INKLUSIVE 48 SEITEN
it security

it management

Der Motor für Innovation
März/April 2025

THOUGHT LEADERSHIP

AB SEITE 14

Aagon

DIE KÜHLREVOLUTION DER KI-ÄRA

Direct Liquid Cooling

Michael Nicolai, Rittal GmbH & Co.KG

RETRIEVAL AUGMENTED GENERATION

Unternehmensspezifische Chat-Applikationen

LLM BENCHMARKING

Die passende KI-Lösung finden

DATA READINESS ALS SCHLÜSSEL

In sechs Schritten die Datenbasis optimieren

www.it-daily.net

IT SECURITY DIGITALEVENT

WE SECURE IT

MITTWOCH 09. & DONNERSTAG 10.04.2025
AB 9UHR

#WesecureIT2025

Infos und Anmeldung

Eine Veranstaltung von itsecurity & it-daily.net

MACHINE INTELLIGENCE VS. HUMAN INTELLIGENCE

LIEBE LESERINNEN UND LESER,

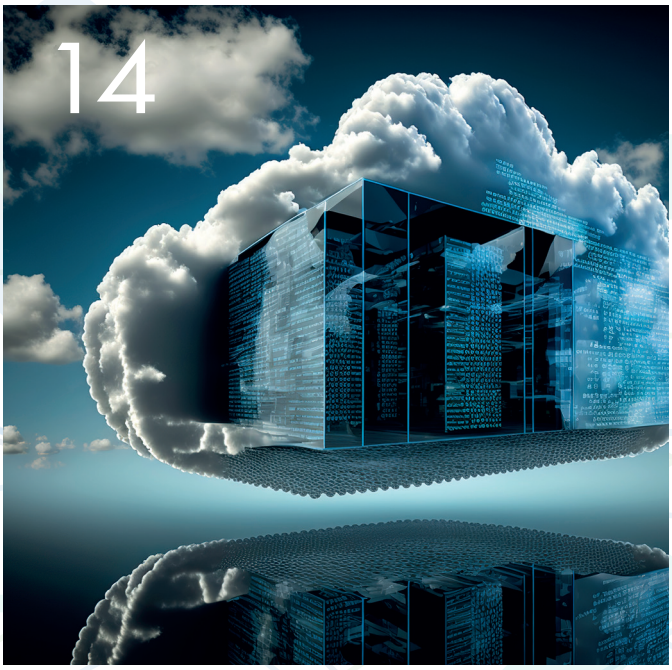
Künstliche Intelligenz überrascht uns manchmal mit ihrer Kreativität an unerwarteter Stelle. Diese als „Halluzinationen" bezeichneten Fehler zeigen, wie wichtig das Zusammenspiel von Mensch und Maschine bleibt – ein Phänomen, das uns täglich begegnet.

Kürzlich sollte eine KI eine Aufgabe für uns erledigen. Es ging um eine inhaltliche Zusammenfassung eines 16seitigen PDFs. Ein Detail kam meiner Kollegin irgendwie spanisch vor, wenn gleich es logisch klang. Also fragte sie dieses Detail bei der KI nach. Und, unglaublich, diese gestand ihren Fehler ein und korrigierte sich. Die KI hatte eine durchaus logische Schlussfolgerung gezogen, die aber so im Originaltext gar nicht stand.

Während die Systeme beeindruckende analytische Fähigkeiten zeigen, fehlt ihnen oft das kontextuelle Verständnis, das Menschen intuitiv mitbringen. Gerade im professionellen Umfeld, wird deutlich, dass KI ein Werkzeug ist – wenn auch ein sehr leistungsfähiges – das menschliche Expertise ergänzt, aber nicht ersetzt.

Das zeigt, ohne Zusammenspiel von Machine Intelligence und Human Intelligence geht es nach wie vor nicht und wir als Mensch sind als Kontrollinstanz notwendig. Aber ich bin mir sicher, viele dieser Kinderkrankheiten werden in den nächsten Jahren ausgemerzt und uns helfen, unsere Arbeit produktiver zu verrichten.

Ulrich Parthier
Publisher it management & it security



INHALT

Farblich hervorgehobene Artikel sind von der Redaktion als besonders lesenswert empfohlen

Inklusive 48 Seiten it security

GUT ZU WISSEN

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

TATORT WEBSITE

ANGRIFFSVERSUCHE NEHMEN WEITER ZU

MEHR WERT
Internet Security Report - Q3 2024

WatchGuard Technologies hat die Ergebnisse des neuesten Internet Security Reports veröffentlicht. Zu den wichtigsten Erkenntnissen gehört, dass die Zahl der Entdeckungen von Malware auf Endgeräten im Vergleich zum Vorquartal um 300 Prozent gestiegen ist. In dem Zusammenhang sticht vor allem die vermehrte Anzahl von Angriffsversuchen ins Auge, bei denen Cyberkriminelle mithilfe von Social-Engineering-Taktiken legitime Websites oder Dokumente für bösartige Zwecke missbrauchen. Bereits seit langem sind Microsoft-Dokumente wie Word und Excel ein beliebtes Mittel, um Benutzer zum Herunterladen von Schadsoftware zu verleiten. Inzwischen haben strenge Anti-Makro-Schutzmaßnahmen für Word-, Excel- und PowerPoint-Office-Dateien jedoch offensichtlich dazu geführt, dass Angreifer zur Verbreitung des Qbot-Trojaners für ein Remote Access Botnet nun OneNote-Dateien instrumentalisieren.

Zudem rückt die Ausnutzung von WordPress-Plug-in-Schwachstellen ins Zentrum der Betrachtung: Bedrohungsakteure versuchen immer öfter, die Kontrolle über bekannte Websites zu erlangen, um bösartige Downloads wie SocGholish zu hosten. Benutzer werden dann zur Aktualisierung ihrer Browser aufgefordert: Sobald dies erfolgt, kommt es zur Ausführung von Malware. Das Gefahrenpotenzial ist dabei keinesfalls zu unterschätzen: WordPress hostet weltweit mehr als 488,6 Millionen Websites, was 43 Prozent aller Websites im Internet entspricht.

Darüber hinaus kann das WatchGuard Threat Lab ein erhöhtes Risiko im Cryptomining-Umfeld belegen. Immer wieder kommt es zum Einsatz von Cryptominern. Die Malware ist darauf ausgelegt, sich auf dem Gerät des Benutzers zu verstecken und dessen Rechenressourcen zu nutzen, um Online-Währungen zu schürfen. Da Kryptowährungen an Wert und Beliebtheit gewinnen, ist auch Cryptomining-Malware wieder im Kommen.

„Die Ergebnisse des Reports für Q3 2024 zeigen eine dramatische Verschiebung zwischen traditionellen und fortschrittlichen Evasive-Malware-Bedrohungen", präzisiert Corey Nachreiner, Chief Security Officer, WatchGuard Technologies. „Es zeigt sich ganz klar, wie schnell sich die Bedrohungslandschaft weiterentwickelt. Deshalb ist es wichtig, umfassende, tiefgreifende Cybersicherheitslösungen einzusetzen, die klassische Bedrohungen schnell abfangen und sich in Echtzeit an neue anpassen können. Unternehmen jeder Größe sollten den Einsatz von KI-gestützter Bedrohungserkennung in Erwägung ziehen, um unerwartete Datenverkehrsmuster zu erkennen und die Verweildauer zu verkürzen, um letztlich die Kosten eines Angriffs zu reduzieren.

www.watchguard.com

WICHTIGE ERKENNTNISSE DES REPORTS

Anstieg von signaturbasierter Erkennung um 40%

Malware ist im Vergleich zum Vorquartal um 15% rückläufig

53% aller Malware-Angriffe fallen auf die Region EMEA

nur 20% der Malware entging den signaturbasierten Scanmethoden

300% tiger Malware-Anstieg auf Endgeräten

Gefährliche Neugier

DIE GRÖSSTEN RISIKEN IM NETZ

Beim Surfen im Netz sind fast 70 Prozent der befragten Arbeitnehmerinnen und Arbeitnehmer unvorsichtig und öffnen gefährliche Inhalte oder scannen unbekannte QR-Codes. Sie nehmen aus Neugierde das Risiko in Kauf, Opfer von Cyberkriminellen zu werden. Das belegt die aktuelle Studie „Cybersicherheit in Zahlen" von der G DATA CyberDefense AG, Statista und brand eins.

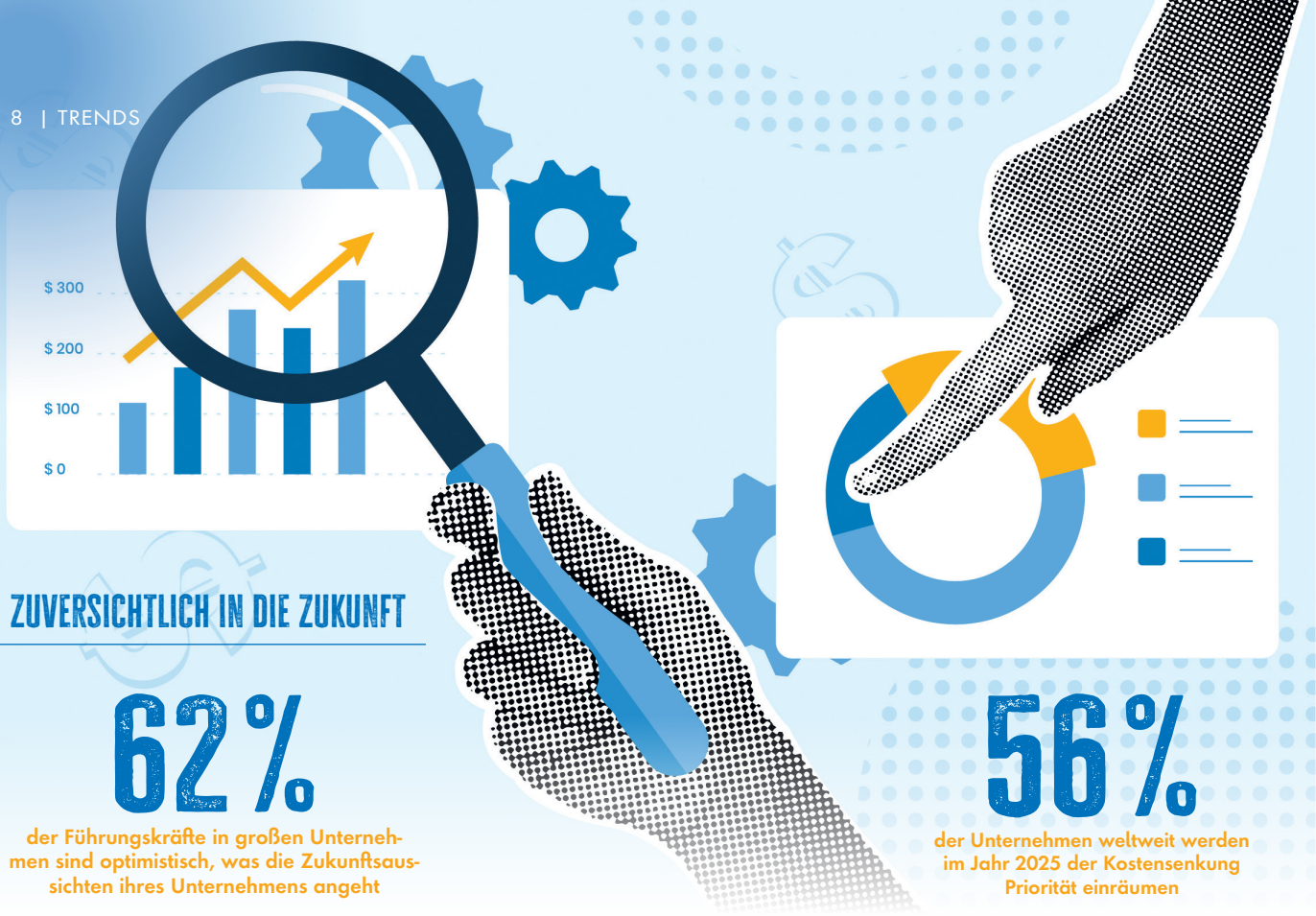
Doch unvorsichtiges Verhalten kann auch die IT-Sicherheit von Firmen gefährden. Auf dem ersten Platz der größten Risiken: Pop-up-Werbung, die beispielsweise mit falschen Gewinnspielen lockt. Das Fatale: Sie können Schadsoftware enthalten oder zu einer Phishing-Seite führen.

Fast ebenso viele Menschen (29 Prozent) öffnen unsichere Webseiten, die als seriöses Angebot getarnt sind. Einen ihnen unbekannten QR-Code, der manipuliert sein und auf eine betrügerische Seite weiterleiten könnte, scannten 22 Prozent der Befragten. Nur ein Drittel gab an, vorsichtig und für keine der angegebenen Gefahren empfänglich zu sein.

www.gdata.de

HABEN SIE SCHON MAL AUS NEUGIER FOLGENDE DINGE GEMACHT?

31 %	auf Pop-up-Werbung geklickt
29,4 %	eine potenziell unsichere Webseite oder Datei geöffnet
16,8 %	einen unbekannten Anhang an einer E-Mail geöffnet
15 %	einen unbekannten USB-Stick in ihren Computer gesteckt
16,9 %	einen fremden Link in einer E-Mail angeklickt
22,4 %	einen unbekannten QR-Code gescannt



ZUVERSICHTLICH IN DIE ZUKUNFT

62 %

der Führungskräfte in großen Unternehmen sind optimistisch, was die Zukunftsaussichten ihres Unternehmens angeht

56 %

der Unternehmen weltweit werden im Jahr 2025 der Kostensenkung Priorität einräumen

ZUNEHMENDER OPTIMISMUS

INVESTITIONSFOKUS AUF INNOVATION, EFFIZIENT UND RESILIENZ

Unternehmen schätzen ihre eigene Lage für 2025 trotz der anhaltenden Unsicherheiten im Marktumfeld in Summe positiver ein als noch im vergangenen Jahr. Trotz der Notwendigkeit zu Kostensenkungen führt dieser Optimismus zu höheren Investitionen, insbesondere in den Bereichen Kundenerlebnis, Lieferketten und Nachhaltigkeit. Ziel ist mehr Innovation, Effizienz, Wettbewerbsfähigkeit und Widerstandsfähigkeit zu erlangen. Das zeigt eine aktuelle Studie des Capgemini Research Institute mit dem Titel „Mit Zuversicht durch die Unsicherheit – Investitionsprioritäten für 2025".

MEHR WERT
Mit Zuversicht durch die Unsicherheit navigieren

62 Prozent der befragten Führungskräfte weltweit (Deutschland 69 %) äußern mit Blick auf ihr eigenes Unternehmen eine höhere Zuversicht für 2025, ein Anstieg von sechs Prozentpunkten gegenüber dem gleichen Zeitpunkt des Vorjahres und 20 Prozentpunkte über dem Wert von 2023 (+15 %-Punkte und +33 %-Punkte in Deutschland). Sie zeigen dabei mehr Vertrauen in ihre eigenen Organisationen als in den globalen Markt insgesamt. Was das globale Marktumfeld in den nächsten 12 bis 18 Monaten angeht sind nur 37 Prozent optimistisch. Dieser Wert liegt nur geringfügig über dem Vorjahreswert.

In einem unsicheren Marktumfeld gehen 56 Prozent davon aus, dass 2025 der Kostensenkung Vorrang vor dem Umsatzwachstum eingeräumt wird. Die Führungskräfte sind sich bewusst, dass dies Investitionen erfordert – die Hälfte gibt an, dass ihre Organisation plant, die Gesamtinvestitionen 2025 zu erhöhen, während knapp ein Viertel mit geringeren Investitionen im Vergleich zu 2024 rechnet und der Rest keine Veränderung erwartet.

Fokus auf Kundenerlebnis, Innovation und intelligentere Lieferketten

Ein Großteil der Zuversicht der Führungskräfte, weltweit wie auch in Deutschland, konzentriert sich weiterhin auf die beiden Bereiche Kundenerlebnis sowie Engineering/Forschung & Entwicklung/Innovation – wobei fast acht von zehn in ersteres und fast drei Viertel der Führungskräfte in das zweite Feld mehr investieren möchten als im Vorjahr. Am stärksten nahm der Anteil von Unternehmen mit mehr Investitionen im Bereich der Umgestaltung der Lieferkette zu: 63 Prozent geben an, dass sie ihre Ausgaben im Jahr 2025 erhöhen werden – im Jahr 2024 war es weniger als die Hälfte. Der Zuwachs liegt im Schnitt bei 9,4 Prozent. Lieferketten der neuen Generation werden KI und IoT integrieren, um die Effizienz zu steigern, Müll zu reduzieren und die Nachhaltigkeitsziele eines Unternehmens zu unterstützen. Als positive Effekte kommen eine bessere Entscheidungsfindung und eine gesamthafte Kostenreduzierung hinzu.

www.capgemini.com

Digitale Gesundheit?

DEUTSCHE UNTERNEHMEN AUF EINEM GUTEN WEG

Zoho hat europäische Unternehmen zu ihren Erfolgen und Herausforderungen bei der digitalen Transformation befragt.

Der Begriff „Digitale Gesundheit" vereint verschiedene Aspekte der digitalen Transformation – von generellen Erfolgen bis konkreten Meilensteinen sowie dem Einsatz von Technologien und Tools.

Die deutschen Ergebnisse im Detail

Ein Drittel (33 %) der befragten Unternehmen hatte 2024 eine gute digitale Gesundheit, 32 Prozent eine durchschnittliche und 35 Prozent eine schlechte. Damit kann Deutschland im Vergleich zum letzten Jahr in der Kategorie der als gut eingestuften Unternehmen ein Plus von 8 Prozentpunkten verzeichnen.

Im Vergleich zum Jahr davor zeigen die Ergebnisse auch, dass sich die meisten Indikatoren für digitale Gesundheit in allen Branchen verbessert haben. So sehen Befragte aus Deutschland etwa KI am ehesten als entscheidend an und profitieren bereits von den Vorteilen (52 %). Auch die Cloud ist weiterhin eine zentrale Technologie – so gaben 60 Prozent der befragten deutschen Führungskräfte an, dass ihr Unternehmen zwei bis drei Cloud-Plattformen nutzt.

44 Prozent der deutschen Befragten gaben an, dass sie mindestens die Hälfte ihrer Geschäfte mit digitalen Hilfsmitteln abwickeln, was einem Anstieg um 10 Prozentpunkte im Vergleich zum Vorjahr entspricht. Der Anteil der Unternehmen, die den größten Teil ihres Geschäfts mit digitalen Hilfsmitteln abwickeln, blieb mit 29 Prozent unverändert, während 16 Prozent bei weniger als der Hälfte der Aufgaben zu digitalen Hilfsmitteln greifen. Die digitale Transformation ist aber immer noch eine Herausforderung, bei der fast 9 von 10 (88 %) der befragten Unternehmen in Deutschland auf Probleme gestoßen sind. Die am häufigsten genannten: Der Aufwand, digitale Tools erfolgreich zu implementieren, war höher als erwartet (34 %), externe Hilfe oder Ressourcen mussten in Anspruch genommen werden, damit digitale Tools besser zusammenarbeiten (34 %) und fehlende Inhouse-Expertise, um Tools richtig einzusetzen (30 %).

www.zoho.com

ES BESTEHT NOCH HANDLUNGSBEDARF

33 % können als digital gesund eingestuft werden

88 % haben Probleme bei ihrer digitalen Transformation

77 % haben ihre Digitalisierungsziele erreicht

50 % sehen in KI die entscheidende Rolle bei der Digialisierung

Direct Liquid Cooling

DIE KÜHLREVOLUTION DER KI-ÄRA

Die Industrie befindet sich in einer Transformation: Künstliche Intelligenz wird immer mehr Teil der Automatisierung. Industrielle KI-Anwendungen sind das Top-Thema der kommenden Hannover Messe. Bei Rittal und Eplan geht es in Hannover nicht nur um die Perspektiven durch Einsatz von KI im Engineering, sondern auch um die Grundlagen der OT in Rechenzentren für KI-Anwendungen. Michael Nicolai, Vertriebsleiter IT Deutschland bei Rittal, erläutert, warum Direct Liquid Cooling als Enabling Technology schnell Einzug in die Datacenter halten muss und wie das funktionieren kann.

it management: *Herr Nicolai, was hat Rittal bewogen, ein IT Infrastruktur-Thema zu einem der Ausstellungs-Highlights einer Industriemesse zu machen?*

Michael Nicolai: Die Industrie steht bekanntermaßen unter hohem Druck. Die wirtschaftliche Situation und weltpolitische Lage bei anhaltendem Fachkräftemangel hierzulande erschweren das dringend benötigte Wachstum. Deep Tech und die industriespezifische Anwendung von KI in der datengetriebenen ‚Industrial Automation' sind wichtige Schlüssel, um in Zukunft mit Know-how ‚Made in Europe' noch Wachstum im harten internationalen Wettbewerb zu erzielen. Daher wird eine Vielzahl von KI-Anwendungen die Messe prägen.

