" in Form von ineffizienten Schritten? Welche Möglichkeiten gibt es, diese Schritte mit KI zu beschleunigen oder zu automatisieren? Mit solchen Fragen können Organisationen herausfinden, welche Use Cases die höchste Relevanz besitzen. Anschließend sollten sie klären, wie groß die Dringlichkeit der einzelnen Anwendungsfälle ist, welche Reichweite sie innerhalb des Unternehmens haben und welche sich vielleicht besonders schnell umsetzen lassen. Am Ende steht eine Art Roadmap, die festlegt, welche Use Cases in welcher Reihenfolge umgesetzt werden sollen.

Welche Kombinationen aus Hardware und Software funktionieren zuverlässig?

Der Aufbau der IT-Plattform für diese Use Cases erfordert dann ebenfalls zahlreiche Überlegungen. Unternehmen müssen klären, welche Server mit welchen GPUs gut funktionieren und welche Storage- und Netzwerk-Komponenten ihre Anforderungen erfüllen können. Über die Hardware hinaus benötigt ihre KI-Fabrik natürlich auch die Software, die die KI-Anwendungen produzieren kann. Dazu zählen Lösungen für Datenintegration, Modelltraining, Bereitstellung, Überwachung, Governance und Sicherheit sowie Integrationsschichten für Fachanwendungen. Diese Lösungen gilt es ebenfalls auszuwählen, und es muss eruiert werden, welche Kombinationen aus Hardware und Software zuverlässig funktionieren.



(Quelle: GettyImages)

Zudem kann es sinnvoll sein, neben der Implementierung der KI-Fabrik ein Datenmanagement-Projekt durchzuführen. Eine saubere, konsistente und strukturierte Datenbasis ist die Grundvoraussetzung für eine funktionierende AI Factory. Ist die Datenbasis im Unternehmen noch nicht vorhanden oder kann diese nicht barrierefrei genutzt werden, sollte es ein Data-Management- oder Data-Mesh-Konzept umsetzen, das sicherstellt, dass die erforderlichen Daten auffindbar, zugänglich, interoperabel und vertrauenswürdig sind.

Nicht zuletzt müssen beim Aufbau einer KI-Fabrik Entscheidungen über die Betriebsorte der IT-Plattform getroffen werden. Soll sie im Rechenzentrum oder am Edge betrieben werden, oder beides? Aus Sicherheits-, Compliance- und Kosten-Gründen wird der Großteil der Plattform zwar in der Regel on-Premises betrieben werden. Es kann aber auch sinnvoll sein, Public-Cloud-Ressourcen einzubinden. Durch hybride Modelle können Unternehmen die Flexibilität und Skalierbarkeit ihrer AI Factory erhöhen und den Zugriff auf zusätzliche Services ermöglichen, während die sensiblen Kernsysteme lokal bleiben.

Geeignete IT-Partner können Unternehmen beim Aufbau einer AI Factory durchgängig unterstützen – mit optimal aufeinander abgestimmten Services, Software und Hardware.

(Quelle: Dell Technologies)

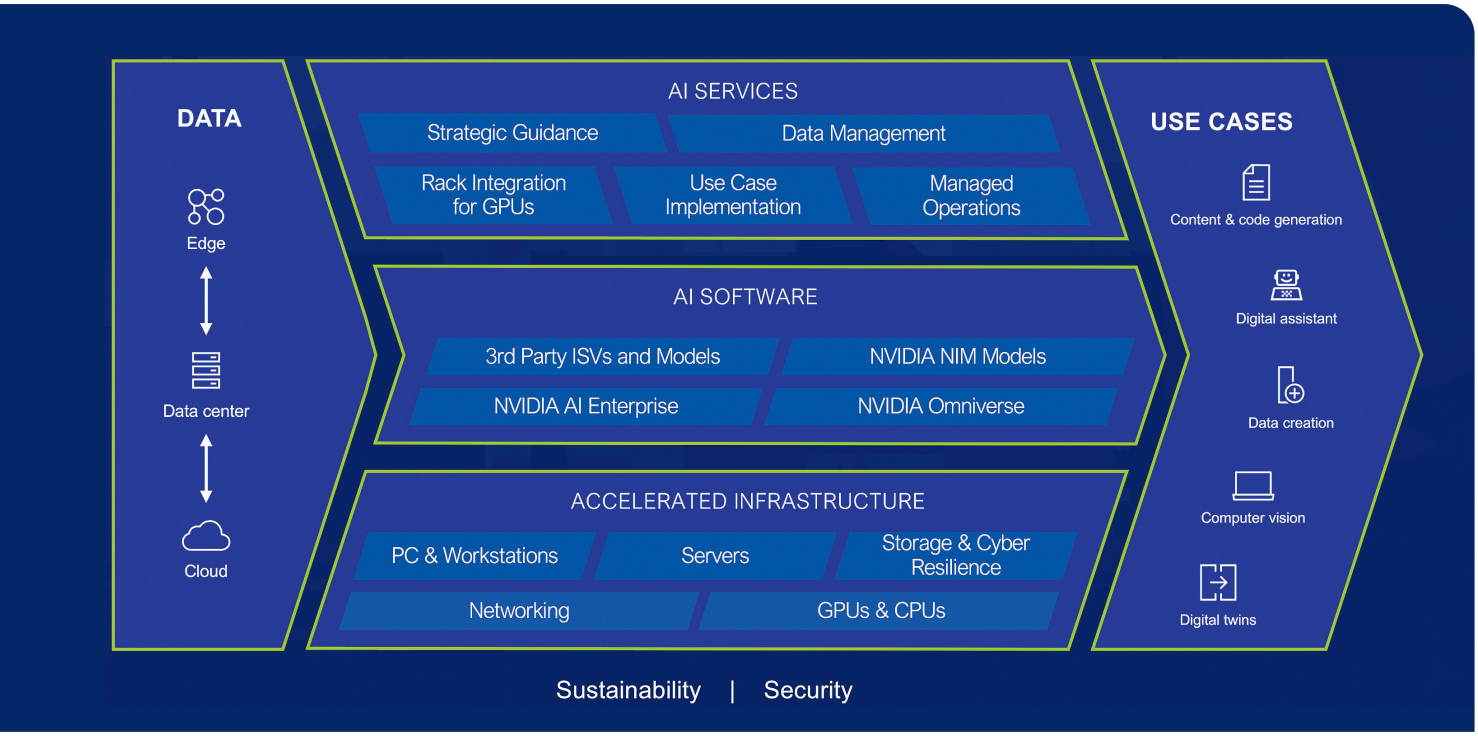
Vordefinierte und getestete Architekturen

Eine AI Factory ermöglicht Unternehmen eine effiziente Implementierung und Skalierung von Künstlicher Intelligenz. Ihr Aufbau ist aber eine anspruchsvolle Aufgabe. Geeignete IT-Partner können Unternehmen dabei maßgeblich unterstützten und enorm entlasten. Das beginnt bereits mit Workshops zur Identifizierung und Priorisierung der Use Cases und setzt sich über gemeinsam durchgeführte Datenmanagement-Projekte fort.

Darüber hinaus bietet ein guter Partner auch validierte Designs für den Aufbau der IT-Infrastrukturen an. Diese Designs enthalten Blaupausen für Architekturen aus Hardware und KI-Software, die bereits getestet und validiert wurden. Sie bieten zudem Empfehlungen für die richtige Dimensionierung und geben detaillierte Anleitungen für das Deployment und den Betrieb der Infrastrukturen. Die Designs decken verschiedene grundlegende Workloads von generativer und agentenbasierter KI ab, ebenso spezifische Workloads beispielsweise für Digitale Assistenten, Computer Vision oder Digital Twins, aber auch den Betrieb von Open-Source-LLMs. Außerdem enthalten sie Empfehlungen und Architekturmuster für die Integration in Public Clouds und unterstützen damit auch hybride Szenarien.

Natürlich müssen diese Designs noch an die individuellen Anforderungen der Unternehmen angepasst werden. Da sie aber bereits getestet und validiert sind, ermöglichen sie Unternehmen eine deutlich schnellere, skalierbarere und risikoärmere Implementierung, als wenn sie ihre KI-Infrastrukturen selbst von Grund auf konzipieren. Idealerweise haben sie dabei die Wahl, die Validated Designs nach Präferenz selbst in die Realität umzusetzen, oder ihre bereits fertigen physischen Ausführungen zu beziehen – auch hier wieder je nach Wunsch als Kauf, Subskription oder Managed Service.

Christian Scharrer, Bruno Maddaloni





DATA SCIENCE MIT BIG DATA

TECHNIKEN, WERKZEUGE UND ALGORITHMEN ZUR ANALYSE GROSSER DATENMENGEN

Mit diesem Buch erhalten Sie einen anschaulichen, praxisnahen und technologieunabhängigen Einstieg in den Umgang mit großen Datenmengen. Dabei kommen vor allem gängige Open-Source-Werkzeuge zum Einsatz, um die dahinterstehenden Konzepte zu verdeutlichen, so dass auch der Einstieg in kommerzielle Produkte problemlos möglich wird. Das Buch startet mit den Herausforderungen, die sich durch die verteilte Verarbeitung von Daten ergeben, sobald diese nicht mehr auf einen Rechnerknoten passen.

Sie lernen, wie Sie Big-Data-Analytics mit Verarbeitungsparadigmen wie Batch-, Micro-Batch- und Stream-Verarbeitung praktisch umsetzen; ebenso wird auf die Vor- und Nachteile von NoSQL-Datenbanken eingegangen. Einblicke zur Visualisierung von Analyseergebnissen, in zufallsbasierte Big-Data-Algorithmen sowie in Referenz-Architekturen für den Aufbau skalierbarer Big-Data-Systeme runden den Inhalt des Buches ab. Die zahlreichen Beispiele im Buch werden auf Basis moderner Container-Technologie (Docker) vorgestellt, so dass Sie Ihr neu erworbenes Wissen auch gleich in der Praxis ausprobieren können.

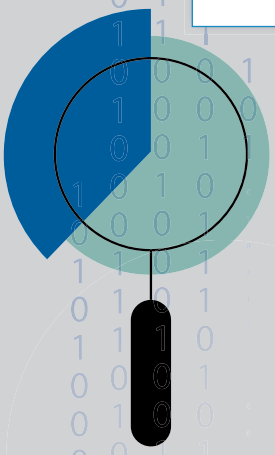
Das kompakte Lehrbuch und Nachschlagewerk für Big Data eignet sich hervorragend für die Verwendung in Studium, Ausbildung und beruflicher Praxis, um dem Umgang mit beständig weiterwachsenden Datenmengen seinen Schrecken zu nehmen.

Aus dem Inhalt:

- Einstieg ins Thema
- Verteilte Systeme
- Big-Data-Management
- NoSQL
- Verarbeitungsparadigmen
- Systemarchitekturen
- Algorithmen und Datenanalyse
- Systementwicklung, -test und -betrieb
- Ausblick



Data Science mit Big Data
–Techniken, Werkzeuge und Algorithmen zur Analyse großer Datenmengen;
Oliver Hummel, Marcus Kessel, Beate Navarro Bullock, Robert Butscher;
Carl Hanser Verlag GmbH & Co.KG; 02-2026



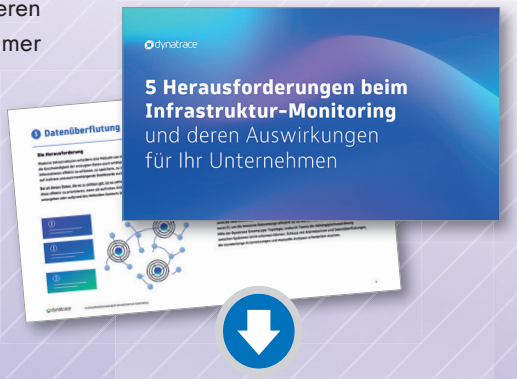
INFRASTRUKTUR-MONITORING NEU GEDACHT

5 HERAUSFORDERUNGEN, DIE SIE KENNEN SOLLTEN

Herkömmliche Monitoringstrategien und -Tools funktionieren einfach nicht mehr. Die moderne IT-Infrastruktur wird immer komplexer und ist durch dynamische Cloud-Umgebungen, containerisierte Anwendungen, die auf Kubernetes laufen, und Microservices-Architekturen gekennzeichnet. Daher stehen ITOps und SRE-Teams vor einigen großen Herausforderungen.

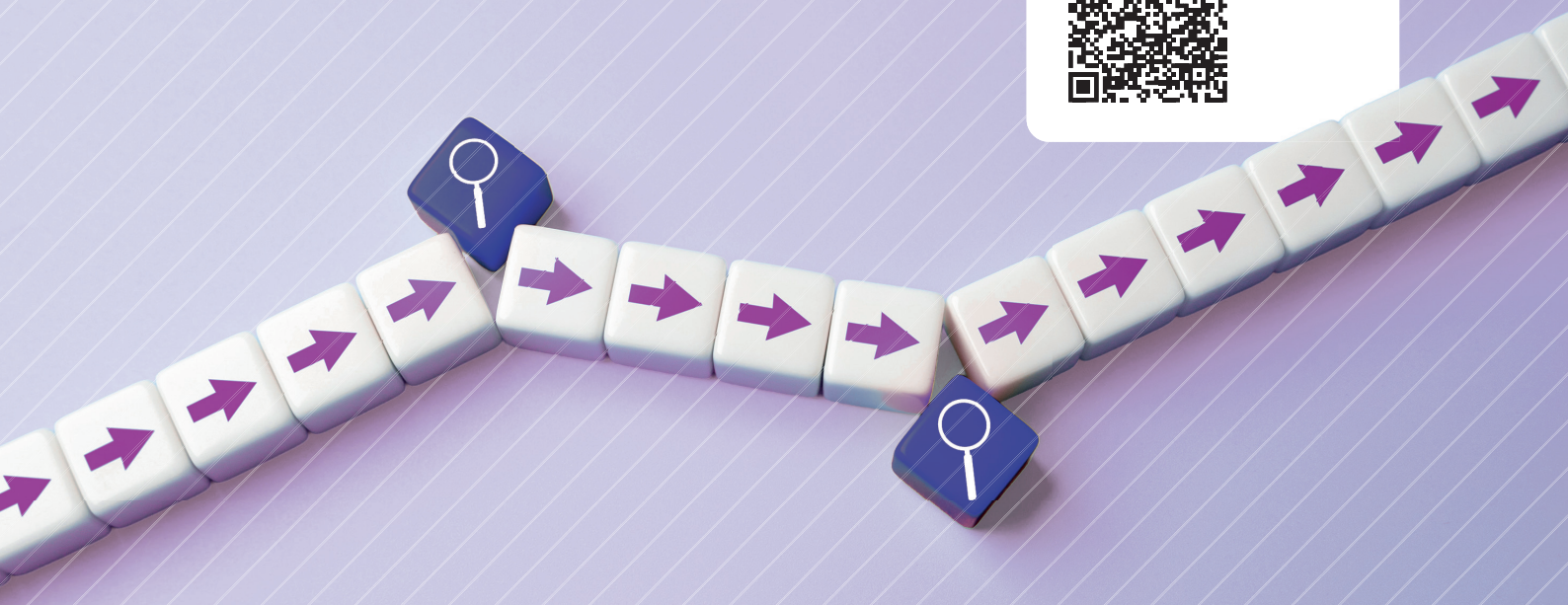
Herkömmliche Tools zum Infrastruktur-Monitoring wurden für eine einfachere Ära statischer, On-Premises-Infrastrukturen entwickelt. Infolgedessen haben Teams, die sich auf diese veralteten Ansätze verlassen, Schwierigkeiten, mit dem schnellen Wandel und den komplexen Abhängigkeiten Schritt zu halten, die die heutige IT-Landschaft und dynamische IT-Technologiestacks ausmachen. Diese Komplexität hat Auswirkungen auf die Art und Weise, wie Teams Daten verwalten und wie schnell sie Probleme erkennen und beheben können.

Wie können Teams einen modernen Ansatz nutzen, um die Monitoring-Herausforderungen von heute zu bewältigen?



WHITEPAPER DOWNLOAD

Das Whitepaper umfasst 8 Seiten und steht kostenlos zum Download bereit.
www.it-daily.net/download



FINANZPROZESSE NEU DENKEN

Die Finanzfunktion wandelt sich von einer administrativen zur strategischen Wertschöpfungseinheit. Große und mittelständische Unternehmen stehen dabei vor einer doppelten Herausforderung: Regulierungen wie DORA erhöhen die Anforderungen an digitale Resilienz und Threat Intelligence, während intelligente Automatisierungstechnologien völlig neue Möglichkeiten eröffnen. Automatisierte Rechnungsprozesse schließen Manipulationsspielräume, Agentic AI trifft dokumentierte Entscheidungen autonom, und Cognitive Operations machen europäische Unternehmen im globalen Wettbewerb konkurrenzfähig.

Für IT-Entscheider gilt: Wer Finanzprozesse heute neu denkt, senkt nicht nur Fehlerrisiken, sondern maximiert zugleich den ROI.



Grundregeln des E-Invoicings

EFFIZIENTERE UND TRANSPARENTERE RECHNUNGSPROZESSE

Trotz EU-Standard: Die E-Rechnung kennt EU-weit zahlreiche länderspezifische Ausprägungen und technische Anforderungen. Worauf man nun achten sollte.

Eine Versandpflicht für elektronische Rechnungen im B2B wird es in Deutschland ab 2027 geben. Andere Länder sind sogar noch eher dran: Belgien, Frankreich und Polen etwa schon 2026. So wird die elektronische Rechnung für Europa Schritt für Schritt zur Normalität. Darauf müssen sich Unternehmen aktuell vorbereiten.

Technische Grundlage für die elektronische Rechnungsstellung ist die europäische Norm EN 16931, auf welche die einzelnen nationalen Regelungen grundsätzlich referenzieren. Das ermöglicht, eine E-Rechnung in einem strukturierten elektronischen Format auszustellen, zu übermitteln und zu empfangen.

Formate der E-Rechnung für Deutschland

In Deutschland kennt man die XRechnung aus dem B2G; in der freien Wirtschaft wird außerdem das ZUGFeRD-Format verwendet. Beide entsprechen in ihren aktuellen Versionen der EN 16931, sind also zulässig. In mehreren EU-Ländern ist daneben BIS Billing 3.0 die technische Basis der E-Rechnung. Wer mit elektronischen Rechnungen zu tun hat, sollte daher alle drei Formate kennen.





WER FRÜHZEITIG SYSTEMATISCH PLANT UND SKALIERBARE STRUKTUREN AUFBAUT, SCHAFFT DIE GRUNDLAGE FÜR NOCH EFFIZIENTERE UND TRANSPARENTERE RECHNUNGSPROZESSE.

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

E-Invoicing bleibt komplex trotz europäischem Standard

So überschaubar und einheitlich, wie es auf den ersten Blick mit der EU-Norm erscheint, geht es bei der Umsetzung in Europa aber eben doch nicht zu. Es zeigt sich eher ein Flickenteppich. Denn unter dem Etikett des europäischen Standards verbergen sich zahlreiche länderspezifische Ausprägungen und technische Anforderungen. Diese sollten nicht unterschätzt werden. EN 16931 gibt nur den technologischen Rahmen vor, innerhalb dessen die Staaten jeweils eigene Formate und Anhänge – die ebenfalls verpflichtend sein können – entwickeln, verwenden und auch wieder ändern dürfen.

Formate, die der EN 16931 entsprechen, sind zum Beispiel OIOUBL (Dänemark) oder FatturaPA (Italien). Jedes von ihnen ist von den jeweiligen nationalen Gesetzgebungen abhängig und muss beachtet werden. Wer also innerhalb von Deutschland eine FatturaPA-Rechnung erhält, ist verpflichtet, sie zu verarbeiten, da es sich um eine offizielle E-Rechnung handelt.

Neben den obligatorischen Feldern enthalten die meisten Formate eine Vielzahl optionaler Felder, deren Nutzung von individuellen Vereinbarungen abhängig ist. Im Zusammenspiel mit dem ERP-System muss dies beachtet werden und erfordert ein anspruchsvolles Feldmapping.

Länderübergreifende Geschäftsaktivitäten als Herausforderung

Standardisierung bringen E-Rechnungen damit bislang vor allem auf nationaler Ebene. Eine einheitliche europäische Standardisierung steht, trotz Bestrebungen wie auf Landesebene, noch aus. Zu unterscheiden ist des Weiteren zwischen B2B- und B2G-Rechnungen, die hinsichtlich Übertragungskanälen, Pflichtfeldern und Formaten voneinander abweichen können. Vorgeschrieben sind in bestimmten Ländern zudem Portale für den Rechnungsversand.

Die nationale Standardisierung allein reicht für Unternehmen nicht aus, die mit internationalen Absatz- und Bezugsmärkten grenzüberschreitend tätig sind. Der Aufwand, den Eingang und künftig den Versand von E-Rechnungen adäquat abzubilden und in Einklang zu bringen mit dem eigenen ERP-System, potenziert sich damit. International agierende Unternehmen sollten daher das E-Rechnungsprojekt als ein Querschnittsprojekt betrachten, das die IT ebenso angeht wie die Fachabteilungen für Steuern, Finanzen und Recht.

Was sind nun die typischen Stolpersteine bei der Umsetzung der E-Rechnungspflicht im internationalen Kontext und



wie lassen sie sich umgehen? Dafür gibt es einige Grundregeln:

Sackgasse Individuallösung oder Aussitzen

Zwei Fehler werden im Zusammenhang mit der E-Rechnung immer wieder begangen und sollten tunlichst vermieden werden. Zum einen neigen viele Firmen dazu, das Thema auszusitzen. Selbst wenn momentan nur wenige elektronische Rechnungen eintreffen oder noch keine direkte Nachfrage von Geschäftspartnern besteht, ist klar: Die gesetzlichen Vorgaben greifen Schritt für Schritt und sind unumkehrbar. Wer jetzt noch untätig bleibt, verspielt wertvolle Vorbereitungszeit und läuft Gefahr, den Anschluss zu verlieren.

Zum anderen setzen manche Unternehmen auf Individuallösungen. Angesichts sich immer wieder schnell ändernder technischer Details und regulatorischer Anforderungen bedeutet eine Eigenentwicklung einen enormen und nie endenden Wartungsaufwand. Kaum ist eine Anpassung umgesetzt, steht schon die nächste bevor. Sinnvoller ist es deshalb, auf erprobte – im besten Fall flexible und cloudbasierte – Standardlösungen zu setzen.

Die xSuite hat dafür im Vorfeld der E-Rechnungspflicht bereits Mitte 2024 mit xSuite eDNA (electronic Document Network Adapter) eine Cloudplattform veröffentlicht, mit der sowohl die Annahme unterschiedlichster E-Rechnungsformate und ihre Umwandlung in ein einfach zu verarbeitendes, standardisiertes Format möglich ist, wie auch die Erstellung und der Versand von Debitorenrechnungen aus SAP SD in XML-Formaten.

Klare Verantwortlichkeiten, Prozesse und Steuerungsinstrumente

Für eine erfolgreiche Umsetzung gibt es allerdings auch einige klare Handlungsempfehlungen. Wichtig ist vor allem der Aufbau eines nachhaltigen Compliance-Prozesses. Das bedeutet, Verantwortlichkeiten und Abläufe so festzulegen, dass gesetzliche Änderungen weltweit kontinuierlich beobachtet, Fristen eingehalten und alle Anpassungen transparent dokumentiert werden können.

Ebenso entscheidend ist es, die bestehenden E-Invoicing-Fähigkeiten innerhalb der Organisation zu identifizieren. Oft sind bereits Tools, Systeme oder Prozesse im Einsatz, mit denen Rechnungen erstellt, empfangen, gemeldet oder verarbeitet werden – Potenziale, die sich möglicherweise erweitern und skalieren lassen.

Schließlich empfiehlt es sich, eine strategische Roadmap für die E-Invoicing-Compliance zu entwickeln. Wer den aktuellen Stand im Unternehmen mit bekannten und absehbaren gesetzlichen Anforderungen vergleicht, erkennt Lücken, Prioritäten und kann konkrete Maßnahmen einleiten. Diese Roadmap ist nicht als starres Dokument zu verstehen, sondern sie ist ein dynamisches Steuerungsinstrument, das sich an ein hochdynamisches regulatorisches Umfeld anpassen muss.

Fazit

Die Umsetzung der E-Rechnungspflicht ist nicht nur ein technisches Update und weit mehr als der Sprung von Papier- und PDF-Formaten zur reinen digitalen (XML-) Rechnung. Es handelt sich vielmehr um ein unternehmensweites Transformationsprojekt mit erheblicher Compliance-Relevanz. Wer frühzeitig systematisch plant und skalierbare Strukturen aufbaut, stellt nicht nur sicher, dass die gesetzlichen Vorgaben erfüllt werden, sondern schafft gleichzeitig die Grundlage für noch effizientere und transparentere Rechnungsprozesse – und das auf globaler Ebene.

Dina Ziems

Agentic AI im Finanzbereich

VOM BURGER ZUM STERNEMENÜ

Während die klassische KI in vielen Bereichen wirtschaftlichen Handelns Einzug gefunden hat, rückt die nächste Generation von KI ins Rampenlicht. Noch gibt es keinen deutschen Namen für diese Technologie, es handelt sich um die Agentic AI. Diese neue Form der KI arbeitet auf einem deutlich höheren Intelligenz-Niveau als die bisherige KI. Sie hat als wesentliches Differenzierungsmerkmal das „Agentic" im Namen, was man mit „handelnd" oder „autonom" übersetzen könnte. Damit ist Agentic AI in der Lage, aktiv Ziele zu verfolgen. Sie trifft Entscheidungen und führt Aktionen eigenständig durch. Diese Eigenschaft macht Agentic AI zu einen idealen „Helferlein", um Finanzabteilungen noch besser zu unterstützen, als es die klassische KI bereits mit hohem Automatisierungspotenzial kann.

Über Fast Food und Gourmet-Essen

Klassische KI und Agentic AI lassen sich im Bereich der Finanzen eines Unternehmens mit der Analogie zu einem Fast-Food- und einem Sterne-Koch visualisieren. Die klassische KI zielt auf ein festgelegtes und beliebig oft replizierbares Ziel in möglichst hoher Geschwindigkeit ab – ähnlich einem Fast-Food-Koch, der immer darum bemüht ist, exakt dieselbe Speise mit demselben Aussehen und Geschmack zuzubereiten. Agentic AI hingegen ist mit gehobener Küche vergleichbar, die den Speisen Variationen gibt und den Anspruch hat, immer ein bisschen besser zu werden.

Übertragen auf die Finanzabteilung überzeugt die klassische KI schon heute mit weitreichenden Vorteilen, beispielsweise in der Automatisierung von Buchungen und Abschlüssen. Sie wiederholt immer wieder denselben erlernten Prozess und unterstützt dadurch das Finanzteam in der täglichen Routinearbeit maßgeblich. Die KI-Innovationen von BlackLine etwa basieren auf den Grundsätzen der Genauigkeit, Effizienz und Intelligenz und liefern so messbare Ergebnisse in Bezug auf Geschwindigkeit, Präzision und Compliance.



DIE VORTEILE DER AGENTIC AI LIEGEN DARIN, DASS SIE MASCHINELLE DENK- UND KOMBINATIONSPROZESSE ERMÖGLICHT – IN EINER VIELFALT UND GESCHWINDIGKEIT, WIE ES EIN MENSCH NICHT KÖNNTE.

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

Dies trifft den Nerv der Wirtschaft, die sehr hohe Erwartungen an den Einsatz von KI hat: Die Wünsche des Managements und der Finanzexperten an die KI spiegeln sich in der aktuellen Studie von BlackLine wider, in der 1.300 Führungskräfte zur KI befragt wurden: Die Erwartungen an den Einsatz von KI im Finanzbereich sind hoch: 35 Prozent der weltweit Befragten erhoffen sich signifikante Produktivitätssteigerungen und 31 Prozent eine Verbesserung der Datenqualität. 25 Prozent befürchten, dass sich die Strukturen in den Finanzabteilungen grundlegend verändern werden. Die CFOs sind dabei jedoch überwiegend positiv: 40 Prozent glauben, dass KI ihnen hilft, fundiertere Entscheidungen zu treffen. In Deutschland sind sich 40 Prozent der CFOs sicher, dass KI die Finanzabteilung zum Positiven verändern wird. 20 Prozent versprechen sich einen Produktivitätsschub. Nur 20 Prozent können noch nicht abschätzen, wie sich KI konkret auswirken wird.

Das nächste Upgrade

Unternehmen, die KI-unterstütze Tools in der Finanzabteilung einsetzen, profitieren bereits heute maßgeblich von dieser Technologie. Standard-Prozesse in der Finanzabteilung werden von KI übernommen und in hoch automatisierten Prozessen abgearbeitet – ganz ähnlich der Analogie zum Fast-Food-Koch. Das geschieht in einer Geschwindigkeit, wie es Fachkräfte ohne diese technische Unterstützung nicht leisten könnten. Zugleich haben die Finanzverantwortlichen Vorteile durch eine höhere Datenqualität, da menschliche Fehler weitestgehend ausgeschlossen sind. Unternehmen, die beispielsweise die KI-unterstützten Tools in der BlackLine-Plattform nutzen, können sich über eine Beschleunigung der Time to Value freuen. Dies wird erreicht, indem die KI rohe Finanzdaten in ausführungsreife Erkenntnisse überführt, um strategische Maßnahmen zu untermauern. Konkret profitiert das Office of the CFO von KI-Funktionen wie dem Document Description Summarizer, der Dokumentinhalte automatisch zusammenfasst, um den Support zu verbessern und Compliance-Lücken zu reduzieren, oder dem

Journals Risk Analyser, der Anomalien in Journaleinträgen identifiziert und potenzielle Prüfungsrisiken hervorhebt.

