it management

Der Motor für Innovation
September/Oktober 2025

INKLUSIVE 80 SEITEN
it security

FIRMENENTWICKLUNG

Mit neuer Strategie in die Zukunft

Florian Buzin, Starface GmbH

THOUGHT LEADERSHIP

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

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

BUZZWORD-BINGO

LIEBE LESERINNEN UND LESER,

„Cloud Native", „AI-driven", „Zero Trust", „Digital Sovereignty" – Bingo! Auf den ersten Blick wirkt es, als spielten wir in der IT nur noch Buzzword-Bingo. Doch dieser Eindruck täuscht: Hinter den vermeintlich „überbewerteten" Schlagworten stecken zentrale Entwicklungen, die unsere Branche prägen, auch wenn sie durch ihren inflationären Gebrauch manchmal abgenutzt wirken.

Die Wahrheit ist unbequemer als das Klischee vom leeren Marketing-Sprech. Denn KI ist nicht nur ein Etikett für Software, sondern verändert Geschäftsprozesse von der automatisierten Code-Generierung bis hin zur prädiktiven Wartung komplexer Infrastrukturen. Digitale Souveränität klingt wie Politiksprech, entscheidet aber längst über Marktchancen und Risiken. Zero Trust ist keine Modeformel, sondern eine überlebenswichtige Strategie für hybride Arbeitswelten.

Und das allgegenwärtige IT-Trilemma aus Innovation, Sicherheit und Kosten? Das lässt sich nicht mit Marketingfloskeln auflösen, sondern fordert klare Entscheidungen, fundierte Strategien und den Mut, auch unbequeme Wahrheiten auszusprechen.

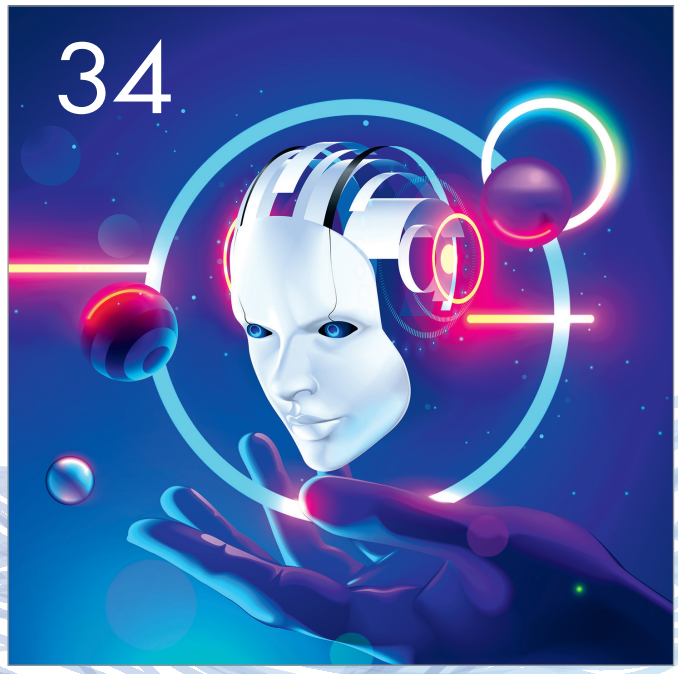
In dieser Ausgabe zeigen wir, was wirklich hinter den Begriffen steckt und welche Perspektiven überraschen, wenn man genauer hinsieht. Nicht jedes Buzzword verdient Aufmerksamkeit, aber die wirklich relevanten Entwicklungen schon – jenseits der Schlagworte, diesseits der Fakten.

Herzlichst,

Lars Becker | Redakteur

INHALT

Farblich hervorgehobene Artikel sind von der Redaktion als besonders lesenswert empfohlen



Inklusive 80 Seiten it security

GUT ZU WISSEN

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

DATENSICHERHEIT

MEHR ALS NUR NICE-TO-HAVE

Vor dem Hintergrund einer agilen Wirtschaftslandschaft, sich verändernden Rechtssituationen und zunehmender Komplexität der IT-Strukturen in den Unternehmen ist es erfreulich, dass sich das Bewusstsein hinsichtlich des Schutzes sensibler Unternehmensdaten offensichtlich verschärft. In einer von TechConsult im Auftrag von eperi durchgeführten Umfrage, gaben 41,7 Prozent der Unternehmen in Deutschland an, unabhängige Penetrationstests und Security Audits durchzuführen und 37,4 Prozent setzen auf eine eigene Datenverschlüsselung, deren Kontrolle ausschließlich ihnen selbst obliegt. 7,1 Prozent hoben hervor, allgemeine Datenschutzmaßnahmen zu planen, ohne jedoch konkrete Angaben zur Methodik oder Vorgehensweise zu machen. Diese Ergebnisse zeigen, dass die Erkenntnis, dass Datenschutz und Compliance von essenzieller Bedeutung für die Sicherheit und Zukunftsfähigkeit eines Unternehmens sind, inzwischen angekommen ist.

Auf Penetrationstests und Security Audits setzen mehrheitlich (60,6 Prozent) vor allem Organisationen mit 2.000 bis 4.900 Mitarbeitenden. Clustert man die Antworten nach den Funktionen der Antwortenden, zeigt sich, dass die IT-Spezialisten mit 46,4 Prozent und die Business-Verantwortlichen mit 37 Prozent auf Audits und Tests vertrauen. Anders ist das Bild, das sich beim Einsatz von Verschlüsselungstechniken zeigt. Auf diese setzen 41, 1 Prozent der Konzerne sowie Unternehmen mit 500 – 1.900 Beschäftigten. Ausgewogener ist hier auch die Einschätzung seitens der Fachleute. Vertreter aus der Business-Fraktion sehen zu 38,6 Prozent und aus der IT-Fraktion zu 36, 1 Prozent in der Verschlüsselung eine gute Möglichkeit, wichtige Unternehmensdaten zu schützen.

Unternehmen der kritischen Infrastruktur setzen auf Verschlüsselung

Ein Blick auf die Branchen macht deutlich, dass Verschlüsselung überdurchschnittlich oft in der öffentlichen Verwaltung (43,5 Prozent), dem Banken- & Versicherungswesen (46,5 Prozent) sowie dem Gesundheits- und Sozialwesen (50 Prozent) zum Einsatz kommt. Eine Ausnahme scheint die Energie- und Wasserversorgung zu sein. Hier setzen lediglich 37,5 Prozent auf Verschlüsselung, aber 50 Prozent auf Penetrationstests und Security Audits.

Fazit

Dass sich die Zeiten geändert haben, Angriffe zur täglichen Realität geworden sind und Datenschutz und Compliance mehr als ein Nice-to-have sind, ist in den Unternehmen angekommen. Deshalb setzt die Mehrheit der Unternehmen auf zeitgemäße Methoden und Technologien, die ihnen helfen, ihre sensiblen Daten und Prozesse zu schützen.

www.eperi.com

Schulungen = Zeitverschwendung?

ÜBER DIE SINNHAFTIGKEIT VON PHISHING-TRAININGS IM ZEITALTER VON KI

Die primäre Verantwortung für den Schutz der Unternehmensdaten sollte bei der IT-Sicherheitsabteilung liegen. Andere Mitarbeitende fungieren als zusätzliche Sicherheitsebene durch das Erkennen verdächtiger E-Mails. Studien zeigen jedoch, dass die Erfolgsrate bei der manuellen Bedrohungserkennung trotz Schulungsmaßnahmen rückläufig ist.

Was bedeutet das im Angesicht von KI?

KIs, vor allem LLMs (Large Language Models), sind auf Maschine-Mensch-Kommunikation optimiert. Sie können dabei nicht nur Worte sinnvoll aneinanderreihen, sondern auch Schreib- bzw. Sprechstile imitieren. Mittels sogenanntem „Prompt Engineering", der Programmierung durch die Eingabe von Befehlen, kann praktisch jeder Nutzer der Maschine mitteilen, wie sie agieren soll. Für Opfer wird es dadurch immer schwieriger, den Unterschied zwischen einer normalen und betrügerischen Kommunikation zu erkennen, zudem verringert die KI die Aufwände und erhöht die Produktivität.

Je schneller und effektiver KI-Lösungen werden, desto häufiger werden sie auch in der Cyberkriminalität eingesetzt, und desto seltener wird der Mensch als Sicherheitsbaustein dies erkennen – unabhängig vom Trainingsgrad.

Wie kann es weitergehen?

In der IT-Sicherheit sind die Bausteine Zero Trust, Cyber Risk Exposure Management (CREM) sowie Detection und Response hinreichend bekannt. Diese Bausteine verringern das Eintrittsrisiko sowie die Auswirkungen von Schadensfällen. Für diese Technologien und Strategien ist es unerheblich, woher der Angriff kommt und warum er nicht abgewendet werden konnte. Es sind, bildlich gesprochen, die Sicherheitsgurte und Airbags, die im Schadensfall das Überleben garantieren. Wenn ein Link-klickender Mitarbeiter dafür verantwortlich ist, dass ein Unternehmen vollverschlüsselt wird, dann ist nicht er das Problem, sondern die eigene Sicherheitsinfrastruktur.

Fazit: Braucht es Schulungen?

Schulungen sind teuer. Nicht nur die Kosten für Einführung der Prozesse, auch der Arbeitsaufwand jedes einzelnen Mitarbeiters ist zu berücksichtigen. Es ist deshalb legitim, den Mehrwert zu hinterfragen. Dieser liegt darin, die Eintrittswahrscheinlichkeit von Cyberattacken zu verringern. Schulungen waren bislang ein wichtiger Bestandteil von Security-Strategien. Aber wie ausnahmslos alles in der Security verliert auch dieser mit der Zeit an Wirkungsgrad. Das bedeutet aber nicht, dass dieser Baustein sofort sinnlos wird. Solange die IT-Sicherheit durch die schiere Anzahl an Einzelereignissen, die geprüft werden müssen, ausgelastet ist, braucht es Schulungen, um diese zu reduzieren.

Schulungen sind vor allem wichtig, wenn es um den Betrug an sich geht und darum, „Red Flags" zu erkennen, wie das Einfordern von Geld oder den Zugriff auf Unternehmensdaten. Auch müssen Mitarbeiter verstehen, warum sie Sicherheitsprozessen, z.B. Multifaktor-Authentifizierung beim Zugriff auf Daten, befolgen müssen und wie Angreifer versuchen, daran vorbeizukommen.

www.trendmicro.com/de

KI-Agenten

STARKES WACHSTUM ERWARTET

Laut Gartner werden bis 2026 rund 40 Prozent aller Unternehmensanwendungen aufgabenspezifische KI-Agenten enthalten – ein signifikanter Anstieg gegenüber weniger als 5 Prozent im Jahr 2025. Diese Entwicklung markiert einen Wendepunkt in der Enterprise-Software-Landschaft. Vor dem Hintergrund der beschleunigten digitalen Transformation werden agentenbasierte KI-Systeme weit über die individuelle Produktivitätssteigerung hinausgehen und durch intelligente Mensch-Agent-Interaktionen neue Maßstäbe für Prozessgestaltung setzen.

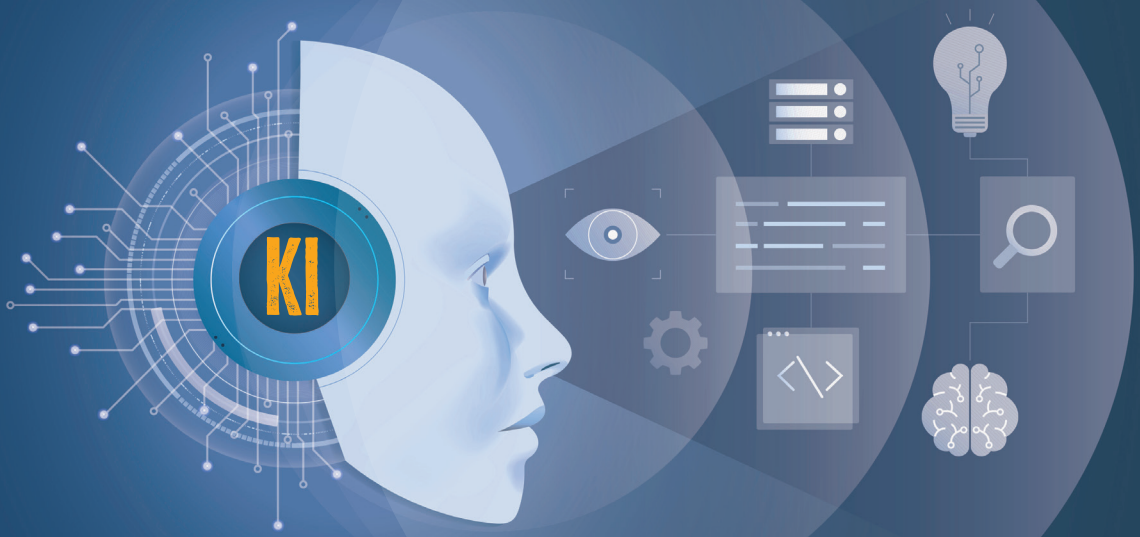
Gartner geht davon aus, dass agentenbasierte KI bis 2035 etwa 30 Prozent des weltweiten Umsatzes mit Unternehmenssoftware ausmachen wird – mehr als 450 Milliarden US-Dollar, verglichen mit nur 2 Prozent im Jahr 2025. „KI-Agenten entwickeln sich rasant weiter. Bis 2026 werden sie sich von einfachen, eingebetteten Assistenten hin zu aufgabenspezifischen Agenten wandeln und bis 2029 zu komplexen Multiagenten-Ökosystemen heranwachsen", erklärt Anushree Verma, Senior Director Analyst bei Gartner.

„Dieser Wandel transformiert Unternehmensanwendungen: von Werkzeugen zur Unterstützung der individuellen Produktivität hin zu Plattformen für autonome Zusammenarbeit und dynamische Workflow-Orchestrierung." CIOs müssen jetzt handeln: Ihnen bleiben zwischen drei und sechs Monaten, um eine fundierte Agentenstrategie zu entwickeln. Wer diese Frist versäumt, riskiert, im Wettbewerb ins Hintertreffen zu geraten. Eine erfolgreiche Umsetzung erfordert einen strategischen Ansatz über alle fünf Phasen der agentenbasierten KI hinweg.

www.gartner.com

DIE ZUKUNFT VON AGENTIC AI IN UNTERNEHMENSANWENDUNGEN

Entwicklungsstufen der KI-Agenten nach Gartner



(Quelle: Gartner)

2025
KI-Assistenten für jede Anwendung

2026
Aufgabenspezifische Agenten-Anwendungen

2027
Kollaborative KI-Agenten innerhalb einer Anwendung

2028
KI-Agenten-Ökosysteme über mehrere Anwendungen

2029
„New Normal" von Unternehmensanwendungen

IT-FACHKRÄFTEMANGEL

SITUATION WEITERHIN KRITISCH

In Deutschland fehlen aktuell 109.000 IT-Fachkräfte – weniger als 2023 (149.000), aber weiterhin problematisch. 85 Prozent der Unternehmen beklagen Fachkräftemangel, 79 Prozent erwarten eine weitere Verschärfung. Paradox: 6 Prozent entließen IT-Personal, 14 Prozent planen weitere Entlassungen, doch 52 Prozent hoffen auf bessere Recruiting-Chancen durch Stellenabbau anderswo.

KI als Chance und Risiko: 8 Prozent setzen KI gegen Fachkräftemangel ein. 27 Prozent erwarten Stellenabbau durch KI, aber 42 Prozent rechnen mit zusätzlichem Bedarf an IT-Experten. 24 Prozent befürchten, IT-Fachkräfte ohne KI-Wissen werden obsolet.

Rekrutierungshürden: Stellenbesetzung dauert 7,7 Monate. Hauptprobleme: überzogene Gehaltsvorstellungen (63%), fehlende Umzugsbereitschaft (44%), mangelnde Unternehmensflexibilität bei mobilem Arbeiten (43%). 25% erhalten keine Bewerbungen.

Quereinstieg wichtig: Nur 27 Prozent der Neueinstellungen haben IT-Studium, 37 Prozent duale Ausbildung, 27 Prozent sind Quereinsteiger. 14 Prozent rekrutieren im Ausland, 45 Prozent sehen US-Politik als Chance für internationale Fachkräfte.

Politische Forderungen: 74 Prozent wünschen wöchentliche statt tägliche Höchstarbeitszeit, 69 Prozent bessere Fachkräfteeinwanderung, 67 Prozent Aktiv-Rente.

www.bitkom.org

Mit neuer Strategie in die Zukunft

FIRMENENTWICKLUNG UND KÜNFTIGE WACHSTUMSPLÄNE

Der Karlsruher Telefonanlagen-Hersteller STARFACE steht 2025 vor dem vermutlich aufregendsten Jahr der Firmengeschichte: Genau zwanzig Jahre nach der Gründung wurde das Unternehmen vor wenigen Monaten durch die englische Gamma Group übernommen. Wir blicken mit dem alten und neuen Geschäftsführer Florian Buzin auf zwei Jahrzehnte TK-Geschichte zurück, und werfen einen Blick auf die Zukunft des UCC-Pioniers.

it management: *STARFACE hatte in diesem Jahr doppelt Grund zum Feiern – zum einen hinsichtlich des 20-jährigen Bestehens, zum anderen mit Blick auf die erfolgreiche Übernahme durch die Gamma Group. Ist es angemessen, vom Beginn und Ende einer Ära zu sprechen?*

Florian Buzin: Über den Beginn einer Ära können wir gerne sprechen – zwei Jahrzehnte STARFACE sind ein guter Grund, um auf unsere Anfänge und die prägenden Momente zurückzuschauen. Vom Ende einer Ära sollten wir aber höchstens im Sinne eines Meilensteins reden, den wir jetzt erfolgreich passiert haben – denn die Reise geht weiter! Unter dem Dach von Gamma stehen uns jetzt ganz neue Möglichkeiten offen, zu neuen, ehrgeizigeren Zielen aufzubrechen.

it management: *Dann beginnen wir doch am Anfang: Was gab seinerzeit den Anstoß zur Firmengründung?*

Florian Buzin: Um das zu verstehen, sollten wir kurz in das Jahr 2005 zurückreisen, eine Zeit, in der die Klapphandys noch Tasten hatten, wo es kein Youtube gab und das Internet Bit für Bit durch das 56K-Modem tröpfelte. In diesem Jahr kündigten die ersten deutschen Provider DSL 16000 an, und wir – das heißt: meine Mitgründerin Barbara Mauve und ich – kamen als Softwaredienstleister ins Grübeln: Welche aufregenden neuen Produkte würde diese unglaubliche Bandbreite ermöglichen? Unsere erste Idee verwarfen wir, die zweite nahm aber schnell konkrete Formen an, und reifte zum Entschluss, eine IP-basierte Telefonanlage zu programmieren.

> ICH WÜRDE DURCHAUS FÜR UNS BEANSPRUCHEN, DASS WIR DIE BRANCHE DURCH STÄNDIGE INNOVATION VERÄNDERT HABEN – HIN ZU EINER NEUEN EINFACHHEIT, KLARHEIT, BENUTZBARKEIT.
>
> **Florian Buzin, CEO und Geschäftsführer, STARFACE GmbH, Managing Director, Gamma Communications, www.starface.com**

it management: *War Telefonie damals nicht ein weitgehend gelöstes Problem?*

Florian Buzin: Nein! Telefonie war damals ein wirklich spannender Markt: Immerhin musste man für internationale Long Distance Calls noch richtig tief in

die Tasche greifen, VoIP versprach also, ein echter Gamechanger zu werden. Und auch die damals allgegenwärtigen ISDN-Anlagen waren ein echtes Ärgernis, das die meisten Firmen lieber früher als später ablösen wollten. Heute kann man sich das nicht mehr vorstellen, aber um seine Nebenstelle umzuleiten, brauchte man 2005 noch einen obskuren geheimen Code – etwas wie: Sternchen, Raute, Dollar-Zeichen, 2, 3, 1, 7. Unser Ziel war es, ein System zu entwickeln, das kinderleicht zu betreiben war – und die Komfort-Features von ISDN ohne Aufpreis unterstützte. Wir prägten dafür den Begriff „Comfortphoning", der uns seither begleitet.

it management: *Was waren denn die großen technischen Meilensteine in zwei Jahrzehnten STARFACE?*

Florian Buzin: Da gab es unzählige bemerkenswerte Lösungen. Die erste, die wir schon angesprochen haben, war die Entwicklung eigener, prinzipiell offener Hardware-Appliances mit standardmäßigen DSL-, ISDN- und Analog-Ports. Ein zweiter Meilenstein war der Wechsel von der reinen Desktop-Telefonie zum Softphone, und – ungefähr zur gleichen Zeit – der Ausbau der TK-Anlage zur UCC-Plattform für alle Kommunikationskanäle. Inklusive mobiler Clients für iPhone und Android, mit denen wir als erster deutscher TK-Anbieter Smartphones in vollwertige Nebenstellen der Telefonanlage verwandelt haben. Im nächsten Schritt ergänzten wir das Portfolio dann um unseren SIP-Trunk STARFACE Connect. Insgesamt würde ich also durchaus für uns beanspruchen, dass wir die Branche durch ständige Innovation verändert haben – hin zu einer neuen Einfachheit, Klarheit, Benutzbarkeit.

it management: *Und was waren die großen unternehmerischen Meilensteine?*

Florian Buzin: STARFACE ist ja als klassisches Bootstrapping-Projekt ohne Drittmittel gestartet, entwickelte sich aber sehr dynamisch, sodass wir nach kurzer Zeit einen Venture Capital-Geber gewannen, der dafür gesorgt hat, dass wir das Projekt zur Marktreife führen konnten. Allerdings fanden wir uns dann sehr schnell in einem reinen Verdrängungsmarkt wieder – denn jedes Unternehmen, mit dem wir sprachen, hatte schon eine Telefonanlage. Also haben wir uns aggressiv als Channel-only-Unternehmen positioniert, um unseren Footprint zu vergrößern, und jeden generierten Lead ohne Wenn und Aber an interessierte Systemhäuser weitergegeben. Dann haben wir diese konsequent zu ihren Kundenterminen begleitet. Dort haben wir gezeigt, was wir können – weg vom Sternchen-Code, hin zu einer zeitgemäßen Lösung – und hatten am Ende im besten Fall einen neuen Kunden und einen neuen Partner. Das war der Grundstein der STARFACE Community, die uns unglaublich engagiert und begeistert unterstützt – und einen Riesenanteil an unserem Erfolg hat.

it management: *Beste Voraussetzungen für weiteres Wachstum also?*

Florian Buzin: Ja, mit Unterstützung der Community konnten wir unsere Marktstellung rasch ausbauen und mehrere Finanzierungsrunden abschließen, die uns alle vorangebracht haben. Die wichtigste Weichenstellung war dann allerdings der Moment, in dem sich uns die Gelegenheit für einen Management Buyout bot. Wir haben die Chance ergriffen, und waren plötzlich wieder komplett eigenständig. Das war ein Riesenschritt, der unser Wachstum enorm beschleunigte.

it management: *Was dann wieder Investoren auf den Plan rief, richtig?*

Florian Buzin: Richtig – durch die geschäftlichen Erfolge, die wir im Nachlauf des Buyouts realisieren konnten, wurde der Private Equity Investor Maxburg auf uns aufmerksam. Das war eine weitere prägende Zusammenarbeit: In den fünf Jahren, die wir zusammenblieben, hat STARFACE zwei Firmen und eine technische Lösung zugekauft und ist unfassbar gewachsen – von 80 Mitarbeitern auf mehr als das Dreifache. Gleichzeitig haben wir auch beim Umsatz entsprechend zugelegt und viele Abläufe professionalisiert. Kurz: Wir sind eine ganz andere Firma geworden. Immer noch nahbar, immer noch eng mit den Partnern verbunden, aber mit einem ganz anderen Standing in der Branche. Es wurde Zeit für den nächsten großen Schritt.

it management: *Und damit schließt sich der Kreis zu Gamma?*

Florian Buzin: Genau. An dem Punkt, den wir erreicht hatten – STARFACE war als weithin sichtbare, angesehene Marke im deutschsprachigen Raum etabliert – gibt es realistisch nur zwei Möglichkeiten: Option eins war, dass wir ein börsennotiertes Unternehmen werden. Option zwei, von einem börsennotierten Unternehmen gekauft zu werden. Also machten wir uns aktiv auf die Suche nach

einem Partner, der uns beim nächsten Wachstumsschritt begleiten würde, und mit dem wir auch über den deutschen Tellerrand hinaus planen konnten. Und der Weg führte uns zu Gamma.

it management: *Bevor wir über die neue Eigentümerin reden, noch eine persönliche Frage: Wie schwer ist Ihnen als Gründer denn die Entscheidung gefallen, STARFACE zu verkaufen?*

Florian Buzin: Das Loslassen war eigentlich ganz einfach. Natürlich ist STARFACE mein Baby. Ich habe das Unternehmen mitgegründet, habe es 20 Jahre mitgeführt und ich habe beobachtet, wie es von sechs auf fast 300 Mitarbeiter gewachsen ist. So eine Company wächst einem selbstverständlich ans Herz. Aber die Übernahme durch ein börsennotiertes Unternehmen war ja lange Teil des Plans, und Gamma entsprach exakt unserem Wunschprofil. Also war es letztlich kein schwieriger Schritt.

it management: *Auch, weil Sie weiterhin Teil des Unternehmens bleiben?*

Florian Buzin: Natürlich, dass ich als Geschäftsführer von STARFACE und Gamma Deutschland an Bord bleiben kann, ist ein wichtiger Pluspunkt. Ich freue mich wahnsinnig darauf, die weitere Entwicklung mitzuverfolgen und mitzugestalten – zumal wir jetzt in ganz neue Sphären vorstoßen können.

it management: *Und warum ist Gamma so ein guter Kandidat?*

Florian Buzin: Gamma steht für ähnliche Werte wie STARFACE: Sie wollen ein innovatives, stark wachsendes Unternehmen sein, schätzen ihre Mitarbeiter und legen Wert auf einen respektvollen Umgang miteinander. Ob auf geschäftlicher, partnerschaftlicher oder Mitarbeiterebene – bei Gamma agiert man mit Anstand und auf Augenhöhe – das passt gut zu unserer Kultur. Das Team ist aber auch ähnlich ehrgeizig wie wir: Wir alle sind uns einig, dass wir uns nicht auf Dauer mit einem dritten oder vierten Rang begnügen werden, sondern ganz oben aufs Treppchen wollen und bereit sind, uns dafür ins Zeug zu legen. Auch da ist die DNA also sehr ähnlich.

it management: *Und welche Schritte folgen nun?*

Florian Buzin: Nun, Gamma hat mit den Übernahmen von HFO, Placetel und jetzt der STARFACE Group – zu der neben STARFACE auch estos gehört – ein starkes, strategisches Signal gesendet: Man hat dort den Anspruch, europaweit deutlich stärker zu werden. Deutschland, dem größten europäischen Markt, kommt dabei eine Schlüsselrolle zu. Insofern wird es hier neben organischem Wachstum sicher auch weiteres anorganisches Wachstum geben – wenn nicht dieses Jahr, dann nächstes.

Ein zweiter Punkt, der uns aktuell beschäftigt, ist die weitere Internationalisierung. Dass wir mit Gamma einen großen Schritt auf das europäische Parkett getan haben, ist für die Zukunft von STARFACE unglaublich wichtig. Durch Gamma haben wir jetzt einen ganzen anderen, größeren Hebel, um unsere Produkte auch in den Ländern, in denen Gamma heute bereits gesetzt ist, zu vermarkten.

it management: *Und wie reagiert die Community?*

Florian Buzin: Bis jetzt wurde die Übernahme überall sehr positiv aufgenommen. Trotzdem sind die Partner natürlich extrem gespannt. Aber sie werden nicht mehr lange auf ihre Antworten warten müssen: Am 24. und 25. September veranstalten STARFACE und estos die jährliche Com.vention im Europa-Park Rust, und dort werden wir der Community einen detaillierten Ausblick auf die Roadmap der nächsten Monate geben können. Das ist ein Termin, auf den wir uns alle sehr freuen – nicht zuletzt, weil die Com.vention schon lange kein reines STARFACE- und estos-Event mehr ist, sondern wirklich die gesamte Branche versammelt – im wahrsten Sinne des Wortes eine große Bühne.

it management: *Herr Buzin, wir danken Ihnen für dieses Gespräch.*

DATENVISUALISIERUNG MIT MICROSOFT POWER BI

DER SCHNELLE EINSTIEG IN DIE WELT VON POWER BI

Visualisieren Sie Ihre Daten schnell, intelligent und ausdrucksstark mit Power BI, um praktisch umsetzbare Ergebnisse zu erhalten.

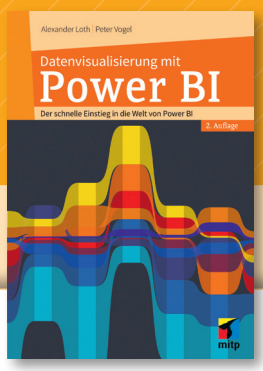
Alexander Loth und Peter Vogel zeigen Ihnen Schritt für Schritt, wie Sie ganz einfach visuelle Analysen erstellen und so selbst komplexe Datenstrukturen verstehen sowie gewonnene Erkenntnisse effektiv kommunizieren können.

Das Buch richtet sich an die folgenden Zielgruppen:

- Alle, die Zugang zu Daten haben und diese verstehen möchten
- Führungskräfte, die Entscheidungen auf Grundlage von Daten treffen
- Analysten und Entwickler, die Visualisierungen und Dashboards erstellen
- angehende Data Scientists

Zum Verständnis dieses Buches und dem Erwerb von Power BI-Kenntnissen sind weder besondere mathematische Fähigkeiten noch Programmiererfahrung nötig. Durch die Integration von Copilot wird der Einstieg sogar noch einfacher, da Sie viele Aufgaben durch einfache Anweisungen in natürlicher Sprache erledigen können. Es eignet sich daher auch für Einsteiger und Anwender, die sich dem Thema Datenvisualisierung und -analyse praxisbezogen nähern möchten, ohne ausschweifende theoretische Abhandlungen.

Die grundlegenden Funktionen von Power BI werden Schritt für Schritt erläutert und Sie lernen, welche Visualisierungsmöglichkeiten wann sinnvoll sind. Die Autoren zeigen Fallbeispiele auf, die weit über eine »Standardanalyse« hinausreichen und gehen auf Funktionen ein, die selbst erfahrenen Nutzern oft nicht hinlänglich bekannt sind. Sie geben Ihnen außerdem wertvolle Hinweise und Tipps, die das Arbeiten mit Power BI merklich erleichtern. So können Sie zukünftig Ihre eigenen Daten bestmöglich visualisieren und analysieren.



Datenvisualisierung mit Microsoft Power BI –
Der schnelle Einstieg in die Welt von Power BI;
Alexander Loth, Peter Vogel;
mitp Verlags GmbH & Co.KG; 11-2025

live
WEBINAR
AM 16.10.2025
UM 10 UHR

HYBRIDES UEM

EFFIZIENZSTEIGERUNG IN KOMPLEXEN IT-UMGEBUNGEN

Der Sprecher
Sebastian Weber,
Chief Evangelist

Sebastian Weber ist Chief Evangelist bei der Aagon GmbH in Soest. Er ist als Experte für Client- und Unified-Endpoint-Management-Systeme sowohl von Aagon-Kunden und -Partnern als auch von Medien häufig zu aktuellen unternehmensrelevanten IT-Themen gefragt.

In einer zunehmend hybriden IT-Landschaft stehen Unternehmen vor der Herausforderung, ihre Geräteverwaltung effizient und übersichtlich zu gestalten. Die Vielfalt an Managementlösungen – insbesondere bei der Integration von Cloud- und On-Premises-Systemen – führt häufig zu einem unübersichtlichen Konsolen-Dschungel. Administratoren jonglieren mit mehreren Oberflächen, um ihre Geräte zu verwalten, Sicherheitsrichtlinien anzupassen und Compliance-Vorgaben zu erfüllen.

Dieser komplexe Ansatz kostet Zeit, bindet Ressourcen und erhöht das Fehlerrisiko.
Genau hier setzt hybrides UEM an: Es vereint die Flexibilität moderner Cloud-Lösungen mit der Kontrolle traditioneller On-Premises-Systeme in einer einzigen, übersichtlichen Oberfläche. Dadurch wird nicht nur die Verwaltung effizienter, sondern auch die Sicherheit gesteigert. Statt sich durch bis zu acht verschiedene Intune-Konsolen zu kämpfen, haben Administratoren mit einem hybriden UEM einen zentralen Zugangspunkt, der alle wesentlichen Funktionen vereint.

Dieser Vortrag richtet sich an IT-Entscheider, Administratoren und alle, die den Spagat zwischen Flexibilität und Kontrolle effizient meistern wollen.

Warum Sie unbedingt dabei sein sollen? Sie erfahren:

- Praxisnahe und verständliche Erklärung wie Unternehmen von der Vereinheitlichung profitieren können und somit die tägliche Arbeit deutlich vereinfacht wird
- Reale Szenarien, wie die Zusammenführung von Microsoft Intune und klassischen On-Premises-Umgebungen gelingt
- Direkter Mehrwert durch ACMP Live-Demo, die zeigt wie mit einer einzigen Konsole die Kontrolle behalten und die Flexibilität genutzt werden kann

Erleben Sie live, wie Sie den Konsolen-Dschungel hinter sich lassen können. Live am 16.10.2025 – **jetzt anmelden!**

GEWINNER ODER GETRIEBENE?

Je mehr wir digitalisieren, desto abhängiger werden wir von externen Akteuren und deren Infrastrukturen. Jeder Algorithmus, jede Cloud-Lösung und jede digitale Plattform schafft potenzielle Abhängigkeiten, die in Krisenzeiten zur existenziellen Bedrohung werden können.

Parallel dazu verspricht Künstliche Intelligenz Effizienzgewinne und neue Geschäftsmodelle. Dabei übersehen viele eine kritische Schwachstelle: KI-Systeme sind nur so stark wie ihre Datengrundlage. Mangelhafte Daten schaffen eine doppelte Abhängigkeit, von externen Anbietern und fehlerhaften Informationen.

Werden europäische Unternehmen zu Gewinnern oder Getriebenen dieser Transformation? Schaffen wir es, sowohl die Innovationskraft neuer Technologien zu nutzen als auch unsere digitale Selbstbestimmung und Datenhoheit zu bewahren?

Gemeinsam stark für europäische Sicherheit

WIE DRIVELOCK STRATEGISCHE PARTNERSCHAFTEN UND PLATTFORMARCHITEKTUR FÜR DIGITALE SOUVERÄNITÄT NUTZT

Europa steht am Scheideweg. In einer Zeit geopolitischer Anspannung, digitaler Abhängigkeiten und wachsenden regulatorischen Drucks wird eines immer klarer: Die Fähigkeit, digitale Systeme zu gestalten, zu steuern und zu schützen, ist zur Voraussetzung für wirtschaftliche, politische und gesellschaftliche Handlungsfähigkeit geworden. Dabei ist die Integration mit europäischen Partnern ein wichtiger Schlüssel zum Erfolg. „Digitale Souveränität" ist dabei weit mehr als ein politisches Schlagwort. Das Management von Interdependenzen ist für Behörden, Unternehmen und kritische Infrastrukturen ein operatives Erfordernis.

Doch wer Souveränität will, muss zuerst Resilienz ermöglichen. Und das mit Tempo, Wirkung und Pragmatismus. Genau hier setzt die DriveLock HYPERSECURE Platform an. Gemeinsam mit strategischen Partnern wie idgard, mit dem DriveLock eine Ende-zu-Ende-Härtung für besonders schützenswerte Daten realisiert, schafft das Unternehmen ein neues Modell europäischer IT-Sicherheit: plattformbasiert. Partnergetrieben. Prinzipiengeleitet.

Souveränität beginnt mit Gestaltungskraft

Digitale Souveränität bedeutet, selbst darüber entscheiden zu können, wie Schutzmaßnahmen gestaltet, umgesetzt und betrieben werden. Sie verlangt Unabhängigkeit, aber keine Isolation. Sie setzt Vertrauen voraus. In Technologie, in Organisationen und in Partnerschaften. In diesem Spannungsfeld entwickelt sich DriveLock zu einem Schlüsselakteur der europäischen Sicherheitsarchitektur.

EUROPÄISCHE RESILIENZ BRAUCHT SOUVERÄNE PLATTFORMEN UND VERTRAUENSWÜRDIGE PARTNER.

Dr. Philipp S. Müller, Vice President Public Sector, DriveLock SE, www.drivelock.com

Mit der HYPERSECURE Platform verfolgt das Unternehmen das Prinzip „eine Plattform, eine Konsole, ein Agent". Die Plattform ist konsequent entlang der vier kritischen Schnittstellen digitaler Organisationen aufgebaut. Menschen, Geräte, Applikationen und Daten. Sie beantwortet auch zwei zentrale Fragen jeder souveränen Sicherheitsarchitektur:

#1 Wie schnell und effektiv kann ich meine Systeme härten?

#2 Wie umfassend und aktuell ist mein Lagebild?

Der DriveLock-Kompass: Sicherheit strategisch denken

Um Organisationen bei dieser Aufgabenstellung zu unterstützen, hat DriveLock den DriveLock-Kompass entwickelt. Er strukturiert Sicherheitsentscheidungen entlang vier Achsen:

- **Souveräne Sicherheit:** Technische und organisatorische Resilienz gegen externe und interne Bedrohungen
- **Managebarkeit:** Einfache Steuerbarkeit, Skalierbarkeit und Auditierbarkeit der Sicherheitsarchitektur
- **Usability:** Nutzerfreundlichkeit und Akzeptanz im Arbeitsalltag
- **Kosten & Wertbeitrag:** Total Cost of Ownership und Return on Mitigation

Dieser Kompass hilft CIOs und CISOs dabei, komplexe Sicherheitsarchitekturen nicht nur technisch, sondern strategisch zu bewerten, etwa im Abwägungsprozess zwischen unterschiedlichen Sicherheitslösungen.

Härtung entlang der vier Dimensionen

Menschen: Der Mensch ist weiterhin Einfallstor Nr. 1 für Cyberangriffe. DriveLock setzt auf verhaltensbasierte Awareness und Human Risk Assessments, die situativ in den Arbeitsalltag eingebettet sind, unterstützt durch den Endpoint-Agenten.

Geräte: Jedes Endgerät ist heute ein potenzieller Angriffsvektor. Mit Device Control, BitLocker-Management und USB-Verschlüsselung schafft DriveLock Schutzmaßnahmen direkt am Gerät.

Applikationen: Application Control mit robustem Whitelisting verhindert das Einschleusen unerwünschter Software und reduziert Angriffsflächen. In Verbindung mit Device Control ergibt sich das bewährte AC/DC-Modell für präventive Endpunktsicherheit.

Daten: Sensible Daten verdienen besonderen Schutz. Hier setzt DriveLock auf die Lösungen seiner Tochterfirma idgard, dem Anbieter von hochsicherem, DSGVO-konformen Datenaustausch auf Basis der Sealed Cloud. Gemeinsam werden Lösungen realisiert, die bereits heute in Ministerien und Behörden im Einsatz sind, etwa als SecureBox Bayern.

Partnerschaft mit Wirkung: DriveLock & idgard

Die Kooperation und Integration mit idgard zeigt exemplarisch, dass technologische Exzellenz und europäische Werte Hand in Hand gehen können. So hat idgard beispielsweise in enger Zusammenarbeit mit dem Bayerischen LSI und dem IT-DLZ Bayern die SecureBox Bayern (SBB) entwickelt: eine cloudbasierte, sichere File-Sharing-Lösung, die rechtlich und operativ souverän ist und sich gleichzeitig einfach für alle Verwaltungsorganisationen skalieren lässt.

Der nächste logische Schritt für einen ganzheitlichen Schutz ist der Schutz des Zugangs in die Cloud durch die DriveLock Security Controls, wo Menschen an Geräten, in Applikationen und an Daten arbeiten. Solche Partnerschaften sind mehr als nur technische Integrationen. Sie sind der institutionelle Ausdruck gemeinsamer europäischer Resilienz.

Architektur, die mitwächst

DriveLock bietet keine punktuelle Sicherheitsmaßnahme, sondern ein skalierbares Modell für einen effektiven Resilienzaufbau in Unternehmen:

- In großen Organisationen können zentrale IT-Stellen den Rollout steuern, ohne lokale Flexibilität zu verlieren.

- In der öffentlichen Verwaltung kann sie als Rückgrat eines Cyber Defense Centers fungieren, wo die DriveLock Services an bestehende Systeme (z. B. SOCs) andocken.

Ein Vorschlag, der aktuell oft diskutiert wird, denkt diese Idee weiter: Ein von mehreren Verwaltungsebenen gemeinsam getragenes Produkt für den digitalen Verwaltungsarbeitsplatz, das Geräte, Menschen, Anwendungen und Daten entlang einer gemeinsamen Plattformlogik schützt.

Fazit

Europa kann Resilienz nicht zentral verordnen, aber es kann sie vernetzt aufbauen. Das erfordert Plattformen, die mit den Menschen und Institutionen arbeiten, nicht gegen sie. Es braucht Partner, die in europäischen Werten verankert sind, aber technologisch global wettbewerbsfähig bleiben.

Die strategische Allianz von DriveLock und idgard zeigt, wie dies gelingen kann. Was als technische Plattform beginnt, wird zum politischen Werkzeug: für mehr digitale Eigenständigkeit, für stärkere Sicherheitsarchitekturen und für ein Europa, das sich im digitalen Raum nicht nur behauptet, sondern gestaltet.

Dr. Philipp S. Müller

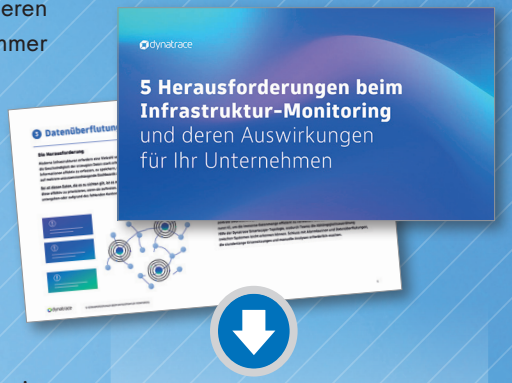
INFRASTRUKTUR-MONITORING NEU GEDACHT

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

Die Basis für erfolgreiche KI

WARUM SAUBERE DATEN DER ENTSCHEIDENDE ERFOLGSFAKTOR FÜR KI-PROJEKTE SIND

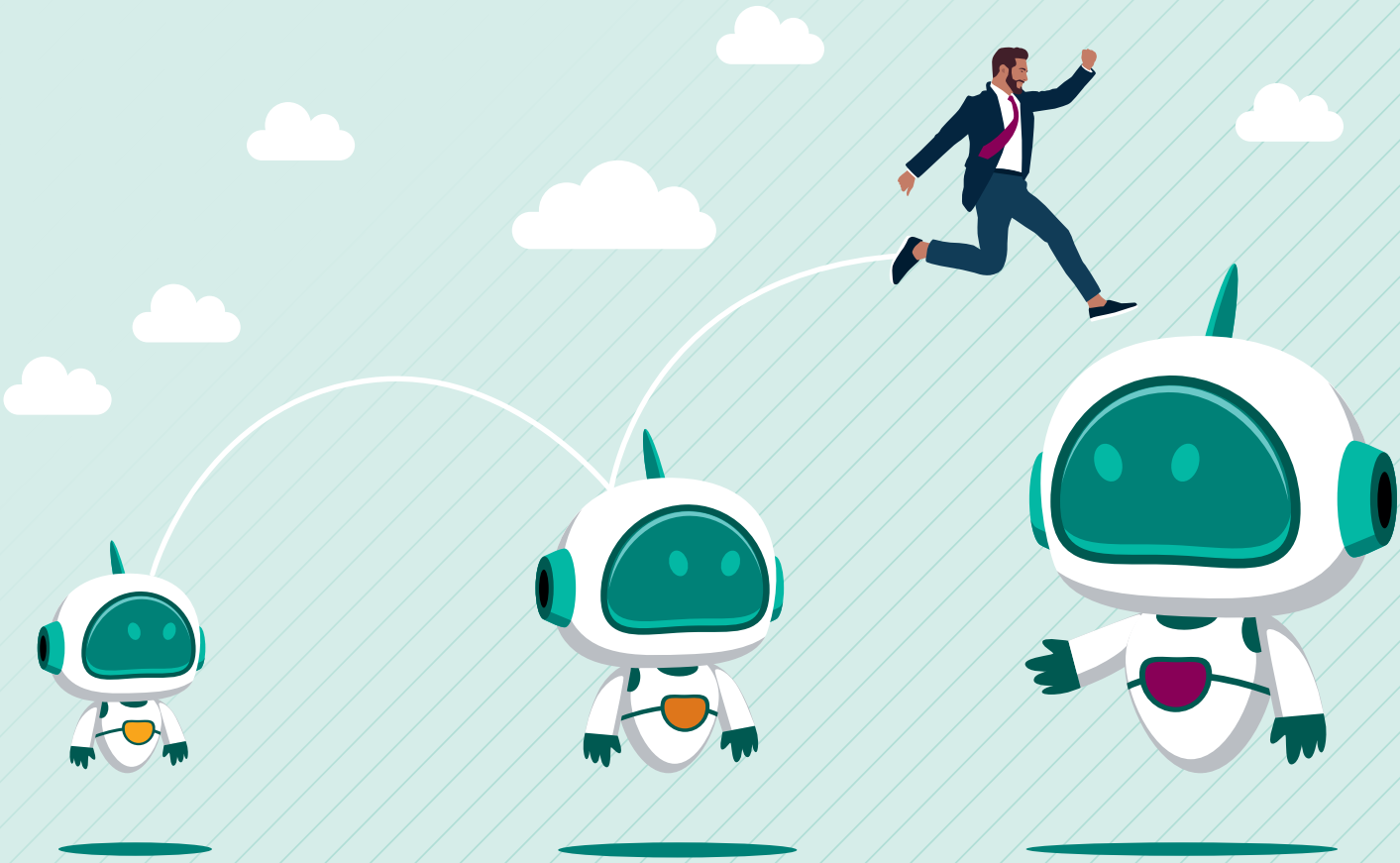
Die aktuell stattfindenden IT-Transformationen sind von einem klaren Trend geprägt: dem Einsatz künstlicher Intelligenz (KI). Diese ist nicht länger Zukunftsmusik, sondern inzwischen ein wichtiger Treiber digitaler Veränderung. Im Rahmen einer von Natuvion und NTT Data Business Solutions umgesetzten Studie zur IT-Transformation, nennen knapp 57 Prozent der Unternehmen die Einführung moderner Technologien, wie beispielsweise KI, als Hauptmotiv für ihr Transformationsvorhaben – ein Rekordwert, der die Richtung vorgibt.

Wer langfristig wettbewerbsfähig bleiben will, investiert besser heute als morgen in KI-basierte Systeme und Prozesse. Doch je stärker KI zur strategischen Zielsetzung wird, desto deutlicher zeigt sich eine zentrale Schwäche: Die Leistungsfähigkeit von KI ist unmittelbar abhängig von der Qualität der verfügbaren Daten. Genau hier klafft eine gefährliche Lücke.

Ohne saubere Daten keine intelligente Entscheidung

KI lebt von Daten – nicht nur hinsichtlich der Quantität, sondern vor allem in Bezug auf deren Qualität. Damit sich die Wirkungskraft von KI voll entfalten kann, braucht es strukturierte, konsistente und zugängliche Informationen. Nur so lassen sich fundierte Analysen durchführen, Automatisierungspotenziale ausschöpfen oder realistische Prognosen treffen. Doch die Realität ist in vielen Unternehmen eine andere. Sie ist geprägt von unvollständigen, inkonsistenten, oder redundanten Daten, Dubletten, Medienbrüchen und fragmentierten Systemlandschaften, die das Potenzial von KI bestenfalls begrenzen, schlimmstenfalls aber sogar in die falsche Richtung lenken.

47 Prozent der im Rahmen der IT-Transformationsstudie 2025 befragten Unternehmen sehen die mangelhafte Datenqualität als größte Hürde ihrer Transformationsprojekte. Damit steht dieses Thema zum vierten Mal in Folge unter den Top drei der größten Herausforderungen –



dieses Jahr sogar auf Platz eins. Vor allem größere Unternehmen oder Konzerne haben hier strukturelle Defizite, denn ihre komplexen Systemlandschaften und historisch gewachsenen Datenbestände erschweren die nachhaltige Bereinigung der Ausgangsdaten.

Die Unvereinbarkeit dieser Aspekte und das sich daraus ergebende Spannungsfeld ist offensichtlich: Unternehmen setzen zwar auf KI und investieren in diese Technologie, liefern den Systemen aber keine verlässliche Datenbasis. So wird aus einem ambitioniert gestarteten Digitalisierungsprojekt oft nur eine digitalisierte Ineffizienz.

KI-Investitionen setzen Data Readiness voraus

Wer die Möglichkeiten von KI wirklich nutzen will, muss deshalb zuerst die Grundlage schaffen. Das bedeutet, Datenbestände müssen geprüft, bereinigt, vereinheitlicht und so aufbereitet werden, dass sie sich strategisch managen lassen. Genau an dieser Stelle verbirgt sich ein Schlüsselfaktor für die erfolgreiche Umsetzung eines Transformationsprojekts: In der Studie gaben 43 Prozent der Unternehmen an, dass Housekeeping-Aktivitäten, wie etwa Bestandsanalysen und Readiness-Checks, entscheidend für den Erfolg ihrer Transformation waren.

Nicht ohne Grund rangiert die „Analyse der bestehenden IT-Landschaft" mit 38,6 Prozent auf Platz 1 der größten Planungshürden. Diese Zahlen zeigen: Die Qualität der Vorbereitung entscheidet maßgeblich über den Output und damit auch über die Qualität von KI-Systemen. Unternehmen, die in diese Basisarbeit Zeit, Manpower und strategische Überlegungen investieren, erreichen signifikant häufiger ihre Transformationsziele – insbesondere dann, wenn KI bereits im Rahmen des Transformationsprojekts selbst eine Rolle spielt. Fest steht: Nur wer weiß, welche Daten in welchem Zustand vorhanden sind, kann diese sinnvoll in Machine-Learning-Prozesse überführen und verlässliche Ergebnisse erzielen.

WER LANGFRISTIG WETTBEWERBSFÄHIG BLEIBEN WILL, INVESTIERT BESSER HEUTE ALS MORGEN IN KI-BASIERTE SYSTEME UND PROZESSE.

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

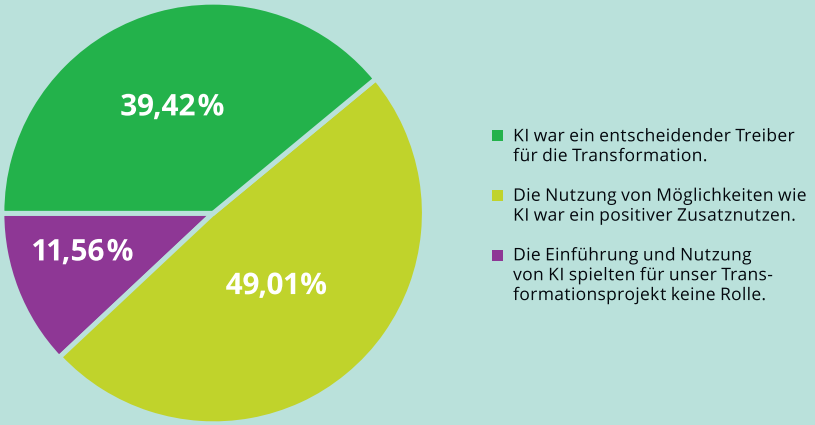
Die Cloud kann KI-Innovationen erleichtern

Ein weiteres zentrales Ergebnis der Studie: Fast die Hälfte der Unternehmen nutzt vermehrt Cloud-Plattformen, um einen schnellen und unkomplizierten Zugang zu KI-Innovationen zu erhalten. Das unterstreicht, dass die Cloud als Enabler gesehen wird. Das löst zwar Technologieprobleme, behebt aber keine Datenmängel. Im Gegenteil, wer fehlerhafte oder falsche Daten migriert beziehungsweise transformiert, dem kann das teuer zu stehen kommen – nicht nur weil unnötige Kosten anfallen, sondern auch, weil diese Daten potenzielle Fehlerquellen mit sich bringen.

Wer also glaubt, durch den Plattformwechsel in die Cloud automatisch KI-ready zu sein, unterschätzt die Komplexität der Anforderungen. Eine strategische Datenbereinigung ist keine Kür, sondern zählt zum Pflichtprogramm beim Umstieg auf ein neues System. Erst dann kann im nächsten Schritt die KI im Cloud-Umfeld ihre volle Wirkung entfalten und das Unternehmen auf das nächste Digitalisierungslevel heben.

So leistungsfähig KI auch ist, sie verändert Arbeitsabläufe, Rollenbilder und Entscheidungsketten. Diese Veränderungen erzeugen Unsicherheit, besonders dann, wenn die Ergebnisse der Systeme nicht nachvollziehbar sind oder wenig vertrauenswürdig erscheinen. Und auch das ist eine Frage der Datenqualität: Je verlässlicher, transparenter und erklärbarer die

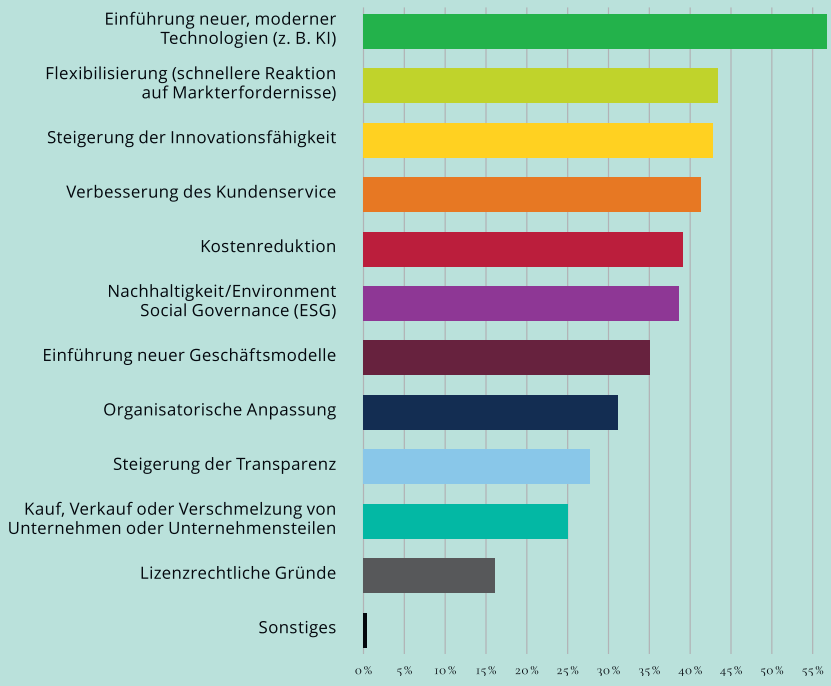
WELCHE ROLLE HAT DIE EINFÜHRUNG UND NUTZUNG VON KÜNSTLICHER INTELLIGENZ (KI) IN IHREM TRANSFORMATIONSPROJEKT GESPIELT?



Datenbasis ist, desto größer ist die Nachvollziehbarkeit und das Vertrauen in KI-gestützte Entscheidungen.

Deshalb rückt auch die Kommunikation als Change-Faktor zunehmend in den Fokus. In der aktuellen IT-Transformationsstudie rangieren Maßnahmen wie „Kommunikationswege etablieren" oder „Bereichsübergreifende Abstimmung" ganz oben auf den To-do-Listen der Unternehmen. Auf die Frage, was sie beim nächsten Mal anders machen würden, steht „bessere Kommunikation mit Abteilungen" mit 35,2 Prozent unangefochten auf dem ersten Platz.

WARUM WURDE DER TRANSFORMATIONSPROZESS IN IHREM UNTERNEHMEN GESTARTET?



IT-Transformation im Spannungsfeld

Gerade mit Blick auf die Datenqualität wundert es nicht, dass insbesondere Projekte mit hohem KI-Anteil häufig als Greenfield-Projekte aufgesetzt werden. Das Ziel: sich von den Altlasten lösen. Doch ein solcher Neustart hat durchaus seinen Preis wie die aktuellen Zahlen zeigen. Nur die Hälfte der Greenfield-Vorhaben bleiben im geplanten Budget und 63 Prozent müssen den Go-live verschieben. Besonders kritisch wird es, wenn darüber hinaus noch ein Anbieterwechsel vorgenommen wird. Dann treten Budgetüberschreitungen von über 30 Prozent drei Mal so häufig auf wie bei denjenigen, die bei ihrem ERP-Anbieter bleiben. Sprich, wer neu anfängt, benötigt ein tiefes Verständnis von der eigenen Datenstruktur sowie eine klare Vorstellung von der eigenen Governance-Strategie – anderenfalls wird aus der „grünen Wiese" schnell ein Minenfeld.

Die IT-Transformationsstudie 2025 macht deutlich: Wer das Ziel KI erreichen möchte, benötigt auf dem Weg dorthin bestmögliche Datenqualität. Ohne eine saubere, integrierte und gepflegte Datenbasis besteht nicht nur die Gefahr, dass das KI-Projekt floppt, sondern auch dass viel Geld ohne Nutzen investiert wird. Technologie allein reicht also nicht für eine erfolgreiche IT-Transformation. Die Systempflege muss stimmen. Die Analyse muss auf verlässlichen Informationen beruhen. Der Wandel braucht Rückhalt im gesamten Unternehmen. Und: Die Daten müssen für heutige und künftige KI-Anwendungen geeignet sein.

Patric Dahse

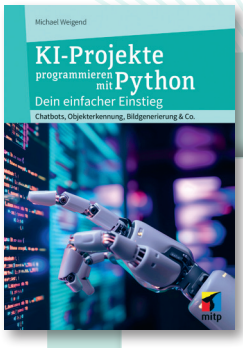
KI-PROJEKTE PROGRAMMIEREN MIT PYTHON

DER EINFACHE EINSTIEG

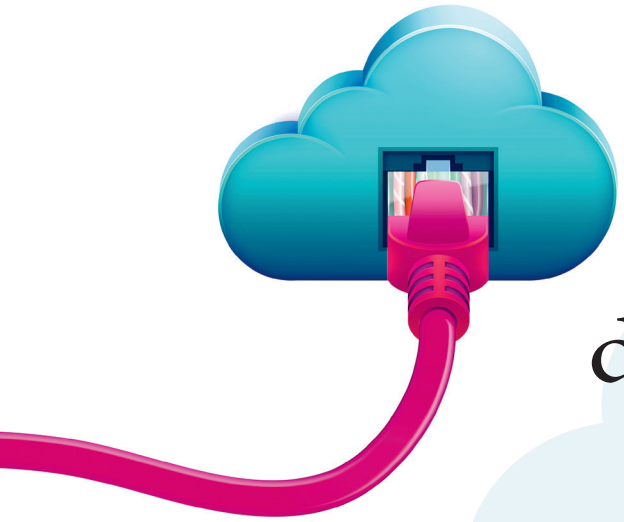
Mit diesem Buch startest du direkt durch: Du lernst künstliche Intelligenz, indem du selbst programmierst – praxisnah, kreativ und verständlich. Schritt für Schritt entwickelst du spannende KI-Anwendungen mit wenigen Codezeilen: vom Chatbot über Bilderkennung bis hin zur Musik- und Bildgenerierung. Du experimentierst mit maschinellem Lernen und verstehst, wie lernende Systeme wirklich funktionieren. Alles, was du brauchst, sind grundlegende Programmierkenntnisse.

Alles dabei – von den Python-Grundlagen bis zu modernen KI-Bibliotheken
Dank klarer Erklärungen und anschaulicher Beispiele findest du dich auch als Einsteiger schnell zurecht. Du lernst alle wichtigen Techniken kennen und setzt sie direkt um – von einfachen Klassifikationsmodellen bis hin zu generativer KI mit GANs, RNNs und Diffusionsmodellen. Dabei nutzt du professionelle Bibliotheken wie NumPy, TensorFlow, Matplotlib, SpaCy und music21.

Programmieren, verstehen, experimentieren
Jedes Kapitel lädt zum Mitmachen ein – mit abwechslungsreichen Aufgaben, anschaulichen Abbildungen und vielen Ideen zum Ausprobieren. Du lernst, wie du KIs mit eigenen Daten trainierst oder Daten aus dem Internet nutzt, um spannende Anwendungen zu entwickeln. Die Programme kannst du entweder lokal auf deinem Rechner umsetzen oder du arbeitest im Browser mit Google Colab.



KI-Projekte programmieren mit Phython –
Der einfache Einstieg,
Michael Weigend,
mitp Verlags GmbH & Co.KG,
10-2025



Augen auf bei der Auswahl des Cloud-Anbieters!