Mit Eplan und Partnern geben wir beispielsweise einen Ausblick, was das für den Steuerungs- Schaltanlagen- und Maschinenbau bedeutet – eines unserer Messe-Highlights für die Industrie. Klar ist aber: Je breiter KI zum Einsatz kommen soll, desto schneller müssen wir auch die Rechenzentren ausbauen und ertüchtigen. KI und High Performance Computing heben die Leistungsdichte auf ein Level, das Neuland bei der gesamten Infrastruktur in Rechenzentren erfordert, insbesondere bei der Kühlung. Hier kommt die jahrzehntelange Erfahrung von Rittal im Bereich der IT-Infrastruktur vom Enterprise- und Colocation-Rechenzentrum bis zur Rolle als Single Source Supplier der Hyperscaler zum Tragen.

it management: *Worin genau besteht das technologische Neuland beim IT-Cooling?*

Michael Nicolai: Bisher wird die Wärme direkt an den Chips vorwiegend mit Luft abgeführt. Direkte Flüssigkühlung war lange eher eine Nischenanwendung, obwohl sie schon lange manche Vorteile bot. Jetzt wird sie fast schlagartig unausweichlich. Denn bei IT-Cooling gelten physikalische Grenzen, die nun überschritten werden. Bis etwa 30kW Leistung pro Rack kann Luft ausreichend Wärme abführen. Aber KI-Anwendungen werden schon bald über 150 kW erfordern. Hier hilft nur die direkte Kühlung der GPUs mit Flüssigkeit. Hersteller wie Nvidia legen ihre neuesten GPUs schon dafür aus. Rittal hat daher in Abstimmung mit Hyperscalern und Server-OEMs eine kompakte, modulare Coolant Distribution Unit (CDU) entwickelt, die den Weg für KI-Anwendungen bereitet. Im kompakten Rack-Format bringt sie auf Basis von Wasser mit Single Phase Direct Liquid Cooling über 1 MW Kühlleistung.

Wenn solche Lösungen in der Praxis Fuß fassen sollen, reicht es aber nicht, nur die Lösung mit der hohen Kühlleistung ins Datacenter zu stellen. Wichtig war uns, schon bei der Entwicklung gleich das Handling im Betrieb mitzudenken. Trotz neuer Technologie sollte sich das System mit möglichst gewohnten Abläufen servicieren lassen. In unsere Entwicklung sind die Impulse unserer globalen Großkun-

Die neue Cooling Distribution Unit kühlt über 1 Megawatt. Ihr Rack-Konzept mit Modulen im Server-Format sorgt für einfaches Handling und Service.
(Quelle: Rittal)

> WENN DIRECT LIQUID COOLING IN DER PRAXIS FUSS FASSEN SOLL, REICHT ES NICHT, NUR DIE LÖSUNG MIT DER HOHEN KÜHLLEISTUNG INS DATACENTER ZU STELLEN.
>
> **Michael Nicolai, Vertriebsleiter IT Deutschland, Rittal GmbH & Co.KG, www.rittal.com**

den und die langjährigen Erfahrungen von Rittal in IT und Industrie eingeflossen – 20 Jahre HD-IT-Cooling und über drei Jahrzehnte Klimatisierung von Steuerungen, Schaltungen und Maschinen unter schwierigsten Industrie-Bedingungen.

it management: *Wie wird die neue Technologie für die RZ-Betreiber besser beherrschbar?*

Michael Nicolai: Wir setzen auf Modularisierung und das standardisierte Open Rack V3, dessen Entwicklung Rittal im Open Compute Project (OCP) vorangetrieben hat: Die Stromversorgung erfolgt über die standardisierte DC Busbar im Rack. Nach diesem Vorbild wird der Server auch mit Anschlüssen im Rack an den zentralen Wasserkreislauf gekoppelt. Funktionseinheiten der CDU wie die Controller Unit und mehrere Kühlmittel-Fördereinheiten (CCUs) sind vollständig modular. Vorteil beim Service: Die Einschübe können wie Server gezogen werden – und zwar per „Hot Swap" im laufenden Betrieb.

Außerdem setzen wir auf Vielfalt bei der Einbindung ins Rechenzentrum. Die höchste Leistung erbringen die Liquid-to-Liquid-Versionen, welche die Wärme über einen Wärmetauscher an einen Facility-Wasserkreislauf abgeben. Die Wassertemperaturen bei dieser Lösung eignen sich auch gut für Wärmerückgewinnung – dringend nötig, um den CO_2-Footprint zu senken.

Für einen einfacheren Start bietet Rittal auch Liquid-to-Air-Versionen an, die ohne Facility-Wasseranschluss auskommen. Auch beschränken wir uns nicht auf das Open Rack V3 in 21 Zoll der ersten Versionen. Es folgen noch Varianten für unsere VX IT Racks in 19 Zoll. Die volle Integration in die Rittal Systemplattform ist ein relevanter Hebel, um die nötige Infrastruktur für AI-Anwendungen großflächig auszurollen.

it management: *Welche Lösungen eignen sich für welche Umgebung?*

Michael Nicolai: Die leistungsstarke Liquid-to-Liquid-Lösung mit 1 MW Kühlleistung war schon bei der ersten Preview ein Publikumsmagnet. Solche Installationen werden vor allem Hyperscaler und große Colocator als Technologietreiber in hoher Stückzahl einsetzen. Vorher werden sie aber ausgiebig testen. Es sind noch viele weitere Fragen zu klären. Worauf kommt es bei der Verrohrung für den gebäudeseitigen Primärkreislauf an? Was ändert sich durch die hohe Leistungsdichte bei der Stromverteilung? Wie wirkt sich Direct Liquid Cooling auf den Service im Betrieb und letztlich das gesamte Rechenzentrum aus? Auch dafür bringen wir unsere Erfahrungen ein und kennen die passenden Anbieter.

Die Ansätze der internationalen Hyperscaler werden mittelfristig wohl die Standards setzen. Darauf kann die agile Colocation-Branche aber nicht warten. Die meisten Colocator sind hochgradig kundenorientiert und wollen schon jetzt ihren Kunden schnellstmöglich gute Voraussetzungen für KI und HPC bieten. Hier kommen die Liquid-to-Air-Versionen ins Spiel, welche die Prozessoren direkt mit einem geschlossenen Wasserkreislauf im Rack und CDU kühlen, aber die Wärme dann über die Rücktür oder Seitenkühler an die Luft im Rechenzentrum abgeben. Sie erreichen zwar nicht die Kühlleistung und Effizienz der Liquid-to-Liquid-Lösungen, aber können schneller in RZ ohne externen Anschluss an den Facility-Wasserkreislauf eingesetzt werden. Mit Ihnen können Colocator eigene Tests mit weniger Aufwand und Investition bewerkstelligen oder für ihre Kunden einzelne „HPC-Inseln" in luftgekühlten RZ schaffen.

Damit haben die Liquid-to-Air-Versionen eine Hebel-Funktion, um Direct Liquid Cooling als Enabling Technology für KI überhaupt in die Rechenzentren zu bringen. Anbieter wie Rittal sowie Planer, Projektentwickler und die Anwender müssen jetzt schnell ihr Know-how zusammenbringen, um die Umbrüche im Gesamtsystem der Rechenzentren mit ‚Best Practices' zu vereinfachen. Dazu arbeiten wir eng mit großen Rechenzentrums-Entwicklern zusammen und installieren kurzfristig eine Teststellung unter realen Bedingungen im Einsatz für ein physikalisches Forschungsinstitut.

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

STRATEGIE ALS PRAXIS

BUSINESS-AGILITÄT UND RESILIENZ DURCH KONSEQUENTES HANDELN IM JETZT

Strategie als Praxis
Business-Agilität und Resilienz durch konsequentes Handeln im Jetzt;
Boris Gloger;
Carl Hanser Verlag GmbH & Co.KG; 06-2025

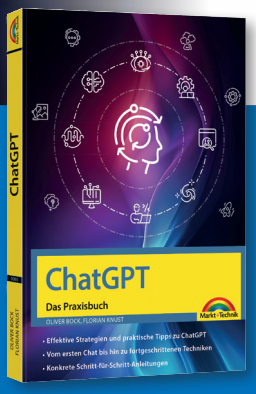
„Agile Strategieentwicklung" bietet einen umfassenden und innovativen Ansatz zur modernen Unternehmensführung. Es verbindet systemisches Denken mit agilen Methoden und betont die Notwendigkeit eines Paradigmenwechsels. Durch die Integration von Konzepten wie Antifragilität und kontinuierlichem Lernen bietet das Buch eine zukunftsfähige und anpassungsfähige Strategieentwicklung, die den Anforderungen der heutigen Geschäftswelt gerecht wird.

CHATGPT

DAS PRAXISBUCH

KI entwickelt sich rasant weiter und bietet immer neue Möglichkeiten und Anwendungen. In ihrem brandneuen Handbuch führen Oliver Bock und Florian Knust die Leser durch die faszinierende Welt von ChatGPT. Sie zeigen aktuelle Trends und Fortschritte auf und bieten einen umfassenden Überblick über die Funktionen und Einsatzmöglichkeiten von ChatGPT.

Dieses Buch ist ein Must-have für jeden, der das volle Potenzial von ChatGPT ausschöpfen möchte. Mit Schritt-für-Schritt Anleitungen und praxisnahen Beispielen machen die Autoren die komplexe Materie auch für Einsteiger verständlich. Der praktische Teil stellt verschiedene Nutzungsszenarien vor und zeigt, wie ChatGPT in den Alltag integriert werden kann.



ChatGPT
Das Praxisbuch,
Oliver Bock, Florian Knust;
Markt+Technik Verlag GmbH, 12-2024

HYBRIDES UNIFIED ENDPOINT MANAGEMENT

Die dezentrale und heterogene Gerätelandschaft in Unternehmen stellt das IT-Management vor neue Herausforderungen. Mit der steigenden Menge verschiedener Endgeräte und Betriebssysteme wächst die Komplexität der Administration erheblich.

Unified Endpoint Management (UEM) bietet hier einen zukunftsweisenden Ansatz. Als strategische Lösung ermöglicht es die zentrale Verwaltung sämtlicher Endpunkte – von klassischen Desktops über mobile Devices bis hin zu Cloud-Workloads. Dabei verschmelzen die Grenzen zwischen traditionellem Client Management und mobilem Device Management zusehends.

Das hybride UEM vereint nun beide Welten und unterstützt Unternehmen dabei, diese Komplexität effizient zu beherrschen. Dies gewährleistet nicht nur operative Effizienz, sondern auch die erforderliche Compliance und Sicherheit im hybriden Arbeitsumfeld, während gleichzeitig die Produktivität gesteigert wird.

Hybrides UEM

DIE OPTIMALE LÖSUNG FÜR ALLE ENDGERÄTE

Client Management heißt die seit langem bekannte Kategorie von Softwarelösungen zur zentralisierten, strukturierten und automatisierten Verwaltung von Endgeräten wie PCs, Servern und mobilen Devices mit Windows- oder Linux-Betriebssystemen. Mittlerweile hat sich anstelle dessen der Begriff „Unified Endpoint Management" (UEM) durchgesetzt. Das hat mehrere Gründe.

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

Erweiterter Fokus:
Cloud-UEM und mobile Endgeräte

Dies bedeutet: Mit gleichbleibender Personalstärke müssen Administrationsabteilungen Systeme aktuell halten und auf Schwachstellen reagieren. Sie müssen dabei den Datenschutz im Auge behalten (Wo darf ich sensible Infrastruktur- und Nutzerdaten ablegen?) sowie ISO-Normen und gesetzliche Regularien erfüllen. So erfordern etwa NIS2 und DORA zusätzliche Dokumentationen und Vorkehrungen.

Der traditionelle Ansatz, Client beziehungsweise Unified Endpoint Management rein on-premises zu betreiben, wird diesen veränderten Anforderungen nicht mehr gerecht. Die Entwicklung führte daher von lokal betriebenen Lösungen über „Mobile Device Management" hin zu cloud-basierten UEM-Systemen. Microsoft Intune ist eines der prominentesten Beispiele für diesen Trend, schon allein deshalb, weil es Bestandteil des Microsoft 365 E3-Enterprise-Lizenzvertrags ist.

On-Premises:
Hohe Funktionalität und Datenschutz

On-Premises-UEM-Systeme bieten zahlreiche Vorteile. Sie werden auf eigenen Servern betrieben – sei es lokal oder in einer Private Cloud – und verfügen über spezialisierte Agenten, die eine umfassende Kontrolle ermöglichen. Microsoft-Dienste (WSUS-Alternative, Defender, BitLocker) lassen sich nahtlos integrieren, ohne auf eine Cloud-Anbindung angewiesen zu sein.

WIE EINE HYBRIDE STRATEGIE AUSSIEHT UND WO DIE SCHWERPUNKTE ZU SETZEN SIND, DARÜBER SOLLTE SICH JEDES UNTERNEHMEN GEDANKEN MACHEN.

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

Ein entscheidender Vorteil ist die Datenhoheit (beim Betrieb eigener Server): Sensible Informationen verbleiben innerhalb der eigenen Infrastruktur und werden nicht für KI-Trainingszwecke verwendet, was in der Cloud immer geschehen kann. Künstliche Intelligenz ist ein wichtiges und zukunftsrelevantes Thema, aber dass vertrauliche Daten von einer GenAI verwendet werden, wird dann doch niemand wollen. Gleichzeitig ist beim lokalen Betrieb der rechtliche Aufwand geringer. Datenverarbeitungsverträge mit Dienstleistern müssen nicht aufwändig verhandelt werden bzw. beschränken sich auf die eigentliche Geschäftsbeziehung und eben nicht auf Firmen- oder Kundendaten.

Eine lokale UEM-Lösung macht das Unternehmen desweiteren unabhängig von Internet- oder Serverstörungen des Cloud-Anbieters; die eigene Infrastruktur bleibt steuerbar. Sie ist auch im Hinblick auf Compliance oft die bessere Wahl. Strenge Vorgaben in sicherheitskritischen Bereichen, die Unabhängigkeit vom Internet vorschreiben – etwa im Umfeld von KRITIS und NIS2 – lassen sich mit On-Premises-Systemen besser umsetzen. Sie sind bei Unternehmen, die in diesem Bereich etwas tun müssen, daher die bevorzugte Betriebsform.

Zudem lassen sich mit einer (mandantenfähigen) UEM-Lösung im eigenen Haus Sicherheitszonen individueller konfigurieren als bei einem Cloud-System „von der Stange". Komplexe Infrastrukturen (Standorte, Arbeitsbereiche) sind über die Lösung verwaltbar, in einem Mix aus online (Verwaltungsabteilungen inkl. Homeoffice) und offline (Produktion, eigene Abteilung & Netz). Mit Low-Code/No-Code werden vorgefertigte Bausteine

EINE LOKALE UEM-LÖSUNG MACHT UNTERNEHMEN UNABHÄNGIG VON INTERNET- ODER SERVER-STÖRUNGEN DES CLOUD-ANBIETERS – DIE EIGENE INFRASTRUKTUR BLEIBT STEUERBAR.

zur Desktop Automation flexibel variiert, bis hin zu Formularen (die auch ohne Internet verfügbar sind).

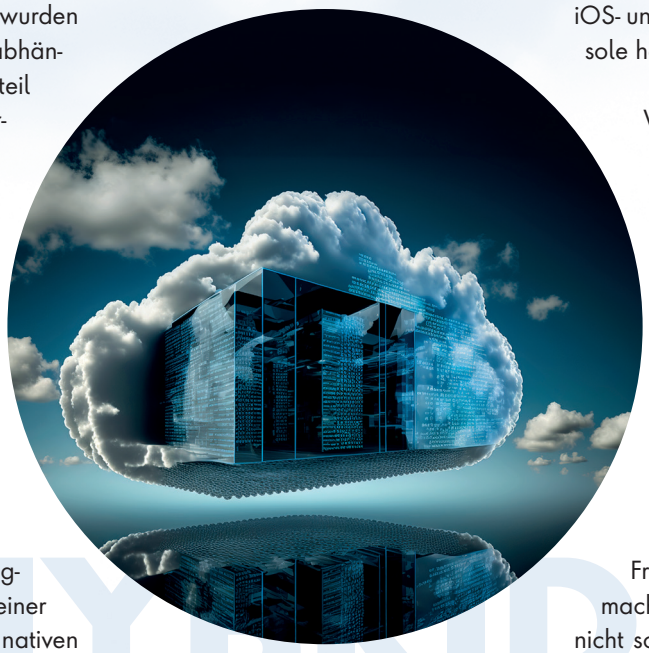
Auf der anderen Seite sind On-Premises-Lösungen mit Investitionen in Hardware und Lizenzen verbunden. Skalierungsprozesse erfordern Zeit und finanzielle Ressourcen. Und die nur eingeschränkte Unterstützung mobiler Endgeräte erweist sich in einer zunehmend mobilen Arbeitswelt inzwischen als Nachteil.

Cloud-UEM: Flexibel, skalierbar, aber mit Einschränkungen

Cloud-basierte UEM-Systeme wurden entwickelt, um Endgeräte ortsunabhängig zu verwalten. Ihr größter Vorteil liegt in der einfachen Skalierbarkeit, der ständigen Aktualisierung und dem Wegfall eigener Infrastrukturkosten. Administrationsaufwände werden minimiert, da sich Wartung und Updates automatisiert über den Cloud-Anbieter regeln.

Eine Bequemlichkeit, die wiederum andere Herausforderungen bereithält: Unternehmen sind stärker abhängig von der Verfügbarkeit der Cloud-Plattform und einer stabilen Internetverbindung. Die nativen Verwaltungsfunktionen eines Client-Betriebssystems sind häufig nur eingeschränkt nutzbar oder nicht mit anderen Systemen vernetzt. Ein Cloud-UEM setzt meist auf die mobile Schnittstelle des Geräts, die im Vergleich zu einem lokalen Agenten deutlich weniger Steuerungsmöglichkeiten bietet. Weist man einem Gerät oder einer Gruppe von Geräten ein Software-Update zu, bleibt nur abzuwarten. Der Zeitpunkt lässt sich nicht beeinflussen, da der Cloud-Anbieter eigenständig entscheidet, wann Sicherheitslücken geschlossen oder Updates ausgerollt werden. Eingriffe wie das Sperren von Ports sind nur begrenzt möglich.

Das Beispiel Intune zeigt die Stärken und Schwächen einer cloud-basierten Lösung. Microsofts Tool bietet mit Funktionen wie der Verteilung von Exe- und MSI-Dateien oder der Gerätesperrung eine solide Grundlage für das Management mobiler Endgeräte. Doch die Grenzen werden schnell sichtbar: Server lassen sich nur mit Zusatz-Tools verwalten, SNMP-Geräte bleiben außen vor, es sei denn, Unternehmen investieren in kostenpflichtige Erweiterungen. Dadurch erhalten Administratoren oft nur einen unvollständigen Überblick über ihre IT-Infrastruktur, was sowohl Sicherheitsrisiken als auch Ineffizienzen begünstigt.



Unternehmen brauchen eine Hybrid-Strategie für das Endgerätemanagement

Der vielversprechendste Ansatz liegt in einer hybriden Strategie: Die Kombination aus Cloud-UEM und On-Premises-Management vereint die Stärken beider Welten. Unternehmen können dadurch sowohl lokale als auch mobile Endgeräte effizient verwalten und sind zugleich weniger anfällig für Ausfälle. Ein Teil der Geräte ist meist immer erreich- und verwaltbar, egal ob der eigene Server ausfällt oder die Cloud.

Geräte- und Benutzer-Gruppen werden bei einem Hybrid-Ansatz aus der Cloud-Lösung in das (führende) On-Premises-UEM überführt und sind darin sichtbar. iOS- und Android-Devices, die das UEM sonst höchstens inventarisiert, lassen sich so viel detaillierter managen. Es werden außerdem mehr Inventarinformationen als bisher in das UEM transferiert. Damit hat die Administrationsabteilung eine Übersicht darüber, welche Geräte nur von der Cloud-Lösung gemanagt werden und welche ausschließlich vom On-Premises-UEM. Resultat ist eine neue Form der Nachverfolgbarkeit in bisher nicht gekannter Detailtiefe. Auch lassen sich sämtliche Arten von Apps an Android-, iOS- und Windows-Geräte aus einer Konsole heraus verteilen.