Im Bereich der Konsolidierung und Finanzanalyse können zum Beispiel die Zusammenfassungsagenten Jahresabschlüsse mühelos zusammenführen und rohe Finanzdaten in umsetzbare Erkenntnisse für F&A-Teams wandeln. Um ein weiteres Beispiel der KI-Unterstützung in der Finanzabteilung zu nennen, verhindert die Intercompany Predictive Guidance Fehler bei Intercompany-Transaktionen, bevor sie das Hauptbuch erreichen. All diese KI-gestützten Funktionen sind bereits heute Realität. Doch was kommt als nächstes, auf welche neuen Intelligenz-Level können sich Unternehmen für die nahe Zukunft einstellen?

Sternekoch in der KI

Die Finanzabteilung genießt bereits heute einen hohen Grad an KI-basierter Automation. Doch für die Zukunft werden der KI noch weitaus komplexere Aufgaben anvertraut und man erwartet, dass die KI eigenständig lernt und durch die gewonnenen Erkenntnisse ihre Aufgabe immer ein bisschen besser löst – wie etwa der Sternekoch, der stets die Optimierung seiner bereits erstklassigen Gerichte zum Ziel hat. Nur mit dem Unterschied, dass dies für die breite Masse erschwinglich ist.

Möglich ist das durch eine neue Generation der künstlichen Intelligenz, die mit einem Kurz- und Langzeitgedächtnis in der Lage ist, eigenständig zu handeln, anstatt nur einem trainierten Muster zu folgen. Die Vorteile der Agentic AI liegen darin, dass sie maschinelle Denk- und Kombinationsprozesse ermöglicht – in einer Vielfalt und Geschwindigkeit, wie es ein Mensch nicht könnte.

Mit Hilfe sogenannter KI-Agenten lassen sich im Finanzwesen deutliche Vorteile erzielen. Dazu gehören beispielsweise Matching-Agenten. Sie beschleunigen die Wertschöpfung durch erhöhte Genauigkeit und Transparenz beim Transaktionsabgleich, indem neue Regeln vorgeschlagen und bestehende verbessert werden. Ein Abweichungsanomalie-Erkennungs-Agent identifiziert automatisch Varianzen und Ausreißer in Echtzeit und schlägt Varianzerklärungen vor. In der Verarbeitung von Zahlungseingängen extrahiert ein Agent Zahlungavis-Daten, ohne dass eine Rechnungsvorlage eingerichtet werden muss, was eine nahtlose Zuordnung von Zahlungseingängen ermöglicht. Weitere Optionen ergeben sich durch Zusammenfassungs- und Übersetzungs-Agenten. Sie steigern die Effizienz im Forderungsmanagement durch KI-generierte Zusammenfassungen und mehrsprachige Übersetzungen.

Fazit

KI im Finanzwesen ist kein Mysterium oder gar eine dunkle Macht, die im Hintergrund Dinge macht, welche Finanzprofis nicht nachvollziehen könnten. KI ist ausschließlich dafür da, mit weniger Aufwand mehr zu erreichen. Sie reduziert den manuellen Aufwand und liefert hochwertige Ergebnisse. Und sie kann in komplexen Finanzsystemen Anomalien in einer Geschwindigkeit und Breite identifizieren, wie es Menschen nicht können.

Die Agentic AI bringt die bisherige KI auf Sternekoch-Niveau ohne dafür den vergleichbaren Preis zu bezahlen. Künftig wird es KI erlaubt sein, eigenständig Schlüsse zu ziehen und anhand von Erkenntnissen und Mustern eigenständig zu lernen. Damit wird der Nutzen nochmals deutlich erweitert und die Finanzexperten haben gleichzeitig den Vorteil, dass die Maschine eigenständig Aufgaben umsetzt. Dies geschieht natürlich unter menschlicher Kontrolle, aber der Finanzprofi wird von allen manuellen Optimierungstätigkeiten aufgrund der Fehler- und Anomalie-Erkenntnisse befreit.

Ralph Weiss



E-Invoicing: Mit dem richtigen Set-up, Fehler vermeiden

WER MANIPULATIONEN, RECHTS- UND KOSTENFALLEN VORBEUGEN WILL, SETZT AUF AUTOMATION UND WEITBLICK

Verfälschte digitale Rechnungen sorgen in Unternehmen jedes Jahr für einen enormen finanziellen Schaden. 2024 lag dieser laut einer Erhebung des Digitalverbands Bitkom bei stolzen 0,8 Milliarden Euro. Allein nach einem einzigen Ermittlungsverfahren bezifferte die Staatsanwaltschaft Leipzig die Verluste mit mehreren Millionen Euro. Ihr war eine Gruppe von Cyberkriminellen ins Netz gegangen, die sich auf Rechnungsbetrug spezialisiert hatte. Kleine und mittlere Unternehmen betrifft der sogenannte „Geldabfluss in Folge von Betrugsversuchen" ebenso wie Großkonzerne oder öffentliche Einrichtungen und Kommunen. Zu den gängigen Methoden zählen das Fälschen von IBAN und Empfängerdaten in den Rechnungen. Doch es gibt im Rahmen der E-Rechnung wirksame Mittel, derartigem Betrug vorzubeugen.



SELBST OHNE GLASKUGEL IST ES MÖGLICH, SICH BEIM THEMA E-INVOICING ZUKUNFTS- UND BUDGETSICHER AUFZUSTELLEN.

Oliver Rauschil, Senior Director Digital Sales EMEA, Quadient, www.quadient.com

Manipulation wirksam verhindern

Viele Unternehmen versenden ihre Rechnungen per E-Mail, meist als Dateianhang im PDF-Format. Diese Vorgehensweise ist ebenso verbreitet wie gesetzeskonform. In der Praxis erweist sie sich allerdings häufig als unsicher. Denn eine E-Mail lässt sich relativ einfach abfangen und die angehängte PDF-Rechnung in einem simplen Texteditor mit wenigen Klicks manipulieren. Cyberkriminelle ersetzen dann die enthaltenen Bankdaten durch eigene Konten, ohne dass der Empfänger es bemerkt.

MEHR WERT
Was bedeutet GoBD?

Es braucht daher einen sicheren Übertragungsweg für alle Arten von elektronisch übermittelten Rechnungen. Dies gilt sowohl für PDF- als auch für hybride und digitale E-Rechnungsformate wie ZUGFeRD, Factur-X oder XRechnung. Einen zuverlässigen Weg stellen E-Rechnungsplattformen bereit. Sie bilden den gesamten Rechnungsprozess vom Erstellen über das Empfangen und Verarbeiten bis hin zum Versenden ab. Bei den angebotenen Versandoptionen gehen Unternehmen auf Nummer sicher, wenn sie eine Ende-zu-Ende verschlüsselte Variante nutzen. Standard ist End-2-End-Encryption ohnehin, sobald die Plattform Rechnungen über ein Übertragungsnetzwerk wie Peppol oder Traffiqx versendet. Spezialisierte Anbieter innerhalb der Netzwerke prüfen dabei zudem eingehende Belege zuverlässig auf Viren und schädliche Inhalte, bevor sie den Empfänger erreichen.

GoBD-Konformität sicherstellen

Eine per E-Mail erhaltene PDF- oder E-Rechnung muss den GoBD (Grundsätzen zur ordnungsmäßigen Führung und Aufbewahrung von Büchern, Aufzeichnungen und Unterlagen in elektronischer Form) entsprechen. Dazu gehört, dass sie nachvollziehbar und unveränderbar – also revisionssicher – gespeichert wird. Ein Abspeichern der E-Mail samt Dateianhang in einem normalen Laufwerksordner erfüllt diese Anforderungen nicht.

Das kann den Rechnungsempfänger teuer zu stehen kommen, falls der Fiskus deshalb den Vorsteuerabzug, einzelne Betriebsausgaben oder gleich die gesamte Buchhaltung nicht anerkennt. Für die nötige Rechtssicherheit sorgt hier eine E-Rechnungsplattform, indem sie zum einen Rechnungen GoBD-konform archiviert. Weiteres Plus: Der komplette Rechnungsprozess wird lückenlos dokumentiert. Das hilft in steuerlicher Hinsicht, aber auch bei Streitigkeiten, etwa wenn es um das Überschreiten von Zahlungsfristen geht.

Durch Automatisierung die Effizienz steigern

Unternehmen können mit der Umstellung auf einen vollautomatisierten E-Rechnungsprozess Effizienzgewinne erzielen, die sich auch in Einsparungen niederschlagen. Um bis zu 60 Prozent lassen sich so Kosten reduzieren! Denn PDF-Rechnungen bleiben gerne im Spam-Ordner hängen oder scheitern am Virenscanner. Und selbst wenn die E-Rechnung als strukturierter Datensatz im Format XRechnung oder

ZUGFeRD gemailt wurde, muss der Anhang aus der E-Mail herausgesucht, gespeichert und in das Rechnungsverarbeitungssystem importiert werden.

Mit einer vollautomatisierten und durchgängigen Verarbeitung vom Posteingang bis zum Verbuchen reduzieren Unternehmen solche manuellen Vorgänge auf ein Minimum. Denn die Rechnung kann direkt in ein ERP- oder Buchhaltungssystem einfließen. Schnittstellen und Konnektoren helfen hier, Medienbrüche zu vermeiden. Zudem prüfen moderne Systeme automatisch, ob das E-Rechnungsformat der EN16931 entspricht, Pflichtfelder richtig befüllt sind und auch sonst rechtliche Anforderungen eingehalten werden. Entsprechend reibungsloser und schneller ist der Prozess und umso zügiger kann die Zahlung erfolgen. Darüber hinaus verbessert eine E-Rechnungsplattform das Kundenerlebnis, indem sie das Rechnungsformat automatisch in ein vom Empfänger unterstütztes und gewünschtes Zielformat konvertiert.

Einmal anpacken, doppelt profitieren

Die elektronische Rechnungsstellung ist nicht zuletzt deshalb komplex, weil jedes Land seinen eigenen nationalen Ansatz wählen kann, inklusive steuerlichem Meldesystem. Ein solches wird spätestens ab 2030 auch in Deutschland greifen. Die Stoßrichtung ist durch die EU-Initiative VAT in the Digital Age (ViDA) bereits klar: Alle Unternehmen, die Waren oder Dienstleistungen an Unternehmen in einem EU-Mitgliedstaat verkaufen, werden früher oder später Umsätze und Mehrwertsteuer in Echtzeit an die Finanzbehörden melden müssen.

Wer daher jetzt beim E-Invoicing auf eine einfache Insellösung setzt, investiert unter Umständen zweimal. Denn es ist davon auszugehen, dass die steuerliche Meldung verpflichtend über eine digitale Plattform erfolgen wird. Die E-Mail stößt spätestens dann an ihre Grenzen. Zudem werden automatisierte Validierungen und Interoperabilität mit internationalen Meldeportalen relevant. All dies sind Funktionen, die selbst so manche ERP-Software nicht oder nur eingeschränkt abbildet – genauso wie die Konvertierung in international nötige Rechnungsformate.

Mit spezialisierten E-Rechnungsplattformen dagegen stellen Unternehmen ihr Rechnungswesen von Anfang an zukunftssicher auf. Denn Anwender kommen damit nicht nur ihrer aktuellen Pflicht zur E-Rechnung nach und minimieren dabei die mit dem E-Mail-Versand verbundenen Risiken. Weil die Plattformbetreiber ihre Systeme kontinuierlich an neue gesetzliche Vorgaben anpassen, erspart dies auch viel eigenen Aufwand. Und gleichzeitig bereitet sich das Unternehmen ohne Mühe schon heute optimal auf ViDA vor.

Fazit

Unternehmen haben die Wahl. Entweder setzen sie die elektronische Rechnungsstellung als ein Pflicht- und IT-Projekt um; nach dem Minimalprinzip und wenn gerade Zeit dafür ist – also gerne in letzter Minute. Oder sie nehmen E-Invoicing als Chance wahr, um ihre Finanzprozesse zu überdenken und eine durchgängige Automatisierung zu realisieren. Damit machen sie gleichzeitig ihre Finanzinfrastruktur zukunftssicher für kommende regulatorische Anforderungen. Doch eines ist auch klar: Cyberkriminelle sind erfinderisch und wissen sich anzupassen. Sicherheits- und Compliance-Aspekte sollten daher bei der Wahl einer E-Rechnungsplattform höchste Priorität haben.

Oliver Rauschil



(Quelle: Quadient)

Cognitive Operations in der Finanzbranche

WIE EUROPA DIE INDUSTRIALISIERUNG KOGNITIVER WORKLOADS ANFÜHREN KANN

Knapp drei Jahre nach der ChatGPT-Veröffentlichung kehrt vielerorts Ernüchterung ein. In Banken, Versicherungen und Verbänden schaffen es viele GenAI-Projekte nicht über den Pilotstatus hinaus. Auch viele Agenten- und Multi-Agenten-Vorhaben, insbesondere bei anspruchsvollen Prozessen wie Kreditentscheidungen, Compliance-Prüfungen oder Risikoanalysen, stehen aktuell auf der Kippe.

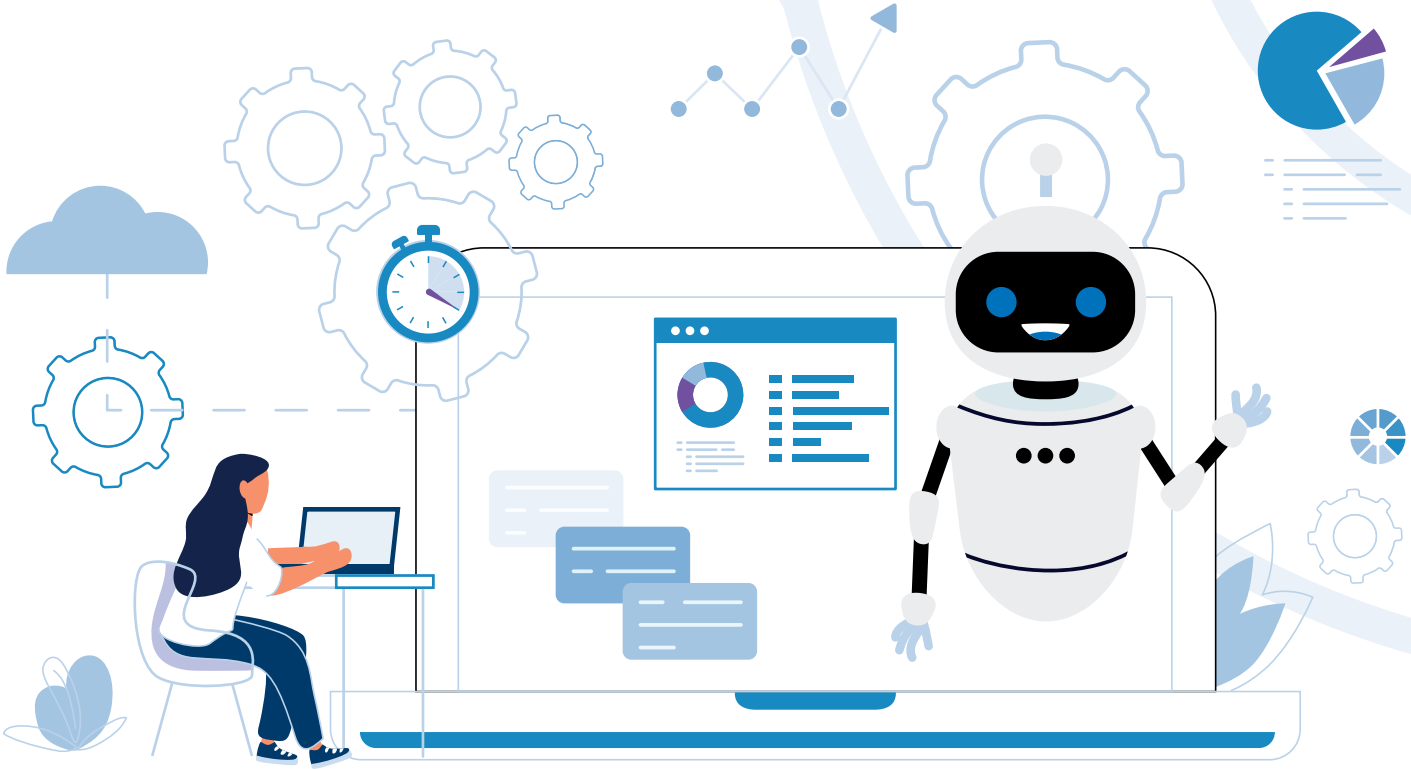
Gleichzeitig wächst der Druck: Demografischer Wandel, steigende Kosten und verschärfte Regulierung verlangen nach Effizienz und Innovation. Die Potenziale generativer KI zu ignorieren, ist keine tragfähige Option.

Die Diskrepanz zwischen technischer Faszination und betrieblicher Realität zeigt: Der Engpass liegt nicht originär in der Technologie, sondern in ihrer Beherrschbarkeit. Gerade dort, wo Vertrauen und Nachvollziehbarkeit zentrale Werte sind, fehlt die Grundlage für den kontrollierten, reproduzierbaren Betrieb kognitiver Systeme.

Das wahre Problem

Die Ursache für das aktuelle Scheitern liegt nicht allein in den Modellen, sondern an fehlenden Strukturen, um diese kontrolliert, reproduzierbar und dauerhaft im Rahmen geschäftlicher Prozesse zu betreiben. Häufig dominiert ein Flickenteppich aus Modellen, Prompts, Pipelines und Prototypen – ohne belastbare Governance, Nachvollziehbarkeit oder Skalierbarkeit. Generative KI kann nur dann produktiv eingesetzt werden, wenn sie sich in bestehende Kontroll-, Audit- und Compliance-Systeme einfügt.

Versuche, diese Komplexität auf Ebene einzelner Artefakte (Prompts, Guardrails, Validierungen) zu lösen, greifen zu kurz. Das allein wird das strukturelle Problem nicht zufriedenstellend lösen. Was fehlt, sind übergreifende Managementprozesse, die sicherstellen, dass alle kognitiven Workloads nach denselben Prinzipien aufgebaut, überwacht und gewartet werden.



Der aktuelle Flickenteppich bremst produktiv nutzbare Innovation:

- Proof-of-Concepts bleiben Insellösungen, weil sich ihre Workflows kaum in produktive Umgebungen überführen lassen.
- Produktive Systeme bleiben fragil, da Monitoring, Qualitätssicherung und effektive Ausführungssteuerung fehlen.
- Änderungen an Modellen oder Daten wirken unkontrolliert auf nachgelagerte Prozesse – ohne klare Rückverfolgbarkeit.

Fakt ist: KI-Workloads lassen sich nicht wie klassische IT-Systeme betreiben. Es braucht neue, industriell gedachte Praktiken für das Management und den produktiven Betrieb kognitiver Prozesse. Gerade in der Finanzwelt ist das bedeutsam: KI-basierte Entscheidungen müssen prüfbar, regelkonform und revisionssicher sein.

Die Lösung

Die Antwort auf diese Fragmentierung ist eine Infrastruktur für Cognitive Operations (CogOps) – eine strukturierte Ausführungsumgebung, die kognitive Prozesse steuerbar, prüfbar und reproduzierbar macht. Was DevOps für Software und MLOps für Modelltraining war, leistet CogOps für kognitive Systeme: Es schafft eine standardisierte Betriebs- und Steuerungsschicht für intelligente Prozesse – vom Reasoning bis zur Entscheidung.

Während MLOps vor allem das Training und Deployment von Modellen adressiert und AIOps operative IT-Systeme mithilfe von KI optimiert, geht CogOps einen Schritt weiter: Es operationalisiert das Denken selbst. CogOps steuert, überwacht und dokumentiert die Ausführung kognitiver Prozesse – unabhängig davon, welche Modelle oder Agenten im Einsatz sind. Damit entsteht eine neue Systemebene: eine Cognitive Operations Infrastructure. Sie fungiert als Produktionsumgebung für vertrauenswürdige Intelligenz – die technische und organisatorische Basis, auf der kognitive



EUROPA KANN VORREITER BEI DER INDUSTRIALISIERUNG KOGNITIVER WORKLOADS WERDEN.

Dr. Christian Gilcher,
CEO und Gründer, embraceableAI,
https://embraceable.ai/

Workloads kontrolliert, validiert und skaliert werden können.

Im Zentrum steht eine Cognitive Runtime, die einzelne Workloads kapselt. Ob Analyse, Entscheidung oder Validierung: Jeder Prozess läuft innerhalb einer Umgebung, die Kontrolle ermöglicht, ohne die kognitive Leistung zu beschneiden. Darauf aufbauend sichern Quality & Compliance-Gates die inhaltliche Zuverlässigkeit. Sie prüfen automatisch, ob Ergebnisse mit Richtlinien, Normen und Policies übereinstimmen. Qualität wird damit nicht nur überprüft, sondern erzwingbar gemacht.

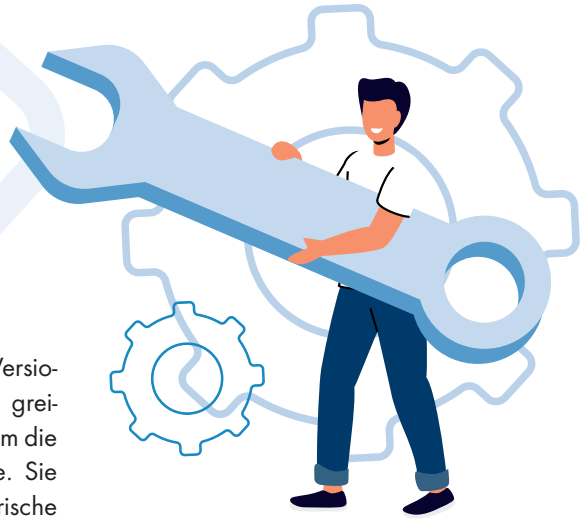
Alle verwendeten kognitiven Artefakte – Modelle, Prompts, Policies, Datenadapter und Logs – werden versioniert verwaltet. Jede Änderung ist nachvollziehbar, jeder Systemzustand reproduzierbar. Parallel dokumentiert die Plattform jeden Schritt transparent: Eingaben, Zwischenergebnisse, Prüfungen und Entscheidungen bilden eine lückenlose, revisionssichere Audit-Spur.

Diese Elemente – Runtime, Gates, Versionierung und Nachvollziehbarkeit – greifen ineinander und bilden gemeinsam die Cognitive Operations Infrastructure. Sie stellt die technische und organisatorische Grundlage für den kontrollierten Betrieb kognitiver Systeme dar: eine Infrastruktur, die Denken industrialisiert, ohne Flexibilität zu opfern, und KI von einem experimentellen Werkzeug in eine systemisch gesteuerte Unternehmensressource verwandelt.

Industrialisierung von KI-Entscheidungen

Mit einer standardisierten Betriebsumgebung ist der erste Schritt getan – doch die eigentliche Herausforderung liegt tiefer: Nicht nur Prozesse müssen stabil laufen, sondern das Denken selbst muss skalierbar, steuerbar und überprüfbar werden. Die marktüblichen KI-Modelle sind dafür nicht geeignet – selbst wenn man sie mit immer größeren Datenmengen und Rechenressourcen trainiert. LLMs und LRMs beruhen auf statistischen Wahrscheinlichkeiten, nicht auf Logik und Kausalität. Sie generieren Antworten, aber keine belastbaren Schlussfolgerungen.

Erst kognitive Systeme, die diese Modelle durch dedizierte Steuerungseinheiten lenken, schaffen die Basis für strukturell zuverlässiges Denken. Diese Module verknüpfen Wahrnehmung, Schlussfolgerung und Bewertung – sie machen maschinelles Denken steuerbar, überprüfbar und nachvollziehbar. Nur Modelle, die durch kognitive Steuerung gelenkt werden, ermöglichen zuverlässige, nachvollziehbare Intelligenz.



Der nächste Schritt besteht darin, diese kontrollierten Denkprozesse in skalierbare Betriebsstrukturen zu überführen. Hier beginnt die Industrialisierung kognitiver Workloads. Was früher Skripte und Container waren, sind heute Reasoning-Flows und Agentenketten – der neue Produktionsfluss intelligenter Systeme. Diese Workloads werden nach industriellen Prinzipien organisiert: mit klar definierten Qualitätsstufen, Prozessschnittstellen und Steuermechanismen. So entsteht ein geschlossenes Kontrollsystem für kognitive Prozesse – die Voraussetzung für das, was Banken und Versicherungen am dringendsten benötigen: Operational Trust.

Business Value:
Schneller, besser, sicherer

CogOps macht aus roher KI ein steuerbares Produktionsgut. Es verbindet technologische Exzellenz mit betrieblich verankerter Verlässlichkeit – und schafft so gerade im Finanzsektor den entscheidenden Hebel für Effizienz, Qualität und Vertrauen.

- **Schneller zur Wirkung:** Standardisierte Workflows verkürzen die Zeit von der Idee bis zur Produktivsetzung. Bausteine und Validierungslogiken werden wiederverwendbar;
- **Bessere Qualität bei geringeren Kosten:** Validierung und Fehlererkennung sind integraler Teil der Pipeline. Frühe Erkennung verhindert teure Nacharbeit und erhöht die Stabilität;
- **Compliance als Systemprinzip:** Jede Entscheidung ist auditierbar, jede Policy nachvollziehbar. CogOps macht Regelkonformität messbar und automatisiert – ein Schlüsselvorteil für regulierte Branchen;
- **Souveränität und Resilienz:** Da Modelle, Daten und Infrastruktur entkoppelt betrieben werden, bleiben Finanzhäuser unabhängig von einzelnen Anbietern oder Regionen. „Made in EU" steht für Kontrolle und Stabilität.

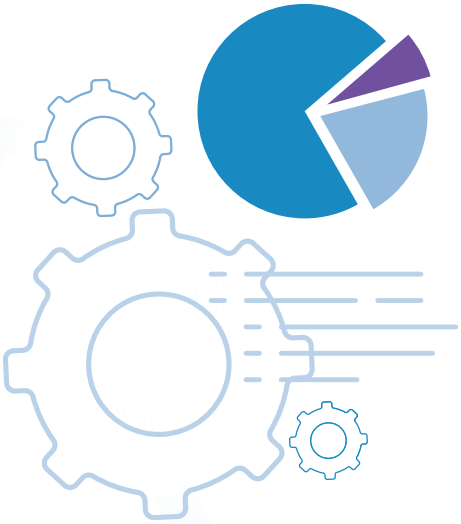
So entsteht ein neues Betriebsmodell: CogOps ermöglicht es, den strategischen Wert von generativer KI im Sinne einer Unternehmensressource real und im großen Maßstab nutzbar zu machen.

CogOps bewährt sich bereits in ersten Projekten

Die Finanzbranche erweist sich als Wegbereiter dieser Entwicklung: Hauck Aufhäuser Lampe nutzt beispielsweise eine kognitive Betriebsumgebung, um hausinterne Compliance-Prozesse zu automatisieren. Mit der lokal betriebenen, modularen KI-Plattform HALLEY hat die Privatbank ein sicheres, revisionsfähiges System geschaffen, das regulatorische Vorgaben, interne Richtlinien und Wissen zentral verfügbar macht. So wird KI gezielt in bestehende Prozesse integriert – ohne Kompromisse bei Datenhoheit und Transparenz.



Technologisch folgt HALLEY klaren Enterprise-Prinzipien: Eventbasierte Microservices, ein durchgängiges Rollen- und Rechtekonzept sowie auditierbare Konfigurationen übertragen ITSM-Standards konsequent auf KI-Anwendungen. Damit zeigt Hauck Aufhäuser Lampe, wie sich Innovation und Compliance in hochregulierten Umgebungen verbinden lassen.



Ein weiterer Early Adopter innerhalb der Finanzbranche ist der Baden-Württembergische Genossenschaftsverband (BWGV). Doch auch außerhalb des Finanzsektors bewährt sich der Ansatz: RWE nutzt Cognitive Operations zur Abbildung anspruchsvoller Fachprozesse, MVV Netze integriert die Plattform in Backoffice-Prozesse, und Industrie- und Handelskammern (IHKs) verwenden sie für wissensintensive Beratungs- und Prüfverfahren. Über alle Branchen hinweg bestätigt sich: Standardisierung und Kontrolle schaffen Vertrauen – und ermöglichen Skalierung.

Fazit und Ausblick

Europäische Banken und Versicherungen stehen am Beginn der Industrialisierung kognitiver Workloads. Nach der Experimentierphase folgt jetzt die Ära von Struktur, Kontrolle und Souveränität. Strukturierte und standardisierte CogOps kann ein europäischer Weg zu produktiver, sicherer und werteorientierter KI-Nutzung werden – nicht durch noch größere Modelle, sondern durch bessere Systemarchitekturen.

Das Ziel ist klar:

KI, die denkt – aber kontrolliert.
KI, die lernt – aber dokumentiert.
KI, die handelt – aber nachvollziehbar bleibt.

Damit hat Europa die Chance, zum Taktgeber der großindustriellen Nutzbarmachung kognitiver Workloads zu werden.