WAS IT-ENTSCHEIDER BEI UCC-ANBIETERN WISSEN MÜSSEN

Ein ständig wachsender Anteil an Unternehmen vertraut ihre Business-Kommunikation Cloud-basierten UCC-Plattformen und Telefonanlagen an. Bei der Auswahl des passenden Anbieters sollten Unternehmen nicht nur auf die angebotene Feature-Palette achten, sondern ganz konkret abfragen: wie hoch ist wirklich die Verfügbarkeit des Anbieters? Wie gut ist die Sprachqualität? Thomas Weiß, CTO bei STARFACE, sieht in dieser Hinsicht die Rechenzentren der UCC-Anbieter im Fokus und erläutert im Interview die wichtigsten Kriterien und Kennzahlen, mit denen sich die Qualität der Rechenzentren als Basis der UCC-Kommunikation bewerten lässt.

it management: *Herr Weiß, die heutige Business-Kommunikation nutzt eine Vielzahl an Kommunikationskanälen, gerade in großen Unternehmen mit verteilten Standorten. Wo sehen Sie hier die größten technischen Herausforderungen?*

Thomas Weiß: Egal ob Mail, Chat, Shared Documents, Telefon oder Videoconferencing – die Kommunikation in Echtzeit ist für unser Arbeitsleben zentral und kritisch. Gleichzeitig sind die technischen Anforderungen für diese Echtzeitkommunikation gestiegen: Für die Calls ihrer Angestellten brauchen Unternehmen nun mal genügend Bandbreite sowie niedrige Latenzen und Jitter – sonst ist der Ton abgehackt oder das Bild friert ein. Es kommt zu Frust bei den Anwesenden, im Worst Case passiert dies während eines wichtigen Kundentermins.

it management: *Ist Sprachbasierte Kommunikation für Sie der kritischste Bereich bei den Qualitätsanforderungen?*

Thomas Weiß: Absolut! Wenn es wirklich wichtig wird, greift man zum Hörer oder vereinbart einen Video-Call. Daher sind diese Kanäle auch die beiden kritischsten im Hinblick auf ausreichende technische Ressourcen und einen reibungslosen Betrieb. Aber auch die anderen UCC-Tools sind natürlich von einer reibungslos funktionierenden Infrastruktur abhängig.

it management: *Worauf sollten Unternehmen bei der Auswahl der Infrastruktur für ihre UCC-Lösungen achten?*

Thomas Weiß: UCC ist heutzutage Cloud-basiert, und wie performant oder verfügbar diese UCC-Clouds sind, hängt zu großen Teilen von den Rechenzentren ab, in denen sie gehostet werden. Der Betrieb eigener Rechenzentren ist in den seltensten Fällen betriebswirtschaftlich vernünftig. Also nutzen Unternehmen dafür die Datacenter der UCC-Anbieter. Doch genau hier ist Vorsicht geboten: Wer erstklassige Audio- und Videoqualität mit geringen Übertragungsstörungen haben möchte, hat bei der Auswahl einiges zu beachten.

it management: *Was genau muss beachtet werden?*

Thomas Weiß: Da wäre etwa das Problem der ‚lauten Nachbarn'. Gerade bei Anbietern von Public Clouds teilen Sie sich die Infrastruktur mit anderen Unternehmen. Als laute Nachbarn bezeichnet man die anderen Cloud-Dienste im gleichen Rechenzentrum, die die vorhandene Bandbreite und Rechenleistung ebenfalls für sich beanspruchen. Hier sind gerade rechenintensive Backup-Prozesse zu Spitzenzeiten ein Kapazitäts-Problem. Das eigene Mailprogramm leidet darunter nicht merklich, die Sprach- und Videoqualität meiner UCC-Lösung oder Cloud-PBX aber sehr wohl. Stellen Sie sich jetzt noch vor, ein ‚benachbartes' Unternehmen wird Opfer eines DDoS-Angriffs: Dann bin ich -obwohl selbst nicht das Ziel- in meiner Kommunikation blockiert oder zumindest stark eingeschränkt.

it management: *Unternehmen sollten ihre Infrastruktur folglich so wählen, dass die ‚Nachbarn' keinen Einfluss auf sie haben.*

Thomas Weiß: Richtig! Für performante und hochverfügbare Audio- und Videoqualität sind die Datacenter-Strukturen von anderen Nutzern komplett zu isolieren. Dafür braucht es getrennte Netze und separate, exklusiv für den UCC-Dienst reservierte Core-Switches. Die Basis dabei ist eine saubere Konfiguration. Das gilt für den Hypervisor (eine Software oder Firmware, die es ermöglicht, mehrere virtuelle Maschinen (VMs) auf einem einzigen physischen Computer zu betreiben) und auch für die Architektur an sich: Compute Nodes müssen klar von den Speicherknoten getrennt werden. Sämtliche Daten sind auf drei ver-

schiedenen Servern zu speichern, um für Ausfälle gerüstet zu sein.

it management: *Das ist aber mehr als Isolierung...*

Thomas Weiß: In der Tat! Auch die Redundanz ist ein entscheidender Faktor für zuverlässige UCC-Kommunikation. Neben einer Datenreplikation auf verschiedenen Servern sollten mindestens zwei Rechenzentren redundant geschaltet sein. Was hier meist vergessen wird: Diese Rechenzentren sollten sich in jeder Hinsicht voneinander unterscheiden, nicht nur beim Standort. Neben einem anderen Betreiber gilt dies vor allem für den technologischen Unterbau, also sämtliche Hard- und Softwarekomponenten.

it management: *Das klingt auf den ersten Blick übertrieben.*

Thomas Weiß: Aber nur so lassen sich Single Points of Failure vermeiden! Es gab durchaus schon Fälle, in denen zwei redundante Rechenzentren durch Probleme bei einer einzigen, in beiden Zentren eingesetzten Software-Lösung ausgefallen sind. Nur UCC-Cloud-Provider, die hier auf jedes Detail achten, schaffen Vertrauen beim Kunden. Überspitzt formuliert: Das Datacenter wird zum Spiegel der Service-Qualität insgesamt – natürlich muss auch die Performance stimmen.

it management: *Welche Netzwerkanforderungen stellt UCC denn konkret an ein Rechenzentrum?*

DAS DATACENTER WIRD ZUM SPIEGEL DER SERVICE-QUALITÄT INSGESAMT – NATÜRLICH MUSS AUCH DIE PERFORMANCE STIMMEN.

Thomas Weiß, CTO, STARFACE GmbH, www.starface.com

Thomas Weiß: UCC benötigt weitaus mehr Bandbreite als die klassischen IT-Dienste. Um jederzeit eine stabile Voice- und Videoübertragung sicherzustellen, sollten beim Uplink 100 Gigabyte pro Sekunde möglich sein. Landläufig gelten innerhalb eines Rechenzentrums bei der Vernetzung von Server- und Storage-Systemen schon 10 Gigabyte als Standard, doch ist dies eigentlich zu wenig. Hier empfiehlt sich eine mehrfache Serveranbindung mit zwei 10GB-Leitungen für Backups und ähnliche Prozesse, während der permanente Daten-Traffic über zwei leistungsstarke 25GB-Leitungen fließt. Erst eine derartige Switching-Architektur mit deutlich höherer Datenrate beschleunigt die Übertragung, verringert die Latenzen und ist wesentlich zuverlässiger.

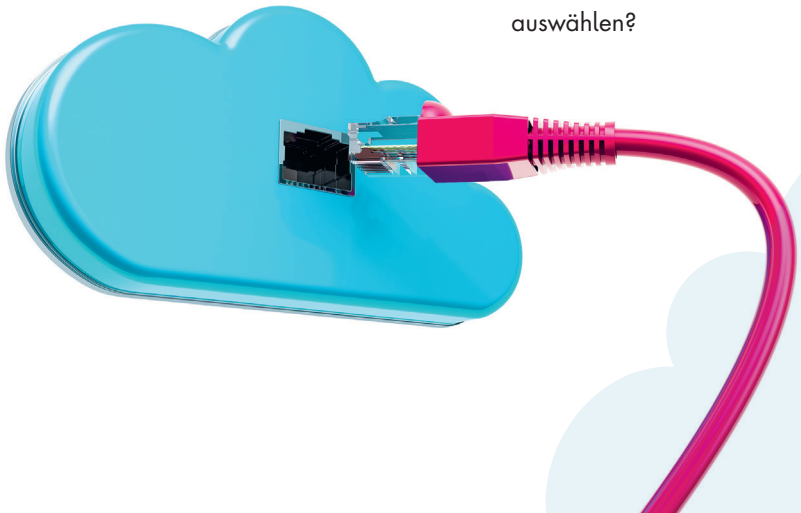
it management: *Worauf müssen Unternehmen noch achten, wenn sie ihren* UCC-Anbieter samt Rechenzentrum auswählen?

Thomas Weiß: Das Stichwort DDoS habe ich vorhin schon einmal genannt und es ist essenziell, dass verlässliche Abwehrmechanismen vorhanden sind, die den bösartigen Datenverkehr im Netzwerk herausfiltern. Ich kann daher jedem nur empfehlen: Informieren Sie sich genau über die Service Level Agreements im Datacenter Ihres UCC-Anbieters. Für Telefonie sollten diese nicht nur den TCP-, sondern auch den UDP-Verkehr umfassen, da UDP für die Sprachqualität bei Voice-over-IP verantwortlich ist. Schauen Sie sich auch die SLA-Werte aus der Vergangenheit an. Achten Sie darauf, ob diese kontinuierlich besser geworden sind und ob das versprochene Level an Verfügbarkeit erreicht oder gar übertroffen wurde. Hundertprozentige Verfügbarkeit gibt es übrigens nicht. Sollte ein Betreiber diesen Wert angeben, spricht das nicht gerade für Transparenz. Dabei braucht es genau diese im Störungsfall: User benötigen eine zentrale Anlaufstelle wie ein Störungsportal, das auch dem Dienstanbieter dabei hilft, Probleme schnell zu beheben.

it management: *Das heißt: die Auswahl des richtigen Datacenter-Anbieters macht den Unterschied?*

Thomas Weiß: Auf jeden Fall! Da die für den UUC-Bereich wichtigen Parameter messbar sind, gibt es aussagekräftige externe Vergleichstests und Monitorings entsprechender Fachexperten. Solche unabhängigen Leistungsvergleiche sollten Unternehmen bei der Wahl ihres zukünftigen UCC-Anbieters unbedingt berücksichtigen.

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



THANK YOU

VON MONITORING ZU OBSERVABILITY

WIE SIE DIE NÄCHSTEN HÜRDEN MEISTERN

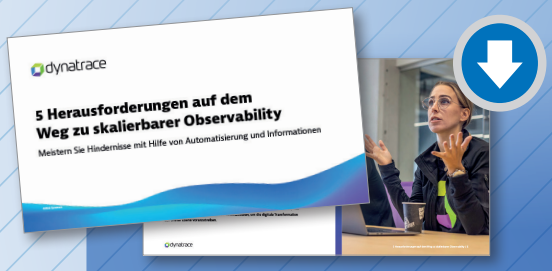
Damit eine digitale Transformation stattfinden kann, müssen alle Anwendungen und digitalen Dienste sowie die dynamischen Multi-Cloud-Plattformen, auf denen diese ausgeführt werden, einwandfrei funktionieren. Wir nennen das „Cloud Done Right".

Allerdings unterscheiden sich dynamische, weit verteilte und cloud-native Technologien grundlegend von ihren Vorgängersystemen. Die durch Microservices, Container und softwaredefinierte Cloud-Infrastrukturen hervorgerufene Komplexität nimmt dabei enorme Ausmaße an und kann von Mitarbeitern in Eigenregie nicht mehr bewältigt werden.

Damit jederzeit klar ist, was in diesen sich stetig verändernden Umgebungen abläuft, muss auch die Observability skaliert werden.

In diesem kostenlosen Whitepaper erfahren Sie:

- Was skalierbare Observability bedeutet
- Welche 5 Hürden Unternehmen überwinden müssen
- Warum Datenmenge, Tool-Sprawl und Fachkräftemangel zum Problem werden
- Wie Sie Observability automatisiert, effizient und zukunftssicher aufbauen



WHITEPAPER DOWNLOAD

Das Whitepaper umfasst 23 Seiten und steht kostenlos zum Download bereit.
www.it-daily.net/download

Digitalisierung auf Rädern

PANASONIC VERNETZT FAHRZEUGE ZU IT-HUBS

Die digitale Transformation endet nicht am Werkstor – sie beginnt oft auf der Straße. In einer zunehmend mobilen Arbeitswelt sind zuverlässige, robuste Endgeräte allein nicht genug. Unternehmen mit Außendienst-, Liefer- oder Einsatzflotten brauchen vernetzte Lösungen, die Technik, Kommunikation und Daten nahtlos in die Fahrzeuge integrieren.

Hier setzen Panasonic TOUGHBOOK Mobility Services an: Sie kombinieren ausfallsichere Hardware mit passenden Einbaulösungen, erstklassiger Konnektivität und umfassendem Support – für eine mobile IT-Infrastruktur, die so leistungsfähig ist wie im Büro.

Beispiel Pannendienst AA
Ein Best Practice liefert der britische Automobilclub AA. Mit über 2.500 Fahrzeugen im täglichen Einsatz war die Herausforderung klar: eine digitale Lösung, die Fahrer, Fahrzeug und Zentrale in Echtzeit verbindet. Panasonic entwickelte eine Connected Vehicle Solution, die neben den TOUGHBOOK Geräten die komplette Fahrzeug-Integration umfasst - samt ergonomischer Bedienung, Stromversorgung, GPS-Navigation, Datenanbindung und sicherem WLAN in einem 25m-Radius um die Servicefahrzeuge. Die Lösung ermöglicht eine effiziente Einsatzsteuerung, reduziert Ausfallzeiten und steigert die Produktivität.

Besonders attraktiv: das flexible Monats-Abo Mobile-IT-as-a-Service, das Hardware, Software und Services bündelt – planbar, skalierbar, kalkulierbar. Und übrigens: Panasonic unterstützt aktiv bei der sicheren Migration auf Windows 11.

Panasonic CONNECT TOUGHBOOK

DIGITALWIRTSCHAFT

GESCHÄFTSLAGE VERBESSERT SICH

Zum ersten Mal seit einem Jahr notiert der Bitkom-ifo-Digitalindex wieder im positiven Bereich bei +1,9 Punkten. Das ist ein Plus von 3,3 Punkten im Vergleich zum Juli. Der Index bildet – wie der ifo-Konjunkturindex - die aktuelle Geschäftslage und die Geschäftserwartungen für die kommenden drei Monate ab und berechnet daraus das Geschäftsklima. Die aktuelle Geschäftslage hat sich bei vielen Unternehmen der IT- und Telekommunikationsbranche verbessert und lag Ende August bei 6,9 Punkten. Im Vormonat waren es noch 0,4 Punkte gewesen. Die Geschäftserwartungen für den weiteren Jahresverlauf sind allerdings noch nicht wieder über der Nulllinie. Sie liegen aktuell wie im Vormonat bei -3,1 Punkten.

Im Vergleich mit der Gesamtwirtschaft ist die Digitalwirtschaft zuversichtlicher. Zum Vergleich: Für die Gesamtwirtschaft weist das ifo-Institut ein Geschäftsklima aus, das mit -5,5 Punkten unter der Nulllinie bleibt. Die Geschäftslage wird dabei mit -3,1 Punkten wie im Vormonat beurteilt, als sie bei -3,0 Punkten lag. Die Geschäftserwartungen in der Gesamtwirtschaft haben sich geringfügig verbessert und lagen im August bei -7,8 Punkten nach -9,7 Punkten im Juli.

www.bitkom.org

Cloud ohne Lock-in

EUROPAS DIGITALE RESILIENZ BEGINNT MIT ECHTER WAHLFREIHEIT

Europäische Cloud-Alternativen zu den US-Hyperscalern stehen im Fokus der Diskussion um digitale Souveränität. Während die technischen Voraussetzungen in Europa durchaus vorhanden sind, scheitert die Umsetzung oft an strategischen und strukturellen Hürden.

Darüber sprachen wir mit Christian Kaul, COO und Co-Founder von Impossible Cloud.

it management: *Herr Kaul, der Ausbau europäischer Cloud-Infrastrukturen gilt als zentral für digitale Souveränität. Warum tut sich Europa dennoch so schwer mit der Umsetzung?*

Christian Kaul: Europas Rückstand ist nicht nur ein technologisches Problem, sondern ein strategisches. Die nötigen Ressourcen sind vorhanden. Wir haben Tausende Rechenzentren, hohe Datenschutzstandards und eine stabile Rechtsordnung. Aber diese Potenziale werden nicht effizient genutzt, weil es an einem gemeinsamen Architekturprinzip fehlt.

Statt bestehende Infrastrukturen miteinander zu vernetzen, investieren viele Akteure in nationale Insellösungen oder lagern ihre Daten in Hyperscaler-Plattformen aus. Die Folge ist eine zunehmende Abhängigkeit von US-Anbietern, bei denen europäische Unternehmen weder die Datenhoheit noch die volle Kontrolle über Zugriffsrechte behalten. Gleichzeitig verhindern komplexe Genehmigungsverfahren und föderale Strukturen einen schnellen, grenzüberschreitenden Ausbau europäischer Alternativen.

Impossible Cloud geht einen anderen Weg. Wir vernetzen bestehende Rechenzentren über standardisierte Schnittstellen, ermöglichen Datenlokalisierung nach datenschutzrechtlichen Vorgaben und kombinieren technische Skalierbarkeit mit vollständiger Kontrolle. Das ist kein Kompromiss, sondern ein Modell, das Europas regulatorische und strukturelle Realität in eine zukunftsfähige Cloud-Strategie übersetzt.

> WER CYBERSICHERHEIT STRATEGISCH DENKT, MUSS BEI DER INFRASTRUKTUR ANFANGEN.
>
> **Christian Kaul, COO und Co-Founder, Impossible Cloud GmbH, de.impossiblecloud.com**

it management: *Was heißt das konkret?*

Christian Kaul: Eine grundlegende Neuausrichtung: Weg von monolithischen Cloud-Regionen hin zu föderierten Architekturen, bei denen bestehende Rechenzentren intelligent orchestriert werden. Unternehmen legen beim Anlegen ihrer Buckets genau fest, wo ihre Daten gespeichert werden sollen. Unsere Plattform bindet zertifizierte Rechenzentren an, die europäischen Datenschutzanforderungen entsprechen. Über Geofencing stellen wir sicher, dass die Daten auch wirklich in der gewählten Region bleiben. Die technische Vernetzung erfolgt über standardisierte Schnittstellen. So entsteht ein verteiltes Cloud-Modell, das Datenströme intelligent steuert, Compliance-Vorgaben erfüllt und eine hohe Verfügbarkeit sicherstellt – ohne neue Infrastruktur bauen zu müssen.

it management: *Ein zentrales Thema auf der it-sa ist Datensicherheit. Wie unterscheiden Sie sich hier von US-Hyperscalern?*

Christian Kaul: Der entscheidende Unterschied liegt in der Kontrolle. Unsere Plattform ermöglicht Unternehmen, genau festzulegen, wo ihre Daten gespeichert werden und wer darauf zugreifen darf. Alle Daten werden während der Übertragung mit TLS verschlüsselt, zusätzlich serverseitig nach dem SSE-S3-Prinzip mit AES-256 gesichert und auf den Speichermedien noch einmal vollständig verschlüsselt. Auf Wunsch können Unternehmen ihre Daten sogar schon vor dem Upload selbst verschlüsseln.

Ein weiterer zentraler Punkt ist die Rechtslage. Unsere Infrastrukturpartner betreiben ausschließlich Rechenzentren in Europa, die unter europäisches Datenschutzrecht fallen. Das bedeutet: Es gibt keine Verpflichtung zur Herausgabe von Daten an Behörden außerhalb Europas. Wir unterliegen nicht dem US Coud Act, und unsere Kunden haben die volle Kontrolle darüber, wo ihre Daten liegen. Für viele Unternehmen ist das nicht nur ein Compliance-Thema, sondern ein strategischer Sicherheitsfaktor.

it management: *Wie gehen Sie mit Fragen zur Zugriffskontrolle um?*

Christian Kaul: Alle Datenbereiche sind bei uns standardmäßig privat. Zugriffsrechte werden über ein identitätsbasiertes Modell vergeben, das einfach zu verwalten ist. Unternehmen können genau festlegen, wer auf welche Inhalte zugreifen darf. Wenn Daten geteilt werden sollen, geschieht das kontrolliert und zeitlich begrenzt über presigned URLs. Für Part-

nerprojekte ermöglichen wir außerdem die Anbindung externer Authentifizierungsdienste wie SAML oder OIDC. So bleibt auch bei komplexen Nutzerstrukturen die Kontrolle vollständig erhalten.

it management: *Ihr Speicherangebot basiert auf dem Prinzip „Always-Hot Storage". Was bedeutet das konkret – und welche Rolle spielt Ihre Plattform im Bereich Sicherheit?*

Christian Kaul: Always-Hot Storage bedeutet, dass alle gespeicherten Daten jederzeit ohne Verzögerung verfügbar sind. Es gibt keine Trennung in „kalte" und „heiße" Speicherklassen, keine Wartezeiten wie bei Glacier und keine Zusatzkosten für den Abruf. Unternehmen können jederzeit auf ihre Daten zugreifen, egal ob sie regelmäßig genutzt oder nur archiviert sind. Das ist besonders wichtig für Anwendungen wie Backups, Datenanalyse oder Langzeitarchive mit direktem Zugriffsbedarf.

Unsere Plattform geht dabei über klassischen Speicher hinaus und integriert Sicherheit von Anfang an. Mit Object Lock können Daten außerdem revisionssicher gespeichert werden. Das schützt zuverlässig vor Ransomware-Angriffen. Zusätzlich setzen wir auf Mehrfaktorauthentifizierung, rollenbasierte Zugriffskontrolle und Geofencing, das eine standortgenaue Datenhaltung innerhalb Europas ermöglicht. So lassen sich Sicherheit, Verfügbarkeit und Kontrolle in einer Lösung verbinden.

it management: *Wie unterscheidet sich Ihr Geschäftsmodell vom typischen Hyperscaler-Ansatz?*

Christian Kaul: Hyperscaler arbeiten oft mit komplexen Preisstrukturen. Abrufkosten, Egress-Gebühren, Mindestlaufzeiten und zusätzliche Gebühren für API-Nutzung machen die tatsächlichen Kosten schwer kalkulierbar. Bei uns ist das anders. Wir verzichten vollständig auf Egress- und API-Kosten. Unternehmen zahlen nur für den tatsächlich belegten Speicherplatz. Es gibt keine Gebühren für das Verschieben, Abrufen oder Ansteuern der Daten. Die Mindesthaltefrist für Objekte beträgt lediglich 24 Stunden. Danach können Daten jederzeit gelöscht oder verschoben werden, ohne Zusatzkosten.

Wer dauerhaft größere Mengen speichern möchte, kann über feste Kapazitätsvereinbarungen zusätzlich sparen, ohne an langfristige Verträge gebunden zu sein. Darüber hinaus ist Impossible Cloud vollständig S3-kompatibel. Bestehende Workflows lassen sich also nahtlos weiterführen, und die Umstellung ist technisch in wenigen Minuten erledigt. Für viele Unternehmen ist das der entscheidende Unterschied. Sie gewinnen Kontrolle zurück, ohne sich auf proprietäre Systeme einzulassen.

it management: *Zum Abschluss: Was ist Ihr Appell an Entscheider auf der it-sa?*

Christian Kaul: Wer Cybersicherheit strategisch denkt, muss bei der Infrastruktur anfangen. Die Zukunft gehört Systemen, die flexibel, kontrollierbar und sowohl technisch als auch rechtlich verlässlich sind. Unternehmen, die heute in europäische Cloud-Alternativen investieren, schaffen sich nicht nur technologische Unabhängigkeit, sondern auch die Grundlage für echte Resilienz im digitalen Raum. Es geht nicht darum, die Großen zu kopieren. Es geht darum, eigene Standards zu setzen. Wer seine Datenhaltung souverän und zukunftssicher aufstellen will, braucht jetzt eine Plattform, die nicht nur europäisches Recht achtet, Sicherheit mitdenkt und wirtschaftlich skalierbar ist, sondern auch genau das erfüllt, was Unternehmen fordern: Made in Germany, rechtskonform, technisch auf Augenhöhe und wirtschaftlich tragfähig.

it management: *Herr Kaul, wir danken für dieses Gespräch.*

Im Klammergriff der Regulierung

KI & EFFIZIENZSTEIGERUNG IM CLOUD-MANAGEMENT

Cloud-Umgebungen entwickeln sich zunehmend zu hochkomplexen Systemen, in denen hybride Infrastrukturen, Multi-Cloud-Strategien und dynamische Workloads parallel gemanagt werden müssen.

Für Unternehmen bedeutet das eine stetig wachsende Herausforderung, denn die Effizienz hängt nicht nur von technischer Leistungsfähigkeit, sondern auch von einer intelligenten Orchestrierung ab. Genau hier entfaltet Künstliche Intelligenz ihr Potenzial. Moderne KI-Systeme sind in der Lage, wiederkehrende Aufgaben wie die Bereitstellung von Ressourcen oder die automatische Skalierung von Anwendungen zu übernehmen.

Besonders wertvoll ist ihre Fähigkeit, Bedarfe vorauszusagen: Mit Hilfe von Simulationen lassen sich zukünftige Ressourcennutzungen präzise prognostizieren. Dadurch können Engpässe rechtzeitig erkannt und verhindert werden – ein entscheidender Faktor für Kostenoptimierung und Betriebssicherheit.

Auch im Bereich der Cybersecurity ist der Einsatz von KI von wachsender Bedeutung: Sie unterstützt bei der Erkennung von Anomalien, identifiziert ungewöhnliche Zugriffsmuster und kann auf Sicherheitsvorfälle teilweise automatisiert reagieren. So wird die operative Belastung von IT-Abteilungen deutlich reduziert.

Praxisbeispiele

Die Erfahrungen zeigen, dass KI im Cloud-Management längst keine Zukunftsvision mehr ist, sondern bereits konkrete Mehrwerte schafft. Ein E-Commerce-Anbieter nutzt KI-gestützte Bedarfsprognosen, um saisonale Spitzen wie Black Friday ohne manuelles Eingreifen zu bewältigen. Finanzdienstleister setzen intelligente Systeme zur automatischen Überwachung von Compliance-Vorgaben ein, wodurch nicht nur regulatorische Risiken minimiert, sondern auch Cyberangriffe frühzeitig erkannt werden.

EU-KI-REGULIERUNG UND UNTERNEHMENSSTRATEGIE

EU-KI-Gesetzgebung 2025-2027

- Verbot Live-Gesichtserkennung
- Verbot Emotionserkennung
- Verbot Social Scoring
- Hochrisiko-System-Regulierung

Unternehmensstrategie

- Governance-Strukturen aufbauen
- Klare Verantwortlichkeiten
- KI-Vision entwickeln
- Compliance-Management
- Risikobewertung

Erfolgskriterium

- Balance Innovation & Risiko
- Nachhaltiger Mehrwert
- Vertrauensbildung
- Wettbewerbsvorteile

Bild 1: Zeigt den Zusammenhang zwischen EU-Regulierung, Unternehmensstrategie und Erfolg. (Quelle: it research)

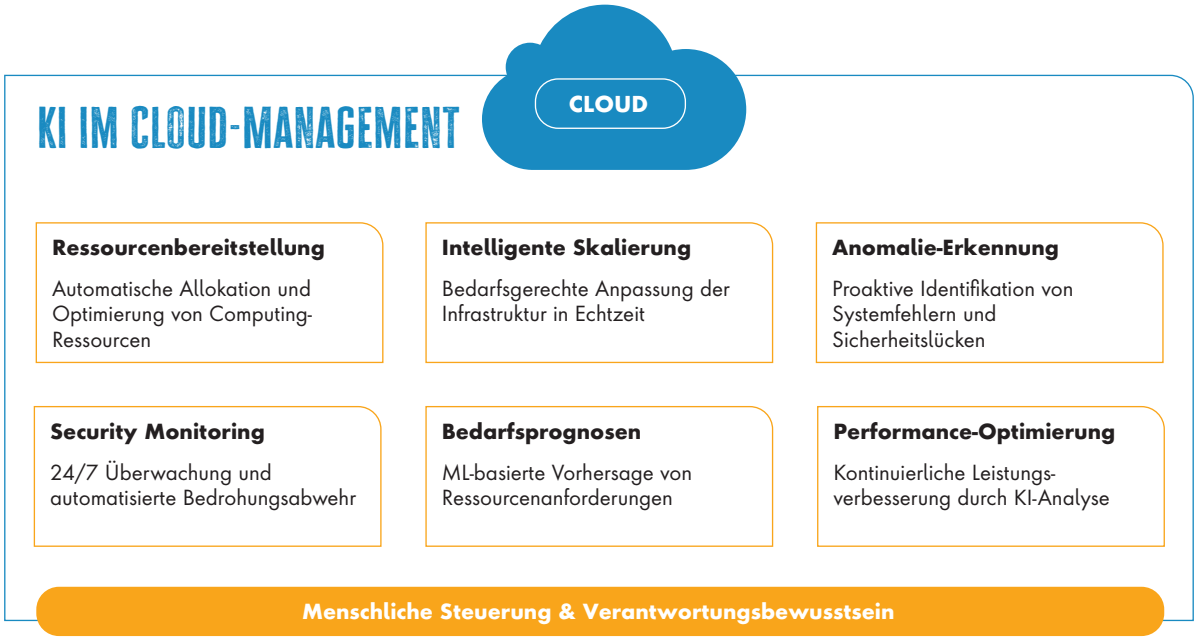


Bild 2: Visualisiert KI-Funktionen im Cloud-Management mit zentraler Cloud und umliegenden Funktionsbereichen. (Quelle: it research)

In der Industrie optimieren Unternehmen ihre Multi-Cloud-Infrastruktur, indem KI-Lösungen dynamisch die jeweils effizienteste Plattform auswählen und so Kosten senken. Trotz aller Automatisierung bleibt der Mensch jedoch unverzichtbar: Expertinnen und Experten steuern die Systeme, treffen ethische Entscheidungen und sorgen dafür, dass Technologie in einem verantwortungsvollen Rahmen eingesetzt wird. Das Zusammenspiel von KI und menschlicher Expertise schafft somit eine symbiotische Partnerschaft, die Cloud-Infrastrukturen flexibler, stabiler und sicherer macht.

Die menschliche Komponente bleibt unverzichtbar

Trotz aller Automatisierung bleibt der Mensch unverzichtbar. Expertinnen und Experten steuern die Systeme, treffen ethische Entscheidungen und sorgen dafür, dass Technologie in einem verantwortungsvollen Rahmen eingesetzt wird. Das Zusammenspiel von KI und menschlicher Expertise schafft eine symbiotische Partnerschaft, die Cloud-Infrastrukturen flexibler, stabiler und sicherer macht. Während KI operative Effizienz und Geschwindigkeit bringt, steuert der Mensch strategische Richtungen und überwacht ethische Grenzen.

Neue regulatorische Rahmenbedingungen

Parallel zu diesen technologischen Möglichkeiten tritt seit Februar 2025 eine neue Ära regulatorischer Rahmenbedingungen in Kraft. Mit der EU-KI-Verordnung werden erstmals europaweit verbindliche Standards gesetzt, die bis 2027 vollständig umgesetzt sein sollen. Diese Regulierung folgt einem gestuften Ansatz: Im Februar 2025 wurden zunächst die gefährlichsten KI-Anwendungen verboten, gefolgt von Pflichten für Foundation Models im August 2025. Die vollständige Regulierung von Hochrisiko-KI-Systemen tritt im August 2026 in Kraft, bevor im August 2027 die finale Umsetzungsfrist für alle Bestimmungen erreicht wird.

Verbotene Anwendungen und Compliance-Anforderungen

Verboten sind dann Anwendungen mit hohen gesellschaftlichen Risiken, darunter Live-Gesichtserkennung im öffentlichen Raum, Systeme zur Emotionserkennung am Arbeitsplatz, Social Scoring von Bürgern sowie kognitive Verhaltensmanipulation. Entscheidend ist dabei nicht der Einsatz von KI an sich, sondern die Art und Weise ihres Einsatzes.

Unterehmen stehen vor der Aufgabe, robuste Governance-Strukturen aufzubauen und Verantwortlichkeiten klar zu definieren. Eine strategische KI-Vision muss entwickelt werden, die sowohl technologische Möglichkeiten als auch ethische Grenzen berücksichtigt. Dabei sind Risikobewertungsprozesse und kontinuierliche Compliance-Überwachung nicht nur rechtliche Notwendigkeiten, sondern auch Wettbewerbsvorteile für vertrauensvolle Unternehmen.

Fazit: Die Zukunft gehört verantwortungsvoller KI

Wer es schafft, technologische Innovation und regulatorische Compliance miteinander zu verbinden, schafft nicht nur nachhaltigen Mehrwert für Kundinnen und Kunden, sondern positioniert sich auch als vertrauenswürdiger Akteur im digitalen Ökosystem der Zukunft. Die EU-KI-Verordnung ist dabei nicht als Hindernis, sondern als Chance zu verstehen: Sie schafft einen Rahmen für vertrauensvolle KI, die gesellschaftlichen Nutzen stiftet und gleichzeitig Risiken minimiert.

Unternehmen, die diese Balance meistern, werden die Gewinner der KI-Revolution sein. Sie kombinieren die operative Exzellenz automatisierter Cloud-Systeme mit der Vertrauenswürdigkeit regulatorischer Compliance und schaffen damit die Grundlage für nachhaltigen Geschäftserfolg in einer KI-getriebenen Zukunft.

Ulrich Parthier

End-of-Life 2025, Cloud-Kosten und KI-Stillstand

WARUM JETZT JEDE IT-ENTSCHEIDUNG TEUER ODER ZUKUNFTSWEISEND WIRD

In deutschen Betrieben herrscht Modernisierungsstau bei der Software – das zeigt eine aktuelle Umfrage unter IT- und Business-Verantwortlichen mittelständischer bis großer Unternehmen. Selbst geschäftskritische Anwendungen basieren demnach oft auf veralteter Architektur. Die Notwendigkeit zur Erneuerung ist offensichtlich, nur der Weg nicht immer eindeutig – und die Budgets werden dringend anderswo benötigt!

Das Ende der On-Premises-Ära?

Wenn ERP-Systeme, Bürosoftware, E-Mail-Server oder Plattformen, auf denen ganze Prozessketten laufen, keinen Support mehr erhalten, werden sie zur Gefahr für ein Unternehmen. Durch Cyber-Kriminelle, Datenverlust, Systemausfälle,... Die Risiken sind bekannt – die Lösungen nicht immer. Beispiel Microsoft: Im Oktober 2025 endet der Support für Windows 10, Office 2016/2019, Exchange Server 2016/2019 und Windows Server 2012. Microsoft präsentiert seine M365-Lösung als logische Weiterentwicklung. Als gäbe es nur diese Option. Doch ist das wirklich so? Ist das Ende der On-Premises-Ära gekommen und ein Wechsel in die Microsoft-Cloud unausweichlich? „Nein", sagt Björn Orth, Geschäftsführer beim Microsoft Solutions Partner VENDOSOFT. „Klassische On-Premises-Modelle bleiben verfügbar – ebenso hybride Mischformen. Damit gibt es weiterhin tragfähige Alternativen zu den Online-Diensten. Es besteht kein Migrationszwang in die Cloud!"

WICHTIGE FRAGEN ZUM END-OF-LIFE

von Office 2016/2019, Exchange Server 2016/2019 und Windows Server 2012:

Kaufsoftware bleibt gefragt

Was jedoch besteht, ist der Druck zur Entscheidungsfindung. Laut der erwähnten Studie der Beratungsgesellschaft Lünendonk planen neun von zehn Unternehmen, bis 2028 mehr als 40 Prozent ihrer Anwendungen cloudbasiert zu betreiben. Aktuell liege die Quote bei vier von zehn. 72 Prozent der Befragten setzen bei Sicherheits- oder Compliance-Themen nach wie vor auf lokale Installationen oder Private-Cloud-Lösungen. Hier ist also auf Jahre hinaus weiterhin Kaufsoftware gefragt und verfolgt man Berichte in den IT-Medien, bleiben gekaufte Microsoft-Lizenzen noch aus einem weiteren Grund attraktiv.

Wachsende Cloud-Ausgaben bremsen KI-Investitionen

Cloud-Dienste werden immer teurer. Das hat einer Studie von Akamai Technologies (Anbieter für Cybersicherheit und Cloud) zufolge bereits spürbare

Konsequenzen. Ein erheblicher Teil von Unternehmen sieht sich demnach gezwungen, Investitionen in Cybersicherheit, neue KI-Projekte und sogar IT-Fachpersonal aufgrund gestiegener Cloud-Kosten hintenanzustellen. Dass Abogebühren unverhältnismäßig anziehen können, darüber spricht auch VENDOSOFT offen mit seinen Kunden. „Selbst als CSP-Provider empfehlen wir kaum einem Unternehmen eine Cloud-only-Strategie", betont Björn Orth. Zu unberechenbar ist Microsoft in der Preispolitik seiner Online-Dienste – und zu gravierend ist die Abhängigkeit, in die sich Unternehmen damit begeben.

Der Mix macht's

Eine Kostenplanung, die bis zu fünf Jahre Bestand hat, gewährleisten nur On-Premises-Modelle. Werden dabei die neuesten Office- oder Server-Lizenzen gebraucht gekauft (wie es VENDOSOFT für seine Kunden vornimmt) und sinnvoll um M365 ergänzt, spart das bis zu 40 Prozent im Vergleich zur reinen Cloud. „Abo-Dienste auf das Nötigste begrenzen", ist die Empfehlung von Björn Orth, um das Risiko jährlicher und möglicherweise unerwartet hoher Preissteigerungen so gering wie möglich zu halten.

IT-Entscheidungen von heute beeinflussen die Budgets von morgen

Die IT-Entscheidungen der kommenden Monate können darüber bestimmen, ob Unternehmen innovationsbereit bleiben – oder in teure Abhängigkeiten geraten. Modernisierung ist unausweichlich. Doch nur wer alle Optionen kennt – von der Cloud bis zur gebrauchten Lizenz – kann wirklich zukunftsfähig planen.

Genau hier setzt strategische Lizenzberatung an: Sie bringt technische Anforderungen, Lizenzmodelle und Budgetplanung zusammen und schafft die Grundlage – um nicht nur kurzfristig funktionale Lösungen zu finden, sondern langfristig tragfähige IT-Architekturen. „Gebrauchte Microsoft-Lizenzen sind dabei ein wichtiger Enabler für die Finanzierung drängender IT-Investitionen", fasst Björn Orth zusammen.

www.vendosoft.de

MEHR WERT

Whitepaper: Microsoft-Supportende 2025

Datensicherheit im Wandel

WORAUF CIOs HEUTE ACHTEN MÜSSEN

Cybersicherheit ist ein Spiegelbild der digitalen Transformation und der damit einhergehenden Anforderungen. Unternehmen müssen ihre Strategien kontinuierlich anpassen, um adäquaten Schutz für ihre digitalen Assets zu bieten. Im Gespräch mit Sascha Puljic, Vice President Central Europe bei Zscaler wird erklärt, worauf es in Zeiten eskalierender Cyberangriffe, KI und einer Souveränitätsdebatte ankommt.

? **it management:** *Herr Puljic, das Management ist heute ganz anders in der Pflicht, für die Sicherheit des Geschäfts zu sorgen, als noch vor wenigen Jahren. Was ist heute besonders wichtig?*

Sascha Puljic: In einer digitalen und komplexen geopolitischen Landschaft steht im Fokus, wo Daten gespeichert und verarbeitet werden. Das ist für europäische Organisationen mit globalem Geschäftsmodell längst kein Luxus mehr – es ist eine Notwendigkeit. Da kommen die Einhaltung regulatorischer Vorgaben zum Tragen, wachsende Kundenansprüche in Bezug auf Datenschutz, aber eben auch nationale Sicherheitsbedenken. All diese Faktoren erfordern eine strengere Kontrolle über die Speicherung und den Umgang mit Daten und CIOs verlangen nach Technologien, die ihnen dabei helfen.

ZERO TRUST-SICHERHEIT IST HEUTE GANZ KLAR ZUM WETTBEWERBSVORTEIL FÜR UNTERNEHMEN GEWORDEN.

Sascha Puljic,
Vice President Central Europe,
Zscaler Germany GmbH,
www.zscaler.com

? **it management:** *Was ist das Hauptanliegen von CIOs hinsichtlich der Souveränität und Sicherheit ihrer Daten?*

Sascha Puljic: Die Herausforderung für Unternehmen in einer vernetzten und Cloud-dominierten Welt ist es, Daten sicher, regelkonform und effizient zu verwalten. Sie müssen zu jeder Zeit nachvollziehen können, wo die Daten vorgehalten und verarbeitet werden. Die verstärkten Anforderungen an den Schutz europäischer Daten vor Drittstaatenzugriff und die Forderung nach klaren Kontrollen ihrer Speicherung und Verarbeitung erfordern mehr Transparenz und Nachvollziehbarkeit. Die Entscheider sind sich bewusst, dass die Einhaltung regulatorischer Anforderungen, nationaler Datenschutzgesetze und die Kontrolle kritischer Infrastrukturen zu Erfolgsfaktoren geworden sind und lassen der Datensicherheit neue Aufmerksamkeit zukommen.

? **it management:** *Gerade für international agierende Unternehmen kann das schnell zur Mammutaufgabe werden …*

Sascha Puljic: Richtig, Datenkontrolle und Souveränität gehen mit unterschiedlichsten Compliance-Anforderungen selbst in Europa einher. Uneinheitliche Gesetzgebungen verlangen nach variierenden Sicherheitsmaßnahmen, erfordern den Überblick über Offenlegungspraktiken und Aufbewahrungspflichten und gehen nicht zuletzt mit unterschiedlichen Strafen für die Nicht-Einhaltung von Gesetzen einher.

? **it management:** *Datenhoheit wird also zum Schlüsselfaktor der Cybersicherheit. Wie hilft Zscaler seinen Kunden dabei?*

Sascha Puljic: Es gilt, die Vertraulichkeit der Daten, ihre Integrität, aber auch ihre Verfügbarkeit in Einklang zu bringen. Unternehmen müssen sich die Frage stellen, in welchen Anwendungen Daten vorgehalten werden, sie sollten die Daten nach Kritikalität klassifizieren und festlegen, wer darauf von intern oder extern Zugriff haben darf. Die Zero Trust Exchange-Plattform wurde aufbauend auf den Prinzipien Privacy by Design und Privacy by Default entwickelt und liefert die nötige Transparenz, aber auch Kontrollfunktion für alle Datenströme. Sie erlaubt die Umsetzung granularer Zugriffskontrollen und ermöglicht die Vorhaltung der Transaktionsdaten in Europa. Solche Governance-Ansätze sind heute nicht nur für die Souveränität der Daten wichtig, sondern auch um unbeabsichtigtes Abfließen in KI-Modelle zu unterbinden.

? **it management:** *Hier sprechen Sie die nächste große Herausforderung an. Die künstliche Intelligenz tritt an, Unternehmensprozesse grundlegend zu verändern.*

Sascha Puljic: Viele Unternehmen sehen in der KI Chancen, komplexe Prozesse zu

automatisieren und dadurch agiler zu werden. Über Jahrzehnte gewachsene IT-Infrastrukturen gehen mit einer ausufernden Komplexität einher. Das Management muss sich mit Strategien zur Komplexitätsreduktion auseinandersetzen, Kosten einsparen und dem Fachkräftemangel entgegenwirken. Ein großes Problem ist die Fragmentierung der IT-Sicherheitslandschaft. Unternehmen haben in den letzten Jahrzehnten Tools und Lösungen von verschiedenen Anbietern implementiert, um den wachsenden Bedrohungen zu begegnen. Diese heterogene Infrastruktur kann jedoch sehr schnell zu einem Sicherheitsrisiko werden.

it management: *Welche Strategie hilft dem CIO bei der Bewältigung dieser selbst geschaffenen Risiken?*

Sascha Puljic: Viele CIOs konzentrieren sich auf die Konsolidierung ihrer Sicherheitsinfrastrukturen. Ziel ist es, eine einheitliche, durchgängige Sicht auf Bedrohungen und Schwachstellen zu erhalten und gleichzeitig Ressourcen effizienter einzusetzen. Plattformstrategien, bei denen Sicherheitslösungen nahtlos integriert werden können, sind hier essenziell. Eine hochintegrierte Security-Plattform hilft dabei, den Verwaltungsaufwand von Hardware abzulösen und hochautomatisierte Prozesse vereinfachen und beschleunigen das Durchleuchten der Datenströme auf Risiken. Unsere Plattform kombiniert den Zero Trust-Ansatz mit den Geschwindigkeitsvorteilen, die künstliche Intelligenz mit sich bringt. Damit lassen sich Zugriffsregeln intelligent erstellen, aber auch Anomalien schnell erkennen und damit Risiken für Datenschutzverletzungen mitigieren.

it management: *KI birgt auch neue Risiken für Datenschutzverletzungen. Wie sollten Unternehmen mit diesem Zwiespalt umgehen?*

Sascha Puljic: Mit dem verstärkten Einsatz von künstlicher Intelligenz sehen wir uns mit neuen Herausforderungen im Bereich der Datensicherheit konfrontiert. KI-Modelle benötigen für ihr Training enorme Mengen an Daten. Das birgt das Risiko, dass vertrauliche oder sensible Informationen missbraucht werden könnten. Gleichzeitig stellt sich die Frage, ob Daten, die in KI-Systeme eingespeist werden, langfristig sicher, nachverfolgbar und transparent bleiben. Dies erfordert Sicherheitslösungen, die nicht nur Compliance sicherstellen, sondern auch in der Lage sind, die Herkunft und Verarbeitung der Daten innerhalb der KI-Wertschöpfungskette nachvollziehbar zu gestalten. Wir sehen nicht zuletzt aus Gründen des Datenschutzes einen gegenläufigen Trend einsetzen – weg von Large Language Modells (LLMs) hin zu Small Language Modells (SLMs). Es geht also um eine bessere Qualität der Daten und nicht mehr nur um Quantität, so dass SLMs mit gezielten Datensätzen für bestimmte Aufgaben trainiert werden.

it management: *Cybersicherheit ist also zum Enabler für Unternehmen avanciert und sichert geschäftskritische Abläufe?*

Sascha Puljic: Das ist tatsächlich der entscheidende Punkt für den CIO heute. Er muss den Mehrwert von Investitionen in Zero Trust-basierte Sicherheit für den Vorstand transparent machen. Es gilt Ausgaben für die IT-Sicherheit nicht nur als Kostenfaktor, sondern als Vorteil zu positionieren und Monetarisierungsmöglichkeiten aufzuzeigen. Investitionen in IT-Sicherheit erlauben durch Optimierung und Automatisierung Einsparungen in anderen Bereichen. So können durch KI-gestützte Sicherheit repetitive Aufgaben eliminiert und Kosten eingespart werden. Datenschutzverletzungen und der Ausfall von Betriebszeiten durch Cyberangriffe lassen sich vermeiden. Zero Trust-Sicherheit ist heute ganz klar zum Wettbewerbsvorteil für Unternehmen geworden.

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

Künstliche Intelligenz als Gamechanger

VON FLACHEN HIERARCHIEN UND ERFOLGREICHEN TEAMS

Der IT-Dienstleister Nagarro hat sich von seinen Anfängen zu einem global agierenden Unternehmen mit Standorten in fast 40 Ländern entwickelt. Im Interview spricht CEO Dr. Manas Human über Agentic AI, kulturübergreifende Zusammenarbeit und die Zukunft der IT-Weiterbildung.

it management: *Herr Dr. Human, Sie haben Nagarro von einem indischen IT-Dienstleister zu einem europäisch positionierten Unternehmen transformiert, ohne die Entwicklungszentren in Indien aufzugeben. Wie haben Sie es geschafft, diese Brücke zwischen den sehr unterschiedlichen Geschäftskulturen zu bauen?*

Dr. Manas Human: Es ist eigentlich ein Missverständnis, dass Nagarro von Anfang an ein indisches IT-Unternehmen war. Als ich meinen Teil von Nagarro gründete, lebte ich gerade in Boston, und die erste Software, die ich entwickelte, war für ein Pharmaunternehmen in Belgien. Im Laufe der Zeit wuchsen wir vor allem in Indien, weil es dort einfach unglaublich viele talentierte IT-Fachkräfte gab. Aber von Anfang an hat uns die Idee angetrieben, dass Menschen in diesem neuen Technologiefeld mithilfe des Internets über Ländergrenzen hinweg zusammenarbeiten können.

JE EINFACHER ES WIRD, SOFTWARE ZU ENTWICKELN, DESTO STÄRKER WERDEN SICH FLACHE HIERARCHIEN UND SELBSTORGANISIERTE TEAMS DURCHSETZEN.

Dr. Manas Human, CEO, Nagarro, www.nagarro.com

Diese Begeisterung treibt uns bis heute an. Unsere Mission lautet: „To make distance and difference irrelevant between intelligent people". In einer Welt, in der Videokonferenzen fast nichts mehr kosten, können wir tatsächlich wie ein einziges Team arbeiten, egal, wo wir uns gerade befinden.

Uns als Unternehmen ist wichtig, dass wir uns auf das konzentrieren, was uns verbindet und was wir gemeinsam haben. Wir reden miteinander über Technologie, Fotografie, Reisen, Essen oder Familie, denn das sind Themen, die uns alle interessieren. So haben wir es geschafft, eine gemeinsame Unternehmenskultur aufzubauen, die sich über fast 40 Länder hinweg erstreckt.

it management: *Bei Nagarro setzen Sie auf Agentic AI und GenAI. Das sind sehr umkämpfte Bereiche - welche konkreten Projekte realisieren Sie damit und wie positionieren Sie sich gegen die große Konkurrenz?*

Dr. Manas Human: Nagarro ist bekannt für die Arbeit mit modernster Technologie, Schnelligkeit und dafür, auch kleinere, intensive Projekte erfolgreich umzusetzen. Genau diese drei Punkte sind besonders wichtig, wenn es um Agentic AI und Gen AI geht. Viele Projekte in diesem Bereich starten aktuell mit Use Cases, die sich relativ einfach implementieren lassen oder für unsere Kunden weniger Risiken mit sich bringen. Hier können wir unsere agile Arbeitsweise mit kleinen, schlanken Teams voll ausspielen und diese Use Cases effizient umsetzen. Gleichzeitig nutzen wir unsere Engineering-Stärken, um sicherzustellen, dass die Lösungen so aufgebaut sind, dass darauf aufbauende Use Cases später mit deutlich geringeren Zusatzkosten implementiert werden können.

Nagarro investiert schon seit vielen Jahren in KI – lange bevor ChatGPT veröffentlicht wurde – und mittlerweile umfasst unsere entsprechende Business Unit fast tausend Mitarbeitende. KI und Generative KI bieten für uns eine großartige Möglichkeit, uns in der Wertschöpfungskette weiter nach oben zu bewegen: Wir liefern nicht nur hervorragende technische Ergebnisse, sondern schaffen auch echten Mehrwert für das Business.

Im Bereich Generative KI haben wir drei klare Schwerpunkte etabliert: Prompt Engineering, Retrieval-Augmented Generation (RAG) sowie die Entwicklung von SLMs und LLMs durch speziell abgestimmte und optimierte Modelle für konkrete Use Cases. Außerdem arbeiten wir daran, AI Agents und Co-Piloten für den Einsatz in Unternehmen zu entwickeln, multimodale und verkörperte KI voranzutreiben und strukturierte, kontextbewusste LLM-Anwendungen zu realisieren. In Verbindung mit unserem tiefen Branchenwis-

sen, etwa im Banking, in der Luftfahrt, im Bereich Automotive oder im Einzelhandel, können wir maßgeschneiderte Lösungen liefern, die echten und messbaren Mehrwert schaffen.

Wir arbeiten mit einigen der weltweit führenden Unternehmen zusammen und entwickeln neben der Arbeit für unsere Kunden mehrere interne KI-Accelerators, die wir in verschiedenen Projekten einsetzen. Ein Beispiel dafür ist Ginger, unser interner digitaler Assistent, der alle Mitarbeitenden mit dem Unternehmen vernetzt. Über die letzten sechs bis sieben Jahre hinweg weiterentwickelt, ist Ginger heute KI-gestützt und ermöglicht alles vom Abrufen von Informationen bis hin zum Versenden personalisierter Benachrichtigungen. Er erinnert vielleicht an den Geburtstag eines Kollegen oder weist auf ein Qualitätsproblem in einem früheren Release hin. In zukunftsorientierten Unternehmen helfen Tools wie Ginger dabei, Kultur, Kommunikation und Arbeitsabläufe lebendig zu halten. Asfinag, Betreiber des österreichischen Autobahn- und Schnellstraßennetzes, hat Ginger beispielsweise unter eigenem Branding eingeführt.

it management: *Der Fachkräftemangel zwingt auch zu neuen Arbeitsformen. Funktionieren flache Hierarchien und selbstorganisierte Teams wirklich bei knappen Ressourcen, oder braucht man dann doch mehr Struktur?*

Dr. Manas Human: Nein, das glaube ich nicht. Zumindest glaube ich das nicht. Ich bin überzeugt, dass uns KI hier zu Hilfe kommen wird. Je einfacher es wird, Software zu entwickeln, desto stärker werden sich flache Hierarchien und selbstorganisierte Teams durchsetzen.

Wenn Arbeit viele einfache, wiederkehrende Tätigkeiten umfasst, ermöglicht Hierarchie erfahrenen Fachkräften, große Gruppen weniger erfahrener Mitarbeitender zu steuern und so Ergebnisse zu erzielen. Mit KI jedoch kann ein Großteil dieser Aufgaben von der Technologie übernommen werden. Hierarchien werden dadurch nicht nur weniger nützlich, sie können sogar hinderlich sein. Wir bei Nagarro sind überzeugt, dass die Art von nicht-hierarchischer Struktur, die wir leben, die Zukunft der IT-Branche ist.

Ich habe dafür einen passenden Vergleich: Stellen Sie sich vor, wie die ägyptischen Pyramiden gebaut wurden – Tausende von Arbeitern, organisiert in einer typischen Hierarchie. Wenn man die Pyramiden heute bauen würde, käme vermutlich ein kleines, selbstorganisiertes Team mit hochmodernen Werkzeugen für das Schneiden und Bewegen von Steinen zum Einsatz. Genau so sehen wir die Entwicklung mit KI.

it management: *Nagarro hat eine eigene `University` aufgebaut. Sind solche internen Bildungseinrichtungen die Zukunft der IT-Weiterbildung?*

Dr. Manas Human: Ich bin davon überzeugt, dass Weiterbildungsprogramme in Unternehmen die klassischen Universitäten mehr und mehr ergänzen und nicht ersetzen werden. Tatsächlich hat Nagarro dabei geholfen, die Plaksha University in Indien mitzugründen – eine gemeinnützige Universität, die mit ihrem vierjährigen Bachelor-Programm den Schwerpunkt auf praxisorientiertes Lernen und Problemlösung legt. Parallel dazu sorgt unsere interne Bildungsplattform NagarroU dafür, dass wir alle auch im Berufsalltag kontinuierlich lernen, denn Bildung ist natürlich etwas, das uns ein Leben lang begleitet.

Das Lernen kann sich dabei sowohl auf Soft Skills als auch auf spezialisierte Technologiegebiete beziehen. Ich selbst habe zum Beispiel über NagarroU einen Kurs zur Stimmmodulation belegt, der mir enorm geholfen hat. Andere wiederum haben vielleicht einen Kurs zur Leitung großer Projekte oder zu einem bestimmten Aspekt von KI besucht. NagarroU fördert dabei eine lebendige Peer-to-Peer-Lernkultur. Foren, Diskussionsplattformen und Kollaborationsräume sind dynamische Begegnungsräume, in denen Wissen geteilt, Lösungen ausgetauscht und gegenseitige Unterstützung gelebt wird.

it management: *Herr Dr. Human, wir danken Ihnen für dieses Gespräch.*

Die nächste Welle der KI

DISRUPTION, INNOVATION UND DIE ZUKUNFT DER INTELLIGENZ

Die Welt steht am Beginn einer neuen Ära: Künstliche Intelligenz (KI) entwickelt sich nicht nur weiter: Sie definiert unsere Vorstellung von Arbeit, Technologie und Innovation neu. Die Jahre 2023 bis 2025 markieren eine beispiellose Disruptionswelle. Was als experimentelles Werkzeug begann, transformiert nun ganze Branchen, Denkweisen und Geschäftsmodelle. Die KI-Zukunft hat begonnen – und sie ist schneller, strategischer und intelligenter, als wir es je erwartet hätten.

Von der Spielerei zur Systemtransformation

Die Entwicklung künstlicher Intelligenz in Unternehmen lässt sich in drei Phasen skizzieren: 2023 war das Jahr des Experimentierens mit generativer KI wie ChatGPT. 2024 leitete die Adoptionsphase ein mit konkreten Pilotprojekten, besonders im Kundenservice und Marketing. 2025 schließlich markiert den Wendepunkt: Unternehmen erkennen, dass KI keine Ergänzung ist, sondern eine Plattform für eine neue Realität der Wertschöpfung.

Doch die Wahrheit ist ernüchternd: Nur rund 1 % der Unternehmen weltweit gelten derzeit als KI-reif. Das Potenzial ist enorm – ebenso wie die Herausforderungen. Datenqualität, Governance, Infrastruktur und ethische Fragen erfordern einen tiefgreifenden Wandel in Organisationen.

Drei Wendepunkte im Sommer 2025

#1 Tesla vs. Nvidia: Der Kampf um die Chip-Hoheit

Tesla hat einen 16,5-Milliarden-Dollar-Deal mit Samsung abgeschlossen, um eigene KI-Chips für autonome Systeme und Roboter zu produzieren. Das ist ein Frontalangriff auf Nvidias Dominanz. Diese vertikale Integration bedeutet nicht nur Unabhängigkeit, sondern signalisiert den Aufstieg maßgeschneiderter Hardwarelösungen, optimiert für spezifische KI-Zwecke. Ähnlich wie Apple einst den M-Chip einführte, markiert Tesla nun den Beginn einer neuen Ära spezialisierter KI-Infrastrukturen.

#2 ChatGPT-5 und der Sprung zur Agentenintelligenz

Im August 2025 veröffentlichte OpenAI GPT-5, wenn auch mit Startschwierigkeiten bei der Qualität der Ergebnisse. Erwartet wird in Zukunft eine „materielle" Verbesserung, insbesondere im Langzeitgedächtnis, der Multimodalität (Text, Bild, Audio, Video) und den Agentenfunktionen. Damit könnte KI von einem bloßen Antwortsystem zu einem autonomen Akteur werden, der proaktiv Aufgaben übernimmt, Prozesse steuert und Schnittstellen eigenständig bedient.

#3 Cognigy – Deutschlands KI geht global

Die Übernahme des Düsseldorfer KI-Unternehmens Cognigy durch NiCE zeigt: Auch Europa kann im globalen KI-Markt durch Spezialisierung und Exzellenz Akzente setzen. Cognigy entwickelt KI-basierte Lösungen für den automatisierten Kundenservice. Die zentrale Technologie von Cognigy ist die sogenannte „Conversational AI", also intelligente virtuelle Assistenten und Chatbots, die in Contact Centern eingesetzt werden, um die Kom-

munikation mit Kunden und Mitarbeitenden zu automatisieren und zu verbessern. Cognigy bleibt als Marke erhalten und wird zum globalen Kompetenzzentrum für Enterprise-Kundenservice mit Conversational AI.

Der Markt verändert sich schneller als je zuvor

Die Marktlandschaft wird fragmentierter und intelligenter. Während OpenAI mit GPT-5 dominiert, positionieren sich Anbieter wie Google (Gemini), Anthropic (Claude), Perplexity und xAI (Grok) durch Spezialisierung. Parallel dazu wächst der Markt für KI-Hardware mit Nvidia (78 % Marktanteil, jedoch rückläufig), AMD, Intel und neuen Eigenentwicklungen von Apple, Google, Tesla und Amazon.

Die neue Architektur der KI-Disruption: Fünf Achsen der nächsten Innovationswelle

Die disruptive Kraft der KI speist sich zunehmend aus tiefgreifenden technologischen und strukturellen Verschiebungen. Die folgende Übersicht zeigt, welche fünf Innovationsachsen die nächste Phase der KI-Evolution prägen:

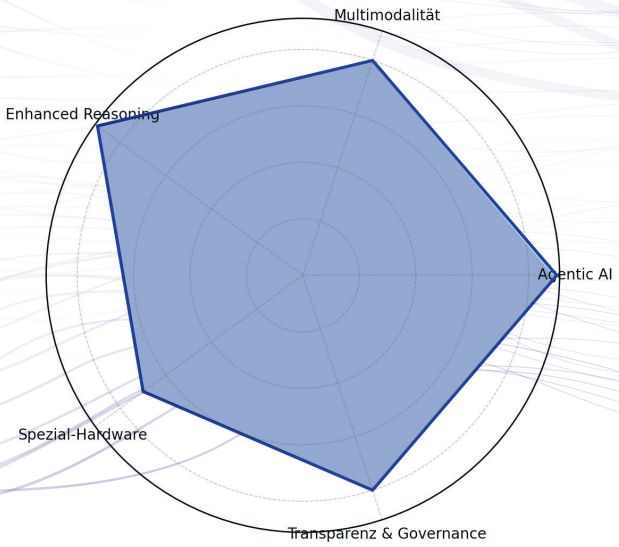
Agentic AI: Diese erste Säule beschreibt autonome Systeme, welche nicht mehr passiv auf Eingaben reagieren, sondern aktiv planen, ausführen und nachsteuern. Diese Systeme übernehmen eigenständig Multi-Step-Tasks wie Recherche, Planung und Umsetzung, führen API-Calls durch und interagieren mit Softwaresystemen. Sie steuern bereits Workflows in IT, HR oder Supply Chain, beispielsweise bei Urlaubsanträgen oder Bestellprozessen. Der entscheidende Paradigmenwechsel liegt darin, dass aus Chatbots digitale Mitarbeiter mit eigenen Verantwortungszonen werden.

Multimodalität: Die zweite Innovationsachse bewirkt eine Verschmelzung der Sinneskanäle. Moderne KI-Modelle wie GPT-5 oder Gemini 2.5 Pro verarbeiten Text, Sprache, Bilder, Audio, Video und strukturierte Daten simultan. Dies ermöglicht natürliche Dialoge mit Bildbezug, etwa in Design oder Technik, und fördert völlig neue UX-Konzepte für Support- oder E-Learning-Anwendungen. Multimodalität erweist sich als Schlüssel zu natürlich wirkender Mensch-Maschine-Interaktion.

Enhanced Reasoning: Als dritte Säule markiert diese den Wandel vom Muster zur Kognition. Die neue Generation von Modellen kann Ursache-Wirkung-Zusammenhänge ableiten, etwa in juristischen Analysen, langfristige Planung durchführen, beispielsweise im Projektmanagement, und sogar Reflexionsprozesse starten, um Lösungen zu optimieren. Dadurch entwickelt sich KI von einem Automatisierer zum kognitiven Co-Piloten.

Spezial-Hardware: Die vierte Innovationsachse umfasst maßgeschneiderte Lösungen statt allgemeine Ansätze. General-Purpose-GPUs werden zunehmend durch Spezialchips ersetzt, wobei Tesla AI-Chips, Google TPUs oder Apple Silicon ihre jeweiligen Plattformen dominieren. Diese sind leistungsfähiger, energieeffizienter und anwendungsspezifisch ausgelegt, was Realtime-Entscheidungen bei

ARCHITEKTUR DER KI-DISRUPTION



Grafik 1:
Die Architektur der KI-Disruption als Radardiagramm. Sie visualisiert die fünf zentralen Innovationsachsen und ihre strategische Relevanz.

Quelle: it research

gleichzeitigem Edge-Einsatz ermöglicht. Hardware wird damit zur strategischen Waffe und nicht nur zur Rechenressource.

Transparenz & Governance: Die fünfte und abschließende Achse macht KI erklärbar und regelbar. Die gesellschaftliche Akzeptanz hängt maßgeblich an der Nachvollziehbarkeit ab. Explainable AI (XAI) hilft dabei, Black-Box-Modelle zu entmystifizieren, während Governance-Frameworks wie der EU AI Act auditable Systeme verlangen. Unternehmen schaffen zunehmend neue Rollen wie Ethikbeauftragte oder Governance Engineers, um diesen Anforderungen gerecht zu werden. (Grafik 1)

Arbeitsmarkt im Wandel: Zerstörung oder Befreiung?

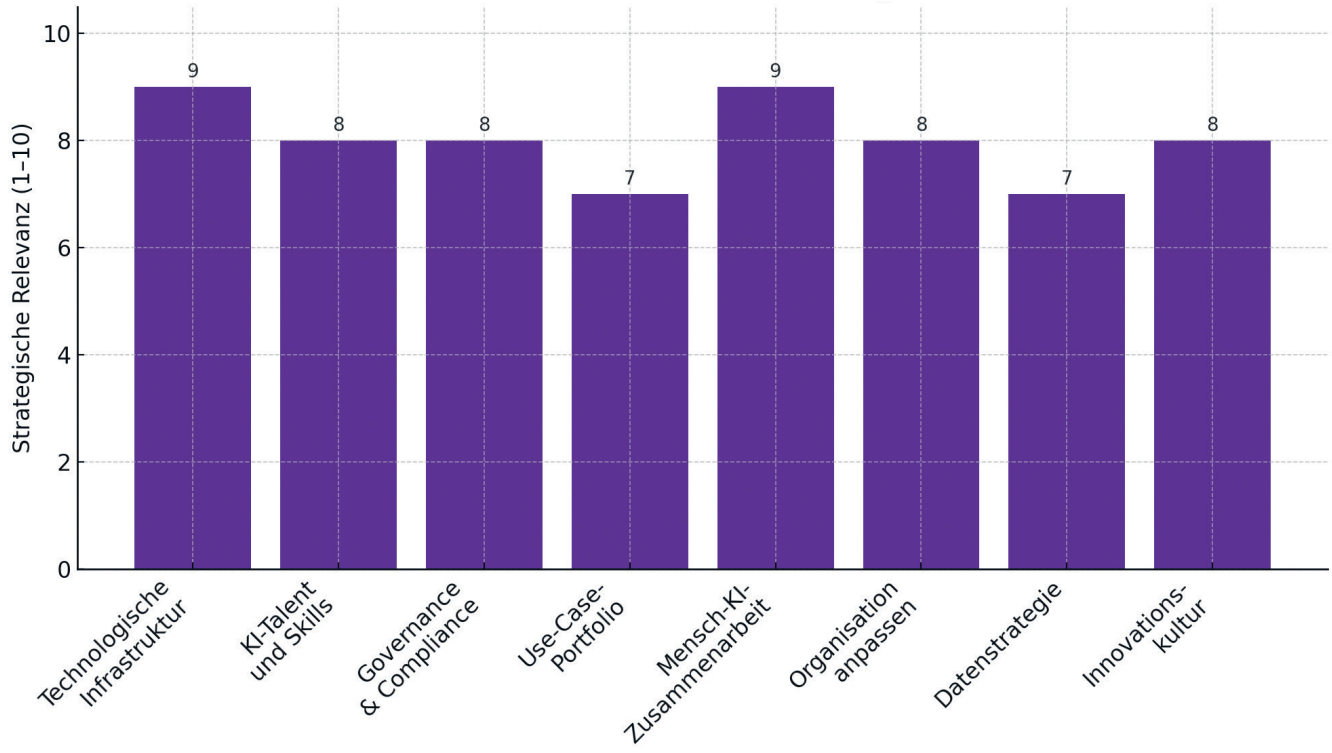
Die Automation repetitiver Aufgaben ist Realität. Prognosen wie die von Anthropic (20 % Arbeitslosenquote möglich) sind alarmierend, aber differenziert zu betrachten. KI ersetzt nicht nur, sie transformiert. Neue Rollen entstehen an der Schnittstelle zwischen Mensch und Maschine: Supervisoren, Prompt-Ingenieure, KI-Governance-Spezialisten.