Wie eine hybride Strategie aussieht und wo die Schwerpunkte zu setzen sind, darüber sollte sich jedes Unternehmen Gedanken machen. Es hängt ganz davon ab, welche Devices man im engeren Zugriff haben möchte. In vielen Fällen ist eine Cloud-Anbindung schlicht ein unnötiger Umweg, wie bei Clients im Büro/Headquarter mit eigenem Serverraum. Relevant ist auch die Frage, wieviel Arbeit die Geräte machen. Smartphone müssen sicher nicht so engmaschig überwacht und gepatcht werden wie Notebooks. Und sie können auch mal ein paar Stunden nicht erreichbar sein, ohne das größere Ausfälle oder Leerläufe drohen.

Obwohl hybride Architekturen eine gewisse Komplexität mit sich bringen, lassen sie sich durch geschickte Integration (will heißen, diese bleibt auf zwei Systeme beschränkt) überschaubar halten. Ein Beispiel für eine gelungene Hybrid-Integration ist Aagon: Das Unternehmen bietet bereits eine Anbindung an Intune über einen Connector und entwickelt derzeit eine weitergehende Integration, die Cloud- und On-Premises-UEM nahtlos verbindet und damit eine ganzheitliche Verwaltung der Client-Infrastruktur ermöglicht.

Sebastian Weber

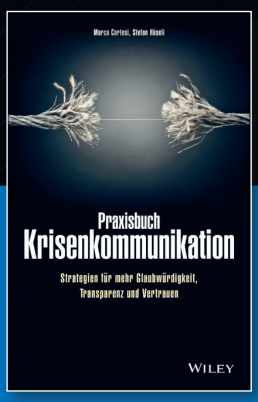
EFFEKTIVE KOMMUNIKATION IN HERAUSFORDERNDEN ZEITEN

EIN NEUER LEITFADEN FÜR VERSCHIEDENE FORMEN DER KRISE

Die Kommunikationslandschaft hat sich massiv verändert: Nicht nur Social Media und Tempo sind veränderte Faktoren, sondern auch neue Arten von Krisen sind entstanden. Das bringt Unternehmen, öffentliche Hand und deren Führungskreise oft genug in schwierige Lagen. Gerade in Krisensituationen ist es entscheidend, richtig zu reagieren. Zwar gibt es Beispiele aus der Praxis, in denen dank guter Kommunikation trotz so mancher Panne unterm Strich das Image gewinnt. Doch das Gegenteil ist leider immer häufiger zu beobachten.

Zwei Fachleute, die sich schon länger dem Thema widmen, haben dazu nun den passenden Leitfaden veröffentlicht: Stefan Häseli, der Schweizer Experte für glaubwürdige Kommunikation hat sich dafür einmal mehr mit Mario Cortesi, seines Zeichens Pressesprecher und bekanntes Gesicht der Stadtpolizei Zürich zusammengetan. In ihrem aktuell veröffentlichten Buch nehmen sie den Leser mit in die komplexe Welt der Krisenkommunikation. Theoretische Grundlagen werden mit praktischen Anwendungs- und Fallbeispielen verbunden.

Wie lassen sich Botschaften klar und vertrauensvoll gestalten? Welche Rolle spielen Ehrlichkeit und Transparenz? Wie geht man um mit zunehmendem Tempo in der Kommunikation und mit sozialen Medien, die offizielle Kanäle unter Druck setzen? Wie wird man den Erwartungen der Öffentlichkeit gerecht? Und was ist zu tun mit Menschen, die dünnhäutiger geworden sind und weniger Loyalität gegenüber Unternehmen und anderen Institutionen zeigen?



Praxisbuch Krisenkommunikation – Strategien für mehr Glaubwürdigkeit, Transparenz und Vertrauen; Marco Cortesi, Stefan Häseli, Wiley-VCH, 02-2025

Digitalisierung bezahlbar gestalten

STRATEGIEN FÜR EFFIZIENTE MICROSOFT-LIZENZIERUNG

Es gibt wohl kein Industrieunternehmen, das nicht dem digitalen Wandel unterliegt – und damit hohen finanziellen Belastungen. Damit neben KI, IoT und smarten Datenanalysen nicht auch noch die Lizenzierung teuer zu Buche schlägt, begleitet der Microsoft Solutions Partner VENDOSOFT Unternehmen durch den Wandel. Die beste IT-Strategie kann laut Geschäftsführer Björn Orth Cloud, On-Premises oder hybrid sein. Es kommt ganz drauf an – wie folgende Beispiele zeigen.

#1 Mitsubishi HiTec Paper Europe: mit on-prem 60 Prozent weniger IT-Kosten

Dem in alle Welt exportierenden Spezialpapierhersteller ist für seine deutschen Produktionsstätten eine IT-Lösung mit stabil laufenden Software-Versionen wichtig. Außerdem: Rechtssicherheit, Kompatibilität zu bestehenden Systemen und ein optimaler Einsatz der jährlichen IT-Budgets. Nach eingehender Beratung durch VENDOSOFT nutzt der Konzern deshalb für seine 600 Beschäftigten Datacenter, Remote Terminal Server, Windows und Exchange Server sowie CAL als gebrauchte On-Premises-Software. Der zuständige IT-Leiter erklärt dazu: „In unserem Produktionsbetrieb muss alles stabil laufen. Wichtiger als die neueste Version einer Software ist ihre Zuverlässigkeit. Deshalb kaufen wir ältere Versionen gebraucht bei VENDOSOFT – das spart uns 60 Prozent gegenüber dem Neupreis."

SO VIEL CLOUD WIE NÖTIG UND SO WENIG WIE MÖGLICH.

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

#2 HOMA Pumpenfabrik: 100.000 Euro Ersparnis durch cleveren Lizenzmix

Der Hersteller für Abwassertechnik stand vor der Herausforderung, seine IT-Infrastruktur modernisieren zu müssen. Den geplanten Neukauf von Microsoft-Lizenzen für Windows-Betriebssysteme, Office und Exchange Server bot ein großer Microsoft-Partner für 215.000 Euro an – ein Schock für den IT-Leiter. So kam das Unternehmen zu VENDOSOFT und hörte erstmals, dass sich die geplante IT-Strategie auch mit gebrauchten Microsoft-Lizenzen umsetzen ließe. Die empfohlene Kombination aus neuen und gebrauchten Lizenzen brachte bereits beim ersten Einkauf 70.000 Euro Kostenersparnis. Als anstand, Cloud-native Arbeitsplätze in die Infrastruktur zu integrieren, vertraute man erneut den Microsoft-Experten. Statt teurer Enterprise-Pläne rieten die zu Microsoft Business Premium, das nahezu die gleichen Funktionen wie E3 bietet – aber nur die Hälfte kostet. Mittlerweile summieren sich die Einsparungen auf über 100.000 Euro und HOMA bezieht sämtliche Microsoft-Lizenzen über VENDOSOFT: von gebraucht über neu bis zur M365-Cloud.

#3 Novamont: neueste Servertechnologie 30 Prozent günstiger

Der internationale Biochemie- und Biokunststoff-Hersteller plante eine Neuausstattung der Arbeitsplätze in seinem Rechenzentrum in Novara (Italien). Die strategische Zielsetzung des Konzerns sah jedoch gleichzeitig die Einsparung von Lizenzkosten vor. VENDOSOFT beriet das Unternehmen daher auf gebrauchte Software. Die Anschaffung der neuesten Microsoft Windows Server als Gebrauchtsoftware ermöglichte Novamont die gewünschte hyperkonvergente IT – bei 30 Prozent geringeren Lizenzkosten gegenüber dem UVP.

#4 Schweizer Markenprimus: On-Premises statt Cloud – 75.000 Euro gespart

Nicht jedes Unternehmen braucht die Cloud. Das trifft auch auf diesen Schweizer Markenfabrikanten von Heizanlagen, Energiespeichern und Wärmepumpen zu. Auf Rat von VENDOSOFT entschieden sich die IT-Verantwortlichen bewusst gegen die Microsoft Cloud. Stattdessen sind ihnen maximale Kontrolle, langfristige Einsparungen und die Unabhängigkeit von Microsoft 365 wichtig.

GUT ZU WISSEN

Kosteneffizienz
Sie möchten Ihr Lizenzmanagement auf Kosteneffizienz überprüfen? Über den QR-Code kostenlos anfragen.

„Da es hier um den reinen Produktionsbetrieb in der Schweiz geht, der vollkommen autark ist, ist eine Cloud-Anbindung nicht notwendig", erklärt Björn Orth. „Mit On-Premises ist dieses Unternehmen optimal ausgestattet." Statt teurer Neulizenzen empfahl VENDOSOFT gebrauchte Office-Pakete, Server und Zugriffslizenzen. Dadurch amortisierte sich die erste Investition von 25.000 Euro bereits nach einem Jahr. Innerhalb von vier Jahren sparte der Wärmepumpenhersteller über 75.000 Euro an Softwarekosten ein.

#5 Anlagenbauer KIESELMANN: 245.000 Euro Einsparung mit Gebrauchtlizenzen

In einem mehrjährigen Lizenzierungsprojekt mit VENDOSOFT wurde der komplette Softwarebestand des Fluidtechnik-Spezialisten KIESELMANN optimiert. Der suchte nach einer kosteneffizienten IT-Strategie für seine acht Gesellschaften und entschied sich bewusst für gebrauchte Microsoft-Lizenzen. Das Ergebnis: 70.000 Euro Investition und eine Ersparnis von 245.000 Euro. Der verantwortliche IT-Leiter ist nachhaltig zufrieden: „Bei Software gibt es keinen Verschleiß. Warum also nicht günstige und audit-sichere Gebrauchtlizenzen nutzen!" Zumal ihn VENDOSOFT nicht nur bei der Beratung, sondern auch in Sachen Dokumentation und Rechteübertragung überzeugt.

#6 John-Deere-Fachhändler: Volle Cloud-Kontrolle und optimale Lizenzierung

Eine kluge Lizenzstrategie zahlt sich bei on-prem genauso aus wie in der Cloud. Das bestätigt die LVA Landtechnik GmbH, ein John-Deere-Fachhändler mit zehn Standorten und 370 Mitarbeitenden. Hier kommt die ganze Bandbreite der Microsoft-365-Pläne zum Einsatz. Die bezieht das Unternehmen bei VENDOSOFT zum günstigsten Preis und spart im Jahr tausende Euro. Vor allem aber spart LVA Landtechnik, weil VENDOSOFT jeden einzelnen Mitarbeitenden mit dem exakt passenden Online-Plan ausstattet. „So viel Cloud wie nötig und so wenig wie möglich", ist dabei die kostensparende Devise von Björn Orth.

#7 Konstruktionsgruppe Bauen: Nachhaltigkeit und Cloud-Kosteneffizienz

Das Ingenieurbüro wollte eine nachhaltige IT-Lösung für seine etwa 150 Mitarbeitenden, die maximale Kosteneffizienz mit Cloud-Flexibilität verbindet. VENDOSOFT setzte ein hybrides Modell aus Microsoft Business Premium, Power BI und bestehenden Gebrauchtlizenzen um. Ergebnis: 23 Prozent Einsparung gegenüber dem Microsoft-UVP und eine CO-reduzierte IT.

Mit der richtigen Lizenzstrategie bleibt die industrielle Transformation bezahlbar. Nicht die Cloud ist hierfür das Maß aller Dinge, sondern die Wirtschaftlichkeit. Deshalb beraten die Microsoft-Experten von VENDOSOFT auch auf Gebrauchtsoftware und hybride Cloud-Modelle. Das spart Kosten, erlaubt wirklich maßgeschneiderte Lösungen und sichert Flexibilität in der langfristigen IT-Strategie.

Angelika Mühleck

Goldgrube Lizenzmanagement

CLEVER FÖRDERN, STATT MÜHSAM GRABEN

IT-Transformation scheint heutzutage vor allem eins zu bedeuten: Eine Menge fancy Tools, Automation an allen Ecken und Enden und natürlich alles in der Cloud – so bleibt man stets up to date und kann dabei noch sparen. Doch ist das wirklich so? Schließlich geht das eigentliche Lizenzmanagement im Rausch des allgegenwärtigen Cloudhypes häufig sang- und klanglos unter oder wird bestenfalls stiefmütterlich behandelt. Und das, obwohl darin eines der größten Einsparpotenziale der gesamten IT steckt.

Lizenzmanagement: Ein Minenfeld aus Kosten und Komplexität

Wer einmal versucht hat, eine vollständige Lizenzbilanz seines Unternehmens zu erstellen, weiß: Es ist eine wissenschaftliche Disziplin für sich. Lizenzmodelle unterscheiden sich drastisch, Vertragsbedingungen ändern sich laufend, und Softwarehersteller sorgen mit schwammigen Klauseln dafür, dass sich Unternehmen schnell in einer Kostenfalle wiederfinden.

Die größten Probleme im Lizenzmanagement:

- Unnötige Kosten durch Überlizenzierung oder nicht genutzte Software
- Mengenrabatte werden nicht genutzt, weil Einkäufe nicht gebündelt werden
- Komplexe Vertragsstrukturen sorgen für fehlenden Überblick
- Compliance-Risiken durch falsche oder doppelte Lizenzierungen
- Fehlende Daten machen strategische Entscheidungen fast unmöglich

DAS LIZENZMANAGEMENT IST IN VIELEN UNTERNEHMEN EIN BLINDER FLECK UND DAMIT EINE RIESIGE GELDVERSCHWENDUNGSMASCHINE.

Linda Schmittner, PR-Managerin, Consulting4IT GmbH, www.consulting4it.de

Kurzum: Wer glaubt, allein durch den Wechsel in die Cloud Geld zu sparen, irrt gewaltig – denn Softwarehersteller lassen sich ihre Abo-Modelle teuer bezahlen. Unternehmen, die ihr Lizenzmanagement nicht strategisch optimieren, verbrennen somit jedes Jahr Unsummen.

Respekt, wer's selber macht – aber schlau geht anders

„Die IT-Abteilung hat das schon im Griff", sind sich viele Unternehmen sicher. Schließlich gibt es festgelegte Budgets und an die wird sich ja auch gehalten. Eine professionelle Softwarelösung für Lizenzmanagement ist vorhanden und somit ist der Ordnung im Lizenzdschungel genüge getan. Ein fataler Denkfehler. Denn es bedarf weit mehr als einer Software, um in Sachen Lizenzen alle Fäden in der Hand zu behalten. So ist es beispielsweise unabdingbar, auch in diesem Bereich einen Experten zu haben, der mit dem nötigen Wissen und genügend Erfahrung die Daten im Blick behält und laufend optimiert, gegensteuert und die richtigen Entscheidungen trifft. Dabei sieht die Realität doch etwas anders aus:

RECHENBEISPIEL: WIE VIEL UNTERNEHMEN WIRKLICH SPAREN KÖNNEN

Ein mittelständisches Unternehmen hat 1.000 Softwarelizenzen und gibt jährlich 500.000 € für Lizenzen und Wartung aus.

Eine detaillierte Analyse durch einen Managed Service zeigt, dass 15 Prozent der Lizenzen nicht genutzt werden. Einsparung: 75.000 €
Durch strategische Vertragsverhandlungen und Konsolidierung kann ein besserer Mengenrabatt ausgehandelt werden. Einsparung: 25.000 €
Compliance-Prüfungen verhindern unerwartete Strafzahlungen und Nachlizenzierungen. Geschätzte Einsparung: 30.000 €
Gesamtersparnis: 130.000 € pro Jahr – und das ausschließlich durch die optimierte Verwaltung durch einen Managed Service.

1. **Fachkräftemangel:** Experten für Lizenzmanagement sind Mangelware – und kosten häufig ein Vermögen.

2. **Zeitfresser:** IT-Teams haben genug mit Incidents, Service-Anfragen und diversen Projekten zu tun – Lizenzoptimierung ist oft das letzte, worum sich jemand kümmern kann, auch weil das Potenzial häufig gar nicht gesehen wird.

3. **Kostenexplosionen:** Viele Unternehmen zahlen über Jahre hinweg zu viel für Software, ohne es zu merken – Stichwort Überlizenzierung. Hinzu kommt der fehlende Überblick über Verträge, Laufzeiten und komplexe Kostenstrukturen.

Fakt ist: Professionelles Lizenzmanagement ist kein IT-Job für nebenbei – es ist ein Spezialgebiet, das strategisches Know-how erfordert.

Managed Services

Statt Ressourcen in teure interne Spezialisten zu stecken, kann es für Unternehmen sinnvoll sein, auf Managed Services für Lizenzmanagement zu setzen. Dabei kümmern sich erfahrene IT-Dienstleister durch regelmäßige Analysen und entsprechende Handlungsempfehlungen kontinuierlich um die Optimierung und Steuerung der Lizenzen. Das spart Zeit und sorgt dafür, dass laufend Kosten eingespart werden.

Die Vorteile von Managed Services im Lizenzmanagement:

- **Kostentransparenz:** Keine unbemerkten Überlizenzierungen mehr
- **Regelmäßige Optimierung:** Lizenzen werden laufend an den Bedarf angepasst
- **Compliance-Sicherheit:** Keine versehentlichen Verstöße gegen Lizenzvereinbarungen
- **IT-Entlastung:** Die eigene IT kann sich auf strategische Projekte konzentrieren

Geht man als Unternehmen noch einen Schritt weiter und nutzt einen Managed Service für umfangreiche IT Analytics Maßnahmen, können auch über das Lizenzmanagement hinaus weitere Optimierungen und Einsparungen in der IT erreicht werden – eine zusätzliche Goldader, die sich massiv auszahlen kann. Ein Beispiel hierfür ist der etablierte DEXOps-Service des Anbieters Consulting4IT GmbH.

Fazit: Lizenzmanagement ist eine strategische Entscheidung

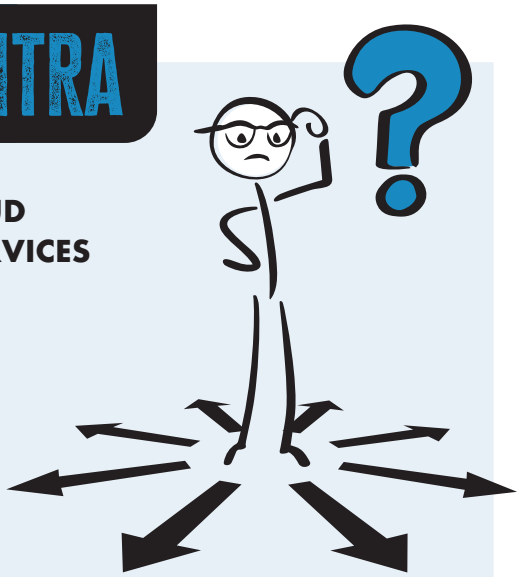
Das Lizenzmanagement ist in vielen Unternehmen ein blinder Fleck und damit eine riesige Geldverschwendungsmaschine. Auch der Wechsel in die Cloud spart nicht automatisch Geld oder macht gar die Lizenzverwaltung obsolet – im Gegenteil. Wer hier keine eigenen Experten einsetzt und stattdessen auf oberflächliche Verwaltungsprozesse setzt, riskiert versteckte Kosten, Compliance-Probleme und unnötige Ausgaben.

Mit professioneller Lizenzverwaltung in Kombination mit Managed Services lassen sich hingegen echte Einsparpotenziale heben. Statt also selbst im Dunkeln zu graben, lohnt es sich, Experten nach den Goldadern im Lizenzmanagement schürfen zu lassen.

Linda Schmittner

PRO & CONTRA

ON-PREMISES, CLOUD UND MANAGED SERVICES



On-Premises:

+ Datenhoheit & Sicherheit
+ Volle Kontrolle über Investitionen
+ Keine laufenden Mietkosten für Software
– Hohe Wartungskosten
– IT-Personal für Pflege und
– Updates erforderlich
– Kaum noch Verfügbarkeit
– neuer On-Premises-Lösungen

Cloud:

+ Flexibilität & Skalierbarkeit
+ Keine eigene Hardware notwendig
+ Regelmäßige Updates durch Anbieter
– Lizenzkosten können steigen
– Abhängigkeit vom Anbieter
– Ohne Monitoring schwer zu optimieren

Kombination mit Managed Services:

+ IT-Entlastung durch externe Experten
+ Optimierte Lizenzverwaltung reduziert Kosten
+ Proaktive Analysen verbessern Performance
– Erfordert Auswahl eines vertrauenswürdigen Anbieters
– Anfangsinvestition in Beratung und Setup
– Laufende Kosten

ERP-Finanzierung im Mittelstand

SOFTWARE-LEASING: NEUE WEGE DER ERP-MODERNISIERUNG

Auf der Suche nach der passenden Finanzierung für ihr umfangreiches Software-Restrukturierungsprojekt entschieden sich die Verantwortlichen der BvL Oberflächentechnik GmbH für eine Zusammenarbeit mit der Miller Leasing GmbH. Die Empfehlung kam von der ams.Solution AG, die eng mit Miller zusammenarbeitet. Über die Vorteile des Leasingsmodells für den mittelständischen Sonderanlagenbauer spricht der Kaufmännische Leiter, Friedhelm Hemmelder.

it management: *Herr Hemmelder, was sprach dafür, das ERP-Projekt über Leasing zu finanzieren?*

Friedhelm Hemmelder: Da es sich bei dem Gesamtprojekt für einen Mittelständler wie BvL um eine relativ große Investition handelte, waren wir in erster Linie daran interessiert, unsere Bilanz zu verkürzen. Diesen Effekt haben wir erzielt, denn wir konnten die Kosten der Leasingraten sofort absetzen.

it management: *Worin liegen die Besonderheiten des Leasingverfahrens im Rahmen von IT-Projekten?*

Friedhelm Hemmelder: Wir arbeiten seit langem mit verschiedenen Standard-Leasinggesellschaften zusammen. Während klassische Leasinggeber in der Regel nur Hardware wie Fahrzeuge und technische Geräte finanzieren, finanziert Miller auch die Software, vor allem jedoch die Lizenzen und darüber hinaus die im Rahmen der Implementierung anfallenden Dienstleistungen und internen Personalkosten.