Dr. Christian Gilcher

DORA und Threat Intelligence

VON DER VORSCHRIFT ZUR PRAKTISCHEN RESILIENZ



DORA IST KEIN WEITERES COMPLIANCE-PROJEKT, SONDERN EIN KULTURWANDEL IN RICHTUNG DATENGETRIEBENER RESILIENZ.

Michael Chalvatzis, Senior Director DACH & Eastern Europe, Recorded Future, www.recordedfuture.com

Mit dem Inkrafttreten des Digital Operational Resilience Act (DORA) im Jahr 2025 haben deutsche Finanzinstitute ein einheitliches Regelwerk für digitale Stabilität erhalten. DORA gilt für Banken, Versicherungen, Investmentgesellschaften, Zahlungsdienstleister und deren IT-Dienstleister. Erstmals verpflichtet die Verordnung auch Drittanbieter wie Cloud-, Software- und Infrastrukturunternehmen. Damit rückt die gesamte Lieferkette in den Fokus der Aufsicht.

Das Ziel ist klar. Die Finanzbranche muss auch in Krisen geschäftsfähig bleiben und kritische Leistungen auch dann erbringen, wenn Systeme ausfallen oder Dienstleister nicht mehr verfügbar sind. Es geht nicht mehr nur um IT-Sicherheit, sondern um operative Widerstandsfähigkeit. Mit DORA verschiebt sich der Fokus von einer rein präventiven und reaktiven Abwehr hin zu einer messbaren, operativen und proaktiven Resilienz digitaler Systeme.

Von der Dokumentation zu den Daten

In der Vorbereitung auf DORA haben viele Finanzinstitute ihre Richtlinien überarbeitet, Meldewege definiert und neue Audits gestartet. Diese Maßnahmen sind notwendig, reichen aber bei Weitem nicht aus. DORA verlangt kontinuierliches Monitoring, schnelle Reaktion und fundierte Entscheidungen auf Basis aktueller Bedrohungslage.

Threat Intelligence liefert dafür den nötigen Kontext. Sie zeigt, welche Angriffsmethoden zunehmen, welche Schwachstellen aktiv ausgenutzt werden und ob gestohlene Zugangsdaten im Umlauf sind. So lassen sich Risiken priorisieren, Schutzmaßnahmen gezielt umsetzen und neue Angriffsmuster früh erkennen.

Auch die Meldepflichten unter DORA erfordern Geschwindigkeit. Schwere Vorfälle müssen teils innerhalb weniger Stunden gemeldet werden. Das gelingt nur mit Systemen, die Bedrohungen automatisch erkennen, bewerten und in den regulatorischen Kontext einordnen. Nur mit diesem Informationsvorsprung lassen sich Fristen einhalten, ohne die Übersicht zu verlieren.

Realistische Tests und sichere Lieferketten

Regelmäßige Resilienztests gehören zu den Kernanforderungen von DORA. Sie zeigen, ob Systeme und Prozesse realen Angriffen standhalten. Ihren Wert entfalten sie aber nur, wenn sie auf realistischen Bedrohungsszenarien basieren. Hier liefert Threat Intelligence den entscheidenden Input: Aktuelle Erkenntnisse über Taktiken, Techniken und Verfahren gezielter Angreifer (TTPs) ermöglichen es, Tests praxisnah zu gestalten und echte Schwachstellen zu erkennen, statt nur formale Anforderungen abzuhaken.

Auch bei der Überwachung externer Dienstleister schreibt DORA klare Verantwortlichkeiten vor. Finanzinstitute müssen die digitale Stabilität ihrer Lieferkette laufend bewerten. Risikoindikatoren, Warnmeldungen bei Vorfällen oder Hinweise auf Schwachstellen in genutzten Anwendungen helfen, Bedrohungen frühzeitig zu erkennen und Gegenmaßnahmen einzuleiten. So bleibt die Sicherheit entlang der gesamten Wertschöpfungskette transparent und steuerbar.

Resilienz als strategischer Vorteil

DORA ist kein weiteres Compliance-Projekt, sondern ein Kulturwandel in Richtung datengetriebener Resilienz. Wer Bedrohungsinformationen nutzt, um Entscheidungen faktenbasiert zu treffen, erfüllt nicht nur regulatorische Anforderungen, sondern stärkt auch seine Wettbewerbsfähigkeit.

Institute, die digitale Resilienz aktiv leben, schaffen Vertrauen bei Kunden, Aufsichtsbehörden und Partnern im eigenen Netzwerk. In einer Welt ständig neuer Cyberbedrohungen zählt nicht allein die Regel, sondern ihre Umsetzung im Alltag.

Michael Chalvatzis



UNSERE THEMEN

it management

Fokusthema: Smart Workplace Evolution & Digital HR

Schwerpunktthemen: ITSM, AI/KI, Cloud Computing, IT & Nachhaltigkeit, SAP-Partnerlösungen, Unified Communications

Die Ausgabe 01/02 2026 erscheint am 16. Januar 2026



UNSERE THEMEN

it security

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

Aagon GmbH (Teaser)	U1
it verlag GmbH	U2, 47, U3
USU Software AG	7
ams.Solution AG	9
GRAU DATA GmbH (Advertorial)	25
E3 / B4B Media	35
SPS/ Mesago Messe Frankfurt GmbH	39
Panasonic Connect Europe GmbH	U4

it security

it verlag GmbH	U2, 35, U3
Cloudflare (Advertorial)	17
Boomi (Advertorial)	21
Beazley	U4

IMPRESSUM

Herausgeber: Ulrich Parthier (08104-6494-14)

Geschäftsführer: Ulrich Parthier, Vasiliki Miridakis

Chefredaktion: Silvia Parthier (-26)

Redaktion: Lars Becker, Carina Mitzschke (nur per Mail erreichbar)

Redaktionsassistenz und Sonderdrucke: Eva Neff (-15)

Autoren: Lars Becker, Lumir Boureanu, Michael Chalvatzis, Dr. Christian Gilcher, André Finken, Kai Hambrecht, Peter Heppt, Ivo Ivanov, Paola Krauss, Frank Laschet, Bruno Maddaloni, Carina Mitzschke, Niels Northe, Silvia Parthier, Ulrich Parthier, Michael Pietsch, Oliver Rauschil, Lennart Rother, Christian Scharrer, 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. 33.
Preisliste gültig ab 1. Oktober 2025.

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.



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

TOUGHBOOK

Mobile-IT-as-a-Service

Reduzierte Komplexität mit Managed Services

Sie benötigen einfache, zuverlässige Mobile-IT Lösungen, die die Produktivität Ihrer Mitarbeitenden steigern, Risiken minimieren und sich nahtlos an Ihre individuellen Anforderungen anpassen?



Profitieren Sie von Ihrem maßgeschneiderten Abo-Modell!

HARDWARE:
Statten Sie Ihr mobiles Team mit den zuverlässigsten und flexibelsten Geräten aus.

ZUBEHÖR:
Optimieren Sie die Hardware-Nutzung für reibungsloses mobiles Arbeiten – überall.

SOFTWARE:
Stärken Sie Ihre mobilen Teams mit leistungsstarken Anwendungen.

SERVICES:
Setzen Sie auf höchste Verfügbarkeit – damit Einsätze unterwegs effizient bleiben.

MONATS-ABO:
Nutzen Sie Ihr Mobile IT Paket einfach skalierbar zu planbaren monatlichen Kosten.

Erfahren Sie, wie TOUGHBOOK Mobile-IT-as-a-Service Ihr Unternehmen unterstützen kann.

Panasonic CONNECT

it security

Detect. Protect. Respond.
November/Dezember 2025



AB SEITE 8

ONEAPP4DEUTSCHLAND – SICHER & COMPLIANT

Digitalisierungs-Turbo

Ismet Koyun, KOBIL Gruppe

POST-QUANTEN-KRYPTOGRAFIE
Vorbereitung auf die digitale Zukunft

IT SECURITY AWARDS 2025
Gewinner auf der it-sa ausgezeichnet

DEEPFAKE-ERKENNUNG
Die Ära der digitalen Täuschung

www.it-daily.net



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

it-daily.net

JETZT
ENTDECKEN!

Inhalt



COVERSTORY

4 **Digitalisierungs-Turbo**
OneApp4Deutschland – zwischen digitaler Vision und Realität

THOUGHT LEADERSHIP

8 **CISO-Know-how darf kein exklusives Gut sein**
Security-Services bringen den Mittelstand auf Enterprise-Level

IT SECURITY

12 **it security AWARDS 2025**
SentinelOne, CrowdStrike, Darktrace und MetricStream ausgezeichnet

16 **Ganzheitliche Sicherheitsstrategien**
Vom Vulnerability Management zum Exposure Management

18 **Vorbereitung auf die digitale Zukunft**
Herausforderungen der Post-Quanten-Kryptografie und Einführung in Unternehmen

22 **Cyber-Resilience**
Wie DriveLock und Idgard Europas digitale Souveränität stärken

25 **Risiko- und Compliance-Management ist machbar**
Von manuellen Prozessen zur KI-gestützten Automation

26 **KI am Edge**
Technologischer Fortschritt im Außendienst

29 **Grundschutz++**
Große Pläne und offene Fragen

30 **Mit DORA zur Datensouveränität**
Einheitliche Sicherheitsstandards für Banken und Versicherungen

33 **Digital Operational Resilience Act**
Neun Monate nach der Einführung

34 **Mobile Sicherheit im Unternehmensalltag**
Der Maßstab für transparente Unternehmenssicherheit

36 **Zero Trust in der Produktion**
Industrie 4.0 vor Cyberangriffen schützen

39 **AXA Future Risks Report 2025**
Cyberrisiken werden in Deutschland stark unterschätzt

40 **Versicherbarkeit von Ransomware**
Warum Prävention und Versicherung zusammengehören

42 **Die neue Ära der digitalen Täuschung**
Deepfakes erkennen, bevor sie Schaden anrichten

Digitalisierungs-Turbo

ONEAPP4DEUTSCHLAND – ZWISCHEN DIGITALER VISION UND REALITÄT

Die Digitalisierung Deutschlands ist ein dringender, aber kein hoffnungsloser Fall. Die Zukunft liegt in einer standardisierten digitalen Plattform, weiß der CEO und Gründer des Security-Spezialisten KOBIL – und zeigt im Interview, wie es gehen kann.

it security: *Es ist ein Dauerthema: Deutschland hinkt bei der Digitalisierung hinterher – ob in der Verwaltung, der Wirtschaft oder im Alltagsleben. Wann und wie werden wir endlich digital, Herr Koyun?*

Ismet Koyun: Wir sind nicht weit davon entfernt. Die Technologie ist da: unsere All-in-One SuperApp. Sicher, benutzerfreundlich und live in fünf Tagen. Unsere City-Apps in Istanbul und Worms sind der Blueprint, um damit ganz Deutschland zu digitalisieren. Dort ist die Plattform erfolgreich im Einsatz und täglich genutzt. Wir haben viele Jahre Erfahrung mit der Digitalisierung von Städten und Kommunen. 3.000 Manntage sind alleine in die Entwicklung unserer Plattform für Deutschland geflossen. Kein anderer Anbieter in Europa hat diese Expertise und Technologie. Und niemand sonst bringt eine Stadt-App in kürzester Zeit live. Unsere Lösung baut Bürokratie ab, ist nutzerfreundlich und hochsicher. Das erleichtert allen den Alltag: Kommunen, Bürgern, Unternehmen, Startups – und schafft Vertrauen. So wird Deutschland digital und zukunftsfähig.



MIT DER ONEAPP4-DEUTSCHLAND STELLEN WIR DIE TECHNOLOGIE BEREIT, UM DEUTSCHLAND FLÄCHENDECKEND ZU DIGITALISIEREN – ICH SAGE, DAS GEHT IN SECHS MONATEN.

Ismet Koyun, CEO und Gründer, KOBIL Gruppe, www.kobil.com

it security: *Wie stellen Sie sich den Alltag mit der OneApp4Deutschland vor?*

Ismet Koyun: Das Leben wandert ins Digitale – auf eine einzige Plattform. Nicht mehr zig verschiedene Apps, Konten und Passwörter. Stattdessen alles in einem: Behördendienste, Banking, Kommunikation, E-Commerce, Mobilität, Kultur. In jeder Stadt in Deutschland.

Dabei geht es nicht nur um Technologie – entscheidend ist die Alltagstauglichkeit. Digitale Services müssen bequem sein, komfortabel, nahtlos, unbürokratisch und leicht zu nutzen. Nur dann werden sie akzeptiert. Und sie müssen absolut sicher sein. Sicherheit ist die Grundlage für Vertrauen. Und Vertrauen die Basis von Erfolg.

Sicherheit hat viele Dimensionen. Wir müssen die persönlichen Daten der Nutzer schützen, aber auch unsere demokratischen Werte. Denn unsere digitalen Infrastrukturen sind Angriffsziel von Kriminellen und autoritären Staaten. Deswegen ist digitale Souveränität unverzichtbar.

it security: *Was ist das Besondere an Ihrer Entwicklung?*

Ismet Koyun: Wir haben die OneApp-4Deutschland als SuperApp gebaut – für Städte, Kommunen und besonders auch Behörden. Jedes Unternehmen, jede Bank, jede Bildungseinrichtung oder Kulturinstitution kann mitmachen und Angebote als MiniApp in die myCityApp integrieren. Auch jedes Startup. Das ist wichtig, denn damit eine solche App funktioniert, braucht es ein breites Angebot.

Als digitale Brieftasche vereint sie alle gängigen Identitäten in einem einzigen Wallet – darunter OZG, Bund-ID, EU-Wallet sowie die qualifizierte elektronische Signatur. Einmal authentifiziert, können Bürger alles nutzen, ohne die App zu verlassen. Zum Beispiel städtische Services, OZG-Leistungen wie Führerscheinanträge, aber eben auch Shopping, Restaurants reservieren oder Theatertickets kaufen. Es ist eine eigene Chat-Funktion integriert sowie ein sicheres Identitäts- und Signatursystem. Eine vergleichbare Technologie gibt es weltweit nicht.



it security: *Sie erwähnen explizit Startups. Welche Rolle spielen Gründer für Sie?*

Ismet Koyun: Startups sind Innovationstreiber. Ohne sie können wir die Digitalisierung nicht schaffen. Wir müssen sie unterstützen, damit sie schneller und unbürokratischer gründen können. Deshalb bieten wir unsere Technologie auch ihnen an. Sie können damit ihre eigene App oder SuperApp erstellen und in unsere myCityApps integrieren – damit haben sie sofortigen Marktzugang. Wir haben auch ein eigenes Venture-Studio gegründet. Startups bekommen damit alles, was sie brauchen: Zugang zu Kunden, zu Partnern, zu Kapital. Und eine sichere, fertige Infrastruktur, die sie sofort nutzen und skalieren können.

it security: *Das klingt in der Theorie überzeugend. Was macht Sie so sicher und gibt es bereits Proof Points?*

Ismet Koyun: Was KOBIL entwickelt hat, wurde zum Standard. Schon in den 1990er Jahren war Cybersecurity mein großes Thema. Ich habe damals unter anderem den TAN-Generator erfunden. Noch heute sind wir darin Marktführer. Wir haben das weltweit erste Patent für digitale Signaturen. Und bereits vor zehn Jahren war mir klar: Digitalisierung kann nur mit einer sicheren, einheitlichen Plattform gelingen. Deshalb haben wir die SuperApp entwickelt – übrigens die einzige sichere SuperApp-Plattform Europas, mehrfach bestätigt vom Forschungs- und Beratungsunternehmen Gartner. Und die Nutzer geben uns recht: Die SuperApp ist seit 2021 erfolgreich im Einsatz und macht Millionen Menschen das Leben leichter.

it security: *Sie sagen selbst: Sicherheit spielt eine zentrale Rolle. Erhöht nicht die Abhängigkeit von einer zentralen Lösung das Risiko?*

Ismet Koyun: Nein. Eine einheitliche Plattform bedeutet nicht, Risiken zu erhöhen, sondern sie werden besser kontrollierbar. Seit über 30 Jahren entwickeln wir Sicherheitstechnologien und werden weltweit von mehr als 100 Millionen Anwendern genutzt. Städte, Behörden, Unternehmen, Startups, Bürger – sie alle können sich auf uns verlassen. Unsere myCityApp beruht auf bewährter Architektur inklusive sicherer digitaler Identität für jeden Nutzer sowie Zero-Trust-Prinzip. Jede Aktion wird geprüft. Künstliche Intelligenz spielt dabei eine wichtige Rolle: Sie erkennt Anomalien in Echtzeit und stoppt Angriffe, bevor sie Schaden anrichten.

Bezahlung, Signaturen, Verträge – alles läuft über verschlüsselte, rechtssichere Prozesse. Ein Alleinstellungsmerkmal ist unsere eigene unabhängige und hochsichere Chat-Technologie. Wer innerhalb der Plattform Transaktionen durchführt oder sich austauscht, kann sich auf absoluten Schutz verlassen.

it security: *Wir haben bislang vor allem über die Digitalisierung von Städten gesprochen. Wie sieht es in der Wirtschaft aus? Wie können Unternehmen ihre Prozesse effizient digitalisieren?*

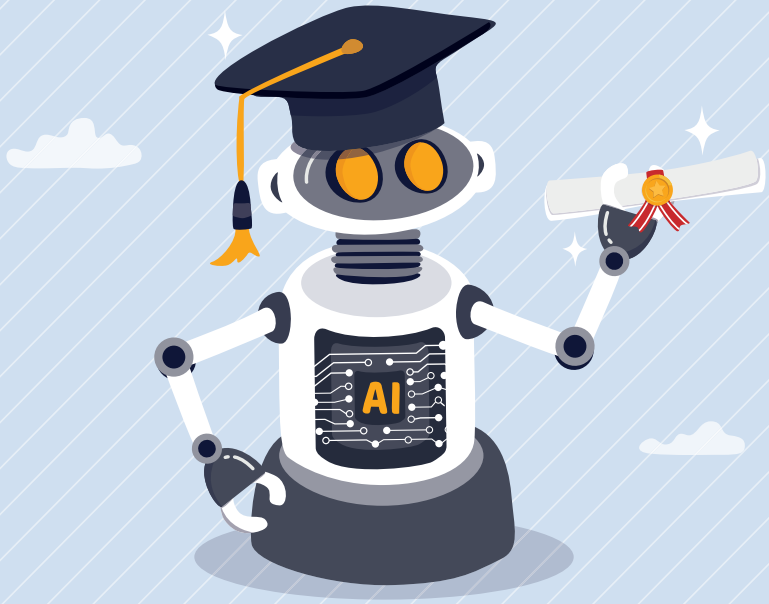
Ismet Koyun: Unternehmen nutzen meist unzählige digitale Tools – von Identität über Kommunikation bis zu Apps. Jede zusätzliche Anwendung bedeutet neue Schnittstellen und Sicherheitsrisiken. Deshalb haben wir die Enterprise-Plattform mPower entwickelt. Auch hier steht im Fokus: Eine Plattform für alles. Damit geben wir Unternehmen ein All-in-One-Tool an die Hand, um Ordnung in ihre digitalen Prozesse zu bringen – bei voller Einhaltung regulatorischer Vorgaben. Das ist bisher einzigartig: Gängige Enterprise-Plattformen decken Teile des digitalen Lifecycles einer Organisation ab, etwa die Dokumentenverwaltung. Aber eine vollumfängliche Plattform mit einem Login für sämtliche Prozesse – vom Onboarding und Offboarding über digitale Signaturen und Kommunikation bis hin zum Identitätsmanagement – das gibt es so noch nicht.

it security: *Welche Weichen müssen jetzt gestellt werden, damit Ihr Vorhaben gelingen kann?*

Ismet Koyun: Allein werde ich es nicht schaffen. Wir brauchen mehr mutige Leute, die Neues wagen. Deutschland ist ein Land der Nein-Sager und Zweifler. Das muss sich ändern – aber das geht nur im Zusammenschluss. Städte, Kommunen, Unternehmen, Bürger und die Politik müssen ihre Kräfte bündeln. Jeder bringt seine Stärken ein. Im Ergebnis entsteht ein digitales Ökosystem, das sicher, intelligent und fair ist. Das die digitale Souveränität in Deutschland und Europa stärkt. Und das unser Land nicht nur digitalisiert, sondern ihm auch zu neuem Glanz verhilft.

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





KÜNSTLICHE INTELLIGENZ UND WIR

STAND, NUTZUNG UND HERAUSFORDERUNGEN DER KI

Generative KI-Systeme schaffen durch die Nutzung von Sprache und Text eine natürliche Schnittstelle zur menschlichen Kommunikation. Viele Nutzende begegnen diesen Systemen mit denselben Maßstäben und Erwartungen, die sie aus dem Umgang mit anderen Personen kennen. Doch gerade diese intuitive Herangehensweise und scheinbare Vertrautheit birgt Risiken – insbesondere, wenn technologische Grundlagen und mögliche Implikationen von KI nicht klar sind.

Um generative KI – und Künstliche Intelligenz insgesamt – fundiert und differenziert beurteilen zu können, bedarf es einer breiten und intensiven Auseinandersetzung mit dem Thema.

Dieses Open Access Buch bietet einen umfassenden Überblick über den aktuellen Stand der Technikentwicklung und die zukünftigen Möglichkeiten der Künstlichen Intelligenz (KI). Experten aus verschiedenen Disziplinen beleuchten die vielfältigen Aspekte der KI, von technischen Grundlagen über ethische Fragestellungen bis hin zu gesellschaftlichen und wirtschaftlichen Auswirkungen. Das Buch wendet sich an Lehrende und Lernende an deutschsprachigen Hochschulen und kann als Lehrbuch außerhalb der Informatik verwendet werden.

Zu den Herausgebern gehören der Wirtschaftswissenschaftler Frank Schmiedchen, der seit 2017 die Studiengruppe Technikfolgenabschätzung der Digitalisierung der Vereinigung Deutscher Wissenschaftler leitet, der ehemalige Vizepräsident der Gesellschaft für Informatik Alexander von Gernler, der Abteilungsleiter Research und Innovation der genua GmbH ist, die Wirtschaftsinformatikerin Martina Hafner, die bei der genua GmbH als Innovationsmanagerin arbeitet, und Klaus Peter Kratzer, der Professor für Informatik an der Technischen Hochschule Ulm war.



Künstliche Intelligenz und Wir – Stand, Nutzung und Herausforderungen der KI; Frank Schmiedchen, Alexander von Gernler, Martina Hafner, Klaus Peter Kratzer (Hrsg.); Springer Vieweg; 10-2025

WENN CISO-EXPERTISE FEHLT

Die Anforderungen an Cybersicherheit steigen kontinuierlich – nicht nur für Großkonzerne, sondern auch für mittelständische Unternehmen. Regulatorische Vorgaben wie NIS2, DORA oder die DSGVO fordern klare Verantwortlichkeiten und qualifizierte Sicherheitsstrategien. Doch während nur ein Bruchteil der Unternehmen weltweit über einen Chief Information Security Officer verfügt, kämpft insbesondere der Mittelstand mit akutem Fachkräftemangel. Wie können kleinere und mittlere Organisationen dennoch ein Enterprise-Level an Cybersicherheit erreichen?



CISO-Know-how darf kein exklusives Gut sein

SECURITY-SERVICES BRINGEN DEN MITTELSTAND AUF ENTERPRISE-LEVEL

Schätzungsweise haben nur 0,009 Prozent der Millionen Unternehmen weltweit einen Chief Information Security Officer (CISO) – meist große Unternehmen und Konzerne. Doch den Bedarf, Cybersecurity strategisch zu betreiben, haben alle Unternehmen. Besonders der Mittelstand und kleinere Unternehmen stehen vor der Herausforderung, die Aufgaben zentraler Rollen wie die des CISO zu erfüllen. Managed Security Services können hier entscheidende Entlastung bringen und einen für Unternehmen jeder Größe realisierbaren, virtueller CISO an Bord holen.

Die Rolle des CISO bzw. Cybersicherheitsverantwortlichen hat sich in den vergangenen Jahren von einer optionalen Position vielfach zu einer regulatorisch geforderten Schlüsselfunktion entwickelt.



Quelle: Sophos

Sowohl die NIS2-Richtlinie der EU als auch der Digital Operational Resilience Act (DORA) sowie der IT-Grundschutz des BSI und die DSGVO fordern eine klare Zuordnung von Verantwortlichkeiten in der Cybersicherheit. Unternehmen müssen nachweisen können, dass Sicherheitsstrategien von einer qualifizierten Instanz definiert, umgesetzt und überwacht werden. Der Sicherheitsverantwortliche fungiert dabei als zentrale Steuerungsstelle für alle Sicherheitsaktivitäten: Er entwickelt Sicherheitsstrategien, priorisiert Risiken, koordiniert die operative Umsetzung und berichtet an die Geschäftsführung.

Gleichzeitig kämpfen Unternehmen mit einem strukturellen Problem: Es fehlt an Fachpersonal und damit auch an CISOs. Der Branchenverband Bitkom rechnet mit einem IT-Fachkräftemangel von über 650.000 Expertinnen und Experten bis 2040. Im Mittelstand ist die Lage besonders angespannt. Viele Unternehmen verfügen weder über das Budget noch über die Attraktivität großer Konzerne, um erfahrene Sicherheitsexperten zu gewinnen und langfristig zu halten. Hinzu kommt, dass Marktforscher prognostizieren, dass rund die Hälfte der CISOs bis 2025 ihre aktuelle Position verlassen wird. Sobald ein erfahrener Sicherheitsexperte ein mittel-

ständisches Unternehmen verlässt, ist Ersatz meist schwer zu finden – die Rekrutierungsprozesse dauern oft viele Monate und verschlingen erhebliche Ressourcen.



Fehlende Expertise erhöht das Risiko

Die Folgen dieses Fachkräftemangels sind bereits deutlich messbar. Der „Sophos State of Ransomware Report 2025" zeigt, dass Unternehmen mit weniger als 500 Mitarbeitenden fehlendes Fachpersonal im Bereich Cybersecurity als zweitgrößtes Sicherheitsrisiko bewerten. In Deutschland führen 44 Prozent der befragten Organisationen erfolgreiche Cyberangriffe – insbesondere Ransomware-Attacken – direkt auf fehlende Kenntnisse und Fähigkeiten zurück, um Bedrohungen rechtzeitig zu erkennen und zu stoppen.

Fehlt eine zentrale strategische Instanz wie der CISO, fehlt häufig auch die langfristige Sicherheitsplanung. Sicherheitsmaßnahmen werden dann eher reaktiv umgesetzt – etwa nach einem Vorfall – anstatt proaktiv auf Basis einer klaren Risikoanalyse.

Bewusst Risiken eingehen

Wie groß der Handlungsdruck tatsächlich ist, zeigen auch die Ergebnisse der Sophos-Managementstudie. Demnach gaben über zehn Prozent der befragten mittelständischen Unternehmen an, bewusst Cybersicherheitsrisiken eingegangen zu sein – eine Situation, die ein erfahrener CISO in der Regel unterbinden würde. Zudem sind sich die Verantwortlichen über ihre schwächere Position am Arbeitsmarkt durchaus im Klaren: Rund 50 Prozent der Manager von Unternehmen mit einer Mitarbeiteranzahl von 50 bis 199 Mitarbeitern sehen größere Organisationen als attraktivere Arbeitgeber für IT-Security-Fachkräfte.

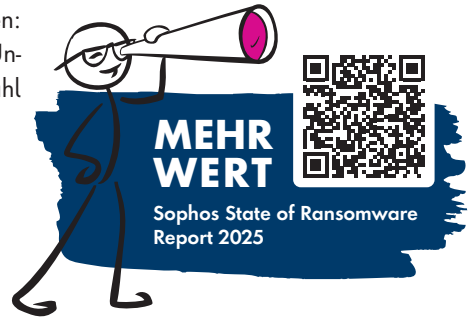
Diese Einschätzung ist angesichts der dynamischen Bedrohungslage besonders problematisch. Angreifer entwickeln ihre Methoden kontinuierlich weiter, nutzen Automatisierung, KI und gezielte Social-Engineering-Techniken. Unternehmen, die Sicherheitslücken aus Ressourcengründen bewusst in Kauf nehmen, setzen ihre Geschäftsfähigkeit zunehmend aufs Spiel.

Managed Security Services als pragmatischer Ausweg

Vor diesem Hintergrund gewinnen Managed Security Services zunehmend an Bedeutung. Sie bieten Unternehmen die Möglichkeit, lückenhafte Fachkenntnisse und Kapazitäten durch externe Expertise zu kompensieren. Besonders im Fokus steht Managed Detection and Response (MDR). MDR kombiniert Endpoint Detection and Response (EDR) sowie Extended Detection and Response (XDR) mit einem spezialisierten, rund um die Uhr aktiven Sicherheitsteam. Diese Expertinnen und Experten erkennen und analysieren Angriffe in Echtzeit und können auch komplexe, manuell gesteuerte Attacken stoppen. Durch den Einsatz moderner Technologien, Machine Learning und KI sind MDR-Teams in der Lage, Bedrohungen zu identifizieren, die klassische Schutzmechanismen oft übersehen.

Dass Managed Security Services Unternehmen in Zeiten hoher Risikopotenziale maßgeblich und wirksam unterstützen, steht außer Frage. Dies bestätigt die Entwicklung von Sophos, der als Lösungs- und Managed-Services-Anbieter gemeinsam mit seinen Partnern über 26.000 Unternehmen mit MDR betreut – bei einem steilen Wachstum von jährlich über 30 Prozent.