Die Arbeitswelt entwickelt sich hin zur Superagency: Menschen delegieren repetitive Aufgaben an KI und konzentrieren sich auf Kreativität, Strategie und Empathie.

Zukunftssicherheit durch KI-Strategie

Unternehmen, die heute handeln, sichern sich entscheidende Vorteile. Erfolgreiche KI-Transformation benötigt ein neues Denken.

DIE 8 SÄULEN DER KI-STRATEGIE

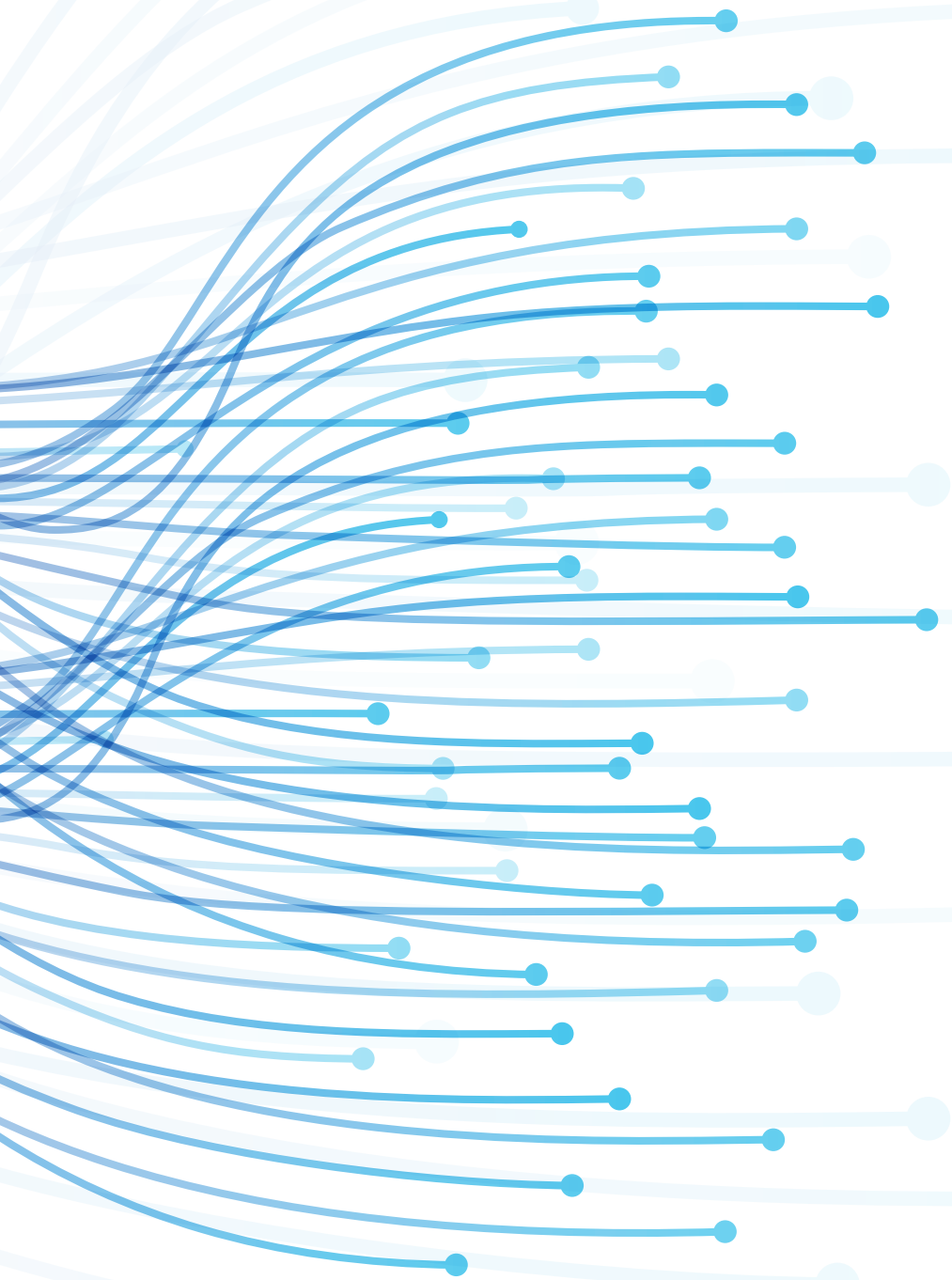


Technologische Führerschaft ohne gesellschaftliche Verantwortung wird nicht skalieren.

Dabei ist KI kein reines Technologieprojekt, sondern ein strategisches Thema. Neue Führungsrollen wie Chief AI Officer gewinnen an Bedeutung, um die Verantwortung über Abteilungen hinweg zu bündeln.

Und was kommt als nächstes?

Zwei Schlüsseltechnologien stehen im aktuellen Gartner Hype Cycle für Künstliche Intelligenz klar im Rampenlicht: KI-Agenten und KI-fähige Daten. Sie zählen zu den dynamischsten Entwicklungen des Jahres und sorgen für hohe Erwartungen – nicht selten gepaart mit überzogenen Hoffnungen. Beide Technologien haben derzeit den Höhepunkt der Phase der „überzogenen Erwartungen" erreicht. (Grafik 2)



Grafik 2 (links): Die „8 Säulen der KI-Strategie – sie zeigt die wichtigsten Handlungsfelder für Unternehmen im KI-Zeitalter.

Quelle: it research

Der Hype Cycle veranschaulicht, wie sich Technologien im Zeitverlauf entwickeln – von ersten Impulsen bis hin zur marktreifen Umsetzung. Die Methodik bietet Entscheidungsträgern eine fundierte Orientierungshilfe: Welche Technologien sind relevant? Wo stehen sie aktuell? Und welches Potenzial haben sie für konkrete Geschäftsziele?

„KI-Investitionen bleiben auf einem hohen Niveau. Doch der Fokus verschiebt sich zunehmend – weg von generativer KI als Allzwecklösung, hin zu den technologischen Grundlagen für nachhaltige Skalierbarkeit und Echtzeitfähigkeit", erklärt Haritha Khandabattu, Senior Director Analyst bei Gartner. „KI-Agenten und intelligente Datenstrukturen sind entscheidend für den nächsten Entwicklungsschritt."

Auch andere Technologien zeigen laut Gartner hohes Potenzial für eine breite Anwendung innerhalb der nächsten fünf Jahre, etwa multimodale KI-Systeme oder KI-TRiSM (Trust, Risk and Security Management). Beide gelten als entscheidend für verantwortungsbewusste und robuste KI-Anwendungen, die Geschäftsprozesse nachhaltig verändern können.

Fazit: Die KI-Zukunft ist da, aber sie verlangt Entscheidungen

Die Zukunft der KI ist keine lineare Fortschreibung, sondern ein exponentieller Sprung. Wer Künstliche Intelligenz als reines Werkzeug betrachtet, unterschätzt ihren disruptiven Charakter. Wer sie hingegen als Plattform für Innovation, Effizienz und Mensch-Maschine-Symbiose versteht, kann ihre volle Kraft entfalten.

Ulrich Parthier

Industrial AI

WARUM CHATGPT ALLEIN NICHT REICHT

Dan Matthews ist Chief Technology Officer (CTO) bei IFS, einem Anbieter von Industrial AI und Enterprise-Software. Im Interview mit Lars Becker, Redakteur it security, erklärt er, warum Industrial AI sich grundlegend von Consumer AI unterscheidet, welche Rolle Agenten in kritischen Infrastrukturen spielen können und warum Datenqualität entscheidend ist.

Lars Becker: *Herr Matthews, was unterscheidet Industrial AI von der Consumer-AI, wie wir sie aus ChatGPT & Co. kennen?*

Dan Matthews: Nehmen wir einmal das Beispiel Wartung: Wenn ich ChatGPT frage, welche PMs wir haben, dann meine ich damit Preventive Maintenance und nicht „Premierminister" oder „Produktmanager". ChatGPT fehlt der industrielle Kontext. Man braucht das Verständnis für die industrielle Sprache, Zugriff auf Informationen, die oft nicht öffentlich verfügbar sind, zum Beispiel Wartungssysteme, technische Handbücher, Serviceanweisungen. Vor allem braucht man vollständige Nachverfolgbarkeit und Erklärbarkeit. Wenn die KI sagt, es ist okay, die Wartung eines Aufzugs um drei Wochen zu verschieben, will man wissen warum. Oberflächliche Antworten reichen nicht aus.

Lars Becker: *Welche KI-Technologien sind besonders relevant für die Industrie?*

Dan Matthews: Es ist ein Mix aus allem. Historisch gesehen gab es schon lange KI in der Industrie. Denken Sie an Machine Learning für Predictive Maintenance. Was sich in den letzten Jahren wirklich geändert hat, ist die Generative KI. Sie eröffnet völlig neue Anwendungsfälle. KI kann plötzlich Dinge tun, die früher menschliche Eingaben erforderten, wie Dokumente lesen und entsprechende Maßnahmen ableiten.

Der andere große Bereich sind die sogenannten Agenten. Wenn ein Lieferant per E-Mail meldet, dass sich eine Bestellung verzögert, muss normalerweise ein Mensch prüfen: Welche Kunden sind betroffen? Beeinflusst das unsere Lieferungen oder Produktion? Haben wir alternative Lieferanten? All diese Interaktionen können Agenten übernehmen.

Deshalb haben wir auch das Silicon Valley Startup „TheLoops" übernommen. Sie haben eine Agenten-Plattform entwickelt, die sehr gut für Industrial AI geeignet ist und die wichtigen Eigenschaften für industrielle Umgebungen mitbringt.

Lars Becker: *Was schätzen Sie, wie weit verbreitet ist denn Agentic AI derzeit in der Industrie?*

Dan Matthews: Es steht noch ganz am Anfang. Zunächst hat jeder irreführenderweise seinen Chatbot zum „Agenten" umbenannt. Wenn wir von Agenten sprechen, meinen wir mehrere Layers: aufgabenfokussierte Agenten für E-Mails oder Systemaktionen, aber auch koordinierende Agenten auf höherer Ebene. Das wird wirklich interessant. Hier können Prozesse vollständig autonom ablaufen, wobei Menschen nur noch bei Entscheidungen einbezogen werden. Das ist noch nicht sehr verbreitet, aber wir sehen enormes Potenzial.

Lars Becker: *Ist Agentic AI nicht riskant, besonders in kritischen Infrastrukturen?*

Dan Matthews: Das hängt vom Anwendungsfall ab. In regulierten Bereichen wie Luftfahrt oder Verteidigung wird es noch lange dauern, bis man keine menschliche Bestätigung mehr braucht, etwa bei der Freigabe eines Flugzeugs als flugtauglich. Aber man kommt sehr weit mit agentischem Verhalten.

Nehmen Sie einen Fehlerbericht: Jemand meldet eine Korrosion an einem Transformator. Heute wird das eingestuft, jemand schaut es an und plant einen entsprechenden Außendienst. Warum sollte das nicht ein Agent machen können? Er kann die Aktivität planen, Ersatzteile bestellen und basierend auf dem Technikbericht weitere Arbeitsaufträge erstellen.

IN REGULIERTEN BEREICHEN WIE LUFTFAHRT ODER VERTEIDIGUNG WIRD ES NOCH LANGE DAUERN, BIS MAN KEINE MENSCHLICHE BESTÄTIGUNG MEHR BRAUCHT. ABER MAN KOMMT SEHR WEIT MIT AGENTISCHEM VERHALTEN.

Dan Matthews, CTO, IFS, www.ifs.com/de

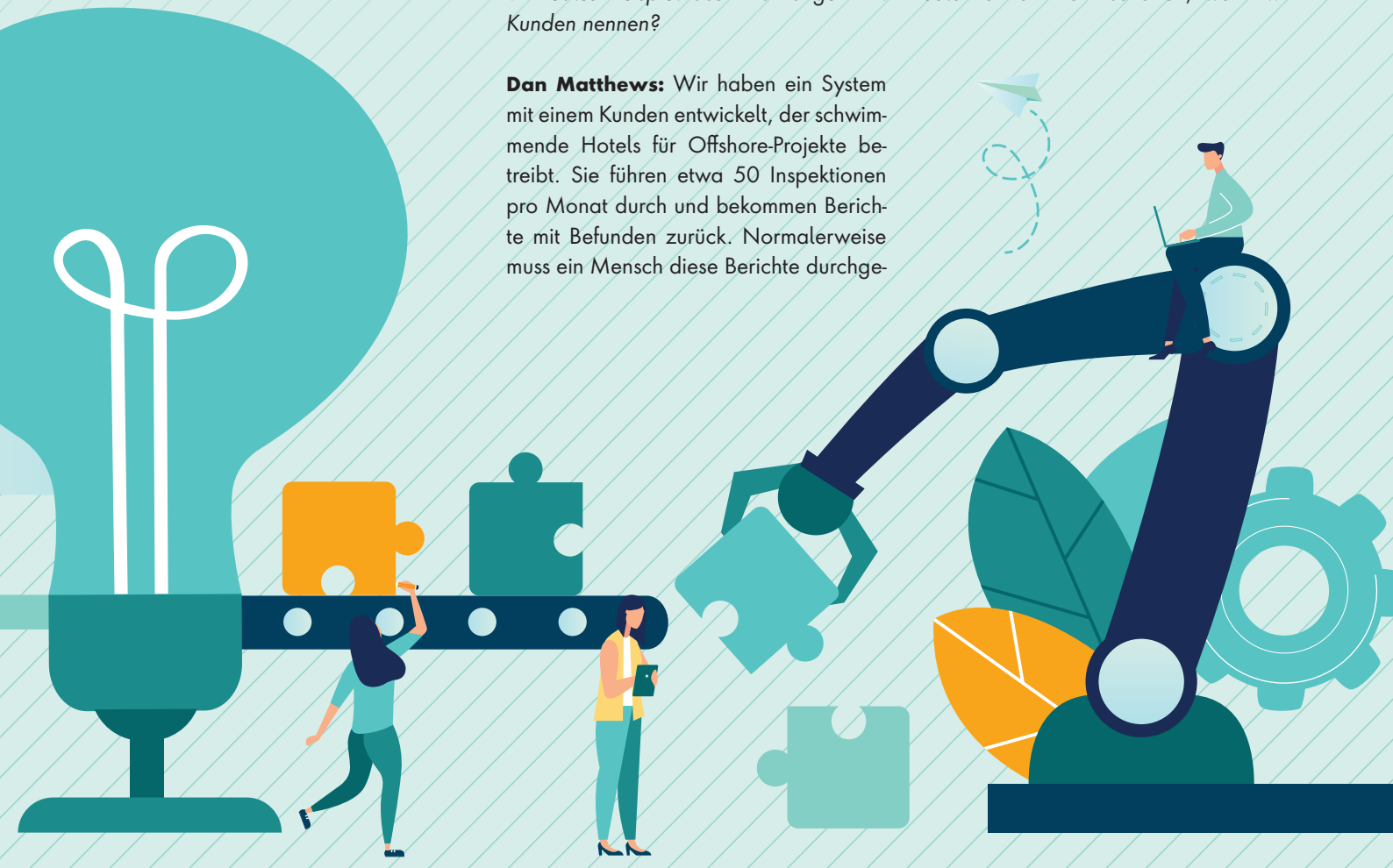
Lars Becker: *Können Sie auch ein reales Beispiel aus Erfahrungen mit Kunden nennen?*

Dan Matthews: Wir haben ein System mit einem Kunden entwickelt, der schwimmende Hotels für Offshore-Projekte betreibt. Sie führen etwa 50 Inspektionen pro Monat durch und bekommen Berichte mit Befunden zurück. Normalerweise muss ein Mensch diese Berichte durchgehen und entsprechende Maßnahmen im System anlegen.

Mit dem System ziehe ich einfach den Inspektionsbericht rein, die KI liest ihn und schlägt Arbeitsaufträge vor. Als Mensch kann ich mit der KI interagieren. Ich kann ihr sagen, dass wir für bestimmte Bereiche andere Pläne haben. Wenn ich zufrieden bin, werden die Aufträge erstellt. Das spart mindestens drei bis vier Stunden pro Bericht.

Lars Becker: *Ist das der Heilige Gral gegen den Fachkräftemangel?*

Dan Matthews: Teilweise ja. Der größte Fachkräftemangel besteht bei praktischen Tätigkeiten - Leute, die Strommasten oder Windräder hinaufklettern. Hier hilft KI, indem sie zum Beispiel vorhersagt, welche Ersatzteile benötigt werden, oder die Gerätehistorie für Techniker zusammenfasst. Dieselben 100 oder 1000 Leute können mehr schaffen, wenn wir



ihnen bei der Vorbereitung helfen. Aber ersetzen kann man sie nicht. Zumindest noch nicht heute oder morgen. Langfristig könnte man sich humanoide Roboter vorstellen, die Strommasten hinaufsteigen, aber das ist noch Zukunftsmusik.

Lars Becker: *Welche Rolle spielt die Datenqualität?*

Dan Matthews: Eine sehr große, und nicht nur Datenqualität, sondern auch die Existenz von Daten an sich. Glücklicherweise können wir auf hochwertige Datenquellen zugreifen. Technische Handbücher mit tausenden Seiten sind meist sehr akkurat. Wir kombinieren diese mit Wartungshistorien und anderen Systemdaten.

Aber manchmal haben Sie gar keine brauchbaren Trainingsdaten. Beispiel: Wir wollten eine KI entwickeln, die vorhersagt, ob Abrechnungen korrekt sind. Aber im System stehen nur genehmigte Ausgaben - abgelehnte werden korrigiert und dann genehmigt. Wie soll die KI lernen, was abzulehnen ist, wenn sie nur positive Beispiele sieht? Deshalb ändern wir manchmal die zugrundeliegenden Systeme wie etwa HR-Software, um mehr verwertbare Daten zu sammeln.

Lars Becker: *Nutzen Sie nur firmeninterne Daten oder auch externe Quellen?*

Dan Matthews: Wir kombinieren mehrere Quellen: Etablierte Large Language Models, die auf Internet-Inhalten trainiert wurden, Dokumente aus dem Document Management. Meist sind das Handbücher und technische Dokumentation sowie die eigentlichen operativen und transaktionalen Daten aus der Anwendung.

Wenn Sie fragen „Ist diese Windturbine in gutem Zustand?", schaut das System auf die Asset-Health-Daten, liest das Handbuch für die Definition von „gutem Zustand", sucht möglicherweise zusätzliche Informationen und kombiniert alles zu einer Antwort.

Lars Becker: *Welche Trends sehen Sie für die nächsten fünf Jahre in der Industrial AI?*

Dan Matthews: Drei große Trends: Erstens Agenten auf höherem Level. Zweitens - und das ist kritisch - Governance, Nachverfolgbarkeit und Vertrauen. Die Leute werden realisieren und fragen: „Wie kann ich dem vertrauen?" In industriellen Anwendungen brauchen wir erklärbare KI, nicht nur eine Magic Black Box, die heute eine Antwort gibt und morgen bei derselben Frage eine andere.

Drittens: Business-to-Business-Interaktionen zwischen Maschinen. Gartner nennt es „Machine Customers". Auf der Consumer-Seite wird es kommen, dass Alexa automatisch bei Amazon einkauft. Im Business-Bereich bin ich noch skeptisch, ob wir bereit sind, Agenten finanzielle Entscheidungen für unser Unternehmen treffen zu lassen.

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

Datenarchivierung

WORM SCHAFFT REVISIONSSICHERHEIT

Revisionssicherheit in der Archivierung und im Dokumentenmanagement ist ein Bestandteil diverser Compliance und Datenschutzvorschriften und soll sicherstellen, dass gespeicherte Daten und Dokumente nicht nachträglich unbemerkt verändert oder gelöscht werden können und jederzeit nachvollziehbar sind. Die sechs wichtigsten Kriterien, um Revisionssicherheit herzustellen, sind:

#1 **Unveränderbarkeit:** Einmal gespeicherte Daten dürfen nicht ohne Nachvollziehbarkeit verändert oder gelöscht werden.

#2 **Nachvollziehbarkeit / Protokollierung:** Jede Änderung (z.B. durch Versionierung oder Änderungsprotokolle) muss vollständig dokumentiert werden – inkl. Wer? Wann? Was?

#3 **Vollständigkeit:** Alle relevanten Informationen müssen vollständig archiviert werden.

#4 **Zugriffs- und Berechtigungskontrolle:** Nur befugte Personen dürfen Zugriff oder Änderungsrechte haben.

#5 **Maschinelle Lesbarkeit:** Dokumente sollten elektronisch lesbar und auswertbar sein.

#6 **Langfristige Verfügbarkeit:** Daten müssen über den gesetzlich vorgeschriebenen Zeitraum (z. B. 10 Jahre bei steuerlich relevanten Unterlagen) sicher gespeichert bleiben.

Allerdings gibt der Gesetzgeber bei Vorschriften wie GoBD, SEC, BAO, GeBÜV der FDA oder DSGVO nicht genau vor, wie die Revisionssicherheit technisch umgesetzt werden soll, um einer Überprüfung standzuhalten. Die technische Entscheidung und Umsetzung bleiben dem einzelnen Unternehmen überlassen.

An dieser Stelle setzt die moderne WORM-Technologie an. Revisionssicherheit für sensible Daten ist mit der WORM-Technologie für Unternehmen gleich welcher Größe oder Branche einfach zu realisieren und sie hat entscheidende Vorteile für lange Aufbewahrungsfristen. Die WORM-Archiv-Softwarelösung FileLock von GRAU DATA archiviert Daten komplett unabhängig von der existierenden Hard- oder Software-Umgebung revisionssicher nach GoBD. Der Vorteil: schnelle Entwicklungszyklen von Soft- und Hardware spielen mit dem WORM-Archiv keine Rolle. Für das WORM-archiv ist es unerheblich, ob es heute auf klassischer Festplatte oder morgen auf einer SSD-Platte egal von welchem Hersteller gespeichert ist.

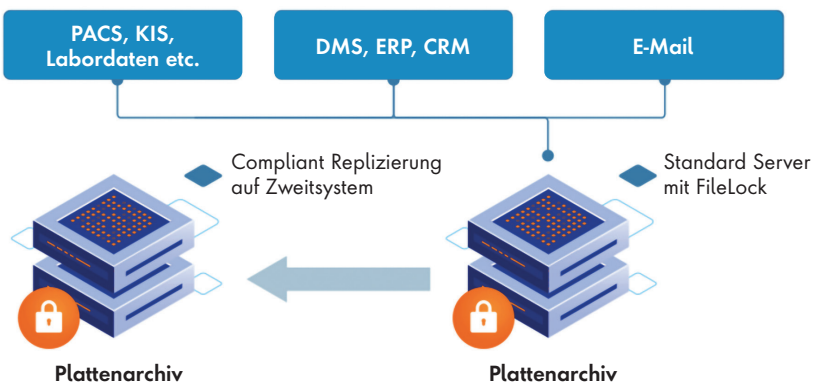
Funktionsweise des Software-WORM

Eine WORM-Software wie GRAU DATA FileLock eignet sich für den Einsatz auf standard Festplattensystemen und auf Windows-Dateisystemen für WORM-Funktionalität. Einmal gespeicherte Dateien werden mit einem Schreibschutz versehen und können anschließend zwar gelesen, aber weder verändert noch vor Ablauf einer definierten Aufbewahrungsfrist gelöscht werden. Die Verwaltung des Datenzugriffs erfolgt über eine spezielle Softwareschicht, die das Schreiben und Lesen von Daten auf der Festplatte oder im Speichernetzwerk kontrolliert. Idealerweise wird der WORM-Schutz auf einer separaten, versteckten Partition umgesetzt, wodurch ein manueller Zugriff, etwa mit Festplattenverwaltungs-Tools, wirkungslos bleibt. Eine zusätzliche Verschlüsselung der Daten erhöht die Sicherheit nochmals.

Fazit

Die revisionssichere Archivierung von Daten sollte mit minimalem administrativem Aufwand verbunden sein. Ein hoher Grad an Automatisierung entlastet IT-Abteilungen nachhaltig über viele Jahre. Gleichzeitig müssen gesetzliche und branchenspezifische Anforderungen an die Revisionssicherheit erfüllt werden – idealerweise durch geprüfte und zertifizierte Lösungen. Eine zukunftssichere Antwort bietet eine plattformunabhängige, schlanke WORM-Softwarelösung, die auch bei kontinuierlichem Datenwachstum und fortschreitender IT-Modernisierung dauerhaft zuverlässig funktioniert.

www.graudata.com



Ganzheitliche HR-Digitalisierung

WIE SAP SUCCESSFACTORS DIE PERSONALDIGITALISIERUNG ORCHESTRIERT

Bei Everllence, ehemals MAN Energy Solutions, arbeiten 15.000 Menschen in über 50 Ländern weltweit an technischen Lösungen für das Zeitalter der Klimaneutralität. Um auch bei der Personalarbeit auf Höhe der Zeit zu sein, standardisiert, digitalisiert und harmonisiert das Unternehmen die HR-Prozesse – mit SAP SuccessFactors als effektive Lösung.

Ein wichtiger Treiber von Everllence ist die Digitalisierung, und so entschied das Unternehmen vor einem Jahr, auch die unternehmenseigenen Prozesse in der Verwaltung und Organisation für die Zukunft aufzustellen. Aufgrund der umfassenden Aufgabenlandschaft rückte das Personalwesen schnell in den Vordergrund.

Aufbau einer global vernetzten HR-Plattform

Die Gründe für Everllence, die HR-Prozesse neu aufzustellen, lagen vor allem in den vielen administrativen Tätigkeiten und der manuellen Bearbeitung von Aufgaben rund um Urlaubsanträge, Zielgespräche und Trainings für die Mitarbeitenden, die mit viel Aufwand zulasten strategischer Überlegungen und der Personalbetreuungsquote einherging. Zudem waren wenige HR-Services gebündelt.

Ziel des Projekts war der Aufbau einer global vernetzten HR-Plattform, um klassische Personalprozesse rund um den Employee Life Cycle in allen Ländern zu standardisieren, harmonisieren, digitalisieren und automatisieren. Gleichzeitig sollten Personalverantwortliche entlastet werden, sodass sie sich auf wertschöpfende Aufgaben konzentrieren können. In diesem Zuge war es Everllence wichtig, alle Bestandteile einer digitalen Neuausrichtung zu betrachten – von Prozessen und Technologien über die Organisation bin hin zur gezielten Befähigung der Mitarbeitenden.

Die Wahl der HR-Systemarchitektur fiel bewusst auf die Cloud-Lösung SAP SuccessFactors als die neueste Entwicklung eines Personalinformationssystems (HRIS), die kontinuierlich auf dem neuesten Stand gehalten wird und den Mitarbeiterlebenszyklus von der Einstellung bis zur Pensionierung vollständig digital abbildet. Für die Umsetzung holte sich das Unternehmen MHP als Transformationspartner hinzu. Die Management- und IT-Beratung überzeugte in der Ausschreibung mit einem ganzheitlichen integrierten Ansatz, einem tiefen Verständnis für Prozesse und Technologien sowie der Erfahrung aus einem großen Referenzprojekt: der Implementierung von SAP SuccessFactors bei dem Automobilzulieferer Brose Fahrzeugteile, die mit der Digitalisierung des gesamten Personalwesens für 30.000 Beschäftigte an rund 70 Standorten in 25 Ländern einherging.

DANK DER EXPERTISE UND DES UMFASSENDEN KNOW-HOWS VON MHP IST UNS EINE SEHR ERFOLGREICHE TRANSFORMATION IM HR-BEREICH GELUNGEN.

Ingrid Rieken, CHRO, Everllence SE, www.everllence.com/

Schnelle Implementierung dank bewährter Frameworks

Ähnlich wie bei Brose sollte es bei Everllence laufen. Zuerst beleuchtete das 30-köpfige Team aus Beratung und Kunde die bestehenden unternehmensspezifischen Prozesse. Auf dieser Basis erstellte es ein globales Template, das den Arbeitsaufwand in der HR verringern und die Prozesse effizienter gestalten sollte. Erst dann wurde der Fokus auf die Einführung des neuen Systems, SuccessFactors als Standardsoftware aus der Cloud, gelegt.

Bestandteile waren die Module OpenText, um digitale Mitarbeiterdaten gesetzeskonform an zentraler Stelle zu speichern, zu erstellen und zu verwalten, Ingentis für den Bereich People Analytics sowie DocuSign/ProSign für das elektronische Unterzeichnen von Dokumenten.

Markus Gardner, Projektleiter bei MHP: „Entscheidend an dieser Stelle ist, den Grundstein für die technische Umsetzung früh mittels eines durchdachten, globalen Rollen- und Prozessdesigns zu legen. Damit einher gehen klar definierte Rollen und Verantwortlichkeiten sowie ein Modell für die spätere Zusammenarbeit."

Als Implementierungsmethode wählte das Team „Fast to Success", eine vorkonfigurierte Lösung, die initial gestartet werden kann und schon nach kurzer Zeit erste Erfolge sichtbar macht. Zudem erzielt sie eine hohe Nutzerakzeptanz und -zufriedenheit. Den Standard passte MHP kundenindividuell hinsichtlich des Rollen-, Prozess- und technischen Designs an. Durch die Konfigurationen wird sichergestellt, dass auf Everllence abgestimmte Prozesse auch mit der neuen Software

weiterhin wie gewünscht laufen. Darüber hinaus wurde auch die HR-IT-Landschaft adaptiert. Dabei fanden unter anderem Integrationen mit SAP HCM und Active Directory sowie eine Anbindung von IAS/IPS statt. Markus Gardner: „Hier kommt es stark auf die Beratungsleistung an. Grundsätzlich wichtig bei der Integration ist, dass alle Systeme, wie ein HCM-System für die Gehaltsabrechnung, mit SuccessFactors kommunizieren. Es muss also ein reibungsloser Daten- und Dokumentenaustausch verschiedener Quellsysteme gewährleistet werden."

GRUNDSÄTZLICH WICHTIG BEI DER INTEGRATION IST, DASS ALLE SYSTEME, WIE EIN HCM-SYSTEM FÜR DIE GEHALTSABRECHNUNG, MIT SUCCESSFACTORS KOMMUNIZIEREN.

Markus Gardner, Associated Partner, MHP Management- und IT-Beratung GmbH, www.mhp.com/de/

Mitarbeitende auf dem Weg mitnehmen

Die größten Herausforderungen bei dem Projekt lagen im Bereich Projektsteuerung und Priorisierung, im kurzfristigen Training und Enablement der Mitarbeitenden und im Change Management. Zeitpläne, durchdachte Konzepte und intelligentes Projektmanagement über „Change Request" boten hierbei wertvolle Unterstützung. In der Hypercare-Phase wurde besonderer Wert darauf gelegt, die Mitarbeitenden – vom CIO bis zum Key User – mit den neuen Prozessen und Technologien vertraut zu machen. Der Fokus lag auf der Kommunikation mit den Stakeholdern und einer positiven Feedbackkultur in Form von Info Sessions für die Führungskräfte, Schulungen für die Personalverantwortlichen sowie Klick-Anleitungen und Erklärvideos für die Mitarbeitenden. Ein gemeinschaftliches Event zum Go-live im firmeneigenen Museum in Augsburg rundete das Projekt ab – inklusive Lessons Learned für alle Mitarbeitenden.

Rundum verbesserte Employee Experience

In einem Zeitraum von nur 18 Monaten implementierten MHP und Everllence die volle SuccessFactors Suite in Deutschland und der Schweiz. Dies geht nicht zuletzt auf den agilen Entwicklungs- und Implementierungsprozess zurück. In einer ersten Projektphase wurden dabei die Module Employee Central, Recruiting, Onboarding und Learning Management live gesetzt. Everllence profitierte so schon von den Vorteilen der Transformation, während in Phase zwei die Module Performance & Goals, Succession & Development und Compensation & Variable Pay folgten. Aufgrund der hohen Relevanz war außerdem das Modul People Analytics Reporting Teil beider Projektphasen. Im nächsten Schritt folgt der globale Rollout auf weitere Länder, der Projektabschluss ist für das Jahr 2027 geplant.

Die Modernisierung der HR-Strukturen und -Prozesse zeigt bereits positive Effekte im Arbeitsalltag: Es gibt nur noch ein einheitliches, digitales System, das den gesamten Employee Lifecycle umfasst. Vom Urlaubsantrag über das Zielgespräch bis hin zur Weiterbildung wird alles per App organisiert. Alle Informationen sind schnell über wenige Klicks abrufbar und auf einen Blick ersichtlich. Papier und Excel-Listen gehören der Vergangenheit an. Durch globale Standards sind die Prozesse nun deutlich schlanker, harmonischer und effizienter. Die Anzahl administrativer Tätigkeiten konnte wesentlich reduziert werden.

Catrin Schreiner

THE STATE OF SMB IT FOR 2026

EINBLICK IN DIE DATEN ZU ITSM-REIFE, TOOL-LÜCKEN, KI UND AUTOMATISIERUNG

Kleine und mittlere Unternehmen (KMU) stehen an einem Wendepunkt in ihrer IT-Entwicklung. 2025 zeichnet sich als ein Jahr ab, in dem die Modernisierung der IT nicht länger optional, sondern eine betriebliche Notwendigkeit ist. Fragmentierte Systeme, wachsende Cyberrisiken, steigende Benutzererwartungen und begrenzte Ressourcen haben ein Umfeld geschaffen, in dem Stillstand nicht mehr tragbar ist.

Angesichts dieser Herausforderungen befinden sich viele KMU an einem Scheideweg. Die Erkenntnis, dass IT Service Management (ITSM) und IT Asset Management (ITAM) einen echten Mehrwert fürs Geschäft bringen können, ist unbestritten – aber dieses Bestreben in die Tat umzusetzen ist schwieriger denn je. Weltweit stellen Unternehmen sich dieselben drängenden Fragen: Halten wir mit unseren Mitbewerbern Schritt? Investieren wir in die richtigen Bereiche? Wie können wir mit begrenzten Budgets die Resilienz und die Performance der IT verbessern?

The State of SMB IT for 2026 liefert auf Basis aktueller Umfragedaten und fundierter Analysen einen ehrlichen Blick darauf, wo KMU heute stehen. Der Bericht beleuchtet die operativen Risiken mangelhafter Integration; zeigt wie die Kombination aus IT-Fachkräftemangel, Budgetdruck und zunehmender Komplexität bei der Gewährleistung von Systemsicherheit und Compliance den Alltag prägen; und welche Rolle KI als Hebel für Resilienz und Wachstum spielt.

WHITEPAPER DOWNLOAD

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

E-Rechnungspflicht

BEREIT FÜR DEN VERSAND AB 2027

Ab 2027 wird der Versand von E-Rechnungen im B2B Pflicht, darauf bereiten sich Unternehmen jetzt vor. xSuite eDNA ist eine flexible, cloudbasierte Austausch- und Konvertierungsplattform für Erstellung, Versand und Annahme elektronischer Rechnungen im XML-Format.

Seit Anfang dieses Jahres gilt in Deutschland die Pflicht zur Annahme von E-Rechnungen im B2B. Noch ist der Anteil eingehender, maschinenlesbarer E-Rechnungen bei den Unternehmen allerdings gering. Dies wird sich grundlegend ändern, wenn ab 1. Januar 2027 auch die Versandpflicht kommt. Viele Unternehmen haben bereits eine Lösung zur automatisierten Verarbeitung von Eingangsrechnungen im Einsatz. Nicht jede kann allerdings auch strukturierte XML-Rechnungen annehmen und verarbeiten, von der Erstellung und dem Versand ganz zu schweigen.

Als auf Rechnungsprozesse spezialisierter Softwarehersteller unterstützt xSuite seit Jahren die SAP-integrierte Verarbeitung von E-Rechnungen. Im Vorfeld der E-Rechnungspflicht hat der Hersteller bereits Mitte letzten Jahres mit xSuite eDNA (electronic Document Network Adapter) eine Cloudplattform auf den Markt gebracht, die beide Seiten bedient: zunächst die Annahme unterschiedlichster E-Rechnungsformate und ihre Umwandlung in ein einfach zu verarbeitendes, standardisiertes Format, seit Juni 2025 auch die Erstellung und den Versand von Debitorenrechnungen aus SAP SD in XML-Formaten (konform mit EN 16931).

Im SAP SD-Modul wird dafür ein Add-on (Transport) installiert, das auf die Nachrichtensteuerung in SAP zugreift. Bei Erstellen einer Faktura in SAP werden die relevanten Daten über die Nachrichtensteuerung abgerufen und an die Cloudbasierte Plattform xSuite eDNA übergeben. Diese führt diverse Prüfschritte gemäß EN 16931 durch (Datenintegrität, Pflichtfelder, Datentypen, Business Rules); Formatumwandlung und weitere Verarbeitungsschritte erfolgen dann vollständig in der Cloud.

Änderungen oder Erweiterungen wie neue E-Rechnungsformate oder -versionen werden zentral in der Cloud implementiert und stehen allen Kunden automatisch zur Verfügung. Dies reduziert auf Kundenseite den Aufwand für die Wartung und sorgt für hohe Flexibilität.

Unternehmen ziehen E-Mail-Versand noch vor

xSuite eDNA bietet zwei Möglichkeiten des Versands: per E-Mail in den Formaten BIS Billing, ZUGFeRD und XRechnung sowie über das Peppol Netzwerk (diverse Formate). Das Portfolio an Ländern und Portalen wird konsequent erweitert.

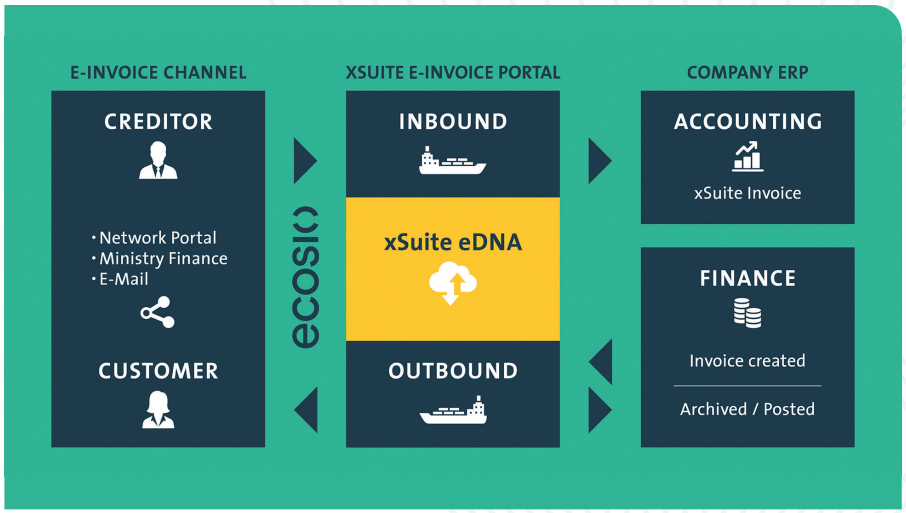
In Deutschland werden schwerpunktmäßig der bereits im B2G etablierte und durch die KoSIT zentral verwaltete deutsche Standard „XRechnung" sowie „ZUGFeRD" genutzt. Letzteres stellt eine hybride Rechnung dar, die aus einem Sichtteil im PDF-Format sowie einem maschinenlesbaren Teil im XML-Format besteht.

Einer xSuite-Umfrage zufolge nehmen 91 Prozent der Befragten das Format ZUGFeRD bereits an, gefolgt von der XRechnung mit 76 Prozent.

Wer auf Nummer sicher gehen will, realisiert zudem das Senden und Empfangen nach dem EU-Standard BIS Billing 3. Die Umfrage ergab auch, dass 95 Prozent der befragten Unternehmen klassischerweise auf den E-Mail-Versand zurückgreifen, während lediglich zehn Prozent bereits auf ein spezielles Portal setzen.

Die Pflicht zur Ausstellung von E-Rechnungen besteht übrigens nur national. Rechnungen aus dem Ausland unterliegen nicht der deutschen Gesetzgebung und können weiterhin als Papierrechnung oder in anderen Formaten versendet werden.

Dina Ziems | www.xsuite.com



ITSM im Bildungssektor

DIGITALE VERWALTUNG FÜR 27.000 USER

Die Stadt Chemnitz zeigt, wie der IT-Betrieb im öffentlichen Bildungssektor funktionieren kann. Mit einer Open Source-ITSM-Software verwaltet das Schulrechenzentrum den gesamten Lehrbetrieb, von interaktiven Tafeln bis zur Service-Infrastruktur. Und das für 27.000 User und über 15.000 Endgeräte.

Für Pioniere im Bildungssystem ist die drittgrößte Stadt in Sachsen schon lange bekannt. Gustav Zeuner etwa, einer der Begründer der Thermodynamik in Deutschland, wurde 1828 in Chemnitz geboren und wirkte dort. Oder Johann Traugott Sterzel. Er hat die naturwissenschaftliche und museale Bildung der gesamten Region entscheidend geprägt.

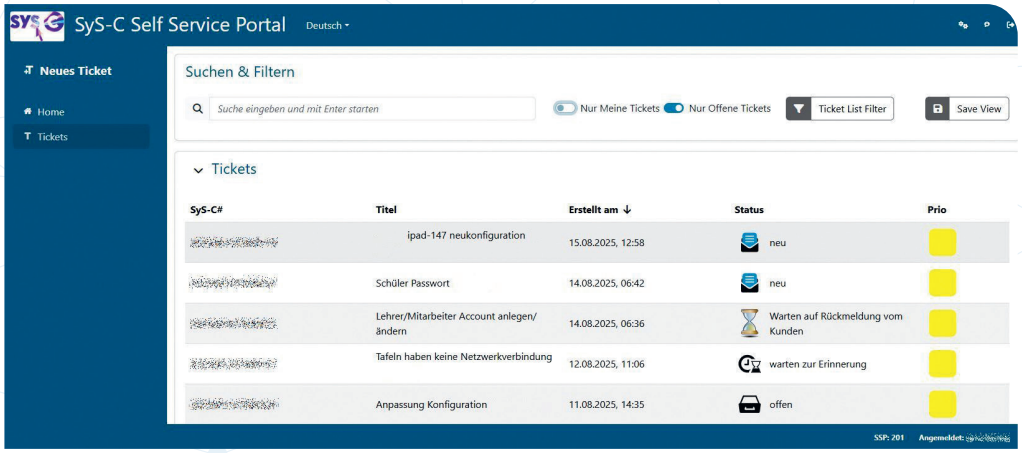
In den Chemnitzer Schulen geht es heute in erster Linie um Digitalisierung. Im Rahmen des Förderprogramms DigitalPakt Schule hat das Schulrechenzentrum Ende 2024 zusammen mit Bürgermeister Ralph Burghart die letzte interaktive Tafel übergeben. Die Modernisierung der Lehrbetriebe begann aber bereits 20 Jahre vorher – so lange existiert das Schulrechenzentrum schon.

Das Potenzial ausschöpfen

Seit der Jahrtausendwende nahm die Technik in den kommunalen Schulen stetig zu. Um diese fachmännisch zu administrieren, schuf die Stadt das Schulrechenzentrum als Systemlösung für die Schulen der Stadt Chemnitz, kurz SyS-C. Der Europäische Sozialfonds und das Bundesministerium für Bildung und Forschung unterstützten das Projekt am Anfang, 2009 wurde es sogar mit dem Innovationspreis Public Private Partnership ausgezeichnet.

Das kleine Team aus anfangs drei Personen konzentrierte sich vor allem auf vier Punkte: Die Homogenisierung und Vernetzung der Schul-IT, eine zentrale Verwaltung, eine vereinheitlichte Supportkultur und die Entlastung der pädagogischen IT-Koordinatoren (PITKOs). Doch mit steigender Gerätedichte, weiteren Lehrbetrieben und neuen Anforderungen wurde die Strukturierung der Supportprozesse zur zentralen Aufgabe.

Das SyS-C-Team um Leiter Sebastian Klost wollte die wachsenden Herausforderungen effizienter gestalten, aber gleichzeitig nicht an Flexibilität verlieren. Deshalb entschied sich das Team 2013, ein Ticketsystem



Per Self Service Portal können die User Probleme melden und die Lösung jederzeit transparent verfolgen.

einzuführen. Die Wahl fiel auf die IT-Service-Management-Software KIX, deren Hersteller ebenfalls in Chemnitz sitzt. Ausschlaggebend waren die vorhandenen OTRS-Kenntnisse der Mitarbeiter, aber auch die Nähe zum Dienstleister war ein Pluspunkt.

Die Pläne waren ambitioniert – zu ambitioniert für das kleine Team und die vielfältigen Aufgaben. Neben dem Endgerätesupport und der Infrastruktur wollten sie beispielsweise auch Neu- und Ersatzausstattungen aufnehmen, berichtet Michael Edler von der Planitz, IT-Administrator im SyS-C: „Wir hatten nicht die Kapazitäten, um unser System zu pflegen und alle Möglichkeiten zu nutzen. Aufgeben wollten wir es aber auch nicht – wir wussten, wie effizient es sein kann." Das Ziel blieb in den folgenden Jahren klar: Nicht nur ein Ticketsystem sollte es sein, sondern eine vollwertige ITSM-Lösung.

2022 änderte sich die Situation, als das SyS-C-Team personelle Verstärkung bekam. Mit nun 15 Mitarbeitenden, den damit einhergehenden Veränderungen in der Organisation und der weiterhin steigenden Zahl an Schulen wollten Michael Edler von der Planitz und seine Kollegen neu starten. Und zwar mit der neuesten Version ihrer ITSM-Software: „Die neue Version bot mit dem geänderten Design eine gute Möglichkeit, die Supportaufgaben neu aufzustellen", so Edler von der Planitz.

Effizient, transparent, digital

Mit dem Wechsel auf die aktuelle Version beschleunigte sich auch die Modernisierung des Supports. Heute ist das System die zentrale Anlaufstelle für alle Anfragen und Prozesse, ganz ohne Insellösungen oder Medienbrüche. Das SyS-C steuert damit alle Supportanfragen, Neu- und Ersatzausstattungen sowie Kommunikationsprozesse mit den Schulen, Auftragnehmern und Herstellern.

Insgesamt betreut das SyS-C 83 Schulen in Chemnitz – 42 Grundschulen, 15 Oberschulen, 7 Gymnasien, 12 Förder- und 7 Berufsschulen. Mit einem enormen Umfang an betreuter Infrastruktur: Über 27.000 Nutzer gehören zum Netzwerk – Schüler, Lehrer und Schulmitarbeiter. Hinzu kommen mehr als 15.000 Endgeräte, darunter rund 9.500 Tablets, 6.000 PCs, 1.700 Apple TVs und 600 Server. 2.400 Access Points und 500 Switches sichern die virtuellen Klassenzimmer ab. Darüber hinaus betreibt das SyS-C in Zusammenarbeit mit dem Medienpädagogischen Zentrum Chemnitz einen Showroom für Schulungen und Testszenarien. Das macht die Integration neuer Technologien nicht nur vorab erlebbar, sondern unterstreicht auch die enge Kooperation zwischen IT und Pädagogen.

> WIR WAREN AUF DER SUCHE NACH EINEM SYSTEM MIT VERSCHIEDENEN ZUGANGSWEGEN, ASSETMANAGEMENT, FAQS UND DER BEREITSTELLUNG VON KENNZAHLEN – UND DAS HABEN WIR GEFUNDEN.
>
> **Michael Edler von der Planitz, IT-Administrator, SyS-C, https://portal.sysc-chemnitz.de/**

Der Fokus des Schulrechenzentrums liegt auf effizienten Prozessen und transparenter Kommunikation. Das beinhaltet den Austausch zwischen SyS-C, PIT-KOs und Lehrkräften bei allen Anliegen rund um Hard- und Software. Und auch die Einbeziehung weiter Auftragnehmer wie Planungsbüros, IT-Firmen oder Bauunternehmen. Lässt sich ein Problem nicht auf Anhieb lösen, geht das Ticket direkt an den jeweiligen Hersteller – und so entsteht eine geschlossene Servicekette.

„Die User können uns über verschiedene Wege erreichen, per Mail, Telefon oder per Web. Alle Planungen kommen in der ITSM-Lösung zusammen. Gleichzeitig konnten wir durch die Open Source-Möglichkeiten einen IT-Stack einbinden, beispielsweise mit Univention und Opsi für das Access Management und die Inventarisierung. Das funktioniert einfach klasse", berichtet Edler von der Planitz. Rund 350 Ticket bearbeiten er und seine Kollegen monatlich. Alle Beteiligten können den Fortschritt ihres Tickets im Self Service Portal verfolgen. Durch die bessere Übersicht haben sich die Meldungen und Nachfragen per Mail bereits deutlich reduziert.

Mit Weitblick zum Ausbau

Den eingeschlagenen Kurs möchte das SyS-C auch in den kommenden Jahren beibehalten. Vor allem das Self Service Portal wollen die Mitarbeiter noch stärker zur zentralen Anlaufstelle für die User ausbauen. Und damit den Mailkontakt weiter reduzieren.

Außerdem möchte das SyS-C-Team Prozessabläufe wie etwa für das On- und Offboarding, Schadensmeldungen oder Garantiefälle erstellen, um für mehr Struktur zu sorgen. Den Aufbau des Assetmanagements auf Basis der ITSM-Lösung bereiten sie auch vor, sodass künftig alle Endgeräte systematisch in der zentralen CMDB verwaltet und deren Lebenszyklen nachvollzogen werden können.

Michael Edler von der Planitz blickt entspannt auf diese Aufgaben: „Wir waren auf der Suche nach einem System mit verschiedenen Zugangswegen, Assetmanagement, FAQs und der Bereitstellung von Kennzahlen – und das haben wir gefunden. Nicht nur unsere Arbeit ist effizienter geworden, sondern auch die der Anwender. Ich freue mich schon darauf, das System noch intensiver zu nutzen."

www.kixdesk.com

KI im Service-Management

REVOLUTION DER IT-SERVICES

Die Digitalisierung hat das Service-Management grundlegend verändert, doch der Einsatz von Künstlicher Intelligenz (KI) markiert einen Wendepunkt, der die Art und Weise, wie IT-Services bereitgestellt und verwaltet werden, revolutioniert. Unternehmen stehen vor der Herausforderung, komplexere IT-Infrastrukturen zu verwalten, während gleichzeitig die Erwartungen der Endnutzer an Verfügbarkeit und Servicequalität kontinuierlich steigen.

Die transformative Kraft der KI im ITSM

Künstliche Intelligenz im IT Service Management (ITSM) ermöglicht es Organisationen, von reaktiven zu proaktiven Servicemodellen überzugehen. Moderne KI-Systeme analysieren kontinuierlich Datenströme aus verschiedenen IT-Systemen, erkennen Muster und Anomalien und können potenzielle Probleme identifizieren, bevor sie sich auf die Endnutzer auswirken. Diese präventive Herangehensweise reduziert nicht nur die Anzahl der Incidents, sondern verbessert auch die Gesamterfahrung der Servicenutzer erheblich.

Die Implementierung von KI-gestützten Chatbots und virtuellen Assistenten hat die erste Kontaktebene des Service Desks revolutioniert. Diese intelligenten Systeme können eine Vielzahl von Standardanfragen automatisch bearbeiten, von Passwort-Resets bis hin zur Bereitstellung von Informationen über Servicestatus. Dabei lernen sie kontinuierlich aus Interaktionen und verbessern ihre Fähigkeit, komplexere Anfragen zu verstehen und zu bearbeiten.

Automatisierung und intelligente Ticket-Klassifizierung

Ein wesentlicher Vorteil von KI im Service-Management liegt in der automatisierten Klassifizierung und Priorisierung von Service-Tickets. Machine Learning-Algorithmen analysieren eingehende Anfragen, extrahieren relevante Informationen und ordnen sie automatisch den entsprechenden Kategorien zu. Dies führt zu einer deutlichen Reduzierung der manuellen Bearbeitungszeit und gewährleistet, dass kritische Issues sofort die angemessene Aufmerksamkeit erhalten.

Die intelligente Weiterleitung von Tickets an die am besten geeigneten Techniker oder Teams basiert auf historischen Daten, Expertise-Profilen und aktueller Arbeitsbelastung. Diese optimierte Ressourcenallokation führt zu schnelleren Lösungszeiten und einer höheren Mitarbeiterzufriedenheit, da Techniker an Aufgaben arbeiten, die ihren Fähigkeiten entsprechen.

Predictive Analytics und proaktives Service-Management

Die Anwendung von Predictive Analytics im Service-Management ermöglicht es Unternehmen, von einem reaktiven zu einem proaktiven Ansatz zu wechseln. KI-Systeme analysieren historische Daten, Leistungskennzahlen und Nutzungsverhalten, um vorherzusagen, wann Systeme gewartet werden müssen oder wann Kapazitätserweiterungen erforderlich sind. Diese vorausschauende Wartung reduziert ungeplante Ausfälle und optimiert die Ressourcennutzung.

KI-gestützte Wissensmanagement-Systeme

Moderne KI-Technologien revolutionieren auch das Wissensmanagement in Service-Organisationen. Natural Language Processing (NLP) ermöglicht es, unstrukturierte Daten aus verschiedenen Quellen zu analysieren und automatisch Wissensdatenbanken zu aktualisieren. KI-Systeme können relevante Lösungsartikel vorschlagen, basierend auf der Ähnlichkeit zu vergangenen Incidents, und dabei helfen, das institutionelle Wissen zu bewahren und zugänglich zu machen.

Integration von KI und ITSM in SAP-Umgebungen

Die Integration von KI-Funktionalitäten in SAP-Umgebungen stellt einen kritischen Erfolgsfaktor für viele Unternehmen dar, die bereits stark auf SAP-Systeme angewiesen sind. SAP-ITSM Integration beschreibt die automatisierte Verbindung von SAP-Systemen mit IT Service Management Plattformen und ermöglicht

Die Grafik zeigt die vier Ebenen des ISTM und wo KI ihren Platz findet.

Quelle: it research

konsistente, systemübergreifende Prozesse für Incidents, Changes und Service Requests.

Der SAP Solution Manager fungiert dabei als zentrale Plattform für IT Service Management in SAP-Landschaften. SAP IT Service Management ist ITIL-basiert, konform und zertifizierte Software zur Verbesserung und Verwaltung von IT-Services-Support und Betriebsaktivitäten. Die Integration von KI-Funktionen in diese Umgebung erfordert eine durchdachte Architektur, die die bestehende SAP-Prozesse respektiert und erweitert.

KI-Integration über SAP Business Technology Platform

SAP Integration Suite ist eine KI-gestützte Integrationsplattform as a Service (iPaaS), mit der Sie eine Vielzahl von Integrationsszenarien vereinfachen können. Diese Plattform bietet die ideale Grundlage für die Implementierung von KI-gestützten Service-Management-Lösungen in SAP-Umgebungen. Die Nutzung von Joule, SAPs KI-Assistent, ermöglicht es, Code zu generieren, Prozesse zu automatisieren und die Produktivität zu erhöhen.

Praktische Umsetzungsschritte für SAP-KI-Integration

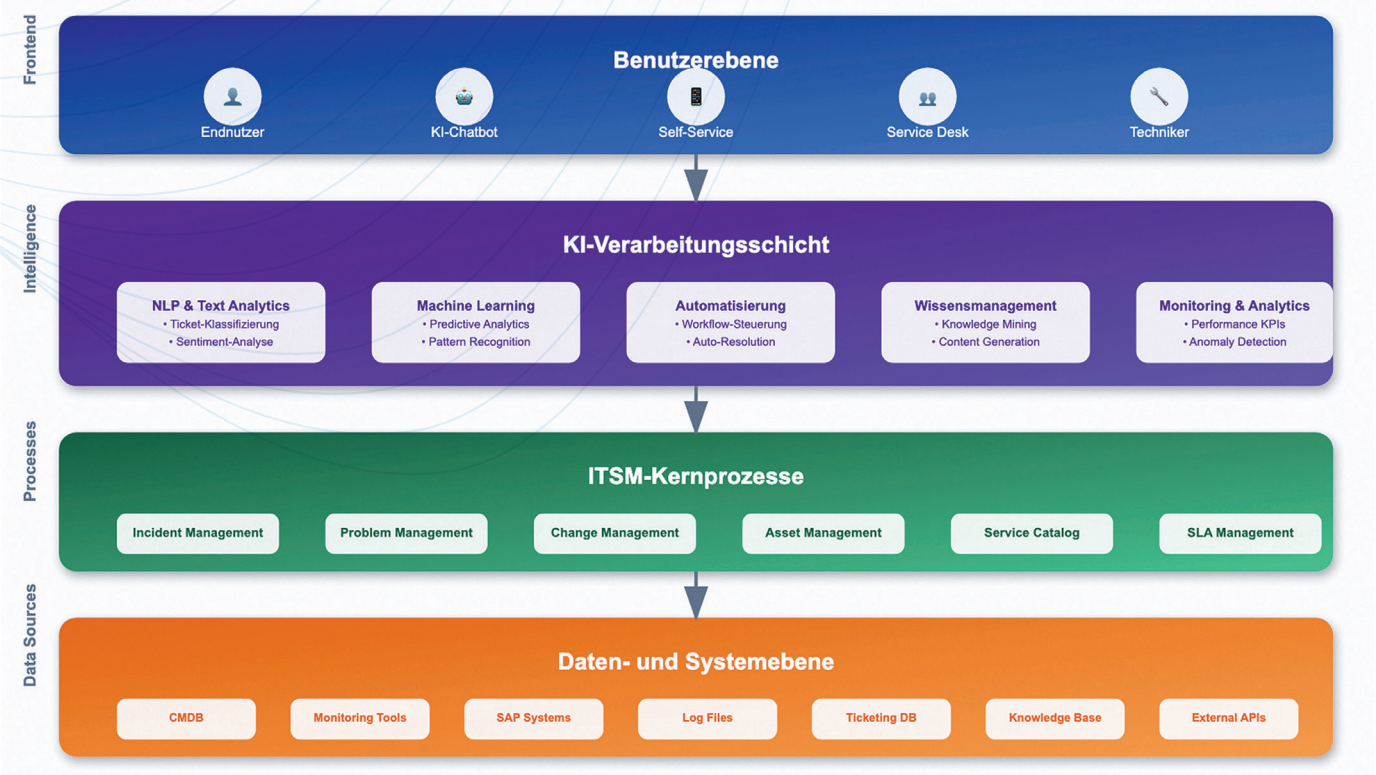
Die erfolgreiche Integration von KI in SAP-basierte ITSM-Umgebungen folgt einem strukturierten Ansatz. Zunächst müssen die bestehenden SAP-Systeme und ihre Datenflüsse analysiert werden, um Integrationspunkte zu identifizieren. Die Implementierung beginnt typischerweise mit der Anbindung von KI-basierten Chatbots an SAP-Service-Portale, gefolgt von der Integration intelligenter Ticket-Klassifizierung in SAP Solution Manager.

Die Datenintegration spielt eine entscheidende Rolle, da KI-Systeme auf qualitativ hochwertige, konsistente Daten angewiesen sind. SAP-Systeme verfügen bereits über umfangreiche Datenbestände, die als Trainingsgrundlage für Machine Learning-Modelle dienen können. Die Herausforderung liegt in der Harmonisierung dieser Daten und der Gewährleistung des Datenschutzes.

Herausforderungen und Erfolgsfaktoren

Die Implementierung von KI im Service-Management bringt verschiedene Herausforderungen mit sich. Datenqualität und -verfügbarkeit sind fundamentale Voraussetzungen für erfolgreiche KI-Anwendungen. Unternehmen müssen sicherstellen, dass ihre Datenbasis sauber, konsistent und umfassend ist. Das Change Management ist ein weiterer kritischer Faktor, da Mitarbeiter oft Bedenken bezüglich der Automatisierung ihrer Aufgaben haben.

KI-INTEGRATION IM SERVICE MANAGEMENT



Aber auch die ethischen Aspekte der KI-Nutzung im Service-Management dürfen nicht vernachlässigt werden. Transparenz in der Entscheidungsfindung von KI-Systemen ist essentiell, um Vertrauen bei Mitarbeitern und Kunden aufzubauen. Unternehmen müssen klare Richtlinien für die Nutzung von KI entwickeln und sicherstellen, dass menschliche Aufsicht und Eingriffsmöglichkeiten erhalten bleiben.

Zukunftsperspektiven und Trends

Die Zukunft des KI-gestützten Service-Managements wird von mehreren Trends geprägt sein. Hyperautomatisierung wird die Grenzen zwischen verschiedenen IT-Prozessen verschwimmen lassen und zu vollständig integrierten, selbstheilenden IT-Infrastrukturen führen. Edge Computing und 5G-Technologien werden neue Möglichkeiten für dezentrale KI-Anwendungen schaffen, die näher am Endnutzer agieren.

Die Entwicklung von Explainable AI wird dazu beitragen, die Akzeptanz von KI-Systemen zu erhöhen, indem sie ihre Entscheidungsprozesse transparenter macht. Dies ist besonders wichtig in regulierten Branchen, wo Nachvollziehbarkeit von Entscheidungen gesetzlich gefordert ist. Als Explainable AI (XAI) oder Erklärbare Künstliche Intelligenz wird der Bereich der KI bezeichnet, der sich darauf konzentriert, die Ergebnisse und Entscheidungen von KI-Systemen für Menschen verständlich zu machen. Ziel ist es, Transparenz und Nachvollziehbarkeit zu schaffen, damit Nutzer verstehen können, wie ein KI-Modell zu einem bestimmten Ergebnis gelangt ist.

Fazit

Künstliche Intelligenz transformiert also das Service-Management fundamental und ermöglicht es Unternehmen, effizientere, proaktivere und nutzerorientierte Services bereitzustellen. Die erfolgreiche Integration von KI in bestehende ITSM-Prozesse, insbesondere in SAP-Umgebungen, erfordert eine strategische Herangehensweise, die technische Implementierung, Change Management und ethische Überlegungen gleichermaßen berücksichtigt.

Unternehmen, die heute in KI-gestütztes Service-Management investieren, schaffen sich entscheidende Wettbewerbsvorteile und bereiten sich auf eine Zukunft vor, in der intelligente Automatisierung zum Standard wird. Der Schlüssel zum Erfolg liegt in der schrittweisen Implementierung, der kontinuierlichen Weiterentwicklung und der Bewahrung des menschlichen Elements in der Servicebereitstellung.

Ulrich Parthier

KI-ITSM IMPLEMENTIERUNGSROADMAP

Von der Strategieentwicklung zur vollständigen KI-Integration

So würde ein Zeit- und Ablaufplan für die KI-Implementierung aussehen.