Nachdem ams.Solution uns auf das Unternehmen aufmerksam gemacht hatte, präsentierten die Miller-Vertreter einige Male direkt hier vor Ort. Aufgrund der Kompetenz und des Know-hows, das sie vermittelten, entwickelte sich über die Zeit ein souveränes Vertrauensverhältnis, was gerade in diesem sensiblen Bereich eminent wichtig ist.

WIR SCHÄTZEN DAS INDIVIDUELLE VORGEHEN DES FINANZIERUNGSDIENSTLEISTERS MILLER LEASING IM RAHMEN DER IMPLEMENTIERUNG DES ERP-SYSTEMS AMS.ERP.

Friedhelm Hemmelder,
Kaufmännischer Leiter,
BvL Oberflächentechnik GmbH

it management: *Was haben Sie konkret über Miller finanziert?*

Friedhelm Hemmelder: Im Kern waren es die Lizenzen, die projektbezogenen Dienstleistungen sowie die Eigenleistungen. Für den Betrieb der neu installierten Software war darüber hinaus auch neue Hardware erforderlich. Das zu dem damaligen Zeitpunkt geplante und mittlerweile errichtete Rechenzentrum wurde in das Leasingkonzept integriert.

it management: *Wie war der Vertrag gestaltet?*

Friedhelm Hemmelder: Es gab einen Grundvertrag für die Software-Lizenzen. Sämtliche Bestandteile über den Grundvertrag hinaus, also beispielweise die bereits erwähnten Dienst- und Eigenleistungen sowie weitere hinzugekaufte Programme, wurden als Unterverträge aufgenommen.

Vorteilhaft war für uns, dass aufgrund der bestehenden Geschäftsbeziehung zwischen ams.Solution und Miller Leasing die Rechnungen sehr unbürokratisch be-

glichen werden konnten. Miller überwies die Zahlungen ohne den Umweg über BvL direkt an ams. Normalerweise nehmen die Zahlungen immer den Weg über den Leasingnehmer.

it management: *Welche Vereinbarungen gibt es bezüglich der Zahlungsmodalitäten?*

Friedhelm Hemmelder: Die Vereinbarung sah vor, dass wir die Rechnungen nach Projektfortschritt erhielten. Dadurch mussten wir nach der Übergabe der Lizenzcodes nicht mehrere hunderttausend Euro auf einen Schlag begleichen. Insbesondere die Zahlungen für die Software und Implementierung hat Miller Leasing dann nach dem tatsächlichen Projektfortschritt übernommen.

Konkret wurde zunächst die Grundrate für die Lizenzen fällig. Nach der Freigabe der Dienstleistungsrechnungen hat Miller diese an ams.Solution bezahlt und die Kosten auf die Grundrate aufgestockt. Vereinfacht gesagt hat Miller alle Zahlungsmodalitäten übernommen. Zudem hat ams direkt an Miller fakturiert.

it management: *Inwieweit ist diese Art der Leasingabwicklung in Ihren Augen besonders?*

Friedhelm Hemmelder: Ich möchte herausheben, dass das erste Jahr leasingratenfrei war und wir erst danach mit der Ratenabzahlung begannen. Dies war gerade in der Corona-Zeit mit all ihren Unwägbarkeiten ein großer Vorteil, der uns finanziell entlastete.

it management: *Wäre dies mit einer Bank oder einer größeren Leasinggesellschaft auch möglich gewesen?*

Friedhelm Hemmelder: Mit einer Bank sowie einer traditionellen, größeren Leasinggesellschaft in dieser individuellen Form wahrscheinlich nicht. Natürlich bezahlen wir jetzt anteilig höhere Raten, weil wir ja eben im ersten Jahr leasingfrei waren.

Tatsache ist, dass die Zahlungsanpassung an unsere kundenindividuellen Bedürfnisse absolut positiv war.

it management: *Wie bewerten Sie, dass Miller keine hauseigene Bank in der Unternehmensgruppe hat?*

Friedhelm Hemmelder: Wir sahen es als einen Vorteil, dass der Dienstleister die Finanzierungszusage eigenständig treffen konnte und in seiner Entscheidung nicht von einer hausinternen Bank abhängig war.

it management: *Was raten Sie Mittelständlern, die ebenfalls eine Finanzierung von ERP-Projekten in Erwägung ziehen?*

Friedhelm Hemmelder: Ich empfehle, mit Blick auf die Kapitalstruktur des jeweiligen Unternehmens das vorrangige Ziel zu definieren: Soll die Bilanz verkürzt werden oder will sich das Unternehmen unabhängiger von der Hausbank machen, weil Leasing die Kreditlinie nicht belastet?

Für uns passten die Konditionen und Rahmenbedingungen so gut, dass wir kürzlich ein weiteres Projekt mit Miller Leasing abgewickelt haben.

it management: *Herr Hemmelder, vielen Dank für das Gespräch!*

SAUBERER PROZESSDURCHLAUF BEI BVL OBERFLÄCHENTECHNIK

Die BvL Oberflächentechnik, gegründet 1989 in Emsbüren, zählt zu den führenden deutschen Herstellern industrieller Reinigungsanlagen. Das Unternehmen ist in 20 Ländern aktiv und entwickelt als Systempartner kundenspezifische Lösungen – von kleineren Waschanlagen bis zu komplexen Großprojekten inklusive eigener Steuerungs- und Software-Systeme.

Bedingt durch eine fragmentierte IT-Landschaft bestehend aus einem funktional limitierten ERP-System und verschiedenen isolierten Einzellösungen, konnten die internen Prozesse des Unternehmens mit der technologischen Produktentwicklung nicht mehr Schritt halten. Um die wachsenden Prozessanforderungen zu bewältigen, initiierte BvL 2019 die Evaluierung einer integrierten ERP-Lösung. Die Wahl fiel 2021 auf ams.erp, ein Multiprojektmanagement-System, das seit November 2022 im Produktiveinsatz ist und speziell auf die Einzelfertigung (Losgröße 1+) ausgerichtet ist. Die Implementation führte zu signifikanten Verbesserungen in Effizienz und Prozesstransparenz. Die Finanzierung des Gesamtprojekts erfolgte über die Miller Leasing GmbH, einen auf IT-Projekte spezialisierten Leasinganbieter, vermittelt durch ams.Solution.

www.ams-erp.com

SAP-Partner-Ökosystem im Wandel

„WER BESTEHEN WILL, MUSS SICH MITENTWICKELN"

Der Weg führt in die Cloud: So klar wie SAP ihre Strategie formuliert, so diskussionswürdig ist sie – zumindest mit Blick auf das Tempo, das der Software-Konzern bei der Umsetzung vorlegt. Die zahlreichen Produktumstellungen und -abkündigungen, die damit einhergehen, haben nicht nur Auswirkungen auf Anwender. Auch für Partner bedeuten sie ein Umdenken. Welche Herausforderungen, aber auch Chancen der Weg von SAP für Partner mit sich bringt, ordnen die beiden Vertreter des DSAG-Partnerbeirats Martin Fischer (Head of Product bei Neptune Software GmbH) und Thorsten Raquet (CEO bei Public Cloud Group) im Interview ein.

ALS PARTNER STEHEN WIR GENAU ZWISCHEN DEM STATUS QUO DER ANWENDER UND DER WUNSCHVORSTELLUNG VON SAP.

Martin Fischer, Head of Product, Neptune Software GmbH, www.neptune-software.com

it management: *Aus seiner Cloud-Strategie macht der Walldorfer Software-Konzern keinen Hehl. Was bedeutet sie für Partner?*

Thorsten Raquet: Die Cloud steht im Zentrum der SAP-Strategie – und das vollkommen zu Recht. Für SAP bedeutet sie ein profitables, zukunftssicheres Geschäftsmodell, für Anwender eröffnet sie neue Möglichkeiten durch flexiblere, skalierbare und wartungsarme Lösungen. Herausfordernd bleibt dabei das hohe Tempo, mit dem SAP diesen Wandel vorantreibt – insbesondere für Unternehmen, die komplexe bestehende Strukturen migrieren müssen. Hier braucht es realistische Migrationspfade, damit der Wechsel für alle Beteiligten machbar bleibt.

Martin Fischer: Tatsächlich sieht die Realität nämlich so aus, dass zahlreiche Anwenderunternehmen nach wie vor auf On-Premises-ERP-Systeme setzen und das voraussichtlich auch noch einige Jahre. Als Partner stehen wir genau zwischen dem Status quo der Anwender und der Wunschvorstellung von SAP. Unser Anspruch ist, es die Anwender mit den Tools und Lösungen zu unterstützen, die sie brauchen. Das fällt uns aber durch kurzfristige Produktumstellungen und -abkündigungen zunehmend schwerer. Diesen Spagat müssen wir meistern, zwischen SAPs „fast-forward" und Kunden, die diese Entwicklungen so schnell einfach nicht mitgehen können oder wollen.

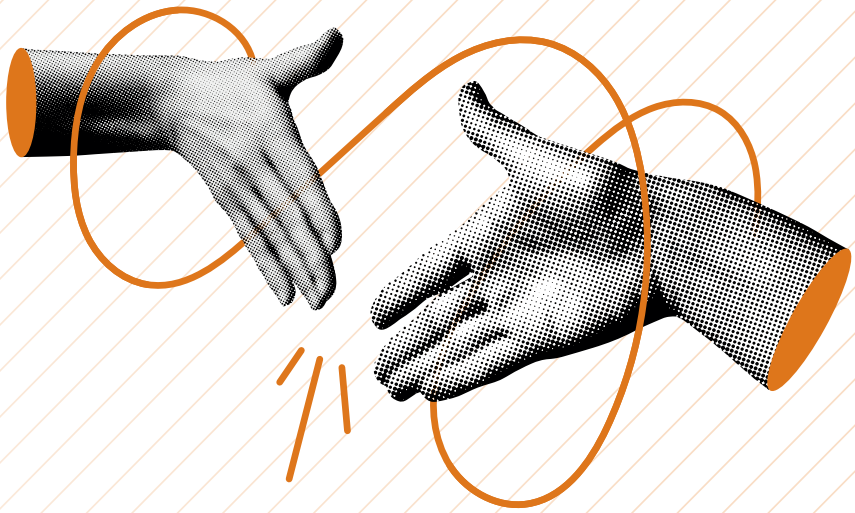
it management: *Inwiefern ist dabei die Kommunikation ein Thema?*

Martin Fischer: Das Ziel von SAP ist eindeutig benannt. Die Maßnahmen, um dort hinzugelangen, werden dagegen häufig stückweise und sehr kurzfristig publik gemacht. Man nehme das Beispiel Classic ABAP-Add-ons. Ohne Vorwarnung kündigte SAP Ende 2023 die bis dato gültigen Zertifizierungen ab – Zertifizierungen, mit denen Anwender und Partner gleichermaßen geplant hatten. Erst im März 2024 wurde die 'Clean-Core-Zertifizierung' schließlich veröffentlicht. Nach einer Hängepartie von rund vier Monaten, in denen unklar war, wie es überhaupt weitergehen soll.

Thorsten Raquet: Ein zentraler Bestandteil von SAPs Cloud-Strategie ist es, den Kern der Systeme zu bereinigen. Die maximale Individualisierung, die in der On-Premises-Welt möglich war, hat über die Jahre zu einem Wildwuchs an Add-ons

PARTNERBEIRAT

Der Partnerbeirat setzt sich für die Interessen der über 1.200 Partnerunternehmen innerhalb der Deutschsprachigen SAP-Anwendergruppe e. V. (DSAG) ein. Dafür steht er im engen konstruktiv-kritischen Dialog mit SAP. Austausch und Information zu weiteren aktuellen Partnerthemen finden Interessierte im DSAG-Mitgliederforum. Auf den DSAG-Technologietagen am 3. April 2025 in Wiesbaden wird der Partnerbeirat ebenfalls mit zwei Sessions vertreten sein: www.dsag.de/techtage.



und Customized-Lösungen geführt. Die Clean-Core-Strategie soll genau hier ansetzen – und das ist aus technischer Sicht nachvollziehbar.

Problematisch wird es allerdings, wenn tiefgreifende Entscheidungen mit massiven Auswirkungen auf das Partner-Ökosystem ohne ausreichenden Vorlauf oder mit unrealistisch kurzen Umsetzungsfristen kommuniziert werden. Besonders kritisch ist es, wenn wichtige Informationen nur mit großen Partnern geteilt werden, während kleinere Anbieter im Dunkeln bleiben. Eine transparente und faire Informationspolitik ist essenziell, damit alle Beteiligten den Wandel erfolgreich mitgestalten können.

? **it management:** *Wie können Partner die aktuelle Lage für sich nutzen? Was raten Sie Ihnen?*

Thorsten Raquet: Die Cloud ist nicht nur das strategische Ziel von SAP, sondern auch für Partner ein enormes Wachstumsfeld. Denn die Nachfrage nach Expertise in der Implementierung, Betreuung und Optimierung von Software-as-a-Service (SaaS)-Lösungen wächst rasant. Darüber hinaus bietet das SAP-Ökosystem mit Tools wie Signavio, LeanIX oder Cloud ALM zahlreiche Möglichkeiten, Unternehmen aktiv bei ihrer Transformation zu begleiten. Klar ist: Wer bestehen will, muss sich mitentwickeln – die Cloud ist kein Trend, sondern die Zukunft.

Martin Fischer: Das Cloud-Feld ist riesig, die Tools sind vielfältig. Gerade bei kleinen und mittleren Partnern muss deshalb ein Umdenken stattfinden. Sie können unmöglich Spezialwissen in allen Bereichen aufbauen. Dass sich das Partnerökosystem hier bereits zu wandeln beginnt, zeigt sich an den ersten Partnerschaften, die Beratungshäuser miteinander eingehen. So etwas wäre noch vor einigen Jahren undenkbar gewesen. Profitieren kann also, wer Change-Management begriffen hat und bereit ist, sich anzupassen.

! **it management:** *Herr Raquet, Herr Fischer, wir danken für dieses Gespräch.*

DIE CLOUD IST NICHT NUR DAS STRATEGISCHE ZIEL VON SAP, SONDERN AUCH FÜR PARTNER EIN ENORMES WACHSTUMSFELD.

Thorsten Raquet,
CEO, Public Cloud Group, www.pcg.io

THANK YOU

Die Zukunft von Prozessoptimierung

KI, PROCESS MINING UND DER DIGITALE ZWILLING ALS SCHLÜSSELTECHNOLOGIEN

DAS ZUSAMMENSPIEL AUS PROCESS MINING, KI UND DEM DIGITALEN ZWILLING BILDET DAS FUNDAMENT FÜR EINE DATENGETRIEBENE ZUKUNFT.

Constantin Wehmschulte, Managing Director, MEHRWERK, https://mehrwerk.net/

Angesichts immer komplexerer wirtschaftlicher Herausforderungen müssen Unternehmen ihre Prozesse präzise steuern und Ineffizienzen beseitigen, um so ihre Wettbewerbsfähigkeit langfristig zu sichern. Traditionelle Optimierungsmethoden stoßen dabei an ihre Grenzen. Gefragt sind smarte, datengetriebene Lösungen, die Abläufe transparenter machen, vorausschauend steuern und kontinuierlich verbessern.

Der Digitale Zwilling entwickelt sich genau zu diesem Gamechanger. Als exaktes Abbild von Geschäftsprozessen erlaubt er eine nie dagewesene Sichtbarkeit und schafft die Grundlage für datengestützte Entscheidungen. In Verbindung mit Process Mining und Künstlicher Intelligenz entsteht ein leistungsstarkes Ökosystem, das nicht nur bestehende Prozesse optimiert, sondern Unternehmen auch hilft, sich flexibel an neue Marktbedingungen anzupassen.

Der Digitale Zwilling als Optimierungsmotor

Datenbasierte Prozessoptimierung wird für Unternehmen immer wichtiger – und der Digitale Zwilling spielt dabei eine zentrale Rolle. Er dient als umfassendes Werkzeug zur genauen Analyse und langfristigen Verbesserung von Geschäftsprozessen. Als Digital Twin of an Organization (DTO) bildet er ein Unternehmen mitsamt all seinen Abläufen vollständig digital ab. Dieses virtuelle Abbild schafft tiefgehende Einblicke in innerbetriebliche Prozesse und bildet die Basis für gezielte, datengestützte Verbesserungen.

Hierbei spielt Process Mining eine Schlüsselrolle, indem es Prozesse sichtbar macht, die in Unternehmenssystemen sonst oft verborgen bleiben. Mit Hilfe digitaler Spuren aus IT-Systemen wird analysiert, wie Arbeitsabläufe tatsächlich ablaufen – nicht nur, wie sie geplant sind. Die gewonnenen Erkenntnisse werden visualisiert, Schwachstellen identifiziert und Optimierungspotenziale aufgezeigt. Darüber hinaus aktualisiert Process Mining den digitalen Zwilling kontinuierlich mit Echtzeitdaten und gewährleistet so dessen dynamische Weiterentwicklung. Dadurch können Fehlerquellen frühzeitig erkannt und Ineffizienzen gezielt beseitigt werden. Das resultierende agile und datengetriebene Prozessmanagement bildet die Grundlage für eine nachhaltig gesteigerte Unternehmensleistung und stärkt die Fähigkeit, flexibel auf Veränderungen zu reagieren.

KI und Process Mining

Dieser durch Process Mining aufbereitete Datenpool bietet den perfekten Nährboden für KI-Systeme, die entscheidend dafür sind, dass Unternehmen das volle Potenzial von Process Mining ausschöpfen. Entsprechend analysiert KI nicht nur die gesammelten Daten, sondern leitet daraus auch proaktiv Handlungsempfehlungen ab. Dadurch lassen sich potenzielle Probleme entschärfen, bevor sie den Geschäftsbetrieb beeinträchtigen. Das Ergebnis ist eine perfekt aufeinander abgestimmte Synergie, die den Unternehmen eine präzise Optimierung der Prozesse und eine proaktive Anpassung an Veränderungen ermöglicht.

Der Schlüssel zur Leistungsfähigkeit dieser Cyber-Kollaboration liegt in der Qualität der zugrunde liegenden Daten. Process Mining spielt dabei eine doppelte Rolle: Einerseits strukturiert und visualisiert es die Prozessdaten, andererseits sorgt es für eine semantische Anreicherung, die KI-Systemen eine aussagekräftige Datenbasis liefert. Diese Kombination aus detailreicher Prozessanalyse und KI-gestützter Optimierung schafft eine dynamische und innovative Infrastruktur. Sie erlaubt es Unternehmen nicht nur, Ineffizienzen zu beseitigen, sondern auch neue Strategien zu entwickeln und ihre Marktanpassungsfähigkeit langfristig zu stärken. Diese Kombination aus detailreicher Prozessanalyse und KI-gestützter Optimierung bildet den Übergang für die nächste Stufe der Prozessintelligenz.

Process Intelligence

Dieser Übergang von Process Mining zu Process Intelligence stellt einen entscheidenden Fortschritt in der Prozessoptimierung dar. Process Intelligence baut auf den Ergebnissen des Process Mining auf und erweitert diese durch die Integration von Echtzeitinformationen und prädiktiven Modellen. Während Process Mining vor allem historische Daten analysiert, ermöglicht Process Intelligence eine kontinuierliche Steuerung und Verbesserung von Prozessen. Dadurch eröffnen sich völlig neue Möglichkeiten: Unternehmen können nicht nur Ineffizienzen beseitigen, sondern auch proaktiv auf Veränderungen reagieren und ihre Abläufe flexibel an neue Anforderungen anpassen.