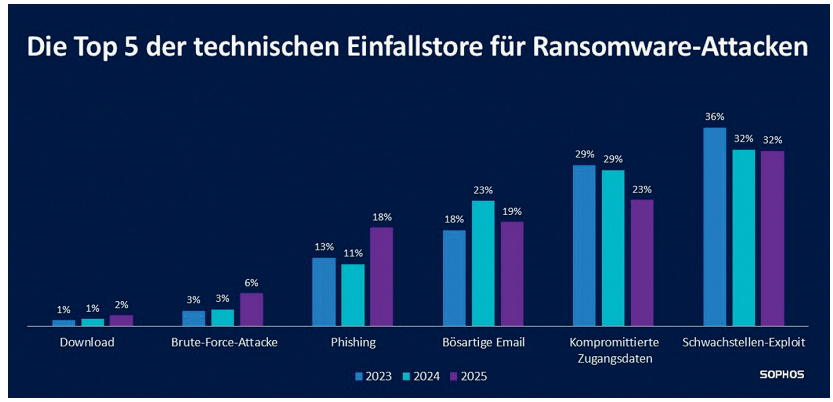
Doch trotz der operativen Vorteile können Managed Services die Rolle des CISO nicht vollständig ersetzen. Insbesondere die strategischen und für das Unternehmen individuell in die Zukunft ausgerichtete Sicherheitskonzep-



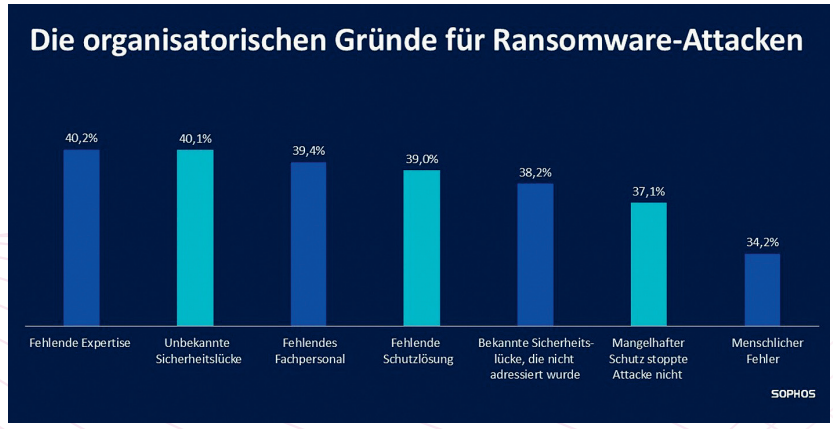
te sind ohne die steuernde Funktion einer CISO-Rolle nicht vollumfänglich abzubilden.

Virtuelle CISOs schließen die Lücke

Ein zusätzlicher Ansatz ist daher der Einsatz eines virtuellen CISOs als Unterstützung zum existierenden IT- und Sicherheitspersonal eines Unternehmens. Im Rahmen eines Managed-Services-Angebots bringen die spezialisierten Sicherheitsstrategen dabei ihre Expertise als externe Dienstleistung in das Unternehmen ein und übernehmen dabei zentrale Aufgaben: Sie entwickeln Sicherheitsstrategien, erstellen Richtlinien, begleiten Audits und beraten die Geschäftsführung – kontinuierlich und mittel- bis langfristig. Die Kombination verschiedener Managed Security Services realisiert so ein schlagkräftiges Resilienzmodell, das sowohl operative Abwehrmaßnahmen als auch strategische Planung abdeckt.



Quelle: Sophos



Quelle: Sophos

Durch die Integration einer KI-gestützten Sicherheitsplattformen mit Managed Services und dem Ansatz des virtuellen CISO lässt sich ein Sicherheitsniveau erreichen, das bisher hauptsächlich großen Konzernen vorbehalten war – und das mit erheblich geringerem Budgetaufwand. Gerade mittelständische Unternehmen können damit ihre Cyberresilienz effektiv stärken und sind nicht weiter ein Spielball der marktbedingten Personalknappheit.



Fazit

Der Fachkräftemangel in der IT-Security ist eine strukturelle Herausforderung, die in den kommenden Jahren eher zunehmen als abnehmen wird. Mittelständische und kleine Unternehmen müssen deshalb neue Wege angeboten werden, um ihre Sicherheit auf Enterprise-Niveau zu heben – ohne die Ressourcen und Budgetgrenzen zu sprengen. Managed Security Services mit virtuellen CISOs bieten hier einen pragmatischen, wirtschaftlich tragfähigen Ansatz, um die Abwehrfähigkeit als auch die strategische Steuerung der Security sicherzustellen. Denn Cybersicherheit sollte kein Privileg großer Konzerne sein, sondern eine Selbstverständlichkeit für Unternehmen jeder Größe.

Michael Veit | www.sophos.com

DEBIAN GNU/LINUX 13

DER UMFASSENDE PRAXISEINSTIEG

Debian ist eine stabile, langlebige und professionelle Linux-Distribution, die ein Höchstmaß an Anpassungsfreiheit bietet. Dieses Buch begleitet Sie von der Installation und der Konfiguration bis hin zum produktiven Einsatz – unabhängig davon, ob Sie Linux-Neuling oder erfahrener Anwender sind. Dank übersichtlicher Strukturierung und anschaulicher Schritt-für-Schritt-Anleitungen ist es sowohl als Einführung als auch zum Nachschlagen geeignet.

System professionell konfigurieren und administrieren

Neben den Grundlagen vermittelt der Autor praxisnahes Wissen für die Linux-Administration: Sie erfahren, wie Sie das System effizient über das Terminal bedienen, Software und Firmware aktuell halten, Prozesse mit Systemd steuern und wiederkehrende Aufgaben mit Cron automatisieren. Auch Sicherheitsaspekte und Backup-Strategien sowie Möglichkeiten zur Systemwiederherstellung werden verständlich und detailliert behandelt.





Debian GNU/Linux 13 –
Der umfassende Praxiseinstieg;
Robert Gödl; mitp Verlags GmbH &Co.KG, 11-2025

Debian effektiv auf Desktop und Server einsetzen

Ob klassischer Arbeitsplatz oder leistungsfähiger Server – dieses Buch zeigt Ihnen alle Grundlagen für den effektiven Einsatz von Debian und unterstützt Sie dabei, das volle Potenzial der Distribution im Alltag oder im professionellen Umfeld auszuschöpfen.

Aus dem Inhalt

- Benutzer und Rechteverwaltung
- Netzwerkkonfiguration
- Apache und MariaDB
- Virtualisierung mit Docker
- Firewall konfigurieren
- Backups und Datenrettung
- Systemwiederherstellung

it security AWARDS 2025

SENTINELONE, CROWDSTRIKE, DARKTRACE UND METRICSTREAM AUSGEZEICHNET

itsecurity AWARD 2025
WWW.IT-SECURITY-AWARD.COM

DIE PREISTRÄGER DER IT SECURITY AWARDS 2025 STEHEN FEST. IN DER 19. AUFLAGE WURDEN HERAUSRAGENDE LÖSUNGEN IN DEN KATEGORIEN CLOUD SECURITY, IAM, INTERNET/WEB SECURITY UND MANAGEMENT SECURITY AUSGEZEICHNET. DIE VERLEIHUNG FAND AM 7. OKTOBER 2025 AUF DER IT-SECURITY-MESSE IT-SA IN NÜRNBERG STATT.

CLOUD SECURITY

SentinelOne Purple AI

Mit SentinelOne Purple AI zeichnete die Jury eine Technologie aus, die nicht nur ein weiteres Tool ist, sondern einen fundamental neuen Ansatz in der Cybersicherheit verkörpert: die Anwendung generativer KI als proaktiven Partner für Sicherheitsanalysten.

Während herkömmliche Security-Plattformen oft nur Alarme generieren und Daten sammeln, setzt Purple AI einen Schritt früher an: bei der menschlichen Expertise.

Die Innovation liegt in einer konversationellen, generative KI-Schnittstelle, die direkt in den Investigions-Workflow des Analysten integriert ist. Dieses Alleinstellungsmerkmal erlaubt es, in natürlicher Sprache mit den Sicherheitsdaten zu interagieren. Statt mühsam manuelle Abfragen in Suchsprachen zu schreiben, kann ein Mitarbeiter einfach fragen: „Untersuche verdächtige Aktivitäten von dieser IP-Adresse in den letzten 24 Stunden und fasse die Ergebnisse für meinen Vorgesetzten zusammen."

Purple AI erledigt die Arbeit sekundenschnell – sie korreliert Daten aus verschiedenen Quellen, erstellt eine nachvollziehbare „Storyline" des Angriffsverlaufs und generiert sogar einen fertigen Report für das Management.

Die Lösung

SentinelOne Purple AI ist primär eine Cloud-native Lösung (SaaS), die jedoch entwickelt wurde, um eine hybride Umgebung nahtlos zu schützen.

Die Purple AI-Plattform wird von SentinelOne in der Cloud betrieben und verwaltet. Kunden interagieren über einen Webbrowser mit der Oberfläche. Es ist keine eigene Hardware-Infrastruktur on-premises erforderlich. Die Plattform kann Daten aus allen Umgebungen aufnehmen und analysieren.

Die KI-Analyse findet zentral in der SentinelOne-Cloud statt, aber die zum Sammeln der Daten benötigten Agenten (für Endpoints, Server, Cloud-Workloads) können überall deployed werden.

MEHR WERT
IT Security Awards 2025



Die Preise nahmen persönlich entgegen: (v.l.n.r.) Aris Koios, Principal Field Tech Strategist, und Ingo Marienfeld, SVP Central Europe, CrowdStrike; Ulrich Parthier, Herausgeber IT Security; Erhan Oezmen, Vice President, SentinelOne; Marco di Meo, VP Sales, Darktrace; Marko Kirschner, SentinelOne

Viele SentinelOne-Partner (MSSPs - Managed Security Service Provider) und SentinelOne selbst bieten an, den Betrieb der gesamten Plattform, inklusive der Überwachung und Reaktion durch ihre SOC-Analysten, als Managed Detection and Response (MDR)-Service zu übernehmen. In diesem Fall „mietet" der Kunde die Expertise und den Service, nicht nur die Software.

Der Unterschied: Warum gerade dieses Produkt?

Viele Plattformen setzen auf KI zur Anomalie-Erkennung oder Automatisierung. Purple AI geht einen entscheidenden Schritt weiter. Es ist nicht nur eine Funktion, sondern ein Kraftmultiplikator für das gesamte Team.

Andere Plattformen liefern die Rohdaten und Alarme (das „Was"). Purple AI liefert die Analyse, die Korrelation, die Zusammenfassung und die Handlungsempfehlung (das „So what" und „What's next").

Es stärkt den Menschen in der Entscheidungsschleife, anstatt ihn zu ersetzen. Genau diese menschenzentrierte Anwendung von KI, die einen echten, quantifizierbaren Mehrwert für überlastete Sicherheitsteams liefert, hat die Jury überzeugt und macht SentinelOne Purple AI zu einem mehr als würdigen Gewinner des IT Security Awards.

https://de.sentinelone.com

IAM

CrowdStrike Falcon Identity Protection

Identity Threat Protection ist im Bereich IAM aktuell eines der wichtigsten Neuerungen.

CrowdStrike ist in erster Linie ein Cybersecurity-Unternehmen, das auf Endpoint Protection (EPP) und Endpoint Detection and Response (EDR) spezialisiert ist. Ihre Kernkompetenz liegt darin, Bedrohungen auf Endgeräten (Laptops, Server, etc.) zu erkennen und zu stoppen.

IAM (Identity and Access Management) ist traditionell ein separates Feld, das sich mit der Verwaltung von Benutzeridentitäten, Zugriffsrechten und Au-

thentifizierung befasst (etwa Tools wie Okta, Microsoft Entra ID/Azure AD, Ping Identity).

Der Anwender als neuer „Endpoint"

CrowdStrike bewegt sich stark in den Bereich der Identity Threat Protection hinein. Das bedeutet, sie betrachten die „Identität" (den Benutzer) als das neue „Endpoint". Wenn ein Angreifer die Anmeldedaten eines Benutzers stiehlt, wird der legitime Account zum Einfallstor. Herkömmliche IAM-Lösungen erkennen das oft nicht, weil der Login technisch „korrekt" aussieht.

Genau hier setzt die CrowdStrike Falcon Identity Protection: an. Es ist ein spezielles Modul, das die Stärken der CrowdStrike-Plattform (EDR, Threat Intelligence) auf Identitätsbedrohungen anwendet. Dabei werden die Active Directory-Umgebung in Echtzeit auf verdächtige Aktivitäten (etwa Brute-Force-Angriffe, Passwort-Spraying, Kerberoasting, ungewöhnliche Zugriffe von Administratoren) überwacht.

Die Plattform korreliert Identitätsereignisse mit anderen Telemetriedaten auf dem Endpoint. Wenn sich also jemand von einem kompromittierten Gerät aus anmeldet, kann sie Software diesen Zusammenhang sofort herstellen und den Vorfall stoppen.

Zudem bietet es die Integration in traditionelle IAM-Lösungen: Die Lösung konkurriert also nicht direkt mit den traditionellen, reinen IAM-Anbietern. Stattdessen integriert es sich mit ihnen. Beispielsweise kann CrowdStrike Risikosignale (beispielsweise „dieser Login kommt von einem infizierten Gerät") an eine IAM-Lösung senden, die dann eine stärkere Authentifizierung (MFA) erzwingt oder den Zugriff blockiert.

Die perfekte Ergänzung

CrowdStrike ist auch im Bereich Identity Security / Identity Threat Detection and Response (ITDR) tätig. Sie betrachten die Identität als kritischen Angriffsvektor und nutzen ihre Plattform, um identitätsbasierte Angriffe zu erkennen und zu bekämpfen, die für traditionelle IAM-Lösungen unsichtbar sind.

In der modernen Sicherheitsarchitektur ergänzen sich traditionelle IAM-Lösungen (die die Türen verwalten) und Lösungen wie CrowdStrike Falcon Identity Protection (die überwachen, ob jemand die Schlüssel gestohlen hat und die Türe missbraucht) ideal.

https://www.crowdstrike.com/de-de

INTERNET/WEB SECURITY

Darktrace ActiveAI Security Platform

Darktrace bietet mit der ActiveAI Security Platform einen proaktiven Ansatz zur Cyber-Resilienz auf einer einzigen Plattform. Unternehmen bekommen frühzeitig einen klaren Überblick über ihre aktuelle IT-Sicherheitssituation, so dass sie potenzielle Schwachstellen oder ungewöhnliche Aktivitäten sehen, bevor daraus ein echter Angriff oder Schaden entsteht. Die Lösung reagiert autonom auf bekannte und unbekannte Bedrohungen.

Dabei unterscheidet sich die Lösung grundsätzlich von anderen durch die Nutzung der KI, denn Darktrace bringt seine KI in die Daten des Unternehmens ein, egal wo sie sich befinden. Anstatt einem KI-System beizubringen, wie ein „Angriff" aussieht, und es an großen Datenseen mit Tausenden von Unternehmensdaten zu trainieren, lernt Darktrace AI aus echten individuellen Geschäftsdaten. So versteht die Lösung, was normal ist, und kann so risikoreiche, anomale Aktivitäten für jedes Asset domänenübergreifend identifizieren. Dies ermöglicht es, subtile Abweichungen zu erkennen, die auf eine Bedrohung hinweisen, einschließlich neuartiger und KI-gesteuerter Cyberangriffe.

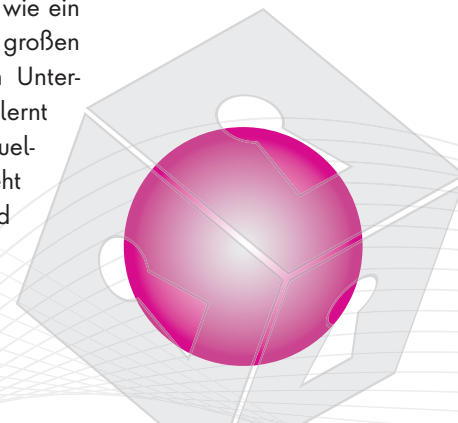
Die Lösung

Die meisten KI-Cybersicherheitslösungen basieren auf der Übertragung von Daten aus dem Unternehmen in große, in der Cloud gehostete Datenbanken, in denen Angriffsmuster erkannt werden, sodass Bedrohungen gestoppt werden können, wenn sie erneut auftreten.

Angreifer nutzen mittlerweile KI-gesteuerte polymorphe Malware, gegnerische KI-Techniken und heimliche laterale Bewegungen – was bedeutet, dass neuartige Angriffe immer häufiger vorkommen. Traditionelle Sicherheitsmodelle werden dadurch wirkungslos, und Verteidiger benötigen eine KI, die mithalten kann. Anstatt aus früheren Angriffen zu lernen, kombiniert Darktrace mehrere KI-Modelle, um das „Normalverhalten" des jeweiligen Unternehmens zu verstehen und ungewöhnliches Verhalten aufzudecken.

Die selbstlernende KI von Darktrace basiert auf einem mehrschichtigen KI-Ansatz, der verschiedene KI-Methoden, -Techniken und -Funktionen strategisch kombiniert. So gelingt es der KI, Verhalten vorherzusagen, Bedrohungen zu erkennen, in Echtzeit zu reagieren und Vorfälle zu analysieren. Alles mit dem Ziel, das Cyberrisiko in Unternehmen zu reduzieren.

https://www.darktrace.com/de





> DAS JAHR 2025 ZEIGT VIELE INNOVATIONEN IM BEREICH DER IT-SECURITY UND SIND MIT SICHERHEIT KI-GETRIEBEN, JEDENFALLS IM HINTERGRUND. ZU VIEL KI-GEHABE TUT DER BRANCHE NÄMLICH ALLES ANDERE ALS GUT.
>
> Ulrich Parthier, Herausgeber it security, www.it-daily.net

MANAGEMENT SECURITY

MetricStream

In einer Welt sich ständig ändernder Risiken und Regularien reicht es nicht mehr aus, Governance, Risk und Compliance (GRC) nur zu verwalten. Ein Wettbewerbsvorteil entsteht, wenn Unternehmen Risikoinformationen in konkrete Maßnahmen umsetzen und ihre Betriebseffizienz steigern können. Genau hier setzt MetricStream an. Der SaaS-Anbieter hebt sich durch einen durchgängig intelligenten und integrierten Plattform-Ansatz von der Konkurrenz ab.

Von der Analyse zur Aktion

Während viele Lösungen Daten sammeln, setzt MetricStream konsequent auf KI, um diese Daten in handlungsrelevante Erkenntnisse zu verwandeln. Die Alleinstellungsmerkmale liegen in der automatisierten, vorausschauenden Intelligenz „across the board":

- **Intelligente Risikoerkenntnisse:** MetricStream vereinfacht das Risikomanagement mit KI-gestützten Risikobewertungen und Kontrolltests. Die Plattform geht über die reine Datensammlung hinaus, indem sie Risikoexpositionen automatisch zusammenfasst und bewertet. Dies beschleunigt die Entscheidungsfindung durch eine intelligentere Risikoreaktion und ein effizienteres Problemmanagement.

- **Automatisierte Compliance:** Statt manueller Lückenanalysen sorgt ein KI-orientierter Ansatz für kontinuierliche Compliance. Die Software integriert regulatorische Updates automatisch, bildet das Compliance-Profil des Unternehmens ab, analysiert die Auswirkungen neuer Vorschriften und vereinfacht die gesamte Richtlinienverwaltung. So schließt sich die Lücke zwischen Vorgabe und Umsetzung nahezu in Echtzeit.

- **KI-gesteuerte Audits:** MetricStream transformiert die Interne Revision vom Prüfer zum proaktiven Berater. KI-gestützte Audits automatisieren die Prüfarbeit vor Ort, heben Kontrolllücken sofort hervor und erstellen automatisch Auditberichte. Das ermöglicht den Teams, sich voll auf die Behebung von Problemen zu konzentrieren, anstatt sich mit Papierkram aufzuhalten.

- **Proaktive Cyber-Resilienz:** Im Bereich Cyber-GRC identifiziert und bewertet die Lösung IT- und Cyberrisiken in Echtzeit. Unternehmen können so ein proaktives, intelligentes Cyber-Programm aufbauen, das kontinuierlich Kontrollen validiert, Sicherheitsrahmen einhält und Richtlinien durchsetzt.

- **Resiliente Lieferketten:** Das Third-Party Risk Management automatisiert Onboarding, Überwachung und KI-gestützte Bewertungen von Partnern. Unternehmen gewinnen Echtzeiteinblicke in ihr gesamtes Ökosystem und stärken so die Widerstandsfähigkeit ihrer Lieferkette effektiv.

Die Vorteile für Anwender

Durch diese KI-gestützte Integration erzielen Anwender einen fundamentalen Shift:

- **Proaktivität statt Reaktivität:** Risiken und Compliance-Lücken werden erkannt, bevor sie zu kritischen Problemen werden.

- **Massive Effizienzsteigerung:** Die Automatisierung manueller Tasks (Bewertungen, Reporting, regulatorisches Tracking) setzt wertvolle Ressourcen frei.

- **Fundierte Entscheidungen:** Echtzeit-Einblicke und konsolidierte Dashboards bieten die Basis für smarte, risikobewusste Entscheidungen auf allen Ebenen.

- **Nachweisbare Resilienz:** Geschäftskontinuität wird durch kontinuierliche Bewertungen und automatisierte Reaktionspläne sichergestellt.

MetricStream positioniert sich nicht einfach als eine weitere GRC-Software, sondern als eine intelligente Operations-Plattform für Resilienz und Effizienz. Für Unternehmen, die Risikomanagement als strategischen Hebel für Agilität und Wettbewerbsvorteil nutzen wollen, ist die Lösung eine überzeugende Option der Spitzenklasse.

https://www.metricstream.com

Ganzheitliche Sicherheitsstrategien

VOM VULNERABILITY MANAGEMENT ZUM EXPOSURE MANAGEMENT



EXPOSURE MANAGEMENT ERWEITERT DEN FOKUS AUF DIE GESAMTE ANGRIFFSOBERFLÄCHE EINES UNTERNEHMENS UND VERBINDET DIE DISZIPLINEN ON-PREM-IT, IDENTITY, OT, CLOUD UND KI.

Nils Rogmann, Head of Competence Center Security, Controlware GmbH, www.controlware.de

Leistungsstarkes Vulnerability Management ist ein tragender Eckpfeiler moderner IT-Sicherheitsstrategien: Es identifiziert und bewertet Schwachstellen in der klassischen IT – also in Servern, Netzwerken und Endpoints – und legt damit die Basis für deren Beseitigung. Doch in einer Welt, in der Angreifer zunehmend lateral denken und über Identitäten, Cloud-Workloads oder industrielle Steuerungen attackieren, geht dieser Ansatz nicht weit genug.

Vom Silo zur holistischen Perspektive

Die größte Schwäche des traditionellen Vulnerability Managements liegt in seinem begrenzten Blickfeld. Schwachstellen werden isoliert erfasst und priorisiert, ohne den Kontext zwischen den verschiedenen Bereichen – etwa zwischen On-Prem-Systemen und Cloud-Identitäten – herzustellen. Das führt dazu, dass Unternehmen zwar wissen, wo Schwachstellen liegen, aber nicht, welche davon wirklich gefährlich sind.



Genau hier setzt das Exposure Management an. Es erweitert den Fokus auf die gesamte Angriffsoberfläche eines Unternehmens und verbindet die Disziplinen On-Prem-IT, Identity, Operational Technology (OT), Cloud und Künstliche Intelligenz (KI). Entscheidend ist dabei der übergreifende Kontext: Erst wenn sichtbar wird, wie ein Angreifer sich von einer kompromittierten Identität über eine ungeschützte Cloud-Komponente bis zu einem kritischen OT-System bewegen könnte, lassen sich Risiken realistisch bewerten und priorisieren.

Sichtbarkeit, Kontext, Priorisierung

Exposure-Management-Plattformen und -Services unterstützen diesen Ansatz optimal: Dank lückenloser Sichtbarkeit über alle relevanten Ressourcen lassen sich Schwachstellen kontinuierlich erfassen und potenzielle Angriffspfade analysieren. Durch die Integration verschiedener Datenquellen – etwa von Asset-Datenbanken, Identity-Management-Systemen, OT-Monitoring und Cloud-Sicherheitsplattformen – entsteht ein einheitliches Lagebild der gesamten Infrastruktur.

Auf dieser Basis können Sicherheitsverantwortliche Risiken nicht nur erkennen, sondern auch im Kontext bewerten. Eine kritische Schwachstelle auf einem isolierten Testsystem hat eine ganz andere Relevanz als dieselbe Schwachstelle auf einem Server mit direktem Zugriff auf Produktionsdaten. Diese Kontextualisierung ermöglicht eine effiziente Priorisierung, und die begrenzten personellen Ressourcen im Security-Team werden gezielt dort eingesetzt, wo sie den größten Effekt erzielen.

Fazit: Von eingeschränkter zu ganzheitlicher Sichtbarkeit

Während klassisches Vulnerability Management in der Regel auf On-Prem-IT fokussiert ist, verfolgt Exposure Management einen ganzheitlichen Ansatz. Der hierdurch gewonnene Kontext erlaubt eine vollumfängliche Bewertung und kontinuierliche Reduzierung des tatsächlichen Risikos. Die Entwicklung vom Vulnerability zum Exposure Management ist kein optionaler Trend, sondern eine notwendige Evolution in der IT-Security. Spezialisierte IT-Dienstleister und Managed Service Provider unterstützen Unternehmen dabei, ihre Silos aufzubrechen und ganzheitliche Transparenz, Kontextualisierung und Priorisierung zu ermöglichen. Denn dies sind die neuen Schlüsselfaktoren moderner Cyber-Resilienz und das Fundament sicherer IT-Infrastrukturen.

Nils Rogmann



Schwachstellenmanagement neu denken

TRANSPARENZ ALS SECURITY-PRINZIP

Wenn es um Cybersicherheit geht, ist es für viele Organisationen schwer, im Spannungsfeld zwischen Schutz und Offenheit die richtigen Entscheidungen zu treffen. Dass Schwachstellen aus Angst vor Reputationsschäden oder Missbrauch möglichst lange unter Verschluss gehalten werden, mag verständlich sein – ist aber keine Lösung. In einer vernetzten Welt darf Schweigen nicht als Schutzschild dienen. Denn echte Sicherheit entsteht nur dann, wenn offen, nachvollziehbar und verantwortungsvoll mit Schwachstellen umgegangen wird.

Mitarbeiter ebenso wie Geschäftspartner erwarten keine absolute Fehlerfreiheit, sondern einen glaubwürdigen Umgang mit Risiken. Legen Unternehmen offen, welche Sicherheitslücken entdeckt, analysiert und behoben wurden, signalisieren sie Kontrolle und Verantwortungsbewusstsein. Darüber hinaus stellen sie klar, dass Transparenz kein Risiko, sondern ein Zeichen technischer Reife ist. So entsteht langfristiges Vertrauen – nicht durch Verschweigen von Problemen, sondern durch den professionellen Umgang mit ihnen.

Aufklärung statt Alarmismus

Transparente Sicherheitskommunikation bedeutet nicht, Panik zu verbreiten, sondern aufzuklären. Wichtig ist, nicht nur zu kommunizieren, dass es eine Schwachstelle gibt, sondern auch welche Systeme betroffen sind, wie hoch das reale Risiko ist und welche Gegenmaßnahmen ergriffen wurden. Eine klare, sachliche Sprache hilft dabei, Fehlinterpretationen zu vermeiden und Mitarbeiter und Kunden gleichermaßen zum richtigen Handeln zu befähigen. Diese Art der Aufklärung trägt wesentlich zur Security Awareness bei – denn nur wer versteht, kann richtig reagieren.

Transparenz bedeutet in diesem Kontext auch, den offenen Umgang mit Fehlern zu fördern, um ein Klima psychologischer Sicherheit zu etablieren, in dem Lernen und kontinuierliche Verbesserung im Vordergrund stehen. Unternehmen sollten dazu ermutigen, den versehentlichen Klick auf einen Phishing-Link, selbst zu melden und konsequent auf Transparenz in der Kommunikation sowie auf die vorrangige Behandlung von Sicherheitsfragen setzen.

Realistische Risikoeinschätzung statt Verharmlosung

Nicht jede Schwachstelle ist gleich kritisch. Eine angemessene Sicherheitskommunikation stellt klar, warum bestimmte Risiken als „niedrig", „mittel" oder „hoch" bewertet werden – und wie diese Einschätzung zustande kommt. Solche Transparenz schafft Verständnis dafür, dass Sicherheitsmanagement immer auch Priorisierung bedeutet. Sie verhindert Überreaktionen, gleichzeitig aber auch Gleichgültigkeit. Wer den Kontext kennt, kann die Bedrohungslage realistisch einschätzen.

Wo Entwickler, Sicherheitsbeauftragte, Kommunikation und Management gemeinsam offen über Schwachstellen sprechen, entsteht eine lernende Organisation. Diese Kultur des offenen Austauschs stärkt das Sicherheitsbewusstsein in allen Bereichen – vom Code bis zur Kundenkommunikation. So wird Security Awareness nicht als Pflichtschulung verstanden, sondern als gelebter Teil der Unternehmenskultur.

Fazit: Transparenz als Stärke statt als Risiko betrachten!