Quelle: it research

Phase 1
Assessment & Strategie
3-6 Monate
- ✓ IST-Analyse
- ✓ Use Case Definition
- ✓ ROI-Bewertung
- ✓ Datenqualität prüfen
- ✓ Team-Skills bewerten
- ✓ KI-Roadmap erstellen
- ✓ Budget planen

Phase 2
Foundation & Pilot
6-9 Monate
- ✓ Infrastruktur setup
- ✓ Daten-Pipeline
- ✓ Chatbot Pilot
- ✓ Auto-Klassifizierung
- ✓ Team Training
- ✓ Governance Setup
- ✓ Erste KPIs messen

Phase 3
Core Implementation
9-15 Monate
- ✓ ML-Modelle trainieren
- ✓ Predictive Analytics
- ✓ Workflow-Automatisierung
- ✓ Knowledge Mining
- ✓ SAP-Integration
- ✓ User Rollout
- ✓ Performance tuning

Phase 4
Advanced Features
15-21 Monate
- ✓ Deep Learning
- ✓ Computer Vision
- ✓ Voice Analytics
- ✓ Edge AI
- ✓ Multi-Channel Integration
- ✓ Advanced Analytics
- ✓ API Ecosystem

Phase 5
Optimization & Scale
21+ Monate
- ✓ Global Rollout
- ✓ Hyperautomatisierung
- ✓ Self-Healing Systems
- ✓ Kontinuierliches Lernen
- ✓ Innovation Labs
- ✓ Ecosystem Partner
- ✓ ROI Maximierung

SAP-KI Integration

Technische Komponenten:
- SAP Business Technology Platform
- SAP Integration Suite
- Joule (SAP KI-Assistent)
- SAP Solution Manager

Integration Points:
- Service Desk Integration
- CMDB Synchronisation
- Workflow Automatisierung
- Monitoring & Alerting
- User Portal Integration
- Analytics & Reporting

Kritische Erfolgsfaktoren

Change Management:
- Frühzeitige Einbindung aller Stakeholder
- Kontinuierliche Kommunikation und Training
- Agile Implementierungsansätze

Datenqualität:
- Saubere, konsistente Datenbasis
- Data Governance etablieren
- Kontinuierliche Datenvalidierung

Governance & Compliance:
- KI-Ethik Richtlinien definieren
- Transparenz und Nachvollziehbarkeit sicherstellen

Performance Monitoring:
- KPIs definieren und kontinuierlich messen
- Feedback-Loops etablieren

Risiken & Herausforderungen

Technische Risiken:
- Legacy System Integration
- Skalierbarkeits-Herausforderungen
- Vendor Lock-in vermeiden

Organisatorische Risiken:
- Widerstand gegen Veränderungen
- Skill-Gap in KI-Technologien
- Unrealistische Erwartungen

Compliance & Ethik:
- DSGVO und Datenschutz
- Algorithmus-Transparenz

Performance Risiken:
- Model Drift und Degradation
- Falsch-positive Ergebnisse

ROI-Entwicklung über die Phasen

Phase 1	Phase 2	Phase 3	Phase 4	Phase 5
-15%	-5%	+25%	+45%	+75%

Kumulativer ROI
basierend auf Effizienzsteigerung, Kosteneinsparungen & Servicequalität

Lerninsel auf dem Hochschulcampus Schmalkalden

Berufsbegleitend studieren

MASTER INFORMATIK UND IT-MANAGEMENT

In der Berufspraxis sind Informatikerinnen und Informatiker gefragt, die neben fachlichem Wissen auch entsprechendes Management-Knowhow besitzen und sowohl die technischen als auch die wirtschaftlichen Fragestellungen eines Unternehmens verstehen. Diese Qualifikationen vermittelt das Masterstudium „Informatik und IT-Management" der Hochschule Schmalkalden. Neben informationstechnischem Vertiefungswissen erlangen die Studentinnen und Studenten die notwendige Kompetenz, aktuelle Trends und Entwicklungen im IT-Bereich bewerten zu können. Darüber hinaus werden Kompetenzen zur erfolgreichen Bewältigung von Führungsaufgaben trainiert, welche eine bereits vorhandene Führungsposition stärken können oder zum Aufstieg in eine Führungsposition befähigen.

Das Studium umfasst fünf Semester und ist mit Selbststudien- und Präsenzphasen so konzipiert, dass sich Berufstätigkeit und Studium optimal vereinbaren lassen. Die Prüfungen sind direkt in den Studienablauf integriert und finden während der mehrtägigen Präsenzphasen statt. Kleine Jahrgangsgruppen und eine individuelle Betreuung sorgen für hervorragende Studienbedingungen. Der nächste Studienkurs startet im Oktober 2025.

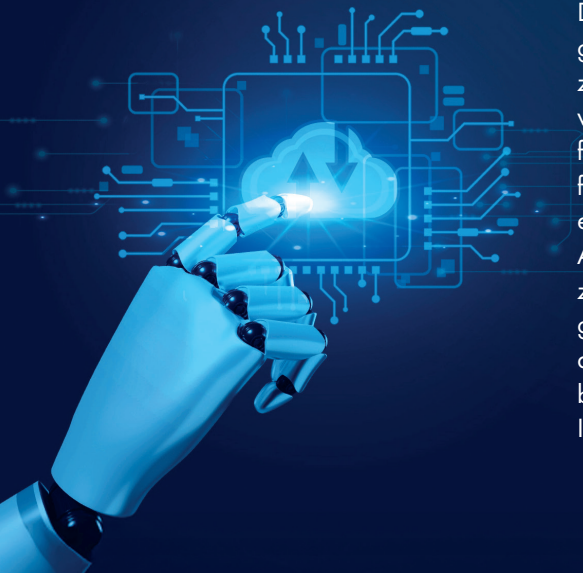
Zulassungsvoraussetzungen sind ein abgeschlossenes Informatik- oder Wirtschaftsinformatik-Studium bzw. ein Studium mit mindestens 50 Prozent Informatik-Inhalten sowie einschlägige Berufserfahrung von mindestens einem Jahr. Absolventinnen und Absolventen eines fachlich einschlägigen dualen Studiums können Praxiszeiten aus ihrem Diplom- oder Bachelorstudium, die über 20 Stunden pro Woche hinausgehen, angerechnet bekommen.

www.hsm-fernstudium.de

Digitale Technologien

WO STEHT DEUTSCHLAND?

Die Studie „Digitale Technologien made in Germany" beleuchtet Deutschlands Position im globalen Wettbewerb um fortgeschrittene Digitalisierungstechnologien und zeigt Wege auf, wie die Innovationskraft hierzulande gestärkt werden kann.



Ergebnisse der Studie im Überblick

Die Untersuchung belegt: Deutschland gehört in Bezug auf Weltklassepatente zu den fünf innovativsten Ländern weltweit. In Europa ist Deutschland sogar führend, insbesondere bei Technologien für vernetzte Mobilität und Energieeffizienz. Aber zugleich zeigt sich auch: Der Abstand zu globalen Innovations-Spitzenreitern wie den USA und China bleibt groß, in einzelnen Technologien auch der zu Südkorea und Japan. Südkorea beweist zudem, wie eine konsequente Innovationspolitik die Wirtschaft stark einbinden und Forschungsergebnisse effizient in die Praxis überführen und umsetzen kann.

Wir identifizieren in der Studie ein zentrales Problem, das Deutschland im globalen Technologiewettbewerb kennzeichnet: Es besteht oftmals eine Finanzierungslücke zwischen der öffentlich geförderten Grundlagenforschung und der kommerzialisierungsorientierten, privaten Investitionsphase. Die Studie empfiehlt Investitionsanreize und eine stärkere Zusammenarbeit zwischen Staat und Wirtschaft, um diese kritische Phase zu überwinden.

www.deloitte.com

MEHR WERT

Digitale Technologien made in Germany

Zukunftsfähige Hardware von Handy bis Data Center

UNABHÄNGIGES DEVICE AS A SERVICE-MODELL

Über Hardware zu reden, scheint im ersten Moment vielleicht nicht so attraktiv wie über Innovationen wie KI zu sprechen. Aber leistungsstarke, einsatzbereite Hardware ist die Basis, damit KI, Edge Computing, Data Center und Modern Workplace mit hybriden Arbeitsmodellen überhaupt funktionieren. Device as a Service-Modelle (DaaS) bieten Unternehmen die Möglichkeit, ohne hohe Anfangsinvestitionen ihre Hardware zukunftsfähig zu machen.

Bei DaaS denken viele an Endgeräte wie Laptop und Smartphone – und an herstellergebundene Verträge. Doch ein globales und herstellerunabhängiges DaaS-Modell gibt Organisationen drei attraktive Möglichkeiten: Sie können Devices unterschiedlicher Hersteller managen. Sie können Devices global verwalten. Und sie können neben PC, Laptop, Smartphone und Tablet auch Devices der Meetingraum-Technik und des Data Centers managen. Das ermöglicht einen Überblick über alle Devices und ein einheitliches Service-Modell.

DEVICE AS A SERVICE IST EIN STRATEGISCHES WERKZEUG, DAS UNTERNEHMEN DABEI UNTERSTÜTZT, IHRE HARDWARE VERÄNDERTEN ARBEITSWEISEN UND INNOVATIONEN ANZUPASSEN.

Dr. Jan Schaumburg, Director Solutions and Delivery, Insight DACH, de.insight.com

Wie funktioniert das Device as a Service-Modell?

Beim DaaS-Modell beziehen Unternehmen Devices unterschiedlicher Hersteller sowie Zubehör über einen externen Dienstleister. Dabei können Organisationen die Hardware entweder kaufen, oder zu einer festgelegten monatlichen Rate leasen. Der Dienstleister übernimmt aber nicht nur die Beschaffung der Hardware, sondern auch deren Bevorratung, Konfiguration, Versand, Reparatur und Modernisierung. Ist das End of Life oder End of Leasing der Geräte erreicht, werden die Devices ersetzt und die inaktuellen Komponenten nach einer zertifizierten Datenlöschung in den Produktkreislauf zurückgeführt oder zertifiziert recycelt.

Welche Vorteile bietet das DaaS-Modell?

➤ **Budget:** Durch den Wandel von einem Capex- in ein Opex-Modell können hohe Anschaffungsinvestitionen vermieden werden. Monatliche Raten schaffen Planbarkeit und Transparenz. Genaue Budgetierungsverfahren werden möglich.

➤ **Logistik:** Durch die Bevorratung von Hardware werden Lieferengpässe vermieden. Bestandsverfügbarkeitsberichte in Echtzeit sind möglich. Der Dienstleister übernimmt den Versand der Geräte an die Unternehmensniederlassung, das Homeoffice des Mitarbeiters oder das Data Center.

➤ **Organisation:** Aufgrund von Bevorratung und Leasing sind Unternehmen in der Lage, schnell ihre IT-Infrastruktur auf geänderte Anforderungen anzupassen. Dadurch, dass der Dienstleister entscheidende Aufgaben des Device-Managements übernimmt, werden interne IT-Abteilungen entlastet.

➤ **Globale Einheitlichkeit:** Ein international aufgestellter Anbieter hat die Möglichkeit, das DaaS-Modell global auszurollen und die Niederlassungen in unterschiedlichen Ländern und auf unterschiedlichen Kontinenten in das Device-Management einzubinden.

➤ **Security:** Das Unternehmen entscheidet zentral, welche Devices verschickt, wie sie konfiguriert und mit welchen Security-Tools sie versehen werden. Das schafft einheitliche Standards und vermeidet Schatten-IT.

➤ **Compliance:** Die zertifizierte Datenlöschung nach Ablauf der Nutzungsdauer sowie die zertifizierte Verschrottung eines nicht mehr reaktivierbaren Geräts stellen sicher, dass die Compliance in Bezug auf Daten gegeben ist.

➤ **Ökologische Nachhaltigkeit:** Durch die planvolle Rückführung der Devices

nach deren End of Life können sie als refurbished Hardware wiederverwendet oder fachgerecht recycelt werden. Das schont wertvolle Ressourcen.

Mobiles Arbeiten und KI-PCs

Durch das mobile Arbeiten verfügen Mitarbeitende heute oft über mehrere Devices: Laptop, Tablet, Smartphone – alles mit dem entsprechenden Zubehör. Das macht das Device-Management komplexer. Die Notwendigkeit von KI-fähigen Rechnern und der Wechsel von Windows 10 auf Windows 11 machen zudem in zahlreichen Fällen ein Upgrade der Hardware nötig. Investitionskosten und Aufwand beim Device-Management können mit Hilfe des DaaS-Modells verringert werden.

Zudem steigert DaaS die User Experience. Statt mehrere Wochen auf eine Komponente zu warten, können Mitarbeiter in Niederlassungen weltweit innerhalb von wenigen Tagen ein neues Device erhalten. Durch die Bevorratung ist es möglich, alle benötigten Geräte bereits konfiguriert in einem einzigen Paket an den Mitarbeiter zu senden, sogenanntes Bundling. Defekte Hardware kann schnell repariert oder ausgetauscht werden. Das alles erhöht entscheidend die User Experience. Zudem verbessert es die Nachhaltigkeitsbilanz. Aufgrund von Reparaturen wird Elektroschrott vermieden. Durch Bundling werden Verpackungsabfall und Lieferwege reduziert und dadurch CO2-Emissionen gesenkt.

Kollaboration ohne Grenzen

Moderne Besprechungsräume sollen heute eine nahtlose Verbindung zwischen Präsenz- und Fernteilnehmenden ermöglichen. Das Wichtigste aber ist: Die Technik muss reibungslos und zuverlässig funktionieren. Beim Meetingraum-Systeme as a Service-Modell unterstützt der Dienstleister herstellerunabhängig bei der Auswahl der Hardware unter Berücksichtigung von Raumgröße, Akustik und Nutzungsszenarien. Dann folgen Installation, Verkabelung und Testung der Hardware sowie die Implementierung der Software. Dabei wird jedes Gerät, jedes Kabel, jede Verbindung, jede Implementierung dokumentiert. Techniker überprüfen regelmäßig die Funktion aller Geräte und führen notwendige Updates durch, damit die Technik immer einsatzbereit ist. Sollte dennoch ein Defekt auftreten oder ein User Probleme bei der Inbetriebnahme des Meetingraums haben, steht ihm ein Help Desk zur Verfügung. Dank der technischen Dokumentation kann der Mitarbeiter den User durch die Problembehebung führen oder veranlassen, dass der Raum gesperrt wird, bis ein Techniker den Defekt behoben hat.

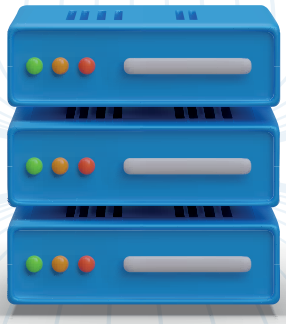
Daten vor Ort

Angesichts strenger Datenschutzanforderungen setzen viele Unternehmen weiterhin auf eigene Rechenzentren. Ein DaaS-Dienstleister kann die Beschaffung und Installation von Servern, Racks, Storages, Netzwerkausrüstung und Verkabelung durch ein professionelles Technikerteam übernehmen – und das global. Am Ende des Lebenszyklus werden die Komponenten ausgebaut und ersetzt. Auch bei der Hardware für Rechenzentren ist Bevorratung und Bundling möglich, sodass Logistikprozesse optimiert werden. Ergänzend besteht die Option, das Management des Rechenzentrums an den Dienstleister auszulagern, wodurch interne Ressourcen weiter entlastet werden.

Mit DaaS Innovation ermöglichen

Besonders in Zeiten, in denen Technologiezyklen immer kürzer werden, bietet DaaS die notwendige Flexibilität, um schnell auf neue Anforderungen reagieren zu können, ohne hohe Anschaffungsinvestitionen tätigen zu müssen. Somit ist Device as a Service mehr als ein reines Beschaffungsmodell. Es ist ein strategisches Werkzeug, das Unternehmen dabei unterstützt, ihre Hardware veränderten Arbeitsweisen und Innovationen anzupassen.

Dr. Jan Schaumburg



DIE UNTERSCHÄTZTE DATENBASIS

WARUM KI-PROJEKTE OFT SCHEITERN

Viele Unternehmen befinden sich mit ihren KI-Projekten noch immer in einer frühen Phase, treten scheinbar permanent auf der Stelle und erzielen so gut wie keinen echten Mehrwert. Diese Situation betrifft jedes dritte Unternehmen weltweit. Denn laut Schätzungen von Gartner scheitern 30 Prozent aller KI- und Generative-AI-Projekte noch in der Pilotphase. Dabei stoßen sie vor allem beim Versuch, ihre Use Cases über das gesamte Unternehmen zu skalieren, an ihre Grenzen.

Das kann verschiedene Gründe haben – zum Beispiel fehlendes Fachpersonal, welches sich mit KI-Technologien auskennt. In den meisten Fällen ist jedoch eine mangelhafte Datengrundlage der Übeltäter. Daten sind laut McKinsey für die Mehrheit der Unternehmen (72 Prozent) sogar die Hauptherausforderung bei dem unternehmensweiten Einsatz von KI.

Die zentrale Frage lautet daher: Hemmen Daten auch den Fortschritt des eigenen KI-Projekts? Wie kommt es dazu und welche Maßnahmen können dagegen helfen?

#1 Infrastrukturen sind zu komplex und Wissen zu verteilt

Mit jeder neuen Technologie, Systeminstanz und Anwendung wird die gesamte IT-Landschaft komplexer. Überall entstehen Daten in unterschiedlichen Formaten, die verarbeitet und gespeichert werden müssen. Dadurch verteilt sich das gesamte Wissen – all die geschäftsrelevanten Informationen – über sämtliche Umgebungen wie Cloud und On-Prem hinweg. So entstehen voneinander getrennte Informationssilos, die für KI-Modelle nur schwer zugänglich sind.

#2 Daten sind veraltet und unbrauchbar

Viele KI-Modelle werden einmalig mit einem bestimmten Datenkontingent verknüpft. Danach erfolgt häufig keine kontinuierliche Datenzufuhr. Aus Sicherheitsgründen wird zudem oft auf eine Anbindung an das öffentliche Internet verzichtet. Das bedeutet allerdings, dass ein Modell nur auf die anfänglich bereitgestellte Datengrundlage zugreifen kann. Dieser mangelt es an Aktualität; die neuesten Kunden-, Produkt- und Betriebsdaten fehlen. Alle Anfragen, die Informationen benötigen, die darüber hinausgehen, bergen das Risiko unpräziser, veralteter sowie lücken- und fehlerhafter Antworten.

#3 Ein Großteil des udgets fließt in kostspieliges Nachtrainieren

Ist das Problem der veralteten Daten einmal erkannt, fällt die Wahl häufig auf regelmäßiges Nachtrainieren um die Informationsgrundlage aktuell zu halten. Doch schon nach wenigen Durchläufen zeigt sich, dass dieser Prozess extrem aufwendig ist – sowohl personell, zeitlich als auch finanziell.

Damit KI-Anwendung genaue, hochwertige und geschäftsrelevante Antworten geben können, müssen folgende Voraussetzungen gegeben sein:

- Daten aus allen relevanten Quellen sind zentral und in Echtzeit zugänglich, um Vollständigkeit und Qualität zu gewährleisten.
- Der Zugriff entspricht höchsten Sicherheits- und Governance-Anforderungen.
- Die Datengrundlage bildet das tagesaktuelle Unternehmensgeschehen ab.

Mithilfe einer Plattform für zentrales Datenmanagement ist all das möglich. Hierfür kommt Datenvirtualisierung zum Einsatz. Anders als bei der klassischen Datenintegration werden die Zugänge zu zahlreichen Quellen entkoppelt, abstrahiert und zentral zusammengeführt. Konsumenten greifen über einen virtuellen Layer in Echtzeit auf die Unternehmensdaten zu – unabhängig davon, wo sie liegen. Die Daten müssen nicht in aufwendigen Prozessen dupliziert, verändert oder in ein weiteres Repository bewegt werden. Innovative Funktionen wie zum Beispiel Deep Research helfen zusätzlich dabei, komplexe Zusammenhänge zu analysieren, Daten zu verknüpfen und Ergebnisse verständlich zu erklären.

www.denodo.com/de


e3mag.com
DEUTSCH
Information und Bildungsarbeit von und für die SAP®-Community
The global independent platform for the SAP® community
ENGLISH
ESPAÑOL
La plataforma global e independiente para la comunidad SAP®
La plateforme indépendante mondiale de la communauté SAP®
FRANÇAIS
SAP® ist eine eingetragene Marke der SAP SE in Deutschland und in anderen Ländern weltweit.

SAP HANA Lock-in

WIE EINE DATENBANKBINDUNG STRATEGISCHE SPIELRÄUME EINSCHRÄNKT

Die strategische Entscheidung von SAP, mit S/4HANA ausschließlich auf die eigene HANA-Datenbank zu setzen, hat eine weitreichende Zäsur in der ERP-Landschaft geschaffen.Was einst als technologischer Durchbruch vermarktet wurde, entwickelt sich für viele SAP-Anwender zunehmend zu einer Herausforderung in Bezug auf digitale Flexibilität und strategische IT-Planung. Der Übergang von AnyDB – der Möglichkeit, verschiedene Datenbanksysteme wie Oracle, Microsoft SQL Server oder IBM DB2 zu nutzen – zu einer singulären Datenbankbindung hat tiefgreifende Auswirkungen auf Innovationsfähigkeit und Investitionsstrategien vieler Unternehmen.

Die Entstehung der HANA-Zentralität

Ursprünglich ermöglichte SAP seinen Kunden mit dem AnyDB-Konzept die freie Wahl der Datenbankplattform. Diese Flexibilität war ein wesentlicher Erfolgsfaktor, da sie es Unternehmen erlaubte, bewährte Datenbankinfrastrukturen zu nutzen und gleichzeitig von der Innovationskraft verschiedener Datenbankhersteller zu profitieren. Mit der Einführung von S/4HANA änderte sich diese Philosophie radikal: SAP koppelte sein modernisiertes ERP-System untrennbar an die eigene HANA-Plattform.

Diese strategische Wende grenzt SAP-Kunden stärker vom dynamischen Datenbankmarkt ab. Während Technologiegiganten wie Google mit Spanner und BigQuery, Microsoft mit Azure SQL und Cosmos DB, IBM mit DB2 und Watson, sowie Oracle mit Autonomous Database kontinuierlich neue Funktionalitäten entwickeln, sind SAP-Anwender auf die Innovationszyklen der HANA-Plattform beschränkt. Besonders im Kontext von Cloud-nativen Technologien, KI-Integration und modernen Datenarchitekturen bieten alternative Datenbanksysteme zum Teil spezialisierte Vorteile.

Kritische Stimmen aus der Anwendergemeinschaft

Die Deutschsprachige SAP-Anwendergruppe (DSAG) hat diese Problematik bereits früh erkannt und artikuliert ihre Bedenken zunehmend deutlicher. In ihrem Investitionsreport 2024 zeigt sich eine bemerkenswerte Zurückhaltung der Anwender: Trotz intensiver Bewerbung liegt SAP ERP bzw. die SAP Business Suite mit 68 Prozent weiterhin deutlich vor S/4HANA On-Premises mit 44 Prozent. Diese Zahlen verdeutlichen, dass sich Unternehmen den Wechsel auf S/4HANA genau überlegen und mögliche Auswirkungen sorgsam abwägen.

Die DSAG fordert von SAP eine Zukunfts-, Planungs- und Investitionssicherheit, die insbesondere für die Konsolidierung und Modernisierung der gewachsenen IT-Landschaften nötig ist. Die zentrale Frage, die DSAG-Technologievorstand Sebastian Westphal formulierte, bringt die Bedenken vieler SAP-Kunden auf den Punkt: „Wird wirklich niemand zurückgelassen?"

Steigende Lizenzkosten als Herausforderung

Parallel zur technischen Abhängigkeit ergeben sich auch finanzielle Herausforderungen für SAP-Kunden. Das E3-Magazin, eine wichtige Publikation der SAP-Community, weist auf Kostenrisiken im neuen Lizenzmodell hin. So können zu großzügig gesetzte Berechtigungen zu ungewollten Mehrkosten führen, wenn bestehende Berechtigungskonzepte ungeprüft auf S/4 migriert werden.

Zudem ist die ursprünglich als Migrationserleichterung beworbene Flat Fee für S/4HANA-Lizenzen heute nicht mehr allgemeiner Standard, was zu deutlich höheren Betriebskosten führen kann – insbesondere für Unternehmen, die bisher auf günstigere Datenbankalternativen gesetzt haben. Gleichzeitig profitieren diese Unternehmen nicht mehr von der technologischen Vielfalt und Dynamik anderer Datenbankanbieter.

ENTWICKLUNG DES HANA-MONOPOLS

BIS 2015

AnyDB-Ära: Freie Wahl zwischen Oracle, Microsoft SQL Server, IBM DB2 und anderen Datenbanken

2015

S/4HANA Launch: Einführung mit exclusiver HANA-Bindung

2025

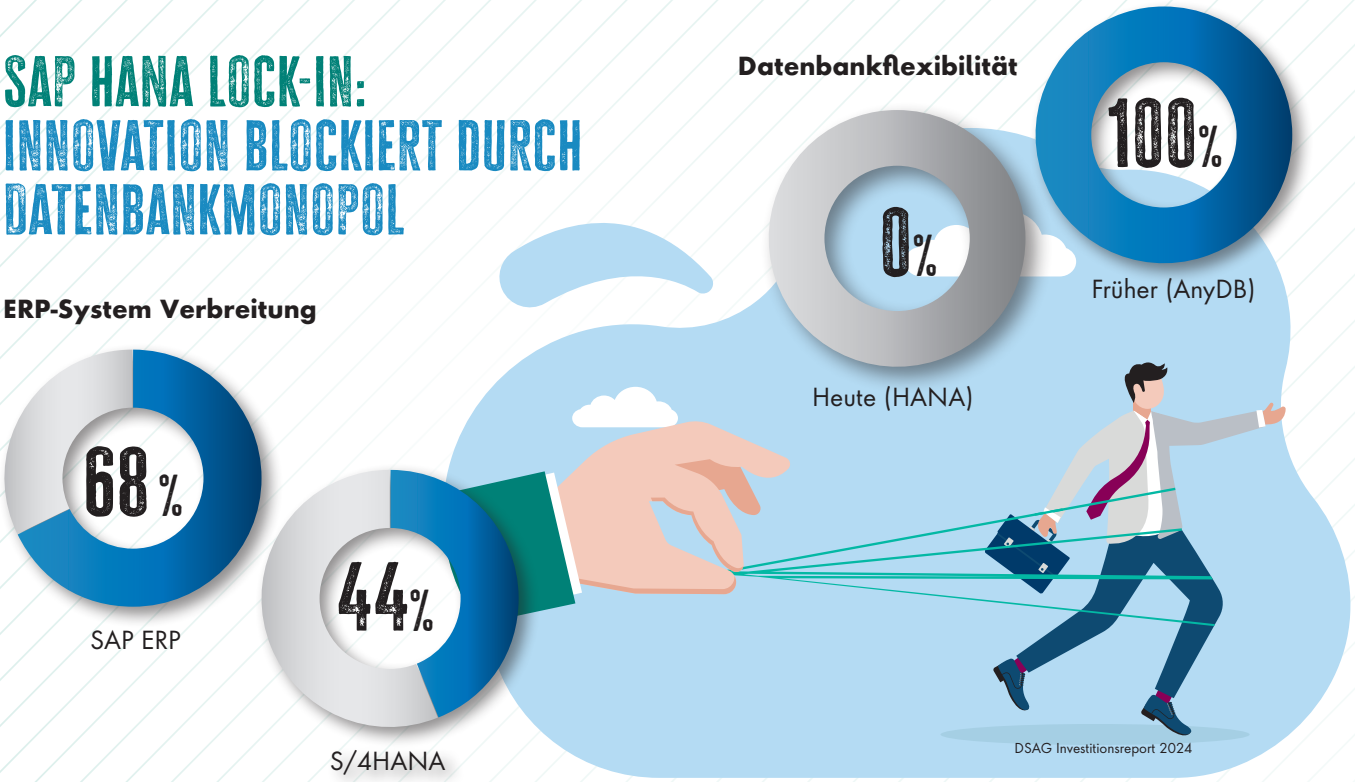
Support-Ende: SAP ERP 6.0 Support läuft aus – Zwang zur Migration

2027

Vollständiger Lock-in: Nur noch HANA-basierte Systeme im Support

DSAG Investitionsreport 2024

SAP HANA LOCK-IN: INNOVATION BLOCKIERT DURCH DATENBANKMONOPOL



Exit-Strategien und Alternativen

Angesichts dieser Entwicklung evaluieren viele Unternehmen Alternativen und zukünftige IT-Szenarien. Das E3-Magazin berichtet von zunehmenden Diskussionen in der SAP-Community rund um die strategische Ausrichtung des ERP-Betriebs.

Eine naheliegende Alternative besteht im Wechsel zu cloud-nativen ERP-Lösungen, die auf modernen, offenen Datenbanktechnologien basieren. Anbieter wie Workday, ServiceNow oder Microsoft Dynamics 365 ermöglichen es Unternehmen, von spezialisierter Datenbanktechnologie zu profitieren, ohne sich an proprietäre Plattformen zu binden. Diese Systeme nutzen oft mehrere Datenbanktechnologien parallel und können so spezifische Stärken gezielt ausschöpfen.

Eine weitere Option ist eine Hybrid-Strategie: Kerngeschäftsprozesse verbleiben zunächst in der SAP-Umgebung, während neue Anwendungen und Analytics-Szenarien auf moderneren Plattformen entwickelt werden. Diese Entkopplung erlaubt es, technologische Innovationen zu nutzen, ohne das gesamte ERP-System zu ersetzen.

Für Unternehmen mit besonders hohen Anforderungen an Flexibilität und Offenheit kann auch ein vollständiger Wechsel zu Open-Source-ERP-Systemen wie Odoo, ERPNext oder Apache OFBiz sinnvoll sein. Diese Lösungen erlauben maximale Datenbankfreiheit und lassen sich individuell auf bestehende Architekturen zuschneiden.

Innovationsdynamik außerhalb des SAP-Kosmos

Die enge HANA-Bindung limitiert den Zugang zu alternativen technologischen Entwicklungen im Datenbankbereich. Während Anbieter wie Google, Oracle oder Microsoft regelmäßig neue Datenbankfunktionen – etwa für Graph-Analysen, Time-Series-Optimierungen oder KI-native Szenarien – veröffentlichen, orientieren sich SAP-Kunden in erster Linie an den Innovationszyklen von HANA. Zwar entwickelt SAP seine Plattform kontinuierlich weiter, jedoch mit einem klaren Fokus auf ERP-spezifische Szenarien und nicht mit der gleichen Breite wie dedizierte Datenbankanbieter.

Dies kann dazu führen, dass SAP-Anwender in bestimmten Innovationsfeldern nicht im selben Tempo profitieren wie Nutzer anderer Plattformen. In datenintensiven Bereichen wie maschinellem Lernen, Echtzeitanalyse oder Data Mesh-Strukturen kann dies zu strategischen Nachteilen führen – abhängig vom jeweiligen Geschäftsfeld und Digitalisierungsgrad.

Fazit: Ein System unter Druck

Die Fokussierung auf SAP HANA bringt für SAP strategische Vorteile – etwa höhere Margen und Kontrolle über die technologische Basis. Gleichzeitig fordert die Community zunehmend Offenheit, Transparenz und Wahlmöglichkeiten. Die Kritik von DSAG und E3-Magazin spiegelt eine wachsende Unsicherheit wider, die viele Unternehmen zum Nachdenken über alternative Szenarien bewegt.

Gerade in Zeiten rasanter technologischer Veränderungen gewinnt Plattformunabhängigkeit an Bedeutung. Unternehmen sollten ihre SAP-Strategie regelmäßig hinterfragen und flexibel gestalten. Denn langfristige Wettbewerbsfähigkeit entsteht dort, wo technologische Offenheit mit wirtschaftlicher Nachhaltigkeit in Einklang steht.

Ulrich Parthier | www.it-daily.net

Vulnerability Management

STRATEGISCHE ENTSCHEIDUNG: WANN SOLLTEN UNTERNEHMEN INVESTIEREN?

Die Verwaltung von Sicherheitsupdates entwickelt sich zu einer kritischen Herausforderung für moderne IT-Abteilungen – denn manuelles Patchen ist teuer und zeitaufwändig. Während automatisierte Patch-Verteilungstools bereits weit verbreitet sind, stehen Unternehmen vor der Frage: Wann rechtfertigt die steigende Komplexität eine Investition in umfassendere Sicherheitslösungen?

Moderne Patch-Prozesse

Die meisten IT-Abteilungen haben längst erkannt, dass manuelle Sicherheitsupdates nicht mehr Stand der Technik sind. Der Wandel zu automatisierten Systemen resultiert direkt aus dem explosiven Wachstum der Zahlen gemeldeter Schwachstellen und der zunehmenden Netzwerkkomplexität. Gleichzeitig sorgen häufigere Vendor-Updates und immer neue Zero-Day-Bedrohungen für zusätzlichen Zeitdruck und damit operativen Stress.

Moderne Automatisierungstools fokussieren sich primär auf die Patch-Distribution, während fortschrittlichere Systeme auch noch kontinuierliche Vulnerability-Überwachung integrieren. Diese Entwicklung entspricht Empfehlungen von Gartner, Forrester und anderen Branchenexperten und spiegelt die praktischen Erfahrungen der Unternehmen wider.

Jeder Tag, der zwischen Bekanntwerden einer Schwachstelle und der Verteilung des dazugehörigen Patches vergeht, gibt Cyberkriminellen zusätzliche Gelegenheit diese auszunutzen. Kein Wunder also, dass der Arbeitsaufwand für IT-Security-Teams mit der zunehmenden Umgebungskomplexität und Gerätediversität beständig weiter steigt. Automatisierte Systeme können den Zeit- und Arbeitsaufwand der IT-Administration im Vergleich zu manuellen Methoden um 30-70 Prozent senken und die mittlere Reaktionszeit (Mean Time To Remediate (MTTR)) bei Sicherheitslücken signifikant verkürzen.

Dramatische Entwicklung der Bedrohungen

Die NIST-Vulnerability-Database dokumentiert eine besorgniserregende Entwicklung (vgl. Tabelle)

ANSTIEG DER GESAMTZAHL DER GEMELDETEN CVES VON JAHR ZU JAHR

2020	18.358	-
2021	20.171	9,9%
2022	23.350	15,7%
2023	28.902	23,8%
2024	40.009	38,4%

Aktuelle Studien zeigen: 65 Prozent der IT-Spezialisten investieren wöchentlich 10-25+ Stunden in Patch-Aktivitäten. Dies entspricht 25-70 Prozent der gesamten Arbeitskapazität eines IT-Teams. Diese Belastung fällt zusätzlich zu regulären Aufgaben an, wie Bereitstellung und Wartung von Endgeräten, den Benutzersupport, die Zusammenarbeit mit Anbietern, die Aktualisierung von IT-Beständen, die Dokumentation der Compliance usw.

Integrierte Vulnerability-Management-Strategien

Automatisierte Patch-Verteilung bildet aber nur einen Baustein einer effektiven Sicherheitsstrategie. Ganzheitliche Vulnerability-Management-Plattformen können den Arbeitsaufwand signifikant reduzieren und gleichzeitig Compliance-Standards sowie den Sicherheitsstatus verbessern.

Effektive Systeme beginnen mit einer automatisch aktualisierten Asset-Inventarisierung. Anhand dieser Datenbasis können integrierte Vulnerability-Scanner Systemfehlkonfigurationen automatisch identifizieren, veraltete Antivirus-Definitionen aufspüren, unverschlüsselte Datenträger hervorheben sowie exponierte Netzwerk-Ports und fehlende System-Updates melden.

Vulnerability-Scanning optimiert die Patch-Priorisierung erheblich. IT-Teams müssen jedoch weiterhin eine Menge Zeit für Update-Tests und -Konfiguration investieren, um Kompatibilität und Systemstabilität zu gewährleisten. Das fehlerhafte CrowdStrike-Update vom Juli 2024 verdeutlicht diese Notwendigkeit. Post-Deployment-Monitoring bleibt essentiell zur Erfolgsvalidierung und Fehlererkennung.

Modernes IT-Management in der Praxis: Managed Software

Wer wirklich effektives Endgeräte Management betreiben will, nutzt deshalb automatisierte Inventarisierung und Software-Verteilung. Durch die Kombination aus Vulnerability Scanner, Update Management und Managed Software ist es möglich, Vulnerability-Scans, Windows-Update-Verwaltung und Third-Party-Patching großflächig zu automatisieren.

Ein Vulnerability Scanner überwacht dabei Netzwerk-Endpoints automatisch auf fehlende Updates, Fehlkonfigurationen und weitere, bekannte Sicherheitslücken.

AKTUELLE STUDIEN ZEIGEN: 65 PROZENT DER IT-SPEZIALISTEN INVESTIEREN WÖCHENTLICH 10-25+ STUNDEN IN PATCH-AKTIVITÄTEN. DIES ENTSPRICHT 25-70 PROZENT DER GESAMTEN ARBEITSKAPAZITÄT EINES IT-TEAMS.

Felix Zech, Head of Customer Engineering, baramundi software GmbH, www.baramundi.com

Im Idealfall gibt es dazu ein zentrales Dashboard, das identifizierte Schwachstellen anhand ihres Schweregrades auflistet und gleich die dazu passenden Remediation-Empfehlungen anzeigt.

Ergänzt wird das durch ein Update Management, das seinen Anwendern granu-

lare Kontrolle über Timing und Distribution von Windows-Updates für Clients und Server bietet. Nur so lässt sich sicherstellen, dass ungetestete oder problematische Updates nicht einfach über das gesamte Unternehmensnetzwerk verteilt werden – eine Vorkehrung, die viele Unternehmen bei dem bereits erwähnten Crowdstrike-Vorfall schmerzhaft vermissen mussten.

Managed Software geht einen Schritt darüber hinaus: Als Service liefert es vollständig validierte, verteil-bereite Patch-Pakete für Third-Party-Anwendungen. Der Dienstleister für seine Kunden überwacht Vulnerability-Datenbanken und Patch-Verfügbarkeit, testet Updates auf Stabilität und Kompatibilität und verpackt sie für sichere Distribution. IT-Administratoren erhalten Benachrichtigungen über verfügbare Pakete und konfigurieren Deployment-Parameter nach den Anforderungen des Kunden.

Wirtschaftlichkeit: Verbesserte Sicherheit und ROI

Managed Software kann beträchtliche Kosteneinsparungen und operative Verbesserungen generieren. Basierend auf Branchenschätzungen ergibt sich folgende ROI-Analyse für ein Netzwerk mit 500-1.000 Endpoints:

IT-Personalkosten:

- Durchschnittsgehalt IT-Administrator: 75.000€/Jahr (6.250€/Monat)
- Typisches Team: 3 Administratoren (18.750€/Monat)
- Arbeitskapazität: 480 Stunden/Monat

Vulnerability-Management-Aufwand:

Bei automatisiertem Scanning und Patch-Deployment, aber überwiegend manuellem Testing:

- Patching-bezogene Aktivitäten: ~240 Stunden/Monat (50% der Teamkapazität)
- Patch-Testing und -Validierung: 100-120 Stunden/Monat (50-60% des Patching-Aufwands)

Einsparpotenzial

Mit geschätzten 30-70 Prozent Zeitreduktion durch Automatisierung kann Managed Software die Testzeit um 30-80 Stunden monatlich reduzieren. Dies entspricht 0,75-2 Vollzeit-Mitarbeitern oder 4.700-12.500€ monatlichen Einsparungen.

Ein weiterer Mehrwert ergibt sich durch konsistentere Patch-Qualität, reduzierte MTTRs und verbesserte Compliance-Metriken. IT-Teams gewinnen zusätzliche Kapazitäten für Prozessoptimierung und strategische Projekte. Ganz nebenbei werden Unternehmen mit professionellen Management-Lösungen auch attraktiver für qualifizierte IT-Fachkräfte, die ihre wertvolle Zeit ungern mit derartiger Routine verbringen.

Strategische Bewertung

Diese Kalkulationen sind insgesamt vergleichsweise konservative Schätzungen – tatsächliche Vorteile variieren je nach individueller Situation. Dennoch macht das ROI-Potenzial Managed Software zu einer relevanten Option für IT-Teams mit dünner Personaldecke.

Die Entscheidung für Managed Software bedeutet optimierte Ressourcennutzung bei gleichzeitiger Verbesserung der Cybersicherheitslage und Compliance – ein entscheidender Faktor angesichts eskalierender Bedrohungen.

Felix Zech

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

it-daily.net

JETZT
ENTDECKEN!

UNSERE THEMEN

it management

Fokusthema: Innovationen 2026

Schwerpunktthemen: 5G, ERP, ITSM, IT & Nachhaltigkeit, eCommerce, Storage/ Data Management

Die Ausgabe 11/12 2025 erscheint am 14. November 2025

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

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, Patric Dahse, Christian Kaul, Ismet Koyun, Carina Mitzschke, Dr. Philipp S. Müller, Silvia Parthier, Ulrich Parthier, Dr. Jan Schaumburg, Catrin Schreiner, Felix Zech, Dina Ziems

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

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

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

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

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

Anzeigenpreise: Es gilt die Anzeigenpreisliste Nr. 32. Preisliste gültig ab 1. Oktober 2024.

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

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

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

Erscheinungsweise: 6 x pro Jahr

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

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

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


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

Aagon

Wir sind dabei!

Nürnberg 07. – 09. Oktober 2025

it sa EXPO CONGRESS

HOME OF IT SECURITY

Ein System. Alle Endpunkte. Maximale Sicherheit. = Hybrides UEM

Fachvorträge – direkt am Puls der Zeit

Diese Vorträge erwarten Sie:

Auf der Bühne

- **Sicher verwalten, smart schützen:**
  Hybrides UEM als Schlüssel zur IT-Security
  Speaker: Sebastian Weber, Chief Evangelist
  07.10.2025 • 13.45 Uhr • Forum D, Halle 7*
- **IT-Sicherheit:**
  Rückgrat für digitale Souveränität und Resilienz in Europa
  Speaker: Fachgruppe des Bundesverbands IT-Mittelstand (BITMi)
  08.10.2025 • 13.00 Uhr • Forum C, Halle 7*

An unserem Aagon Stand

Freuen Sie sich auf spannende Kurzvorträge rund um die Themen **IT-Security und Unified Endpoint Management (UEM).** Unsere Experten teilen praxisnahe Einblicke und aktuelle Trends – kompakt, verständlich und direkt vor Ort.

*Änderungen der Foren und Halle vorbehalten

Hier finden Sie uns:

Unser Aagon-Stand:
Halle 7, Stand 7 – 434

Unser Partner-Stand:
Halle 6, Stand 6 – 125

Jetzt **Gratis-Ticket** sichern

Einfach scannen und den Code **AagonITSA2025** verwenden:

Weitere Informationen finden Sie unter

www.aagon.com/it-sa2025

CRN CHANNEL AWARDS DEUTSCHLAND 2024 GEWINNER SOFTWARE-HERSTELLER DES JAHRES Aagon GmbH

READERS' CHOICE IP INSIDER AWARD 2024

techconsult PUR 2025 Professional User Rating ★ 5-FACH ★ ★ CHAMPION ★

GetApp BEST FUNCTIONALITY & FEATURES 2024

Software Advice BEST CUSTOMER SUPPORT 2024

it security

Detect. Protect. Respond.
September/Oktober 2025

CYBERSICHERHEIT ALS HOCHLEISTUNGSSPORT

Digitaler Wettkampf

Marcus Wailersbacher, NCP engineering GmbH

STORMSHIELD
Digitale Souveränität
ab Seite 14

genua.
KI und IT-Sicherheit
ab Seite 18

KOBIL
Digitale Identität
ab Seite 22

DIE PERPLEXITY FILES

Problem, Fehlverhalten und Lösungen

IT SECURITY ASSESSMENT

Ganzheitliche Cybersicherheitsstrategie

GenAI-SICHERHEIT

Mit KI-Tools durch die Hintertür

www.it-daily.net

Treffen Sie uns live

it-daily.net itsecurity

it verlag

Nur für Messebesucher
👉 Booklet Ransomware

Trends & Themen
💬 Diskutieren Sie mit uns

Nur vor Ort
📍 Messe-Highlights

it security Awards 2025
🏆 Live-Verleihung

Halle 9 / Stand 208 | 07. - 09. Oktober 2025 | Nürnberg

itsa

HOME OF IT SECURITY

Ulrich Parthier

Carina Mitzschke

Lars Becker

REKORDE

LIEBE LESERINNEN UND LESER,

nach hervorragenden Zahlen im vergangenen Jahr mit 25.830 Fachbesuchern (+33 Prozent) geht das Wachstum der it-sa weiter: Die IT Security Messe nutzt für ihre diesjährige Ausgabe erstmalig fünf Hallen und die Ausstellungsfläche wächst um 12 Prozent auf über 950 Aussteller. Nürnberg festigt damit seine Position als „Home of IT Security" und behauptet sich erfolgreich gegenüber Konkurrenten wie der GITEX in Berlin oder der Infosecurity in London. Was für eine Entwicklung!

Und unser it-sa-Spezial? Folgt dem Trend und bricht seinerseits Rekorde beim Seitenumfang. Was normalerweise als kompakter Teil unseres IT Security Magazins erscheint, dominiert nun das gesamte Heft. Anscheinend ist das Einstellen von Rekorden ansteckend.

Aber ehrlich: Bei der Fülle an Innovationen und Weiterentwicklungen blieb uns keine andere Wahl. Von KI-gestützten Security-Tools, die endlich halten, was sie versprechen, über den Status quo bei Zero Trust und neue IAM-/PAM-Ansätze bis hin zu den brennendsten Fragen: Wie unterstützen und entlasten wir unsere Mitarbeiter in der IT-Sicherheit wirklich?

Die it-sa 2025 zeigt, wohin die Reise geht. Die Innovationen und Themen, die auf der Messe im Mittelpunkt stehen werden, verdienen deshalb mehr als nur oberflächliche Betrachtung. Also haben wir ihnen den Großteil unseres Heftes gewidmet.

Manchmal muss man eben mit den Gegebenheiten wachsen. In der IT Security Branche ist das ohnehin Pflicht.

Viel Spaß beim Lesen!
Ihr Redaktionsteam

it-sa Spezial

AUF

it-daily.net

TOP-THEMEN UND STARKE STIMMEN FÜR SECURITY-ENTSCHEIDER!

Kein scam, daily promise.

👉 zum it-sa Spezial

it sa

HOME OF IT SECURITY

WARUM DIGITALE IDENTITÄT MIT SICHERHEIT BEGINNT

LIEBE LESERINNEN UND LESER,

Digitale Kriminalität nimmt signifikant zu. Wir müssen überall mit Cyberangriffen rechnen. Auf die Stromversorgung, staatliche Institutionen, Unternehmen, Banken. Hackerangriffe können ganze Betriebe lahmlegen und bis in die Insolvenz treiben Deshalb muss Sicherheit zur Selbstverständlichkeit werden. Nicht nur für den Schutz des Einzelnen, sondern auch, um die Handlungsfähigkeit der Unternehmen zu wahren.

Dafür braucht es ein sicheres digitales Ökosystem, das alltagstauglich ist. Der beste Weg dorthin ist eine Technologie-Plattform, die unterschiedliche digitale Angebote in einem geschützten Raum zusammenführt – inklusive Nachweis-, Bezahl- und Chat-Optionen. Die Eintrittskarte dafür ist eine verifizierte, digitale Identität für alle.

Diese digitale Identität beginnt mit Sicherheit. Aber Sicherheit ist kein isoliertes Element, sondern muss das gesamte Nutzererlebnis begleiten: Sie beginnt beim Onboarding, ist Bestandteil jeder Interaktion – und endet erst mit einem sicheren Offboarding. Nur so entsteht Vertrauen. Und Vertrauen ist das Fundament jeder digitalen Identität.

Das geballte Know-how auf der it-sa zeigt: Deutschland hat den Innovationsgeist, um solche Ideen umzusetzen. Was wir jetzt brauchen, sind Mut, Willenskraft und den Rückhalt der Politik. Dann können wir sicher in die digitale Zukunft gehen.

Herzlichst,

Ismet Koyun
CEO und Gründer | KOBIL Gruppe

INHALT

COVERSTORY

IT-SA SPEZIAL

Farblich hervorgehobene Artikel sind von der Redaktion als besonders lesenswert empfohlen

Im digitalen Wettkampf

CYBERSICHERHEIT ALS HOCHLEISTUNGSSPORT

Angesichts der globalen Bedrohungslage ist Cybersicherheit in Europa, bildlich gesprochen, gleichermaßen Spitzen- wie Breitensport. Marcus Wailersbacher, Chief Sales & Marketing Officer bei NCP, spricht im Interview über die zunehmenden und sich wandelnden Anforderungen an die Lösungen und das Portfolio von NCP. Außerdem gibt er seine Einschätzungen zur Entwicklung der Märkte und äußert Wünsche an die Politik.

it security: *Herr Wailersbacher, besondere Zeiten erfordern besondere Lösungen. Traditionell ist die it-sa für NCP die Plattform für Neuheiten. Was hat NCP diesmal zu bieten?*

Marcus Wailersbacher: In der Tat haben wir eine Vielzahl an inkrementellen Verbesserungen, aber auch größere Neuheiten im Gepäck. So sind wir stolz darauf, umfassende neue Funktionen unserer vom BSI bis zur Geheimhaltungsstufe „VS-NfD" zugelassenen Lösung vorstellen zu können. Beispielsweise Site-to-Site am VS GovNet Server, das Windows Pre-Logon bei unserem VS GovNet Connector sowie die Verteilung von Server-Zertifikaten über das zentrale Management. Außerdem arbeiten wir mit Hochdruck an der nächsten Produktgeneration, hierzu werden wir auf der it-sa erste „Sneak-Previews" geben. Zusammenfassend lässt sich aber sagen: Wir setzen den eingeschlagenen Weg in Richtung Zero-Trust-Architekturen konsequent fort und das, indem wir Zero Trust ganzheitlicher als je zuvor denken.

Ein besonderer Schwerpunkt in diesem Jahr liegt auch auf der Ausweitung unserer technologischen Partnerschaften. Das Ziel: einfach sicher – durch das orchestrierte Zusammenspiel starker Lösungen, „Made in Germany".

it security: *Sicherheit einfach machen, das ist ein gutes Stichwort. Was verbinden Sie persönlich damit?*

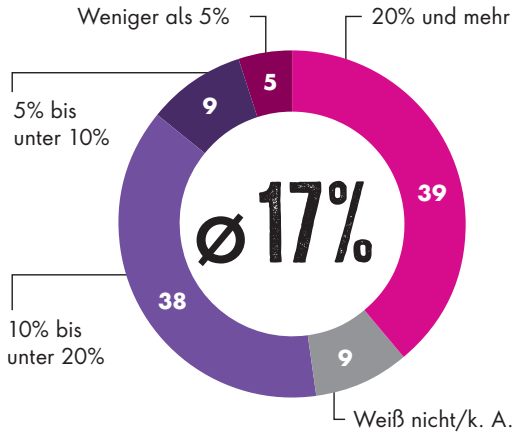
Marcus Wailersbacher: Die Customer Experience ist es, die entscheidet. Ein hohes Maß an Sicherheit sollte nicht mit einer schlechten Anwendererfahrung für den Nutzer bzw. den Administrator verbunden sein. Das haben wir uns bei NCP auf die Fahne geschrieben und das gilt übrigens auch für unsere für VS-NfD zugelassenen Produkte. Und ich wage auch zu behaupten: Mehr Flexibilität als mit uns geht nicht!

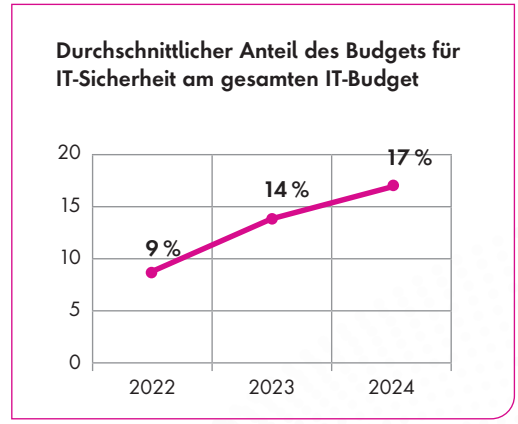
Bei flexiblen IT-Hochleistungslösungen wie den Produkten von NCP liegt es auch an den Administratoren, die Potenziale voll auszuschöpfen. Damit kommen wir zum Enablement und einem wichtigen neuen Baustein in unserem Portfolio, der interaktiven NCP Academy, die wir noch in diesem Jahr als Online-Trainingsplattform starten werden.

> SICHERHEIT UND NUTZERFREUNDLICHKEIT SINNHAFT ZU VEREINEN IST UNSER TÄGLICHER ANSPORN.
>
> **Marcus Wailersbacher, Chief Sales & Marketing Officer, NCP engineering GmbH, www.ncp-e.com**

CYBERSICHERHEIT: INVESTITIONSBEREITSCHAFT STEIGT

Wie hoch ist geschätzt der Anteil des Budgets für IT-Sicherheit am gesamten IT-Budget Ihres Unternehmens?



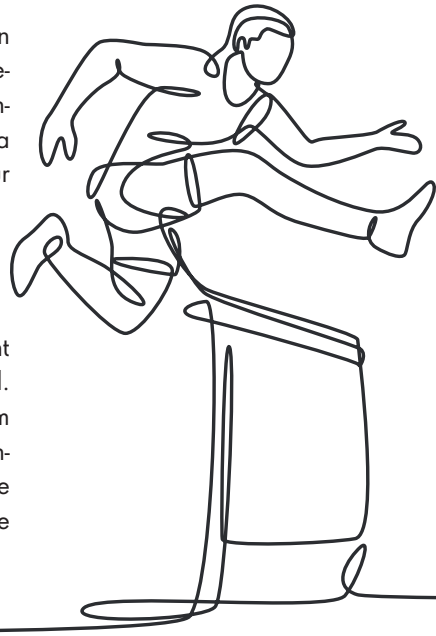


Basis: Alle Unternehmen (n=1.003) | Quelle: Bitkom Research 2024| Angaben in Prozent

it security: *Ein Begriff, der derzeit wie kein anderer die Gespräche prägt, ist „Digitale Souveränität". Sicher auch bei NCP, oder?*

Marcus Wailersbacher: Ja, ganz besonders bei NCP, denn wir sehen uns als deutscher Hersteller konsequent der „IT Security – Made in Germany" verpflichtet. Wir leisten damit unseren Beitrag zu einer wichtigen gesamtgesellschaftlichen Aufgabe – damit Anwender in Deutschland und Europa erstklassige Alternativen haben. Für die Nutzer unserer Lösungen im VS-NfD Umfeld versteht sich das von selbst. Diese Prämisse gilt für NCP aber auch im Umfeld von Großunternehmen, im Public & Government Bereich sowie für den Mittelstand. Denn dort geht es gleichermaßen um den konsequenten Schutz hochsensibler Informationen. Denken Sie beispielsweise an pharmazeutische und medizintechnische Entwicklungen oder an Forschungsprojekte im Maschinenbau.

it security: *Sind das dann nicht die gleichen Anforderungen wie beim Arbeiten mit VS-NfD?*



Marcus Wailersbacher: Genau richtig, die Maßstäbe an den Schutz der Informationen und Infrastrukturen sollte in beiden Fällen nahezu identisch sein. Und für die Anwender von NCP ist der Weg zu VS-NfD in der Regel nicht weit, viele Kunden haben sich sogar für einen parallelen Betrieb entschieden. Auch hier bieten wir volle Flexibilität.

it security: *Wenn wir „Made in Germany" aufgreifen – spüren Sie denn ein geändertes Nachfrageverhalten?*

Marcus Wailersbacher: Der überwiegende Anteil unserer Gesprächspartner trifft Entscheidungen bewusst –

it-sa Expo&Congress

Besuchen Sie uns in **Halle 7A-516**

oder besser – bewusster in Bezug auf das Herkunftsland. Das belegen auch diverse Studien. Es zeigt sich: Wenn es um die Bereitschaft, die Möglichkeit, vielfach auch die Fähigkeit geht, entsprechend zu investieren, dann gibt es natürlich Beschränkungen. An dieser Stelle setzen wir – wie viele andere auch – großes Vertrauen in die Initiativen der Bundesregierung, des Digitalministeriums und des BSI.

it security: *Und gilt das auch international?*

Marcus Wailersbacher: In Europa steigt die Nachfrage speziell nach unseren NATO Restricted/EU Restricted Lösungen spürbar. Aber auch darüber hinaus und mit der gesamten Produktpalette ist „IT Security – Made in Germany" gesucht. Daher investieren wir viel Energie in neue Partnerschaften in unseren definierten Zielmärkten, um gemeinsam unsere starken Lösungen dort anzubieten, wo sie dringend gebraucht werden. Spanien und Australien sind da nur zwei der Märkte. Selbstverständlich spielt die NCP engineering Inc. in den USA ebenfalls weiter eine wichtige Rolle in unseren Wachstumsplänen, da wir hier sehr nahe an unseren wichtigen globalen Partnern Aryaka, HPe/Juniper Networks und WatchGuard Technologies positioniert sind.

it security: *Falls Ihre Kunden bei den IT-Investitionen priorisieren müssen, wozu raten Sie ihnen?*

Marcus Wailersbacher: Seriöse Quellen schätzen die jährlichen Schäden durch Cyberangriffe auf ähnliche oder sogar höhere Summen als die jährlichen Kosten der Corona-Pandemie. Das bedeutet: an der Sicherheit dürfen wir nicht (mehr) sparen – das können wir uns auf Dauer nicht leisten. Und jeder, der ein Cyber-Schadenereignis erlebt hat, wird klar in seiner Priorisierung sein.

it security: *Eingangs haben Sie bereits die Begriffe Zero Trust und die umfassende Antwort von NCP zu diesem Ansatz angesprochen. Verraten Sie uns etwas mehr dazu?*

Marcus Wailersbacher: Wie in der Vergangenheit, hat NCP auch an dieser Stelle konsequent auf die Anwender und deren Feedback gehört. Im Gegensatz zu anderen Lösungen im Zero Trust Umfeld bietet unser Ansatz deshalb einen praktikablen und sinnhaften Weg von On-Premises Architekturen hin zu hybriden Infrastrukturen und der Cloud. Das zielt insbesondere auf flexible Migration- bzw. Evolutionspfade ab. Aber auch für Bestandskunden bieten wir eine optimale Ergänzung und Weiterentwicklung zu den eingesetzten NCP-Produkten. Wichtig sind u.a. erweiterte Funktionen des policy-basierten Zugriffshandlings – auch innerhalb der geschützten Umgebung. Das Stichwort ist hier lateral movement, sowie die feingranulare Zugriffssteuerung im Sinne einer Microsegmentation bis auf Applikations- oder Dienstebene.

it security: *Geht Zero Trust dann nicht zwangsläufig mit Einschränkungen für die Nutzer einher?*

Marcus Wailersbacher: Nun, prinzipiell ist es ja das, worum es bei der ZTNA-Philosophie geht. Den Zutritt oder Zugriff auf einer Least Privilege bzw. Need-to-know Basis einzuschränken. Ihre Frage zielt aber im Kern auf die Erfahrung, dass mehr Sicherheit auch oft weniger Nutzerfreundlichkeit oder eine Beeinträchtigung der Arbeitsabläufe mit sich bringt. Das zu vermeiden ist die Kunst und genau die Stärke von NCP. Sicherheit und Nutzerfreundlichkeit sinnhaft zu vereinen ist unser täglicher Ansporn.

it security: *Last but not least noch zu einem Thema, das zunehmend an Bedeutung gewinnt: Nachhaltigkeit. Wie stellt sich NCP hier den Anforderungen der Kunden und der diversen Stakeholder?*

Marcus Wailersbacher: In der Tat ist das ein wichtiges Themengebiet in unserem täglichen Arbeiten sowie unserer Ausrichtung als Unternehmen insgesamt. Die Berücksichtigung von ökologischen Aspekten, eine nachhaltige Beschaffung, das ist für uns ebenso eine Verpflichtung und eine Priorität wie es die Einhaltung von ethischen Standards oder von Arbeits- und Menschenrechten ist. Die Bronze-Zertifizierung durch EcoVadis zeigt uns, dass wir auf dem richtigen Weg sind.

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

Vom Training zum Sieg

CYBERSICHERHEIT ALS SCHLÜSSELKOMPETENZ IN DER DIGITALEN WELT

Cybersicherheit ist kein Sprint, sondern eher ein Dauerlauf mit wechselndem Terrain. Wer in einem Umfeld bestehen will, das sich fortlaufend verändert, muss wie im Hochleistungssport Ausdauer beweisen, sich an neue Bedingungen anpassen und stetig weiterentwickeln. Punktuelle Maßnahmen greifen zu kurz. Gefragt ist eine Sicherheitsstrategie, die mitwächst und sich flexibel auf neue Risikolagen einstellt – und das schnell und oft.

Wie im Profisport kommt es auf die Abstimmung im gesamten Team an. Technologie, Prozesse und Menschen müssen optimal zusammenspielen. Eine gut aufgestellte Organisation kennt ihre Rollen, trainiert regelmäßig Abläufe und agiert auf Basis gemeinsamer Werte. Awareness-Maßnahmen, Notfallübungen und strukturiertes Incident Response Management sind das Äquivalent zu Spielanalysen, Taktiktraining und Mentalcoaching. Nur wer vorbereitet ist, kann im Ernstfall schnell und wirksam reagieren.

NCP unterstützt dies durch zentral steuerbare und hochsichere VPN-Lösungen, die Echtzeit-Einblicke liefern und prompte Reaktionen auf sicherheitsrelevante Vorfälle ermöglichen – inklusive automatisierter Richtlinienverteilung und Benutzerverwaltung.

Vertrauenswürdige Herkunft als Erfolgsfaktor

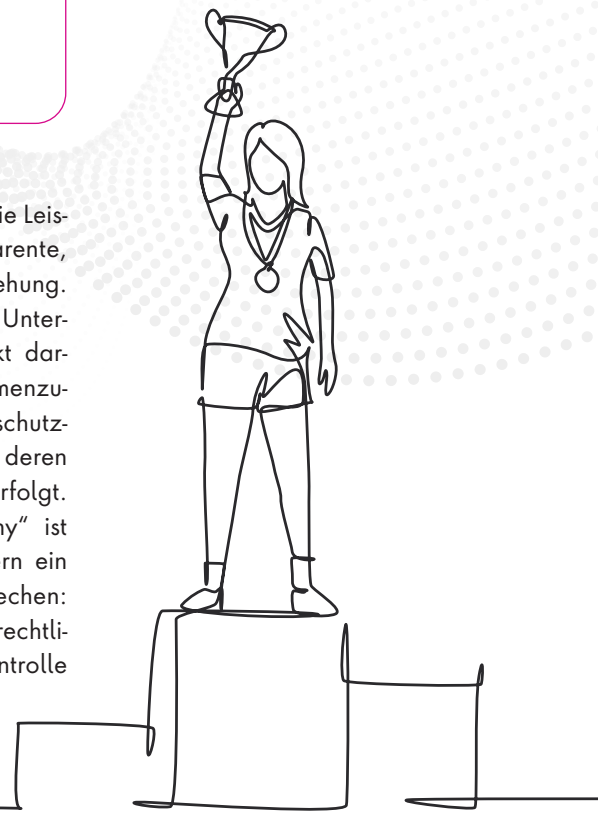
Im globalen Wettbewerb gewinnen die Herkunft und Transparenz von IT-Lösungen zunehmend an Bedeutung.