Dank der Echtzeitdaten lassen sich unerwartete Engpässe frühzeitig erkennen und potenzielle Herausforderungen vorausschauend bewältigen. So wird Process Intelligence nicht nur zu einem leistungsstarken Werkzeug zur Prozessoptimierung, sondern auch zu einem strategischen Instrument, das nachhaltige Wettbewerbsvorteile sichert und Unternehmen dabei unterstützt, ihre Ziele schneller und effizienter zu erreichen.

Erfolgsstrategie der Zukunft

Der Erfolg moderner Unternehmen hängt immer stärker davon ab, wie effizient sie Daten nutzen und daraus konkrete Handlungsempfehlungen ableiten. Das Zusammenspiel aus Process Mining, KI und dem digitalen Zwilling bildet das Fundament für eine datengetriebene Zukunft. Diese Technologien schaffen Transparenz, Flexibilität und ermöglichen eine Automatisierung, die weit über traditionelle Prozessoptimierung hinausgeht.

Unternehmen, die frühzeitig auf diese innovativen Ansätze setzen, sichern sich nicht nur Wettbewerbsvorteile, sondern stärken auch ihre Innovationskraft und Marktposition. Der gezielte Einsatz von Process Intelligence ergänzt dabei die Vorteile von Process Mining und dem digitalen Zwilling, indem er eine kontinuierliche Prozessüberwachung und -optimierung ermöglicht. So werden Unternehmen agiler und besser in der Lage, sich an Veränderungen anzupassen. Deshalb gehört die Zukunft den Unternehmen, die diese Potenziale für sich nutzen und ihre Branche aktiv mitgestalten – sie sind die Treiber des Wandels und formen die Wirtschaft von morgen.

Constantin Wehmschulte

KI als strategischer Wachstumstreiber

MEHR ALS PERSÖNLICHE PRODUKTIVITÄT

Viele Unternehmen nutzen bereits generative KI-Tools (GenAI-Tools) wie Microsoft 365 Copilot, um Routineaufgaben zu automatisieren. Doch operative Effizienzsteigerungen sind nur der erste Schritt. Der eigentliche Mehrwert entsteht, wenn KI strategisch in Unternehmensprozesse eingebettet wird. Auch im Feld der KI-Agenten kratzen vereinzelte Automatisierungslösungen bisher nur an der Oberfläche der Wertschöpfung – entscheidend ist, KI gezielt als echten Business Driver zu etablieren.

Wie gelingt dieser wichtige Schritt? Vielen Unternehmen fehlt es an einer übergreifenden KI-Strategie. Klare KPIs, dokumentierte Workflows und eine durchdachte Roadmap sind selten. Erst wenn Unternehmen über kurzfristige Effizienzgewinne hinausdenken und KI gezielt in bestehende Arbeitsprozesse integrieren, entfaltet sie ihr volles Potenzial.

Gerade in Zeiten knapper personeller Ressourcen wird die Leistungsfähigkeit von KI besonders deutlich: Sie steigert nicht nur die Produktivität, sondern verbessert Entscheidungsprozesse, optimiert Workflows und schafft Freiräume für wertschöpfende Tätigkeiten. Um diese Vorteile langfristig zu sichern, muss KI jedoch über isolierte Anwendungsfälle hinauswachsen – hin zu einem strategischen Treiber für Transformation, Innovationskraft und nachhaltigen Unternehmenserfolg.

Ein bewährtes Framework für die erfolgreiche KI-Integration

Die Praxis zeigt: Eine erfolgreiche KI-Integration erfordert einen strukturierten Ansatz. Basierend auf umfangreicher Projekterfahrung haben wir ein Framework entwickelt, das Unternehmen hilft, mit KI langfristigen geschäftlichen Mehrwert zu schaffen. Es gliedert den KI-Einsatz in drei aufeinander aufbauenden Stufen – für eine schrittweise und nachhaltige Implementierung.

#1 Kurzfristig: Individueller Impact – Der erste Schritt zur Veränderung

Viele Unternehmen starten mit GenAI-Tools wie M365 Copilot, um Mitarbeitende bei alltäglichen Aufgaben zu unterstützen – etwa durch automatisierte Dokumentenerstellung, E-Mail-Zusammenfassungen oder Meeting-Protokolle. KI erleichtert den Wissensaustausch, indem sie Informationen schneller auffindbar macht und strukturiert bereitstellt. Dabei sollten Unternehmen gezielt vorgehen:

- **Use Cases definieren:** Abteilungen, Funktionen und Rollen mit dem größten Nutzen identifizieren.
- **ROI messbar machen:** Zeiteinsparungen je Nutzergruppe analysieren.
- **Mitarbeitende einbinden:** Schulungen und Austausch für den Umgang mit KI.
- **Change-Management aktiv steuern:** Neue Arbeitsweisen müssen eingeführt und nachhaltig etabliert werden.

Kurzfristige Effizienzgewinne durch KI-Tools sind messbar und schaffen die Grundlage für langfristige Veränderungen. Doch Unternehmen sollten an diesem Punkt nicht stehen bleiben: Der nächste Schritt besteht darin, KI tief in bestehende Prozesse zu integrieren, um über Produktivitätssteigerungen hinaus langfristigen Mehrwert zu erzielen.

#2 Mittelfristig: Funktionaler Impact – Prozesse mit KI optimieren

Wird KI über einzelne Anwendungsfälle hinaus strategisch in Unternehmensprozesse integriert, eröffnen sich neue Wertschöpfungspotenziale. Besonders in datenintensiven Abläufen kann sie Effizienzgewinne erzielen und manuelle Arbeitsschritte deutlich reduzieren.

Ein Beispiel hierfür sind Ausschreibungsprozesse im Einkauf. Die Durchführung von Ausschreibungen umfasst zahlreiche manuelle Schritte – von der Bedarfsformulierung über die Dokumentenerstellung bis zur Anbieterauswahl. KI kann diesen Prozess beschleunigen, indem sie Unterlagen optimiert, passende Lieferanten identifiziert und eingehende Angebote analysiert. Das verkürzt die Time-to-Market und verbessert die Vergleichbarkeit.

Auch im Releasemanagement zeigt sich das Potenzial von KI. Beispielsweise müssen bei der Erstellung von Produkt- und Marketingdokumentationen Texte strukturiert, Produktinformationen kategorisiert und Inhalte in mehreren Sprachen erstellt werden. KI erstellt und übersetzt Dokumente automatisch und bündelt relevante Informationen aus verschiedenen Quellen. Das beschleunigt die Markteinführung und sorgt für eine einheitliche Kommunikation.

KI-Agenten: Die nächste Stufe der Automatisierung

KI-Agenten setzen auf der Prozessebene neue Maßstäbe: Sie steuern Abläufe aktiv, vernetzen Anwendungen und treffen datengetriebene Entscheidungen. Dabei optimieren sie nicht nur bestehende Workflows, sondern ermöglichen völlig neue Geschäftsmodelle.

Ihr Erfolg hängt jedoch von einer klaren Strategie ab. Unternehmen müssen definieren, in welchen Prozessen KI-Agenten den größten Mehrwert bieten – sei es bei der Automatisierung operativer Abläufe oder bei der Entwicklung digitaler Services. Wer sie gezielt integriert, steigert Effizienz und Skalierbarkeit und sichert sich langfristig Wettbewerbsvorteile.

DER EIGENTLICHE MEHRWERT ENTSTEHT, WENN KI STRATEGISCH IN UNTERNEHMENSPROZESSE EINGEBETTET WIRD.

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

#3 Langfristig: Business Impact – KI als Treiber für strategische Unternehmensziele

KI entfaltet ihren vollen Mehrwert, wenn sie über einzelne Anwendungen hinaus strategisch integriert wird. Entscheidend ist, wie sie Innovation fördert, Wertschöpfung optimiert und datenbasierte Entscheidungen ermöglicht. KI steigert die Effizienz, unterstützt kreative Prozesse und hilft, Märkte schneller zu analysieren. Um diese Mehrwerte zu realisieren, bedarf es jedoch einer klaren Strategie:

- Welche Geschäftsziele werden beeinflusst?
- Wo lassen sich Effizienzgewinne messen?
- Wie kann der Business-Value langfristig optimiert werden?

Eine Business Value Analyse und definierte KPIs machen den Erfolg messbar. Darauf aufbauend gilt es, eine Roadmap zu entwickeln, um den Einsatz von KI gezielt zu steuern und kontinuierlich zu optimieren.

Goal-Setting als Schlüssel zur KI-Transformation

Ein effektives Zielsetzungsframework, wie OKR (Objectives and Key Results), hilft dabei, diese strategischen Fragen zu beantworten und die KI-Transformation zielgerichtet voranzutreiben. OKR ermöglicht es, langfristige Visionen für den Wandel zu definieren, klare jährliche Ziele zu setzen und messbare Ergebnisse zu ermitteln, die die Erfolgskontrolle erleichtern.

Angenommen, das strategische Ziel eines Unternehmens ist die Steigerung der Effizienz und Wettbewerbsfähigkeit durch den Einsatz von KI. Dies kann in konkrete Jahresziele übersetzt werden, wie die Implementierung einer kompakten KI-Strategie bis Ende des Jahres oder die Integration von KI-Use-Cases in allen relevanten Organisationseinheiten.

KURZFRISTIGE EFFIZIENZGEWINNE DURCH KI-TOOLS SIND MESSBAR UND SCHAFFEN DIE GRUNDLAGE FÜR LANGFRISTIGE VERÄNDERUNGEN.

Lisa Burr, Managing Consultant, Expert AI Solutions, Campana & Schott, www.campana-schott.com

Ein wichtiger Bestandteil ist dabei die regelmäßige Überprüfung des Fortschritts und die Anpassung der Ziele, um den Business Value kontinuierlich zu steigern und die KI-Strategie zu optimieren.

Fazit und Ausblick

KI ist mehr als ein Effizienz-Tool – sie verändert Geschäftsprozesse, Entscheidungsfindung und Zusammenarbeit. Erfolgreiche Unternehmen nutzen KI nicht nur zur Automatisierung, sondern optimieren den Einsatz datenbasiert und entwickeln neue Formen der Mensch-KI-Interaktion.

Mit KI-Agenten steht die nächste Entwicklungsstufe bevor. Sie steuern nicht nur Prozesse, sondern orchestrieren Workflows und schaffen neue Geschäftsmodelle. Unternehmen, die KI nicht strategisch verankern, riskieren langfristige Wettbewerbsnachteile. Die Transformation hat gerade erst begonnen. Wer frühzeitig eine klare Strategie entwickelt, bleibt wettbewerbsfähig und sichert sich nachhaltigen Erfolg.

Lisa Burr, Marco Heid

Data Readiness als Schlüssel zum KI-Erfolg

WIE UNTERNEHMEN IN SECHS SCHRITTEN IHRE DATENBASIS OPTIMIEREN

KI-Modelle, die mit Daten von geringer Qualität erstellt wurden, kosten Unternehmen bis zu sechs Prozent ihres Jahresumsatzes. Das hat eine Studie von Vanson Bourne und Fivetran ergeben. Die folgenden sechs Schritte zeigen den Weg zu einer soliden Datengrundlage als unverzichtbare Basis für ein datengetriebenes Geschäftsmodell.

SCHRITT 1:

Welche Aufgaben sollen mit KI gelöst werden?

Wenn der Anwendungsfall klar ist, gilt es zu klären, ob Generative KI hierfür tatsächlich am besten geeignet ist. Manchmal reichen auch eine einfachere prädiktive Modellierung oder fest programmierte empirische Regeln aus. Wenn man Projekte gemäß strategischer Geschäftsfelder definiert, zum Beispiel über Anwendungsfälle und Key-Metriken, kann man fundierte Entscheidungen treffen.

Zu den Anwendungsfällen, die für Generative KI prädestiniert sind, zählen:

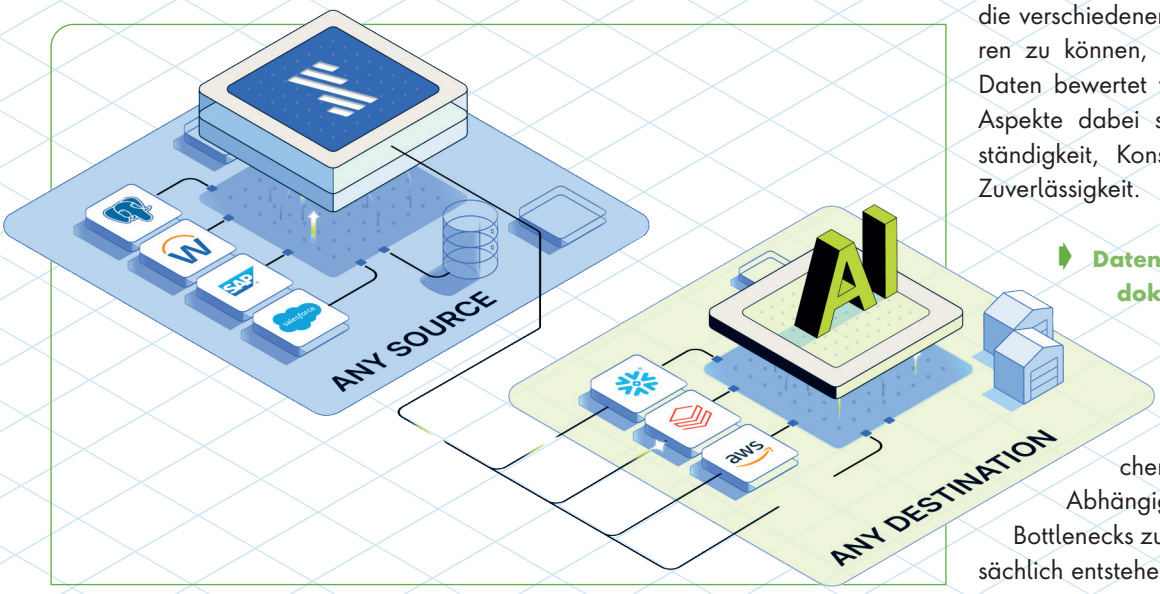
- Schnelles Erstellen von Medien-Inhalten, Software-Code und digitaler Assets aller Art
- Zusammenfassung und Erkenntnisse aus großen Mengen unstrukturierter Daten
- Automatisierung, die natürliche Sprache verstehen und erzeugen oder auf unstrukturierte Daten zugreifen muss, zum Beispiel Chatbots

SCHRITT 2:

Datenquellen identifizieren und auflisten

Wenn klar ist, dass Daten der Schlüssel für die erfolgreiche Nutzung Generativer KI ist, wird offensichtlich, dass die Datennutzung optimiert und Datensilos abgeschafft werden müssen. Nur so können KI-Modelle auf viele unterschiedliche Daten zurückgreifen. Dazu gehört:

- **Datenquellen identifizieren:** Die Quellen sollten Datenbanken, Dateisysteme, Cloudspeicher, externe Datenquellen, APIs sowie unstrukturierte Daten wie E-Mails oder Dokumente umfassen. Befragt man verschiedene Teams und Abteilungen nach ihren spezifischen Datenquellen, kann man sichergehen, keine relevanten Datenquellen zu übersehen.
- **Daten katalogisieren und klassifizieren:** Für jede Datenquelle sollte der darin enthaltene Datentyp – Kundeninformationen, Transaktionsdaten, Sensordaten oder ähnliches – festgehalten werden. Außerdem empfiehlt es sich, die Daten nach ihrer Sensibilität, den regulatorischen Anforderungen und Unternehmensprioritäten zu klassifizieren.
- **Datenqualität bewerten:** Um die Verwertbarkeit der Daten beurteilen und die verschiedenen Datenströme priorisieren zu können, muss die Qualität der Daten bewertet werden. Entscheidende Aspekte dabei sind Genauigkeit, Vollständigkeit, Konsistenz, Aktualität und Zuverlässigkeit.
- **Datenzugriff und -nutzung dokumentieren:** Eine Dokumentation darüber, wie auf die Daten zugegriffen wird, von wem und zu welchem Zweck, ermöglicht, Abhängigkeiten und potenzielle Bottlenecks zu erkennen bevor sie tatsächlich entstehen.



Ihre Datenstrategie ist die Grundlage für Ihre KI-Strategie. (Quelle: Fivetran)

- **Aktualisierungsrhythmus**: Es gilt zu verstehen, wie oft bestimmte Daten aktualisiert und für Auswertungen abgerufen werden. Damit lässt sich festlegen, wie häufig die jeweiligen Daten im KI-Modell aktualisiert werden müssen.

SCHRITT 3:

Datenziel bestimmen

Das Datenvolumen wächst ständig. Um die Daten trotzdem sinnvoll nutzen zu können, benötigen Unternehmen ein einheitliches Repository, das alle Daten vereint. Das vereinfacht den Datenzugriff, das Management der Daten und es sorgt für Datensicherheit. Bei der Auswahl der Destination sollten Verantwortliche Folgendes beachten:

- Die Destination muss alle erforderlichen Datentypen verarbeiten können. Davon hängt ab, ob ein Data Warehouse oder ein Data Lake geeignet ist. Für unstrukturierte Daten ist ein Data Lake das Ziel der Wahl.

- Skalierbarkeit, Kosten und die Integration mit anderen Elementen des Daten-Ökosystems gilt es ebenfalls zu berücksichtigen. Bei kleinerem Datenvolumen können Data Warehouses kostengünstiger sein, Data Lakes empfehlen sich bei größeren Volumen.

- Anzahl und Art der Analysen: Soll das Datenziel für mehrere Analysen verwendet werden? Bei diesen Überlegungen sollte im Vordergrund stehen, die Architektur so schlank und so einfach wie möglich zu halten.

SCHRITT 4:

Integration von Datenquellen in ein zentrales Repository

Unternehmen können Daten nur dann für KI modellieren, wenn sie sich an einem zentralen Ort befinden. Mit einem Tool wie Fivetran lassen sich Konnektoren zu jeder Datenquelle einrichten, die die Daten automatisch in die zentrale Plattform verschieben. Ist eine Datensynchronisation in Echtzeit erforderlich, muss das Tool Change Data Capture (CDC) unterstützen.

WER ALL DIESE SCHRITTE BEFOLGT, KANN EIN GENAI-PROJEKT REALISIEREN, DAS DEM UNTERNEHMEN HILFT, NEUE MASSSTÄBE DER EFFIZIENZ UND EFFEKTIVITÄT ZU ERZIELEN UND DEN UNTERNEHMENSWERT ZU STEIGERN.

Tobias Knieper, Marketing Lead DACH, Fivetran, www.fivetran.com

Um die Sicherheit der Daten auch dann zu gewährleisten, während sie in Bewegung sind, muss die Lösung zur Datenintegration eine Ende-zu-Ende-Verschlüsselung bieten, sensible Daten blocken und hashen können sowie Deployment-Optionen bieten, die mit den entsprechenden Vorschriften konform sind.

Außerdem müssen die Daten oft verarbeitet werden, bevor sie für generative KI nutzbar sind, etwa indem Textfelder miteinander verknüpft werden.

SCHRITT 5:

Design und Implementierung von Retrieval-Modellen

Retrieval Augmented Generation (RAG) erweitert Prompts mithilfe einer Vektordatenbank um Kontextinformationen. So ermöglicht RAG genauere und spezifischere Ergebnisse bei gleichzeitig effizienterer Nutzung der Ressourcen.

Wer RAG nutzen möchte, sollte eine Daten-Pipeline für eine Vektordatenbank erstellen. Diese muss Rohtext oder andere Medien aus dem zentralen Repository in numerische Darstellungen umwandeln, die für das Basismodell lesbar sind. Deshalb ist es sinnvoll, eine Vektordatenbank zu wählen, die mit dem Basismodell kompatibel und einfach nutzbar ist.

Das Retrieval-Modell selbst muss eine Benutzeroberfläche haben, die in der Lage ist, Prompts von Nutzern zu akzeptieren, diese mit Kontext aus der Vektordatenbank anzureichern, an das Basismodell weiterzugeben und schließlich die Outputs zu empfangen.

Dabei kann es sinnvoll sein, einen Knowledge Graphen zu nutzen, um semantische Informationen fest zu kodieren. Denn diese Graphen erhöhen die Relevanz und Genauigkeit von GenAI-Ergebnissen.

SCHRITT 6:

Modell iterieren und verfeinern

Es ist entscheidend, die Modelle sorgfältig auf Pannen oder Fehler zu testen. Durch Iteration und Verfeinerung auf Basis von echtem Nutzer-Feedback können Unternehmen sicherstellen, dass ihre Modelle zuverlässig und effektiv sind – und gleichzeitig sensible Informationen schützen.

Zudem muss sichergestellt werden, dass das Retrieval-Modell exakte und sachliche Ergebnisse liefert. Sensible Informationen wie Geschäftsgeheimnisse oder persönlich identifizierbare Informationen dürfen jedoch unter keinen Umständen preisgegeben werden. Dies lässt sich durch vorgelagerte Governance- und Sicherheitspraktiken erreichen, v. a. durch Blocking oder Hashing sensibler Daten.