Eine offene Vulnerability-Berichterstattung zeigt nicht Schwäche, sondern Stärke. Sie steht für Verantwortungsbewusstsein, Lernbereitschaft und technische Exzellenz.

Eine Organisation, die Sicherheitslücken transparent behandelt, reduziert langfristig Risiken, stärkt das Vertrauen ihrer Stakeholder und schafft eine Kultur, in der Sicherheit nicht als Hemmnis, sondern als Qualitätsmerkmal verstanden wird.

Stefan Henke



TRANSPARENZ IN DER KOMMUNIKATION VON SCHWACHSTELLEN MUSS TEIL DER SECURITY-KULTUR WERDEN.

Stefan Henke, RVP DACH, Cloudflare, www.cloudflare.com

Vorbereitung auf die digitale Zukunft

HERAUSFORDERUNGEN DER POST-QUANTEN-KRYPTOGRAFIE UND EINFÜHRUNG IN UNTERNEHMEN

Seit einigen Jahren erhält ein Szenario in der Cybersicherheit zunehmende Aufmerksamkeit: Böswillige Akteure würden bereits heute verschlüsselte Daten mit dem Ziel sammeln, sie zu einem späteren Zeitpunkt zu entschlüsseln, wenn Quantencomputer über ausreichende Rechenleistung verfügen. Dieser Ansatz, bekannt als „harvest now, decrypt later", basiert auf einer einfachen Annahme: Was heute unlesbar ist, könnte morgen transparent werden.

Um dieser latenten Bedrohung zu begegnen, ist die Post-Quanten-Kryptografie (PQC) zu einer Priorität geworden. Sie umfasst alle kryptografischen Methoden, die entwickelt wurden, um den beispiellosen Fähigkeiten des Quantencomputings standzuhalten. Dazu gehört insbesondere die Post-Quanten-Verschlüsselung, die sich auf den Schutz der Vertraulichkeit von Daten durch geeignete Verschlüsselungsalgorithmen konzentriert. Laut einer von der ANSSI veröffentlichten Studie sind 50 Prozent der befragten Organisationen den Risiken künftiger Quantenangriffe ausgesetzt, insbesondere im Zusammenhang mit der Nutzung von VPNs oder langfristigen Zertifikaten. Die französische Cybersicherheitsbehörde fordert die Nutzer postquantenfähiger Lösungen auf, ihre Migration so bald wie möglich vorzubereiten.



DIE POST-QUANTEN-VERSCHLÜSSELUNG FINDET ÜBERALL DORT ANWENDUNG, WO KRYPTOGRAFIE BEREITS UNVERZICHTBAR IST.

Marine Goninet, New Offering & EU Strategy Coordinator, Stormshield, www.stormshield.com

Prinzipien und Ziele der Post-Quanten-Verschlüsselung

Die Post-Quanten-Verschlüsselung bezieht sich auf eine Reihe neuer kryptografischer Algorithmen, die so konzipiert sind, dass sie der Rechenleistung zukünftiger Quantencomputer standhalten. Im Gegensatz zu aktuellen Technologien, die häufig auf mathematischen Problemen beruhen, deren Lösung für herkömmliche Computer Jahre dauern würde, sind diese neuen Ansätze so ausgelegt, dass sie robust bleiben – selbst wenn Maschinen die Gesetze der Quantenphysik nutzen, um gleichzeitig eine große Zahl möglicher Lösungen zu prüfen. Wesentlich ist, dass diese Verschlüsselung mit unserer aktuellen Hardware kompatibel ist, was bedeutet, dass sie schrittweise eingeführt werden kann, ohne auf das tatsächliche Erscheinen von Quantencomputern warten zu müssen.

Die Post-Quanten-Verschlüsselung findet überall dort Anwendung, wo Kryptografie bereits unverzichtbar ist: sichere Kommunikation, Finanztransaktionen, Cloud-Speicherung, kritische Infrastrukturen oder vernetzte Geräte. Bestimmte Branchen müssen diesem Übergang jedoch besondere Aufmerksamkeit widmen. Der Bankensektor stützt sich zum Beispiel stark auf die Sicherheit des Zahlungsverkehrs und den Schutz sensibler Kundendaten. Ebenso kann es sich das Gesundheitswesen, wo die Sicherheit von Patientendaten und professioneller Kommunikation entscheidend ist, nicht leisten, in dieser Transformation zurückzubleiben. Für diese Sektoren ist die Antizipation der Quantenbedrohung keine Option, sondern eine strategische Notwendigkeit – insbesondere im Hinblick auf die gesetzlich vorgesehene Zeitspanne, in der Daten vertraulich bleiben müssen.

Fortschritte der Post-Quanten-Kryptografie

Die Standardisierung der Post-Quanten-Kryptografie ist ein laufender Prozess, der hauptsächlich vom NIST (National Institute of Standards and Technology) gesteuert wird. Ziel ist es, Algorithmen zu validieren, die robust, leistungsfähig und sicher gegenüber den Bedrohungen künftiger Quanten-



computer sind. Über die Auswahl sicherer Algorithmen hinaus umfasst diese Standardisierung auch die Definition von Best Practices für deren Implementierung, um Fallstricke im praktischen Einsatz zu vermeiden.

Technologisch treten zwei Schlüsselkonzepte hervor: Hybridisierung und Crypto-Agility. Hybridisierung bedeutet, herkömmliche Algorithmen mit postquantenfähigen Algorithmen zu kombinieren, um den Übergang abzusichern – als Überbrückung der Zeit, die für langfristige Tests der Robustheit der neuen Algorithmen benötigt wird. Crypto-Agility bezeichnet unter anderem die Fähigkeit eines Systems, bei Identifizierung einer Schwachstelle schnell den Algorithmus zu wechseln. Da beide Konzepte für die Begleitung des Übergangs zur PQC entscheidend sind, werden sie je nach Anwendungsbereich standardisiert oder in Empfehlungen aufgenommen.

Gleichzeitig unterscheidet sich der Reifegrad der Akteure. Auf Anbieterseite ist eine gewisse Mobilisierung zu beobachten: Viele folgen aktiv den aktuellen Empfehlungen und integrieren die neuen Standards sukzessiv in ihre Produkte. Auf Anwenderseite hingegen zeigt sich ein gemischtes Bild: Einige Branchen warten auf klare Richtlinien, während andere, die besonders sicherheitssensibel sind, die kommenden Veränderungen bereits vorwegnehmen.

Die Rolle europäischer Behörden

In Frankreich spielt die ANSSI eine zentrale Rolle bei der Sensibilisierung für die Bedrohung, die das Quantencomputing für bestehende kryptografische Systeme darstellt. Neben technischen Empfehlungen rät die Behörde gemeinsam mit ihren europäischen Partnern, Kosten, Zeitpläne und Komplexität der Migration zur PQC frühzeitig zu antizipieren, um einen übereilten und riskanten Übergang zu vermeiden.

Ebenso wichtig ist ihre Mitwirkung an internationalen Standardisierungsarbeiten, um sicherzustellen, dass zukünftige globale Standards sicherheitsrelevante Anforderungen im europäischen Kontext berücksichtigen und die gewählten Lösungen technisch wie operativ mit lokalen Vorgaben kompatibel sind.

Auf regulatorischer Ebene sind die Grundlagen für diesen Übergang bereits gelegt. In Europa beispielsweise wird der Cyber Resilience Act (CRA) Lieferanten verpflichten, strenge Anforderungen einzuhalten – einschließlich der Einhaltung von State-of-the-Art-Kriterien in der Kryptografie – mit Bewertungen, die je nach Kritikalität der Lösungen geplant sind. Auf europäische Ebene verweisen zudem mehrere Gesetze bereits auf kryptografische Pflichten: Sensible Nutzer wie bestimmte Verwaltungen oder Betreiber müssen weiterhin sicherstellen, dass ihre Systeme modernste Technik integrieren. Je nach Bedarf sollten auch nicht sensible Nutzer, die nicht denselben Verpflichtungen unterliegen, darauf achten, dass ihre Anbieter Lösungen offerieren, die den Standards der Post-Quanten-Kryptografie entsprechen.

Mit der Entwicklung der Quantentechnologien wird die Implementierung der Post-Quanten-Kryptografie zu einer wesentlichen Herausforderung für die Sicherheit von Informationssystemen. Dieser Übergang erfordert eine schrittweise Anpassung der Infrastrukturen und die Koordination zwischen den verschiedenen Akteuren dieser Industrie. Über die technischen Aspekte hinaus wirft er auch organisatorische und strategische Fragen auf, die angegangen werden müssen, um eine wirksame Umsetzung zu gewährleisten.

Marine Goninet

KI OHNE GOVERNANCE-KONZEPT?

ALARMIERENDE SICHERHEITSLÜCKEN

Während Unternehmen Millionen in Künstliche Intelligenz (KI) investieren, fehlen elementare Sicherheitskonzepte und Kontrollmechanismen. Eine neue Studie der internationalen Normierungsorganisation BSI (British Standards Institution) zeigt: Die Wirtschaft jagt Produktivitätsgewinnen und Kostensenkungen hinterher, ohne die Risiken im Griff zu haben – und steuert damit auf massive Probleme zu.

Die globale Studie wertet über 100 Geschäftsberichte multinationaler Konzerne aus und stützt sich auf zwei weltweite Befragungen von mehr als 850 Führungskräften im Abstand von sechs Monaten. Das Ergebnis: Eine gefährliche Kluft zwischen öffentlichen Versprechen und tatsächlicher Umsetzung.

Fehlendes Sicherheitskonzept

So wollen beispielsweise 61 Prozent der deutschen Führungskräfte ihre KI-Investitionen im kommenden Jahr erhöhen. Die Gründe: höhere Produktivität (62 %) und niedrigere Kosten (52 %). Zwei Drittel (66 %) sehen KI sogar als unverzichtbar für ihr Wachstum.

Die Kehrseite: Nur jedes vierte deutsche Unternehmen (25 %) hat überhaupt ein KI-Sicherheitskonzept. Selbst bei Großkonzernen ist es nur jedes zweite (50 %). Besonders kritisch ist der Umgang mit Daten: Nur 31 Prozent der Führungskräfte wissen, mit welchen Daten ihre KI-Systeme trainiert werden.

Risiken werden ignoriert

30 Prozent der Befragten sehen KI bereits als Schwachstelle ihres Unternehmens. Trotzdem haben nur 34 Prozent Standards für neue KI-Tools. Nur gut die Hälfte (58 %) bezieht KI-Risiken in ihre Compliance ein. Formale Risikoprüfungen führen sogar nur 38 Prozent durch.

Was passiert bei KI-Pannen? Die meisten Unternehmen wissen es nicht. Nur 42 Prozent dokumentieren Probleme systematisch. Nur 30 Prozent haben Notfallpläne. Jedes zehnte Unternehmen könnte ohne KI-Tools gar nicht mehr arbeiten.

Gleichzeitig verschlingen KI-Projekte Ressourcen: 35 Prozent der Befragten mussten andere Vorhaben dafür opfern. Trotzdem verhindern nur 25 Prozent teure Doppelentwicklungen zwischen Abteilungen.

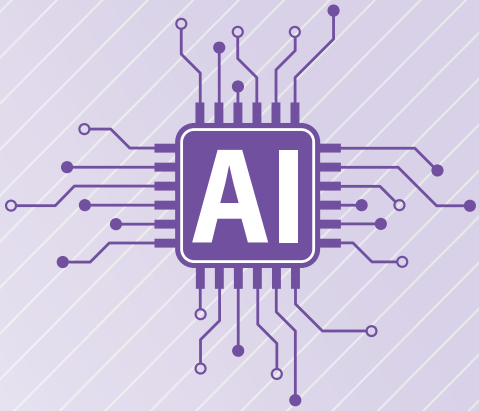
www.bsigroup.com

MEHR WERT

Trust in AI: Grounded in Governance

IMPLEMENTIERTE SICHERHEITSMASSNAHMEN





Die Eroberung der Unternehmens-KI

KI-AGENTEN IM AUFWIND

Der World AI Appreciation Day bietet Gelegenheit, darüber nachzudenken, wie weit die KI in den letzten Jahren gekommen ist. Denn es geht nicht mehr um experimentelle Anwendungsfälle.

Unternehmen treiben die KI-Nutzung voran, müssen sich aber auch der wachsenden Gefahr von Ungenauigkeiten und Verzerrungen bewusst sein. In Szenarien, insbesondere in sensiblen Bereichen wie Audits, Personalbeschaffung und Preisgestaltung, muss die menschliche Belegschaft weiterhin für die Handlungen ihrer KI-Agenten verantwortlich sein.

In diesem Jahr erleben wir einen explosionsartigen Anstieg des Interesses an KI-Agenten. Endnutzer und Unternehmen sind gleichermaßen begeistert davon, die Vorteile der KI in ihre täglichen Aufgaben zu integrieren. Wir beobachten, wie sich die digitale Transformation zu einer agentenbasierten Transformation wandelt. Und einige Unternehmen florieren.

Was folgt, ist ein Muster, das wir bereits kennen. Unternehmen, die einen Plattformansatz für die Verwaltung ihrer Datenpipelines, Sicherheit und Governance für alle digitalen Assets, einschließlich APIs, verfolgen, sind besser in der Lage, vertrauenswürdige Daten zu identifizieren und zu nutzen, die als Grundlage für ihre KI-Frameworks dienen. Und sie sehen echte Ergebnisse. Diese Unternehmen sind besser in der Lage, Erkenntnisse zu gewinnen, die alle ihre kritischen Anwendungsökosysteme umfassen – sie haben begonnen, das Potenzial ihrer vernetzten Daten auszuschöpfen.

Unternehmen mit Low-Code-Plattformen können auch ihre eigenen Agenten orchestrieren und dabei ganz einfach die erforderlichen Sicherheitsvorkehrungen einbauen, da sie wissen, dass Änderungen über die Low-Code-Plattform schnell und transparent vorgenommen werden können. Durch die Anwendung von Governance über die von den Agenten verwendeten Tools (z. B. APIs) sowie die Überwachung der Agenten selbst gewinnen sie das nötige Vertrauen, um in einer Welt voranzukommen, die sicherlich noch einige Überraschungen bereithält.

GenAI im Wandel

Allein im letzten Jahr haben wir einige unglaubliche Fortschritte bei GenAI gesehen – von verbesserten LLMs über eine stärkere Fokussierung auf Protokolle (MCP, A2A, ACN, ACP) bis hin zu Verbesserungen bei den Inferenzmethoden und einer noch stärkeren Demokratisierung von GenAI durch die Verbreitung von Open-Source-Modellen. KI/GenAI wird sich in immer kürzeren Innovationszyklen weiterentwickeln, die Datenmengen werden exponentiell zunehmen und neue Formen von Cyberangriffen werden auftauchen. Die Nutzung der Leistungsfähigkeit von GenAI und der damit verbundenen Wettbewerbsvorteile liegt im Schutz von Unternehmensdaten und automatisierten Prozessen durch ein Governance-Framework, das bereits bei der Integration ansetzt.

Fazit

Die Förderung des Einsatzes von KI in allen Geschäftsbereichen wird immer wichtiger, und noch nie war es so wichtig, verantwortungsbewusste KI, Datensicherheit und Governance in allen Bereichen zu berücksichtigen.

Da sich die Technologielandschaft ständig weiterentwickelt, kann der Aufbau von composable KI-Agenten, also modularen, flexiblen KI Systemen, eine schnelle Implementierung ermöglichen, ohne dass man sich auf ein Modell oder Framework festlegen muss.

Ann Maya



NOCH NIE WAR ES SO WICHTIG, VERANTWORTUNGSBEWUSSTE KI, DATENSICHERHEIT UND GOVERNANCE IN ALLEN BEREICHEN ZU BERÜCKSICHTIGEN.

Ann Maya,
EMEA CTO, Boomi, www.boomi.com

Cyber-Resilience

WIE DRIVELOCK UND IDGARD EUROPAS DIGITALE SOUVERÄNITÄT STÄRKEN

DriveLock zählt zu den führenden deutschen Anbietern für Endpoint- und Datensicherheit. Mit der Übernahme der idgard GmbH stärkt das Unternehmen seine strategische Position im Bereich digitaler Souveränität. Gemeinsam verfolgen DriveLock und idgard das Ziel, eine europäische Sicherheitsplattform zu etablieren, die Unternehmen, Verwaltungen und kritische Infrastrukturen gleichermaßen schützt – vom Endpoint bis zur sicheren Cloud. Im Interview erläutert Arved Graf von Stackelberg, CEO beider Unternehmen, wie sich Cyber-Resilienz ganzheitlich denken lässt und warum Europa jetzt handeln muss.

it security: *Herr Graf von Stackelberg, Europa spricht viel über digitale Souveränität. Doch zwischen Anspruch und Wirklichkeit klafft oft eine Lücke. Woran liegt das?*

Arved Stackelberg: Europa fehlt eine gemeinsame Architektur. Wir haben viele hervorragende Einzellösungen. Aber echte Resilienz entsteht erst, wenn Endgeräte, Daten und Prozesse zusammenspielen. Gleichzeitig zeigt sich: Es reicht nicht aus, Angriffe lediglich zu erkennen. Das funktioniert in Zeiten von KI auch gar nicht mehr ohne weiteres. Unser Ansatz bei DriveLock ist daher, Angriffe von vornherein zu blockieren, und zwar unabhängig davon, ob sie erkannt werden oder nicht.

it security: *Und wie genau kann das funktionieren?*

Arved Stackelberg: DriveLock setzt auf zwei zentrale Bausteine, mit denen wir Angriffe präventiv verhindern: Application Control und Device Control.

Stellen Sie sich Application Control wie die Gäste-Liste eines Clubs vor. Wer darauf steht, darf rein – in unserem Fall dürfen nur Anwendungen auf der Allow-Liste ausgeführt werden. So bieten wir maximalen Schutz vor Mal- und Ransomware. Das intelligente Allow-Listing von DriveLock minimiert den Pflegeaufwand dieser Listen und verhindert durch automatisiertes Lernen die Implementierung und Ausführung unbekannter Anwendungen. So wird verdächtiger Code gar nicht erst aktiv.

Der zweite Baustein unserer Schutzstrategie ist Device Control, also die Kontrolle von Wechseldatenträgern wie USB-Sticks oder externen Festplatten. Diese können Einfallstore für Malware-Angriffe und Datenabfluss sein. Wir definieren deshalb exakt, wer wann welche Geräte wie nutzen darf. Alles andere wird schlichtweg nicht ausgeführt. Damit kommt Schadsoftware nicht hinein und sensible Daten nicht unkontrolliert hinaus.

it security: *Sind Unternehmen damit schon ausreichend geschützt oder fehlt noch eine weitere Ebene der Sicherheit?*

Arved Stackelberg: Nein. Für echte Cyber-Resilienz reicht es nicht, einzelne Angriffe abzuwehren. Auch Informationen und Daten müssen geschützt werden. Deshalb haben wir mit der Akquise der idgard GmbH das DriveLock Lösungsportfolio strategisch erweitert. Unser Ziel ist, Organisationen das Recht und die Kontrolle über die eigenen Daten zu geben und sie nicht in fremde Hände zu legen. Wir stehen seit Jahren für Endpoint- und Geräteschutz. Mit idgard ergänzen wir diese Sicherheitsarchitektur um die Datenebene.

Unternehmen können sensible Informationen an einem geschützten Ort ultrasicher und kontrollierbar speichern und sie gezielt für Partner oder Behörden freigeben. Jeder Zugriff ist dokumentiert, jede Datenbewegung nachvollziehbar. Dank Konzepten wie Shared Links ist dabei jedes Unternehmen automatisch DSGVO-konform. So wird Datenschutz zum integralen Bestandteil der Infrastruktur, nicht zur nachgelagerten Pflicht.

Die technische Basis bildet die Sealed Cloud von idgard. Die patentierte Technologie stellt sicher, dass Daten während des Transports und im Speicher verschlüsselt bleiben, während sie in einem abgeschotteten Bereich verarbeitet werden können. Außer den berech-



CYBER-RESILIENZ IST LÄNGST KEINE REIN TECHNISCHE FRAGE MEHR, SONDERN EINE POLITISCHE UND GESELLSCHAFTLICHE AUFGABE.

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



tigten Personen hat niemand Zugriff, selbst wir als Betreiber nicht. Wir planen damit künftig auch KI-Anwendungen sicher integrierbar zu machen, etwa in der Medizin, Industrie oder Verteidigung, wo hochsensible Informationen für Forschung oder Analyse genutzt werden können, ohne dass sie die geschützte Umgebung verlassen.

it security: *Wie zahlt die Verbindung von DriveLock und idgard auf das Ziel ein, Europa digital unabhängiger zu machen?*

Arved Stackelberg: Mit der Integration entsteht eine durchgängige Sicherheitsarchitektur vom Endgerät bis zur Cloud. Sie bildet das Fundament für eine europäische Plattform, die Unternehmen und Behörden souveräne IT- und Datensicherheit bietet. Bisher haben wir den Endpoint so abgesichert, dass unsere Kunden darauf ihre Cloud-Strategie aufbauen können. Mit idgard erweitern wir dieses Fundament um die sichere Plattform in der Cloud, über die sich Daten mit Dritten geschützt und DSGVO-konform teilen lassen. Künftig wollen wir die Technologie so weiterentwickeln, dass idgard Unternehmen die einzigartige Möglichkeit eröffnet, ihre Daten auch sicher für KI-Anwendungen zu nutzen. So können sie etwa Informationen anreichern oder KI-Modelle trainieren, ohne dass sie die geschützte Umgebung verlassen. idgard wird damit weltweit die einzige Lösung sein, die Unternehmen die Arbeit mit KI und sensibelsten Daten ermöglicht, ohne Kompromisse bei Datenhoheit und Souveränität.

Die DriveLock HYPERSECURE Platform erweitern wir kontinuierlich um Partnerlösungen aus Deutschland und Europa, die unsere hohen Sicherheits- und Souveränitätsstandards teilen. Denn kein Hersteller kann alles allein abdecken. So entsteht Schritt für Schritt ein europäisches Sicherheitsökosystem – vergleichbar mit einem kuratierten App-Store für Sicherheit: geprüft, zertifiziert und vollständig in Europa betrieben.

it security: *Welches Ziel verfolgen Sie damit konkret?*

Arved Stackelberg: Wir schaffen im Kontext der Endgeräte- und Datensicherheit digitale Souveränität für Organisationen – von Unternehmen über Verwaltungen bis hin zu kritischen Infrastrukturen und ganzen staatlichen Strukturen. Politik und Investoren unterstützen diesen Weg ausdrücklich, weil gerade in KRITIS-Einrichtungen und Verteidigungsorganen ein Ausfall oder Datenleck die nationale Sicherheit und das Vertrauen der Bevölkerung unmittelbar gefährden kann.

it security: *Warum ist es so wichtig, digitale Souveränität gerade jetzt aufzubauen?*

Arved Stackelberg: Europa muss sich wappnen. Russlands Angriff auf die Ukraine zeigt, wie schnell sich die geopolitische Lage zuspitzen kann. Ich rechne nicht mit einem physischen Angriff auf Deutschland, wohl aber mit koordinierten Cyberangriffen, etwa auf Randbereiche wie das Baltikum oder andere exponierte Regionen. NATO- und Sicherheitsexperten erwarten seit Jahren gezielt koordinierte Cyberattacken. Genau darauf müssen wir uns vorbereiten. Deshalb bauen wir die Plattform so aus, dass Deutschland und Europa bis 2028 gegen Cyberangriffe widerstandsfähig sind und andererseits auch unabhängiger von ausländischen Clouds agieren können. idgard spielt dabei eine zentrale Rolle. Die Lösung ist nicht nur ein weiterer technologischer Baustein, sondern ein Beweis dafür, dass Europa leistungsfähige, souveräne Cloud- und Datendienste entwickeln kann. Die Sealed-Cloud-Technologie geht weit über klassische Verschlüsselung hinaus. Sie trennt den Datenzugriff physisch und logisch. Selbst der Betreiber hat keine Einsicht. Damit schafft sie das Fundament, auf dem Unternehmen ihre sensibelsten Informationen sicher in Europa speichern und verarbeiten können.

Souveränität bedeutet genau das: Handlungsfähig zu sein und zu bleiben. Deshalb müssen Technologien in Europa entwickelt, betrieben und kontrolliert werden. Mit Lösungen wie idgard können wir Daten-Souveränität sichern. Digitale Sicherheit in Europa ist kein Versprechen, sondern Realität, wenn sensible Daten hier gespeichert, verarbeitet und geschützt werden.

Cyber-Resilienz ist längst keine rein technische Frage mehr, sondern eine politische und gesellschaftliche Aufgabe. Wir unterstützen sie mit einer gemeinsamen Plattform, die Daten, Prozesse und Schutzmechanismen in Europa vereint – für Resilienz made in Europe.

it security: *Herr Graf von Stackelberg, vielen Dank für dieses ausführliche Gespräch.*



GEHACKTES E-MAIL-KONTO

CHECKLISTE FÜR DEN ERNSTFALL

Fast jede zehnte Person, die im Vorjahr von Cyberkriminalität betroffen war, erlebte laut Cybersicherheitsmonitor 2025 einen Fremdzugriff auf einen Online-Account (8 %). Insbesondere ein kompromittiertes E-Mail-Konto kann dabei gravierende Folgen haben. Um Verbraucherinnen und Verbraucher im Ernstfall gezielt zu unterstützen, veröffentlichen das Bundesamt für Sicherheit in der Informationstechnik (BSI) und das Programm Polizeiliche Kriminalprävention der Länder und des Bundes (ProPK) eine gemeinsame Checkliste. Diese beschreibt Schritt für Schritt das Vorgehen im Ernstfall und gibt zugleich Tipps zur Prävention.

MEHR WERT
Checkliste BSI

Die Checkliste ist kostenfrei auf den Webseiten von BSI und ProPK verfügbar.

Risiko- und Compliance-Management ist machbar

VON MANUELLEN PROZESSEN ZUR KI-GESTÜTZTEN AUTOMATION – GRANULAR UND IN ECHTZEIT



UM MODERNE RANSOMWARE-ANGRIFFE EFFEKTIV ZU ENTSCHÄRFEN, SIND NEUE ANSÄTZE ERFORDERLICH.

Jörg von der Heydt, Regional Director DACH, Bitdefender, www.bitdefender.de

Das Problem heißt Komplexität – auch und besonders in der Cybersicherheit: Zum einen ist die eigene IT-Infrastruktur zunehmend heterogen, zum anderen sind intelligentere und weitreichende Angriffe selbst für moderne Security-Lösungen kaum noch zu erkennen. Zudem haben IT-Sicherheitsteams noch andere Aufgaben: Sie sollen digitale Prozesse schützen, Regelkonformität gewährleisten sowie das Unternehmenswachstum unterstützen. Sicherheitsverantwortliche benötigen KI-basierte Technologien, um der Menge und der Komplexität der an sie gestellten Aufgaben Herr zu werden.

In modernen IT-Architekturen mangelt es oft an aussagekräftiger Transparenz über das reale Gefahrenpotential und das Risiko für das Unternehmen. Häufig fehlen leistungsfähige und integrierte IT-Sicherheitsplattformen, da vielerorts isolierten und spezialisierten Nischen-Tools der Vorzug gegeben werden. Dieser Flickenteppich führt zu Fehlkonfigurationen und falschen Interpretation von Daten und Vorfällen. Zudem sind in Unternehmen meist mehrere Akteure parallel für IT-Security-, Compliance- und Risiko-Management zuständig. Prozesse werden dadurch trotz zunehmenden Fachkräftemangel doppelt betreut.

CISOs benötigen eine Cyber-Security-Umgebung, die bestenfalls umfassende Funktionalitäten zur Bewältigung der vielschichtigen Anforderungen bereitstellt:

#1 einen Überblick über den aktuellen Risiko-Status – dynamisch, einheitlich und in Echtzeit;

#2 Sicherheits-Mechanismen, die konkrete Risiken und potenzielle Gefahren selbstständig und dynamisch identifizieren und Policies sowie System-Härtung automatisiert anpassen; sowie

#3 Compliance-Mechanismen, die sowohl Audit-konforme Berichte für alle essenziellen Standards zur Verfügung stellen als auch helfen, unzulängliche Compliance effizient zu korrigieren.

Künstliche Intelligenz liefert direkt umsetzbare Vorschläge, um Risiken, die sich aus betriebssystemnahen Applikationen und deren userbasierter Nutzerverhalten ergeben, zu erkennen und Sicherheitsrichtlinien dynamisch und selbstständig anzupassen. Solche Lösungen entfalten ihre Wirksamkeit sowohl als integrierter Bestandteil einer XDR-Plattform, als auch als eigenständige Ergänzung zu 3rd-Party-XDR-Systemen.

Das „Ende" von Ransomware

Um moderne Ransomware-Angriffe effektiv zu entschärfen, sind neue Ansätze erforderlich. Da sich via legitimer, betriebssystemnaher Applikationen und Services selbst vorhandene EDR-Agenten einfrieren lassen, braucht es neue Abwehrtechnologien. Hunderte von Apps, die auf jedem Windows-Endgerät vorhanden, aber nur von wenigen Usern benötigt werden, stellen eine immense Angriffsfläche dar.