TECHNOLOGISCHE INNOVATION, REGELMÄSSIGE ANALYSEN, STRATEGISCHE ENTSCHEIDUNGEN UND DISZIPLINIERTE UMSETZUNG SIND KEIN SELBSTZWECK, SONDERN VORAUSSETZUNGEN FÜR NACHHALTIGE SICHERHEIT.

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

Im Spitzensport zählt nicht nur die Leistung, sondern auch ihre transparente, regelkonforme und faire Entstehung. Dementsprechend achten Unternehmen und Behörden verstärkt darauf, mit Partnern zusammenzuarbeiten, deren Produkte Datenschutzanforderungen genügen und deren Entwicklung nachvollziehbar erfolgt. IT Security „Made in Germany" ist kein bloßes Schlagwort, sondern ein Qualitäts- und Sicherheitsversprechen: nachvollziehbare Entwicklung, rechtliche Absicherung und volle Kontrolle über die eigenen Daten.

NCP erfüllt diese Anforderungen konsequent und steht als Anbieter mit Entwicklung, Support und Hosting in Deutschland für Transparenz, technische Qualität und digitale Souveränität. Unsere Kunden erhalten nicht nur leistungsfähige Produkte, sondern behalten die Hoheit über ihre sensiblen Daten ohne versteckte Abhängigkeiten oder fragwürdige Zugriffsrechte. NCP stellt hochsichere VPN-Lösungen zur Verfügung, die unter anderem vom BSI zugelassen sind und für die Geheimhaltungsstufen VS-NfD, NATO RESTRICTED und EU RESTRICTED eingesetzt werden dürfen. Zertifizierungen nach BSI-Vorgaben schaffen zusätzliche Verlässlichkeit. In Zeiten wachsender digitaler Risiken ist dies ein entscheidender Vor-

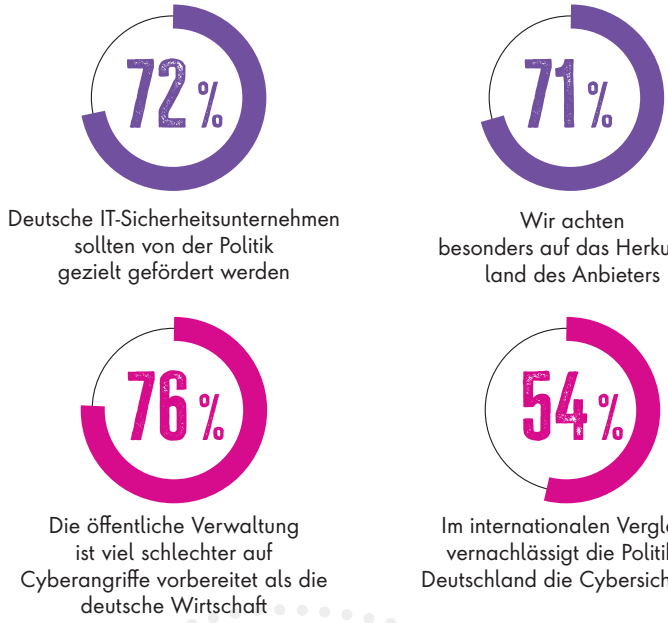


teil für Organisationen, die sich nicht nur technisch absichern, sondern auch regulatorisch auf der sicheren Seite bewegen wollen.

Doch Sicherheit bedeutet nicht nur Schutz auf technischer Ebene, sondern auch klare Strukturen und flexible Verwaltung in komplexen Umgebungen. Wie in einem großen Sportverein, in dem mehrere Teams unter einem Dach ihre eigenen Spielstrategien verfolgen, aber dennoch von gemeinsamen Trainingsanlagen und einer zentralen Organisation profitieren, funktioniert auch die Mandantenfähigkeit bei NCP. Sie ermöglicht es verschiedenen Organisationseinheiten, sicher und unabhängig auf dieselbe Plattform zuzugreifen, obwohl sie klar getrennte Mannschaften mit eigenen Strukturen bleiben. Ziel ist es, eine flexible, effiziente und übersichtliche Verwaltung in komplexen IT-Umgebungen zu schaffen.

IT-SICHERHEIT IST EINE FRAGE DER DIGITALEN SOUVERÄNITÄT.

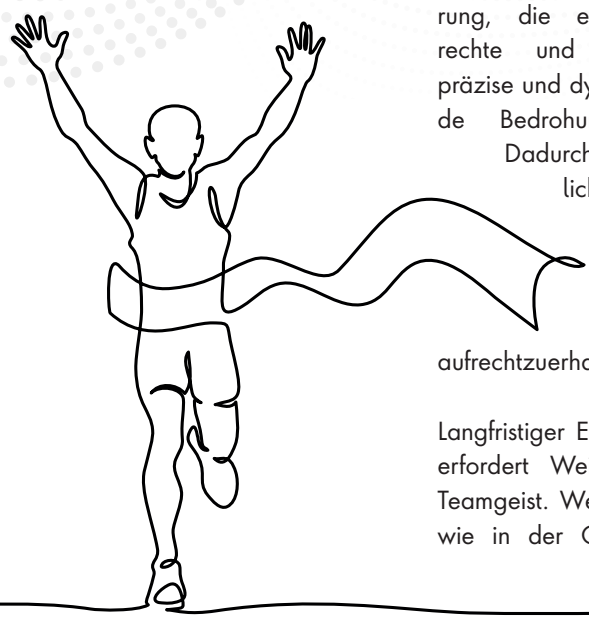
Inwieweit treffen die folgenden Aussagen zu?



Basis: Alle Unternehmen (n=1.003) | Prozentwerte für »Trifft voll und ganz zu« und »Trifft eher zu«
Quelle: Bitkom Research 2024

Cyber-Resilienz braucht Haltung und Ausdauer

Ein zentrales Ziel ist der Aufbau von Cyber-Resilienz – die Fähigkeit, nicht nur Bedrohungen zu erkennen und abzuwehren, sondern auch im Angriffsfall funktionsfähig zu bleiben. Das erfordert flexible Sicherheitsarchitekturen, die wie ein trainierter Athlet schnell zwischen Angriff und Verteidigung umschalten können. Reaktionsgeschwindigkeit, Robustheit und Anpassungsfähigkeit sind entscheidend. NCP unterstützt diese Anforderungen mit seiner granularen Richtliniensteuerung, die es ermöglicht, Zugriffsrechte und Sicherheitsmaßnahmen präzise und dynamisch an sich ändernde Bedrohungslagen anzupassen. Dadurch behalten IT-Verantwortliche die volle Kontrolle und können flexibel auf Vorfälle reagieren, um den Betrieb auch unter Angriffsszenarien aufrechtzuerhalten.



Langfristiger Erfolg in der IT-Sicherheit erfordert Weitblick, Kontinuität und Teamgeist. Werte, die im Spitzensport wie in der Cybersicherheit gleichermaßen gelten. Technologische Innovation, regelmäßige Analysen, strategische Entscheidungen und disziplinierte Umsetzung sind kein Selbstzweck, sondern Voraussetzungen für nachhaltige Sicherheit. Nur wer diese Prinzipien verinnerlicht, bleibt nicht nur im Spiel, sondern gestaltet das Spielgeschehen aktiv mit.

NCP begleitet alle Kunden mit Erfahrung, Verlässlichkeit und einem klaren Fokus auf digitale Souveränität. Wie ein Coach, der das ganze Team im Blick hat, bieten wir nicht nur die Tools, sondern auch das Know-how und die strategische Perspektive, um Sicherheit dauerhaft erfolgreich umzusetzen. Denn in einem digitalen Wettkampf, der keine Pausen kennt, zählt am Ende nicht nur der einzelne Sieg, sondern die Konstanz über die gesamte Saison hinweg.

Christian Albrecht

IT SECURITY DIGITALEVENT

SAVE THE DATE

WE SECURE IT

12. & 13. NOVEMBER 2025
AB 9UHR

#WesecureIT2025

Eine Veranstaltung von itsecurity & it-daily.net

Digitale Unabhängigkeit sichern

DIGITALE SOUVERÄNITÄT DARF KEIN SCHLAGWORT BLEIBEN

Die Diskussion um Europas digitale Abhängigkeit von außereuropäischen Technologieanbietern gewinnt an Brisanz. Während Unternehmen und Institutionen zunehmend auf Alternativen setzen, stellt sich die Frage nach den strategischen Auswirkungen dieser Entwicklung auf die europäische Wirtschaft und Sicherheit. Darüber sprachen wir mit Pierre-Yves Hentzen, Vorsitzender und CEO von Stormshield.

it security: *Herr Hentzen, immer wieder ist von Europas digitaler Abhängigkeit die Rede. Wie ernst ist die Lage tatsächlich?*

Pierre-Yves Hentzen: Sehr ernst! Laut dem französischen Verband Cigref fließen rund 80 Prozent der europäischen Ausgaben für Software und professionelle Cloud-Dienste in die USA – das sind etwa 265 Milliarden Euro. Das bedeutet konkret: Die allermeisten Werkzeuge, die heute für den Betrieb von Unternehmen, für öffentliche Verwaltungen und für staatliche Institutionen unverzichtbar sind, stammen von Anbietern außerhalb Europas.

Damit geben wir einen erheblichen Teil unserer Handlungsfreiheit aus der Hand. Und es geht nicht nur um Bequemlichkeit oder Kosten, sondern um etwas Existenzielles: um strategische Autonomie, wirtschaftliche Stabilität und die Fähigkeit, unsere nationale Sicherheit dauerhaft zu schützen. Diese Abhängigkeit ist ein strukturelles Risiko, das nicht mehr ignoriert werden darf.

it security: *Was genau versteht man unter digitaler Souveränität?*

Pierre-Yves Hentzen: Digitale Souveränität bedeutet im Kern, dass ein Staat oder eine Gemeinschaft die Kontrolle über ihre digitale Infrastruktur behält. Das umfasst die Hoheit über Netzwerke, Rechenzentren sowie Cloud-Dienste und ebenso die Fähigkeit, Datenströme zu überwachen und deren Sicherheit zu garantieren. Es bedeutet auch, dass man eigene digitale Lösungen entwickeln kann und sicherstellt, dass sämtliche Arbeitsweisen mit den geltenden Gesetzen und Standards in Einklang stehen. Wer auf diesen Anspruch verzichtet, begibt sich in Abhängigkeit von externen Anbietern – und macht sich damit verwundbar. Die Folge können Einschränkungen der politischen Handlungsspielräume, eine Verlangsamung lokaler Innovationskraft oder sogar eine gezielte Einflussnahme durch fremde Staaten sein.

it security: *Können Sie Beispiele für die Gefahren einer solchen Abhängigkeit nennen?*

Pierre-Yves Hentzen: Ja, dafür gibt es mehrere konkrete Beispiele. In den letzten Jahren haben wir Preissprünge von bis zu 4.000 Prozent bei bestimmten Komponenten gesehen. Das zeigt, wie verwundbar Lieferketten sind, wenn man keine eigene Produktions- und Wertschöpfungskette hat. Gleichzeitig

stehen unsere kritischen Infrastrukturen – darunter Energieversorger, Rüstungsunternehmen, industrielle Produktionsbetriebe und europäische Behörden – unter Druck durch ausländische Gesetzgebung wie den US-amerikanischen CLOUD Act. Dieser erlaubt es US-Behörden, auf Daten europäischer Unternehmen zuzugreifen, selbst wenn sie physisch auf Servern in Europa liegen. Damit geraten geschäftliche wie politische Informationen unter ausländische Kontrolle. Die Konsequenzen sind weitreichend: Verlust von Geschäftsgeheimnissen, Schwächung der Wettbewerbsfähigkeit und im schlimmsten Fall eine Gefährdung der nationalen Sicherheit.

it security: *Welche Antworten hat die Europäische Union bislang gefunden?*

Pierre-Yves Hentzen: Die EU hat die Notwendigkeit von Gegenmaßnahmen erkannt und eine mehrgleisige Strategie entwickelt. Auf regulatorischer Ebene wurden Instrumente wie die Datenschutz-Grundverordnung, der Cyber Resilience Act oder das europäische Zertifizierungssystem EUCC geschaffen. Sie sollen klare Spielregeln setzen, die einerseits den Schutz von Individuen und Organisationen stärken und andererseits Wirtschaft und Behörden Orientierung geben. Parallel dazu gibt es Programme zur Forschungs- und Innovationsförderung. Über „Horizon Europe 2025" stellt die Kommission mehr als 7,3 Milliarden Euro bereit, allein 1,6 Milliarden davon fließen in die lokale Entwicklung künstlicher Intelligenz. Hinzu kommt die Stärkung der Zusammenarbeit der Mitgliedstaaten – etwa beim Informationsaustausch, bei der Entwicklung gemeinsamer Standards und beim Aufbau einer besseren Reaktionsfähigkeit auf Vorfälle. Das alles sind wichtige Schritte, die zeigen, dass Europa den Handlungsbedarf verstanden hat.

it security: *Das klingt nach einem klaren Plan. Warum geht es dennoch so schleppend voran?*

Pierre-Yves Hentzen: Weil es eine Diskrepanz zwischen Einsicht und Umsetzung gibt. Die Zahlen sprechen eine deutliche Sprache: Laut einem aktuellen Ipsos- und Yousign-Barometer betonen zwar rund 78 Prozent der Entscheidungsträger in Europa, dass lokale Technologien wichtig seien, aber nur 32 Prozent setzen sie tatsächlich bei Investitionen an erste Stelle. Das zeigt, dass sich viele der Sachlage bewusst sind, ihre Entscheidungen im Alltag jedoch anders ausfallen. Gründe sind oft kurzfristige Kostenüberlegungen, eingefahrene Strukturen oder schlicht die Marktmacht der großen außereuropäischen Anbieter. Hier braucht es Mut und Konsequenz. Wir können nicht auf Dauer über „europäische Champions" reden, ohne die Rahmenbedingungen so zu gestalten, dass sie tatsächlich entstehen können. Deshalb wird man ernsthaft diskutieren müssen, ob verbindlichere Maßnahmen nötig sind – beispielsweise die Bevorzugung europäischer Anbieter bei öffentlichen Ausschreibungen oder Quotenregelungen, die eine Mindestnutzung europäischer Technologien sicherstellen.

it security: *Wie könnte ein solcher Wandel konkret aussehen?*

Pierre-Yves Hentzen: Es geht darum, dass wirtschaftliche und institutionelle Akteure ihre Entscheidungen bewusst souverän treffen. Das bedeutet: Sie sollten Produkte und Dienste bevorzugen, die europäischen Anforderungen genügen und eine transparente Einschätzung der damit verbundenen Risiken erlauben. Dabei muss man immer mehrere Dimensionen berücksichtigen: geopolitische Risiken, Fragen der Sicherheit und strategische Interessen. Es gibt hierbei kein Patentrezept. In manchen Situationen steht Sicherheit im Vordergrund, in anderen die Nachvollziehbarkeit der Herkunft oder die Fähigkeit zur Interoperabilität. Wichtig ist, dass wir uns nicht auf starre Kriterien versteifen, sondern abwägen. Nur so lassen sich Fehlentwicklungen verhindern, die das Gesamtsystem schwächen würden.

DIGITALE SOUVERÄNITÄT DARF NICHT ALS NEBENTHEMA BEHANDELT WERDEN, SONDERN MUSS IN ALLEN BEREICHEN MITGEDACHT WERDEN – BEI INNOVATION, BEI REGULIERUNG UND BEI FRAGEN DER GOVERNANCE.

Pierre-Yves Hentzen, Vorsitzender und CEO, Stormshield, www.stormshield.com

it security: *Welche Rolle spielt dabei die Zertifizierung von IT-Produkten?*

Pierre-Yves Hentzen: Eine sehr große. Eine Zertifizierung durch eine nationale oder europäische Cybersicherheitsbehörde – wie etwa das deutsche BSI oder die ANSSI in Frankreich – bietet ein belastbares Fundament an Vertrauen. Denn sie basiert auf einem vielschichtigen Prüfverfahren. Dazu gehören eine detaillierte Überprüfung des Quellcodes, die Identifizierung möglicher Schwachstellen, die Sicherstellung, dass keine Hintertüren eingebaut

sind, und umfangreiche Robustheitstests unter realistischen Bedingungen. Zudem überwacht die ANSSI zum Beispiel die gesamte Produktionskette – von der Entwicklung bis zu späteren Updates. Damit wird garantiert, dass Sicherheit kein einmaliger Zustand ist, sondern über den gesamten Lebenszyklus hinweg erhalten bleibt. Für Unternehmen bedeutet das: Sie können sich auf geprüfte Produkte verlassen und haben damit eine Grundlage, um digitale Risiken durch souveräne Technologien wirksam zu minimieren.

it security: *Reicht das aus, um Europas digitale Abhängigkeit zu überwinden?*

Pierre-Yves Hentzen: Nein, selbstverständlich nicht allein. Wir brauchen einen ganzheitlichen Ansatz. Dazu gehört, dass europäische Technologieunternehmen viel stärker zusammenarbeiten – sei es durch gemeinsame Entwicklungen, Lizenzmodelle oder auch Fusionen. Ebenso entscheidend sind die Förderung von Start-ups und die enge Einbindung der Universitäten, die das notwendige Know-how und die nächste Generation von Fachkräften hervorbringen. Wir müssen digitale Talente nicht nur ausbilden, sondern auch in Europa halten – mit attraktiven Karrierewegen, wettbewerbsfähigen Gehältern und langfristigen Perspektiven. Ein weiterer Punkt ist, dass Europa seine eigenen Werte – etwa im Datenschutz oder bei ethischen Leitlinien für KI – als Wettbewerbsvorteil begreift. Wenn wir zeigen, dass technologische Innovation und Werteorientierung zusammengehen können, schaffen wir ein Modell, das auch international überzeugt.

it security: *Welche Rolle spielt der geopolitische Kontext bei all dem?*

Pierre-Yves Hentzen: Eine ganz zentrale. Wir leben in einer Zeit zunehmender Spannungen und geopolitischer Fragmentierung. In einem solchen Umfeld bedeutet digitale Abhängigkeit, dass man sich politisch erpressbar macht. Wer kritische Technologien nicht selbst beherrscht, läuft Gefahr, im Ernstfall den Zugriff zu verlieren oder Bedingungen diktiert zu bekommen. Deshalb darf digitale Souveränität nicht als Nebenthema behandelt werden, sondern muss in allen Bereichen mitgedacht werden – bei Innovation, bei Regulierung und bei Fragen der Governance. In Frankreich zeigt sich beispielsweise, dass die Synergien zwischen zivilen und militärischen Anwendungen stärker genutzt werden könnten, um eine robuste industrielle Basis zu schaffen. Diese Verbindung könnte ein Modell für Europa insgesamt sein.

it security: *Zum Abschluss: Was wäre Ihre wichtigste Empfehlung an europäische Entscheidungsträger?*

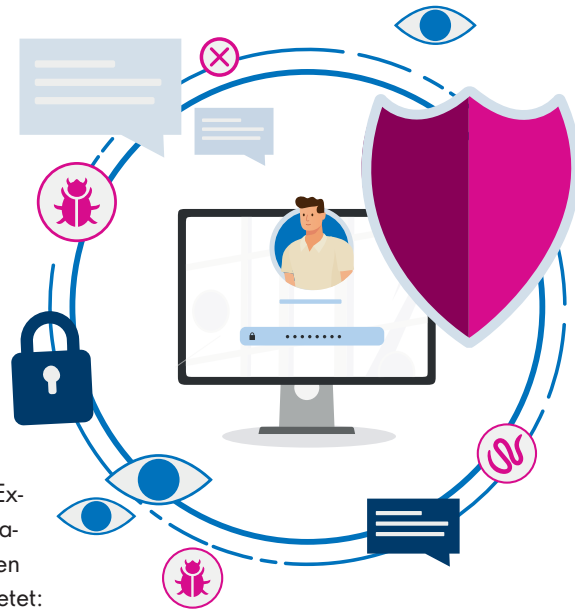
Pierre-Yves Hentzen: Meine Botschaft ist klar: Hören Sie auf, nur über digitale Souveränität zu reden – handeln Sie! Investieren Sie konsequent in eigene Technologien, schaffen Sie ein Umfeld, das Innovation belohnt, und sorgen Sie dafür, dass Talente in Europa bleiben und wirken können. Setzen Sie bei sensiblen Infrastrukturen ausschließlich auf zertifizierte europäische Lösungen. Nur wenn wir all diese Schritte gemeinsam gehen, können wir unsere digitale Unabhängigkeit sichern und verhindern, dass wir im Zeitalter wachsender Bedrohungen und geopolitischer Unsicherheiten zum Spielball fremder Interessen werden.

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

THANK YOU

Die externe Angriffsoberfläche sichern

ZENTRALE SICHTBARKEIT VON IT-ASSETS MIT INTERNETKONNEKTIVITÄT



Sehen, was der Hacker sieht – das ist eine Grundvoraussetzung, um Cyberangriffe abzuwehren. Das Bitdefender GravityZone External Attack Surface Management (EASM) zeigt daher Unternehmen sowie Managed Service Providern (MSP) IT-Assets mit Internetanbindung und die damit einhergehenden Schwachstellen. Das Add-On der Bitdefender GravityZone verbessert die Cyberabwehr durch Erkennen, Überwachen und Verwalten dieser expandierenden Angriffsoberfläche in einer zentralen Plattform. GravityZone EASM scannt und mapped verschiedene Asset-Kategorien wie öffentlich exponierte IP-Adressen, ablaufende oder abgelaufene Zertifikate und verwundbare, weil öffentlich verfügbare IT-Dienste.

MEHR WERT

GravityZone EASM

Die digitale Transformation, Cloud-Anwendungen, Remote-Arbeit und verstärkt eingebundene Infrastrukturen von Dritten wie Partnern und Kunden, tragen dazu bei, dass sich die externe Angriffsoberfläche von IT-Infrastrukturen ständig erweitert. Ohne eine einheitliche und umfassende Übersicht bleiben insbesondere ungenutzte Domänen, fehlkonfigurierte Cloud-Instanzen oder abgelaufene Zertifikate oft unentdeckt. Hacker finden jedoch diese Schwachstellen bei ihren permanenten Internet-basierten Scans nach exponierten Systemen.

Bitdefender GravityZone External Attack Surface Management hilft, diese Lücken zu schließen. Die Lösung bietet:

➜ **Kontinuierliches Erkennen der Assets mit Internet-Konnektivität –** Die Lösung entdeckt, mapped und analysiert dem Internet gegenüber exponierte Systeme. So lassen sich Risiken schnell bewerten, Schwachstellen identifizieren und Maßnahmen ergreifen, bevor die Hacker agieren können. EASM verzeichnet jedes dieser IT-Elemente wie etwa IPv4- und IPv6-Adressen, IP-Blöcke, E-Mail-Adressen, Domänen, Subdomänen, Geräte, Applikationen, Zertifikate, Anbindungen an Drittsysteme oder eine vorhandene Schatten-IT innerhalb von etwa 30 Minuten. Eine solche Abwehr berücksichtigt auch nicht verwaltete oder vergessene Elemente der IT.

➜ **Kontinuierliches Überwachen, Melden und Priorisieren –** GravityZone EASM überwacht Schwachstellen sowie Fehlkonfigurationen über interne wie externe Assets hinweg – auch solche unter der IT-Verwaltung von Partnern, Kunden oder Anbieter in der Supply Chain. Die sofortigen Alarme liefern priorisiert umfassende Informationen zu exponierten Systemen, abgelaufenen Zertifikaten und Hochrisiko-Gefahren. Abwehr und Remediation erfolgen als Teil eines einheitlichen Prozesses.

➜ **Teil einer Plattform –** GravityZone EASM ist nahtlos in die Bitdefender GravityZone integriert. Sicherheitsexperten können mit dieser Plattform Gefahren analysieren und Schwachstellen priorisieren. Zusätzlich profitieren Administratoren von weitreichenden Funktionen für das Sicherheitsmanagement: Damit setzen sie Sicherheitsregeln durch oder konfigurieren Zugangskontrollen - aus einer einzigen Plattform heraus.

Ohne zusätzliche Agenten oder Endpunktinstallationen bietet Bitdefender GravityZone EASM einen funktionsstarken Ansatz, um externe Risiken zu identifizieren und zu verstehen. GravityZone EASM ist ein Add-On der Bitdefender GravityZone, der Bitdefender-Plattform für Sicherheit, Risikoanalyse und Compliance. Diese bietet Endpunktschutz (EPP), Endpoint Detection and Response (EDR), Extended Detection and Response (XDR) und cloudnative Sicherheit.

www.bitdefender.com

it-sa Expo&Congress

Besuchen Sie uns
in **Halle 8-420**

Bitdefender

KI transformiert die IT-Sicherheit

VOM ANALYSE-TOOL ZUR AKTIVEN VERTEIDIGUNGSLINIE

Künstliche Intelligenz verändert die IT-Security und Cybersicherheit grundlegend – sowohl auf Angreifer- als auch auf Verteidigerseite. Wie ist die aktuelle Situation, wie entwickelt sie sich – und wie können sich Unternehmen und öffentliche Institutionen am besten gegen moderne Bedrohungen absichern? Matthias Ochs, Geschäftsführer des deutschen IT-Sicherheits-Spezialisten genua GmbH, ein Unternehmen der Bundesdruckerei-Gruppe, gibt Antworten.

it security: *Herr Ochs, wie profitieren Angreifer von den Möglichkeiten, die KI bietet?*

Matthias Ochs: KI unterscheidet nicht zwischen Gut und Böse. Daher können auch Angreifer KI nutzen, um beispielsweise große Datenmengen schneller und effizienter auszuwerten und potenzielle Angriffsvektoren zu identifizieren. Sie können KI-Methoden verwenden, um ihre Angriffstechniken zu verfeinern und zu verbessern. Ein Beispiel dafür ist die Verwendung von KI-generierten E-Mails für Spear-Phishing-Angriffe. Diese können mittlerweile sehr überzeugend sein und die Opfer beispielsweise dazu bringen, sensible Informationen preiszugeben. Darüber hinaus können Angreifer KI nutzen, um Deepfakes zu erstellen, die sehr realistisch und somit besonders gefährlich sind. Damit lassen sich zum Beispiel Identitäten von Personen missbrauchen, um falsche Informationen zu verbreiten.

Insgesamt stellen wir eine schnell zunehmende Professionalisierung auf Seiten der Cyberkriminellen fest, was nicht zuletzt dem verstärkten Einsatz von KI geschuldet ist.

it security: *Wie sollen Unternehmen und Institutionen auf die dynamische Bedrohungslage reagieren?*

Matthias Ochs: Um auf KI-gestützte Angriffe angemessen reagieren zu können, müssen sich Unternehmen und Institutionen zunächst mit der Technologie auseinandersetzen. Sie müssen die Fähigkeiten und Grenzen von KI grundlegend verstehen. Nur dann ist eine sinnvolle Risikoeinschätzung möglich. Dabei reicht es nicht, einen Fachartikel über KI zu lesen oder an einem Webinar teilzunehmen. Vielmehr muss man die Technologie ausprobieren und praktische Erfahrungen sammeln. Nur so bekommt man ein Gefühl für ihre Möglichkeiten und Grenzen.

Das ist auch ein wesentlicher Grund, warum wir uns bei genua schon sehr lange intensiv mit dem Thema KI beschäftigen. Nur mit fundiertem Wissen lassen sich Lösungen für die IT-Sicherheit entwickeln, die unsere Kunden zuverlässig auch vor KI-generierten Angriffen schützen und so ihren Betrieb sicherstellen. Und die auch den sicheren lokalen Einsatz generativer KI-Anwendungen im eigenen Unternehmen ermöglichen.

it security: *Ist zwingend der Einsatz von KI erforderlich, um die immer ausgefeilteren Angriffe erfolgreich abzuwehren?*

Matthias Ochs: Angreifer können heute die geballte Leistung von Rechenzentren nutzen, um ihre Malware mithilfe von KI zu entwickeln sowie automatisiert zu optimieren und zu variieren. Sie agieren mit „Machine Speed". Es ist diese enorme Geschwindigkeit in der Skalierung und in der Variation, die KI-basierte Angriffsmethoden so gefährlich macht. Ob man ab einem bestimmten Punkt zwingend KI braucht, um sie abzuwehren, ist schwer zu sagen. Klar ist: KI kann ein wichtiger Verstärker sein für die Abwehr. Daher wollen wir die Technologie selbstverständlich auch in der Verteidigungssituation einsetzen. Wichtig ist, dass der Einsatz von KI sorgfältig geplant erfolgt. Schließlich müssen wir sicherstellen, dass die Vorteile der KI-Nutzung nicht dadurch konterkariert werden, dass sie neue Schwachstellen und somit neue Risiken etabliert.

Andererseits sollten wir nicht vergessen, dass sich KI-generierte Angriffe auf technischer Ebene nicht fundamental von herkömmlichen Attacken unterscheiden. Auch hier wird zum Beispiel versucht, über manipulierte Netzwerkpakete Schwachstellen im Netzwerkstack auszunutzen und Maschinen in einen undefinierten Zustand zu bringen.

Daher ist eine durchdachte, auf den Paradigmen Security by Design und Defense in Depth basierende und mit zuverlässigen, vertrauenswürdigen Komponenten umgesetzte Sicherheitsarchitektur eine gute Basis für die Abwehr KI-generierter Angriffe.

it security: *Die abzusichernde IT-Landschaft ändert sich schnell. Welche Herausforderungen für die IT Security stehen derzeit im Fokus?*

Matthias Ochs: Die zunehmende Heterogenität von IT-Infrastrukturen ist ein großes Problem. Viele Unternehmen setzen eine komplexe Mischung aus lokalen und cloudbasierten Systemen und Diensten ein. Das macht es schwierig, eine umfassende IT-Sicherheitsstrategie zu entwickeln. Hinzu kommen steigende Anforderungen durch eine immer strengere Regulierung. Viele, besonders kleine und mittelständische Unternehmen sind mit der Situation überfordert. Sie benötigen die Hilfe externer Dienstleister.

Eine weitere neue Herausforderung ist der lokale Betrieb generativer KI in Unternehmen und Behörden – ein Trend, der stark zunimmt. Datenschutz, Compliance sowie die Vertraulichkeit und Integrität der verwendeten Daten sind dabei essenziell. Der Schlüssel für einen sicheren, souveränen Einsatz generativer KI liegt im Aufbau einer ganzheitlich geschützten Infrastruktur, die auf einer zuverlässigen Zero-Trust-Architektur mit mehrschichtiger Netzwerkabsicherung basiert.

NUR WER GRUNDLEGEND VERSTEHT, WIE DIE TECHNOLOGIE FUNKTIONIERT UND WAS DAMIT MÖGLICH IST, KANN SICH AUF IHRE AUSWIRKUNGEN VORBEREITEN UND SEINE IT-SICHERHEITSSTRATEGIE OPTIMIEREN.

Matthias Ochs, Geschäftsführer, genua GmbH, www.genua.de

it security: *IT-Sicherheit war schon immer erklärungsbedürftig. Jetzt kommt noch KI hinzu. Was können Unternehmen und Behörden tun, um ihre IT in diesem dynamischen Umfeld bestmöglich abzusichern?*

Matthias Ochs: Bewährte IT-Sicherheitsstrategien verlieren nicht plötzlich an Bedeutung. Perimeterschutz, Netzwerksegmentierung, Endpunktsicherheit, Schnittstellenkontrolle usw. bilden vielmehr weiterhin die Grundlage einer leistungsfähigen Verteidigung. Zusätzlich benötigen wir neue Fähigkeiten, etwa um unsere eigenen Regeln in einem Cloud Deployment wie Azure durchzusetzen.

Die Zusammenarbeit mit vertrauenswürdigen Partnern ist ein guter Ansatz, um die dynamischen Herausforderungen, die ein sicherer Betrieb der eigenen IT mit sich bringt, zu meistern.

it security: *Ein Blick in die Zukunft: Welche Entwicklungen auf Basis von KI sind in den nächsten Jahren für die IT Security und Cybersicherheit zu erwarten?*

Matthias Ochs: KI wird sicher eine immer wichtigere Rolle in der IT-Sicherheit und Cybersicherheit spielen. Wir müssen uns klarmachen, dass KI-basierte Anwendungen mit „Machine Speed"

KI UND WIR

genua und die Bundesdruckerei haben sich aktiv mit mehreren Expertenbeiträgen am neuen Fachbuch „KI und Wir" beteiligt.
Darüber hinaus haben wir das Sponsoring für die Open-Access-Lizenz übernommen.

und zunehmender Eigenständigkeit agieren. Je mehr Rechenleistung ihnen zur Verfügung steht, desto schneller erzielen sie beeindruckende – aber eben möglicherweise auch besorgniserregende Ergebnisse.

Übertragen auf die Netzwerksicherheit bedeutet das: Wir müssen Antworten auf diese Herausforderung entwickeln. Denkbar sind hier KI-gestützte Agenten, die beispielsweise die Regeln von Netzwerksicherheitskomponenten in Echtzeit an die jeweilige Bedrohungslage anpassen. Eine wichtige Rolle werden auch quantenresistente Verschlüsselungstechnologien spielen – die in Lösungen von genua bereits heute integriert sind.

it security: *Wird KI die Cybersicherheit langfristig revolutionieren? Sind zum Beispiel KI-gestützte „One sizes fits all"-Systeme für die IT Security denkbar?*

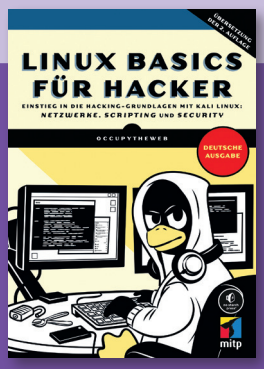
Matthias Ochs: KI verändert grundlegend, wie wir mit Computern interagieren. Die Technologie ist eine Revolution für die gesamte Digitalbranche mit Auswirkungen in alle Lebensbereiche. Sie setzt auch für die IT-Sicherheit neue Impulse, keine Frage. Ein „One sizes fits all"-System für die IT-Sicherheit wird es jedoch nicht geben – dafür ist die IT-Landschaft zu komplex, sind die Anforderungen der Akteure in der digitalen Welt zu unterschiedlich.

Es ist wichtig, dass Unternehmen und öffentliche Einrichtungen sich mit dem Themenkomplex KI auseinandersetzen. Denn nur, wer grundlegend versteht, wie die Technologie funktioniert und was damit möglich ist, kann sich auf ihre Auswirkungen vorbereiten und seine IT-Sicherheitsstrategie optimieren – und so letztlich den eigenen Betrieb sicherstellen und seine Resilienz verbessern.

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

LINUX-BASICS FÜR HACKER

EINSTIEG IN DIE HACKING-GRUNDLAGEN MIT KALI LINUX



Linux-Basics für Hacker
- Einstieg in die Hacking-Grundlagen mit Kali Linux; OccupyTheWeb; mitp Verlags GmbH & Co.KG; 02-2026

Für alle, die sich das erste Mal mit Hacking, Cybersicherheit und Penetration Testing beschäftigen, ist Linux Basics für Hacker der ideale Einstieg. Mit Kali Linux – einer speziell für digitale Forensik und Penetration Testing entwickelten Linux-Distribution – erlernen Sie die Grundlagen von Linux und machen sich mit den Werkzeugen und Techniken vertraut, die nötig sind, um ein Linux-System zu verwalten und zu kontrollieren.

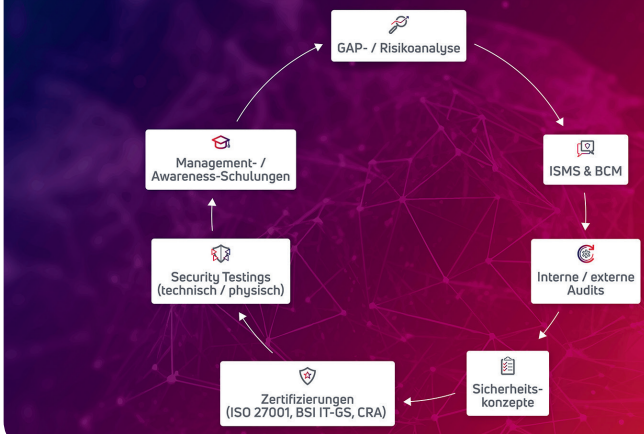
Sie erfahren, wie Kali in einer virtuellen Maschine installiert wird, und lernen die wichtigsten Linux-Konzepte kennen. Anschließend stehen Grundlagen wie Textverarbeitung im Terminal, Dateirechte und Verzeichnisberechtigungen sowie das Arbeiten mit Umgebungsvariablen im Mittelpunkt. Darauf aufbauend lernen Sie grundlegende Hacking-Konzepte wie Security, Anonymität und das Scripting mit Bash und Python kennen.

Zahlreiche Schritt-für-Schritt-Anleitungen und praktische Übungen helfen Ihnen, Ihr Wissen zu testen und zu vertiefen.

Dies ist die Übersetzung der 2. englischen Auflage. Sie wurde umfassend aktualisiert – unter anderem im Hinblick auf neue Sicherheitskonzepte für Root-Rechte, Änderungen bei Bluetooth und Logging-Funktionen sowie mit einem neuen Kapitel über den Einsatz von KI in der Cybersicherheit.

Cybersecurity vs. „Papersecurity“

COMPLIANCE UND DER SCHRITT DARÜBER HINAUS



Die mediale Aufmerksamkeit für eine sich zuspitzende Bedrohungslage durch Cyberangriffe, Phishing-Attacken, Datenspionage und gesteuerte Fehlinformationen wächst. Waren es bislang vornehmlich Fachkreise, die sich mit diesem wachsenden Risiko beschäftigten, so nimmt heute die allgemeine Sensibilisierung hinsichtlich der Anfälligkeit unserer Infrastrukturen, Systeme und Anwendungen zu. Nicht zuletzt geschieht dies aufgrund immer neuer Statistiken zu Schadensvolumina durch erfolgreiche Angriffe. Die Risiken für die Leistungsfähigkeit von global vernetzten IT-Systemen, physischen Infrastrukturen, Mitarbeitenden und Lieferketten nehmen zu. Faktoren sind unter anderem Naturkatastrophen und geopolitische Abhängigkeitsverhältnisse.

Proaktiver Schutz ist essenziell

Die Lehren, welche Legislative und Exekutive in Deutschland und Europa aus diesen Entwicklungen ziehen, präsentieren sich uns seit geraumer Zeit in Form neuer oder aktualisierter Regulatorik wie NIS2, CRA, DORA und weiterer Richtlinien.

Die Umsetzung beschäftigt heute eine Vielzahl von Verantwortlichen in Organisationen und Unternehmen, ebenso wie externe Dienstleister und jeden einzelnen von uns. Denn ohne proaktive und reaktive Maßnahmen droht die Gefahr erheblicher finanzieller Verluste, Reputationsschäden und langanhaltender Betriebsunterbrechungen.

Entscheidend für die Optimierung der Resilienz von Organisationen und deren Geschäftsprozessen ist eine ganzheitliche Betrachtungsweise, die alle potenziellen Risiken umfasst.

Der Weg zu mehr Sicherheit

Entsprechend empfiehlt es sich, Organisationen mit einem holistischen Ansatz zu betrachten. Entscheidende Prozessschritte hin zu einer sicheren Organisation beziehungsweise Unternehmung sind etwa die Folgenden:

- Initiale GAP- beziehungsweise Risikoanalysen
- Implementierung eines umfassenden Informationssicherheits- und Business Continuity Managements
- Regelmäßige interne und externe Audits
- Durchführung passender Zertifizierungen
- Entwicklung von relevanten Sicherheitskonzepten
- Routinemäßige, technische und physische Security Tests
- Regelmäßige Management- und Awareness-Schulungen

Die Integration dieser Punkte in die Unternehmensstrategie kann nicht nur die Krisenreaktionsfähigkeit im Notfall erhöhen, sondern nachhaltig die proaktive Widerstandsfähigkeit gegenüber einer komplexen Risikolandschaft optimieren. Dabei gilt, dass meist keine vollständige Neuausrichtung bestehender Strukturen notwendig wird, sondern lediglich eine gezielt gesteuerte Integration neuer Aspekte in vorhandene Sicherheitsprozesse.

Professionelle Unterstützung auf allen Ebenen

Organisationen und Unternehmen stehen dieser Herausforderung nicht allein gegenüber. So entwickelt beispielsweise infodas, ein Airbus Tochterunternehmen spezialisiert auf Cyber und IT, seit über fünf Jahrzehnten klassifizierte Cybersicherheitsprodukte gegen den ungewollten Datenabfluss. Zum höchst zugelassenen Produktportfolio kommt auch ein ganzheitlicher Cybersecurity-Beratungsansatz. Als BSI-zertifizierter IT-Sicherheitsdienstleister ist infodas zur Unparteilichkeit verpflichtet und bringt die Erfahrung in der Konzeption und Integration von Informationssicherheit unterschiedlicher Arten und Organisationen mit: Von der GAP-Analyse, über die Implementierung eines ISMS und Audit-Unterstützung bis hin zu Business-Continuity und offenen oder geheimen Security-Tests. infodas bestimmt kundennah und individuell schützenswerte Ressourcen und unterstützt bei der Implementierung einer umfangreichen Cybersecurity-Strategie über alle Organisationsebenen hinweg.

www.infodas.com

Digitale Identität als Schlüssel zur Cyber-Resilienz

WIE DIGITALE SICHERHEIT DIE HANDLUNGSFÄHIGKEIT VON UNTERNEHMEN STÄRKT

Cyberangriffe nehmen exponentiell zu – sie können staatliche Institutionen und ganze Betriebe lahmlegen. Ismet Koyun ist CEO von KOBIL und erläutert im Gespräch mit Ulrich Parthier, Publisher it security, wie Organisationen durch digitale Sicherheitstechnologien handlungsfähig bleiben.

Ulrich Parthier: *Sind aktuelle digitale Infrastrukturen zu verwundbar?*

Ismet Koyun: Im Grunde genommen, ja. Die Verwundbarkeit steigt mit der Komplexität. Digitale Systeme sind stark vernetzt, aber oft fragmentiert gesichert. Unternehmen nutzen verschiedenste Softwarelösungen, bauen Schutzmechanismen punktuell auf. Aber Hackerangriffe zielen nicht auf einzelne Server, sondern auf ganze Lieferketten, Identitäten, Authentifizierungsprozesse.

Es reicht nicht aus, einzelne Systeme oder Anwendungen zu schützen. Denn so entstehen Lücken, die Angreifer nutzen. Es braucht eine durchgängige Sicherheitsarchitektur, die alle Prozesse umfasst: von der ersten Anmeldung bis zur letzten Transaktion.

Ulrich Parthier: *Wie funktioniert das und wie lässt es sich in der Praxis umsetzen?*

Ismet Koyun: Eine ganzheitliche Sicherheitsstruktur ist ein dynamischer Prozess. Dazu gehören organisatorische Maßnahmen, Notfallpläne und Schulungen, um das Bewusstsein bei allen Mitarbeitenden zu schärfen. Aber eben auch technische Innovationen.

Sicherheit muss bereits bei der Architektur digitaler Systeme als zentrales Element integriert sein – Security by Design. Mehrstufige Schutzmechanismen sorgen für Resilienz durch verschiedene Verteidigungslinien. Sicherheit muss prozessübergreifend gewährleistet sein: durch End-to-End-Verschlüsselung, Integrationsfähigkeit und Monitoring. Jede Transaktion muss geschützt und in Echtzeit auf mögliche Betrugsversuche geprüft werden.

Gerätebindung ist eine wichtige Maßnahme, gerade bei sensiblen Vorgängen wie Online-Banking oder Bezahlfunktionen. Insgesamt ist ein speziell auf den eigenen Bedarf zugeschnittenes Zusammenspiel von Zugang, Authentifizierung und Betrugserkennung notwendig.

Ulrich Parthier: *Welche Rolle spielt digitale Identität dabei?*

Ismet Koyun: Mit einer geschützten digitalen Identität wird ganzheitliche Sicherheit erst möglich. Nur wenn zweifelsfrei feststeht, wer ich bin und wer mein Gegenüber ist, kann ich sicher kommunizieren, Verträge abschließen oder Zahlungen ausführen. Dies sollten Unternehmen immer im Kopf behalten, wenn sie ihren Kunden digitale Services anbieten.

Ohne verifizierte Identität entstehen Risiken: Fake-Accounts, Betrug, Manipulation. Je mehr Prozesse automatisiert ablaufen, etwa in Zusammenhang mit Agentic AI, desto wichtiger wird die Sicherheit bei der Identitätsprüfung. Wir brauchen digitale Identitäten, die fälschungssicher und bestenfalls universell einsetzbar sind. Identität ist nicht nur ein Zugang, sie ist die Eintrittskarte in das digitale Leben. Sie schafft Verbindlichkeit für alle Beteiligten und ist die Voraussetzung für funktionierende digitale Ökosysteme.

Ulrich Parthier: *Lassen sich Identitäten überhaupt wirksam absichern, wo künstliche Intelligenz inzwischen täuschend echt kommuniziert und handelt?*

Ismet Koyun: Das ist eine der größten Herausforderungen für IT-Verantwortliche – und sie wird mit jeder neuen KI-Generation akuter. Die Grenzen zwischen realen und synthetischen Identitäten verschwimmen. Authentifizierungsverfahren nur durch Passwörter oder einmalige Logins reichen nicht aus.

Nötig ist ein dynamisches, risikobasiertes Identitätsmanagement, das jede Interaktion in Echtzeit überprüft. Dazu gehören adaptive Multi-Faktor-Authentifizierung, kontinuierliches Session-Monitoring und Verhaltensbiometrie. Verhält sich ein Nutzer beim Eintippen des Passworts ungewöhnlich, kann das System automatisch die Sicherheitsstufe hochsetzen – etwa durch eine zusätzliche Biometrie-Prüfung oder vorübergehende Zugriffsbeschränkung.

Zero Trust ist das entscheidende Prinzip: Keine Anfrage und kein Nutzer werden pauschal als vertrauenswürdig eingestuft. Stattdessen wird jede Aktion überprüft – kontinuierlich und abhängig vom Kontext, vom Gerät, vom Nutzerverhalten. So lassen sich KI-gestützte Identitätsfälschungen und automatisierte Angriffe zuverlässig erkennen und stoppen.

Ulrich Parthier: *Wie kann in digitalen Räumen Sicherheit gewährleistet bleiben, wenn immer mehr Dienste vernetzt werden?*

Ismet Koyun: Indem man Services nicht einzeln schützt, sondern ganzheitlich denkt. Die Zukunft gehört Plattformen, die unterschiedliche Dienste unter einem sicheren Dach bündeln. Sie müssen so gebaut sein, dass sie nur verifizierte Akteure zulassen – ob Nutzer oder KI-Agent. Innerhalb dieses

DIE ZUKUNFT GEHÖRT PLATTFORMEN, DIE UNTERSCHIEDLICHE DIENSTE UNTER EINEM SICHEREN DACH BÜNDELN.

Ismet Koyun, CEO, KOBIL, www.kobil.com

geschützten Raums können dann Prozesse nahtlos ablaufen: Identifizieren, Bezahlen, Kommunizieren. Das reduziert Risiken, weil es klare Regeln, standardisierte Abläufe und eine zentrale Infrastruktur gibt. Sicherheit ist nicht auf die Anwendung beschränkt – sie ist die Grundlage, auf der das gesamte Ökosystem funktioniert. Verwirklichen lässt sich ein solcher universeller Ansatz über digitale SuperApp-Plattformen mit breitgefächerten Funktionen und integriertem Identitätsmanagement.

Bei KOBIL verfolgen wir genau diese Philosophie mit unserer modularen mPower Lösung. Sie umfasst den Schutz für Anwendungen, aber eben auch: eine rechtssichere und vertrauenswürdige digitale Identität, sichere und DSGVO-konforme Kommunikation, digitale Signaturen und Dokumentenfreigabe sowie Identity-gebundene Zahlungen. Das Ganze abgesichert durch bewährte mehrfache Schutzschichten und neueste KI-Technologie. Nicht umsonst schützt KOBIL digitale Infrastrukturen bei mehr als 5.000 Unternehmen und Organisationen weltweit, darunter SAP, IBM, ABB, Migros Bank, Commerzbank, die Deutsche Bundesversammlung und viele mehr.

Ulrich Parthier: *Die wenigsten Unternehmen verfügen über Ressourcen und Know-how, um eigene Super-Apps zu entwickeln. Lösungen von globalen Konzernen bergen ein großes Datenschutz-Risiko. Fehlt es in Europa an einer technologischen Basis für hochsichere Plattformen?*

Ismet Koyun: Keineswegs. Es gibt diese Lösungen, auch in Europa. Digitale Plattformen, die unterschiedlichste Arten von Services vereinen und dadurch für verschiedene Branchen interessant sind: zum Beispiel für Banken, Versicherungen, Mobilitätsanbieter, Behörden und Städte. In Istanbul ist seit Jahren unsere Secure SuperApp mit mehr als fünf Millionen Nutzern im Einsatz. Auf Basis derselben Technologie von KOBIL wird in Worms gerade eine City-App eingeführt, die als Vorreiter für weitere deutsche Städte dienen kann.

Unternehmen können unsere Technologie für ihre eigene SuperApp nutzen. Der Vorteil: Sie greifen auf eine skalierbare Plattform zu, ohne selbst entwickeln zu müssen. Und sie bekommen damit sämtliche integrierte Sicherheitsfunktionen. Auch für Startups ist das interessant, die so von Grund auf ein sicheres Business aufbauen können, das in allen Aspekten gegen Cyberangriffe geschützt ist.

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

Identitätsmanagement

DIGITALE SOUVERÄNITÄT NEU DENKEN

Wer digitale Eigenständigkeit sichern möchte, benötigt mehr als technische Zugriffskontrollen. Digitale Souveränität bedeutet eine klare Steuerbarkeit von Systemen, Datenflüssen und Identitäten. Identity and Access Management bildet dabei das strategische Fundament sicherer IT-Architekturen.

Cloud-Dienste, hybride Infrastrukturen und externe Anbieter versprechen Flexibilität, führen aber oft zu einem schleichenden Kontrollverlust. Viele Unternehmen wissen nicht mehr genau, wer wann auf welche Ressourcen zugreift und unter welchen Bedingungen.

Geopolitische Spannungen, neue Angriffsmuster, unkontrollierte KI-Nutzung und Richtlinien wie NIS2 oder DORA verschärfen die Anforderungen an Sicherheit und Transparenz. Die Fähigkeit, digitale Systeme eigenständig zu steuern, wird zum strategischen Erfolgsfaktor. Wo diese Steuerbarkeit fehlt, drohen Sicherheits- und Haftungsrisiken. Einzelne Sicherheitsmaßnahmen reichen nicht mehr aus. Unternehmen brauchen ein tragfähiges Fundament, das jederzeit Kontrolle über kritische Prozesse ermöglicht. Zentrale Voraussetzung ist ein souveränes IAM.

Architektur entscheidet über digitale Handlungsfähigkeit

Digitale Souveränität verlangt eine Architektur, die Zugriffe sicher und flexibel steuert – auch in komplexen, regulierten Umgebungen. Ein interoperables, modular aufgebautes IAM bildet das Fundament: Es integriert Authentifizierung (Identitätsprüfung), Autorisierung (Zugriffsvergabe) sowie die automatisierte Zuweisung von Rechten und Rollen. Zudem unterstützt es Zero Trust, bei dem kein Zugriff als selbstverständlich gilt, sondern kontextbasiert validiert wird.

Digitale Souveränität verlangt strategisches Identitätsmanagement

Digitale Souveränität entsteht nicht allein durch Architektur, sondern durch gezielte Steuerung. IAM wird oft auf technische Aufgaben reduziert, tatsächlich erfüllt es eine übergeordnete Kontrollfunktion: Es regelt, wer worauf zugreifen darf, unter welchen Bedingungen und mit welcher Nachvollziehbarkeit. Wer digitale Souveränität ernst nimmt, muss diesen Prozess aktiv gestalten. Drei Prinzipien bestimmen, wie wirksam ein IAM digitale Identitäten schützt:

➤ Zugriff kontextbezogen steuern

Zugriffsentscheidungen müssen sich an Faktoren wie Standort, Gerätezustand, Uhrzeit oder Risikobewertung orientieren. Adaptive Freigaben erhöhen Sicherheit und Benutzerfreundlichkeit.

➤ Authentifizierung risikobasiert absichern

Robustes Identitätsmanagement erfordert mehrstufige Verfahren, passwortlose Logins, adaptive Prüfungen und lückenlose Protokolle – ohne die Produktivität zu beeinträchtigen.

➤ Datenschutz architektonisch verankern

Ein souveränes IAM bezieht Datenschutz von Anfang an mit ein: durch transparente Löschkonzepte, revisionssichere Protokollierung und einen verantwortungsvollen Umgang mit sensiblen Daten.

Wer zu spät handelt, verliert digitale Handlungsfähigkeit

Digitale Souveränität entscheidet, ob Unternehmen ihre Systeme, Daten und Schnittstellen in einer vernetzten Welt noch eigenständig steuern können. Wer ausschließlich auf technische Sicherheit setzt, greift zu kurz. Erst wenn klar geregelt ist, wer worauf zugreifen darf und wie dies kontrolliert wird, entsteht eine belastbare Grundlage für Sicherheit, Compliance und Resilienz.

IAM übernimmt dabei eine zentrale Rolle: nicht als Werkzeug der IT, sondern als Instrument strategischer Führung. Wer seine Identitäten nicht vorausschauend steuert, verliert die Kontrolle über digitale Schlüsselprozesse.

Stephan Schweizer

WER SEINE IDENTITÄTEN NICHT VORAUSSCHAUEND STEUERT, VERLIERT DIE KONTROLLE ÜBER DIGITALE SCHLÜSSELPROZESSE.

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

Privileged Access Management

WELCHE PROBLEME KANN PAM FÜR IHR UNTERNEHMEN LÖSEN?

Privileged Access Management (PAM) unterstützt Unternehmen bei der Bewältigung kritischer Cybersicherheitsherausforderungen wie unkontrolliertem Zugriff, Insider-Bedrohungen, Secret Sprawl und unsicheren Remote-Verbindungen.

EMA Research fand heraus, dass 54 Prozent der Unternehmen Nicht-Mitarbeitern privilegierten Zugriff auf das Unternehmensnetzwerk gewähren – was ein enorm großes Risiko darstellt, da diese Konten die Hauptziele von Cyberkriminellen sind.

Hier sind einige Beispiele dafür, welche organisatorischen Herausforderungen PAM lösen kann.

#1 Unkontrollierter Zugriff auf privilegierte Konten

Privilegierte Konten bieten weitreichenden Zugriff auf kritische Systeme – ihr Missbrauch kann gravierende Folgen haben. PAM begrenzt Risiken durch sichere Speicherung von Anmeldeinformationen, rollenbasierten Zugriff (Role-Based Access Control, RBAC), Just-in-Time-Zugriff (JIT) und lückenlose Sitzungsüberwachung.

#2 Insider-Bedrohungen

Privilegierte Insider können den Zugriff missbrauchen, um Daten zu stehlen oder den Betrieb zu stören – oft ohne entdeckt zu werden. PAM begrenzt dies durch vollständige Sitzungsaufzeichnung, Prüfpfade und Echtzeitwarnungen. Der JIT-Zugriff minimiert das Risikofenster.

#3 Offenlegung von Anmeldedaten und Geheimnissen

Unsichere Speicherung sensibler Zugangsdaten wie Passwörter, SSH-Schlüssel und API-Token begünstigt Datendiebstahl. PAM schützt Geheimnisse in verschlüsselten Tresoren und automatisiert die Passwortrotation.

#4 Verbreitung von Geheimnissen (Secrets Sprawl) in DevOps

Hartcodierte Geheimnisse gefährden Sicherheit und Wartung. PAM zentralisiert und verschlüsselt Geheimnisse, injiziert sie zur Laufzeit und entlastet Entwickler.

#5 Unsicherer Fernzugriff

Remote-Zugriffe über unsichere Geräte und Netzwerke vergrößern die Angriffsfläche. PAM schützt mit verschlüsselten Tunneln (ohne VPN) und Remote Browser Isolation – für sichere Verbindungen und volle Überwachung.

#6 Dauerhafte Privilegien

Dauerhafter Zugriff führt zu Privilege Creep. Wenn sie kompromittiert werden, ermöglichen diese Konten laterale Bewegungen. PAM eliminiert den ständigen Zugriff durch JIT-Bereitstellung und Durchsetzung der geringsten Rechte, wodurch potenzielle Schäden reduziert werden.

#7 Manuelle Zugriffsverwaltung

Manuelle Bereitstellung und Zurücksetzung von Passwörtern sind ineffizient und fehleranfällig. PAM automatisiert den Zugriff über SCIM-Integration, unterstützt Single Sign-On (SSO) und senkt die Belastung des Helpdesks.

#8 Mangelnde Sichtbarkeit

Ohne Transparenz kann Missbrauch unbemerkt bleiben und die Einhaltung der Vorschriften versagen. PAM bietet Einblicke mit Sitzungsaufzeichnung, Anomalieerkennung und SIEM-Integration.

#9 Compliance-Anforderungen

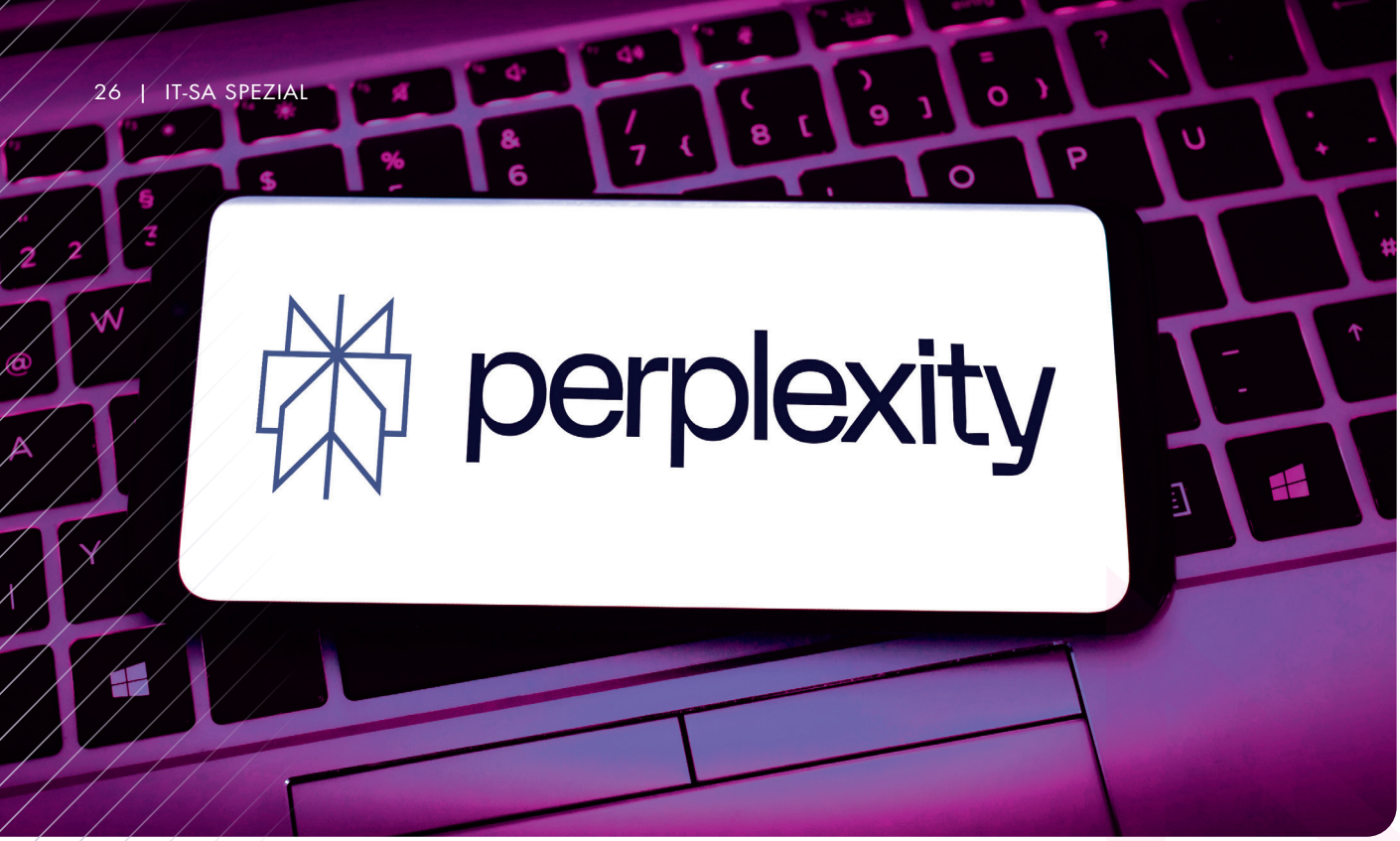
Vorschriften wie DSGVO, HIPAA und SOX erfordern strenge Zugriffskontrollen und Protokollierung. PAM gewährleistet die Einhaltung von Multi-Faktor-Authentifizierung (MFA), detaillierten Protokollen und Segregation of Duties (SoD).

Lösen Sie die heutigen Zugriffsrisiken mit KeeperPAM

KeeperPAM bietet umfassende Funktionen, darunter die Durchsetzung der geringsten Rechte, Echtzeitüberwachung, detaillierte Protokollierung, automatisierte SCIM-Bereitstellung und die Möglichkeit zur Integration mit SIEM-Tools. Durch die Implementierung von KeeperPAM können Unternehmen Zugriffsrisiken wirksam begegnen und ihre allgemeine Sicherheitslage stärken, indem sie sicherstellen, dass der privilegierte Zugriff streng kontrolliert wird.

www.keepersecurity.com

it-sa Expo&Congress
Besuchen Sie uns in **Halle 7-607**
KEEPER



Die Perplexity Files

CLOUDFLARE VS. PERPLEXITY AI: PROBLEM, FEHLVERHALTEN UND LÖSUNGEN

Cloudflare hat Perplexitys heimliche Crawler-Nutzung enttarnt. Das wirft einige grundsätzliche Fragen auf.

Wenn robots.txt zur Farce wird

Website-Betreiber stehen vor einem fundamentalen Dilemma: Die jahrzehntelang bewährten Standards für die Kommunikation mit automatisierten Crawlern werden von einer neuen Generation von KI-Unternehmen systematisch ignoriert. Was bisher als Gentlemen's Agreement zwischen Website-Betreibern und Suchmaschinen funktionierte, wird von gewinnorientierten AI-Startups als hinderliches Relikt behandelt.

Der Perplexity-Fall illustriert dabei nur die Spitze des Eisbergs. Während traditionelle Suchmaschinen wie Google zumindest oberflächlich robots.txt-Direktiven respektierten, etabliert sich eine neue Kategorie von Datensammlern, die ihre millionenschweren Geschäftsmodelle auf der unrechtmäßigen Aneignung fremder Inhalte aufbauen. Dies bedroht nicht nur Urheberrechte, sondern untergräbt auch die wirtschaftlichen Grundlagen vieler Content-Anbieter.

Perplexitys systematisches Fehlverhalten

Der Fall Perplexity AI ist geeignet für ein Kapitel eines Lehrbuchs für Datenmissbrauch und illustriert das Ausmaß dieser problematischen Praktiken auf besonders drastische Weise. Das in San Francisco ansässige Unternehmen entwickelte ein ausgeklügeltes System zur Umgehung von Schutzmaßnahmen, das weit über simple robots.txt-Ignorierung hinausging. Perplexity setzte sowohl offizielle als auch heimliche Crawler ein.

Diese heimlichen Crawler gaben sich als normale Google Chrome Browser auf macOS-Systemen aus und nutzten dabei rotating IP-Adressen außerhalb der bekannten Perplexity-Ranges. Durch den systematischen Wechsel zwischen verschiedenen Autonomous System Numbers (ASNs) erschwerte das Unternehmen die Rückverfolgung seiner Aktivitäten erheblich. Insofern war die Verschleierungstaktiken des Unternehmens bemerkenswert sophistiziert.