Wie bei jeder Software werden im Laufe der Nutzung ab und an unvorhergesehene Probleme auftreten. Diese sollten zum Anlass genommen werden, weiter zu iterieren und das Modell weiter zu optimieren und zu verfeinern. Der Aufbau, die Bereitstellung und die Pflege eines Retrieval-Modells verdient die kontinuierliche Aufmerksamkeit von Experten.

Tobias Knieper

KI-Bias: Zwischen Euphorie und Datenfallen

SICHERSTELLEN DER DATENINTEGRITÄT IM ZEITALTER DER GENERATIVEN KI

Seit dem Aufkommen der generativen künstlichen Intelligenz (KI) hat sich die Unternehmenslandschaft in eine neue Welt der Effizienz und Innovation verwandelt. Viele betrachten generative KI als die ultimative Wunderwaffe im Arsenal von Unternehmen - sie rationalisiert Prozesse, entdeckt neue Wege für Innovationen, analysiert Massen von Daten innerhalb von Sekunden und personalisiert sogar das Kundenerlebnis.

WENN KI DURCH KONTEXTBEZOGENE DATEN GESPEIST WIRD, KÖNNEN UNTERNEHMEN SICHER SEIN, DASS SIE DIE RELEVANTESTEN UND ZUVERLÄSSIGSTEN ERGEBNISSE FÜR ALLE MÖGLICHEN ANWENDUNGEN ERZIELEN UND GLEICHZEITIG DIE WAHRSCHEINLICHKEIT VON DATENVERZERRUNGEN MINIMIEREN.

Tendü Yogurtçu, PhD,
Chief Technology Officer, Precisely,
www.precisely.com

Dieses breite Spektrum an Vorteilen hat dazu geführt, dass sich laut einer Bitkom-Studie erstmals 59 Prozent der deutschen Unternehmen mit KI beschäftigen – 20 Prozent wiederum nutzen sie bereits und 37 Prozent planen oder diskutieren die Nutzung in der Zukunft.

Trotz steigender Beliebtheit ist der Einsatz von KI jedoch nicht immer eine Erfolgsgarantie. Viele Unternehmen haben KI in ihre Systeme implementiert, ohne ihre Daten und Prozesse angemessen vorzubereiten, was zu zahlreichen Problemen führt.

Zudem stellt der EU AI Act, dessen erste Umsetzungsfrist am 2. Februar war, das weltweit umfassendste Gesetzwerk zur Regulierung künstlicher Intelligenz dar und regelt den Einsatz von KI-Systemen, die ein „unannehmbares Risiko" darstellen können, beispielsweise durch Verbote von:

- KI, die unterschwellig oder täuschend die Entscheidungen einer Person manipuliert.
- KI, die Schwachstellen wie Alter, Behinderung oder sozioökonomischen Status ausnutzt.
- KI, die Menschen, die Verbrechen begehen, aufgrund ihres Aussehens verdächtigt.
- KI, die biometrische Daten verwendet, um auf die Eigenschaften einer Person (wie beispielsweise sexuelle Orientierung) zu schließen.

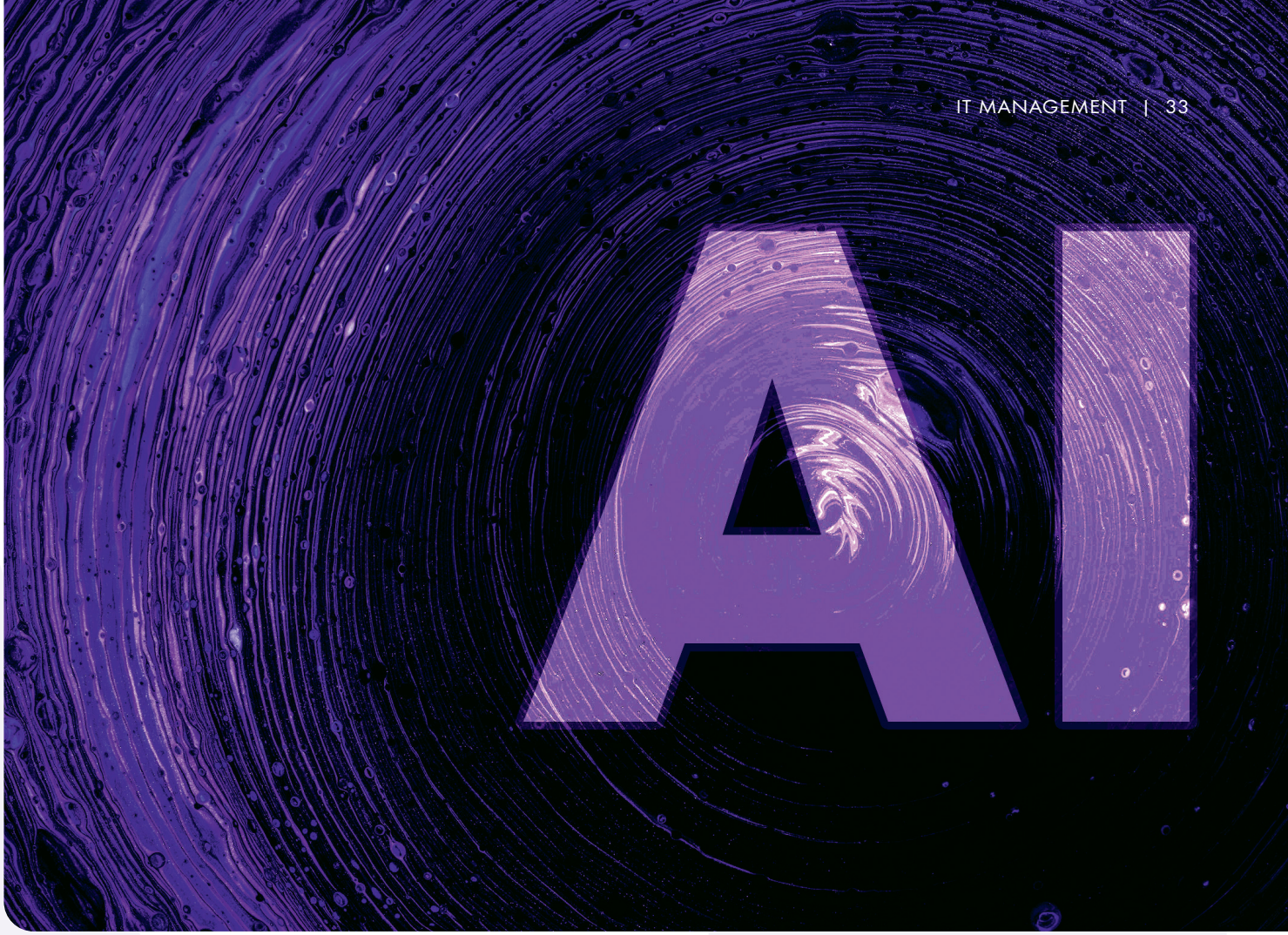
Weitere Vorschriften für die Steuerung von KI-Modellen mit „allgemeinem Verwendungszweck" werden mit Stufe 2 des EU AI Acts im August 2025 gültig.

Wenn KI schief geht

Obwohl sie als unparteiisch wahrgenommen wird, ist die KI in Wirklichkeit ein Produkt der Daten, die ihr zugrunde liegen. Wenn beispielsweise die Daten, die einem KI-Modell zugrunde liegen, nicht ausreichend repräsentativ sind, ist die Wahrscheinlichkeit groß, dass die Resultate verzerrt sind. Tatsächlich ist KI-Verzerrung - die Erzeugung falscher Ergebnisse aufgrund ungenauer, unvollständiger oder unzuverlässiger Daten - eines der größten Probleme, mit denen moderne Unternehmen im Zusammenhang mit KI zu kämpfen haben.

In vielen Unternehmen sind die Daten entweder in Silos untergebracht, veraltet, nicht standardisiert, voller Duplikate oder es fehlt ihnen der nötige Einblick, um sie nutzbar zu machen. Dies führt zu einer Reihe von Problemen, wie beispielsweise irrelevante oder ungenaue Ergebnisse, die in der Praxis zu erheblichen Konsequenzen führen können.

In der Finanzdienstleistungsbranche wird KI beispielsweise häufig für die Kreditwürdigkeitsprüfung von Kreditantragstellern eingesetzt. Wenn jedoch die Daten, die zum Trainieren des KI-Modells verwendet werden, verzerrt sind, kann dies zu ungerechten Ergebnissen führen. Wenn beispielsweise die historischen Daten eine unverhältnismäßig hohe Anzahl von Kreditausfällen bei einer bestimmten demografischen Gruppe enthalten, könnte das



KI-Modell lernen, diese Gruppe mit einem höheren Risiko zu assoziieren. Infolgedessen könnte das Modell Personen aus dieser demografischen Gruppe in unfairer Weise Kredite verweigern, selbst wenn sie finanziell stabil und kreditwürdig sind.

Dies geschieht bereits in der realen Welt. So wurde festgestellt, dass das KI-System eines Finanzinstituts Frauen benachteiligt. Das System wurde anhand historischer Daten trainiert, die bestehende geschlechtsspezifische Vorurteile bei der Kreditvergabe widerspiegelten. Infolgedessen wurde Frauen eher ein Kredit verweigert oder es wurden ihnen ungünstigere Konditionen angeboten als Männern mit vergleichbaren Finanzprofilen. Diese Voreingenommenheit setzte nicht nur bestehende Ungleichheiten fort, sondern schadete auch dem Ruf des Finanzinstituts und führte zu einer behördlichen Überprüfung.

Da KI in alle Aspekte der Geschäftswelt integriert wird, sind die Unternehmen letztlich dafür verantwortlich, dass die Daten genau und zuverlässig sind, da die Auswirkungen nachteilig sein können. Die Untermauerung dieser Tools mit vertrauenswürdigen Daten ist für jedes Unternehmen, das die endlosen Möglichkeiten der KI nutzen möchte, von entscheidender Bedeutung. Daher versuchen viele Unternehmen, ihre Datenintegrität zu verbessern, indem sie der Datenintegration, der Datenqualität und -governance, der Standortintelligenz und der Datenanreicherung Priorität einräumen.

Aufbrechen von Silos mit Datenintegration

Viele Unternehmen sind anfällig für KI-Verzerrungen, da sie über eine Vielzahl von Daten verfügen, die in verschiedenen Systemen und in unterschiedlichen Formaten gespeichert sind. Wenn Daten über verschiedene Geschäftsbereiche und Datenplattformen hinweg siloartig angeordnet sind, ist es äußerst schwierig, eine genaue und einheitliche Sicht auf die Daten des Unternehmens zu erstellen. Infolgedessen spiegeln die Ergebnisse der KI die verfügbaren Informationen möglicherweise nicht vollständig wider, was zu unwirksamen Empfehlungen führen kann, zum Beispiel zu Marketingkampagnen, die die neuesten Verkaufsdaten nicht berücksichtigen.

Durch die Integration kritischer Daten in Cloud-, lokalen und hybriden Umgebungen sowie über Geschäftsfunktionen hinweg können Unternehmen sicherstellen, dass die Daten integriert, vollständig, konsistent und genau sind - was die Zuverlässigkeit der KI-Ergebnisse verbessert und das Risiko von Fehlern und Verzerrungen verringert.

Aufbau robuster Rahmenwerke für Datenqualität und Governance

Das Sammeln einer Vielzahl von Daten und deren Übersetzung in ein einheitliches Format reicht allein nicht aus, um KI-Verzerrungen zu verhindern. Daten können immer noch ungenau sein, inkonsistent, fehlen oder Duplikate enthalten. Folglich ist die Aufnahme aller relevanten und kritischen Daten nur der erste Schritt

- Unternehmen müssen auch die Qualität und Governance der Daten sicherstellen, die die KI-Modelle speisen.

Eine robuste Datenqualitätsstrategie sollte Tools umfassen, die den Zustand der Daten kontinuierlich überwachen, kritische Daten bereinigen, von Duplikaten befreien und validieren sowie Dashboards und automatisierte Workflows erstellen können. Dies hilft Unternehmen, Datenqualitätsprobleme proaktiv zu beobachten, zu erkennen und schneller und einfacher zu beheben.

Data Governance hilft dabei, Technologie, Mitarbeitende und Prozesse aufeinander abzustimmen, so dass Unternehmen ein umfassenderes Verständnis ihrer Daten erhalten. Dies schafft eine bessere Sichtbarkeit, die die Verantwortlichkeit und Qualität der Datenbestände eines Unternehmens stärkt und eine korrekte Überwachung ermöglicht, um die Einhaltung von Datenschutz- und Sicherheitsvorschriften zu gewährleisten. Durch die Kombination von Datenqualitäts- und Governance-Rahmenwerken können Unternehmen den Umfang, in dem vertrauenswürdige Erkenntnisse aus ihren Daten und KI-Modellen gezogen werden können, erheblich verbessern. Data Governance ist auch ein wichtiger Bestandteil der KI-Governance.

Daten für kontextuelle Relevanz anreichern

Unabhängig davon, ob Daten genau oder vollständig sind, sind ihre Ergebnisse ohne Kontext anfällig für Verzerrungen, da sie nicht in der Lage sind, die subtilen und komplexen Details zu berücksichtigen, die den Wert der Daten verändern könnten. Wenn beispielsweise KI zur Vorhersage der Flugnachfrage über ein Kalenderjahr hinweg eingesetzt wird und die verwendeten Daten das Jahr der COVID-Pandemie enthalten, wären die Daten ohne den richtigen Kontext keine genaue Darstellung der normalen Fluggewohnheiten. Damit die Daten keine Verzerrungen aufweisen, müssen sie auch den Kontext enthalten, um die Auswirkungen von Anomalien zu beseitigen.

Die Anreicherung von Daten mit vertrauenswürdigen Datensätzen von Drittanbietern und raumbezogenen Erkenntnissen kann Unternehmen dabei helfen, die Vielfalt ihrer Daten zu verbessern und gleichzeitig unentdeckte Muster aufzudecken, die zuvor übersehen worden sein könnten. Zu den Datensätzen, die diese Einblicke verbessern, gehören demografische Daten, detaillierte Adressinformationen, Verbraucherverhalten, Daten zu Points of Interest und Umweltrisikofaktoren.

Wenn KI durch kontextbezogene Daten gespeist wird, können Unternehmen sicher sein, dass sie die relevantesten und zuverlässigsten Ergebnisse für alle möglichen Anwendungen erzielen und gleichzeitig die Wahrscheinlichkeit von Datenverzerrungen minimieren.

Datenintegrität ist der Schlüssel zum KI-Erfolg

Unternehmen sehen in der KI den neuen Goldrausch der Technologiewelt und somit die ultimative Möglichkeit, wettbewerbsfähig zu bleiben. Mit dem zunehmenden Einsatz von KI steigt jedoch auch die Zahl der Unternehmen, die unter KI-bezogenen Problemen leiden, darunter auch Verzerrungen. Die Abschwächung von Verzerrungen erfordert Maßnahmen zur Beseitigung von Verzerrungen in den Daten, zur Abschwächung von algorithmischen Verzerrungen und zur systematischen Überprüfung der algorithmischen Entscheidungsfindung.

Folglich müssen Unternehmen sicherstellen, dass die zum Trainieren ihrer KI-Modelle verwendeten Daten und die für KI-Vorhersagen genutzten Daten zuverlässig sind. Wenn die Daten ungenau oder irrelevant sind, kann dies zu erheblichen Auswirkungen führen, einschließlich Geldstrafen und Rufschädigung.

Unternehmen müssen heute mehr denn je proaktiv handeln, wenn es darum geht, eine sinnvolle, nachhaltige Datenstrategie zu entwickeln, die Datenintegration, Daten-Governance und -Qualität, Location Intelligence und Datenanreicherung kombiniert. Auf diese Weise können sie KI und generative KI nutzen, um datengesteuerte Entscheidungen zu beschleunigen.

Tendü Yogurtçu

Hannover Messe

KI SPIELT EINE ZENTRALE ROLLE

Unter dem Motto „Industrial Transformation – Energizing a Sustainable Industry" zeigen rund 4.000 Unternehmen des Maschinenbaus, der Elektro- und Digitalindustrie sowie der Energiewirtschaft Lösungen für die Produktion und Energieversorgung der Zukunft. Dabei wird Künstliche Intelligenz eine zentrale Rolle spielen. „Künstliche Intelligenz wird die gesamte Wertschöpfungskette produzierender Unternehmen revolutionieren und damit ihre Wettbewerbsfähigkeit erheblich steigern", sagt Dr. Jochen Köckler, Vorsitzender des Vorstands der Deutschen Messe AG.

Zu den ausstellenden Unternehmen zählen globale Tech-Unternehmen wie Bosch, Google, Microsoft, Schneider Electric oder Siemens sowie mittelständisch geprägte Technologieführer wie Beckhoff, Festo, Harting, ifm, LAPP, Phoenix Contact, Rittal, Schaeffler oder SEW. Namhafte Forschungsinstitute wie Fraunhofer oder das KIT (Karlsruher Institut für Technologie) skizzieren die Industrielösungen für morgen und mehr als 300 Startups aus unterschiedlichen Technologiefeldern zeigen Innovationen mit disruptivem Potenzial.

Technologie-Mix für die Industrie der Zukunft

Von der Digitalisierung komplexer Produktionsprozesse über den Einsatz von Wasserstoff zum Betrieb ganzer Produktionsanlagen bis hin zur Anwendung von KI zur Optimierung von Fertigungsabläufen zeigt die HANNOVER MESSE ein ganzheitliches Bild der technologischen Möglichkeiten für die Industrie von heute und morgen. Dabei geht es um das Zusammenspiel von Robotik, künstlicher Intelligenz, Antriebstechnologien, souveränen Datenräumen (Manufacturing X), erneuerbaren Energien, Wasserstoff und vielen weiteren Technologien wie etwa dem industriellen Metaverse.

„Das Einzigartige an der HANNOVER MESSE ist, dass wir Entscheidungsträger auf jeder Ebene ansprechen", sagt Köckler. „Ob Produktionsleitende eine neue Robotiklösung zur Automatisierung ihrer Anlage suchen oder ein Geschäftsführer bzw. eine Geschäftsführerin den Weg in die digitale Zukunft für das gesamte Unternehmen ebnen will – auf der HANNOVER MESSE finden sie ihre Ansprechpartner. Es geht sowohl um punktuelle Lösungen als auch um die umfassende Transformation ganzer Unternehmen – und es geht immer um Wettbewerbsfähigkeit."

Partnerland Kanada

„Wettbewerbsfähigkeit hängt aber auch von politischen Rahmenbedingungen ab", betont Köckler. Genau hier sieht er eine weitere Stärke der HANNOVER MESSE: „Seit jeher ist sie das Bindeglied zwischen Wirtschaft und Politik." Es geht nicht nur um den Austausch – in Hannover kann die Politik hautnah erleben, wie Technologien für mehr Effizienz, Nachhaltigkeit, Wettbewerbsfähigkeit und Wohlstand sorgen. Und das nicht nur auf deutscher oder europäischer Ebene, sondern global, wie zum Beispiel mit dem Partnerland Kanada.

„Mit Kanada als Partnerland haben wir einen starken, innovativen Partner, der perfekt zum Konzept der Messe passt: führend bei Digitalisierung und erneuerbaren Energien und ein verlässlicher geostrategischer Partner", fügt Köckler hinzu.

Als Partnerland 2025 wird Kanada seine Beziehungen zu Europa stärken und Partnerschaften zwischen kanadischen und globalen Unternehmen aufbauen, die sich auf digitale Technologien, industrielle Transformation und robuste Lieferketten konzentrieren. Zur kommenden HANNOVER MESSE plant Kanada eine Beteiligung mit mehr als 200 kanadischen Unternehmen aus den Bereichen Automatisierung, Clean-Tech, Elektromobilität, Künstliche Intelligenz, Robotik sowie Wasserstoff.

www.hannovermesse.de

Retrieval Augmented Generation

ENTWICKLUNG EINER UNTERNEHMENSSPEZIFISCHEN CHAT-APPLIKATION IN MICROSOFT AZURE

Der Durchbruch der generativen künstlichen Intelligenz hat Unternehmen dazu ermutigt, KI-basierte Chat-Anwendungen für Kunden und Mitarbeiter anzubieten. Kunden erwarten beispielsweise eine ChatGPT-ähnliche Erfahrung bei Fragen und Antworten sowie bei Kundendienstlösungen und keine Chatbots, die vordefinierte Antworten liefern. Ebenso wünschen sich Mitarbeiter moderne Tools, die den unternehmensinternen Wissensaustausch fördern und die Effizienz bei der täglichen Arbeit steigern. Anwendungen wie ChatGPT können nicht direkt in einer Unternehmensumgebung eingesetzt werden. Diese Chatbots fußen auf Large Language Models (LLMs), die in der Regel auf vorab trainierten Modellen basieren. Da diese LLMs mit öffentlich zugänglichen Daten trainiert werden, verfügen sie nicht über Kenntnisse, die auf unternehmensspezifischen Informationen basieren. Diesem Problem versucht man beispielsweise mit dem RAG-Konzept (Retrieval Augmented Generation) zu begegnen.