KI kann effektiv unterstützen und die Angriffsfläche um bis zu 95 Prozent reduzieren: Die Nutzung sogenannter Living-Off-The-Land-(LOTL) Apps wird pro User kontinuierlich analysiert – und angepasst. Dabei werden diese Apps nicht nur blockiert, sondern deren Nutzung auf die notwendigen und unkritischen Befehle reduziert. All dies erfolgt automatisch und dynamisch. Auch Änderungen von User-Rollen werden so laufend berücksichtigt. Unverzichtbar bleiben die Kompetenz und Erfahrungen externer IT-Sicherheitsexperten mit aktuellem Wissen zur regionalen und branchenspezifischen Gefahrenlage. Erst damit können Sicherheits-, Risiko- und Compliance-Management unabhängig von Branchenzugehörigkeit und Unternehmensgröße ihre Aufgaben für Cybersicherheit erfüllen.

Jörg von der Heydt



KI am Edge

TECHNOLOGISCHER FORTSCHRITT IM AUSSENDIENST

Ob in der Versorgungsindustrie, in der Fertigung oder bei Polizei- und Verteidigungskräften, der Bedarf, größere Datenmengen vor Ort zu erfassen, zu analysieren und in verwertbare Informationen umzuwandeln, wächst stetig. Bisher nutzten mobile Fachkräfte häufig Cloud-Services, deren Verfügbarkeit von Netzwerkanbindung und Sicherheitsaspekten abhängig ist.

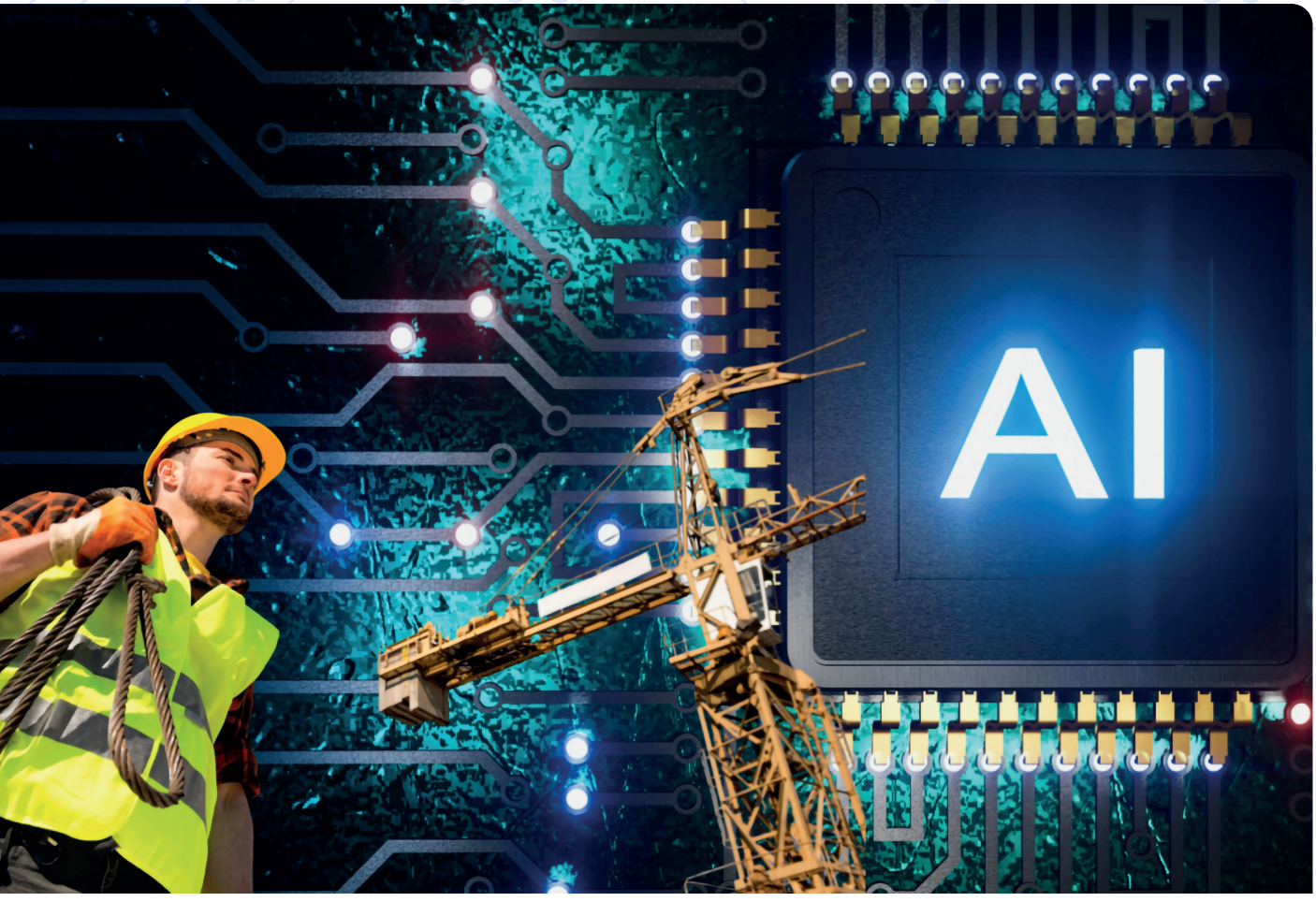
Mit dem TOUGHBOOK 40 und TOUGHBOOK G2 integriert Panasonic KI-Funktionen direkt in die Geräte, die unabhängig von Cloud-Verbindungen und Netzwerkverfügbarkeiten arbeiten.

Möglich ist dies durch die KI-fähigen Intel-Prozessoren, die mit einer dedizierten Neural Processing Unit (NPU) ausgestattet sind. Diese wurde speziell für den Einsatz von KI-Anwendungen entwickelt und ermöglicht lokale Echtzeit-Datenanalysen am Rande des Netzwerks. So können Fachkräfte im Außendienst komplexe Daten sofort verarbeiten und schnelle Entscheidungen basierend auf Echtzeitinformationen treffen.



Sichere KI-Lösungen am Edge

Die Entwicklung immer ausgefeilterer Datenmodelle als Basis für KI-Lösungen führt dazu, dass die Datenmenge, die mobilen Außendienstmitarbeitern zur Verfügung steht, sprunghaft ansteigt. Die Edge-Verarbeitung auf den beiden



neuen TOUGHBOOK Modellen unterstützt mobile Fachkräfte dabei, diese großen Datenmengen optimal und mit einem sicheren Zugriff direkt vor Ort zu nutzen. Dabei behalten Nutzer jederzeit die volle Kontrolle: Statt sie in die Cloud hochzuladen, verarbeitet die KI die Daten direkt auf dem Gerät, ohne Abhängigkeit von externen Rechenzentren. Dies schützt zum einen geistiges Eigentum und sensible Unternehmensinformationen. Zum anderen entfallen durch die Edge-Verarbeitung auch die Latenzzeiten, die beim Übertragen großer Datenmengen entstehen können. Mitarbeiter im mobilen Außendienst sind deshalb in der Lage, sicherer, schneller und zuverlässiger zu arbeiten.

Mehr Effizienz und Produktivität durch KI

Die Integration von KI in die TOUGHBOOK Serie markiert einen Wendepunkt für die mobile Arbeitswelt: Unternehmen erhalten nicht nur leistungsstarke Geräte, sondern auch die Möglichkeit, die Arbeit ihrer Außendienstteams neu zu definieren. Ob auf entlegenen Baustellen, in Produktionshallen mit eingeschränktem Zugang zum Netz oder bei Einsätzen in sicherheitskritischen Umgebungen: KI-gestützte Anwendungen im Außendienst können in Echtzeit Analysen erstellen, Dokumentationen automatisieren oder bei Sicherheitsaufgaben unterstützen. Auch Schulungsszenarien lassen sich optimieren: KI kann Wissenslücken im Unternehmen identifizieren und maßgeschneiderte Trainings entwickeln.

Gerade in Zeiten, in denen mobile Fachkräfte in herausfordernden Umgebungen mit weniger Ressourcen immer mehr leisten müssen, stellt KI auf diese Weise Produktivität, Autonomie und Effizienz sicher: Durch Automatisierung werden mobile Mitarbeiter innerhalb der nächsten zehn Jahre den Fokus weg von manuellen Routineaufgaben hin zu den Aufgaben verlagern können, die menschliches Eingreifen tatsächlich weiterhin erfordern. Dies wird die Art und Weise verändern, wie Außendienstmitarbeiter mit Technologie, Kunden und ihrer Umgebung interagieren.



DAS PANASONIC TOUGHBOOK ERMÖGLICHT ES UNTERNEHMEN, DEN TECHNOLOGISCHEN FORTSCHRITT IM MOBILEN AUSSENDIENST SICHER UND PRAXISNAH ZU NUTZEN.

Jonathan Tucker, Head of Product and Servie Solution Center, Panasonic Toughbook, https://eu.connect.panasonic.com

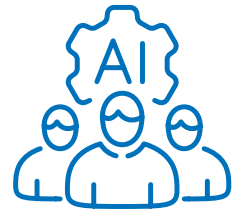
Den Einsatz von Technologie vereinfachen

In den kommenden fünf bis zehn Jahren wird Außendienstmitarbeitern eine nie dagewesene Vielzahl an technologischen Lösungen zur Verfügung stehen. Die Herausforderung besteht nun darin, das Potenzial von KI zu nutzen, um den Einsatz solcher Technologien zu vereinfachen. So werden beispielsweise Touchscreen-Displays in Fahrzeugen schon heute oft durch Head-up-Displays ergänzt, die Fahrern wichtige Informationen liefern, ohne dass sie den Blick von der Straße abwenden müssen. Die Frage ist nun, wie KI oder Sprachsteuerung ihnen dabei helfen kann, die Informationen während der Fahrt nicht nur wahrzunehmen, sondern unmittelbar und vor allem sicher auf sie zu reagieren. Erkennen mobile Mitarbeiter diese Vorteile der KI, wird das den Einsatz von KI-Funktionen noch schneller vorantreiben.

„KI hat inzwischen einen Reifegrad erreicht, dank dem Unternehmen beim Einsatz von KI-Tools einen entscheidenden Unterschied in Bezug auf Arbeitsweisen und Produktivität spüren können. Und das bereits zu einem Zeitpunkt, an dem wir immer noch am Anfang einer langfristigen Entwicklung stehen. In den nächsten Jahren wird sich KI von einem unterstützenden Werkzeug zu einem echten Entscheidungspartner entwickeln. Während heute noch die Assistenzfunktion im Vordergrund steht, wird KI bald unabhängig von der Netzwerkumgebung zunehmend in der Lage sein, komplexe Muster zu erkennen, Vorhersagen zu treffen und konkrete Handlungsempfehlungen auf Basis riesiger Datenmengen zu geben – etwa in der Industrie 4.0. Für Unternehmen kann dies den entscheidenden Unterschied im Wettbewerb machen", sagt Jon Tucker, Head of Product and Service and Solution Centre bei Panasonic TOUGHBOOK.

Panasonic TOUGHBOOK stellt für den Einsatz von KI-Funktionen auf mobilen Geräten zusätzlich Support-Services und Sicherheitskonzepte bereit. Ziel ist die Unterstützung von Unternehmen bei der Digitalisierung mobiler Arbeitsprozesse – von der Automatisierung wiederkehrender Tätigkeiten über datengestützte Analysen bis zur vernetzten Zusammenarbeit.

https://toughbook.de



Sicherheitsbedenken und Unsicherheiten

KI-EINSATZ BEI IT-DIENSTLEISTERN

Künstliche Intelligenz hat sich bei deutschen IT-Dienstleistern fest etabliert: Sie nutzen die Technologie nicht nur intern, sondern bieten zunehmend KI-basierte Lösungen für ihre Kunden an. Das zeigt die aktuelle, repräsentative Hiscox IT-Umfrage 2025. Während KI-Projekte die Auftragsbücher füllen, dämpfen Unsicherheiten rund um Datensicherheit, rechtliche Rahmenbedingungen und Versicherungsschutz die Aufbruchstimmung in der Branche. IT-Profis sehen dringenden Handlungsbedarf – und fordern mehr Sicherheit und Orientierung in einem dynamischen Marktumfeld.

77 Prozent der befragten IT-Dienstleister nutzen KI fast immer oder häufig. Nur 6 Prozent geben an, dass sie selten bis nie KI einsetzen. Vor allem größere Unternehmen setzen verstärkt auf KI, während kleinere Betriebe noch etwas zögerlicher sind.

Gleichzeitig wächst das Geschäft rund um KI rasant: Bereits 57 Prozent der Unternehmen bieten KI-Dienstleistungen an, drei von vier Befragten erwarten einen weiteren Anstieg der KI-Aufträge – insbesondere bei der Entwicklung KI-basierter Anwendungen und strategischer Beratung.

Herausforderung KI

Trotz der großen Akzeptanz bleibt der Umgang mit Künstlicher Intelligenz herausfordernd: 92 Prozent sehen zwar KI als eine Technologie, die die Arbeit erleichtert, aber 46 Prozent beurteilen KI auch als potenzielles Sicherheitsrisiko und weitere 37 Prozent sehen KI kritisch, da die erzielten Ergebnisse oft von niedriger Qualität seien. 61 Prozent der IT-Dienstleister fürchten eigene Schäden durch den Einsatz von KI, 60 Prozent sehen auch Risiken bei der Bereitstellung KI-gestützter Lösungen für Kunden.

Die größten Risiken im Zusammenhang mit KI sehen IT-Profis aktuell bei einem möglichen Datenmissbrauch (55 Prozent), Datenschutzverletzungen (42 Prozent), Verletzungen geistiger Eigentumsrechte (36 Prozent) und der allgemeinen Fehleranfälligkeit der Technologie (36 Prozent).

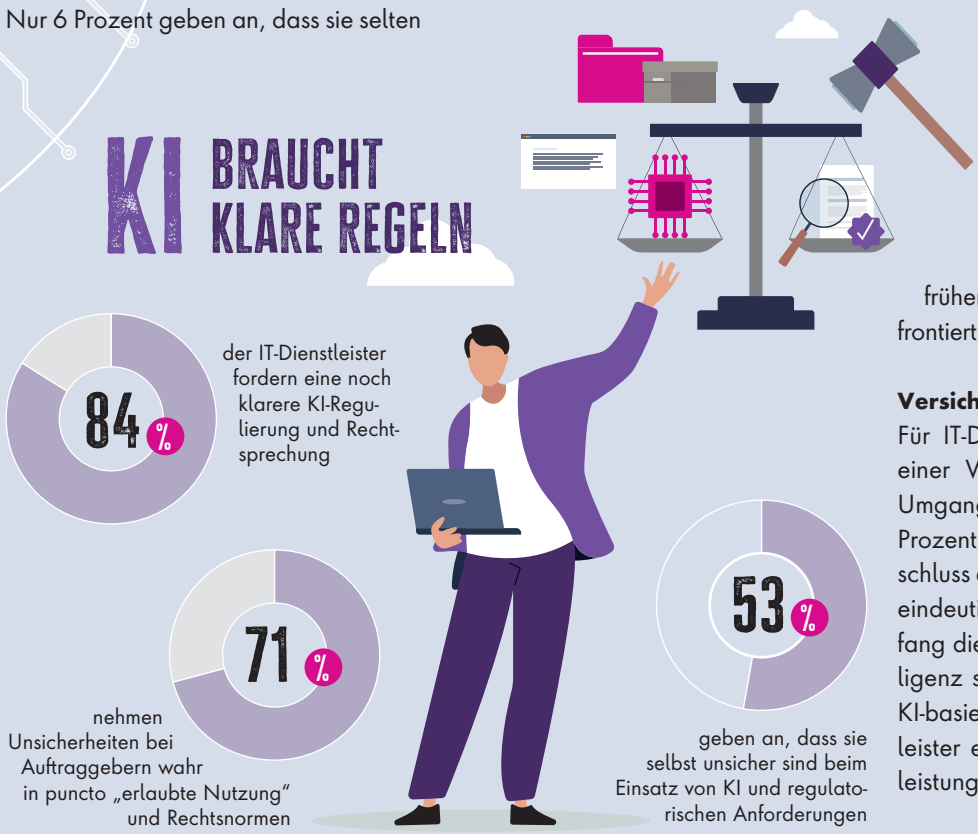
Auch die weiterhin unklare Rechtslage wird als Problem wahrgenommen.

Was die Unsicherheit noch weiter schürt: Insgesamt nehmen die Forderungen der Auftraggeber wegen vermeintlicher Schlechtleistungen spürbar zu – nur ein Viertel der Unternehmen blieb im vergangenen Jahr davon verschont. Und 55 Prozent der IT-Dienstleister gaben an, dass sie häufiger als früher mit solchen Forderungen konfrontiert werden.

Versicherer in der Pflicht

Für IT-Dienstleister ist beim Abschluss einer Versicherung zentral, dass der Umgang mit KI explizit geregelt ist: 85 Prozent der Befragten ist beim Abschluss einer Versicherung wichtig, dass eindeutig geregelt ist, in welchem Umfang die Nutzung von Künstlicher Intelligenz sowie mögliche Schäden durch KI-basierte, selbst durch die IT-Dienstleister erbrachte Lösungen und Dienstleistungen abgedeckt ist.

www.hiscox.de





(Quelle: INFODAS GmbH)

Neda Pashah, Principal Cybersecurity Standards and Audit, INFODAS GmbH, auf der diesjährigen it-sa in Nürnberg.

Grundschutz++

GROSSE PLÄNE UND OFFENE FRAGEN

Die Umstellung auf Grundschutz++ beschäftigt derzeit eine Vielzahl von Anwendern, Auditoren, Institutionen, Dienstleistern, Schulungsanbietern und Tool-Herstellern. Viele stehen vor grundlegenden Fragen in Bezug auf Umstellung, Migration und Veränderung für die tägliche Praxis. Als interessierter Beobachter und aktives Mitglied der Stand-der-Technik-Community möchten wir in diesem Beitrag unsere bisherigen Erkenntnisse, Beobachtungen und Eindrücke zusammenfassen.

Was wissen wir bisher?

In der Vergangenheit erschien jährlich ein überarbeiteter Informationssicherheits-Anforderungskatalog. Seit 2023 veröffentlichte das BSI kein neues Kompendium mehr und präsentierte seine Vision stattdessen auf Fachveranstaltungen. Doch viele Teilnehmende verließen die Events ernüchtert und mit wenigen neuen Informationen sowie ohne konkrete Umsetzungsbeispiele. Die Botschaft des BSI bleibt dennoch klar: ‚Cybersicherheit ist mess- und automatisierbar'.

Im Zuge dieser Vision rückten Schlagworte wie ‚Kennzahlen, Satzschablonen, Praktiken, Blaupausen, Handlungsworte, Metadaten, OSCAL, JSON, agile Veröffentlichung und Sicherheitsniveau' in den Vordergrund. Was zunächst nach mehr Komplexität klingt, soll langfristig für mehr Messbarkeit und Automatisierung sorgen. Aber wie passt das zu den bekannten Konzepten wie Basis-, Standard- oder Kernabsicherung? Was wird aus Strukturanalyse, Schutzbedarfsfeststellung und Modellierung?

Orientierung an ISO/IEC 27001

Ein zentrales Merkmal des Grundschutz++ ist die deutlich stärkere Anlehnung an die ISO/IEC 27001. Damit rückt der Top-down-Ansatz in den Vordergrund. Es soll ein risikoorientiertes Informationssicherheits-Managementsystem (ISMS) eingeführt werden, klar gegliedert in die bekannten PDCA-Phasen (Plan – Do – Check – Act), die sich in entsprechenden ISMS-Praktiken wiederfinden.

Ein Blick ins Detail: Praktiken und Blaupausen

Die Praktiken sind Bestandteil der Kataloge, die vom BSI über GitHub in den maschinenlesbaren OSCAL-Datenformaten JSON und XML veröffentlicht sind. Diese bilden sowohl die Methodik als auch die Sicherheitsanforderungen ab. Zudem erfolgt die Auswahl geeigneter Sicherheitsanforderungen nicht wie bisher durch Modellierung der Bausteine, sondern über die Auswahl der Blaupausen unter Berücksichtigung der ersten Einschätzung des Schutzbedarfs. Diese grundlegende Einstufung wurde im Zuge der Modernisierung vereinfacht: Anstelle von drei Stufen kann nun zwischen zwei Stufen - ‚normal' (entspricht dem allgemeinen Stand der Technik) und ‚erhöht' - gewählt werden. Die Blaupausen enthalten eine vordefinierte Auswahl der Praktiken mit entsprechenden Sicherheitsanforderungen. Wer die Praktiken in einem anderen Format als JSON oder XML anzeigen möchte, braucht allerdings einen entsprechenden Konverter.

Fazit

Grundschutz++ ist kein einfaches Update, sondern eine grundlegende Neuausrichtung hin zu mehr Flexibilität, Effizienz und Automatisierung. Derzeit fehlt jedoch ein übergreifendes Gesamtbild sowie konkrete, nachvollziehbare Beispiele für eine Sicherheitskonzeption. Bislang liegen auch kaum Beispiele für eine Transition vom IT-Grundschutz zu Grundschutz++ vor und die angestrebte Messbarkeit bleibt vorerst theoretisch.

Ein frühzeitiger Einstieg in das neue Konzept sowie eine IST-Aufnahme des aktuellen Standes in der eigenen Institution sind dennoch sinnvoll und empfehlenswert. Panik ist jedoch nicht angebracht, denn bis zur vollständigen Einführung bleibt ausreichend Zeit, um sich strukturiert vorzubereiten.

www.infodas.com

Mit DORA zur Datensouveränität

EINHEITLICHE SICHERHEITSSTANDARDS FÜR BANKEN UND VERSICHERUNGEN

Als Teil der kritischen Infrastruktur ist der Finanzsektor ein beliebtes Ziel für Cyberangriffe. Bei Banken oder Versicherungen geht es schließlich schnell um Milliarden-Beträge. Mit der DORA-Verordnung möchte die EU nun für mehr Sicherheit sorgen. Die Regularien darin, insbesondere zu Exit-Strategien, sind zwar anspruchsvoll, können aber auch ein Weg hin zur Datensouveränität sein.

Cyberattacken auf Finanzunternehmen sind inzwischen fast alltäglich. Im Sommer 2023 konnten digitale Bankräuber etwa an Kundendaten der Deutschen Bank, Postbank, Comdirect oder ING gelangen, indem sie eine Schwachstelle im File-Transfer-Tool MOVEit ausnutzten. Im Frühjahr 2025 wurde mehrere deutsche Finanzhäuser Opfer einer koordinierten DDoS-Attacke. Und nur wenige Wochen später erwischte es den spanischen Versicherer Asefa – an rund 200 Gigabyte an Daten sollen die Täter gelangt sein.



DORA WIRD ZU EINEM WICHTIGEN FAKTOR DER DATENSOUVERÄNITÄT UND MACHT DIE STRUKTUREN DES FINANZSEKTORS GLEICHZEITIG UNABHÄNGIGER, WIDERSTANDSFÄHIGER UND ZUKUNFTSSICHER.

Sönke Liebau,
Mitgründer und CPO, Stackable GmbH,
https://stackable.tech/de/

Um solche Vorfälle einzudämmen, hat die Europäische Union den Digital Operational Resilience Act, kurz DORA, auf den Weg gebracht. Sie möchte damit die Cyberresilienz von Banken, Versicherungen und Finanzdienstleistern auf ein einheitliches Niveau in der ganzen EU heben. Seit Januar 2025 sollen die Institute u.a. nachweisen, wie sie auf Angriffe, Systemausfälle oder den Wegfall externer Dienstleister reagieren. Dazu zählen dauerhafte Schutzmaßnahmen genauso wie klare Reaktionspläne für den Ernstfall.

Datensouveränität im Fokus

Das zentrale Motiv hinter allen DORA-Details ist die Datensouveränität. Also die Fähigkeit eines Unternehmens, jederzeit die Kontrolle über geschäftskritische Daten zu haben. Und das unabhängig vom Standort, Speicherort oder von einem externen Dienstleister. Die Finanzinstitute brauchen dabei nicht nur eine Transparenz über alle genutzten Komponenten. Sie sollen bei allen Datenflüssen auch auf eine revisionssichere Dokumentation achten und vorzugsweise auf proprietäre Lösungen verzichten, die einen Anbieterwechsel erschweren oder gar unmöglich machen.

Die Datensouveränität geht aber über die technischen Fragen hinaus. In einem Markt, der immer digitaler wird, entscheidet sie über regulatorische Compliance, die Unabhängigkeit von einzelnen Anbietern und letztendlich über die Wettbewerbsfähigkeit. Um einen weiteren Schritt hin zu dieser Unabhängigkeit zu gehen, beinhaltet DORA verschiedene Vorgaben. Besonders anspruchsvoll sind dabei belastbare Exit-Strategien.

Die Rolle der Drittanbieter

Neu an DORA ist, dass die Regulierung erstmals Drittanbieter direkt einbezieht. Die Cybersecurity liegt damit nicht mehr allein bei den Finanzhäusern, sondern auch bei den jeweiligen IT-Dienstleistern. Und um den Wegfall oder Wechsel eines Dienstleisters zu kompensieren, legt DORA einen besonderen Fokus auf Exit-Strategien. Jedes Finanzunternehmen soll nachweisen, dass es kritische Dienste jederzeit auf einen anderen Anbieter übertragen kann. Und das nicht nur theoretisch, die Pläne müssen regelmäßig getestet und an aktuelle Umstände angepasst werden.

Was sich zunächst wie eine simple Vorsichtsmaßnahme liest, wird in der Praxis schnell zu einer großen Herausforderung. Ein reibungsloser Anbieterwechsel setzt schließlich voraus, dass die Daten vollständig dokumentiert sind, in offenen Formaten vorliegen und die Systeme interoperabel sind. Lückenhafte Dokumentationen, fehlende Migrationstests oder proprietäre Lösungen werden dabei schnell zum Hindernis. Und wer das Thema vernachlässigt, riskiert

nicht nur Strafen, sondern schlimmstenfalls die Handlungsfähigkeit des Unternehmens.

In der Wolke oder vor Ort?

Auch die Infrastruktur muss bei DORA mitgedacht werden. Zwar verdrängt die Verordnung Cloud-Dienste nicht, verschärft aber die Anforderungen. Bei vielen Instituten haben sich deshalb hybride und Multi-Cloud-Modelle durchgesetzt, um Abhängigkeiten zu verringern und Vorgaben zur Portabiliät zu erfüllen. Aber parallel erleben auch On-Prem-Infrastrukturen ein neues Hoch: Wo besonders sensible Daten genutzt werden und kein Weg an der Kontrolle vor Ort vorbeiführt, bleibt das hauseigene Rechenzentrum die erste Wahl.

Das Ergebnis ist eine immer komplexere IT-Landschaft, in der Cloud und On-Premises nebeneinander im Einsatz sind. Und deshalb auch reibungslos miteinander funktionieren müssen. Wer diese Flexibilität nicht von Anfang an einplant, baut neue Abhängigkeiten auf, die DORA eigentlich abschaffen soll.

Open Source als entscheidendes Puzzleteil

Open Source-Technologien sind inzwischen keine Randerscheinung mehr, sondern fester Bestandteil vieler Unternehmen, wie der aktuelle Open Source-Monitor des Branchenverbands Bitkom zeigt. Open Source hilft aber nur, wenn die Projekte professionell gepflegt werden und durch klare Governance-Prozesse abgesichert sind. Denn: Vernachlässigte Open Source-Komponenten können ein ebenso großes Risiko darstellen wie veraltete proprietäre Lösungen. Hier hilft ein Anbieter, der nicht nur für die Sicherheit einzelner Komponenten sorgt, sondern eine komplette Supply Chain Security nachweisen kann.

Vor allem modulare, interoperable Datenplattformen auf Open Source-Basis sind ein wichtiges Puzzleteil bei der DORA-Umsetzung. Auch wir von Stackable haben uns deshalb von Beginn an für eine Open Source-Architektur entschieden, samt nachvollziehbarer Software-Lieferkette und variabler Infrastruktur. Sie bringen bei DORA den Vorteil, dass sich Szenarien für einen Anbieterwechsel realistisch simulieren lassen, ohne den laufenden Betrieb zu gefährden.

Mit der Mischung aus Datenübertragung, Vernetzbarkeit und dokumentierter Infrastruktur können Finanzinstitute Exit-Tests durchführen, die nicht nur den DORA-Ansprüchen gerecht werden, sondern auch im Ernstfall funktionieren. Auch Technologien wie GitOps, bei denen Infrastruktur als Code verwaltet wird, helfen, Migrationsprozesse reproduzierbar und transparent zu gestalten und gleichzeitig die Nachvollziehbarkeit gegenüber Aufsichtsbehörden zu erhöhen.

Wer diese Punkte beachtet, kann den größten Nutzen aus DORA ziehen. Dann werden die Vorgaben nicht zur Last, sondern zum Hebel: Mit modularen, offenen Plattformen erreichen Unternehmen nicht nur Compliance, sondern gewinnen auch an Flexibilität – sie können identische Workloads je nach Bedarf im eigenen Rechenzentrum oder bei einem Hyperscaler betreiben.

Was ist zu tun?

CIOs und CISOs sollten die vorhandene IT-Landschaft jetzt grundlegend unter die Lupe nehmen. Und dabei die entscheidenden Fragen stellen: Wie reproduzierbar laufen Migrationen ab? Sind unsere Daten portabel genug? Gelingt mit den eingesetzten Komponenten ein bruchloser Anbieterwechsel? Und ist unsere Dokumentation wirklich vollständig, um Prüfungen standzuhalten?