Der Cloudflare-Beweis

Cloudflare konnte dieses Fehlverhalten durch ein kontrolliertes Experiment eindeutig nachweisen. Das Unternehmen erwarb mehrere neue Domains mit restriktiven robots.txt-Dateien, die jeglichen automatisierten Zugriff explizit untersagten. Trotz dieser klaren Vorgaben war Perplexity in der Lage, detaillierte Informationen über die Inhalte dieser gesperrten Seiten zu liefern, als Cloudflare-Ingenieure dem System entsprechende Fragen stellten.

Erste Hilfe gegen AI-Crawler

Angesichts dieser Herausforderungen müssen Website-Betreiber ihre Schutzstrategien grundlegend überdenken

und mehrschichtige Abwehrsysteme implementieren. Cloudflares Ein-Klick-Lösung stellt derzeit die effektivste Sofortmaßnahme dar. Über eine Million Kunden haben diese Option bereits aktiviert, die alle bekannten AI-Bots blockiert. Die Funktion ist selbst für kostenlose Cloudflare-Nutzer verfügbar und kann im Dashboard unter „Security > Bots" aktiviert werden.

Ergänzend sollten Website-Betreiber ihre robots.txt-Dateien um spezifische AI-Crawler erweitern, auch wenn deren Wirksamkeit durch Fälle wie Perplexity in Frage gestellt wurde. Server-seitige Blockierungen durch User-Agent-Filter und IP-Range-Sperren bieten zusätzlichen Schutz, erfordern jedoch regelmäßige Updates.

Abwehrstrategien

Fortgeschrittene Abwehrstrategien konzentrieren sich auf die Verhaltensanalyse und Erkennung unnatürlicher Browsing-Muster. Anti-Bot-Technologien wie CAPTCHAs, Honeypots und IP-Throttling können helfen, zwischen menschlichen Nutzern und automatisierten Systemen zu unterscheiden. Content-Verschleierung durch dynamische Generierung und JavaScript-basierte Einblendung erschwert es Crawlern zusätzlich, wertvollen Inhalt zu extrahieren.

Das AI-Labyrinth

Das AI-Labyrinth stellt eine revolutionäre Abwehrstrategie dar: Statt Crawler einfach zu blockieren, werden sie in komplexe Netzwerke aus Fake-Content gelockt. Diese „Honeypot"-Seiten sind mit realistisch wirkenden, aber für Menschen uninteressanten Inhalten gefüllt und durch unendliche Link-Strukturen verbunden.

Crawler, die in diese digitalen Labyrinthe geraten, verschwenden nicht nur massive Ressourcen, sondern sammeln auch völlig wertlose oder sogar bewusst irreführende Daten. Dies sabotiert die Qualität der trainierten AI-Modelle und macht das unrechtmäßige Scraping wirtschaftlich unattraktiv

Die Zukunft ethischer Datennutzung

Cloudflares geplanter Pay-per-Crawl-Marktplatz könnte eine nachhaltige Lösung für den Konflikt zwischen AI-Unternehmen und Content-Erstellern bieten. Dieses System würde es KI-Firmen ermöglichen, transparent und legal auf Website-Inhalte zuzugreifen, während Website-Betreiber für die Nutzung ihrer wertvollen Daten kompensiert werden.

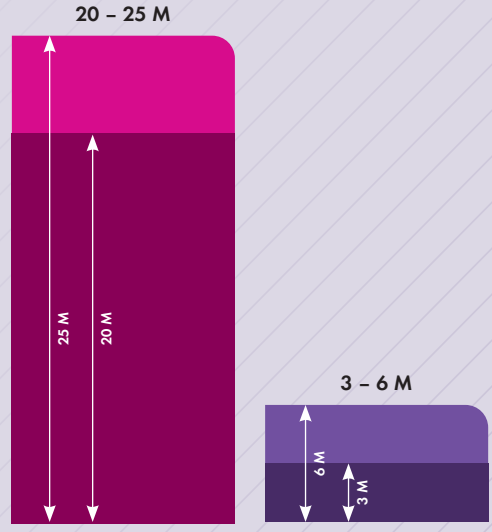
Ein solcher Marktplatz könnte verschiedene Preismodelle unterstützen: von pauschalen Lizenzgebühren über nutzungsbasierte Abrechnung bis hin zu gewinnbeteiligungsbasierten Modellen. Dies würde heimliche Scraping-Praktiken durch legitime Geschäftsbeziehungen ersetzen und eine Win-Win-Situation für alle Beteiligten schaffen.

Professionelle Bot-Protection-Services wie DataDome, HUMAN Security oder BotGuard bieten spezialisierte Lösungen mit Echtzeit-Erkennung in Millisekunden. CDN-basierte Dienste von Anbietern wie Cloudflare, AWS oder Akamai integrieren Schutzmaßnahmen direkt in die Infrastruktur-Ebene. Ergänzend können rechtliche Strategien durch verschärfte Terms of Service und die Vorbereitung von DMCA-Takedown-Notices die Position der Website-Betreiber stärken.

Parallelen

Das Ganze erinnert an das Thema Websiten und Werbung versus Adblocker. Die Parallelen zwischen der AI-Crawler-Problematik und dem Adblocker-Dilemma sind tatsächlich frappierend und zeigen ähnliche Grundkonflikte auf.

PERFLEXITY AI: OFFIZIELLE VS. HEIMLICHE CRAWLER-AKTIVITÄTEN



Zahlen zeigen das Ausmaß:
Neben den offiziellen Crawlern, die bereits 20-25 Millionen Anfragen täglich generierten, setzte das Unternehmen zusätzliche „Stealth-Crawler" ein, die weitere 3-6 Millionen Requests pro Tag durchführten.

Quelle:
Cloudflare Security Research, August 2025

➤ **Kostenlose Inhalte gegen Gegenleistung:** In beiden Fällen stellen Website-Betreiber kostenlose Inhalte zur Verfügung und erwarten dafür eine bestimmte „Gegenleistung" - bei Werbung die Aufmerksamkeit der Nutzer, bei AI-Crawlern die Kontrolle über die Datennutzung. Sowohl Adblocker als auch aggressive Crawler „brechen" diesen impliziten Vertrag.

➤ **Technisches Wettrüsten:** Beide Bereiche zeigen das gleiche Muster eines eskalierenden technischen Wettrüstens. Website-Betreiber entwickeln Anti-Adblocker-Technologien, Adblocker werden daraufhin sophistizierter. Genauso entwickeln sich Bot-Detection und Crawler-Umgehungstechniken gegenseitig weiter.

➤ **Legitimität der Umgehung:** Interessant ist, dass beide Praktiken rechtlich meist im Graubereich operieren. Adblocker-Nutzer argumentieren mit ihrer Privatsphäre und Performance, AI-Unternehmen mit „Fair Use" und öffentlich verfügbaren Daten.

Entscheidende Unterschiede

➤ **Direkte vs. indirekte Monetarisierung:** Hier liegt der Kernunterschied. Werbung blockiert primär die Einnahmen, während AI-Crawler die Inhalte selbst „stehlen" und für kommerzielle Zwecke verwerten. Ein Adblocker-Nutzer konsumiert immer noch den ursprünglichen Content, aber ein AI-System kann diesen Content später reproduzieren und damit konkurrieren.

➤ **Nutzen für den Einzelnen vs. Unternehmen:** Adblocker dienen primär dem individuellen Nutzer (bessere Ladezeiten, weniger Ablenkung, Privatsphäre). AI-Crawler dienen dagegen primär kommerziellen Interessen von Unternehmen, die damit Milliarden-Dollar-Geschäfte aufbauen.

➤ **Skalierung und Automatisierung:** Ein Adblocker blockiert nur für einen einzelnen Nutzer. AI-Crawler hingegen „skalieren" das Problem - sie sammeln Millionen von Inhalten automatisiert und verwerten diese systematisch.

Lösungsansätze im Vergleich

➤ **Bezahlmodelle:** Beide Bereiche experimentieren mit ähnlichen Lösungen. Wie Websites „Adblocker-Nutzer" bitten, ein Abo abzuschließen, könnte der Pay-per-Crawl-Marktplatz eine strukturierte Monetarisierung ermöglichen.

➤ **Technische Eskalation:** Cloudflares AI-Labyrinth erinnert an Anti-Adblocker-Technologien - beide versuchen, unerwünschte automatisierte Systeme zu verwirren oder zu blockieren.

➤ **Branchenstandards:** In beiden Fällen entwickeln sich langsam Industriestandards. Bei Werbung gibt es „Acceptable Ads"-Programme, bei AI könnte es ähnliche ethische Frameworks geben.

Der entscheidende Unterschied

Während das Adblocker-Problem primär ein Einnahmenproblem ist (Nutzer konsumieren Content, zahlen aber nicht dafür), ist das AI-Crawler-Problem ein Verwertungsrechtsproblem (Content wird ohne Erlaubnis kommerziell weiterverwertet). Das macht die AI-Problematik rechtlich und ethisch komplexer, da hier nicht nur Einnahmen verloren gehen, sondern die komplette Kontrolle über die eigenen Inhalte.

Interessant ist auch: Viele Nutzer sehen Adblocker als legitimes Recht an, während heimliches AI-Scraping selbst von technikaffinen Nutzern oft als problematisch empfunden wird. Das könnte daran liegen, dass bei Adblockern der Nutzer selbst entscheidet, während bei AI-Crawlern große Konzerne über die Köpfe der Website-Betreiber hinweg agieren.

TO-DOS FÜR WEBSEITENBETREIBER

1. **Cloudflare AI-Bot-Blocker aktivieren**
2. **robots.txt erweitern**
3. **Server-seitige Filterung**
4. **Monitoring einrichten**

Fazit

Der Perplexity-Skandal markiert einen entscheidenden Wendepunkt in der Auseinandersetzung zwischen KI-Unternehmen und Content-Erstellern. Er zeigt nicht nur die Grenzen traditioneller Schutzmaßnahmen auf, sondern auch die Notwendigkeit innovativer, mehrschichtiger Abwehrstrategien.

Website-Betreiber können nicht mehr darauf vertrauen, dass ethische Standards von allen Marktteilnehmern respektiert werden. Stattdessen müssen sie proaktive, technologiegestützte Schutzmaßnahmen implementieren und sich auf eine neue Ära der digitalisierten Content-Kontrolle einstellen.

Cloudflares Reaktion mit dem AI-Labyrinth und dem geplanten Pay-per-Crawl-Marktplatz könnte dabei wegweisend für die gesamte Branche werden und Standards für ethische AI-Datensammlung etablieren. Die Zeit der kostenlosen, unregulierten Datensammlung geht zu Ende – Website-Betreiber bekommen endlich die Werkzeuge an die Hand, ihre wertvollen Inhalte zu schützen und zu monetarisieren.

Ulrich Parthier

All-in-one-Lösung für sichere E-Mails

EINFACH UMSETZEN, UMFASSEND GESCHÜTZT

Ob Kundenkommunikation, Vertragsunterlagen oder interne Informationen: E-Mails transportieren täglich geschäftskritische Daten und sind zugleich ein Einfallstor für Angriffe. Die Secure-E-Mail-SaaS-Lösung von SEPPmail schützt Unternehmen umfassend: Verschlüsselung, digitale Signatur, Zertifikat, intelligenter Filter und der sichere Versand großer Dateien (LFT) sind in einem Service vereint – intuitiv bedienbar, rechtssicher und DSGVO-konform.

it-sa Expo&Congress
Besuchen Sie uns
in **Halle 7-232**
SEPPMAIL

Echte Sicherheit – sofort einsetzbar
Der Clou: Die Cloud-Lösung kann in nur 30 Minuten integriert werden – ohne komplizierte Einrichtungen, administrativen Aufwand oder lange IT-Prozesse. Anwender müssen sich nicht umstellen, und auch die IT-Abteilungen profitieren von minimalem Aufwand. Neben Cloud auch als On-Premises – SEPPmail passt sich an bestehende Infrastrukturen an und wächst mit den Anforderungen. Auch sensible Bereiche wie Personalabteilungen oder der Versand von medizinischen Befunden im Gesundheitswesen lassen sich so problemlos absichern.

Einfach sicher kommunizieren – mit Vertrauen
Sichere E-Mail-Kommunikation darf nicht kompliziert sein. SEPPmail schafft Vertrauen in jede versendete Nachricht – durch nachvollziehbare Sicherheitsmechanismen, benutzerfreundliche Prozesse und technische Zuverlässigkeit. Das Ziel: Kommunikation, die geschützt, verständlich und für alle Beteiligten komfortabel ist. Damit E-Mails das bleiben, was sie sein sollen – ein sicheres und zuverlässiges Kommunikationswerkzeug im Geschäftsalltag.

www.seppmail.com/de/technologie/

Der blinde Fleck im Identitätsmanagement

WARUM IAM-RISIKOANALYSEN BEI DEN DATEN BEGINNEN

Während sich Unternehmen intensiv mit externen Cyberbedrohungen beschäftigen, übersehen sie oft die größten Risiken in den eigenen Systemen: privilegierte Accounts, verwaiste Berechtigungen und unkontrollierte Datenzugriffe. Eine systematische IAM-Risikoanalyse nach IT-Grundschutz deckt Schwachstellen auf und erfüllt gleichzeitig die Anforderungen an ein strukturiertes Risikomanagement gemäß BSI-Standards – doch die meisten Ansätze setzen am falschen Ende an.

Datenzugriff? Der entscheidende Perspektivwechsel

Traditionelle IAM-Konzepte konzentrieren sich auf die Verwaltung von Benutzerkonten. Dabei ist die entscheidende Frage eine andere: Welche Daten sind für mein Unternehmen wirklich kritisch? Sie würden doch sicher zustimmen, dass ein Administrator mit Vollzugriff auf Testdaten am Ende weniger riskant ist als ein Sachbearbeiter mit Schreibzugriff auf alle Kundendaten. Eine effektive Risikoanalyse beginnt daher genau hier - bei den Daten selbst.

In 3 Schritten von den Daten zum Risiko

SCHRITT #1:

Datenbereiche analysieren

Der erste Schritt orientiert sich an den IT-Grundschutz-Kategorien Vertraulichkeit, Integrität und Verfügbarkeit. Welche Daten dürfen nicht in falsche Hände geraten? Welche dürfen nicht verändert werden? Welche müssen jederzeit verfügbar sein? Anschließend erfolgt die Einschätzung, wie kritisch ein Verlust oder eine Manipulation der Daten für das Unternehmen wäre – von nur geringen Auswirkungen bis existenzbedrohend.

SCHRITT #2:

Berechtigungen zuweisen

Nun wird analysiert, welche Berechtigungen auf diese kritischen Datenbereiche zugreifen können. Dabei werden sowohl Zugriffsart (lesend, schreibend) als auch Umfang (gesamter Datenbereich oder nur Teile) erfasst. So hat ein Vertriebsmitarbeiter vielleicht lesenden Zugriff auf alle Kundendaten, aber schreibenden nur auf seine eigenen Kunden.

SCHRITT #3:

Schwachstellen erfassen

Eine systematische Einbeziehung von Schwachstellen ist sehr wichtig, um das Risiko von Konten und Personen berechnen zu können. Mögliche Schwachstellen könnten z.B. eine fehlende Multifaktor-Authentifizierung sein, Pflichtschulungen, die noch ausstehen, oder Kennwörter, die länger nicht geändert wurden.

Automatische Risikobewertung

Aus den ersten beiden Schritten errechnet die IAM-Software automatisch die Kritikalität von Konten basierend auf den Zugriffsmöglichkeiten auf kritische Daten. Die finale Risikobewertung kombiniert diese Account-Kritikalität mit den identifizierten Schwachstellen. So kann ein erfahrener Administrator mit privilegierten Berechtigungen durch umfassende Schulungen ein geringeres Gesamtrisiko aufweisen als ein ungeschulter Mitarbeiter.

Nachhaltiges Risikomanagement statt Stichproben

Komplexe IT-Landschaften und sich ständig ändernde Berechtigungsstrukturen machen eine kontinuierliche Risikoüberwachung für jedes Unternehmen unverzichtbar. Moderne IAM-Systeme unterstützen Sie dabei systematisch und wandeln die manuelle Einzelfallbetrachtung in einen kontinuierlichen, automatisierten Prozess. Der datenorientierte Ansatz gewährleistet somit, dass kritische Konten und Personen im Unternehmen rechtzeitig identifiziert werden – die Grundlage für eine effektive Risikobewertung im Identity & Access Management.

Thomas Gertler
www.daccord.de

daccord: Die IAM-Software, die Sicherheit und Effizienz vereint

MODULARES IDENTITY & ACCESS MANAGEMENT FÜR JEDE UNTERNEHMENSGRÖSSE

Komplexe Berechtigungsstrukturen, manuelle Prozesse und immer aufwändigere Compliance-Anforderungen – ein modernes IAM muss mehr leisten als nur Benutzerverwaltung. daccord bietet fünf aufeinander abgestimmte Bundles, die Identity & Access Management zum strategischen Wettbewerbsvorteil machen.

Die daccord Bundles im Überblick

Identity Analysis: Wollen Sie Berechtigungen in Ihrer IT-Umgebung kontinuierlich und nachhaltig kontrollieren?

Permission Analysis: Benötigen Sie Informationen zu Personen, Konten und Berechtigungen bis in die Tiefe?

Provisioning: Was, wenn Berechtigungen sich von heute auf morgen ändern? Wollen Sie neue Zuweisungen automatisch ablaufen lassen?

Identity Lifecycle: Benötigen Sie automatisierte Workflows für Ein- und Austrittsprozesse Ihrer Mitarbeiter oder sonstige Veränderungen wie Abteilungswechsel, Elternzeiten?

Governance: Muss Ihr Unternehmen regulatorische Anforderungen erfüllen? Sind (Re-)Zertifizierungs-Prozesse und das Aufdecken von Missständen wie Funktionstrennungskonflikte (SoD) für Sie wichtig?

Full-Stack: Das Rundum-Sorglos-Paket, das alle daccord-Funktionalitäten vereint. Ihre komplette IAM-Lösung für maximale Effizienz.

Warum Kunden daccord wählen

Modular skalierbar: Starten Sie mit einem Bundle und erweitern Sie Ihr daccord-System nach Bedarf. So kann es sukzessive wachsen und immer mehr Effizienz und Sicherheit im Unternehmen gewährleisten.

Praxisorientiert entwickelt: Entstanden aus über 20 Jahren IAM-Beratung, löst daccord sehr praxisorientiert die Herausforderungen in Unternehmen verschiedenster Größen und Branchen.

KI-unterstützt: Moderne Algorithmen automatisieren Routineaufgaben und erkennen Anomalien, bevor sie zum Problem werden.

Compliance-Ready: Vorgefertigte Richtlinien und Reports unterstützen gängige Regulatorien wie die EU-DSGVO, MaRisk oder NIS2.

www.daccord.de

it-sa Expo&Congress

Besuchen Sie uns in **Halle 7-349**

Verpassen Sie nicht die zwei Fachvorträge von Thomas Gertler, Lead-Architekt der IAM-Software daccord

Am 07.10.25, 11:45 Uhr in Halle 7, Forum D
Versteckte Gefahren: Riskante Accounts erkennen und kritische Daten schützen

Am 08.10.25, 13:45 Uhr in Halle 7, Forum D
KI meets Identity & Access Management – Status Quo und Ausblick

daccord

Künstliche Intelligenz

UNGLÜCKSBRINGER ODER RETTER IM CYBERRAUM?

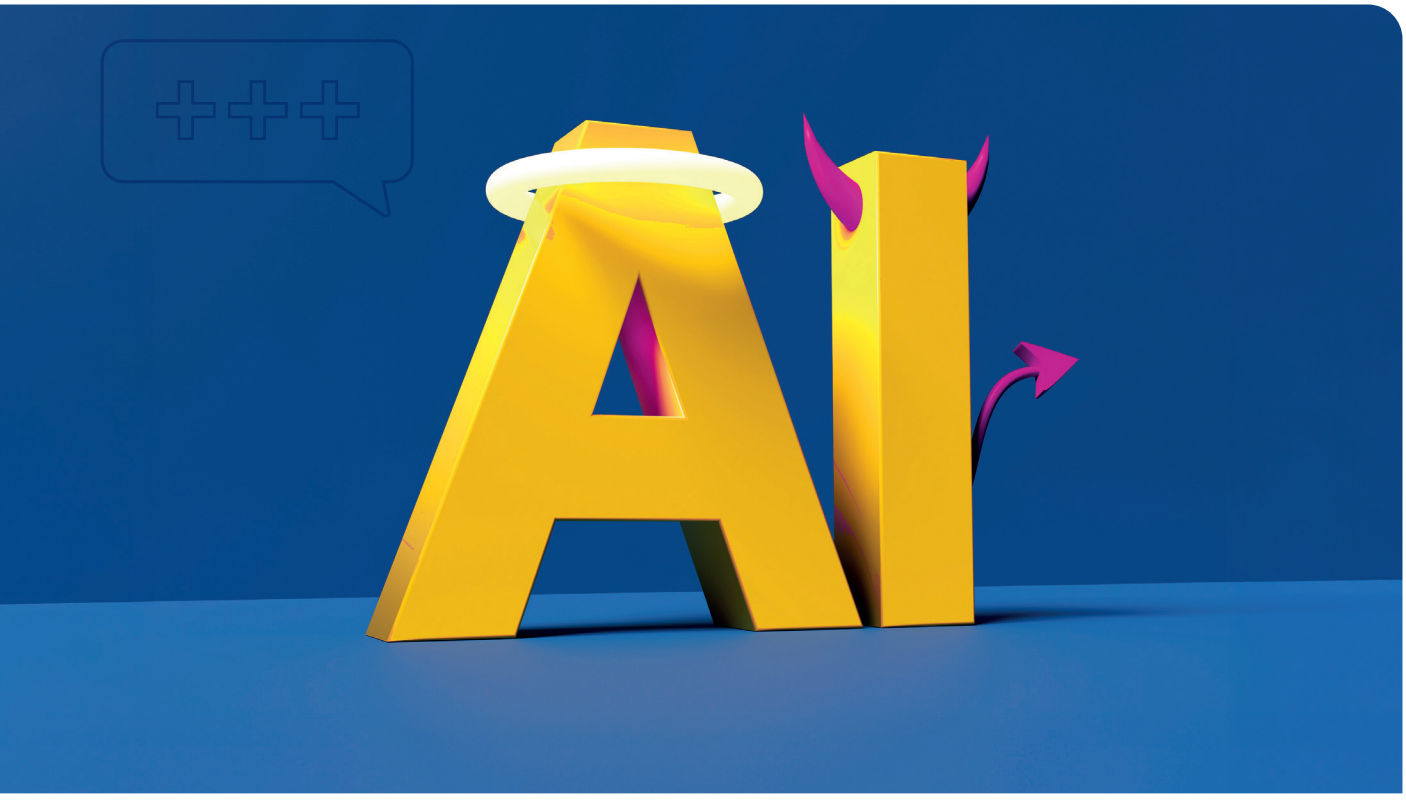
Künstliche Intelligenz ist die Zukunftstechnologie. In Bezug auf Cybersecurity stellt sich die Frage, wer diese Technologie am besten für seine Ziele nutzt. KI hat unbestritten Vorteile für die Sicherheit, für den Channel und für das Überwinden der Spezialistenknappheit. Aber sie wird auch von den Cyberkriminellen eingesetzt. Darüber haben wir mit Stefan Fritz, Director Channel Sales für Sophos EMEA Central von Sophos, gesprochen.

it security: *Herr Fritz, die einen sagen KI sei eine Gefahr, insbesondere für die Cybersicherheit. Andere sind sich sicher, dass KI das wirksamste Mittel für die Security darstellt. Wie schätzen Sie das Potenzial von KI ein?*

Stefan Fritz: Beide Aussagen sind richtig. Allerdings wird KI heute unterschiedlich intensiv eingesetzt. In Bezug auf die Cybersicherheit liegen Nutzen und Vorteil meiner Meinung nach im Moment sehr deutlich auf der Seite der Verteidiger.

it security: *Das heißt, dass KI im Cyberschutz und im Rennen zwischen Angreifern und Verteidigern die Nase vorne hat?*

Stefan Fritz: Das ist richtig. Die Cyberkriminellen nutzen zwar ebenfalls KI, allerdings laut unserer Forschungen weit weniger strategisch als man meinen könnte. KI kommt bei vergleichsweise simplen Aufgaben wie der Erstellung von Phishing-Mails oder Social Engineering zum Einsatz, dafür aber massenhaft. Hingegen gibt es bis heute kaum Anhaltspunkte, dass Cyberkriminelle KI bei der Erstellung ihrer Malware mit eigens erzeugten und trainierten LLMs einsetzen. Das brauchen sie auch nicht, denn mit den traditionellen Angriffs-



Tools und -Strategien erreichen sie bislang immer noch die meisten ihrer Ziele.

it security: *Und wie sieht es auf der Seite der Verteidigung aus?*

Stefan Fritz: Unternehmen wie Sophos bieten Sicherheits-Plattformen mit KI, die Anomalien und Angriffe erkennen und verhindern – weit besser als es traditionelle Security-Software könnte. Damit der Vorsprung vor den Cyberkriminellen Bestand hat, investieren wir sehr viel in die Forschung in unseren Labs und nutzen eigens erstellte beziehungsweise trainierte KI-Modelle und LLMs, die speziell auf die Risikopotenziale ausgerichtet sind. Das ist bedeutend mehr Aufwand, als es die Cyberkriminellen mit KI betreiben, und das ist der Grund, weshalb die KI der Sicherheit aktuell viel mehr bietet als den Angreifern.

it security: *In welcher Hinsicht kann die KI Ihrer Meinung nach den Unternehmen zusätzlich helfen?*

Stefan Fritz: Hier kommt ein Bereich ins Spiel, der mindestens so wichtig ist wie das Erkennen und Verhindern von Angriffen. Der Markt leidet seit Jahren unter einer Knappheit an Security-Spezialisten. Ein Ausweg für Unternehmen sind Security-Dienstleistungen durch leistungsfähige Partner. Aber auch diese brauchen immer mehr Kapazitäten. Hier kommt die KI ins Spiel.

it security: *Wie dramatisch ist Ihrer Meinung nach die Knappheit an Security-Spezialisten und der Druck auf die Verantwortlichen?*

Stefan Fritz: Da liegt zurzeit einiges im Argen. Im aktuellen Sophos State of Ransomware Report 2025 berichten 76 Prozent der befragten IT-Fachleute von Burnout. Knapp 20 Prozent beschreiben dies als „ständiges" Problem. Dieses Problem verschärft sich, denn 69 Prozent berichten, dass Ermüdung und Burnouts im Bereich Cybersicherheit von 2023 bis 2024 zugenommen haben. Hilfreich zur Lösung dieser Herausforderung sind MDR-Services. 92 Prozent der Befragten haben diese beiden Symptome im Bereich Cybersicherheit durch MDR-Services verringert. Aber wie gesagt, der Fachkräftemangel liegt nicht nur bei Unternehmen, sondern auch bei unseren Partnern.

UNTERNEHMEN WIE SOPHOS BIETEN SICHERHEITS-PLATTFORMEN MIT KI, DIE ANOMALIEN UND ANGRIFFE ERKENNEN UND VERHINDERN – WEIT BESSER ALS ES TRADITIONELLE SECURITY-SOFTWARE KÖNNTE.

Stefan Fitz, Director Channel Sales, Sophos EMEA Central, www.sophos.com

it security: *Kann die KI auch den IT-Dienstleistern helfen?*

Stefan Fritz: Unsere Partner erhalten ebenso wie Unternehmen durch KI einen bedeutenden Sicherheits-, Ressourcen- und Zeitgewinn – beispielsweise durch automatisierte Reaktion auf von KI entdeckte Anomalien. Damit erhalten die Security-Spezialisten die nötigen Ressourcen für das Aufspüren und Schließen von Sicherheitslücken oder für strategische Aufgaben. Ein Beispiel: Wie könnten Unternehmen oder IT-Dienstleister die Vorgaben wie NIS2 umsetzen, wenn die Last der täglichen Security-Administration keinen Raum dafür lässt? KI ist die Antwort darauf.

it security: *Das heißt, KI ist nicht nur eine wichtige Komponente für die Sicherheit, sondern auch für die strategische Resilienz im Business?*

Stefan Fritz: Unternehmen schaffen mit KI ein höheres Sicherheitsniveau. Zudem setzt die Technologie die nötigen Ressourcen bei den Sicherheits-Teams frei, um die Strategie im Cyberschutz voranzutreiben und richtlinienkonform zu bleiben. Das gilt auch für unsere Partner. Sie bieten mit KI ihren Kunden eine maßgeblich höhere Sicherheit, und schaffen gleichzeitig im eigenen Unternehmen den Raum für mehr Dienstleistung und Business.

Zusammengefasst wird KI bei den Cyberkriminellen aktuell eher auf niedrigem Level eingesetzt und die Cybersecurity hat mit ihrer Forschung und Entwicklung spezieller LLMs die Nase im KI-Rennen vorne. Darüber hinaus schafft KI maßgebliche Vorteile strategischer Natur, darunter bei der Problemlösung des Fachkräftemangels und für das Business der Systemhäuser und MSPs.

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

Herausforderung Mikrosegmentierung

ZERO-TRUST-KOMPLEXITÄT ÜBERWINDEN

> DIE ÜBERWACHUNG VON NETZWERKVERBINDUNGEN ERMÖGLICHT PRÄZISE FIREWALL-REGELN.
>
> **Kay Ernst, Regional Sales Manager DACH, Zero Networks, www.zeronetworks.com**

Mikrosegmentierung ist ein zentrales Element von Zero-Trust-Architekturen, da sie Netzwerkverkehr engmaschig kontrolliert und die Angriffsfläche verringert. Die Umsetzung scheitert jedoch oft an der hohen Komplexität, unzureichenden Ressourcen, Betriebsunterbrechungen, eingeschränkter Skalierung und mangelnder Transparenz.

Mikrosegmentierung ist komplex und teuer, da unter anderem alle Anwendungsabhängigkeiten und Netzwerkflüsse zu erfassen sind. Manuelles Tagging ist zeitintensiv, während herkömmliche Lösungen zu Fehlkonfigurationen führen können. Fehlkonfigurierte Richtlinien können legitimen Datenverkehr blockieren. Wachsende Hybrid- und Multi-Cloud-Umgebungen erschweren die Skalierung von Richtlinien, wodurch Sicherheitslücken drohen. Die Erstellung effektiver Segmentierungsrichtlinien scheitert oft an unklaren Netzwerkverhältnisse.

Zero Networks adressiert diese Herausforderungen durch automatisierte Richtlinienerstellung, einen agentenlosen und skalierbaren Ansatz, die Minimierung von Betriebsrisiken sowie verbesserte Sichtbarkeit und Ressourceneffizienz. Die Implementierung erfolgt ohne einen Agenten auf den zu schützenden Endpunkten in verschiedenen Infrastrukturen. Die Überwachung von Netzwerkverbindungen ermöglicht präzise Firewall-Regeln ohne manuelles Tagging. Adaptive Richtlinien passen sich in Echtzeit an, um Ausfallzeiten infolge von versehentlich blockiertem Traffic zu reduzieren. Umfassende Einsichten in den Netzwerkverkehr unterstützen die Identifizierung von Abhängigkeiten und Risiken. Die Automatisierung schließlich senkt den Bedarf an hochspezialisierten Fachkräften und beschleunigt Projekte, was Kosten einspart.

Kay Ernst


ninjaOne®
Besuchen Sie uns auf der
it-sa in Halle 7, Stand 504
Schluss mit dem
IT-Security-Frust
Reduzieren Sie Sicherheitslücken
Schützen Sie sich vor Ransomware
Härten Sie Ihre Endpunkte

Digitale Infrastruktur? Widerstandsfähig und Agil!

UNIVERSELLE SICHERHEIT MIT ZERO TRUST EVERYWHERE

Zero Trust basiert auf der Grundidee, dass keinem Gerät, User oder keiner Anwendung von Natur aus vertraut wird – unabhängig davon, ob sie sich innerhalb oder außerhalb des Unternehmensnetzes befinden. Stattdessen erfordert dieses Sicherheitsmodell, dass jede Interaktion authentifiziert, autorisiert und kontinuierlich überwacht wird. Mit seiner Sicherheitsplattform erweitert Zscaler nun Zero Trust Everywhere und dehnt damit die Prinzipien des Zero Trust-Ansatzes auf neue Bereiche der digitalen Infrastruktur aus.

Egal wo die digitale Kommunikation heute im Unternehmen stattfindet, muss der Schutz von Assets gegen unerwünschten Zugriff berücksichtigt werden. Doch viele Bereiche waren bisher noch nicht unter dem Schutzschirm eines Zero Trust-Ansatzes abgedeckt. In einer Zeit, in der Bedrohungen sowohl innerhalb als auch außerhalb traditioneller Unternehmensnetzwerke exponentiell zunehmen, muss das Zero Trust-Modell in die Breite und Tiefe ausgeweitet werden. Zero Trust ist eine moderne Sicherheitsstrategie, die darauf abzielt, jede Verbindung und jeden Datentransfer zu überprüfen und zu validieren. Zscaler treibt diese Vision voran und bietet Lösungen für User, Cloud Workloads, IoT/OT-Geräte und sich ständig wandelnde Geschäftsanforderungen im Bereich der Mobilität und sogar von KI-Agenten.

Das Ziel ist es, Unternehmen in die Lage zu versetzen, ihre Infrastruktur widerstandsfähiger, agiler und sicherer zu gestalten. Dabei schafft Zscaler die Voraussetzungen für eine sichere und effiziente Durchführung von geschäftlichen Prozessen – unabhängig von Ort, Gerät oder Netzwerk. Mit Zero Trust Everywhere wird sichergestellt, dass alle Zugriffe und Interaktionen in der digitalen Infrastruktur konsistent und umfassend geschützt werden, ohne Einschränkungen durch geografische Standorte oder traditionelle Netzwerksicherheitsmodelle.

Zero Trust Everywhere – eine neue Sicherheitsvision

Bislang war Zero Trust-basierte Segmentierung auf Ebene des Users zu einer benötigten Anwendung, auf Ebene von Workloads oder einzelnen Geräten möglich. Am Beispiel des Users wird die Grundfunktion von Zero Trust transparent: Zero Trust for Users bedeutet, dass jeder Benutzer – ob remote, in einem Büro oder unterwegs – kontinuierlich authentifiziert und autorisiert wird. Hierbei werden erweiterte Identitätsprüfungen wie Multi-Faktor-Authentifizierung (MFA) und biometrische Verfahren eingesetzt und der Zugriff erfolgt nach dem Prinzip der geringstmöglichen Rechte. Durch die Zscaler Zero Trust Exchange wird sichergestellt, dass jeder User unabhängig von seinem Standort durch definierte Zugriffsrichtlinien nur auf die Anwendungen und Daten zugreifen kann, die für seine Aufgabe erforderlich sind. Gleichzeitig wird der Datenverkehr verschlüsselt und durch kontinuierliches Monitoring

auf Bedrohungen überprüft, was eine sichere und performante Arbeitsumgebung schafft.

Analog greift der Zero Trust-Ansatz für Clouds und stellt auch hier sicher, dass alle Anwendungen und Daten innerhalb der Cloud gegen unautorisierten Zugriff oder Datenlecks geschützt sind, unabhängig davon, ob sie sich auf Amazon Web Services (AWS), Microsoft Azure, Google Cloud oder einer anderen Plattform befinden. Auch die Bereiche IoT (Internet of Things) und OT (Operational Technology) rücken zunehmend in den Fokus von Cyberkriminellen, da diese Geräte oft nicht mehr über angemessene Sicherheitsfunktionen verfügen und leicht angreifbar sind. Zero Trust for IoT/OT setzt darauf, jedes Gerät, jede Maschine und jede Verbindung innerhalb des Netzwerks permanent zu validieren. Durch strenge Mikrosegmentierung werden Zugriffe auf sensible Geräte und Daten eingeschränkt. Diese Sicherheit wird durch kontinuierliche Analysen erweitert, die potenzielle Bedrohungen in Echtzeit erkennen und darauf reagieren können.

Zero Trust für 5G und mobile Netzwerke

Mit dem Aufkommen von 5G-Technologie entstehen neue Chancen, aber auch neue Sicherheitsrisiken. Mit Zscaler Cellular wird die Vision von „Zero Trust Everywhere" auf den Bereich der Mobilkommunikation erweitert. Diese Ausdehnung des Zero Trust-Ansatzes greift für mobile Netzwerke und alle Arten mobiler Dinge, die über eine SIM-Karte oder eSIMs angebunden werden können. Auf diese Weise kommen auch mobil kommunizierende Dinge – von Handheld-Devices in der Logistik bis hin zu autonomen Fahrzeugen – unter den Schutzschirm der Zero Trust Exchange-Plattform. Sie stellt sicher, dass Daten, die über mobile Netzwerke übertragen werden, vollständig geschützt sind, Bedrohungen frühzeitig abgewehrt werden und nur autorisierte Zugriffe ermöglicht werden.

ZERO TRUST IST EINE UMFASSENDE VISION, DIE ALLE ASPEKTE DER DIGITALEN INFRASTRUKTUR EINES UNTERNEHMENS SICHERN UND NAHTLOS MITEINANDER VERKNÜPFEN SOLL.

Kevin Schwarz, Head of CTOs in Residence, Zscaler Germany GmbH, www.zscaler.com

Die Ausdehnung auf KI-Anwendungen

Künstliche Intelligenz verändert die Arbeitsweise von Unternehmen und bringt gleichzeitig neue Sicherheitsherausforderungen mit sich. KI-Anwendungen und KI-Agenten, die große Datenmengen verarbeiten oder damit trainiert werden, erfordern eine präzise Kontrolle über Datenverwendung und Datenintegrität und deshalb auch granulare Zugriffskontrollen.

Dementsprechend sollte die Zero Trust-Segmentierung auch hier Anwendung finden, wo es auf den Kern der Datensicherheit ankommt und Einblick geben, wer auf was Zugriff hat. Hier kommen beispielsweise Anwendungsbereiche zum Tragen, bei denen ein KI-Agent über neue Protokolle wie MCP mit anderen Systemen kommunizieren soll und oder mit anderen Agenten interagiert. Dabei ist es wichtig die Kontrolle zu haben, worauf zugegriffen und wie bzw. worüber kommuniziert werden darf. Gleichzeitig bedarf es in der Nutzung von GenKI einer tieferen Granularität. Sichtbarkeit auf Prompt-Ebene wird benötigt, wenn Unternehmen seinen Mitarbeitenden z.B. Copilot und/oder Kunden Chatbots bereitstellen.

Zscaler hat seine Plattform mit Funktionen erweitert, die speziell auf KI-Anwendungen ausgerichtet sind. Dies beinhaltet den Schutz sensibler Daten während des Trainings von KI-Modellen, die Verhinderung von Manipulation oder Datenlecks sowie die Absicherung von KI-gesteuerten automatisierten Prozessen. Mit diesen Erweiterungen können Unternehmen die Vorteile der KI voll ausschöpfen, ohne Sicherheitsanforderungen zu kompromittieren. Auch wenn Agentic KI derzeit noch in der Anfangsphase ist, tun Unternehmen angesichts der Geschwindigkeit der Weiterentwicklung neuer Anwendungsbereiche schon heute gut daran, für die Sicherheit ihrer Daten zu sorgen.

Ausblick

Zero Trust ist eine umfassende Vision, die alle Aspekte der digitalen Infrastruktur eines Unternehmens sichern und nahtlos miteinander verknüpfen soll. Gerade im Zeitalter von GenKI ist Zero Trust relevanter denn je. Mit Lösungen, die auf User, Clouds, IoT/OT-Geräte und mobile Netzwerke abzielen, sowie Erweiterungen für KI-Anwendungen und SecOps, ist die Zero Trust Exchange-Plattform universell aufgestellt, um Unternehmen ganzheitlichen Schutz zu bieten. Organisationen sind damit in der Lage, sicher, flexibel und innovativ zu agieren – unabhängig davon, wie sich die digitale Bedrohungslandschaft weiterentwickelt.

Kevin Schwarz

Warum Zero Trust jetzt so wichtig ist

IHR NETZWERK IST OFFEN WIE EIN SCHEUNENTOR – ZERO TRUST MACHT ES WIEDER SICHER

Hybrides Arbeiten, mobile Mitarbeiter und eine Vielzahl von IoT-Geräten haben die Netzwerkgrenzen aufgelöst. Doch nicht nur das Homeoffice ist ein Risiko: Im Access-Netzwerk befinden sich zahlreiche Systeme wie Drucker, Gebäudesteuerungen oder IoT-Devices, die sich nicht mit klassischen Endpoint-Lösungen wie EDR absichern lassen. Diese Schwachstellen bieten Angriffsflächen für Cyberkriminelle.

ZERO-TRUST IST DER SCHLÜSSEL FÜR DAUERHAFTE ABSICHERUNG.

Stefan Tiefel, Senior Market Development Manager (Security & Network), www.noris.de

Zero Trust begegnet dieser Herausforderung mit einem klaren Prinzip: „Niemals vertrauen, immer überprüfen." Jede Zugriffsanfrage wird konsequent validiert – unabhängig davon, ob sie von innen oder außen kommt.

Die Säulen einer Zero-Trust-Architektur

Ein wirksames Zero-Trust-Modell basiert auf folgenden Kernprinzipien:

- **Identitätsbasierte Sicherheit:** Zugriff nur für authentifizierte und kontinuierlich geprüfte Identitäten.
- **Geräte- und Endpunktsicherheit:** Während klassische Geräte mit EDR geschützt werden, müssen IoT- und agentenlose Geräte über Netzwerkkontrollen abgesichert werden.
- **Least Privilege Access:** Jeder Nutzer und jedes Gerät erhalten die für Sie nur minimal notwendigen Rechte.
- **Mikrosegmentierung:** Das Netzwerk wird in isolierte Bereiche aufgeteilt, um Angreifer am lateral Movement zu hindern.
- **Datenzentrierte Sicherheit:** Verschlüsselung und DLP schützen sensible Daten direkt.
- **Automatisierung:** Sicherheitsrichtlinien werden automatisiert und adaptiv umgesetzt, um Bedrohungen in Echtzeit zu erkennen.

Zero Trust umsetzen: Ein pragmatischer Ansatz

Die Einführung von Zero Trust erfolgt schrittweise:

#1 **Risikoanalyse:** Identifizieren Sie Schwachstellen – besonders bei agentenlosen Geräten im Netzwerk.

#2 **Roadmap & Priorisierung:** Starten Sie mit sensiblen Bereichen und skalieren Sie schrittweise.

#3 **Cloud- und On-Premises vereinheitlichen:** Zero Trust gilt für lokale und Cloud-Ressourcen.

#4 **Bestehende Infrastruktur nutzen:** Zero Trust lässt sich oft durch Erweiterung bestehender Systeme realisieren.

#5 **Mitarbeiter sensibilisieren:** Zero Trust funktioniert nur mit einer gelebten Sicherheitskultur.

Die Vorteile für Ihr Unternehmen
Zero Trust bietet entscheidende Mehrwerte:

- **Sicherheit im Access-Netzwerk und von überall:** Standard Clients und nicht-agentenfähige Geräte werden effektiv geschützt.
- **Reduktion der Angriffsfläche:** Jeder Zugriff wird überprüft, das Risiko von lateral Movement minimiert.
- **Compliance-Vorteile:** Bessere Nachvollziehbarkeit für DORA, NIS2 & Co.
- **Flexibilität & Skalierbarkeit:** Zero Trust wächst mit Ihrem Unternehmen. Egal ob Cloud, neue Geräte oder neue Geschäftsbereiche.
- **Produktivität & Nutzerfreundlichkeit:** Sichere Zugriffe ohne VPN-Barrieren.
- **Kostensicherheit:** Weniger Sicherheitsvorfälle senken langfristig die IT-Kosten.

Fazit
Zero Trust ist mehr als eine Antwort auf Homeoffice-Risiken. Es ist der Schlüssel, um hybride Arbeitsmodelle, Cloud-Dienste und unsichere Access-Netzwerke dauerhaft abzusichern. Wer sein Unternehmen zukunftssicher machen will, kommt an Zero Trust nicht vorbei.

Stefan Tiefel

it-sa Expo&Congress
Besuchen Sie uns in **Halle 7-212**
noris network

NDR als kritischer Baustein

ERST NDR VERVOLLSTÄNDIGT XDR-LÖSUNGEN

In der sich wandelnden Cybersicherheitslandschaft hat sich Extended Detection and Response (XDR) als leistungsfähiger Ansatz erwiesen. Das gezielte Zusammenführen einzelner Sicherheitstools bringt nicht nur mehr Transparenz, sondern liefert die Grundlage einer weitgehend automatisierten Bedrohungsabwehr. Doch trotz aller Vorteile fehlt vielen XDR-Lösungen ein entscheidendes Element: Network Detection and Response (NDR).

NDR spielt seine Stärken gezielt bei der Überwachung der Aktivitäten innerhalb eines Netzwerks aus – ganz unabhängig davon, ob dieses durch On-Premises-, Cloud- oder hybride Strukturen gekennzeichnet ist. Der zusätzliche Sicherheitsmechanismus greift in der Regel, wenn andere Maßnahmen zum Endgeräte- und Identitätsschutz bereits versagt haben. Sobald sich ein Angriff seitwärts im Netzwerk ausbreitet, Command-and-Control-Verbindungen aufgebaut werden, Datenexfiltration startet, Zugriffsberechtigungen in böswilliger Absicht erweitert und Netzwerkstrukturen ausgespäht werden, kann NDR zum Retter in der Not werden.

MIT NDR LÄSST SICH DER GESAMTE NETZWERKVERKEHR AUS JEDER RICHTUNG DURCHLEUCHTEN.

Bill Munroe, Senior Director Product Marketing, WatchGuard Technologies, www.watchguard.com/de

NDR erkennt Schwachstellen und Datenkompromittierung

Endpoint Detection and Response (EDR), Identity and Access Management (IAM), Cloud Security Management (CSM) und E-Mail-Sicherheit sind allesamt wichtige Komponenten einer XDR-Lösung und decken kritische Bedrohungsoberflächen im XDR-Prozess ab. Allerdings verwenden Angreifer zunehmend „Living-off-the-land"-Techniken (LotL), bei denen sie legitime Anmeldeinformationen oder Fehlkonfigurationen ausnutzen, anstatt herkömmliche Malware einzusetzen. NDR schließt genau diese Lücke: Sowohl der Nord-Süd- als auch der Ost-West-Netzwerkverkehr – und somit alle Datenströme innerhalb der Umgebung und über Firewalls hinweg – werden kontinuierlich überwacht, um verdächtiges Verhalten, Richtlinienverletzungen und Ausbreitungsversuche von Angreifern zu identifizieren.

NDR deckt Cloud-Strukturen und lokale Netzwerke ab

Die Notwendigkeit von NDR offenbart sich besonders in den sich verändernden Arbeitswelten. Moderne Organisationen agieren immer stärker im Rahmen hybrider IT-Strukturen, bei denen Anwendungen, Daten und Benutzer über lokale, Cloud- und Multi-Cloud-Umgebungen verteilt sind. Angreifer machen sich diese Komplexität zunutze, indem sie falsch konfigurierte Cloud-Berechtigungen, API-Schwachstellen und nicht überwachte Netzwerksegmente ausspielen, um Unternehmen zu infiltrieren.

Viele Sicherheitslösungen konzentrieren sich entweder auf On-Premises- oder Cloud-Ressourcen. Im Gegensatz dazu schafft NDR Klarheit für beides. Durch die Analyse des Netzwerkverkehrs auf Basis aller Datenflüsse und Pakete inklusive Anreicherung dieser Informationen mit Protokolldaten von SaaS-Anwendungen und Cloud-Umgebungen sowie den Logs von Identitätsplattformen kann NDR Hinweise auf Kompromittierung zuverlässig erkennen – ganz unabhängig davon, aus welcher Richtung diese kommen.

Wie NDR die Sicherheit in der Cloud und On-Premise verbessert:

#1 NDR überwacht den Datenverkehr in Cloud-Umgebungen und identifiziert anomale API-Aufrufe, ungewöhnliches Benutzerverhalten, nicht autorisierte Datentransfers und falsch konfigurierte Speicherzugriffe.

#2 In Hybridumgebungen erkennt NDR ungewöhnliche Verbindungen zwischen lokalen Netzen und Cloud-Infrastruktur und weist auf Datenexfiltration oder kompromittierte VPN-Zugangsdaten hin.

#3 NDR unterstützt Zero-Trust-Implementierungen durch kontinuierliche Überwachung und Analyse des gesamten Netzwerkverkehrs auf Richtlinienverstöße und unberechtigte Zugriffsversuche.

Risiko: XDR-Lösungen verzichten auf NDR

Trotz des Aufstiegs von XDR zur bevorzugten Cybersicherheitslösung integrieren viele Anbieter keine NDR-Funktionen von Haus aus. Stattdessen verlas-

sen sie sich in erster Linie auf EDR mit Agenten auf möglichst vielen Gerätetypen, was zwar nützlich ist, aber nicht ausreicht, um netzwerkbasierte Bedrohungen zu erkennen. Auf diese Weise entstehen leicht blinde Flecken.

Risiken von XDR ohne NDR:

#1 **Übersehene Insider-Bedrohungen:** Böswillige Insider und kompromittierte Konten bleiben ohne netzwerkbasierte Verhaltensanalyse unentdeckt.

#2 **Ineffektive Erkennung von Querverkehr:** Wenn es keine Transparenz auf Netzwerkebene gibt, können sich Angreifer unerkannt zwischen Systemen bewegen.

#3 **Unvollständige Cloud-Sicherheit:** API-Missbrauch und Cloud-Fehlkonfigurationen fallen oftmals nicht auf.

#4 **Geringe Wirksamkeit zur Aufdeckung von Angriffen auf die Lieferkette:** Schwachstellenbasierte Angriffe sind die verheerendste Angriffsmethode im Werkzeugkasten der Cyberkriminellen und werden es auch bleiben, solange NDR nicht flächendeckend eingesetzt wird.

#5 **Langsame Reaktion auf Vorfälle:** Ohne NDR-Erkenntnisse kommen XDR-Plattformen Bedrohungen oft erst dann auf die Spur, wenn der Schaden bereits eingetreten ist. Die durchschnittliche Reaktionszeit (MTTR) beträgt dann Wochen oder Monate.

Viele Unternehmen mit EDR-basierten XDR-Lösungen wiegen sich in Sicherheit, dabei bleiben ohne NDR nicht zu unterschätzende Lücken, die es Angreifern ermöglichen, über längere Zeiträume unentdeckt im Netzwerk zu operieren.

Cloudbasierte NDR-Lösungen

In der Vergangenheit erforderten NDR-Lösungen teure Hardware-Appliances und einen erheblichen Aufwand für die Bereitstellung vor Ort. Diese Hürde erschwerte vielen Unternehmen die Einführung und führte dazu, dass sie sich ausschließlich auf endpunkt- und protokollbasierte Sicherheitslösungen verließen. Mit den heutigen cloudbasierten NDR-Lösungen gibt es diese Einschränkungen nicht mehr.

Vorteile von cloudbasierten NDR-Lösungen:

#1 **Preis und Skalierbarkeit:** Ein Einsatz teurer Hardware vor Ort ist nicht erforderlich, es ergeben sich attraktive Preismodelle, die mit der Nutzung skalieren.

#2 **Bereitstellung:** Die Funktionalität kann in hybriden und Multi-Cloud-Umgebungen schnell ausgerollt werden.

#3 **KI-gesteuerte Erkennung:** Maschinelles Lernen verbessert die Erkennung von Anomalien, reduziert Fehlalarme und erhöht die Genauigkeit.

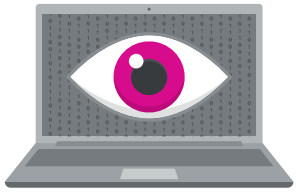
#4 **Nahtlose XDR-Integration:** Cloudbasierte NDR-Lösungen sind einfach in bestehende XDR-Plattformen integrierbar und ergänzen die fehlende Visualisierungsebene.

Auf diese Weise wird NDR für Unternehmen jeder Größe zugänglich und die Erkennung von Bedrohungen auf Netzwerkebene bleibt nicht länger allein Organisationen mit großen Sicherheitsbudgets vorbehalten.

Fazit: NDR ist keine Kür, sondern Pflicht für XDR

Im Zuge der Weiterentwicklung von Cyberbedrohungen müssen XDR-Lösungen vollständige Transparenz bieten, sowohl im Hinblick auf Endgeräte als auch auf Netzwerkstrukturen. Nur mit NDR ist es effektiv möglich, kompromittierte Anmeldeinformationen, Seitwärtsbewegungen und Insider-Bedrohungen in hybriden IT-Umgebungen zu erkennen. Unternehmen, die sich auf XDR ohne NDR verlassen, setzen sich einem erheblichen Risiko aus. Dabei ist die Integration von Netzwerkerkennung in XDR dank cloudbasierter NDR-Lösungen kein Luxus mehr – vielmehr gilt es als Notwendigkeit, um umfassenden Schutz zu gewährleisten.

Bill Munroe



Mit dem Auge eines Hackers

LÜCKEN IN DER ANGRIFFSOBERFLÄCHE SCHLIESSEN

Hacker sehen als erstes die externe Angriffsfläche ihrer Opfer. Um eine IT effizient zu verteidigen, müssen Sicherheitsverantwortliche diese Perspektive übernehmen. Notwendig ist eine Sicherheitsplattform, welche die verantwortlichen Teams schnell zu den exponierten Lücken führt.

Zur externen Angriffsfläche gehören sämtliche IT-Elemente mit Konnektivität an das Internet samt Schwachstellen. Für die Analyse und das Schließen dieser Flanken gegenüber Cyberangriffen kommt es auch darauf an, unbekannte, vergessene, abgelaufene und damit nicht verwaltete oder fehlkonfigurierte Assets zu identifizieren.

Die externe Angriffsoberfläche verwalten

Wichtig für die gezielte Abwehr ist das proaktive Identifizieren exponierter Elemente der IT. Denn Hacker spüren diese bei einer öffentlich verfügbaren Domain mit CT Logs und Public DNS Records einfach auf. Dazu benutzen sie frei verfügbare Tools zur Internet-Aufklärung.

Wer externe Angriffsoberflächen schließen will, muss sich daher denselben Überblick, den die Hacker haben, verschaffen und kontinuierlich exponierte Schnittstellen, Dienste und Schwachstellen entdecken sowie analysieren. Alle exponierten IP-Adressen, auslaufende oder abgelaufene Zertifikate, verwundbare öffentliche Dienste oder offene Ports sind vollständig durch einen Scan zu verzeichnen.

Assets und Artefakte

Was der Hacker sieht, muss die Abwehr in einer zentralen Ansicht einfach verwalten können. Ein zentrales Dashboard zeigt das Gesamtbild. Ebenso finden Anwender auch Name Server, die für Zone-Transfers verwundbar sind – die eine potenzielle Schwachstelle darstellen.

Darüber hinaus kommt es auf die Übersicht über die zu einem Asset gehörigen Artefakte an, mit den jeweiligen spezifischen Komponenten und Indikatoren. Sie liefern wichtige Informationen über Probleme, Schwachstellen sowie Fehlkonfigurationen und damit die entscheidenden Details, um die Exposition eines Assets zu bewerten. Zu Artefakten gehören Zertifikate, IP Blöcke, DNS Records und Dienste.

Schotten dicht

Die Abwehr muss sich schnell im Dashboard an die einzelnen Schauplätze bewegen können. Eine Verwaltung externer Angriffsoberflächen kann kontinuierlich alle exponierten Assets scannen, katalogisieren und die verknüpften Schwachstellen verzeichnen.

Eine External Attack Surface Management (EASM)-Lösung, die einen Dienst mit einer bekannten CVE identifiziert, kann also alle Ressourcen ansteuern, welche der bedrohte Dienst benutzt. Derart beweglich können IT-Abwehrteams ihr Patching und ihre Anstrengungen, Schäden zu minimieren, priorisieren. Ebenso kann eine mit einem Asset verknüpfte IP-Adresse oder eine E-Mail-Adresse, die im Verlauf eines Ereignisses markiert wird, über das Ereignis direkt angesteuert werden. Derart zielgenau vorzugehen, verkürzt die Analyse und die Eingrenzung des Vorfalls und damit die Aufenthaltsdauer der Hacker im Netz. Das verringert einen potenziellen Schaden.

Sich mit den Augen der Anderen sehen

Nur wer weiß, wie sich seine IT dem Hacker präsentiert, kann seine äußere Angriffsoberfläche schließen. Ihr Management ergänzt das herkömmliche Risikomanagement für Endpunkte um einen enorm wichtigen Beitrag. Unnötige oder riskante Expositionen ans Internet müssen gesehen und gezielt geschlossen werden, um die Eintrittstore für Angreifer zu reduzieren.

Grzegorz Nocoń

NUR WER WEISS, WIE SICH SEINE IT DEM HACKER PRÄSENTIERT, KANN SEINE ÄUSSERE ANGRIFFSOBERFLÄCHE SCHLIESSEN.

Grzegorz Nocoń,
Trusted Security Advisor, Bitdefender,
www.bitdefender.com

KI in der Cybersicherheit

UNTERSTÜTZUNG FÜR MICROSOFT 365

Microsoft 365 ist zentrale Plattform moderner Arbeitsumgebungen und zugleich ein häufiges Ziel von Cyberangriffen. Phishing-Mails, manipulierte Links in Teams und Fehlkonfigurationen führen regelmäßig zu Sicherheitsvorfällen.

KI-gestützte Assistenzsysteme ergänzen hier die Abwehr. Sie automatisieren die Analyse gemeldeter E-Mails, priorisieren Bedrohungen und liefern unmittelbar verständliches Feedback an Benutzer. Gleichzeitig prüfen sie URLs in Echtzeit, z. B. in Microsoft Teams, mittels Reputationsdatenbanken, heuristischer Analysen und Sandboxing, um potenzielle Gefahren frühzeitig zu erkennen.

Diese Lösungen nutzen trainierte Machine-Learning-Modelle, die kontinuierlich aus aktuellen Angriffsmustern lernen und Erkennungsraten verbessern. Sie sind nahtlos in Microsoft 365 integriert, arbeiten jedoch unabhängig von dessen nativer Infrastruktur, was zusätzliche Sicherheit bietet.

Ein Beispiel ist der AI Cyber Assistant von Hornetsecurity. Er kombiniert Bedrohungserkennung, Automatisierung und Benutzerinteraktion in einer Plattform. So werden Security-Teams nicht nur entlastet, sondern Anwender zugleich geschult. Dies stellt eine wichtige Ergänzung etablierter Schutzmechanismen dar.

Dadurch gewinnen IT-Security-Teams mehr Zeit für strategische Aufgaben, während Anwender direkt im Arbeitsalltag für Cybergefahren sensibilisiert werden.

www.hornetsecurity.com

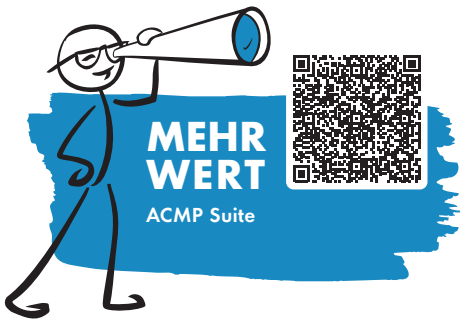
it-sa Expo&Congress
Besuchen Sie uns in **Halle 8-510**

Zentrale Schaltstelle für Sicherheit und Compliance

MIT HYBRIDEM UEM ZU UMFASSENDER SICHERHEIT

Cyberattacken werden immer häufiger und raffinierter. Deswegen müssen Unternehmen permanent ihre Sicherheitsstrategie konsolidieren und nachhaltig stärken. Ideale Basis dafür sind Unified Endpoint Management (UEM)-Systeme in hybrider Ausführung. Wie eine solche Verbindung aus klassischem Client-Management- und moderner Cloud-Integration aussieht, zeigt UEM-Spezialist Aagon auf der it-sa 2025 mit seinem neuen ACMP Intune Management. Messemotto: Ein System. Alle Endpunkte. Maximale Sicherheit. = Hybrides UEM

Sicherheitsrichtlinien kohärent über alle Endpunkte hinweg umsetzen, ohne Medienbrüche oder redundante Verwaltungsprozesse – das schafft insbesondere in heterogenen IT-Landschaften mehr Effizienz und Sicherheit. Genau dort ist es aber zugleich extrem anspruchsvoll. Denn die Verwaltung von Endgeräten in Unternehmen hat sich in den letzten Jahren stark weiterentwickelt; klassische Desktops stehen neben Notebooks und Smartphones, mobile Betriebssysteme sind zu verwalten.



Cloud und On-Premises kombiniert

Derart verteilte Infrastrukturen aus Homeoffice- und Inhouse-Arbeitsplätzen benötigen neue Formen der Administration. Hergebrachte On-Premises Client-Management-Systeme decken keine iOS- und Android-Geräte ab und genügen daher nicht mehr. Diese Geräte werden bislang oft mit cloud-basierten UEM-Systemen verwaltet, von denen Microsoft Intune das bekannteste und gebräuchlichste ist.

Die Cloud bietet Skalierbarkeit und Mobilität, während Inhouse-Systeme ihre Stärken bei der Sicherheit und Kontrolle ausspielen. Beides kombiniert Aagon in seiner ACMP Suite mit einem neuen Intune Management, also einer Integration von Intune in das eigene UEM. Ergebnis ist eine zentrale Plattform, über die sich einheitlich sowohl klassische Windows-Clients im lokalen Netzwerk administrieren lassen als auch moderne, cloud-verwaltete Endgeräte. Hybrid bedeutet hier: volle Kontrolle, unabhängig vom Standort oder Verwaltungsmodell des Endpunkts.

Speziell hinsichtlich der Sicherheit haben rein cloud-basierte Lösungen erhebliche Nachteile gegenüber einem lokal installierten UEM-System. Es geht damit los, dass Admins insgesamt nur eine Teilansicht ihrer IT-Infrastruktur erhalten und Risiken daher leichter übersehen. Für die Verwaltung von Servern braucht es wiederum Zusatzlösungen. Funktionale Einschränkungen finden sich außerdem bei der Administration von SNMP-Geräten sowie einer detaillierten Inventarisierung.

Defender und BitLocker über das UEM steuern

Ein vollwertiges UEM demgegenüber verfügt über eigene Agenten und bietet größere Vielfalt durch manuelle Clients, Agents oder ein zusätzliches Gateway. Es beinhaltet Funktionen wie Remote Control, Lizenzmanagement, Asset Management oder Windows Update Management für Clients und Server und

Microsoft365, an die bei Intune gar nicht zu denken ist. Sogar Microsoft-Lösungen wie Defender und BitLocker lassen sich direkt darüber steuern – auch ohne Cloud-Anbindung.

Weil sich die Daten in der eigenen Umgebung befinden, sind sie sehr gut geschützt; das Unternehmen ist außerdem unabhängig vom Internet und Status des Servers in der Cloud. Weitere Vorteile eines lokalen Systems: Sicherheitsbereiche lassen sich gut voneinander abgrenzen und individuelle Lösungen mit No-Code/Low-Code einrichten.

Frühwarnsystem für IT-Schwachstellen

Bei Aagon arbeitet das Modul „Security Detective" mit einem weiteren Modul „Schwachstellenmanagement" zusammen und sammelt alle wichtigen Informationen über die lokale Konfiguration jedes Windows-Client-Rechners im Netzwerk – unter anderem den Zustand von Virenschutz, Spyware-Schutz, Firewall sowie den Status aller privaten und öffentlichen Netzwerke. So erkennt es sicherheitsrelevante Konfigurationsabweichungen auf Endgeräten rechtzeitig und meldet potenzielle Risiken automatisiert. Die Administrationsabteilung hat jederzeit den Überblick über alle Einstellungen und Parameter des Windows Security Centers – ein Frühwarnsystem für IT-Schwachstellen. Relevante Sicherheitsinformationen stehen in einer zentralen Datenbank zur Verfügung.