Grundlagen zu Large Language Modellen

LLMs sind fortgeschrittene KI-Modelle, die speziell für das Verstehen und Erzeugen menschlicher Sprache entwickelt wurden und Anwendungen wie ChatGPT antreiben. Sie stammen aus dem Bereich der natürlichen Sprachverarbeitung (Natural Language Processing, NLP) und verwenden tiefe neuronale Netze, um eine menschenähnliche Sprachverarbeitung zu simulieren. Diese Netze werden mit großen Datensätzen trainiert, um Muster, Strukturen und Bedeutungen in der Sprache zu erkennen. Frühere Architekturen wie RNNs und LSTMs bildeten die Grundlage für die Verarbeitung sequen-

tieller Daten, stießen aber an ihre Grenzen, wenn es um den Umgang mit langfristigen Abhängigkeiten ging. Die Einführung von Transformatoren, die Daten mit Hilfe eines Selbstaufmerksamkeitsmechanismus parallel verarbeiten, hat das Feld revolutioniert, da sie eine präzisere Erfassung komplexer Zusammenhänge ermöglichen. Transformatoren wurden so zur Grundlage moderner LLMs und erweiterten deren Fähigkeiten im Bereich des Sprachverstehens und der Sprachgenerierung erheblich.

LLMs haben bemerkenswerte Fähigkeiten gezeigt, was sie zu einer beliebten Wahl für den Aufbau von KI-Chatbots macht. Allerdings werden LLMs wie GPTs mit Daten trainiert, die Informationen und Wissen enthalten, das nur bis zu einem bestimmten Zeitpunkt verfügbar ist. Das bedeutet, dass sie nur Fakten kennen und referenzieren können, die bis zu ihrem Trainingsstichtag existierten. Folglich sind ihnen alle Ereignisse oder Fortschritte, die nach diesem Stichtag stattgefunden haben, unbekannt.

Der Wissensstand des OpenAI GPT-4o ist beispielsweise auf Oktober 2023 begrenzt. Darüber hinaus können LLMs Antworten generieren, die plausibel klingen, aber tatsächlich falsch sind, ein Phänomen, das als Halluzination bekannt ist. Dies liegt daran, dass die Modelle so konzipiert sind, dass sie auf der Grundlage von Mustern in ihren Trainingsdaten kohärente Texte erzeugen, selbst wenn diese Muster zu falschen Schlussfolgerungen führen.

Eine weitere Einschränkung vortrainierter LLMs besteht darin, dass diese Modelle auf öffentlich zugänglichen Daten trainiert werden und keinen Zugriff auf die internen Informationen einer Organisation haben. Folglich können die Modelle keine Fragen beantworten, die Kenntnisse über die internen Daten einer Organisation erfordern. Diese Einschränkung bedeutet, dass, wenn beispielsweise ein Unternehmen einen Chatbot auf der Grundlage eines vorab trainierten LLM für seinen Kundenservice erstellen möchte, das vorab trainierte LLM die internen Informationen, Vorschriften und Richtlinien des Unternehmens nicht kennt.

Es gibt verschiedene Ansätze, um die genannten Einschränkungen vortrainierter LLMs zu überwinden. Eine dieser Lösungen ist das Konzept der „Retrieval Augmented Generation" (RAG). Bei diesem Ansatz wird das LLM mit einer Retrieval-Komponente kombiniert, die Informationen aus einer externen Datenquelle abruft und an das LLM weitergibt, um die Antworterstellung zu verbessern.

DAS RAG-KONZEPT ERMÖGLICHT ZUSÄTZLICH ZU DEN GENERIERTEN ANTWORTEN DIE BEREITSTELLUNG VON QUELLVERWEISEN, WAS INSBESONDERE BEI UNTERNEHMENSINTERNEN, NICHT-ÖFFENTLICHEN DATEN VON VORTEIL IST.

Prof. Dr. Peter Preuss, FOM Hochschule für Ökonomie & Management Stuttgart und geschäftsführender Gesellschafter bei People Consolidated GmbH, www.fom.de/de.html

RAG-Konzept

Das RAG-Konzept wurde 2020 von Patrick Lewis und seinem Team bei Facebook AI Research eingeführt. RAG kombiniert vortrainierte Sprachmodelle mit einer Retriever-Komponente. Wenn der Benutzer eine Frage stellt (Prompt), erhält der Retriever zunächst die Frage und sucht in der externen Datenquelle nach zugehörigen Informationen. Anschließend werden die ursprüngliche Frage und die aus der externen Datenquelle abgerufenen Daten an das LLM weitergeleitet, um die Antwort zu generieren. Das bedeutet, dass das LLM die Antwort auf der Grundlage der aus der externen Datenquelle abgerufenen Informationen generiert (siehe Bild 1).

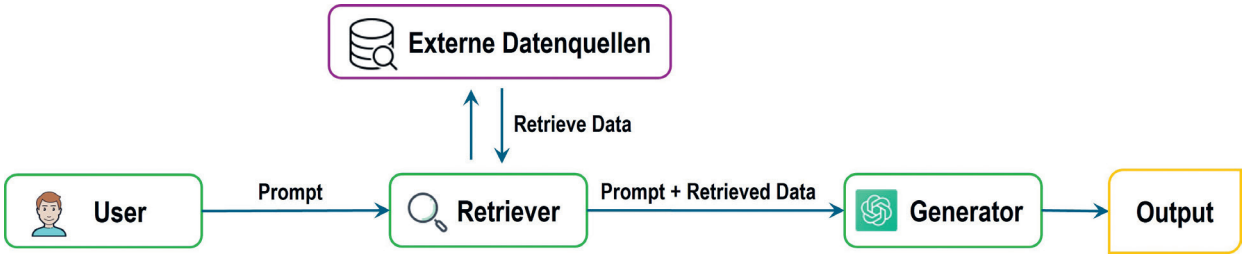


Bild 1: Workflow eines RAG-Systems

Der Retriever in einem RAG-System durchsucht die externe Datenquelle, wobei sowohl Sparse-Ansätze (Schlüsselwort-Matching) als auch Dense-Ansätze (Vektorsuche) verwendet werden, um relevante Informationen zu finden. Die Kombination beider Methoden in einem hybriden Ansatz ermöglicht eine präzisere und umfassendere Informationssuche, die durch Ranking-Modelle weiter verfeinert werden kann, um die relevantesten Ergebnisse zu priorisieren. Der Generator, in der Regel ein leistungsfähiges LLM wie GPT-4, nutzt die vom Retriever bereitgestellten Informationen zusammen mit seinem zuvor trainierten Wissen, um kontextrelevante und kohärente Antworten zu generieren. Die Qualität des RAG-Systems hängt stark von der externen Datenquelle ab, die reichhaltige und organisierte Daten für effiziente Suchprozesse bereitstellen muss.

Umsetzung des RAG-Konzepts in Microsoft Azure

Die Umsetzung des RAG-Konzepts mithilfe der Azure-Infrastruktur umfasst verschiedene Dienste, die zusammen die Funktionalität und den Betrieb einer unternehmensindividuellen Chatbot-Anwendung ermöglichen (siehe Bild 2).

Azure Document Intelligence extrahiert automatisch Daten aus den Dokumenten und verwendet vorgefertigte oder benutzerdefinierte Modelle zur Analyse und Bereinigung von Texten. Azure OpenAI bietet Modelle für die Einbettung und Sprachgenerierung, wobei das Einbettungsmodell für die Vektorisierung und das GPT-Modell für die Antwortgenerierung verwendet werden. Azure AI Search bietet hybride Suchfunktionen durch die Kombination von Text- und Vektorsuche und organisiert Daten in durchsuchbaren Indizes, ergänzt durch Funktionen wie Re-Ranking und semantische Suchabfragen. Azure Web App hostet die Anwendung, ermöglicht die automatische Skalierung und unterstützt die kontinuierliche Bereitstellung und Integration, was die Entwicklungs- und Betriebsprozesse vereinfacht.

Darüber hinaus verbessern Azure-Plattformdienste wie Microsoft Entra ID die Sicherheit und Zugriffskontrolle, indem sie Authentifizierungsmechanismen für Dienste bereitstellen. Azure Monitor überwacht Leistung und Kosten, während Azure Cost Management die Budgetplanung und Kostenkontrolle unterstützt. Die Dienste werden in verschiedenen Stufen angeboten, wobei die richtige Auswahl entscheidend ist, da sich Kapazitäten, Funktionen und Kosten je nach Service-Stufe stark unterscheiden. Der Einsatz von stufengestützten Preismodellen für Dienste wie Azure AI Search erfordert eine sorgfältige Planung, da Änderungen der Service-Stufe nach der Bereitstellung nicht mehr möglich sind.

Beispiel Erbrecht

Um das Ganze zu testen, wurde eine Chat-Applikation implementiert, die Fragen zum deutschen Erbrecht beantwortet. Die Anwendung basiert auf dem zuvor beschriebenen RAG-Konzept und als externe Daten werden PDF-Dateien verwendet, die Lehrbücher, Gesetzestexte und Fallbeispiele zum Erbrecht enthalten.

Mit Hilfe von Azure Document Intelligence wurde der Text aus den PDFs extra-

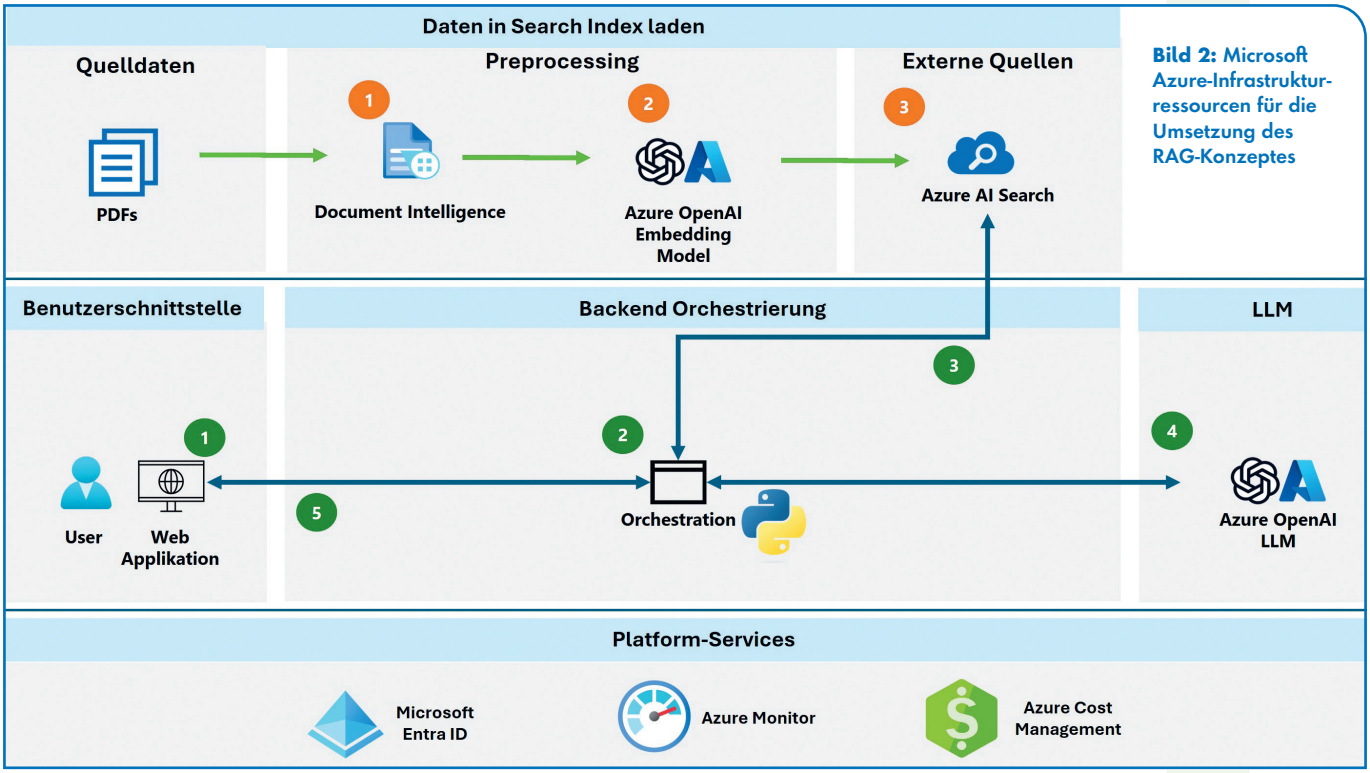


Bild 2: Microsoft Azure-Infrastrukturressourcen für die Umsetzung des RAG-Konzeptes

hiert und mit einem Layout-Modell analysiert, das Dokumentstrukturen wie Absätze und Seitenzahlen erkennt. Anschließend wurde der extrahierte Text in kleinere Abschnitte (Chunks) unterteilt, wobei eine dynamische Logik verwendet wurde, um sinnvolle Start- und Endpunkte zu definieren und Kontextverlust zu vermeiden. Diese Chunks wurden in JSON-Dateien gespeichert, die neben dem Text auch Vektordarstellungen enthalten, die mit einem Azure OpenAI Einbettungsmodell generiert wurden. Die JSON-Dateien wurden in einem Azure AI Search Index gespeichert, der Text- und Vektorfelder für hybride Suchfunktionen kombiniert und zusätzliche Metadaten wie Seitenzahlen und Namen von Quelldokumenten enthält.

Insgesamt wurden 1030 Dokumente mit circa 700 Seiten extrahiertem Text hochgeladen. Der Upload in den Index erfolgt über eine Python-Funktion, die die Verbindung zu Azure AI Search herstellt und die JSON-Dokumente verarbeitet. Dieses System ermöglicht eine durchsuchbare Datenquelle, die als Grundlage für die Chat-Anwendung dient und gleichzeitig die Herkunft der Informationen durch Metadaten nachvollziehbar macht.

DIE IMPLEMENTIERUNG EINES RAG-SYSTEMS MIT AZURE-DIENSTEN ERFORDERT RESSOURCEN WIE AZURE AI SEARCH, AZURE OPENAI, AZURE DOCUMENT INTELLIGENCE UND AZURE WEB APP.

Naeem Nazari,
Cloud Engineer, Accenture,
www.accenture.com

Schlussbetrachtung

Die Implementierung eines RAG-Systems mit Azure-Diensten ist möglich und erfordert nur wenige Ressourcen wie Azure AI Search, Azure OpenAI, Azure Document Intelligence und Azure Web App, die als Platform-as-a-Service (PaaS) bereitgestellt werden. Die Verfügbarkeit und Funktionalität der Azure-Ressourcen variierten jedoch je nach Standort, was eine sorgfältige Planung erfordert, um Kosten und Effizienz zu optimieren. Azure bietet flexible Skalierungsmöglichkeiten, so dass Anwendungen zunächst kostengünstig entwickelt und später für die Produktion auf leistungsstärkere Ebenen migriert werden können.

Das RAG-Konzept ermöglicht zusätzlich zu den generierten Antworten die Bereitstellung von Quellverweisen, was insbesondere bei unternehmensinternen, nicht-öffentlichen Daten von Vorteil ist. Insgesamt bietet Azure eine hilfreiche Infrastruktur für die Entwicklung von RAG-basierten Anwendungen, erfordert jedoch eine sorgfältige Planung und eine gut vorbereitete Datenquelle, um erfolgreich zu sein.

Prof. Dr. Peter Preuss, Naeem Nazari

LLM Benchmarking

DIE PASSENDE KI-LÖSUNG FINDEN

Max Mustermann ist umgezogen und muss bei seiner Versicherung seine Adresse ändern – am liebsten per App oder E-Mail. Adressänderungen wie diese sind ein Standardprozess, der sowohl bei seinem als auch bei anderen Versicherern zig 1.000 Mal in der Woche vorkommt – und dabei hohe manuelle Aufwände und ein großes Fehlerpotenzial mit sich bringt. Die Lösung? Intelligente Prozessautomatisierung mit der Power von LLMs!

Large Language Models (LLMs) wie Claude, Llama und GPT sprießen wie Pilze aus dem Boden, sind alle unterschiedlich gut für spezifische Use Cases geeignet und bringen wiederum eine Vielzahl an Vor- und Nachteilen mit sich. Aber welches LLM ist nun das Beste für Ihre individuellen Herausforderungen?

Best of Breed

Angesichts der rasanten Entwicklungen auf dem LLM-Markt stehen Unternehmen vor der Qual der Wahl? Insiders Technologies bietet mit einem Best-of-Breed-Ansatz immer das aktuell beste LLM für die individuellen Bedürfnisse.

Möglich wird das durch ein konsequentes und kontinuierliches LLM Benchmarking und ein damit verbundenes Monitoring der unterschiedlichen Modelle auf dem globalen Technologiemarkt

Model	Performance
claude_3.5_sonnet	90,10
gpt_4o	87,11
gemini_1_5_pro	86,98
mistral_large_2	85,64
gpt_4_turbo	84,83
mistral_large	83,78
claude_3_haiku	82,21
gpt-3.5-turbo	81,55
gpt_4o_mini	77,99
gemini_1_5_flash	76,76
llama_3_1_70b	76,46
mixtral_8x7b	74,22
insiders_private	72,33
llama_3_1_8b	72,01
mistral_7b	63,73

Das Insiders LLM Benchmarking zeigt nicht nur die aktuellen Top-Performer unter den LLMs auf, sondern bietet auch einen anschaulichen Überblick über alle im Data to Process-Bereich relevanten Modelle. Dabei ist es nicht immer die beste Lösung, ausschließlich auf die leistungsstärksten Modelle zu setzen. Je nach individuellen Anforderungen kann ein Modell mit spezifischen Eigenschaften, wie das Insiders Private LLM mit seinem Fokus auf Datenschutz, für unterschiedliche Unternehmensanforderungen geeignet sein.

LLM Benchmarking

Ein LLM Benchmarking wie das von Insiders, basiert auf einem spezialisierten IDP-Benchmark, der aus der Expertise als KI- und Softwareunternehmen sowie DFKI-Spin-Off entwickelt wurde. Der Fokus liegt dabei besonders auf der Versicherungs- und Finanzbranche. Die standardisierten Testdaten decken typische Geschäftsvorgänge dieser Branchen ab und ermöglichen eine Bewertung der LLM-Performance in den relevanten Bereichen. Die Testmenge umfasst verschiedene Dokumenttypen wie Adress- und Namensänderungen, Prämienrechnungen, Schadensberichte, SEPA-Mandate und medizinische Dokumente, die als Basis für gängige Geschäftsprozesse dienen.

INSIDERS LLM BENCHMARKING

Im Ranking von 15 ausgewählten LLMs wurde die Gesamtperformance unter Berücksichtigung der Extraktions- und Klassifikationsleistung sowie der verbleibenden Nachbearbeitungsaufwände bewertet. An der Spitze steht Claude 3.5 Sonnet von Anthropic mit einem Score von 90,10, gefolgt von GPT-4o von OpenAI, dem aktuellen Medienliebling, mit 87,11. Den dritten Platz sichert sich Gemini 1.5 Pro von Google mit 86,98.