Wer diese Punkte möglichst schnell abklärt, sorgt nicht nur für Rechtssicherheit, sondern auch für einen nachhaltigen Vorteil. So wird DORA zu einem wichtigen Faktor hin zur Datensouveränität und macht die Strukturen des Finanzsektors gleichzeitig unabhängiger, widerstandsfähiger und zukunftssicher.

Sönke Liebau



NDR als Schlüsseltechnologie

DORA-COMPLIANCE NEU GEDACHT

Obwohl der Stichtag längst hinter uns liegt, arbeiten Finanzinstitute noch immer daran, die DORA-Anforderungen konsequent in ihre täglichen Abläufe zu integrieren. Aktuelle Umfragen deuten darauf hin, dass viele deutsche Banken und Finanzdienstleister kritische Maßnahmen noch gar nicht umgesetzt haben – vor allem hinsichtlich der Klassifizierung von sicherheitsrelevanten Vorfällen sowie der detaillierten Berichterstattung. Hier kommt Network Detection and Response (NDR) ins Spiel.

Eine NDR-Lösung eignet sich ideal, um Unternehmen in ihrer DORA-Strategie maßgeblich zu unterstützen – konkret in diesen Bereichen:

➤ **IKT-Risiken managen**
(Art. 5-15 DORA)
DORA verlangt eine laufende Risikoanalyse, den Einsatz technischer Schutzmaßnahmen sowie kontinuierliches Monitoring. NDR-Lösungen unterstützen dies durch umfassende Netzwerksichtbarkeit. Ergänzend liefern sie historische Daten und Threat Intelligence Feeds, die fundierte Risikoanalysen ermöglichen.

➤ **Vorfälle erkennen und klassifizieren, Bericht erstatten**
(Art. 17-23 DORA)
DORA schreibt ein schnelles Erkennen, Klassifizieren und Melden von IKT-Vorfällen vor. NDR-Tools analysieren dafür laufend den Netzwerkverkehr und erkennen mithilfe von KI effizient verdächtige Abweichungen sowie unerlaubte Zugriffsversuche (Incident Detection).

➤ **Drittanbieterrisiken managen**
(Art. 28-39 DORA)
Zur Erfüllung der DORA-Vorgaben müssen auch externe IKT-Dienstleister überwacht und gemanagt werden. NDR schafft hier Transparenz, indem es den Netzwerkverkehr von SaaS-, Cloud- und Remote-Diensten analysiert. Im Zuge dessen macht eine NDR-Lösung auf ungewöhnliche Verbindungen oder Datenabflüsse aufmerksam.

➤ **Informationen austauschen**
(Art. 40 DORA)
DORA fordert von Finanzinstituten, dass sie sich untereinander über Bedrohungen und Schwachstellen austauschen. NDR-Lösungen integrieren sich in Threat-Intelligence-Plattformen, erleichtern so den standardisierten Austausch und identifizieren Hinweise auf eine Kompromittierung.

Da eine moderne NDR-Lösung Netzwerke effizienter durchsucht und so verdächtige Aktivitäten und Bedrohungen schneller erkennt als herkömmliche Tools, erweist sie sich als zentrale Schlüsseltechnologie – sowohl bei der effizienten Bedrohungsjagd als auch zur Einhaltung der DORA-Anforderungen. Dennoch bleiben auch bei ihnen trotz der umfangreichen Funktionen gewisse Limitierungen bestehen.

So besteht das Risiko von Sichtbarkeitslücken, sobald die überwachenden Sensoren umverlegt und neu konfiguriert werden müssen. Zudem kommen unzählige, größtenteils verschlüsselte Daten aus verschiedenen Richtungen gleichzeitig ins Netzwerk und bewegen sich hindurch (lateraler East-West Traffic). Sowohl lateraler als auch verschlüsselter Datenverkehr sind für NDR-Lösungen nur schwer einzusehen. Ihre Stärken liegen vielmehr bei entschlüsseltem Verkehr. Allerdings stellen gerade verschlüsselte Daten eine große Gefahr dar: 86 Prozent der Cyberbedrohungen sind im verschlüsselten Datenverkehr verborgen. Und NDR ist nur dann wirksam, wenn das Tool die Anomalien auch sieht.

Deshalb ist es wichtig, für vollständige Sichtbarkeit zu sorgen – und zwar bis hinunter auf Netzwerkebene (Deep Observability).

www.gigamon.com





Digital Operational Resilience Act

NEUN MONATE NACH DER EINFÜHRUNG

Als die EU den Digital Operational Resilience Act (DORA) einführte, sollte damit die Grundlage für moderne Cybersicherheit im Finanzsektor geschaffen werden. Neun Monate später stellt sich die Frage, wie weit die Finanzinstitute mit der Umsetzung sind. Erste Anzeichen sind vielversprechend, die angestrebten Resilienz-Ziele zu erreichen.

DORA soll die operative Resilienz im gesamten Sektor erhöhen, indem systemische Risiken – insbesondere von IKT-Drittanbietern – adressiert werden. Dazu werden Organisationen an gemeinsame Standards in fünf Bereichen gebunden rund um Risikomanagement, Meldung von Vorfällen oder auch Tests der operativen Resilienz.

Wo DORA Wirkung zeigt

Die Sorgfaltspflicht und Aufsicht gegenüber Dritten sind Bereiche, in denen DORA erste Erfolge liefert. Die Verordnung hat Maßnahmen im Ökosystem der Finanzdienstleistungen formalisiert, die seit Jahren bekannt sind. DORA fördert Lieferantenregister, durchsetzbare Prüfungsrechte und einen risikobasierten Ansatz für die Integration von IKT-Lieferanten. Dabei handelt es sich um Maßnahmen zur Stärkung der Abwehr, die dazu beitragen, die Transparenz zu verbessern und potenzielle Risiken zu identifizieren. Gerade Vorfälle in der Lieferkette zeigen, wie sich eine Schwachstelle auf den gesamten Sektor auswirken kann und unterstreichen die Notwendigkeit eines durchgängigen Einblicks in Datenströme, robuster Tests sowie konsistenter Berichterstattung. Die Schaffung dieser gemeinsamen Grundlage ist unerlässlich, um sicherzustellen, dass das Finanzwesen auch bei größeren Störungen effektiv funktioniert.

Cloud Sicherheit als Meilenstein für DORA

Eine der bedeutendsten Erkenntnisse von DORA ist die Notwendigkeit, das Fachwissen und Verständnis im Bereich Cloud zu vertiefen. Funktionsübergreifende Schulungen und eine engere Zusammenarbeit zwischen Rechts-, Beschaffungs- und Technikteams helfen dabei die richtigen Fragestellungen anzugehen. Externe Perspektiven bestätigen, dass Verantwortlichkeit, Governance und klare Berichtsmechanismen funktionsübergreifend vernetzt sein müssen.

Nachdem der Rechtsrahmen im Wesentlichen fertiggestellt ist – einschließlich der im Juli 2025 finalisierten Verordnung über die Vergabe von IKT-Dienstleistungen an Subunternehmer –, wenden sich die Regulierungsbehörden nun der Kontrolle und Durchsetzung zu. Die nächste Phase wird sich auf die Klassifizierung von Vorfällen, zeitnahe Benachrichtigungen und die Prüfung technischer und verfahrenstechnischer Kontrollen in kontrollierten Szenarien konzentrieren. Die Effizienz dieser vorbereitenden Maßnahmen wird sich erst in realen Vorfällen zeigen, die schnelles und entschlossenes Handeln erfordern. Dann wird sich zeigen, ob die Dokumentation mit der operativen Leistungsfähigkeit übereinstimmt.

Harmonisierungsbemühungen der EU

DORA ist Teil einer umfangreicheren Initiative, zu der auch NIS2, der EU AI Act und das neue europäische Cybersicherheits-Zertifizierungssystem für Cloud-Dienste (EUCS) gehören. Diese Rahmenwerke haben gemeinsame Merkmale wie die Rechenschaftspflicht, Überwachung durch Dritte und die Meldung von Vorfällen, vervielfachen aber den Aufwand für Organisationen. Die Europäische Kommission hat diese Herausforderung erkannt und bemüht sich um eine Vereinfachung und Harmonisierung dieser Vorschriften durch ihr bevorstehendes Digital Omnibus-Paket. Diese Initiative zielt darauf ab, den Verwaltungsaufwand und die Compliance Kosten – insbesondere im Bereich der Berichterstattung – zu reduzieren und gleichzeitig hohe Standards für Sicherheit, Fairness und Datenschutz aufrechtzuerhalten.

James Tucker



EINE DER BEDEUTENDSTEN ERKENNTNISSE VON DORA IST DIE NOTWENDIGKEIT, DAS FACHWISSEN UND VERSTÄNDNIS IM BEREICH CLOUD ZU VERTIEFEN.

James Tucker, Head of CISO, EMEA, Zscaler, www.zscaler.de

Mobile Sicherheit im Unternehmensalltag

DER MASSSTAB FÜR TRANSPARENTE UNTERNEHMENSSICHERHEIT

Am 23. Juli 2025 hat Samsung als erster Hersteller das IT-Sicherheitskennzeichen des Bundesamts für Sicherheit in der Informationstechnik (BSI) für ausgewählte mobile Endgeräte und Smart-TVs erhalten. Umfasst sind die aktuellen Smartphones der Galaxy-A-Serie (A26, A36, A56) sowie das TV-Portfolio 2025.*

Das Kennzeichen bestätigt die Einhaltung geltender Sicherheitsanforderungen des BSI. Für Unternehmen ist dieser Schritt ein deutliches Signal: IT-Sicherheit auf mobilen Geräten ist nicht nur Kür, sondern Pflicht – und kann ein strategischer Erfolgsfaktor sein.

Mobile Endgeräte als Achillesferse der IT

Smartphones und Tablets sind längst integraler Bestandteil von Arbeitsprozessen. Doch gerade hier können neue Risiken entstehen. Phishing-Angriffe zielen auf mobile Messaging-Apps, kompromittierte Geräte dienen als Zugangstor in Unternehmens-Clouds, und hybride Arbeitsmodelle mit Bring-Your-Own-Device (BYOD) vergrößern die Angriffsflächen zusätzlich.

Während Server und Netzwerk aufwendig geschützt werden, bleiben mobile Endgeräte häufig das schwächste Glied der Kette. Unternehmen sollten deshalb nicht nur Geräte bereitstellen, sondern auch Verwaltung, Sicherheit und Compliance nahtlos integrieren.

Schutz von Grund auf

Eine mögliche Antwort liefert die Samsung-Knox-Plattform. Sie setzt auf „Security by Design" und verankert Schutzmechanismen bereits auf Hardwareebene. Dazu gehören unter anderem Secure Boot, das isolierte Knox Vault oder Integritätsprüfungen, die Manipulationen am Betriebssystem erkennen können.

Knox zeichnet sich durch einen mehrschichtigen Ansatz aus: Hardware, Betriebssystem und Management-Tools greifen ineinander. Dadurch entsteht eine konsistente Sicherheitsarchitektur, die sich in bestehende Unternehmens-IT einbinden lässt, ohne dass zusätzliche Schutzmechanismen nachgerüstet werden müssten.

Schutz ohne Zusatzgeräte

Einen besonderen Stellenwert nimmt bei Samsung Knox Native ein. Die gemeinsam mit dem BSI entwickelte Lösung erhielt Ende 2023 die Einsatzerlaubnis für den Umgang mit Verschlusssachen bis VS-NfD („Verschlusssache – Nur für den Dienstgebrauch").

Kern ist das nach CC EAL 6+ (Common Criteria Evaluation Assurance Level) zertifizierte eingebettete Secure Element (eSE), das als Hardwareanker im Gerät verbaut ist. In Kombination mit einem Java-Card-Applet werden Schlüssel und Zertifikate direkt im Gerät gespeichert. Damit lassen sich E-Mails, Kalender oder Kontakte verschlüsseln, ohne das externe Hardware wie Smartcards oder spezielle SD-Karten nötig wären.

Für Unternehmen in regulierten Branchen wie dem Gesundheitswesen und der Finanzindustrie bietet Knox Native sensible Kommunikation ohne Medienbrüche. Die kalkulierbaren Lizenzkosten erleichtern zudem die Budgetplanung.

Effizienz für IT-Abteilungen

Neben technischer Sicherheit zählt in der Praxis auch die Frage, wie sich eine große Geräteflotte verwalten lässt. Hier setzt Knox Suite an. Sie ermöglicht es, neue Geräte automatisiert in Betrieb zu nehmen, Sicherheitsupdates zentral zu verteilen und Integritätsprüfungen durchzuführen. Auch die Integration in bestehende UEM-Systeme ist möglich.

WAS DAS BSI-IT-SICHERHEITSKENNZEICHEN BRINGT

- Bestätigt die Einhaltung der BSI-Standards (diese umfassen z. B. BSI TR-03180 A, ETSI EN 303 645)
- Schafft Transparenz zu Sicherheits- und Update-Standards
- Bietet über QR-Code direkten Zugang zu BSI-Produktinformationen
- Bietet Kauforientierung für Sicherheit und Vertrauen bei der Geräteauswahl

Für IT-Abteilungen kann das eine deutliche Verringerung des manuellen Aufwands bedeuten. Onboarding-Prozesse können beschleunigt, Compliance-Vorgaben einfach umgesetzt und die Gesamtkosten für Verwaltung und Support verringert werden.

Sicherheitslabel macht Qualität sichtbar

Mit dem IT-Sicherheitskennzeichen liefert Samsung nicht nur ein Signal an Endkunden, sondern auch eine Kauforientierung für Unternehmen. Beschaffungsentscheidungen können sich an den geprüften und bestätigten Standards orientieren, Compliance-Officers erhalten eine Grundlage für Audits, und das Risikomanagement kann von einem externen Nachweis der Gerätesicherheit profitieren.

Ausblick

Die Bedrohungslage entwickelt sich kontinuierlich weiter. Samsung adressiert dies unter anderem mit Knox Matrix, das Sicherheitsfunktionen geräteübergreifend koordiniert, sowie mit quantengeschützter Kryptografie, die klassische Verschlüsselungsverfahren langfristig ergänzt. Hinzu kommt Knox Enhanced Encrypted Protection (KEEP), das personalisierte KI-Funktionen durch app-spezifische Speicherbereiche schützt.



DAMIT WIRD DEUTLICH: MOBILE SICHERHEIT IST KEIN STATISCHER ZUSTAND, SONDERN EIN PROZESS, DER SICH AN NEUE TECHNOLOGIEN UND ANGRIFFSFORMEN ANPASSEN MUSS.

Nima Baharian-Shiraz, Senior Presales Consultant, Samsung Electronics Germany GmbH, www.samsung.com

Damit wird deutlich: Mobile Sicherheit ist kein statischer Zustand, sondern ein Prozess, der sich an neue Technologien und Angriffsformen anpassen muss.

Fazit

Mit der Kombination aus technologischer Absicherung durch Knox Native, effizientem Management über die Knox Suite und dem BSI-Kennzeichen setzt Samsung einen Standard in der Unternehmenssicherheit.

Für IT-Verantwortliche bedeutet das: Mobile Security sollte nicht mehr bloß optional sein. Wer in geprüfte und verwaltbare Produkte investiert, kann Risiken reduzieren, Compliance unterstützen und eine belastbare Grundlage für die digitale Transformation schaffen.

Nima Baharian-Shiraz

* Eine aktuelle Übersicht der gekennzeichneten Geräte steht auf der BSI-Homepage zur Verfügung: www.bsi.bund.de/it-sik/samsung



Haben Sie etwa eine Ausgabe der itmanagement und itsecurity

verpasst?

...mit einem Abo wäre das nicht passiert.



ZUM ABO

it-daily.net/leser-service

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.

it-daily.net

Zero Trust in der Produktion

INDUSTRIE 4.0 VOR CYBERANGRIFFEN SCHÜTZEN



LETZTLICH GEHT ES NICHT NUR DARUM, CYBERATTACKEN ABZUWEHREN. ES GEHT UM DIE SICHERUNG VON LIEFERKETTEN, PRODUKTIONSQUALITÄT UND UM DIE SICHERHEIT ALLER MITARBEITENDEN.

Udo Fink, Senior Manager Security (CNEE) & Digital Identity EMEA, DXC Technology, https://dxc.com/de/de

Die moderne Fabrik ist ein hochvernetztes, datengesteuertes Ökosystem: Maschinen kommunizieren über Cloud-Infrastrukturen, Sensoren erfassen Produktionsdaten in Echtzeit, KI-Systeme treffen operative Entscheidungen. Diese Vernetzung steigert Effizienz erheblich, schafft aber massive Angriffsflächen. Darüber sprachen wir mit Udo Fink, Senior Manager Security Central, Northern und Eastern Europe (CNEE) & Digital Identity EMEA bei DXC Technology.

it security: *Herr Fink, warum ist Zero Trust gerade für Produktionsunternehmen ein so drängendes Thema?*

Udo Fink: Die industrielle Fertigung hat sich inzwischen zu einem hochkomplexen, hypervernetzten Ökosystem entwickelt (Stichwort Industrie 4.0). Maschinen kommunizieren über die Cloud oder mit Netzwerken anderer Unternehmen, tausende Sensoren erfassen Daten in Echtzeit, digitale Zwillinge simulieren Szenarien und KI-Systeme treffen operative Entscheidungen. All diese Entwicklungen steigern Effizienz und Produktivität. Doch sie vergrößern auch die Angriffsfläche für Cyberkriminelle.

Daneben gibt es klassische Probleme: Unzählige Hersteller von Produktionsmaschinen haben Fernwartungszugriff und machen damit Netzwerke in der Industrie löchrig wie Schweizer Käse. Oftmals ist unbekannt, welche Geräte tatsächlich in diese Netze integriert sind – es gibt kein konsistentes Asset Management. Darüber hinaus sind die Produktionsnetzwerke oftmals nicht stark genug von IT-Netzwerken getrennt, so dass sie ein Einfallstor für die gesamte IT der Unternehmen darstellen. Nicht zuletzt sind viele der Geräte in der Produktion vergleichsweise alt und haben Schwachstellen, für die es keine Patches mehr gibt und sie können nicht mit modernen Schutzmaßnahmen ausgestattet werden.

Traditionelle Abwehrmechanismen reichen in dieser Umgebung nicht mehr aus. Denn bei Produktionsnetzen handelt es sich schon lange nicht mehr um geschlossene Systeme mit klar abgegrenztem Perimeter. Deshalb und angesichts der zunehmenden Verflechtung von IT und OT (Operational Technology) wird Zero Trust auch in der Fabrikhalle zur Pflicht.

it security: *Wie funktioniert Zero Trust in der Produktionsumgebung konkret?*

Udo Fink: Das Prinzip von Zero Trust ist simpel: ständig verifizieren statt vertrauen. Jedes Gerät, jede Maschine, jeder Nutzer und jede Anwendung gelten zunächst als potenziell kompromittiert.

Sobald eine dieser Instanzen in irgendeiner Weise mit einer anderen Instanz kommunizieren möchte, werden unter anderem Identität, Zustand und Verhalten überprüft. Bevor ein Sensor beispielsweise Daten ins Netzwerk einspeisen darf oder eine speicherprogrammierbare Steuerung (SPS) einen Befehl annimmt, findet eine genaue Verifizierung statt. Nur wenn die Anfrage alle Kriterien erfüllt, wird Zugriff gewährt. Dieser Prozess wird bei jeder Verbindung aufs Neue durchgeführt. Gleichzeitig lassen sich klare Zugriffsprivilegien vergeben: Mitarbeitende, Maschinen und Anwendungen erhalten nur die Rechte, die sie für ihre Aufgabe brauchen – nicht mehr.



Für noch höhere Sicherheit wird das Netzwerk zudem in mehrere Segmente unterteilt und mittels Zugangskontrollen quasi abgeriegelt. Sollte ein Angreifer seinen Weg hinein finden, kann er sich nicht ungehindert seitlich durch das gesamte System bewegen.

it security: *Viele Produktionsunternehmen haben bereits Firewalls und Multi-Faktor-Authentifizierung im Einsatz. Warum reichen diese Maßnahmen nicht aus?*

Udo Fink: Diese Maßnahmen sind absolut notwendige grundlegende Security-Bausteine, reichen jedoch in den heutigen hypervernetzten Ökosystemen nicht mehr aus. Firewalls zum Beispiel schützen nur, solange der Perimeter noch eine klare Grenze darstellt. In der modernen Produktionsumgebung ist das allerdings kaum mehr der Fall. Oder: Wir sagen jedem Unternehmen, dass es Multi-Faktor-Authentifizierung unbedingt einrichten muss, denn sie stärkt den Zugriffsschutz deutlich. Doch wenn ein Angreifer ein System mit einer kritischen Sicherheitsschwachstelle als Einfallstor findet und sich von dort ausbreiten kann, nützt auch sie nichts.

Zero Trust bringt all diese Maßnahmen in einen übergeordneten Rahmen. Es geht nicht mehr darum, Angreifer nur draußen zu halten, sondern jede einzelne Verbindung zu überprüfen und Sicherheit somit zu einem kontinuierlichen Prozess zu machen. Gerade angesichts der immer gefährlicheren Bedrohungslage – fast jede zehnte Ransomware-Attacke im zweiten Quartal 2025 richtete sich gegen Produktionsunternehmen – brauchen Unternehmen einen solchen ganzheitlichen Ansatz.

Ein besonders drastischer Fall ereignete sich Anfang September bei Jaguar Land Rover, als eine massive Cyberattacke die gesamte Produktion lahmlegte. Erst Ende des Monats konnte nach Angaben des Unternehmens wieder damit begonnen werden, die Produktion schrittweise hochzufahren. Währenddessen gewährte die britische Regierung dem Unternehmen Kreditgarantien über umgerechnet 1,7 Milliarden Euro, um Arbeitsplatzverluste beim Hersteller selbst und bei seinen Zulieferern zu vermeiden. Dieses Beispiel zeigt, welchen enormen volkswirtschaftlichen Schaden Cyberangriffe heute anrichten können – und es wird nicht das letzte seiner Art bleiben.

it security: *Welche konkreten Maßnahmen und Schritte empfehlen Sie?*

Udo Fink: Wie immer bei Security-Themen ist ein ausbalancierter, ganzheitlicher Ansatz absolut notwendig, da Angreifer immer das schwächste Glied in der Kette von Schutzmaßnahmen identifizieren und dort angreifen.

Unsere Empfehlung ist ein schrittweises Vorgehen: Man kann OT-Security-Monitoring-Lösungen (wie z.B. Microsoft Defender for IoT) sehr gut dazu verwenden, die Produktionsumgebungen zu scannen und ein besseres Verständnis über die Umgebung und die vorhandenen Geräte zu erlangen. Begleitend dazu sollte ein OT-Security-Konzept erstellt werden, in dem alle genannten Maßnahmen aus dem Zero-Trust-Ansatz eine Rolle spielen können. Durch diese proaktiven Maßnahmen wird der Schutzstandard der Umgebung erhöht. Zusätzlich sollte als reaktive, überwachende Maßnahme ein OT Security Monitoring eingeführt und mit dem Security Operations Center (SOC) des Unternehmens integriert werden, um Angriffe frühzeitig erkennen und bestenfalls abwehren zu können.

it security: *Wohin entwickelt sich Zero Trust?*

Udo Fink: Zero Trust ist heute der Standard, aber die Bedrohungslandschaft entwickelt sich rasant weiter. Angrei-



fer setzen KI ein, um täuschend echte Deepfakes oder Phishing-E-Mails zu erstellen. Das bedeutet, dass sich die Sicherheit ebenso weiterentwickeln und adaptiver werden muss. „Beyond Zero Trust" ergänzt die Grundprinzipien von Zero Trust um intelligente Mechanismen. KI-gestützte Systeme analysieren das Verhalten von Geräten und Nutzern in Echtzeit, erkennen Abweichungen und leiten automatisch Gegenmaßnahmen ein. Angriffe lassen sich so stoppen, bevor sie Schaden anrichten.



In der Produktion passt sich die Sicherheit somit der Komplexität hochautomatisierter Fertigungsumgebungen an, ohne Prozesse auszubremsen. Denn letztlich geht es nicht nur darum, Cyberattacken abzuwehren. Es geht um die Sicherung von Lieferketten, Produktionsqualität und um die Sicherheit aller Mitarbeitenden. Wer hier frühzeitig auf eine skalierbare Zero-Trust-Architektur setzt, bereitet seinen Betrieb auf die Herausforderungen der digitalen Zukunft vor.

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



CYBER-RESILIENZ IN KLEINEN TEAMS

KEINE OPTIONALE FRAGE MEHR

Cyber-Resilienz ist heute geschäftskritische Notwendigkeit. Kleine Teams verfügen oft nicht über ausreichende Budgets, Mitarbeiterkapazitäten oder Infrastruktur eines vollwertigen SOC. Sie müssen dieselben Standards erfüllen, ohne über dieselben Ressourcen zu verfügen.

Gleichzeitig steigt der Druck zur Einhaltung von Vorschriften. Die DORA-Verordnung in der EU und die neuen Offenlegungsvorschriften der SEC in den USA gelten auch für kleinere Unternehmen. Von den Teams wird erwartet, dass sie Transparenz, Überprüfbarkeit und Aufbewahrung auf Unternehmensniveau bieten, ohne über die Budgets oder das Personal eines Großunternehmens zu verfügen.

Die Transparenzlücke

Die meisten schlanken Sicherheitsteams wissen um die Bedeutung einer schnellen Erkennung und Reaktion. Aber mehr Tools bedeuten oft auch mehr Komplexität. Herkömmliche SIEMs zwingen Teams zu den folgenden Kompromissen: Sie können nur protokollieren, was das Budget zulässt. Sie müssen „wenig schwerwiegende" Warnmeldungen herausfiltern, um eine Überlastung der Analysten zu vermeiden. Und sie sind gezwungen, sich zwischen starrer Automatisierung oder fehlendem Kontext zu entscheiden.

Diese Lücken erhöhen das Risiko. Fehlende DNS-Protokolle, unentdeckter Diebstahl von Anmeldedaten oder fehlgeschlagene Korrelationen schaffen blinde Flecken.

Cyber-Resilienz ohne Kompromisse

Kleinere Unternehmen können sich keine anfälligen Arbeitsabläufe, Lücken in der Abdeckung oder Tools leisten, für deren Betrieb ein Vollzeit-Team erforderlich ist. Aber sie können es sich auch nicht leisten, zu warten. Resilienz muss von Anfang an integriert werden.

https://graylog.org/

AXA Future Risks Report 2025

CYBERRISIKEN WERDEN IN DEUTSCHLAND STARK UNTERSCHÄTZT

Die Deutschen unterschätzen die Risiken durch Cyberangriffe und Künstliche Intelligenz. Das zeigen die Ergebnisse des Future Risks Reports, einer weltweiten Umfrage im Auftrag der AXA Gruppe, die durch das Meinungsforschungsinstitut Ipsos im Mai und Juni 2025 durchgeführt wurde.

In Deutschland wurden für die Studie 2.000 Personen und zusätzlich 157 Experten online befragt. Die Teilnehmenden wurden gebeten, fünf Top Risiken auszuwählen und diese Risiken nach ihrer Relevanz für die Gesellschaft in den nächsten fünf bis zehn Jahren zu ordnen. Besonders auffällig dabei ist, dass die Einschätzung hinsichtlich künftiger Risiken deutlich von jener der Gesamtbevölkerung abweicht. Während Experten Cyberrisiken 2025 auf dem vierten Platz und Risiken durch Künstliche Intelligenz und Big Data auf Platz sechs der Risiken sehen, spielen Cyberrisiken 2025 für die Bevölkerung eine geringere Rolle – sie wurden auf Platz zehn eingeordnet. Die Risiken durch Künstliche Intelligenz und Big Data gehören laut den Studienergebnissen in der deutschen Bevölkerung gar nicht zu den zehn am stärksten wahrgenommenen Risiken.



UM KÜNSTLICHE INTELLIGENZ FÜR DIE GESELLSCHAFT, ABER AUCH FÜR UNTERNEHMEN OPTIMAL NUTZEN ZU KÖNNEN, MUSS DIE GESELLSCHAFT ZUKUNFTSFÄHIG WERDEN.

Dr. Marc Zimmermann, Vorstand, AXA Versicherung AG, www.AXA.de

„Hier sehen wir eine wesentliche gesellschaftliche Aufgabe. Den vielfältigen Chancen durch Künstliche Intelligenz stehen diverse Risiken gegenüber. Missbrauch, Fehlinformation und Cyber-Angriffe müssen wir sehr ernst nehmen", so Dr. Marc Zimmermann, Vorstand für Sachversicherungen von AXA.

Das hatte zuletzt der Cyber-Angriff auf einen IT-Dienstleister gezeigt, der den Flughafen Berlin im September 2025 längere Zeit lahmlegte.

„Um Künstliche Intelligenz für die Gesellschaft, aber auch für Unternehmen optimal nutzen zu können, muss die Gesellschaft zukunftsfähig werden – es braucht Aufklärung über Nutzen und Risiken, aber auch durch Unterstützung bei Schäden", bekräftigt Marc Zimmermann.