Kernelement jeder UEM-Plattform ist das Patch Management. Es sorgt für eine zeitnahe und automatisierte Verteilung von Updates für Windows und Drittanbieter-Software. Updates sind sicherheitskritisch, weswegen Patch Management von zentraler Wichtigkeit für die IT-Security ist. Quasi täglich erscheinen heute neue Updates, Patches und Aktualisierungen, die Sicherheitslücken schließen und Funktionen verbessern. Doch wer kennt schon den Patch-Status jedes einzelnen Rechners im Netzwerk? Wer das Thema Updates den Usern überlässt, müsste ihnen zum einen lokale Admin-Rechte vergeben und zusätzlich darauf vertrauen, dass diese alle Updates selbstständig bemerken und auch immer zeitnah installieren – das ist illusorisch. Kritische Sicherheitslücken, Kompatibilitätsprobleme zwischen Programmversionen und hoher Arbeitsaufwand für den Support wären die Folge.

Inventarisierung als Basis

Ein umfängliches Inventory & Asset Management schließlich liefert vollständige Transparenz über Hard- und Software. Es stellt daher eine weitere essenzielle Grundlage für jede Sicherheitsstrategie dar. Auch zu diesem Bereich zeigt UEM-Hersteller Aagon auf der it-sa 2025, wie er dieses Thema angeht. Zur netzwerkweiten Inventarisierung pusht oder verteilt das UEM einen kleinen Software-Agenten auf jeden Client. Die Client Software hält die Kommunikation zwischen dem lokalen Computer und dem UEM-Server aufrecht, liefert in frei definierbaren Intervallen Inventardaten an ihn und nimmt in der anderen Richtung Aufträge entgegen. Bereits nach wenigen Augenblicken stehen über 150 Hardware-Daten und sämtliche Details der Windows-Installation auf dem Server zur Verfügung. Bei installiertem Client oder Ausführen des OneScan-Clients werden mehrere tausend Daten, zum Beispiel mithilfe eines Hyper-V Scanners, ausgelesen.

Die Inventarisierung gehört bei Aagon zum Basismodul ACMP Core, das die Grundlage ist für Nutzung und Ineinandergreifen der weiteren Module wie Desktop Automation (Client Management), Lizenzmanagement, Security Detective oder Helpdesk (Ticket Management). Alle Funktionsmodule müssen auf die Inventarisierung zugreifen, die damit den Grundstein für ein erfolgreiches Endpoint Management darstellt.

UNTERNEHMEN BRAUCHEN HEUTE UMFASSENDE LÖSUNGEN, UM DIE STETIG STEIGENDEN ANFORDERUNGEN AUS NIS-2, BSI IT-GRUNDSCHUTZ ODER KRITIS-DACHGESETZ WEITERHIN GUT ZU BEWÄLTIGEN.

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

Intune-Portale zusammenfassen

Durch eine enge Verzahnung einzelner Funktionsbausteine untereinander sowie zusätzlich mit Microsoft Intune wird das UEM zur zentralen Schaltstelle für IT-Sicherheit und Compliance. Denn gegenüber der alleinigen Geräteverwaltung mit Intune ermöglicht es eine umfassendere IT-Automatisierung. Skripte zur Fehlerbehebung oder Software-Rollouts lassen sich zentral steuern, ohne dass jemand manuell eingreifen muss. Auch mehrere Intune-Portale können in der ACMP Suite zusammengefasst werden. Unternehmen brauchen heute solche umfassenden Lösungen, um die stetig steigenden Anforderungen aus NIS2, BSI IT-Grundschutz oder KRITIS-Dachgesetz weiterhin gut zu bewältigen.

Sebastian Weber

Digitale Identitäten im Finanzwesen

RISIKOQUELLE ODER SICHERHEITSANKER?

Die digitale Transformation hat die Bedeutung von Identitäten im Finanzwesen verändert. Kunden, Mitarbeitende und Partner agieren zunehmend digital, wodurch Identitätsdaten nicht nur Zugang ermöglichen, sondern auch eine wachsende Angriffsfläche darstellen.

Studien zeigen, dass 80 Prozent der Finanzdienstleister bereits Sicherheitsvorfälle im Zusammenhang mit unzureichender Authentifizierung erlebt haben. Dabei entstanden durchschnittliche Schäden von rund zwei Millionen US-Dollar pro Fall. Besonders betroffen sind Kundenkonten. Allein 2024 stieg die Zahl erfolgreicher Kontoübernahmen (Account Takeover) um 354 Prozent. Veraltete Authentifzierungsverfahren, wiederverwendete Passwörter und mangelnde Verifikation bieten dabei Einfallstore. Auch interne Identitäten geraten zunehmend in den Fokus. Auch externe Partner stellen ein Risiko dar, wenn sie dauerhaft gültige oder weitreichende Berechtigungen erhalten.

DIGITALE IDENTITÄTEN SIND FÜR FINANZINSTITUTE EIN STRATEGISCHER SICHERHEITSANKER, NICHT NUR EIN TECHNISCHER ZUGANGSMECHANISMUS.

Adam Preis, Director Product/ Solution Marketing, Ping Identity, www.pingidentity.com

Integrierter Ansatz

Ein zukunftsfähiger Schutzansatz für digitale Identitäten muss drei zentrale Gruppen berücksichtigen: Kunden, Mitarbeitende und B2B-Partner. Trotz unterschiedlicher Anforderungen lassen sich gemeinsame Grundsätze ableiten:

➤ **Threat Detection & Response:** Echtzeitüberwachung und Verhaltensanalysen sind die Basis für die Erkennung verdächtiger Aktivitäten, wie ungewöhnliche Transaktionsmuster oder Login-Versuche aus risikobehafteten Regionen.

➤ **Adaptive Multi-Faktor-Authentifizierung (MFA):** Anstelle von generischen MFA-Anforderungen sollten Authentifizierungsmaßnahmen situativ und risikoorientiert erfolgen z.B. bei abweichenden Geräten oder Transaktionen über einem bestimmten Schwellenwert.

➤ **Identitätsprüfung mit Biometrie:** Biometrische Liveness-Prüfungen sind ein Mittel, um kritische Prozesse gegen KI-basierte Identitätsfälschungen zu sichern.

➤ **Dynamische Autorisierung:** Rollenbasierte Zugriffskontrollen reichen nicht mehr aus. Stattdessen müssen Entscheidungen künftig kontextabhängig getroffen werden, beispielsweise basierend auf Standort, Uhrzeit oder Gerätezustand.

➤ **Identity Governance und Administration (IGA):** Automatisierte Prozesse zur Vergabe, Überwachung und Entziehung von Zugriffsrechten schaffen Transparenz und unterstützen regulatorische Anforderungen.

IAM-Konvergenz als Schlüssel

Derzeit setzen viele Finanzinstitute auf getrennte IAM-Systeme für Kunden, Mitarbeitende und Partner. Das Resultat sind Silostrukturen, doppelte Wartung, inkonsistente Richtlinien und eine fragmentierte Risikobewertung. Moderne Architekturen verfolgen deshalb eine konvergente Herangehensweise. Alle Arten von Identitäten werden von Identitätsplattformen zentral verwaltet, orchestriert und gesichert. Der Vorteil: Weniger Kosten, vollständige Kontrolle und lückenlose Auditierbarkeit.

Identitätsmanagement als Zukunftssicherung

Digitale Identitäten sind für Finanzinstitute ein strategischer Sicherheitsanker, nicht nur ein technischer Zugangsmechanismus. Das erfordert einen Paradigmenwechsel: Weg von Insellösungen, hin zu einer ganzheitlichen, risikobasierten Identity-Security-Strategie. Angesichts wachsender KI-Bedrohungen und regulatorischer Anforderungen wird verlässlicher Identitätsschutz zur Basis digitaler Resilienz im Finanzsektor.

Adam Preis

SASE aus Europa für Europa

VOM RISIKO ZUM WETTBEWERBSVORTEIL

Datenschutz, Cyberresilienz und Compliance sind für europäische Unternehmen längst strategische Imperative. Durch EU-Regulierungen wie NIS2, Cyber Resilience Act und DORA sowie globale Standards wie IEC 62443 steigt der Druck, die gesamte IT-Infrastruktur und -Architektur, inklusive Lieferanten, nicht nur leistungsfähig, sondern auch auditierbar, kontrollierbar und regelkonform zu gestalten.

it-sa Expo&Congress
Besuchen Sie uns in **Halle 6-320**

Die Wahl eines passenden SASE-Anbieters wird damit eine Frage der regulatorischen Sicherheit und wirkt sich auf die Anbieterwahl aus, sagen 72 Prozent der Führungskräfte, wie eine aktuelle Studie zeigt.

Den Spagat erfolgreich meistern

Unternehmen brauchen Partner, die nicht nur technologische Exzellenz bieten, sondern die europäische Regulierungslandschaft verstehen, zur eigenen Maxime machen und damit die eigene Compliance im Griff haben und darüber hinaus durch ihre Lösungen und Services bei der Einhaltung nachweislich unterstützen.

Open Systems mit Sitz in der Schweiz erfüllt genau diese Anforderungen: Der erfahrene Managed-SASE-Anbieter verbindet seit über 35 Jahren Cybersicherheit und Netzwerkkonnektivität auf einer in Europa entwickelten, hochsicheren Cloud-Plattform. Diese integriert Zero Trust Network Access, Secure Web Gateway, Cloud Access Security Broker und Firewall-as-a-Service zu einer holistischen Lösung. Das Ergebnis: ein hochsicheres, skalierbares Netzwerk mit Rund-um-die-Uhr-Support durch zertifizierte Security Engineers – inklusive Monitoring, Protokollierung und feingranularer Zugriffskontrolle. So wird Compliance vom Risiko zum Wettbewerbsvorteil. Mit Open Systems gelingt der Spagat zwischen regulatorischer Sicherheit und technischer Zukunftsfähigkeit – auch in kleinen Teams.

www.open-systems.com/de/

opensystems
Cybersecurity-Spezialistin von Swiss Post

RANSOMWARE

SCHADSOFTWARE MIT KI ENTDECKT

Sicherheitsexperten von ESET haben eine neue Schadsoftware entdeckt, die Künstliche Intelligenz erstmals gezielt für Ransomware nutzt. Das Programm mit dem Namen PromptLock verwendet ein lokal installiertes KI-Sprachmodell, um im laufenden Angriff automatisch Skripte zu erzeugen. Genau das macht es so besonders. Die KI entscheidet selbst, welche Dateien durchsucht, kopiert oder verschlüsselt werden. Für IT-Sicherheitsforscher ist PromptLock ein deutliches Warnsignal.

Die Software generiert sogenannte Lua-Skripte, die plattformübergreifend auf Windows, Linux und macOS funktionieren. Je nach System durchsucht PromptLock lokale Dateien, analysiert sie und entscheidet anhand vorher festgelegter Textbefehle, ob Daten verschlüsselt oder ausgespäht werden. Eine Funktion zur Zerstörung von Dateien ist offenbar bereits vorbereitet, aber noch nicht aktiv.

Ein Vorgeschmack auf das, was noch kommen könnte

Für die Verschlüsselung verwendet PromptLock den SPECK-Algorithmus mit 128 Bit. Geschrieben wurde die Schadsoftware in der Programmiersprache Golang. Erste Varianten sind auf der Analyseplattform VirusTotal aufgetaucht. Zwar geht ESET derzeit davon aus, dass es sich um ein Proof-of-Concept handelt, doch die Gefahr sei real.

Die Software nutzt laut ESET ein frei verfügbares Sprachmodell, das lokal über eine API angesteuert wird. Die KI erstellt die Angriffsskripte also direkt auf dem infizierten Rechner – ohne Verbindung zur Cloud. Selbst die Bitcoin-Adresse für die Erpressung ist im Prompt eingebaut. Sie führt kurioserweise zu einem Wallet, das scheinbar dem Bitcoin-Erfinder Satoshi Nakamoto gehört.

www.eset.de

Intelligente Datenklassifizierung

SENSIBLE DATEN IN KOMPLEXEN IT-UMGEBUNGEN SICHTBAR UND SCHÜTZBAR MACHEN

Unternehmen können nur schützen, was sie kennen. Aber wo liegen die sensiblen Daten, die keinesfalls in falsche Hände geraten dürfen, und über welche Kanäle werden sie geteilt? Data Discovery und Datenklassifizierung liefern diese Informationen – sind bei den riesigen Datenmengen aber kaum noch manuell möglich. KI ist der entscheidende Helfer.

Eine der wichtigsten Aufgaben von Security-Teams ist es, die sensiblen Daten eines Unternehmens zuverlässig zu schützen. Das können personenbezogene Daten sein, die nicht auf Servern außerhalb der EU landen dürfen, interne Dokumente, die nur über freigegebene Cloud-Services ausgetauscht werden sollen, oder geistiges Eigentum wie Quellcode und Konstruktionsdaten, das ein Unternehmen keinesfalls verlassen darf – egal, auf welchem Wege.

Die große Herausforderung: Daten wachsen rasant und sind über Geräte, Server und Clouds verteilt – ihre Wege lassen sich kaum noch nachvollziehen. Selbst eine Kundenliste auf einem geschützten Server ist nicht automatisch sicher. Sie kann heruntergeladen, kopiert oder über verschiedene Kanäle weitergegeben werden.

Schulungen allein reichen nicht

Sensible Informationen verschwinden oft in Dark Data – Daten, die für Unternehmen unsichtbar bleiben und bis zu 80 Prozent des Datenbestandes ausmachen. Schulungen schärfen zwar das Bewusstsein, verhindern aber menschliche Fehler nicht. Zudem können die Daten auch über ein Datenleck abfließen – Unternehmen benötigen daher unbedingt technische Lösungen, um Richtlinien zum Schutz ihrer Daten durchsetzen zu können. Der Schlüssel dafür sind eine lückenlose Data Discovery und eine genaue Datenklassifizierung, denn erst wenn alle Daten korrekt erfasst und kategorisiert wurden, sind Sicherheitslösungen tatsächlich in der Lage, die Richtlinien auf alle Daten und Kanäle, über die sie fließen, anzuwenden.

Ein Überblick über den Datenbestand

Die Data Discovery spürt Daten über alle Speicherorte hinweg auf, erstellt einen Katalog und zeigt, wer auf welche Daten zugreifen kann. Dies hilft, Datenrisiken einzuschätzen und übermäßige Berechtigungen zu entziehen – ein wichtiger Schritt bei der Umsetzung von Zero Trust. Schließlich stellt eine Rechtevergabe nach dem Least-Privilege-Prinzip sicher, dass Mitarbeiter nur exakt die Berechtigungen erhalten, die sie für ihre Tätigkeiten benötigen.

Darüber hinaus werden durch die Data Discovery auch redundante, veraltete und überflüssige Daten sichtbar, die unnötig Speicherplatz belegen und die Storage-Kosten nach oben treiben.

Automatische Klassifizierung mit KI

Erst der umfassende Überblick über den Datenbestand erlaubt es, alle Daten zuverlässig zu klassifizieren. In der Vergangenheit war das eine äußerst aufwendige Aufgabe, weil Daten manuell verschiedenen Kategorien zugeordnet werden mussten, doch inzwischen lässt sich der Vorgang mit KI weitgehend automatisieren. Dabei spielen je nach eingesetzter Lösung ganz unterschiedliche KI-Techniken zusammen – zusätzlich zu klassischen Regeln und Regular Expressions, die Inhalte filtern und damit die Klassifizierung effizienter machen.

Da wären vor allem Small Language Models (SLM), die wie Large Language Models (LLM) natürliche Sprache verarbeiten und die Inhalte von Dateien, Mails, Websites und Chats verstehen. SLMs besitzen anders als LLMs kein breites Allgemeinwissen, sondern sind hochspezialisiert – in diesem Fall auf Datenklassifizierungen. Dadurch liefern sie bessere Ergebnisse, haben nur einen Bruchteil der Größe von LLMs und sind viel ressourcenschonender.

Hinzu kommen sogenannte „Bag of Words"-Modelle, die die Häufigkeit von Wörtern in Dateien untersuchen, was bei der thematischen Einordnung hilft und die Genauigkeit der Klassifizierung verbessert. Deep Neuronal Network Classifiers helfen bei der qualitativen Bewertung der Inhalte und es kommen auch statistische Verfahren aus dem Bereich des Machine Learnings zum Einsatz, etwa Bayessches Lernen, die Vorhersagen treffen und die Klassifizierungsergebnisse verfeinern.

Richtlinien passend zum Risiko

All diese Klassifizierungsmechanismen sorgen dafür, dass der Datenbestand korrekt klassifiziert wird – und beispielsweise eine Produktnummer nicht mit einer Sozialversicherungsnummer verwechselt wird. Den einzelnen Daten-

Data Discovery und Datenklassifizierung machen sensible Daten sichtbar, die sich in dem riesigen Berg an Dark Data verstecken, den die meisten Unternehmen angesammelt haben

(Quelle: Forcepoint)

mustern werden jeweils Kategorien und Unterkategorien zugewiesen und sie erhalten Tags, sodass Security-Teams sehr detaillierte Richtlinien erstellen können. Idealerweise bietet die eingesetzte Sicherheitslösung dabei mehr Möglichkeiten als „Erlauben" und „Blockieren", damit Unternehmen abgestuft auf leichte und schwere Sicherheitsverletzungen reagieren können. Beim Speichern einer Präsentation mit Finanzdaten genügt meist ein automatisches Aktivieren der Verschlüsselung.

In der Anfangsphase sollten Unternehmen die Richtlinien zudem nur für hochkritische Aktivitäten wie den Versand von Kundendaten an Empfänger außerhalb des Unternehmens oder den massenhaften Upload von Daten zu verdächtigen Zielen im Internet tatsächlich durchsetzen. Für andere Aktivitäten reicht ein Monitoring zunächst aus, um die Datenbewegungen im Unternehmen besser zu verstehen und die Auswirkungen der Richtlinien zu überprüfen. Möglicherweise zu strikte Richtlinien lassen sich dann noch anpassen, sodass sie Mitarbeiter nicht bei der Arbeit behindern.

Klassifizierung verfeinern

Eine gute Datenklassifizierung kommt ohne KI-optimierte Hardware aus und braucht auch auf Standardsystemen nur wenige Millisekunden für ihre Entscheidungen. Security-Teams können diese noch verbessern, indem sie korrekte Klassifizierungen bestätigen und falsch klassifizierte Daten mit zusätzlichen Informationen den Klassifizierungsprozess erneut durchlaufen lassen.

Unterstützt die eingesetzte Datensicherheitslösung dann noch ein sogenanntes Fingerprinting, lassen sich die wertvollsten Daten eines Unternehmens besonders einfach schützen. Fachbereiche stellen in diesem Fall ihre wichtigsten Dokumente wie Verträge, Personaldaten, Finanzinformationen oder Konstruktionszeichnungen bereit, damit Fingerabdrücke der Daten erstellt werden können, anhand derer sie an anderer Stelle wiedererkannt werden – etwa an neuen Speicherorten, beim Versenden via E-Mail oder beim Teilen mit einem KI-Tool. Selbst wenn nur ein Teil der Originaldokumente dort auftaucht oder sich ihre Inhalte in einem Screenshot verstecken, werden sie zuverlässig identifiziert und die entsprechenden Richtlinien aktiviert.

Um langfristig ein hohes Datensicherheitsniveau zu erreichen, dürfen Unternehmen die Data Discovery und Datenklassifizierung allerdings nicht als einmalige Aufgabe betrachten. Schließlich werden bestehende Daten kontinuierlich bearbeitet, kopiert und verschoben, und es kommen stetig neue Daten hin. Es handelt sich vielmehr um eine dauerhafte Aufgabe, weshalb Unternehmen auch eine Lösung auswählen sollten, bei der für die Discovery-Scans keine separaten Gebühren anfallen. Ansonsten können die regelmäßigen Scans zu einem großen Kostenfaktor werden und empfindliche Löcher ins Security-Budget reißen.

Fabian Glöser
www.forcepoint.com

Sicherheit und Resilienz in der IT

WORAUF ES WIRKLICH ANKOMMT

Cyberangriffe sind in Deutschland mittlerweile Alltag. Unternehmen jeder Größe sehen sich wachsenden Bedrohungen ausgesetzt – von gezielten Attacken bis hin zu groß angelegten Phishing-Kampagnen. Neben dem Risiko von Datenverlust oder finanziellen Schäden steht immer auch die Verfügbarkeit der Geschäftsprozesse auf dem Spiel. Sicherheit und Resilienz sind deshalb zwei Seiten derselben Medaille.

Lange lag der Fokus auf Schutzmaßnahmen wie Firewalls, Virenscannern oder Zero-Trust-Architekturen. Doch selbst die beste Verteidigung kann nicht alle Angriffe verhindern. Wichtig ist daher auch eine Antwort auf die Frage, wie Unternehmen auf Vorfälle reagieren und sich davon erholen.

Resilienz bedeutet, Störungen abzufangen, Schäden zu begrenzen und den Geschäftsbetrieb schnell wieder aufzunehmen. Dazu gehören technische Fähigkeiten wie die automatische Wiederherstellung von Daten, aber auch klare Verantwortlichkeiten, regelmäßige Notfallübungen und Krisenkommunikation.

Ein ganzheitlicher Ansatz umfasst vier Handlungsfelder:

#1 **Analyse und Vorsorge:** Bedrohungen einschätzen, Schwachstellen erkennen, Compliance sichern.

#2 **Zero Trust:** Schutz geschäftskritischer Daten und Anwendungen.

#3 **Erkennung und Reaktion:** kontinuierliche Überwachung und schnelle Reaktion.

#4 **Wiederherstellung:** automatisierte Wiederherstellung von Prozessen und Daten.

Für mehr Sicherheit und Resilienz braucht es einen integrierten Ansatz, der Technik, Prozesse und Menschen verbindet. Entscheidend ist, Sicherheit als kontinuierlichen Prozess zu begreifen. Nur so bleiben Unternehmen flexibel und widerstandsfähig.

www.kyndryl.de

Cybersicherheit mit Wazuh – Bedrohungen mit Open-Source-Software erkennen, analysieren und abwehren; Frank Neugebauer; Carl Hanser Verlag GmbH & Co.KG; 08-2025

CYBERSICHERHEIT MIT WAZUH

BEDROHUNGEN MIT OPEN-SOURCE-SOFTWARE ERKENNEN, ANALYSIEREN UND ABWEHREN

Die Open-Source-Sicherheitsplattform Wazuh kombiniert verschiedene Sicherheitsfunktionen wie Intrusion-Detection-Systeme (IDS), File Integrity Monitoring (FIM) und Vulnerability Management in einer einzigen Umgebung. Damit lassen sich bösartige Aktivitäten frühzeitig erkennen, Systeme auf unautorisierte Änderungen überprüfen und potenzielle Schwachstellen identifizieren.

Nach einer Einführung in die grundlegenden Konzepte und Fachbegriffe werden Sie Schritt für Schritt durch die praktische Anwendung von Wazuh und den Aufbau einer Testumgebung geführt. Sie bauen im Laufe des Buches ein kleines Netzwerk aus virtuellen Maschinen auf, das sowohl Wazuh als auch verschiedene Betriebssysteme enthält. In dieser Testumgebung konfigurieren und verwenden Sie Wazuh in einem realistischen Szenario, um den vollen Funktionsumfang der Plattform kennenzulernen. Dabei erstellen Sie Ihre eigenen Abfragen, Decoder und Regeln.

Zahlreiche Use Cases veranschaulichen darüber hinaus typische Bedrohungsszenarien, die Sie mit Wazuh erkennen und beheben können.

Sichere mobile Kommunikation

ZERTIFIZIERTE HARDWARE-ANKER FÜR DEN SCHUTZ SENSIBLER DATEN

Mobiles Arbeiten ist heute fester Bestandteil des Berufsalltags – in Unternehmen ebenso wie in Behörden und in Bereichen, in denen mit sensiblen Informationen umgegangen wird. Doch je mehr mobile Geräte im Einsatz sind, desto größer wird die Angriffsfläche für Cyberkriminelle. Für Organisationen, die auf reibungslose Abläufe und den Schutz vertraulicher Daten angewiesen sind, stellt sich daher die Frage: Wie lässt sich Sicherheit gewährleisten, ohne Flexibilität und Effizienz einzuschränken?

Samsung hat darauf eine klare Antwort: **Knox Native.** Entwickelt in enger Zusammenarbeit mit dem Bundesamt für Sicherheit in der Informationstechnik (BSI) bietet diese Lösung einen zertifizierten Hardware-Anker[1] direkt im Gerät. Das embedded Secure Element (eSE) ist nach Common Criteria EAL 6+ zertifiziert und für die Verarbeitung von Verschlusssachen des Geheimhaltungsgrades „VS – Nur für den Dienstgebrauch" geeignet. Damit können vertrauliche Informationen direkt auf dem Smartphone oder Tablet geschützt werden – ohne zusätzliche Hardware oder komplizierte Zusatzlösungen.

Vollwertiger Smartcard-Ersatz

Der Mehrwert geht jedoch über reine Datensicherheit hinaus. Knox Native verwandelt ausgewählte Samsung Galaxy Geräte auf Wunsch in einen vollwertigen Smartcard-Ersatz. So können sie nicht nur für die geschützte Kommunikation, sondern auch für den Zugang zu Gebäuden, die Bezahlung in der Kantine oder die Freigabe von Druckaufträgen genutzt werden. Das kann Zeit sparen, Administrationsaufwände reduzieren und Alltagsprozesse für Mitarbeitende komfortabel machen.

Damit die Geräteflotte jederzeit sicher und einsatzbereit bleibt, lässt sich Knox Native nahtlos mit der **Knox Suite** verbinden. Diese Plattform bündelt zentrale Werkzeuge für Einrichtung, Verwaltung, Sicherheitsrichtlinien und Update-Management. IT-Teams können so Geräte zentral steuern, Sicherheitsstandards einheitlich umsetzen und neue Anwendungen unkompliziert ausrollen – auch in großen oder heterogenen Umgebungen.

Zertifiziert für mehr Vertrauen

Seit Sommer 2025 tragen ausgewählte Samsung Geräte zudem das offizielle **IT-Sicherheitskennzeichen** des BSI. Dieses Label steht dafür, dass Hersteller ihre Produkte nach vom BSI anerkannten Sicherheitsstandards geprüft haben[2] und bietet Unternehmen wie Anwender*innen ein hohes Maß an Transparenz und Vertrauen.

Wer erfahren möchte, wie sich mobile Endgeräte sicher in bestehende IT- und Digitalisierungsstrategien einbinden lassen, kann dies live auf der it-sa erleben. **Besuchen Sie Samsung in Halle 9-509** und sprechen Sie mit den Expertinnen und Experten über Ihre individuellen Anforderungen.

https://www.samsung.com/de/business/

it-sa Expo&Congress
Besuchen Sie uns in **Halle 9-509**

SAMSUNG

[1] Weitere Informationen zur Zertifizierung: https://www.samsung.com/de/business/mobile-solutions/samsung-knox-native/

[2] Weitere Informationen in der Pressemeldung zum Thema: https://news.samsung.com/de/transparente-it-sicherheit-fur-user-samsung-gerate-jetzt-mit-it-sicherheitskennzeichen-des-bsi

GenAI-Sicherheit

MIT HILFE VON KI-TOOLS AB DURCH DIE HINTERTÜR

Die rasante Verbreitung generativer KI-Tools bringt neue Sicherheitsrisiken mit sich, die klassische Schutzmaßnahmen zunehmend umgehen. Neben den bekannten OWASP Top 10 für LLMs rücken zusätzliche, bislang weniger beachtete Gefahren in den Vordergrund, insbesondere im Zusammenspiel mit modernen Browser-Technologien und multimodalen Systemen.

Eine der kritischen Schwachstellen, die praktisch alle browserbasierten GenAI-Tools betrifft und über einen bisher übersehenen Angriffsvektor funktioniert: sind Browser-Erweiterungen.

Man-in-the-Prompt-Angriffe

Die als „Man-in-the-Prompt" bezeichnete Angriffsmethode nutzt die Implementierung moderner GenAI-Tools aus. Die Forscher von LayerX haben eine neue Exploit-Klasse entdeckt, die diese Tools direkt über einen bisher übersehenen Angriffsvektor angreift: Das bedeutet, dass praktisch jeder Benutzer oder jede Organisation, die Browsererweiterungen in ihren Browsern installiert haben, potenziell betroffen sind.

Der Angriff funktioniert, weil die Eingabefelder von KI-Tools typischerweise Teil des Document Object Model (DOM) der Webseite sind. Dadurch können Browser-Erweiterungen mit entsprechenden Skript-Berechtigungen direkt auf die Eingabeaufforderungen zugreifen, diese manipulieren oder komplett ersetzen. Das Perfide dabei: Es werden keine besonderen Berechtigungen benötigt, da viele Erweiterungen bereits standardmäßig auf DOM-Elemente zugreifen können.

Die globale Reichweite macht Man-in-the-Prompt-Angriffe besonders gefährlich. Die Tragweite des Problems wird durch die enormen Nutzerzahlen der betroffenen Plattformen deutlich. Die Sicherheitslücke betrifft alle führenden GenAI-Tools, die über den Browser zugänglich sind (vgl. Bild 1).

Zusätzlich sind alle intern entwickelten LLM-Tools betroffen, die über Webbrowser bereitgestellt werden. Die Analyse ergab, dass 88 Prozent der Teilnehmer in der „Prompt Injection Challenge" erfolgreich einen GenAI-Bot dazu brachten, sensible Informationen preiszugeben.

ChatGPT als Hacker-Copilot missbraucht

In einem Proof-of-Concept demonstrierten Forscher von LayerX, wie eine kompromittierte Browser-Erweiterung ohne spezielle Berechtigungen ChatGPT für bösartige Zwecke einsetzen kann.

Der Angriff läuft dabei vollständig im Hintergrund ab: Eine bösartige Erweiterung öffnet unbemerkt eine ChatGPT-Registerkarte, injiziert manipulierte Prompts, extrahiert die Antworten und leitet diese an externe Server weiter. Anschließend löscht sie den gesamten Chat-Verlauf, um ihre Spuren zu verwischen. Nutzer bemerken von diesem Vorgang nichts, da alles automatisiert im Hintergrund geschieht.

Bild 1 | KI-Bedrohungen: Angriffsvektoren und Risiken

Bedrohungsklasse	Beispiele	Betroffene Systeme	Kritikalität
OWASP Top 10 Basis	Prompt Injection, Output Handling	Alle LLM-Systeme	Sehr hoch
Browser-basierte Angriffe	Man-in-the-Prompt, DOM-Manipulation	Web-basierte KI-Tools	Sehr hoch
Erweiterte Bedrohungen	Data Drift, Shadow AI	Interne/Fine-tuned LLMs	Hoch
Multimodale Angriffe	Context Leakage, Deepfakes	Bild/Audio-KI-Systeme	Hoch
Supply Chain	Kompromittierte Plugins, Models	Alle KI-Implementierungen	Mittel-Hoch

Google Workspace besonders gefährdet

Noch kritischer wird die Situation bei Google Gemini mit Workspace-Integration. Hier können Angreifer über manipulierte Browser-Erweiterungen auf alle Daten zugreifen, für die der Nutzer Leseberechtigungen besitzt. Dazu gehören E-Mails, Dokumente, Kontakte, freigegebene Ordner und Meeting-Protokolle.

Der Nutzer erhält möglicherweise eine KI-Antwort mit einer URL, die zum Verlust von Informationen führt. Sobald der User auf den Link klickt, werden die Informationen an einen entfernten Angreifer gesendet. Diese Angriffsmethode ist besonders heimtückisch, da sie die vertrauensvolle Beziehung zwischen Nutzer und KI-System ausnutzt.

Interne LLMs im Visier der Cyberkriminellen

Während kommerzielle GenAI-Tools bereits hohes Risikopotenzial bergen, stellen unternehmensinterne LLM-Implementierungen die eigentlichen Hochwertziele dar. Diese Systeme werden häufig mit vertraulichen Unternehmensdaten trainiert oder verfügen über Zugriff auf sensitive Informationen wie Quellcode, Rechtsdokumente, Finanzprognosen oder M&A-Strategien.

Das Problem verschärft sich dadurch, dass interne GenAI-Tools oft mit höherem Vertrauen entwickelt werden und weniger Sicherheitsvorkehrungen gegen feindliche Eingaben implementiert haben. Eine der Hauptsorgen bei LLMs ist die Prompt-Injection, eine Variation von Anwendungssicherheits-Injection-Cyberangriffen, bei denen Angreifer bösartige Anweisungen in anfällige Anwen dungen einschleusen.

Traditionelle Security-Tools versagen

Herkömmliche Unternehmenssicherheitslösungen wie Data Loss Prevention (DLP), Secure Web Gateways oder Cloud Access Security Broker (CASB) können diese Art von Angriffen nicht erkennen. Sie haben keinen Einblick in DOM-Manipulationen auf Browser-Ebene und können weder Prompt-Injections noch unbefugten Datenzugriff durch manipulierte Eingabeaufforderungen identifizieren.

Schutzmaßnahmen für Unternehmen

Organisationen sollten ihren Fokus von anwendungsbasierten Kontrollen auf die Überwachung des Browser-Verhaltens verlagern. Effektive Gegenmaßnahmen umfassen die kontinuierliche Überwachung von DOM-Interaktionen innerhalb von GenAI-Tools und die Erkennung von Event-Listenern oder Webhooks, die mit KI-Eingabeaufforderungen interagieren können.

Das Blockieren riskanter Browser-Erweiterungen basierend auf Verhaltensrisiken statt nur auf Berechtigungslisten ist essentiell. Da statische Bewertungen aufgrund fehlender spezieller Berechtigungen versagen, müssen Unternehmen auf dynamisches Extension-Sandboxing und Publisher-Reputation setzen.

Zusätzlich sollten Organisationen die Manipulation und Exfiltration von Daten in Echtzeit auf Browser-Ebene verhindern. Dies erfordert neue Sicherheitslösungen, die speziell für die Herausforderungen des GenAI-Zeitalters entwickelt wurden.

Erweiterte Bedrohungslandschaft jenseits der OWASP Top 10

Während die OWASP Top 10 für LLMs bereits ein umfassendes Risikospektrum abdecken, zeigen aktuelle Entwicklungen weitere kritische Gefährdungen auf, die Unternehmen berücksichtigen müssen. Dazu zählen:

Data Drift und exploitables Modellverhalten entsteht durch kontinuierliches Fine-Tuning, das LLMs unvorhersehbar verändert. Neue Systemreaktionen können etablierte Sicherheitsfilter umgehen und bisher unbekannte Schwachstellen schaffen.

Shadow AI im Unternehmen beschreibt den unkontrollierten Einsatz externer KI-Tools durch Mitarbeiter. Diese Schatten-IT führt zu ungesicherten Datenabflüssen, da Angestellte oftmals sensible Unternehmensinformationen in öffentliche KI-Systeme eingeben, ohne die Sicherheitsimplikationen zu verstehen.

KI-generierte Exploits und Malware stellen eine besonders perfide Bedrohung dar. LLMs können ausgenutzt wer-

den, um automatisiert Phishing-Kampagnen oder Schadcode zu erzeugen, oft ohne ausreichende Gegenprüfung der generierten Inhalte.

Deepfake und Voice Clone Automation ermöglichen täuschend echte Video- und Audiogenerierung, was das Risiko für CEO-Fraud und andere Social-Engineering-Angriffe exponentiell erhöht. Die Manipulation von Audio-, Video- und Textinhalten zur Täuschung von Mitarbeitern und Systemen wird zunehmend automatisiert und schwerer erkennbar.

Context Leakage bei multimodalen Systemen entsteht durch die Verbindung von Text, Bild und Audio. Neue Angriffsvektoren ergeben sich beispielsweise durch versteckte Informationen in Bilddaten, die von herkömmlichen Sicherheitssystemen nicht erkannt werden.

Grenzen klassischer Security-Tools

Die Analyse zeigt deutlich, dass traditionelle Unternehmenssicherheitslösungen wie Data Loss Prevention (DLP), Cloud Access Security Broker (CASB) oder Secure Web Gateways keine DOM-Manipulationen auf Browser-Ebene erkennen können. Prompt Injection und automatisierte Datenabflüsse bleiben oft unentdeckt, da diese Tools nicht für die spezifischen Herausforderungen der KI-Ära konzipiert wurden.

Interne LLMs als Hochrisikoziele

Besonders kritisch wird die Situation bei intern eingesetzten LLMs, die hochsensible Unternehmensdaten wie Quellcode, M&A-Strategien oder juristische Dokumente verarbeiten. Diese Systeme verfügen oft über unzureichende Schutzmaßnahmen gegen Injection-Angriffe oder Datenlecks, da sie in vermeintlich sicheren Netzwerkumgebungen betrieben werden.

Erweiterte Handlungsempfehlungen

Effektive Gegenmaßnahmen erfordern einen ganzheitlichen Ansatz, der über traditionelle Sicherheitsmaßnahmen hinausgeht. Die kontinuierliche Überwachung von DOM-Interaktionen und Prompt-Manipulation ist essentiell, ebenso wie dynamisches Sandboxing für Browser-Erweiterungen.

Die Realtime-Erkennung und Blockierung verdächtiger Datenflüsse muss durch spezialisierte Governance-Richtlinien für die KI-Nutzung im Unternehmen ergänzt werden. Besonders wichtig ist die Kontrolle von Shadow AI durch umfassende Aufklärung der Mitarbeiter über die Risiken unkontrollierter KI-Nutzung

Fazit: Sicherheitsarchitektur neu denken

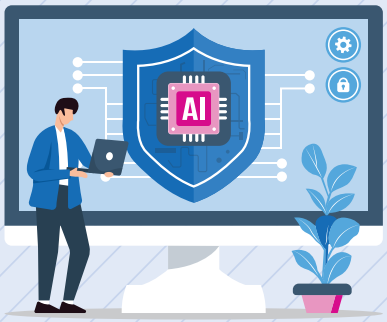
Die neue Bedrohungslage rund um generative KI-Tools erfordert ein radikales Umdenken in der IT-Sicherheit. Die Entdeckung der Man-in-the-Prompt-Angriffe markiert nur einen Wendepunkt in einer sich rapide entwickelnden Bedrohungslandschaft. Besonders browserbasierte Angriffspfade, Shadow AI und multimodale Lecks zeigen, dass klassische Sicherheitsansätze allein nicht mehr ausreichen.

Unternehmen müssen ihre GenAI-Governance-Strategien dringend überarbeiten und Browser-Sicherheit als kritischen Baustein ihrer KI-Sicherheitsarchitektur verstehen. Nur mit speziell entwickelten Sicherheitslösungen, einer robusten Governance und kontinuierlicher Weiterbildung der Mitarbeiter lassen sich die enormen Produktivitätsvorteile generativer KI sicher nutzen.

Ulrich Parthier | www.it-daily.net

➤ ➤ ➤ Bild 2 | Betroffene GenAI-Tools nach Reichweite

GenAI-Tool	Monatliche Besuche	Man-in-the-Prompt	Multimodale Risiken	Shadow AI Potenzial
ChatGPT	5 Milliarden	Ja	Ja (GPT-4V)	Sehr hoch
Gemini	400 Milliarden	Ja	Ja (Bard/Gemini Pro)	Hoch
Copilot	160 Milliarden	Ja	Ja (Code/Office)	Hoch
Claude	115 Milliarden	Ja	Ja (Claude 3)	Mittel
Perplexity	275 Milliarden	Ja	Begrenzt	Mittel



KI in der Cybersicherheit

PLATTFORMLÖSUNGEN GEGEN FRAGMENTIERTE SICHERHEITSÖKOSYSTEME

Künstliche Intelligenz (KI) ist für Cyberkriminelle zu einem signifikanten Multiplikator geworden. Mit ihr können sie ihre Angriffe schneller, flexibler und unbemerkter als je zuvor durchführen. Phishing-Kampagnen, die früher leicht an Grammatikfehlern oder falschen Logos zu erkennen waren, nutzen heute generative KI, um einwandfreie, personalisierte E-Mails zu erstellen, die Führungskräfte, Kollegen oder Zulieferer fast perfekt imitieren. Malware ist durch KI in der Lage, in Echtzeit Sicherheitsmaßnahmen zu analysieren, Angriffsvektoren zu wechseln und sogar das Verhalten legitimer Nutzer nachzuahmen. Ransomware könnte mithilfe von KI Back-Ups deaktivieren, bevor sie Daten verschlüsselt und Botnetze selbstständig anhand von Finanzdaten vielversprechende Ziele priorisieren.

Gleichzeitig ist der Einsatz von KI zur Abwehr von Cyberbedrohungen oft nicht einfach, denn obwohl einzelne KI-gestützte Sicherheits-Tools wie EDR, SOAR und XDR ihre Aufgaben oftmals zuverlässig erfüllen, sind sie in vielen Unternehmen nicht miteinander integriert. Diese Fragmentierung des Sicherheitsökosystems bedeutet, dass die einzelnen Phasen komplexer, mehrstufiger Cyberangriffe nicht miteinander in Verbindung gebracht werden – und führt so zu blinden Flecken, Fehlalarmen und verzögerten Reaktionen auf Vorfälle.

ManageEngine Log360: Von SIEM zur zentralen Sicherheitsplattform

Um KI bestmöglich selbst als Multiplikator für Cybersicherheit zu nutzen, benötigen Unternehmen eine zentrale Sicherheitsplattform, die Telemetriedaten aus allen Ebenen des Unternehmens – von Endpunkten, Netzwerken, Cloud-Umgebungen, Identitätsmanagementsystemen, Firewalls und Drittanbieter-Tools – aggregiert und in einen Kontext setzt. Dieser Ansatz transformiert KI von einem reaktiven Tool in einen proaktiven Sicherheitsstrategen, der in der Lage ist, Angriffe zu antizipieren, autonom Bedrohungen zu identifizieren und Schwachstellen zu beheben, Sicherheitsrichtlinien dynamisch und in Echtzeit durchzusetzen und datenbasiert weitere Maßnahmen zur Verbesserung der Sicherheit vorzuschlagen.

Die Zukunft der KI für die Cybersicherheit liegt in diesem plattformbasierten Security Control Tower-Modell. ManageEngine hat deshalb auf Basis seiner bewährten SIEM-Lösung Log360 entwickelt, eine einheitliche Sicherheitsplattform, die speziell darauf ausgerichtet ist, Datensilos abzubauen. Durch die Integration von Protokollen, Ereignissen und Telemetriedaten (zum Beispiel aus CASB, SASE, Firewalls) erstellt Log360 ein umfassenderes Bild der Sicherheitslage.

ManageEngine Log360 bietet zudem domänenübergreifende Integration durch eine nahtlose Kombination von Daten aus Cloud-Workloads, lokalen Servern, OT-Systemen und SaaS-Anwendungen sowie benutzerdefinierte Datennarrative: SOC-Teams können mit der Lösung auf ihre Anforderungen zugeschnittene Workflows für die Bedrohungssuche definieren, etwa zur Verfolgung seitlicher Bewegungen im System, um Phishing-Versuche zu erkennen oder um Verbindungen zwischen fehlgeschlagenen Anmeldungen und Datendiebstahl zu identifizieren.

Die Ära fragmentierter Sicherheitslösungen ist vorbei

Mit Log360 zeigt ManageEngine, wie zentralisierte Daten, toolübergreifende Integration und kompetente agentenbasierte KI die Effizienz von SOCs transformieren können. KI-gesteuerte Bedrohungen erfordern eine Verteidigungsstrategie, die ebenso anpassungsfähig und vernetzt ist wie die Angriffe selbst und in diesem Wettrüsten sind Plattformlösungen ein Eckpfeiler für die Cybersicherheit.

Subhalakshmi Ganapathy

KI IST FÜR CYBERKRIMINELLE ZU EINEM SIGNIFIKANTEN MULTIPLIKATOR GEWORDEN.

Subhalakshmi Ganapatahy, Chief IT Security Evangelist, ManageEngine, www.manageengine.com

IT-Automatisierung

TYPISCHE IMPLEMENTIERUNGSHÜRDEN UMGEHEN

AUTOMATISIERUNG IST KEIN „SET AND FORGET"-ANSATZ. SIE MUSS AUF UNTERNEHMENSZIELE ABGESTIMMT SEIN.

André Schindler, Senior Vice President of Global Sales, NinjaOne GmbH, www.ninjaone.de

IT-Teams stehen heute vor enormen Herausforderungen. Budgets schrumpfen, Teams werden kleiner – doch IT-Umgebungen wachsen stetig. Transformation, Cyber-Bedrohungen und unzählige Endpoints bedeuten: IT-Profis müssen mehr leisten mit weniger Ressourcen. Studien zeigen: Im Schnitt können sie nur 85 Prozent der täglichen Tickets bearbeiten – eine enorme Belastung.

Hier setzt Automatisierung an. Sie übernimmt wiederkehrende Aufgaben, steigert Effizienz, senkt Kosten, reduziert Fehler und beschleunigt Prozesse. Sie schafft Freiräume für Innovation, digitale Transformation und strategische Arbeit, die Unternehmen zukunftsfähig macht.

Warum Automatisierung jetzt zählt

Automatisierung optimiert kritische Aufgaben wie Patch-Management, Softwarebereitstellung, User-Onboarding, Compliance und Security. Ein Beispiel ist automatisiertes Endpoint Management: Alle Laptops, Server und Mobilgeräte bleiben automatisch aktuell, abgesichert und compliant – ohne mühsame manuelle Eingriffe.

Bis 2025 werden 80 Prozent der Unternehmen intelligente Automatisierung einsetzen. Sie reduziert Kosten, minimiert Risiken und schützt IT-Teams vor Überlastung. Für stark beanspruchte Abteilungen ist Automatisierung nicht optional, sondern ein strategisches Muss.

Auf starken Fundamenten aufbauen

Der Erfolg hängt von stabilen Grundlagen ab. Veraltete Systeme verursachen „technische Schulden", bremsen Innovation und müssen überbrückt werden. Unternehmen können entweder interne Teams mit der Modernisierung beauftragen oder externe Partner einbinden.

Zentral bleibt die Datenqualität. Automatisierung benötigt präzise, strukturierte Daten. Ohne sie sind Ergebnisse inkonsistent. Investieren Unternehmen jedoch in sauber aufbereitete Daten, lassen sich bis zu 70 Prozent der Workflows automatisieren – mit erheblichen Effizienz- und Kostenvorteilen.

Sicherheit zuerst – immer

Für IT- und Security-Teams bringt Automatisierung Verlässlichkeit. Remote Work vergrößert Angriffsflächen, verstreute Geräte erfordern ständige Aufmerksamkeit. Automatisierung setzt Updates, Patches und Compliance in Echtzeit durch, minimiert Schwachstellen und schützt sensible Daten.

Darüber hinaus schafft sie Transparenz, um Ineffizienzen und Risiken über alte wie neue Systeme hinweg sichtbar zu machen – eine Grundlage für proaktive Sicherheitsstrategien und nachhaltige Resilienz.

Der Weg nach vorn

Automatisierung ist kein „Set and Forget"-Ansatz. Sie muss auf Unternehmensziele abgestimmt sein – ob Kostenreduktion, Effizienzsteigerung oder höhere Sicherheit. Regelmäßige Überprüfungen stellen sicher, dass Automatisierung mit der Organisation wächst und dauerhaft geschäftlichen Mehrwert liefert.

Vorausschauende IT-Leiter sehen darin nicht nur Entlastung, sondern einen klaren Wettbewerbsvorteil. Automatisierung reduziert Komplexität, strafft Abläufe und legt die Basis für langfristigen Erfolg. Unternehmen, die Automatisierung strategisch einsetzen, verbessern nicht nur ihre operative Leistungsfähigkeit, sondern stärken auch ihre Position am Markt.

André Schindler

ISO 27001 und TISAX®

WIE SICH UNTERNEHMEN AUF NIS2 VORBEREITEN SOLLTEN

NIS2 lauert für viele Unternehmen am Horizont – aktuell wird eine Verabschiedung schon für Ende 2025 erwartet.

Diese Zeit sollten Unternehmen nutzen, um sich nachhaltig auf die neue Regelung vorzubereiten. Unternehmen, die nach ISO 27001 oder TISAX® zertifiziert sind, haben einen Vorteil: ISO 27001 deckt eine Vielzahl der geforderten NIS2-Vorgaben ab, z.B. Cyber-Hygiene, Incident Management, Teile der Lieferkettensicherheit und Kryptografie. Zusätzlich müssen ggf. die Bereiche Business Continuity und Governance erweitert sowie eine Multi-Factor-Authentification (MFA) und Meldepflicht eingeführt werden.

TISAX® erweitert die ISO 27001 um spezifische Regelungen für Unternehmen in der Automobilindustrie, fordert konkrete Umsetzungen und stellt Schutzklassen, Prüfziele und Prüfverfahren bereit. TISAX® enthält darüber hinaus spezifische Anforderungen beispielsweise beim Prototypenschutz, bei Drittlandtransfers und beim Datenschutz. Bei Unternehmen in entsprechenden Branchen lohnt sich daher häufig direkt die Umsetzung beider Standards. Das ist jedoch nicht immer sinnvoll. Gerade für kleinere mittelständische Unternehmen genügt oft die Umsetzung von ISO 27001 oder TISAX®.

In fünf Schritten zu NIS2

1. **Bestandsaufnahme:** ISO 27001-/TISAX®-Status prüfen
2. **Gap-Analyse:** NIS2-spezifische Lücken identifizieren
3. **Roadmap erstellen:** Maßnahmen planen und priorisieren
4. **Umsetzung starten:** Prozesse, Technik und Governance anpassen
5. **Externen Support einbinden:** Für gezielte Beratung und operative Unterstützung

Jochen Sandvoß | www.mhp.com

Zero-Trust-Strategien

SICHERHEITSKONZEPTE IN EINER DYNAMISCHEN BEDROHUNGSLANDSCHAFT

Cybersicherheit hat sich von einem technischen Problem zu einem Imperativ in den Vorstandsetagen entwickelt. Während sich die digitale Transformation in der gesamten DACH-Region beschleunigt, erweitern hybride Arbeit, Cloud-Dienste und Fernzugriff sowohl Chancen als auch Risiken. Damit vergrößert sich die Angriffsfläche – und die Kompromittierung von Anmeldeinformationen bleibt der häufigste Angriffsvektor.

Der Verizon 2024 Data Breach Investigations Report zeigt, dass über 60 Prozent der Sicherheitsverletzungen gestohlene Anmeldedaten betreffen.

Riskante Verhaltensweisen, wie die Wiederverwendung von Passwörtern oder das Speichern von Anmeldeinformationen in ungesicherten Formaten, offenbaren tiefere Probleme in der Sicherheitskultur und Governance des Unternehmens.

Um die Gefährdung zu minimieren, müssen sich Unternehmen Zero-Trust-Prinzipien zu eigen machen. Alle Anmeldungen, Aktionen und Zugangsdaten müssen gesichert werden – unabhängig vom Standort des Gerätes.

Privileged Access Management (PAM) ist für dieses Modell unerlässlich und beschränkt den Zugriff auf sensible Systeme, basierend auf Rolle und Kontext.

MEHR WERT
Keeper Security Infobericht

Ein moderner Ansatz für das PAM
Moderne PAM-Lösungen sind so konzipiert, dass sie die Einschränkungen älterer Systeme überwinden. Während ältere Plattformen große Budgets, komplexe Bereitstellungen und langwieriges Onboarding erfordern, sind die heutigen Cloud-basierten Lösungen:

- **Schnell bereitzustellen:** gemessen in Tagen, nicht in Monaten
- **Einfach zu bedienen:** intuitive Benutzeroberflächen, die den Schulungsaufwand minimieren
- **Kostengünstig:** sowohl für KMUs als auch für große Unternehmen zugänglich
- **Umfassend:** Verwaltung von Anmeldedaten, Geheimnissen und Fernzugriff von einer einzigen Plattform aus

Für Unternehmen bedeutet dies eine erhöhte Resilienz ohne erhöhte Komplexität.

Modernes PAM ist wichtiger denn je
Unternehmen, die PAM-Lösungen einsetzen, berichten von erheblichen Betriebs- und Sicherheitsvorteilen. Die jüngste Studie „Securing Privileged Access" von Keeper Security zeigte, dass von denjenigen, die eine PAM-Lösung eingeführt haben:

- **53 %** den Schutz sensibler Daten verbesserten
- **48 %** eine bessere Transparenz und Kontrolle über privilegierte Konten erhielten
- **49 %** angaben, dass die Effizienz bei der Verwaltung von Anmeldeinformationen verbessert wurde
- **49 %** Sicherheitsvorfälle im Zusammenhang mit dem Missbrauch von Privilegien reduzierten

UM DIE GEFÄHRDUNG ZU MINIMIEREN, MÜSSEN SICH UNTERNEHMEN ZERO-TRUST-PRINZIPIEN ZU EIGEN MACHEN. ALLE ANMELDUNGEN, AKTIONEN UND ZUGANGSDATEN MÜSSEN GESICHERT WERDEN.

Martin Sawczyn,
Solutions Engineer, Keeper Security,
www.keepersecurity.com

Vom Netzwerk zum Identitätsperimeter
Die Identität ist der bestimmende Perimeter in der Unternehmenssicherheit. Da Unternehmen ihre Abläufe in hybriden und Cloud-basierten Umgebungen zunehmend modernisieren, ist die Sicherung digitaler Identitäten, ob menschlich oder KI-basiert, zu einer wichtigen Priorität geworden. Die Konvergenz von Passwortmanagement, privilegiertem Zugriff und Geheimnissteuerung in der Cybersicherheit ist ein starker Indikator für diese veränderte Denkweise.

Den ersten Schritt machen
Moderne PAM-Lösungen stärken den Schutz von Anmeldeinformationen, fördern Compliance und senken die Komplexität. Zero-Trust-PAM ermöglicht Unternehmen in der gesamten DACH-Region den Wechsel von reaktiver Verteidigung zu proaktiver Kontrolle.

Martin Sawczyn

Strategisches Frühwarnsystem

WER DNS NUR ALS NETZWERK-TOOL SIEHT, HAT DIE KONTROLLE SCHON VERLOREN

Stellen Sie sich vor, jemand würde jeden Tag durch Ihre Eingangstür spazieren, ohne dass Sie es merken. Kein Alarm, kein Protokoll, keine Reaktion. Genau das passiert in vielen Unternehmen – nur digital. Der Angreifer kommt über das DNS. Wer heute noch glaubt, DNS sei nur ein Netzwerkdienst, hat den Ernst der Lage nicht verstanden. Während Angreifer oft schneller skalieren als Verteidiger reagieren können, ist DNS längst zur ersten Verteidigungslinie geworden.

Die unsichtbare Frontlinie

Cyberangriffe sind meist leise, persistent und oft monatelang unentdeckt. Besonders in regulierten Branchen – Energie, Finanzen, Behörden – ist das fatal. Denn hier geht es nicht nur um Daten, sondern um Vertrauen, Versorgungssicherheit und staatliche Souveränität.

Und genau hier liegt das Problem: Das DNS wird in vielen Organisationen noch immer wie ein Relikt aus der IT-Vergangenheit behandelt. Es mag inzwischen über 40 Jahre alt sein aber es ist mehr denn je auch ein strategischer Kontrollpunkt. Wer das DNS versteht, kontrolliert den Datenfluss. Wer DNS ignoriert, verliert die Kontrolle. Erschwerend kommt hinzu, dass 91 Prozent der Unternehmen weltweit schon zwei oder mehr Cloud-Anbieter nutzen. Das erhöht nicht nur die Komplexität, sondern auch die Angriffsfläche. Veraltete DNS-Einträge, fragmentierte IP-Adressräume, fehlende Transparenz – ein Paradies für Angreifer. Und ein Albtraum für Sicherheitsverantwortliche.

DNS als Frühwarnsystem denken – nicht nur als Infrastruktur-Tool

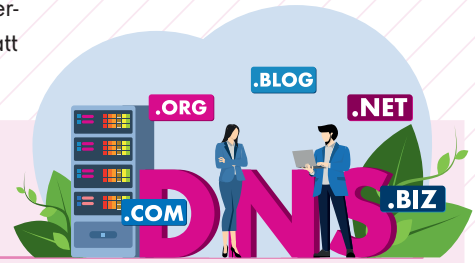
Bei Infoblox verstehen wir DNS daher als mehr als Infrastruktur-Klempnerarbeit – für uns ist es ein strategisches Frühwarnsystem, das in dieser komplexen Welt eindeutige Einblicke liefert und Security somit einfacher macht. Infoblox Threat Intel verarbeitet 70 Milliarden DNS-Events täglich und schafft es so 82 Prozent der Bedrohungen zu erkennen, bevor sie Schaden anrichten – im Schnitt 68,4 Tage vor einer Attacke. Das ist kein Zufall. Denn Infoblox verfolgt einen präventiven Ansatz: Statt auf Malware zu reagieren, analysieren wir die Infrastruktur, die Angreifer im Vorfeld aufbauen – etwa neu registrierte Domains, DNS-Telemetrie und verdächtige Muster. So erkennen unsere Lösungen verdächtige Aktivitäten, blockieren gefährliche Anfragen und liefern Kontext für schnelle Entscheidungen. Und das, bevor die Bedrohung zuschlägt.

NIS2: DNS wird zur Pflicht

Dieser präventive Ansatz ist nicht nur ein Game-Changer. Er hilft auch bei Compliance-Fragen. Denn auch die neue EU-Richtlinie NIS2 verändert die Spielregeln. DNS wird darin explizit als kritischer Dienst genannt – mit Anforderungen an Sicherheit, Resilienz und Transparenz. Unternehmen müssen künftig nachweisen, dass sie DNS nicht nur nutzen, sondern aktiv absichern.

PDNS (Protective DNS) wird dabei zur Schlüsseltechnologie. Die EU-Agentur ENISA empfiehlt PDNS bereits als Best Practice. Damit ist wird klar, dass DNS-Sicherheit nicht mehr optional, sondern regulatorisch verankert ist.

Wolfgang Huber | www.infoblox.com



WAS JETZT ZÄHLT

- **DNS sichtbar machen:** Wer nicht weiß, was im DNS passiert, weiß nicht, was geschützt werden muss.
- **PDNS als Pflicht verstehen:** Nicht als Add-on, sondern als integraler Bestandteil jeder Sicherheitsstrategie.
- **Security und Netzwerk zusammen denken:** DNS ist die Brücke für einen schnellen und notwendigen Informationsaustausch – Infoblox liefert das Geländer.
- **Regulatorik als Hebel nutzen:** Wer heute investiert, ist morgen nicht nur sicherer, sondern auch audit-ready.

Zero Trust

FUNDAMENT FÜR NACHHALTIGE COMPLIANCE

Cyberrisiken und Regularien wie NIS2 oder DORA verlangen neue, ganzheitliche Sicherheitsstrategien. In der Praxis etabliert sich dafür immer stärker ein Zero-Trust-Ansatz, der auf das Prinzip „Never trust, always verify" setzt. Eine technologische Lösung, die es für Zero Trust braucht, ist ZTNA (Zero Trust Network Access). Es bietet Schutz vor unautorisierten Zugriffen bei gleichzeitiger Erfüllung regulatorischer Anforderungen. Da die Umsetzung komplex ist und tief in die IT-Architektur eingreift, setzen mehr und mehr Unternehmen auf die Unterstützung von Experten und entsprechenden Managed Services. Entscheidend ist dabei die Wahl des passenden Service-Modells.

Bei einem Ansatz mit vollständiger Auslagerung übernimmt ein externer Partner Planung, Implementierung, Betrieb und Weiterentwicklung der ZTNA-Infrastruktur – inklusive 24/7-Monitoring und Anpassung an neue Anforderungen. Alternativ ermöglicht ein Co-Management-Modell die enge Zusammenarbeit zwischen interner IT und externen Spezialisten. So lassen sich Know-how und Ressourcen effizient kombinieren, etwa bei Migration, Dokumentation oder Nutzerakzeptanz. Obwohl ZTNA an Bedeutung gewinnt, scheitern viele Migrationen weiterhin, da es ohne erfahrene Partner häufig an Best Practices und bewährten Vorgehensweisen mangelt.

ZTNA ist ein Produkt, das je nach Reifegrad, Ressourcen und strategischer Ausrichtung individuell eingesetzt und ausgeweitet werden sollte. Der Schlüssel für langfristig erfolgreiche Transformationen und Compliance liegt dabei in der richtigen Kombination aus Technologie, Expertise und Prozesskompetenz.

Stefan Keller

ZTNA IST EIN PRODUKT, DAS JE NACH REIFEGRAD, RESSOURCEN UND STRATEGISCHER AUSRICHTUNG INDIVIDUELL EINGESETZT UND AUSGEWEITET WERDEN SOLLTE.

Stefan Keller, Chief Product Officer, Open Systems, www.open-systems.com/de/

Identity-First Security

ZERO TRUST FÜR ALLE DIGITALEN IDENTITÄTEN

Cyberangriffe werden immer raffinierter und stellen Unternehmen vor zunehmend komplexe Herausforderungen. Herkömmliche Sicherheitskonzepte stoßen dabei an ihre Grenzen. Zero Trust hat sich als moderner Ansatz etabliert, der auf der Grundregel basiert, niemals blind zu vertrauen. Stattdessen wird jeder Zugriff streng geprüft und jede digitale Identität konsequent geschützt.

Im Zentrum steht dabei die digitale Identität als zentrale Verteidigungslinie. Nur wer genau weiß, wer auf welche Ressourcen zugreift und unter welchen Bedingungen, kann wirksame Sicherheitsmaßnahmen etablieren. Ein Customer Identity and Access Management (CIAM) bildet die Basis, um diesen komplexen Anforderungen gerecht zu werden.

Ihr Partner für sichere, digitale Identitäten

Nevis begleitet Unternehmen auf dem Weg zu einem ganzheitlichen Zero-Trust-Konzept. Mit der Nevis ID, einer flexiblen CIAM-Plattform, schützen wir digitale Identitäten, bewerten Risiken adaptiv und steuern Zugriffe präzise. Die Plattform vereint Multi-Faktor-Authentifizierung, adaptive Zugriffskontrollen, Single Sign-On und Identity Orchestration in einer skalierbaren On-Premises-Lösung.

Komfort und Sicherheit gehen dabei Hand in Hand: Passwortlose Verfahren wie FIDO2-Passkeys und biometrische Authentifizierung ermöglichen einen reibungslosen Zugang ohne Kompromisse bei der Sicherheit. So entsteht eine Sicherheitsarchitektur, die den Anforderungen moderner IT-Umgebungen gerecht wird.

Zero Trust verlangt zudem dynamische Risikoanpassung. Standort, Gerätetyp oder Nutzerverhalten fließen in Zugriffsentscheidungen ein, sodass nur legitime Anfragen durchgelassen werden. Verdächtige Aktivitäten werden in Echtzeit erkannt und automatisch blockiert. So reduzieren Unternehmen ihre Angriffsfläche und stärken das Vertrauen von Kunden und Partnern.

Besonders in regulierten Branchen ist Transparenz unverzichtbar. Die Nevis ID Plattform protokolliert sämtliche Zugriffe umfassend und erfüllt hohe Compliance-Anforderungen wie NIS2 und DORA. Unternehmen gewinnen dadurch nicht nur Sicherheit, sondern auch Kontrolle über ihre IT-Umgebungen und stärken ihre digitale Souveränität.

Individuelle Strategien für nachhaltige Sicherheit

Die Implementierung von Zero Trust ist kein kurzfristiges Projekt, sondern eine strategische Transformation. Wir unterstützen Sie bei der Planung und Umsetzung Ihrer Zero-Trust-Initiativen: von der Priorisierung kritischer Systeme über Pilotprojekte bis hin zur Integration in bestehende Prozesse.

Mit einem starken Fokus auf dem Schutz digitaler Identitäten ebnen Unternehmen den Weg zu einer widerstandsfähigen, zukunftsfähigen IT-Sicherheitsarchitektur, die nicht nur aktuellen Bedrohungen standhält, sondern aktiv Wettbewerbsvorteile schafft.

Identity-First Security beginnt bei der Cloud-Plattform für alle digitalen Identitäten! Besuchen Sie Nevis auf der it-sa 2025 und erleben Sie, wie digitale Identitäten für Kunden, Partner und Maschinen neu gedacht werden – nahtlos, sicher und ganz ohne Passwort.

Gemeinsam mit vier starken Partnern zeigen wir: Zero Trust beginnt mit Vertrauen in die Identität. Mit der neuen Nevis ID Plattform bringen wir Einfachheit, Vertrauen und Zero Trust in Einklang.

Unser Expertenteam präsentiert Ihnen vor Ort passgenaue Strategien für mehr Sicherheit, Compliance und digitale Souveränität – und gibt exklusive Einblicke in die neuesten Entwicklungen.

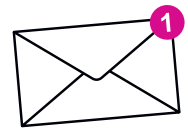
www.nevis.net

it-sa Expo&Congress
Besuchen Sie uns in **Halle 6-345**

nevis®

Sichere E-Mails?

GANZ LUFTIG, GANZ LEICHT - DANK MODERNER CLOUDLÖSUNGEN



Vertrauliche Informationen gehören nicht in ungesicherte E-Mails. Doch klassische Verschlüsselungslösungen wirken oft abschreckend: zu komplex, zu aufwendig, zu teuer. Moderne Cloudlösungen machen es anders – sie bringen Sicherheit, Effizienz und Benutzerfreundlichkeit in Einklang.

Mit cloudbasierten Diensten lassen sich E-Mails verschlüsseln, signieren und rechtskonform versenden – ganz ohne lokale Server, komplizierte Zertifikatsverwaltung oder Schulungsbedarf. Standards wie S/MIME und PGP sind meist integriert, ebenso der sichere Versand großer Dateianhänge und die Möglichkeit zur Authentifizierung über sichere Links. Besonders praktisch: Auch Empfänger ohne eigene Lösung können vertrauliche Nachrichten über ein sicheres Webportal lesen und beantworten. Der Austausch bleibt geschützt, ohne dass zusätzliche Software oder technisches Wissen nötig ist. Gerade für Unternehmen, deren Mitarbeiter im Homeoffice arbeiten oder die international agieren, bieten solche Lösungen die nötige Flexibilität. Datenschutz, Compliance und Effizienz lassen sich damit ideal kombinieren, und das ohne Kompromisse bei der Nutzererfahrung oder der Sicherheit sensibler Daten.

Datenschutz muss nicht schwer sein

Moderne Lösungen zeigen, wie leicht digitale Sicherheit sein kann, und machen endgültig Schluss mit Technikfrust: Einfach starten, durchatmen, sicher senden. Denn E-Mail-Sicherheit sollte kein Luxus sein, sondern ein selbstverständlicher Bestandteil moderner Kommunikation – leicht zugänglich, wirkungsvoll und überall verfügbar. So gelingt Datenschutz mit Leichtigkeit.

www.seppmail.co

Value Add Distribution für die IT

DIE UNTERNEHMENS-IT STÄRKEN

In einer Zeit, in der Cyberbedrohungen komplexer, die Technologielandschaft vielfältiger und IT-Budgets knapper werden, stehen Unternehmen vor der Herausforderung, ihre IT-Sicherheit kontinuierlich auf dem neuesten Stand zu halten. Value Add Distributoren (VAD) sind in diesem Umfeld weit mehr als reine Logistikdrehscheiben zwischen Herstellern und Fachhandel. Sie bringen zusätzliches technisches Know-how, marktreife Services und praxisnahe Beratungsangebote ein und unterstützen Partner und Security-Teams, schneller zu reagieren, Risiken zu minimieren und Ressourcen optimal einzusetzen.

Mehrwert seit über 40 Jahren
Westcon-Comstor zählt seit über vier Jahrzehnten zu den führenden VADs weltweit. Mit einem breit gefächerten Herstellerportfolio – von globalen Marktführern bis zu innovativen Spezialisten – und einem ausgeprägten Servicegedanken begleitet das Unternehmen seine Partner und deren Kunden entlang des gesamten Projektlebenszyklus, vom Konzept bis zum laufenden Betrieb.

Westcon-Comstor versteht Distribution als End-to-End-Unterstützung – und das spiegelt sich auch im Leistungsportfolio des VADs wider:

- **3D Lab:** Über die interaktive Plattform können Partner komplexe IT-Architekturen realitätsnah erfahren und demonstrieren.
- **Tech Xpert-Community:** Ein Netzwerk erfahrener technischer Spezialisten, die ihr Wissen regelmäßig in Workshops, Webinaren und Networking-Veranstaltungen weitergeben.
- **Flex:** Flexible Finanzierungslösungen ermöglichen es, Projekte schneller umzusetzen und Kunden bedarfsgerecht zu bedienen.
- **AWS-Programm:** Westcon-Comstor unterstützt beim erfolgreichen Einstieg in den AWS Marketplace – und somit beim Erschließen eines attraktiven, zukunftsorientierten Vermarktungskanals für Security-Lösungen, von dem auch die Endkunden profitieren.
- **Value Add Services** Von Presales- und Marketingunterstützung über Schulungen bis hin zu maßgeschneiderten Support-Angeboten.

Dieses breite Angebot steigert nicht nur die Effizienz, sondern eröffnet Partnern neue Geschäftschancen – bei gleichzeitig höherer Kundenzufriedenheit.

www.westconcomstor.com

WESTCON-COMSTOR AUF DER IT-SA 2025

Vom 7. bis 9. Oktober wird Nürnberg erneut zum Mittelpunkt der IT-Sicherheitsbranche – und Westcon-Comstor ist 2025 wieder mittendrin. Am Messestand 9-334 dreht sich alles um tiefgreifendes Know-how, Networking und konkrete Lösungen. Gemeinsam mit Cisco und den Partnern Verizon und Conscia präsentiert der VAD sein Leistungsspektrum und steht für persönliche Gespräche bereit.

Besucher dürfen sich auf einige Highlights freuen:
Spannende Kooperation:
Gemeinsam mit den whitelisthackers, bekannt für ihre Angriffssimulationen und Live-Hacking, bietet Westcon-Comstor den Besuchern in Halle 9 ein vielfältiges Programm am Messestand.

Services und Mehrwerte:
Vor Ort können Besucher das Leistungsportfolio von Westcon – samt dem 3D Lab, den vielfältigen Value Add Services und dem AWS-Programm – kennenlernen und sich individuell beraten lassen.

Beste Kaffeepause der Messe:
Zwischen den Vorträgen lädt Westcon-Comstor wie gewohnt zum wahrscheinlich besten Kaffee der it-sa ein – ideal zum Netzwerken und fachlichen Austausch.

Wer auf der it-sa nicht nur Produkte sehen, sondern Experten treffen und konkrete Security-Ansätze mitnehmen möchte, findet am Stand von Westcon-Comstor den idealen Anlaufpunkt. Der Besuch lohnt sich – nicht nur fachlich.

KI IN DER CYBERSICHERHEIT

BLEIBT DER MENSCH UNVERZICHTBAR?

Arctic Wolf hat neue Ergebnisse aus seinem aktuellen 2025 AI Report, der die Balance zwischen Mensch und KI als Erfolgsfaktor für Security Operations untersucht, veröffentlicht.

Sicherheitsteams sehen sich heute mit einem unaufhörlichen Strom von tausenden Alerts aus fragmentierten Tools und isolierten Datenquellen konfrontiert. Mit begrenztem Personal und Ressourcen müssen sie schnelle, risikoreiche Entscheidungen treffen, welche Alarme untersucht werden sollen.

ZENTRALE ERGEBNISS DES REPORTS

99 %
der Unternehmen geben an, dass KI-Funktionen ihre Investitionen in Cybersicherheitslösungen beeinflussen werden

73 %
haben KI bereits in ihre Cybersicherheitsstrategie integriert

52 %
wollen ihre Teams für den Umgang mit KI weiterbilden

KI als entscheidender Faktor

Dieser zunehmende Druck ist der Grund, warum KI zu einem entscheidenden Faktor in Cybersicherheitsstrategien geworden ist. Unternehmen betrachten KI nicht nur als Werkzeug, sondern als Partner in Security Operations. Sie nutzen moderne Bedrohungserkennung, um bösartige Aktivitäten schneller zu identifizieren, setzen Large Language Model-Assistenten zur Unterstützung von Analysen ein und automatisieren wiederkehrende Aufgaben durch KI-gestützte Workflows. In Kombination mit menschlicher Expertise können diese Fähigkeiten das Rauschen durchdringen, die Alert Fatigue reduzieren, Untersuchungen beschleunigen und Sicherheitsteams ermöglichen, sich auf die wirklich relevanten Bedrohungen zu konzentrieren.

Gerade in Deutschland gewinnt dieser Ansatz an Bedeutung: Der akute Fachkräftemangel in der IT-Sicherheit erschwert es Unternehmen, ausreichend qualifizierte Expertinnen und Experten zu finden. KI kann hier Sicherheitsteams entlasten, indem Routineaufgaben automatisiert und Analysen beschleunigt werden – ersetzt wird die menschliche Expertise dadurch jedoch nicht. Im Gegenteil: Die Studie zeigt, dass der Erfolg von KI maßgeblich von menschlicher Expertise und abhängt.

Auch regulatorisch gewinnt das Thema an Gewicht: Vorgaben wie NIS2 oder DORA verpflichten Unternehmen in Europa, klare Verantwortlichkeiten und menschliche Kontrollmechanismen im Cyber-Risikomanagement zu verankern. Das unterstreicht, dass KI in der Cybersicherheit zwar ein wichtiges Werkzeug ist, ihre Ergebnisse jedoch weiterhin von Menschen geprüft und verantwortet werden müssen.

www.arcticwolf.com

Security & Resiliency

SCHUTZ UND WIDERSTANDSFÄHIGKEIT FÜR DIE DIGITALE ZUKUNFT

In unserer digitalen Welt sind Cyberangriffe tägliche Realität: Jedes Unternehmen muss davon ausgehen, früher oder später betroffen zu sein. Auch ohne absolute Sicherheit gibt es Strategien, die Risiken zu minimieren und handlungsfähig zu bleiben.

Mit den Security Services von Kyndryl bieten Unternehmen einen integrierten Ansatz, um Bedrohungen frühzeitig zu erkennen, sich wirksam zu schützen und Angriffe abzuwehren. Dank der Cyber Resiliency Services sind Unternehmen nach einem Vorfall schnell wieder arbeitsfähig.

Der entscheidende Vorteil von Kyndryl: Wir kombinieren Schutz und Resilienz. Wir stärken die Abwehr und sichern zugleich die schnelle Erholung nach Cyber-Angriffen.

Das Kyndryl Security und Resiliency Services Portfolio umfasst:

- **Security Assurance Services:** Bewertung von Risiken und Compliance, Transparenz über Bedrohungen.
- **Zero Trust Services:** Schutz geschäftskritischer Daten und Anwendungen.
- **Security Operations & Response Services:** kontinuierliche Überwachung und schnelle Reaktion.
- **Incident Recovery Services:** automatisierte Wiederherstellung von Prozessen und Daten.

Unser Ansatz verbindet jahrzehntelange Erfahrung im Betrieb geschäftskritischer Systeme mit modernster Technologie. Mit Kyndryl Consult beraten wir Unternehmen ganzheitlich und begleiten die sichere digitale Transformation. Über die Integrationsplattform Kyndryl Bridge gewinnen Kunden Transparenz und Kontrolle über ihre IT-Umgebungen. Und mit Kyndryl Vital entwickeln wir mit Partnern und Kunden Lösungen für komplexe Herausforderungen.

Unser Ziel: Wir minimieren das Risiko von Cyberangriffen, stärken Ihre Widerstandskraft und sichern ihre Zukunft.

www.kyndryl.de

kyndryl

IT-SICHERHEIT HEUTE UND MORGEN

NEUE BEDROHUNGEN UND ALTE INSELLÖSUNGEN

STUDIEN-DOWNLOAD

Das Studie umfasst 13 Seiten und steht kostenlos zum Downloadbereit.

www.it-daily.net/download

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

Die folgende Studie beschäftigt sich daher mit folgenden Fragestellungen:

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

Sichere KI

NEUE BEDROHUNGEN, NEUE SCHUTZSTRATEGIEN

KI-Systeme unterscheiden sich grundlegend von klassischen IT-Anwendungen und bringen neue, teils schwer kalkulierbare Sicherheitsrisiken mit sich – etwa durch manipulierbare Trainingsdaten, schwer nachvollziehbare Entscheidungswege, neuartige Entwicklungsprozesse und den Betrieb an sich.

Angriffsvektoren reichen von Data Poisoning über Adversarial Attacks und Model Inversion bis hin zu Membership Inference Attacks. Betroffen ist dabei nicht nur der Betrieb, sondern bereits die Entwicklung. Risiken entstehen durch unsichere Open-Source-Bibliotheken, ungeschützte MLOps-Pipelines oder fehlende Governance in KI-Projekten.

Die Absicherung von KI-Systemen muss daher ganzheitlich erfolgen – sowohl in der Entwicklungsphase als auch zur Laufzeit. Trainingsdaten, Modelle und Entwicklungsumgebung sollten vor Manipulation geschützt werden. Im Betrieb gilt es, Eingaben, Modelllogik, Ausgaben sowie die Ausführungsumgebung abzusichern – insbesondere gegen Datenlecks, ungewollte Informationspreisgabe und unautorisierte Zugriffe.

Wichtige Leitplanken liefern neue Standards wie ISO/IEC 27090, die erstmals ein systematisches Sicherheits-Framework für KI-Systeme definieren. Der EU AI Act verpflichtet Anbieter zu Risikobewertung, Robustheit, Transparenz und Schutzmaßnahmen – insbesondere bei Hochrisiko-Anwendungen. Ergänzend bieten Frameworks wie die OWASP ML Top 10 und MITRE ATLAS praxisnahe Orientierung zur Abwehr KI-spezifischer Bedrohungen.

Benedikt Bauer | www.mhp.com

UMSETZUNG VON NIS2-COMPLIANCE

WARUM SIE ZUR HERAUSFORDERUNG WIRD

Viele KMUs stehen der Umsetzung von NIS2 nicht nur wegen der neuen regulatorischen Anforderungen skeptisch gegenüber – sondern weil sie bereits heute im Tagesgeschäft mit strukturellen und personellen Engpässen zu kämpfen haben. Für viele KMUs sieht es in der Realität wie folgt aus:

➤ **Unterbesetzte IT-Abteilungen**
Fachkräftemangel ist ein bekanntes Problem; oft stoßen die IT-Abteilungen bereits mit dem Tagesgeschäft an ihre Belastungsgrenze

➤ **Unklare Verantwortlichkeiten**
Intern, aber auch bei Auslagerung bestimmter IT-Dienste. Die Zusammenarbeit mit externen Dienstleistern führt oft zur Verwischung von Zuständigkeiten, was im Ernstfall die Lage kritisch verschlechtern kann

➤ **Ungenügende IT-Infrastruktur**
Nicht mitgewachsene IT-Abteilungen, aber auch, wenn bei der Ergänzung der IT-Systeme hinweg die systematische Sicherheitsarchitektur vergessen wurde

➤ **Externe IT-Dienstleister**
kümmern sich um die Grundfunktionalität, haben aber oft keinen spezifischen Cyber Security-Fokus

➤ **Fehlendes Know-how**
zu Bedrohungsszenarien und Verteidigungsstrategien

➤ **Begrenzte finanzielle Ressourcen**
für IT-Sicherheitsmaßnahmen

www.vargroup.de

Cloud Managed Services

MEHR SICHERHEIT, EFFIZIENZ UND TRANSPARENZ FÜR DEN CLOUD-BETRIEB

Controlware Cloud Managed Services vereinen Sicherheit, Governance, Geschwindigkeit und Kostentransparenz zu einem belastbaren Preis- und Betriebsmodell für Public-Cloud- Infrastrukturen und reduzieren gleichzeitig operative Herausforderungen durch reproduzierbare Qualität und klare Verantwortlichkeiten.

Grundsätzlich ist es ratsam, den Einstieg in einen Cloud Managed Service mit einem Security-Check vor dem Betriebsübergang zu beginnen – professionell durchgeführt von einem Managed Service Provider. Ein solcher Security-Check deckt Fehlkonfigurationen und schwache Identitätskontrollen bereits im Vorfeld auf, schafft eine Governance- und Compliance-Baseline und priorisiert Risiken für die Transition – somit werden Sicherheitsdefizite nicht in den Managed Service-Betrieb übernommen.

Einheitliche Standards

Da Policies üblicherweise einer Dynamik unterliegen, ist kontinuierliches Policy-Management ein wesentliches Service-Element. Belastbares Monitoring erfasst Metriken und Logs zentral und schärft Alarm-Schwellwerte dynamisch. Definierte Alarmregeln erzeugen bei kritischen Ereignissen automatisiert Tickets und sind agil in die Betriebsprozesse eingebunden – wodurch Service Level messbar und überprüfbar werden. Das Sicherheitsfundament bildet der Controlware SecureHub als Cloud-DMZ nach dem Hub-Spoke-Prinzip. Ein zentraler Hub stellt geteilte Dienste bereit, isoliert Spokes und kapselt Workloads. Bei den Kernkomponenten handelt es sich um Cloud-basierte Sicherheitssysteme, die einen kontrollierten Übergang zwischen Internet, On-Premises Data Center und der Public Cloud-Umgebung gewährleisten. Optional können Bastion Hosts, Load Balancer, Application Gateways oder DDoS Protection die Richtliniendurchsetzung und Segmentierung ergänzen. Dieser Ansatz trennt Geschäftsbereiche sauber und setzt einheitliche Standards durch.

Moderne Workloads sind in der Regel Container-basiert und laufen in Kubernetes-Umgebungen mit standardisierten Lebenszyklen, Admission-Kontrollen und abgesichertem Ingress. Virtuelle Maschinen profitieren von kuratierten Images, automatischem Patching und Rollen-basierten Zugriffsmodellen.

Belastbare Sicherheit wird aber nicht ausschließlich am Perimeter durchgesetzt. Ein Cloud-nativer SOC-Service, wie von Controlware im Rahmen der Cyber Defense Services zur Verfügung gestellt, adressiert Cloud-spezifische Bedrohungen. Die Kombination mit Cloud Posture (CSPM) und Exposure Management reduziert Fehlkonfigurationen sowie bekannte Schwachstellen. Zudem schützen Agenten-basierte Workload Protection-Lösungen die Runtime moderner Public Cloud-Anwendungen. Im Zusammenspiel mit Identity Protection- und Detection & Response-Mechanismen lassen sich diese nahtlos in bestehende Controlware MDR-Services einbinden.

Cloud Managed Services

Die Controlware Cloud Managed Services erlauben kontinuierliche Analysen der Infrastruktur, schaffen Transparenz bzgl. Verbrauch und Kosten, zeigen unterausgelastete Ressourcen sowie ineffiziente Betriebsszenarien auf und schlagen Maßnahmen vor – vom Rightsizing über Reservations bis hin zur automatisierten Abschaltung in Randzeiten. Getragen wird der Cloud Managed Service von ITIL-basierten Prozessen im Controlware Cloud Management Center – von Service Desk über Incident und Change Handling bis zu Reporting und regelmäßigen Reviews. Durch detailliertes Reporting bleibt der Cloud-Betrieb für Fachbereiche transparent, sicher und effizient.

Die Kombination von praxisgeprüften Architektur-Blueprints, Automatisierung per IaC und Pipeline-Integration in Verbindung mit Monitoring und etablierten Service-Prozessen schafft die Grundlage für resilienten, auditierbaren und transparenten Cloud-Betrieb – heute und in Zukunft.

Frank Melber

Nicht zur Zielscheibe werden

WIE UNTERNEHMEN IHRE ANGRIFFSFLÄCHE FÜR CYBERBEDROHUNGEN REDUZIEREN KÖNNEN

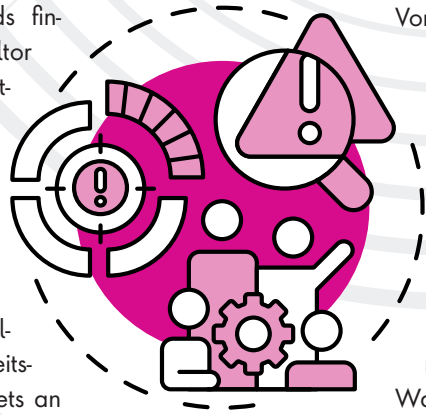
UNTERNEHMEN, DIE SCHNELL WACHSEN, ÜBERSEHEN OFT DIE SUBTILEN WARNSIGNALE FÜR EINEN BEVORSTEHENDEN CYBERANGRIFF.

Sneha Banerjee, Enterprise Analyst, ManageEngine, www.manageengine.com

Cyberangriffe kommen selten aus dem Nichts. Die meisten Angreifer bereiten sich gründlich vor und suchen aktiv nach ungeschützten Unternehmen. Diese Anzeichen sind nicht immer so offensichtlich wie schwache, kontinuierlich wiederverwendete Passwörter oder veraltete Software, die nicht zuverlässig aktualisiert wurde.

Fünf subtile Warnzeichen für einen bevorstehenden Cyberangriff

Die digitale Präsenz vieler Unternehmen wächst oft fast unbemerkt, aber ihr Sicherheitsbudget hält mit diesem Wachstum nicht mit. Mit jedem neuen Tool, jeder Cloud-Plattform und jeder Drittanbieter-App steigt die Chance, dass ein Angreifer alte Konten, nicht mehr genutzte Testumgebungen oder ungeschützte Clouds finden und als Einfalltor nutzen kann. Dementsprechend sollten Unternehmen kontinuierlich online wie auch offline die Augen nach solchen vergessenen Ressourcen offenhalten, um ihre Sicherheitsstrategie und -budgets an ihren tatsächlichen digitalen Fußabdruck anzupassen.



Wenn wichtige Mitarbeiter – insbesondere Führungskräfte – auf Geschäftsreisen, im Urlaub oder nach Feierabend ihre privaten Endgeräte für arbeitsbezogene Aufgaben nutzen, kann dies ebenfalls eine unsichtbare Schwachstelle darstellen, denn diese Geräte sind oft nicht durch die MDM- oder Endpunkt-Erkennungstools des Unternehmens geschützt. Schon ein einziges kompromittiertes Gerät kann Angreifern Zugriff auf Quellcodes, Kundeninformationen oder Finanzdaten verschaffen. Die IT-Verantwortlichen im Unternehmen müssen an dieser Stelle streng sein: Sicherheitsstandards und Richtlinien gelten für alle, einschließlich der Führungsebene.

Besonders vorsichtig sollten Unternehmen dann sein, wenn andere Unternehmen in ihrem Netzwerk oder ihrer Lieferkette bereits Opfer eines Angriffs geworden sind. Insbesondere kompromittierte Zulieferer mit API- oder Datenzugriff werden von Angreifern gerne als erstes Einfalltor in weitere Unternehmen genutzt. Regelmäßige Überprüfungen aller Partner sollten ebenso Standard sein, wie ein System für diese, um Vorfälle zu melden.

Auch wenn sich Phishing-E-Mails häufen, kann dies ein Warnzeichen dafür sein, dass Angreifer die Sicherheitsmaßnahmen eines Unternehmens austesten. Was wie Spam aussieht, könnte tatsächlich die erste Phase eines gezielteren Angriffs sein. Unternehmen sollten deshalb jede Phishing-Mail ernst nehmen und nach Mustern suchen, beispielsweise ob bestimmte Standorte oder Positionen bevorzugt zum Ziel werden.

Und nicht zuletzt sollten sich Unternehmen darüber im Klaren sein: Cyberkriminelle lesen dieselben Nachrichten, Pressemitteilungen und LinkedIn-Beiträge wie Kunden und Investoren. Unternehmen, die gerade eine große Finanzierungsrunde abgeschlossen oder eine wichtige Partnerschaft angekündigt haben, fallen wahrscheinlicher ins Visier von Angreifern. Öffentliche Erfolge gehen oftmals mit großen Veränderungen in Unternehmen einher, während denen IT-Sicherheit unter Umständen nicht die Hauptpriorität ist. Angreifer setzen genau darauf, weshalb Unternehmen solche Phasen auch stets als Risikomultiplikator für Cyberbedrohungen behandeln sollten.

Aufmerksamkeit ist die beste Verteidigung

Unternehmen, die schnell wachsen, übersehen oft die subtilen Warnsignale für einen bevorstehenden Cyberangriff. Mit etwas Aufmerksamkeit und den entsprechenden Sicherheitslösungen kann ein Unternehmen jedoch nach wie vor seine Angriffsfläche effektiv reduzieren und selbst den komplexen Bedrohungen von heute einen Schritt voraus sein.

Sneha Banerjee

Drittzugriff absichern

BASIS FÜR EMBEDDED FINANCE

Embedded Finance erlebt derzeit einen starken Aufschwung und transformiert das Finanzwesen, indem es neue Möglichkeiten schafft und bestehende Prozesse effizienter gestaltet. So wurden beispielsweise im Jahr 2021 in den USA bereits Transaktionen im Wert von 2,6 Billionen US-Dollar über sogenannte Embedded-Finance-Lösungen abgewickelt. Experten rechnen damit, dass dieser Wert bis zum Jahr 2026 auf über sieben Billionen US-Dollar steigen wird. Um das volle Potenzial von Embedded Finance auszuschöpfen, ist eine sichere und anpassungsfähige Verwaltung des Zugriffs durch Drittparteien unerlässlich.

Third-Party Access als zentrale Herausforderung

Die Integration von Finanzdienstleistungen über APIs und externe Kooperationen eröffnet zwar ein breites Spektrum an Möglichkeiten, beinhaltet jedoch auch ein erhebliches Risikopotenzial. Die größte Herausforderung besteht darin, sensible Daten zu schützen und die Infrastruktur sicher und effizient zu nutzen. Werden Prozesse für die Einarbeitung von Mitarbeitenden manuell durchgeführt und der Zugang zu verschiedenen Systemen durch viele verschiedene Kontrollen gesteuert, kann das zu Sicherheitslücken führen. Herkömmliche Identity-and-Access-Management-(IAM)-Systeme sind für die Verwaltung großer Mengen externer Parteien nicht geeignet und stoßen bei Delegation, Skalierung und Governance an ihre Grenzen.

Warum Legacy-IAM versagt

Traditionelle IAM-Tools sind häufig darauf ausgelegt, die Verwaltung interner Mitarbeitenden oder Endkunden zu unterstützen. Für komplexe, multinationale Partnernetzwerke sind sie jedoch oft nicht flexibel genug. Dies führt zu manuellen Prozessen und unsicheren Zugriffsmechanismen, wodurch die Sicherheit des gesamten Systems beeinträchtigt werden. Außerdem ist es schwierig, Vertrauen in der gesamten Partnerlandschaft zu etablieren. Dies ist ein kritischer Aspekt, denn Angriffe wie Deepfakes und Identitätsmissbrauch nehmen in unserer Zeit zu. Die Lösung für moderne Zugriffs- und Identitätsanforderungen sind moderne IAM-Plattformen.

Moderne IAM-Plattformen, die auf „Identity Fabrics" setzen, bieten eine integrierte Lösung für die Verwaltung von Identitäten und Zugriffen Dritter. Das macht sie zu einer effizienten und benutzerfreundlichen Option. Sie ermöglichen föderierte Identitätsmodelle und unterstützen Bring-Your-Own-Identity (BYOI). Durch feingranulare Zugriffskontrollen wird sichergestellt, dass Partner nur die benötigten Rechte erhalten, und durch automatisierte Prozesse wird die Sicherheit optimiert. So haben Finanzdienstleister die Möglichkeit, den vollen Wert von Embedded Finance zu erschließen, ohne die Kontrolle zu verlieren.

Ohne starke Identitätsinfrastruktur kein Erfolg

Um den zukünftigen Erfolg von Embedded Finance sicherzustellen, ist eine zuverlässige Identitätsinfrastruktur erforderlich, die den strengen Sicherheitsanforderungen entspricht. Unternehmen müssen den Zugriff Dritter zuverlässig verwalten, um die Sicherheit und Integrität der Daten zu gewährleisten. Nur so können sie regulatorischen Anforderungen gerecht werden und das Vertrauen ihrer Kunden wahren. Moderne Identity-Fabrics bieten die für den Erfolg von Embedded Finance entscheidende Skalierbarkeit und Sicherheit. Sie sind somit eine wichtige Komponente für einen sicheren und reibungslosen Ablauf der Finanztechnologie. Unternehmen werden dabei von Partnern wie Ping Identity mit innovativen Lösungen für Identitätsmanagement und Zugriffskontrolle unterstützt.

www.pingidentity.com

MEHR WERT
Financial Services

it-sa Expo&Congress

Ping Identity.

Besuchen Sie uns in **Halle 6-427**

Schluss mit „Patient Zero“

WARUM UNTERNEHMEN DOMAINS BLOCKIEREN MÜSSEN, BEVOR DER ERSTE KLICK ERFOLGT

WER HEUTE NOCH DARAUF SETZT, NICHT „PATIENT ZERO“ ZU SEIN, HANDELT FAHRLÄSSIG.

Stephan Fritsche, Central Europe Security Lead, Infoblox, www.infoblox.com

Was wäre, wenn der erste Klick auf eine bösartige Domain gar nicht erst stattfinden würde? Cyberangriffe werden immer raffinierter, schneller und gezielter – die Vorstellung, dass ein Angriff erst erkannt und gestoppt werden kann, nachdem das erste Opfer – der „Patient Zero“ – infiziert wurde, ist nicht nur naiv, sondern gefährlich.

Die Realität: Angriffe im Sekundentakt

Cyberkriminelle nutzen heute automatisierte Tools, KI-gestützte Malware und andere Tools, um ihre Opfer skalierbar und immer effizienter zu täuschen. Bei Infoblox haben wir allein im vergangenen Jahr über 100 Millionen neue Domains beobachtet – gut ein Viertel mussten wir als bösartig oder zumindest verdächtig einstufen. Viele dieser Domains sind nur eine kurze Zeit aktiv, bevor sie wieder verschwinden. Klassische Sicherheitslösungen, die auf Signaturen oder IOC-Feeds basieren, kommen in einer Vielzahl von Fällen also schlicht zu spät.

Besonders perfide: Die Eintrittsbarrieren für Cyberkriminelle sind heute so niedrig wie nie. KI-gestützte Tools liefern auf Knopfdruck täuschend echte Phishing-Kampagnen – inklusive personalisierter Inhalte, gefälschter Login-Seiten und Social-Engineering-Skripte. Wer früher noch technisches Know-how brauchte, braucht heute nur ein Ziel. Spätestens damit ist das „Patient Zero“-Modell überholt.

Was das DNS über Angriffe weiß, bevor sie beginnen

DNS wird oft als technisches Grundrauschen wahrgenommen – als notwendige, aber oft ignorierte Infrastruktur. Doch genau hier liegt der strategische Hebel: DNS ist der erste Berührungspunkt (fast) jeder digitalen Kommunikation. Bevor ein Gerät eine Verbindung aufbaut, bevor ein Browser eine Seite lädt, bevor ein Skript ausgeführt wird, steht eine DNS-Anfrage.

Richtig genutzt lassen diese DNS Informationen die Verteidiger tiefer in die Struktur, das Verhalten und die Herkunft von Domains blicken. So lassen sich Muster erkennen, die auf eine spätere missbräuchliche Nutzung hindeuten – und das lange bevor eine Domain tatsächlich für einen Angriff eingesetzt wird.

Diese Position macht das DNS einzigartig: Wer das DNS intelligent auswertet, erkennt Bedrohungen, bevor sie sich entfalten. Wer das DNS für sich zu nutzen weiß, kann Angriffe stoppen, bevor sie beginnen.

Vier Schritte raus aus dem Reaktionsmodus

- **DNS als Sicherheitslayer etablieren:** DNS ist nicht nur Infrastrukturkomponente, sondern ein strategischer Kontrollpunkt. Wer das DNS im Security Stack ignoriert, lässt eine der effektivsten Verteidigungslinien ungenutzt.

- **Von reaktiv zu präventiv:** Sicherheitsstrategien müssen sich vom „Patient Zero“-Modell verabschieden. Ziel muss es sein, Angriffe vorbeugend zu verhindern – nicht nur reaktiv zu erkennen und ihre Auswirkungen zu beheben.
- **Automatisierung nutzen:** Moderne DNS-Sicherheitslösungen integrieren sich in bestehende Security-Stacks und ermöglichen automatisierte Reaktionen auf Bedrohungen.
- **Sicherheitsarchitektur vereinfachen:** Das DNS kann als verbindendes, Einblicke schaffendes Element zwischen Netzwerk Assets, Endpoints und der Cloud dienen – ohne zusätzliche Agenten, ohne Silos, ohne Fingerpointing zwischen Teams.

Fazit

Die Zeit des Hoffens ist vorbei. Wer heute noch darauf setzt, nicht „Patient Zero“ zu sein, handelt fahrlässig. DNS-basierte Sicherheitsansätze zeigen, dass es auch anders geht: proaktiv, intelligent und effektiv. Es ist Zeit, den Paradigmenwechsel zu vollziehen – bevor der nächste Klick zum Desaster wird.

Stephan Fritsche

Sicher ist, was beweglich bleibt

ADAPTIVE SECURITY-ARCHITEKTUR STATT SCHUTZWALL

Firewalls, Richtlinien, VPN – über Jahrzehnte wurde Sicherheit als Schutzwall gedacht. Doch diese Mauern bröckeln. Menschen arbeiten mobil, Daten fließen in Multi-Clouds, Systeme sind per APIs verknüpft, KI automatisiert Prozesse. Jede Verbindung vergrößert die Angriffsfläche und verändert sie.

Statische Sicherheitsarchitekturen stoßen hier an ihre Grenzen. Entscheidend ist die Fähigkeit, in Echtzeit kontextbezogene Entscheidungen zu treffen: Darf ein bestimmter Nutzer von einem unbekannten Gerät aus auf sensible Daten zugreifen? Ist das Verhalten einer Anwendung plausibel im Abgleich mit der üblichen Nutzung? Adaptive Architekturen verknüpfen für die Antworten Telemetrie, Richtlinien und lernende Systeme.

KI als Treiber – und Bedrohung zugleich

Künstliche Intelligenz eröffnet dafür neue Möglichkeiten: Security-Systeme erkennen Muster, die Menschen entgehen würden, prognostizieren Angriffsverläufe oder isolieren ungewöhnliches Verhalten automatisch. Kurzum: KI-basierte Lösungen schützen proaktiv und automatisiert. Doch KI ist nicht nur Teil der Lösung – sie ist auch Teil des Problems. Angreifende setzen längst selbst generative Modelle ein, etwa für präziseres Phishing oder um Erkennungsregeln zu umgehen.

Fünf Phasen für echte Sicherheit

Um mit der aktuellen Bedrohungslage resilient umgehen zu können, heißt das für die Praxis: weg von Einzelmaßnahmen, hin zu einem vernetzten und souveränen Security-Ansatz, der Erkennung, Schutz, Überwachung, Reaktion und Wiederherstellung integriert.

ACP auf der it-sa 2025

Der Security Cycle von ACP zeigt, welche fünf Phasen zu einem strukturierten Prozess für nachhaltige, adaptive Sicherheit führen – einem Prozess, der hilft, Sicherheit dauerhaft beweglich zu halten.

Werner Schwarz | www.acp-gruppe.com

it-sa Expo&Congress
Besuchen Sie uns
in **Halle 7A-322**

USABLE SECURITY

MENSCHENZENTRIERTE CYBERSICHERHEIT

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) hat ein Whitepaper zum Thema „Usable Security – Handlungsfelder menschzentrierter Cybersicherheit" veröffentlicht. Es beleuchtet die Frage, wie Sicherheitsmechanismen in digitalen Produkten und Anwendungen stärker an den Bedürfnissen der Verbraucherinnen und Verbraucher und ihrem digitalen Alltag ausgerichtet werden können, um das IT-Schutzniveau grundsätzlich zu erhöhen.

Um dieses Ziel zu erreichen, zeigt das Whitepaper die Herausforderungen und Lösungsansätze für eine menschzentrierte Cybersicherheit auf. Dabei werden vier zentrale Handlungsfelder skizziert: Gebrauchstauglichkeit, Zugänglichkeit, Transparenz und Akzeptanz. In diesen Feldern veranschaulichen die Autorinnen und Autoren, wie Sicherheitsmechanismen so gestaltet werden können, dass sie für die Nutzenden verständlich, leicht bedienbar und akzeptabel sind, sicher angewandt werden können und zugleich effektiv sind. Jedes Handlungsfeld wird durch konkrete Gestaltungsprinzipien und praxisnahe Beispiele fundiert.

Das Whitepaper definiert Usable Security als zentrales Qualitätsmerkmal von digitalen Produkten und Anwendungen. Es bildet eine Blaupause und Grundlage zu deren Gestaltung und Bewertung. Die Publikation richtet sich an Akteure aus Politik, Wirtschaft, Wissenschaft und Zivilgesellschaft sowie an die Fachöffentlichkeit.

www.bsi.bund.de

WHITEPAPER
Usable Security

Wie VADs Mehrwerte schaffen

VOM HERSTELLER ÜBER DEN CHANNEL ZUM ENDKUNDEN

IT-Landschaften werden immer komplexer. Reseller, Dienstleister und ihre Kunden stehen deshalb zunehmend vor der Herausforderung, Lösungen zu finden, die technologisch ausgereift, wirtschaftlich tragfähig und nachhaltig betreibbar sind. Value Add Distributoren (VADs), wie Westcon-Comstor, spielen hier eine Schlüsselrolle: Sie bündeln marktführende Herstellerlösungen und ergänzen diese durch Services, die Partner dabei unterstützen, Endkunden mit spürbarem Mehrwert zu betreuen.

Vertriebliche Services mit direktem Kundeneffekt

Westcon-Comstor verbindet Vertriebsunterstützung mit klarer Kundenorientierung. Wer Cloud-Projekte umsetzen möchte, profitiert von der engen Anbindung an führende Marktplätze, wie z. B. Amazon Web Services (AWS). Partner erhalten nicht nur Unterstützung beim Zugang zur Plattform, sondern auch bei Angebotserstellung, Lizenzierung und Integration. Für Endkunden heißt das: Cloud-Strategien lassen sich schneller und risikoärmer realisieren – egal ob bei der Migration bestehender Systeme oder beim Aufbau neuer Anwendungen.

Noch stärker wirkt dieser Nutzen im Zusammenspiel mit weiteren Services. So senken etwa flexible Finanzierungsmodelle die Hürden für neue Investitionen und datengestützte Insights aus dem Westcon iD Programm helfen dabei, Kundenbedürfnisse präziser zu identifizieren. Im Rahmen der Professional Services stellt Westcon-Comstor zudem flexible technische Ressourcen und Beratungslösungen für anbieter- und technologieübergreifende Implementierungen während des gesamten Projektlebenszyklus bereit. Gemeinsam mit den Global Supply Chain Services stellen diese sicher, dass Projekte weltweit zuverlässig umgesetzt werden. Ergänzt durch eine Reihe von Marketing Services besteht ein durchgängiges Paket – von Beratung und Finanzierung bis zur Bereitstellung –, das sowohl für den Channel als auch für den Endkunden wertvolle Mehrwerte bietet.

Technische Services als Garant für erfolgreiche Projekte

Auch auf technischer Ebene profitieren Channel und Kunden vom integrierten Service-Ansatz. Im 3D Lab lassen sich Lösungen in Multi-Vendor-Umgebungen realitätsnah erfahren und kombinierte Anwendungsfälle demonstrieren, bevor sie beim Endkunden eingeführt werden. Das senkt Risiken und schafft Sicherheit in der Entscheidungsphase. Parallel bietet Tech Connex als Community-Forum wertvolle Impulse, die direkt in Projekte einfließen können.

Ein weiterer Baustein ist die Westcon Academy, die Fachkräfte mit herstellerzertifizierten Trainings ausstattet. So bleiben Partner-Teams stets auf dem neuesten Stand – und Endkunden profitieren von Projekten mit maximaler Expertise. Abgerundet wird dies durch Pre-Sales- und Post-Sales-Support, der den gesamten Projektlebenszyklus professionell begleitet.

Mit dieser Kombination aus Demoumgebungen, Schulungen und kontinuierlicher Unterstützung sorgt Westcon-Comstor dafür, dass Projekte nicht nur zuverlässig, sondern auch langfristig erfolgreich umgesetzt werden.

Nachhaltigkeit als strategischer Faktor

Westcon-Comstor hat es sich zum Ziel gesetzt, seine CO_2-Emissionen bis 2050 auf Netto-Null zu reduzieren – validiert durch die Science Based Targets initiative (SBTi). Dies unterstützt Partner dabei, auch ihre eigenen Klimaziele glaubwürdig zu untermauern.

Reseller und Dienstleister erhalten durch Westcon-Comstor die passenden Werkzeuge, Services und das Know-how, um ihre Kundenbeziehungen zu stärken. Für Endkunden bedeutet das: weniger Risiko, mehr Planungssicherheit, schnellere Ergebnisse und ein konkreter Beitrag zu mehr Nachhaltigkeit. So wird aus Distribution echter Mehrwert – entlang der gesamten Wertschöpfungskette.

www.westconcomstor.com

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

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

Strategisches IT Security Assessment

DER SCHLÜSSEL ZUR GANZHEITLICHEN CYBERSICHERHEITSSTRATEGIE

Unternehmen stehen vor der Herausforderung, komplexe IT-Infrastrukturen, regulatorische Anforderungen und eine dynamische Bedrohungslage miteinander zu vereinen. Ein strategisches IT Security Assessment bietet hierfür einen systematischen Rahmen: Es liefert Klarheit über den aktuellen Sicherheitsstatus, identifiziert Risiken und Schwächen und schafft die Basis für zukunftsfähige Entscheidungen.

Phasenmodell

Ein solches Assessment verläuft in mehreren ineinandergreifenden Phasen. Es beginnt mit einer präzisen Zieldefinition und einer klaren Abgrenzung des Untersuchungsrahmens. Hierbei wird festgelegt, welche Geschäftsbereiche, Systeme und Prozesse betrachtet werden sollen. Dieser Schritt ist entscheidend, um den Fokus richtig zu setzen und sicherzustellen, dass das Assessment strategisch relevante Aspekte erfasst. Auch regulatorische Anforderungen wie die NIS2-Richtlinie, branchenspezifische Standards oder interne Governance-Vorgaben fließen in diesen ersten Schritt ein.

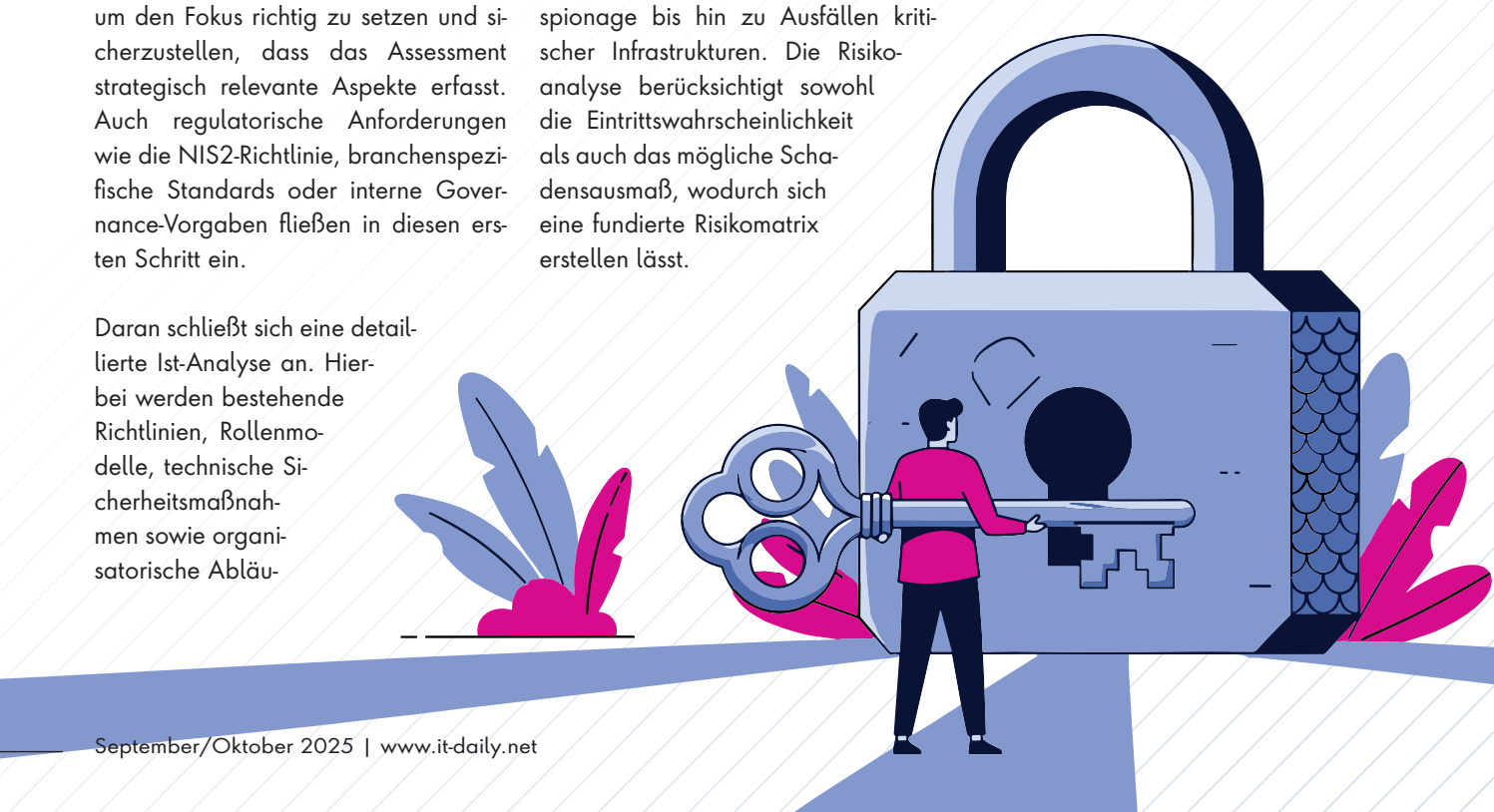
Daran schließt sich eine detaillierte Ist-Analyse an. Hierbei werden bestehende Richtlinien, Rollenmodelle, technische Sicherheitsmaßnahmen sowie organisatorische Abläufe erhoben und dokumentiert. Die Methoden reichen von Interviews mit Schlüsselpersonen über die Analyse von Richtliniendokumenten bis hin zur technischen Überprüfung von Konfigurationen oder der Netzarchitektur. Ziel ist es, ein möglichst vollständiges Bild der Sicherheitslandschaft zu zeichnen – sowohl auf strategischer als auch auf operativer Ebene.

Bedrohungs- und Risikoanalyse

Auf Basis dieser Informationen folgt eine umfassende Bedrohungs- und Risikoanalyse. Dabei werden potenzielle Bedrohungsszenarien identifiziert und deren Auswirkungen auf die Organisation bewertet. Je nach Unternehmensgröße und Branche stehen hier unterschiedliche Szenarien im Vordergrund - von Ransomware-Angriffen über Industriespionage bis hin zu Ausfällen kritischer Infrastrukturen. Die Risikoanalyse berücksichtigt sowohl die Eintrittswahrscheinlichkeit als auch das mögliche Schadensausmaß, wodurch sich eine fundierte Risikomatrix erstellen lässt.

Parallel dazu erfolgt eine Reifegradbewertung der vorhandenen Sicherheitsmaßnahmen. Diese orientiert sich häufig an etablierten Standards wie ISO/IEC 27001, dem NIST Cybersecurity Framework oder dem BSI IT-Grundschutz. Ziel ist es, das bestehende Sicherheitsniveau systematisch zu bewerten – von organisatorischen Strukturen über technische Schutzmechanismen bis hin zur Sicherheitskultur. Diese Analyse macht deutlich, wo Lücken bestehen, aber auch, welche Stärken ausgebaut werden können.

Auf dieser Basis werden konkrete Handlungsempfehlungen abgeleitet. Dabei geht es nicht nur um die technischen Maßnahmen, sondern auch um Fragen wie Verantwortlichkeiten, Schulungskonzepte oder In-



vestitionsprioritäten. Die Empfehlungen werden nach Wirkung, Aufwand und Umsetzbarkeit priorisiert. Neben kurzfristigen Quick Wins stehen dabei auch langfristige strategische Maßnahmen im Fokus, etwa der Aufbau eines ISMS oder die Einführung eines Zero-Trust-Modells.

Den Abschluss bildet ein umfassender Bericht, der sowohl die Erkenntnisse als auch die vorgeschlagenen Maßnahmen transparent darstellt. Dieser dient als Kommunikationsinstrument gegenüber der Geschäftsleitung, Aufsichtsorganen oder externen Prüfern. Besonders wertvoll ist die Ableitung einer konkreten Roadmap, die das Unternehmen über Monate hinweg strategisch begleitet – mit klaren Zielen, Meilensteinen und Verantwortlichkeiten.

Strategische vs. operative IT Security Assessments

Ein vollständiges IT Security Assessment muss sowohl strategische als auch operative Aspekte berücksichtigen. Während sich diese beiden Dimensionen ergänzen, unterscheiden sie sich fundamental in Fokus, Tiefe und Zielsetzung.

#1 Strategische Dimension

Das strategische Assessment betrachtet die IT-Sicherheit aus der Vogelperspektive. Im Mittelpunkt stehen langfristige Ausrichtung, Governance-Strukturen und die Einbettung der Cybersicherheit in die Unternehmensstrategie.

IN EINER ZUNEHMEND VERNETZTEN WELT IST IT-SICHERHEIT WEIT MEHR ALS NUR EIN TECHNISCHES THEMA. SIE IST EIN STRATEGISCHER ERFOLGSFAKTOR.

Ulrich Parthier, Publisher, it security, www.it-daily.net

Hier werden Fragen beantwortet wie: Entspricht die Sicherheitsstrategie den Geschäftszielen? Sind die Verantwortlichkeiten klar definiert? Wie ist das Unternehmen für zukünftige Bedrohungen aufgestellt?

Die strategische Betrachtung umfasst die Bewertung von Sicherheitsrichtlinien, die Analyse der Organisationsstrukturen im Bereich Cybersicherheit sowie die Prüfung der Integration von Sicherheitsaspekten in Geschäftsprozesse. Besonders relevant sind dabei regulatorische Compliance, Risikomanagement-Frameworks und die strategische Ressourcenplanung. Das Ergebnis sind langfristige Handlungsempfehlungen, die oft strukturelle Veränderungen oder Investitionen in neue Technologien und Kompetenzen beinhalten.

#2 Operative Dimension

Das operative Assessment hingegen fokussiert sich auf die konkrete Umsetzung und den täglichen Betrieb der Sicherheitsmaßnahmen. Hier geht es um die detaillierte Analyse einzelner Systeme, Prozesse und Kontrollen. Zentrale Fragen sind: Funktionieren die implementierten Sicherheitsmaßnahmen wie vorgesehen? Wo bestehen konkrete Schwachstellen? Wie effektiv sind die aktuellen Schutzmaßnahmen?

Die operative Betrachtung umfasst technische Penetrationstests, Vulnerability-Scans, die Überprüfung von Konfigurationen und die Analyse von Sicherheitsprozessen im Detail. Dabei werden konkrete Schwachstellen identifiziert, bestehende Kontrollen validiert und die Effektivität von Incident-Response-Prozessen bewertet. Das Ergebnis sind präzise, oft kurzfristig umsetzbare Maßnahmen zur Behebung identifizierter Sicherheitslücken.

Synergien zwischen Strategy und Operations

Strategische Prioritäten für operative Assessments:

- Ableitung konkreter Prüffelder aus strategischen Zielen
- Bewertung der operativen Umsetzung strategischer Vorgaben
- Identifikation von Lücken zwischen Strategie und Realität
- Validierung der Wirksamkeit strategischer Investitionen

Operative Erkenntnisse für strategische Planung:

- Feedback über die Praxistauglichkeit strategischer Konzepte
- Identifikation struktureller Schwächen durch operative Befunde
- Priorisierung strategischer Maßnahmen basierend auf akuten Risiken
- Ressourcenplanung auf Basis operativer Aufwände

Die größte Wirkung entfaltet ein Assessment, wenn beide Dimensionen systematisch verknüpft werden. Strategische Erkenntnisse informieren die operative Prüfung, während operative Befunde die strategische Ausrichtung validieren oder korrigieren. Nur durch diese Verzahnung entsteht ein realistisches und handlungsleitendes Gesamtbild der Sicherheitslage.

Assessment-Ansätze nach Unternehmensgröße

Die Durchführung eines IT Security Assessments muss an die spezifischen Gegebenheiten und Ressourcen des jeweiligen Unternehmens angepasst werden. Dabei unterscheiden sich Großunternehmen und mittelständische Betriebe nicht nur in der Komplexität ihrer IT-Landschaften, sondern auch in verfügbaren Budgets, personellen Ressourcen und regulatorischen Anforderungen.

Assessment-Schwerpunkte Großunternehmen

Bei Großunternehmen stehen Komplexitätsmanagement und Governance im Vordergrund. Dazu zählen:

- Multi-dimensionale Organisationsstrukturen mit verschiedenen Geschäftsbereichen
- Internationale Standorte mit unterschiedlichen regulatorischen Anforderungen
- Komplexe IT-Landschaften mit Legacy-Systemen und modernen Cloud-Infrastrukturen
- Ausgeprägte Compliance-Anforderungen durch Börsennotierung oder Branchenregulierung
- Etablierte Governance-Strukturen mit dedizierten Sicherheitsorganisationen

Das Assessment muss die Vielzahl an Standorten, Systemen und Stakeholdern berücksichtigen. Regulatorische Compliance spielt eine zentrale Rolle, da Großunternehmen oft strengeren Auflagen unterliegen und höhere Bußgelder riskieren. Die Herausforderung liegt in der Koordination verschiedener Bereiche und der Harmonisierung unterschiedlicher Sicherheitsstandards. Gleichzeitig verfügen Großunternehmen über spezialisierte Sicherheitsteams und höhere Budgets, was detailliertere und umfangreichere Assessments ermöglicht.

Das Assessment umfasst typischerweise eine tiefgreifende Analyse der Governance-Strukturen, die Bewertung konzernweiter Sicherheitsrichtlinien und die Prüfung der Wirksamkeit von Kontrollen über verschiedene Geschäftsbereiche hinweg. Besonders relevant sind dabei Themen wie Datenklassifizierung, privilegiertes Zugriffsmanagement und die Sicherheit von Cloud-Hybrid-Umgebungen.

Assessment-Schwerpunkte Mittelstand

Anders sehen die Schwerpunkte im Mittelstand aus. Dort zählen Effizienz und pragmatische Lösungen. Die Gründe hierfür sind:

- Begrenzte personelle und finanzielle Ressourcen
- Weniger spezialisierte IT-Sicherheitsexpertise intern verfügbar
- Fokus auf business-kritische Systeme und Prozesse
- Pragmatische Umsetzung von Sicherheitsmaßnahmen
- Höhere Abhängigkeit von externen Dienstleistern und Cloud-Services

Mittelständische Unternehmen benötigen Assessment-Ansätze, die ihre begrenzten Ressourcen optimal nutzen. Der Fokus liegt auf der Identifikation der kritischsten Risiken und der Entwicklung kosteneffizienter Lösungen. Da oft keine dedizierten Sicherheitsspezialisten vorhanden sind, muss das Assessment verständliche und umsetzbare Empfehlungen liefern. Die IT-Landschaft ist meist weniger komplex, aber dafür oft gewachsen und heterogen.

Das Assessment konzentriert sich auf die Absicherung geschäftskritischer Prozesse und Daten. Dabei werden praktikable Lösungen bevorzugt, die ohne großen Personalaufwand umsetzbar sind. Besonders relevant sind Themen wie Backup-Strategien, E-Mail-Sicherheit, Endpoint Protection und die sichere Nutzung von Cloud-Services. Die Empfehlungen müssen ein ausgewogenes Verhältnis zwischen Sicherheitsniveau und Wirtschaftlichkeit bieten.

Gemeinsame Herausforderungen - unterschiedliche Lösungsansätze

Beide Unternehmensgrößen stehen vor ähnlichen grundlegenden Herausforderungen wie Ransomware, Phishing oder Compliance-Anforderungen. Die Lösungsansätze unterscheiden sich jedoch erheblich. Während Großunternehmen

auf hochspezialisierte Tools und dedizierte Teams setzen können, müssen mittelständische Unternehmen auf standardisierte, leicht handhabbare Lösungen zurückgreifen.

Ein besonders wichtiger Unterschied liegt in der Behandlung von Risiken. Großunternehmen können sich umfassende Risikomanagement-Systeme leisten und haben oft die Ressourcen, auch geringere Risiken zu adressieren. Mittelständische Unternehmen müssen hingegen priorisieren und sich auf die kritischsten Bedrohungen konzentrieren. Dies erfordert eine andere Herangehensweise bei der Risikobewertung und -behandlung.

Die Kommunikation der Assessment-Ergebnisse muss ebenfalls angepasst werden. Während in Großunternehmen detaillierte technische Berichte für verschiedene Stakeholder erstellt werden können, benötigen Mittelständler kompakte, handlungsorientierte Zusammenfassungen, die auch von IT-Generalisten verstanden und umgesetzt werden können.

Fazit

Ein strategisches IT Security Assessment ist ein unverzichtbares Instrument für Unternehmen jeder Größe. Der Schlüssel zum Erfolg liegt in der angemessenen Balance zwischen strategischer Weitsicht und operativer Präzision sowie in der Anpassung an die spezifischen Gegebenheiten des jeweiligen Unternehmens. Nur durch diese maßgeschneiderte Herangehensweise können Organisationen eine Cybersicherheitsstrategie entwickeln, die sowohl ihren aktuellen Schutzzielen entspricht als auch zukunftsfähig bleibt.

Ulrich Parthier

IT-Security Assessments sind systematische Bewertungen des Informationssicherheitsniveaus einer Organisation. Sie helfen dabei, Risiken und Schwachstellen zu identifizieren, und bilden die Grundlage für Sicherheitsstrategien. Ein moderner Ansatz berücksichtigt sowohl strategische als auch operative Dimensionen und passt sich an die spezifischen Bedürfnisse verschiedener Unternehmensgrößen an.

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:
Christian Albrecht, Sneha Banerjee, Benedikt Bauer, Lars Becker, Stephan Fritsche, Subhalakshmi Ganapatahy, Fabian Glöser, Stefan Keller, Ismet Koyun, Frank Melber, Carina Mitzschke, Bill Munroe, Thomas Gertler, Wolfgang Huber, Grzegorz Nocon, Silvia Parthier, Ulrich Parthier, Adam Preis, Jochen Sandvoß, Martin Sawczyn, André Schindler, Kevin Schwarz, Werner Schwarz, Stephan Schweizer, Stefan Tiefel, Sebastian Weber

Anschrift von Verlag und Redaktion:
IT Verlag für Informationstechnik GmbH
Ludwig-Ganghofer-Str. 51, D-83624 Otterfing
Tel: 08104-6494-0,
Fax: 08104-6494-22

E-Mail für Leserbriefe: info@it-verlag.de
Homepage: www.it-daily.net

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

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

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

Anzeigenpreise:
Es gilt die Anzeigenpreisliste Nr. 32.
Preisliste gültig ab 1. Oktober 2024.

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

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

Erscheinungsweise: 6 x pro Jahr

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

Bankverbindung:
VRB München Land eG,
IBAN: DE90 7016 6486 0002 5237 52,
BIC: GENODEF10HC

Beteiligungsverhältnisse nach § 8, Absatz 3 des Gesetzes über die Presse vom 8.10.1949: 100 % des Gesellschafterkapitals hält Ulrich Parthier, Sauerlach.

Abonnementservice: Eva Neff,
Telefon: 08104-6494-15, E-Mail: neff@it-verlag.de

Das Abonnement ist beim Verlag mit einer dreimonatigen Kündigungsfrist zum Ende des Bezugszeitraumes kündbar. Sollte die Zeitschrift aus Gründen, die nicht vom Verlag zu vertreten sind, nicht geliefert werden können, besteht kein Anspruch auf Nachlieferung oder Erstattung vorausbezahlter Beträge.

CYBER-ANGRIFFE

TIPPS FÜR DEN SCHUTZ

Die Zahl und Heftigkeit der Attacken auf Unternehmen über das Internet steigen ständig. Herkömmliche Prozesse zur Wiederherstellung von Daten und Systemen funktionieren oft nicht mehr, da Backups oder Sicherheitsanwendungen zerstört sind. Zum Schutz vor solchen existenzgefährdenden Cyberangriffen sollten Unternehmen folgende Tipps beherzigen:

#1 Vorbereitet sein: Richten Sie ein abteilungsübergreifendes Sicherheitsteam ein.

#2 Proaktiv handeln: Informieren Sie sich über Ransomware-Banden und ihre Tools, Techniken und Verfahren (TTPs).

#3 Angriffsfläche reduzieren: Ermitteln und schließen Sie kritische Sicherheitslücken, insbesondere wenn sie wichtige Systeme betreffen oder häufig von Cyberkriminellen ausgenutzt werden.

#4 Backups schützen: Nutzen Sie Backup-Systeme, die von der produktiven Umgebung getrennt sind und unveränderliche Daten speichern.

#5 Ransomware-Schutz verstärken: Identifizieren Sie Sicherheitslücken auf Basis der von Ransomware-Banden genutzten ATT&CK-Techniken.

#6 Ransomware erkennen: Decken Sie Anomalien in der CPU- und Festplattennutzung auf sowie ungewöhnliche Netzwerkprotokolle, die von Ransomware-Banden verwendet werden.

#7 Schnell reagieren: Suchen Sie nach Staging-Umgebungen zur Datenexfiltration und isolieren Sie infizierte Hosts sämtlicher Netzwerke.

#8 Offen kommunizieren: Kommunizieren Sie mit internen Beteiligten und der Öffentlichkeit, um Gerüchte zu vermeiden.

Unternehmen sollten diese Tipps als Leitplanken für die Stärkung ihrer Cyber-Resilienz nutzen. Denn die wahre Stärke von Cyber-Resilienz liegt nicht in einer Standardlösung, sondern im Zusammenspiel von Menschen, Prozessen und Technologie.

www.cohesity.com

INSERENTENVERZEICHNIS


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

KOBIL

mPower™ by KOBIL

Deutschlands digitale Plattform für die Zukunft

- Sichere digitale Identität
- Digitale Vertragsunterzeichnung & Zahlung
- Vertrauenswürdige Kommunikation

KOBIL bei Gartner® 2025:
Einziger SuperApp-Anbieter Europas, gelistet in 8 Hype Cycles™

Alles in einer App. Alles in einem Wallet.

Für Behörden. Für Unternehmen. Für Start-ups.

GDPR · PSD2 · Privacy · eIDAS · OPEN BANKING EUROPE · CCPA READY · SWIFT

Über 5.000 Kunden vertrauen KOBIL Sicherheitstechnologie

Deutsche Telekom · AIRBUS · DATEV · COMMERZBANK · MIGROSBANK · SIEMENS

Engineered in Germany

KOBIL auf der it-sa: Halle 9 / 9-346

+49 (0) 6241 3004 0 · kobil.com · hello@kobil.com