Erhebliche Zweifel an der Handlungsfähigkeit von Behörden

Auch die Behörden in Deutschland bekommen im Hinblick auf den Umgang mit Cyberrisiken in Deutschland keine guten Bewertungen. Dass sie gut auf Cyberrisiken vorbereitet sind, glaubt noch nicht einmal jeder Dritte der Deutschen (28 Prozent). Unter den Experten ist sogar nur rund jeder fünfte Befragte der Meinung, die Behörden seien gut vorbereitet (22 Prozent). Bei der Frage nach der Vorbereitung auf Risiken der Künstlichen Intelligenz traut nur ein geringfügiger Anteil von zwei Prozent der Experten den staatlichen Behörden Handlungsfähigkeit zu. In der Bevölkerung gibt immerhin noch jeder Vierte (24 Prozent) an, Vertrauen in die Behörden zu haben. Auch hier besteht Handlungsbedarf.

www.AXA.de

ÜBER DEN FUTURE RISKS REPORT

Der AXA Future Risks Report ermittelt jährlich die Wahrnehmung künftiger Risiken in einer Umfrage unter Experten und in der breiten Öffentlichkeit durch eine bevölkerungsrepräsentative Befragung. Das Meinungsforschungsinstitut Ipsos führte im Mai und Juni 2025 im Auftrag von AXA 23.000 Interviews in 18 Ländern der Welt. In Deutschland wurden 2.000 Personen und zusätzlich 157 Experten online befragt. Die Ergebnisse der Studie sind repräsentativ für die deutsche Bevölkerung ab 18 Jahren. Neben Deutschland wurden Ergebnisse in siebzehn weiteren Ländern aus Europa, Asien, Nord- und Südamerika ermittelt. 2025 erscheint der AXA Future Risks Report bereits zum zwölften Mal in Folge.



Versicherbarkeit von Ransomware

WARUM PRÄVENTION UND VERSICHERUNG ZUSAMMENGEHÖREN

Jahresabschlüsse, große Verkaufsaktionen, wie Black Friday und Weihnachten sowie Budgetausgaben: das vierte Quartal ist traditionell eine Phase erhöhter Bedrohung und damit ein Stresstest für die Cybersicherheit in KMUs. Angreifer, die ohnehin verstärkt den Mittelstand ins Visier nehmen, wissen das. Sie legen ihre Ransomware-Attacken strategisch in diesen Zeitraum, in dem Unternehmen darauf angewiesen sind, ihren Betrieb aufrechtzuerhalten. Denn kritische Fristen machen Ausfallzeiten für Unternehmen wesentlich kostspieliger. Dies erhöht den wahrgenommenen Wert eines erfolgreichen Angriffs und steigert die Wahrscheinlichkeit einer Lösegeldzahlung.

Zudem führen impulsive Technologiekäufe und übereilte Implementierungen zum Jahresende dazu, dass in Unternehmen unbeabsichtigt neue Sicherheitslücken entstehen können.

Ransomware nimmt erneut Fahrt auf

Dass in den kommenden Wochen mit einer Ransomware-Welle zu rechnen ist, lässt sich auf Portalen wie ransomware.live beobachten: Schon Mitte Oktober 2025 lag die Zahl der Ransomware-Opfer bei rund 81,7 Prozent des gesamten Werts aus Oktober 2024. Bei unveränderter Rate wird erwartet, dass die Zahl der Opfer im Oktober 2025 auf etwa 866 ansteigen wird – ein Plus von rund 58 Prozent gegenüber dem Vorjahr.

In kaum einer Zeit des Jahres sind Netzwerke und Mitarbeitende daher so stark gefordert wie im vierten Quartal.

Menschliche Faktoren als Einfallstor

Neben den genannten Punkten spielt auch der Faktor Mensch eine entscheidende Rolle. Phishing und Social Engineering, die häufig den ersten Angriffsvektor für Ransomware darstellen, steigen im Zusammenhang von Feiertagen tendenziell erheblich. So nutzen Cyberkriminelle etwa aus, dass Mitarbeitende durch Feiertagsplanungen, Einkäufe und den Stress zum Jahresende abgelenkt sind. Angreifer versenden überzeugende Köder wie gefälschte Versandbenachrichtigungen, Feiertagsaktionen oder dringende „Jahresend"-Anfragen. Dies trifft auf unvorbereitete Mitarbeiter, was die Klick- und Kompromittierungsraten erhöht.

Zum Jahresende verändern sich zudem häufig interne Abläufe: Neue Zeitarbeitskräfte, auslaufende Praktikumsverträge oder Urlaubsvertretungen führen zu verzögerten Anpassungen in der Zugangsverwaltung. Werden Benutzerkonten nicht rechtzeitig deaktiviert, entstehen unnötige Risiken.

Dass viele Unternehmen im Dezember sogenannte Change Freezes verhängen, um keine Systeme mehr zu verändern, schafft ein weiteres Risiko: Sicherheitsupdates oder Patches werden aufgeschoben und bietet Cyberkriminellen gute Angriffsmöglichkeiten.

Diese Gemengelage macht besonders den Mittelstand verwundbar. Ransomware-Angriffe treffen auf Strukturen, die laut BSI oft keine dedizierten IT-Security-Teams haben. Entsprechend hoch ist der potenzielle Schaden: Der Ausfall zentraler Systeme kann binnen Stunden ganze Wertschöpfungsketten lahmlegen.



KI verschärft die Bedrohungslage
Ebenfalls beobachten lässt sich, dass KI die Dynamik von Cyberangriffen massiv verändert. Täter gestalten Phishing-Mails und betrügerische Webseiten heute so täuschend echt, dass selbst geübte Anwender sie kaum erkennen. Über sogenannte Phishing-as-a-Service-Plattformen werden Angriffe standardisiert, skaliert und mit KI-gestützten Tarnmechanismen versehen. Folglich hat sich laut CYBERsicher die Zahl der in Deutschland veröffentlichten Hackerattacken zwischen 2021 und 2024 auf KMU mehr als vervierfacht.

Warum ganzheitlicher Versicherungsschutz entscheidend ist
Angesichts der vielfältigen Natur von Cyberangriffen reicht ein isolierter Blick heute nicht mehr aus. Denn Ransomware verursacht nicht nur technische, sondern auch betriebswirtschaftliche und reputationsbezogene Schäden. Entsprechend müssen Unternehmen ihre Absicherung ganzheitlich denken: Während eine Cyberversicherung in der Regel die Kosten für IT-Forensik, Wiederherstellung, Betriebsunterbrechung und Krisenkommunikation abgedeckt, schützt eine Vertrauensschadenversicherung vor Social Engineering oder CEO-Fraud. Dies trifft zu, wenn einem Betrieb beispielsweise Schäden durch Täuschung oder gefälschte Anweisungen an Mitarbeitende entstehen.

IT-, Software-, Technologie- und Telekommunikationsunternehmen brauchen zusätzlich eine IT-Haftpflichtversicherung. Sie schützt vor Risiken, die etwa durch IT-Ausfälle und menschliche Fehler, wie z. B. Schäden durch Verspätungen, Verstöße gegen Vertraulichkeitsvereinbarungen entstehen oder durch Ansprüche aus Gefährdungshaftung wie aus Service Level Agreements. In dieser Kombination entsteht ein Sicherheitsnetz, das technische und organisatorische Risiken gleichermaßen abdeckt.



ZUM JAHRESENDE STEIGT FÜR DEN MITTELSTAND TRADITIONELL DAS RISIKO, ZIELSCHEIBE VON RANSOMWARE-ATTACKEN ZU WERDEN.

Vincenz Klemm, Mitgründer und Geschäftsführer, Baobab Insurance, www.baobab.io

Neben einem ganzheitlichen Versicherungsschutz müssen Unternehmen außerdem präventive Maßnahmen aktiv umsetzen und implementieren. Dazu gehören etwa folgende Punkte:

- **Regelmäßige Back-ups:** Sicherheitskopien sind ein zentrales Element einer effektiven IT-Sicherheitsstrategie. Sie sollten an einem sicheren, externen Ort gespeichert und regelmäßig überprüft werden. Auf diese Weise können Unternehmen Ausfallzeiten minimieren, da wichtige Unternehmensdaten nach einem Angriff schnell bereitstehen und der Geschäftsbetrieb zügig fortgesetzt wird.

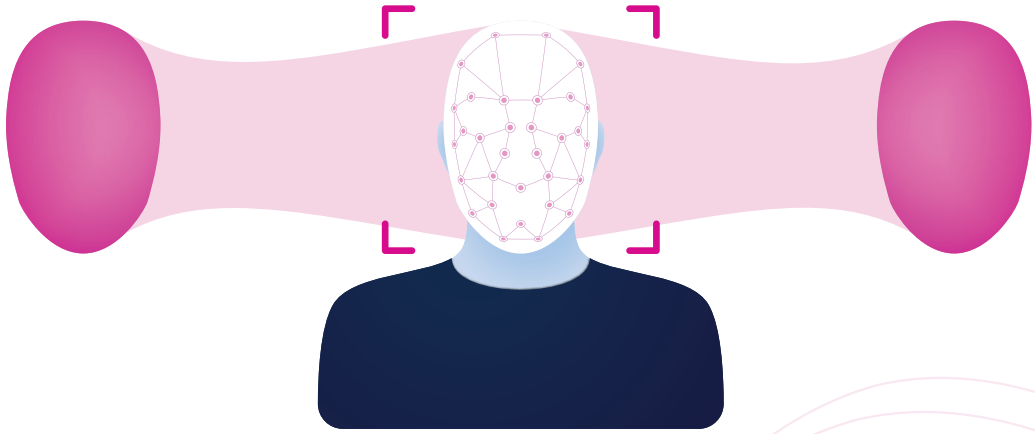
- **Passwortmanagement und gezielte Zugangsbeschränkungen:** Passwörter mit mindestens 8–12 Zeichen, eine Kombination aus Groß- und Kleinbuchstaben, Zahlen und Sonderzeichen. Wer auf diese Punkte achtet, stärkt den Schutz sensibler Daten. Eine Zwei-Faktor-Authentifizierung schafft zusätzliche Sicherheit. Außerdem sollten Unternehmen genau definieren, wer Zugriff auf welche Systeme und Daten benötigt, einschließlich externer Dienstleister. Die Maßgabe: Zugang sollten nur Personen haben, die ihn für ihre Arbeit benötigen.

- **Schulungen und Awareness-Trainings durchführen:** Sind Mitarbeitende nicht darin geschult, Sicherheitsrisiken wie verdächtige E-Mails oder Nachrichten zu erkennen, bieten sie ein potenzielles Einfallstor ins Unternehmen. Zu den Präventivmaßnahmen sollten daher regelmäßige Teamschulungen und -Trainings gehören.

KI verbessert IT-Sicherheit
Einen besonderen Stellenwert nehmen außerdem KI-gestützte Monitoring-Systeme ein: Ein kontinuierlicher DeepScan betrachtet den Betrieb von außen, erkennt ungewöhnliche Aktivitäten und bewertet Risiken automatisiert. Auf diese Weise lassen sich Schwachstellen schließen, bevor sie ausgenutzt werden. Dazu nutzt der Scan tagesaktuelle Informationen und analysiert den Bestand von Firewalls, Back-ups sowie E-Mail-Filterlösungen. Auf dieser Basis lassen sich etwa die möglichen Kosten für die IT-Forensik bewerten oder Betriebsunterbrechungen, Cyberbetrug und Datendiebstahl vorhersagen. Das Ergebnis ist ein ganzheitliches Risikoprofil.

Prävention und ganzheitlicher Versicherungsschutz
Zum Jahresende steigt für den Mittelstand traditionell das Risiko, Zielscheibe von Ransomware-Attacken zu werden. Besonders brisant ist, dass KI die Geschwindigkeit, Raffinesse und Zielgenauigkeit von Angriffen erhöht. Unternehmen müssen daher auf zwei Säulen setzen: präventive Schutzmaßnahmen und einen ganzheitlichen Versicherungsschutz aus Cyber- und Vertrauensschadenversicherung sowie gegebenenfalls einer IT-Haftpflichtpolice. Zusammen bilden sie das Rückgrat von IT-Sicherheit. Die natürlich auch über das Jahresende hinaus Bestand haben muss.

Vincenz Klemm



Die neue Ära der digitalen Täuschung

DEEPFAKES ERKENNEN, BEVOR SIE SCHADEN ANRICHTEN

Früher galt ein Foto als Beweis. Heute reicht das nicht mehr. Mit generativer KI lassen sich in Sekunden täuschend echte Bilder, Stimmen und Videos erzeugen – und selbst geschulte Augen und Ohren erkennen die Fälschung kaum noch. Tools wie ChatGPT, ElevenLabs oder spezialisierte Deepfake-Generatoren produzieren realistisch wirkende Inhalte auf Knopfdruck.

Diese Entwicklung führt zu einer Explosion komplexer Cyberattacken. Mitarbeitende und Privatpersonen sind oft unvorbereitet: Laut Microsoft Digital Defense Report 2024 gehen neun von zehn Cyberangriffen auf menschliches Fehlverhalten zurück. Gartner (2025) berichtet, dass bereits 44 Prozent der Unternehmen Vishing-Angriffe erlebt haben. Besonders gefährlich ist die Kombination aus Social Engineering und KI-basierter Stimmklonung.

Deepfakes als neue Social-Engineering-Waffe

Bereits Anfang 2024 fiel der britische Ingenieurbaukonzern Arup einem Deepfake-Video-Scam zum Opfer: Ein Mitarbeiter wurde in eine gefälschte Videokonferenz gelockt, in der sämtliche Teilnehmende (darunter der vermeintliche CFO) digital erzeugt waren. Innerhalb weniger Tage gingen 25 Millionen US-Dollar verloren.

DEEPFAKES IM SOZIALEN UMFELD

Der Mensch steht im Fokus von Cyberattaken ...

- Mitarbeiter verursachen bereits 9 von 10 Cyberangriffen [1]
- KI-Fortschritte ermöglichen eine neue Welle von hochentwickelten Cyberangriffen [2,3,6]
- Mitarbeiter sind nicht vorbereitet auf neue Kategorien von KI-Angriffen [3,4,5]

... und GenAI-Social Engineering nimmt rasant zu

ARUP	Januar 2024 Per Videokonferenz
pepco group	Februar 2024 Raffinierter Phishing Angriff
Ferrari	Juli 2024 Ferrari CEO eingeschüchtert

1 Harvard BR, McKinsey Avast, 2 CSO Online, SWR, Security Intelligence, 3 StationX, 4 Cybertalk, DarkTrace, 5 Barracuda, 6 Microsoft, 7 Gartner (2025)

FALLSTUDIE: SHINY HUNTERS VISHING ATTACK AUF SALESFORCE

Der Angriff

1. Vishing-Anruf

- IT-Service-Desks werden werden von vermeintlichen Salesforce Mitarbeitern angerufen
- Druck wird aufgebaut: „Sicherheits-problem muss sofort gelöst werden", Kundendaten betroffen

2. Autorisierung einer App

- Angreifer leiten die Zielperson dazu, eine scheinbar legitime App oder „Connected App" freizugeben
- Manipulierte Salesforce Data Loader/OAuth-App wird installiert

3. Schaden

- Angreifer erhalten API-Zugriff auf Salesforce-Instanz
- Massenexport von Kundendaten und CRM-Informationen möglich
- Sensible Daten können für Erpressung oder weitere Angriffe missbraucht werden

Wie man sich davor schützen kann

1. Mitarbeiterschulungen

- Simulation von Vishing-Angriffen (revel8)
- Mitarbeiterschulungen zu Social Engineering

2. Rollenbasierte Zugriffsrechte

- Minimalrechte für Nutzer & Apps
- Nur geprüfte Apps zulassen

3. Überwachung & Reaktion

- Alerts bei Massen-Exporten
- Klare Melde- und Notfallprozesse

Inzwischen sind die Angriffe noch komplexer geworden, wie der Fall Salesforce/Shiny Hunters im Sommer 2025 zeigt.

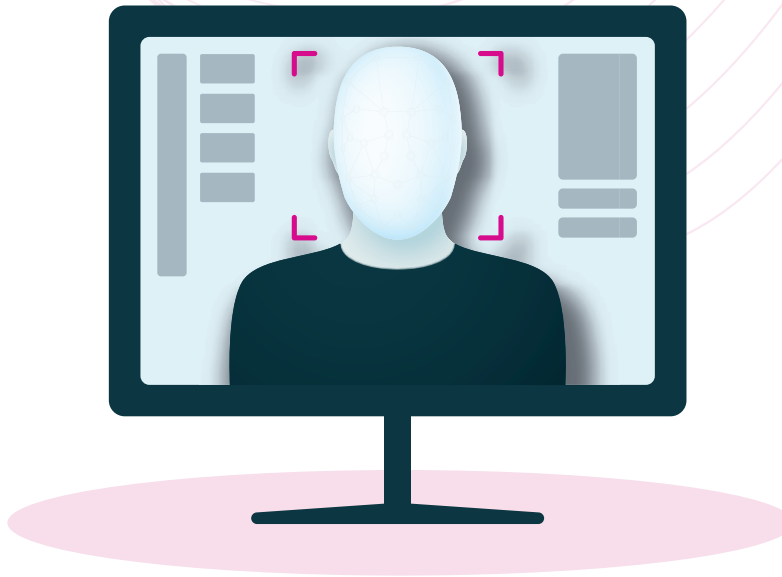
Case Study: Der Salesforce Voice Phishing Angriff

Die international agierende Hackergruppe Shiny Hunters, auch bekannt als UNC6040, nutzte Deepfake-Stimmen, um sich gegenüber IT-Service- und Helpdesk-Mitarbeitenden als internes Salesforce-Support-Team auszugeben.

Der Anruf: Angreifer gaben sich als technische Ansprechpartner aus und meldeten angebliche Sicherheitsprobleme („A security issue must be resolved immediately"). Der psychologische Druck war hoch, Kundendaten sollten angeblich betroffen sein.

Die Aktion: Während des Gesprächs wurden die Opfer angewiesen, Salesforce-Administrationsseiten wie „connected app / setup" aufzurufen. Dort genehmigten sie - im Glauben, eine offizielle App zu aktivieren - eine manipulierte Anwendung, häufig eine abgeänderte Version des legitimen Salesforce Data Loader.

Die Folgen: Durch die Autorisierung erhielten die Angreifer OAuth-Tokens mit weitreichenden Rechten. Diese nutzten sie, um massenhaft CRM-Daten (Kundenlisten, Support-Logs) zu exportieren. Anschließend forderten sie Lösegeld und drohten mit der Veröffentlichung.



HERAUSFORDERUNGEN BEI DER TECHNISCHEN DEEPFAKE-ERKENNUNG

1. Probabilistische Bewertung

- Technische Deepfake-Erkennung liefert lediglich einen Wahrscheinlichkeits-/Likelihood-Score
- Es muss weiterhin eine Entscheidung über Schwellenwerte getroffen werden
- Es wird false positives und false negatives Ergebnisse geben

2. Überlastung des Security-Teams

- SOC-Team wird mit Alarmmeldungen überhäuft
- Weiterhin hoher Aufwand bei der Untersuchung von Deepfakes
- Kritische Verantwortung bei interdisziplinären Anrufen

3. Remediation-Strategie

- Mitarbeiter müssen wissen, was im Falle eines Deepfakes zu tun ist
- Anruf beenden? Nach Verifizierung fragen?
- Risiko einer Betriebsunterbrechung

4. Ungeschützte Kanäle bleiben bestehen

- Angreifer kontaktieren Nutzer weiterhin über andere Kanäle
- WhatsApp? FaceTime? Telefon?
- Daher ist zusätzlicher Schutz erforderlich

Zu den betroffenen Marken zählten laut Berichten von BBC und SLCyber (2025) unter anderem Gucci, Balenciaga und Alexander McQueen, deren Kundendaten über kompromittierte Salesforce-Instanzen abflossen. Google bestätigte eine Verbindung zwischen diesem Angriff und den Shiny Hunters.

Zwischen Stimme und Vertrauen

Privatpersonen hingegen geraten zunehmend in emotionale Fallen. Kriminelle imitieren vertraute Stimmen oder Behördenmitarbeitende, um Vertrauen aufzubauen. Die Geschichte klingt plausibel, die Stimme echt und das Opfer reagiert instinktiv.



Einige einfache, aber effektive Maßnahmen helfen, sich zu schützen:

- **Familien-Safeword:** Ein zuvor vereinbartes Kennwort dient als interne Verifizierung bei Notfällen.
- **Kontrollfrage:** Eine Frage stellen, deren Antwort nur echte Angehörige kennen („Wie heißen Deine vier Kinder?“ statt fünf).
- **Kanalwechsel:** Bei Unsicherheit das Gespräch beenden und über einen vertrauten Kanal rückversichern.
- **Ruhe bewahren:** Angreifer setzen gezielt auf Zeitdruck und Emotion. Wer 20–30 Sekunden innehält, kann rationaler entscheiden.
- **Keine sensiblen Daten preisgeben:** Seriöse Organisationen im Jahr 2025 fordern niemals TAN, PIN oder Passwörter am Telefon.

Technik allein reicht nicht

Zum einen gibt es technische Möglichkeiten, die Echtheit von Audio- und Videoinhalten durch sogenannte Deepfake-Detection-Algorithmen zu überprüfen. Diese Systeme analysieren digitale Signaturen, Pixelmuster oder Sprachfrequenzen, um Hinweise auf Manipulation zu erkennen. Sie sind ein wichtiger Bestandteil moderner Sicherheitsstrategien, eignen sich jedoch nicht als alleinige Maßnahme.

Ein zentrales Problem liegt in der kurzen Halbwertszeit solcher Modelle: Detection-Systeme werden auf bestehenden Deepfake-Generatoren trainiert und liefern dort gute Erkennungsraten. Erscheinen jedoch neue KI-Modelle, müssen auch die Erkennungsalgorithmen erneut angepasst und trainiert werden. Das führt zu einem hohen Wartungs- und Updateaufwand, der viele Security-Teams zusätzlich belastet.

Zudem arbeiten diese Systeme probabilistisch. Sie liefern also nur eine Wahrscheinlichkeit, ob ein Inhalt echt oder manipuliert ist. Organisationen müssen daher selbst festlegen, ab welchem Schwellenwert ein Deepfake als erkannt gilt: Bei 90 Prozent? Oder erst ab 99 Prozent? Diese Festlegung beeinflusst unmittelbar die Zahl an False Positives und False Negatives, und damit die operative Belastung des Security-Teams.

Auch die Folgeprozesse müssen klar definiert sein: Was geschieht, wenn der Schwellenwert überschritten wird? Wird der Anruf automatisch unterbrochen, eine Warnmeldung ausgegeben oder eine manuelle Überprüfung eingeleitet? Jedes Szenario hat Auswirkungen auf Nutzerakzeptanz, Produktivität und Reaktionszeiten.

Selbst mit einer Integration in Plattformen wie Microsoft Teams oder Zoom bleiben viele inoffizielle Kommunikationskanäle (etwa WhatsApp oder private Mobiltelefone) ungeschützt. Angreifer nutzen genau diese Lücken, um Sicherheitsmaßnahmen zu umgehen.

Fazit: Wachsamkeit bleibt der beste Schutz

KI-Modelle werden immer besser, Deepfake-Generatoren immer zugänglicher. Deshalb gilt: Technische Erkennung allein reicht nicht aus. Entscheidend bleibt die Awareness der Mitarbeitenden, also die Fähigkeit, verdächtige Situationen selbst zu erkennen, zu hinterfragen und richtig zu reagieren. Moderne Awareness-Programme wie revel8 setzen hier an, indem sie Mitarbeitende mit realitätsnahen Simulationen und praxisbasierten Trainings (wie einen typischen CEO-Fraud per Deepfake-Anruf) auf genau diese Szenarien vorbereiten. Jede Privatperson muss sich darauf einstellen, dass Täuschungen künftig noch realistischer wirken.



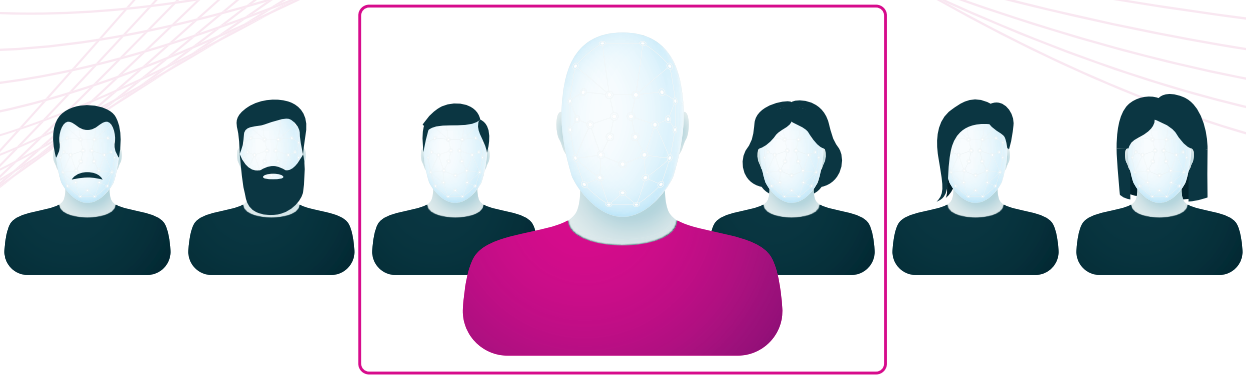
KI-MODELLE WERDEN IMMER BESSER, DEEPFAKE-GENERATOREN IMMER ZUGÄNGLICHER. DESHALB GILT: TECHNISCHE ERKENNUNG ALLEIN REICHT NICHT AUS.

Julius Muth, Co-Founder & CEO, revel8 GmbH, www.revel8.ai/

Der Unterschied liegt nicht in der Technologie, sondern im Verhalten der Menschen, die sie nutzen.

In Zukunft wird sich die Verteidigung stärker auf adaptive KI-Systeme und kontinuierliches Verhaltenstraining stützen müssen – kombiniert mit klaren Richtlinien für Mensch-Maschine-Interaktion. Doch trotz technologischer Fortschritte bleibt Aufklärung die wirksamste Verteidigung. Wer vorbereitet ist, erkennt Deepfakes, bevor sie Schaden anrichten.

Julius Muth



IMPRESSUM

Herausgeber: Ulrich Parthier (08104-6494-14)

Geschäftsführer: Ulrich Parthier, Vasiliki Miridakis

Chefredaktion: Silvia Parthier (-26)

Redaktion: Lars Becker, Carina Mitzschke
(nur per Mail erreichbar)

Redaktionsassistenz und Sonderdrucke: Eva Neff (-15)

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

Autoren:
Nima Baharian Shiraz, Lars Becker, Marine Goninet, Stefan Henke, Jörg von der Heydt, Vincenz Klemm, Sönke Liebau, Ann Maya, Carina Mitzschke, Julius Muth, Silvia Parthier, Ulrich Parthier, Nils Rogmann, James Tucker, 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. 33.
Preisliste gültig ab 1. Oktober 2025.

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.



DIGITALER BETRUG

OPFERZAHLEN NEHMEN ZU

Digitale Sicherheit ist längst kein Randthema mehr – sie bildet die Grundlage für Vertrauen, schützt die finanzielle Stabilität und bewahrt die persönliche Identität. Die neue Ping Identity Consumer Survey 2025 macht deutlich, wie groß die Belastung durch digitale Betrugsversuche in Deutschland ist. Bereits ein Viertel der Verbraucher hierzulande wurde Opfer von Betrug, Scam oder Identitätsdiebstahl. Das ist keine theoretische Gefahr, sondern für viele eine reale Erfahrung. Das Vertrauen der Deutschen in die Institutionen, die ihr digitales Leben verwalten, ist entsprechend erschüttert. Nur 12 Prozent haben noch volles Vertrauen in Organisationen, die ihre Identitätsdaten online verwalten, während 29 Prozent wenig oder gar kein Vertrauen haben. Zugleich geben 69 Prozent an, heute besorgter um die Sicherheit ihrer persönlichen Daten zu sein als noch vor fünf Jahren.

Trotz der zunehmenden Bedrohungslage fühlen sich nur 48 Prozent der Menschen ausreichend über aktuelle Betrugsmaschen informiert. Die andere Hälfte empfindet sich damit als ungeschützt und orientierungslos. Diese Unsicherheit führt dazu, dass viele Verbraucher bereit wären, auf digitale Bequemlichkeiten zu verzichten, um ihre Identität zu schützen, sei es bei der Nutzung sozialer Medien, beim Online-Shopping oder sogar beim Online-Banking.

Insgesamt ergibt sich für Deutschland ein deutliches Stimmungsbild: Die Verbraucher sind besorgt und zunehmend misstrauisch. Sie erwarten von Unternehmen, Politik und Technologieanbietern klare Maßnahmen. Nur durch transparente KI-Nutzung, verbindliche Regulierungen und eine konsequente „Identity-first"-Strategie kann das verlorene Vertrauen langfristig wiedergewonnen werden.

www.pingidentity.com

MEHR WERT
Studie: Bridging the Trust Gap

Cyberkriminelle überall da tut Hilfe not



Mehr Infos dazu im Printmagazin

itsecurity

und online auf www.it-daily.net

CYBERATTACKEN IM KEIM ERSTICKT

In einer Welt voller Cyber-Risiken existieren keine Regeln. Mit Full Spectrum Cyber von Beazley bleiben Versicherungsnehmer im Kampf gegen Cyberkriminalität immer einen Schritt voraus - denn eines der besten Teams der Branche hält ihnen den Rücken frei.

#GameOnCyber

Erleben Sie unser
Cyber-Ökosystem auf beazley.de

beazley

Insurance. Just different.