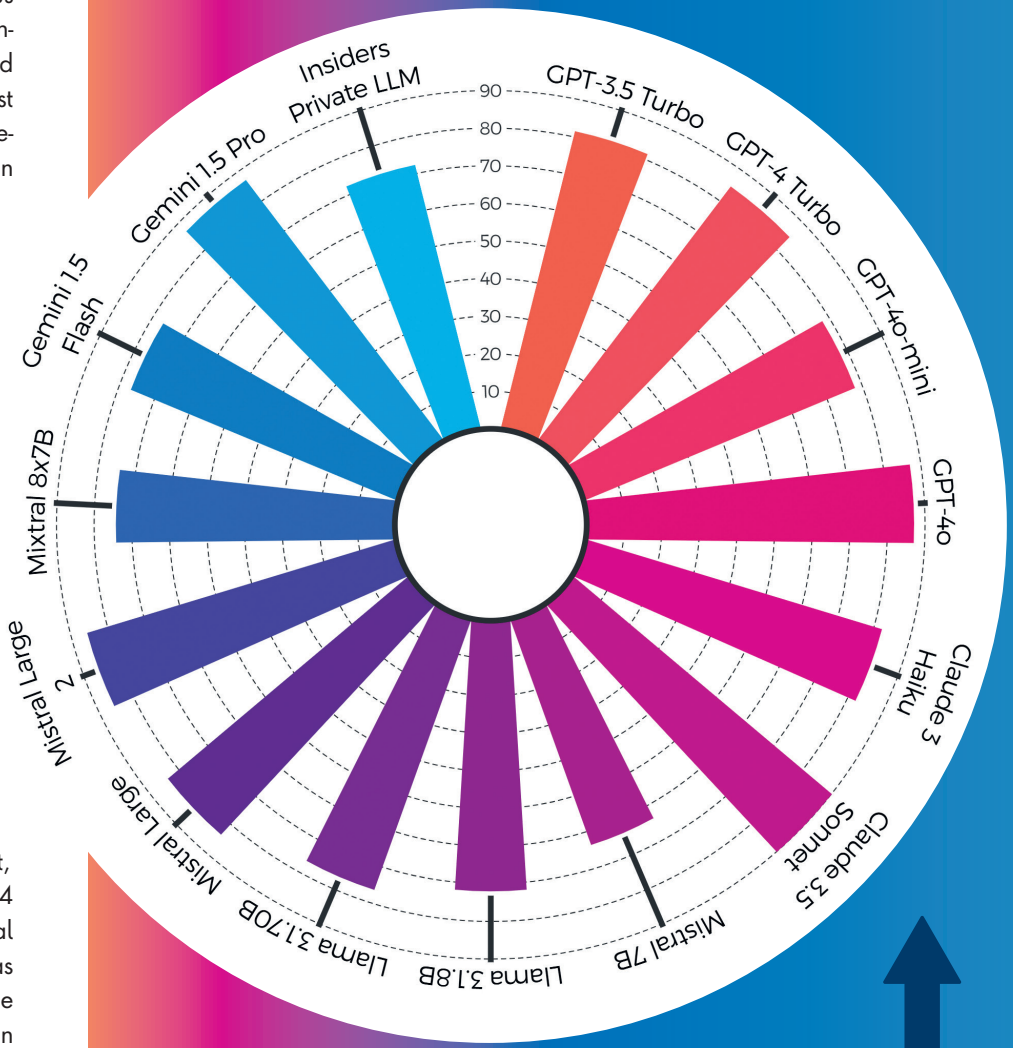
Das LLM Benchmarking ist ein kontinuierlicher Prozess, der den „Best-of-Breed-Ansatz bei Insiders antreibt." Dadurch wird stets den Überblick über die Performance der neuesten LLMs behalten und es kann sichergestellt werden, dass die Kunden mithilfe der flexiblen LLM-Integration der Insiders OvAltion Engine immer die bestmögliche Lösung für ihre Bedürfnisse nutzen. KI-Experten überwachen laufend die leistungsfähigsten Technologien und passen die LLM-Integration in allen Produkten entsprechend an die Markt- und Technologieentwicklungen an.

Mit dem Best-of-Breed-Ansatz erhalten die Kunden die Möglichkeit, hybride Architekturen zu schaffen, die das Beste aus der Welt der externen LLMs und der Insiders-KI-Technologien vereinen – und zwar ohne, dass sich die Kunden selbst zeitintensiv mit den rasanten und komplexen Entwicklungen auf dem globalen LLM-Markt beschäftigen müssen.

Aktueller Performancecheck

Das Insiders LLM Benchmarking bildet regelmäßig die Gesamtperformance verschiedener LLMs ab. In diesem standardisierten Performancecheck werden diejenigen LLMs getestet, die von den Insiders KI-Experten in einer Vorauswahl als besonders geeignet für den Einsatz im Data to Process-Bereich identifiziert wurden. Das umfasst unter anderem ihre jeweilige Performance in den Arbeitsfeldern Informationsklassifikation und -extraktion.

Im aktuellen LLM Benchmarking wurden 15 verschiedene Modelle getestet, darunter bekannte Namen wie GPT-4 Turbo, Claude 3.5 Sonnet und Mistral Large sowie das Insiders Private LLM. Das Ranking der Gesamtperformance, in die sowohl die Leistung im Bereich Extraktion als auch in Klassifikation einfließen, ermöglicht dadurch einen Vergleich der LLMs in Bezug auf die jeweilige Leistungsfähigkeit in Relation zu den verbleibenden Nachbearbeitungsaufwänden.



Quelle: Insiders Technologies, Januar 2025"

Das aktuelle LLM Benchmarking zeigt, dass die bekannten US-amerikanischen LLM-Anbieter aufgrund ihrer immensen Rechenpower und der Menge an Trainingsdaten, wie erwartet, die Nase vorn haben. Auf Platz 1 im Gesamtranking landet Claude 3.5 Sonnet von Anthropic mit einem Score von 90,10, dicht gefolgt vom Medienstar GPT-4o von OpenAI mit 87,11. Den dritten Platz belegt Gemini 1.5 Pro von Google mit 86,98.

Im Vergleich mit den LLMs der US-Tech-Giganten erreicht das Insiders Private LLM zwar eine geringere Gesamtperformance von insgesamt 72,33, punktet jedoch durch seine unübertroffenen Datenschutzstandards. Dies ist seitens des Anbieters ein ganz bewusster Tradeoff, der speziell für informationssensible Branchen wie Versicherungen und Finanzen entscheidend ist. Hier müssen sensible Daten wie Personalausweise, SEPA-Mandate oder medizinische Informationen schnell und zuverlässig verarbeitet werden, ohne dabei Kompromisse beim Datenschutz einzugehen.

Das Insiders Private LLM wird von dem Softwareunternehmen in der eigenen Cloud selbst betrieben und unterliegt dem bekannten, hohen Datenschutzlevel. Während große externe LLMs zudem oft von Faktoren wie Drosselungen oder Rate Limits betroffen sind und der Datenfluss nicht immer transparent nachvollzogen werden kann, bietet das Insiders Private LLM volle Unabhängigkeit und Skalierbarkeit nach den individuellen Kundenbedürfnissen. Mit einer ISO 27001-zertifizierten Infrastruktur und der nahtlosen Integration in bestehende Systeme garantiert es somit maximale Sicherheit und volle Kontrolle für Kunden mit höchsten Datenschutzansprüchen.

Was bedeutet also „das beste“ LLM?
Bei der Frage nach dem Besten geht es nicht nur um die reine Power. Gerade im Versicherungs- und Finanzbereich müssen Unternehmen oft zwischen Leistung und Sicherheit abwägen. Hinzukommen individuelle Vorgaben und Präferenzen der Unternehmen in Bezug auf Kosten, Geschwindigkeit und Dunkelverarbeitung.

Durch die Kombination aus state-of-the-art Deep Learning-Verfahren, tiefgehender LLM-Expertise und über 25 Jahren Branchenerfahrung im Finanz- und Versicherungsmarkt bietet Insiders seinen Kunden leistungsfähige Automatisierungslösungen, die speziell auf die Bedürfnisse sicherheitskritischer Anwendungsfälle zugeschnitten sind und gleichzeitig höchstmögliche Performance liefern.

Je nach individuellen Anforderungen im Spannungsfeld von Performance, Latenz, Dunkelverarbeitung und Kosten ermöglicht das Unternehmen durch die Integration von LLMs von Drittanbietern seinen Kunden einen bequemen und variablen Zugang zu genau dem LLM, das sie wirklich brauchen. Trotz der etwas besseren Ergebnisse externer LLMs ist das Insiders Private LLM eine attraktive Lösung für diejenigen Unternehmen, die höchste Datenschutzstandards einhalten müssen.

Somit muss nicht zwischen Performance und Sicherheit entscheiden werden. Das Insiders LLM Benchmarking ist dabei der verlässliche Referenzpunkt, um im schnelllebigen LLM-Markt den Durchblick zu behalten.

www.insiders-technologies.com/

MIT SAP S/4HANA IN DIE CLOUD

STRATEGIEPAPIER SAP CLOUD-ERP-LÖSUNGEN

Cloud-Dienste und -Lösungen sind allgegenwärtig. Allein in Deutschland nutzen laut dem Branchenverband Bitkom fast 90 Prozent der Unternehmen Cloud Computing, etwa für Speicherplatz, Rechenleistung und Office-Software. Die Vorteile: hohe Flexibilität, minimierte Investitionen und Betriebsaufwände sowie ein sofortiger Zugriff auf Innovationen.

Auch im ERP-Bereich führt kein Weg an der Cloud vorbei. SAP bietet mit SAP S/4HANA Cloud, Public Edition und SAP S/4HANA Cloud, Private Edition zwei Cloud Varianten seiner Business Software an, sowie die darauf zugeschnittenen Einführungspakete GROW with SAP und RISE with SAP. Welche Bereitstellungsoptionen sich jeweils am besten eignet, hängt von den individuellen Gegebenheiten, Anforderungen und Prioritäten eines Unternehmens ab.

Unser Strategiepapier zeigt Ihnen die verschiedenen Optionen auf und erleichtert die Auswahl der richtigen SAP Cloud-Edition.

WHITEPAPER DOWNLOAD

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

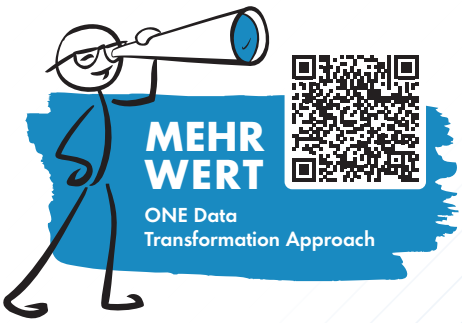
ONE Data Transformation Approach

DIRIGENT EINES RIESIGEN ORCHESTERS

Die Komplexität der digitalen Transformation von Unternehmen ist in vielerlei Hinsicht eine Herausforderung - nicht zuletzt deshalb, weil es kaum Berater gibt, die mit allen Herstellern und Migrationsmethoden vertraut sind. Das hat zur Folge, dass in vielen Transformationen mehrere Beratungsunternehmen mit verschiedenen Kernkompetenzen involviert sind. Helfen kann nach Auffassung von Patric Dahse, CEO von Natuvion, der ONE Data Transformation Approach.

Ulrich Parthier: *In Ihrer aktuellen Studie geben circa 43 Prozent der Manager zu, dass sie ihre Transformationsziele nicht oder nur zum Teil erreicht haben. Warum ist die Quote so hoch?*

Patric Dahse: Um das beurteilen zu können, muss man die Ziele der Unternehmen kennen. Im Rahmen der Studie wurde ermittelt, dass neben organisatorischen Anpassungen vor allem die Einführung neuer Technologien wie KI oder Go-To-Market-Agilität sowie die Steigerung der Innovationsfähigkeit typische Transformationsziele sind. Dass so viele Manager antworten, nicht alle ihre Ziele erreicht zu haben, liegt wahrscheinlich daran, dass sie die IT-Transformation unterschätzt haben. Was sehr viele Unternehmen vergessen, ist, dass eine Transformation ein wirklich großes und oft langwieriges Projekt ist. Da ändern sich schon mal die Anforderungen und Parameter im Verlauf des Projekts. In einem IT-Transformationsprojekt flexibel zu reagieren, ist durchaus schwierig und komplex.



Ulrich Parthier: *Was kann man dagegen tun und mit welchen Herausforderungen kämpfen die Unternehmen?*

Patric Dahse: Bei der Migration auf neue Systeme gibt es eine Vielzahl an Anforderungen. Viele Fragestellungen müssen im Vorfeld geklärt werden, etwa die Frage welche Daten möchte ich mitnehmen, was muss ich archivieren oder möchte ich die Migration nutzen, um andere Herausforderungen gleich mitzulösen? Datenreduktion, Qualitätserhöhung, Prozessanpassungen – das alles muss bedacht werden.

Inzwischen gibt es viele Vorgehensweisen, Methoden und Philosophien, wie man Daten und Prozesse in neue Systeme überführt. Eine Herausforderung aber bleibt. Davon sind sowohl mittelständische als auch große Unternehmen betroffen: Die digitale Transformation ist ein riesiges Projekt, das viele Monate, wenn nicht sogar Jahre, für die Vorbereitung, Durchführung und Nacharbeit in Anspruch nimmt – erst recht, wenn Schnittstellen und Insellösungen betroffen sind. Das Problem: Es passieren Fehler. Ob während der Vorbereitung oder weil man beim Migrationsszenario irrt. Das alles verlängert ein solches Projekt drastisch und führt nicht selten dazu, dass man in diesen Fällen mehrere Schritte zurückgehen muss.

Ulrich Parthier: *Das hört sich wenig motivierend an. Wie lässt sich das vermeiden?*

Patric Dahse: Es ist wichtig zu verstehen, dass das Problem nicht nur in der Migration liegt. Der Schlüssel ist die Integration verschiedener Quellen und Daten. Denn die Daten müssen zu den Prozessen passen. Deswegen ist ein systematisches Vorgehen erfolgskritisch. Interessanterweise sehen das auch die Befragten unserer Studie so. Das Top-Management hat mit über 40 Prozent geantwortet, dass sie viel früher anfangen würden, wenn sie nochmals in der gleichen Lage wären. Über 50 Prozent der verantwortlichen IT-Manager würde

sich beim nächsten Mal viel mehr Zeit nehmen. Deshalb können wir nur sagen: Je besser die Vorbereitung, desto besser die Ergebnisse. Das belegen ja auch die Ergebnisse unserer und anderer Untersuchungen.

? **Ulrich Parthier:** *Sie sagen, Ihr ONE Data Transformation Approach könnte helfen. Wie?*

Patric Dahse: Wir sehen nicht nur anhand der Studie, sondern auch in der täglichen Praxis, dass für Unternehmen eine IT-Transformation ein komplexes Projekt ist, mit dem sie sehr wenig Erfahrung haben. Etwa 40 Prozent der Manager sagen, dass sie für ihre IT-Transformation neue Kompetenzen aufbauen mussten und 34 Prozent geben zu, dass sie die fehlende Erfahrung des eigenen Teams überrascht hat. Und es wird nicht besser. Laut Bitkom sollen allein in Deutschland im Jahr 2040 rund 663.000 IT-Fachkräfte fehlen. Das sind 510.000 mehr als 2024. Umso dringender brauchen die Unternehmen einen Transformationsansatz, der sie einerseits erfolgreich durch diesen komplexen Prozess führt, ihnen aber andererseits höchstmögliche Flexibilität ermöglicht.

Gerade Unternehmen, die nur wenig Transformationserfahrung haben, müssen oft feststellen, dass Weichen, die sie zu Beginn gestellt haben, ihnen mitten im Prozess große Probleme bereiten.

Hier setzt der ONE Data Transformation Approach an. Das ist eine von uns entwickelte Methode, die Beratung und Softwaretools optimal kombiniert, typische Fallstricke vermeidet und Unternehmen bestmöglich vorbereitet. Außerdem gewinnen Kunden mit unserem Ansatz hohe Flexibilität. Das bedeutet, dass sie besser auf Veränderungen reagieren oder gar andere Projekte, wie etwa den Geschäftsjahreswechsel, bei der Transformation gleich mitmachen können. Der ONE Data Transformation Approach ist ein flexibler Ansatz für eine große Anzahl an Anforderungen.

UNSERE EXPERTISE IN VIELEN BRANCHENSEGMENTEN ZEIGT DEM KUNDEN DEN OPTIMALEN WEG, WIE ER SEINE DATEN BESTMÖGLICH AUF DEN NEUEN SYSTEMEN NUTZT.

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

? **Ulrich Parthier:** *Wie funktioniert der ONE Data Transformation Approach?*

Patric Dahse: Der ONE Data Transformation Approach ist eine integrierte Methode, in der das Know-how von mehr als 1.000 IT-Transformationen steckt - von erfolgreichen Mittelständlern wie dem FC Bayern München bis zu internationalen Konzernen wie VW, BMW, E.ON oder Vattenfall.

Der ONE Data Transformation Approach wird durch sehr leistungsstarke Werkzeuge unterstützt, etwa indem wir im Rahmen der Vorbereitung mit über 500 Analysen das zu transformierende System intensiv untersuchen. So entsteht eine solide Grundlage für die meisten Weichenstellungen einer Transformation. Mit der richtigen Transformationsplattform, beispielsweise dem Natuvion DCS, und Tools für die Testdatenautomatisierung, das Projektmanagement oder die Stilllegung von Altsystemen wird das Konzept abgerundet. So vereint der ONE Data Transformation Approach in einem integrierten Ansatz die erfolgreichen Methoden mit den passenden Werkzeugen.

? **Ulrich Parthier:** *Ist dieser Ansatz in allen Branchen gleich effizient und erfolgreich?*

Patric Dahse: Grundsätzlich ist der Ansatz in allen Branchen gleich effektiv. Vielleicht muss ich betonen, dass wir nicht nur die Daten von A nach B schaufeln, sondern dass unsere Expertise in vielen Branchensegmenten dem Kunden den optimalen Weg zeigt, wie er seine Daten bestmöglich auf den neuen Systemen nutzt. Beispielsweise bei den Energieversorgern, der Automobilbranche oder der öffentlichen Verwaltung und Life Science gibt es nur wenige Transformationsdienstleister, die die Prozesse und Systeme besser verstehen als wir. Mit diesem Erfahrungsschatz können wir nahezu allen Branchen helfen.

? **Ulrich Parthier:** *Haben Sie ein konkretes Beispiel für Ihre Branchenexpertise?*

Patric Dahse: Da fällt mir ein Schweizer Energieversorger ein. Als Vorbereitung zum Projekt hatte das Team des Kunden im Vorfeld eine intensive Analyse gemacht und sich intern auf ein Migrationsszenario verständigt. Dann bekamen wir den Auftrag, die Migration durchzuführen und schon im allerersten Workshop stellte man fest, dass entscheidende Dinge nicht oder unzureichend analysiert worden waren. Alles, was das Unternehmen sich schon erarbeitet hatte, wurde über den Haufen geworfen. Das ging nur, weil wir die zugrundeliegenden Geschäftsprozesse und IT-Systeme wie unsere eigene Westentasche kennen und die Businessziele des Kunden verstanden haben.

! **Ulrich Parthier:** *Herr Dahse, herzlichen Dank für das Gespräch.*

IT-Selbstheilungsprozesse

STRATEGIE & PRAXIS IN EINKLANG MITEINANDER BRINGEN

In der digitalen Transformation entwickeln sich IT-Selbstheilungsprozesse zu einem entscheidenden Werkzeug für Unternehmen. Diese fortschrittliche Automatisierungsstrategie ermöglicht es technischen Systemen, Probleme selbstständig zu erkennen, zu analysieren und zu lösen, ohne menschliches Eingreifen. Der Weg dorthin gleicht einem evolutionären Prozess, ähnlich wie bei der Entwicklung selbstfahrender Autos in der Automobilindustrie.

Fünf Schritte zur selbstheilenden IT-Infrastruktur

Der Transformationsprozess erstreckt sich über einen Zeitraum von 5-10 Jahren und umfasst folgende zentrale Entwicklungsstufen:

#1 Implementierung der unveränderlichen Infrastruktur als Code (IaC)

Die Grundlage bildet die Automatisierung des Server-Provisionings durch IaC. Statt manueller Konfiguration in verschiedenen Dashboards werden einfache, verständliche Manifeste verwendet. Moderne Tools wie Kubernetes und Terraform transformieren dabei fehleranfällige manuelle Prozesse in optimierte Softwarebereitstellungspipelines.

#2 Umfassende automatisierte Tests

Die gesamte Codebasis wird durch automatisierte Tests abgedeckt, die parallel zur Entwicklung erstellt und aktualisiert werden. Dies gewährleistet die kontinuierliche Stabilität der Systemkomponenten und verhindert Ausfälle bei neuen Produktionsversionen.

#3 Ganzheitliche Protokollierung und Überwachung

Logging- und Monitoring-Tools werden bereits in der Systemarchitektur verankert. Sie erfassen detaillierte Leistungsdaten und ermöglichen die Erstellung von Reaktionshandbüchern für wiederkehrende Probleme. Diese Datenbasis bildet das Fundament für maschinelles Lernen zur automatischen Problembehandlung.

#4 Intelligente Warnmeldungen und präskriptive Analyse

Moderne Überwachungstools liefern detaillierte Fehlerberichte und können die

Problemlösungszeit um bis zu 90 Prozent verkürzen. Durch präventive Auslöser werden Probleme verhindert, bevor sie entstehen, was die Systemstabilität erheblich verbessert.

#5 Kontinuierliches Lernen und Optimierung

Die eingesetzten Machine-Learning-Algorithmen werden ständig mit neuen Daten trainiert. Dies führt zu einer zunehmend autonomen Infrastruktur, die weniger menschliche Intervention benötigt.

Die Vorteile

Die Implementation einer selbstheilenden IT-Infrastruktur bietet zahlreiche Vorteile:

- Reduzierung ungeplanter Ausfälle
- Optimierung der Ressourcennutzung
- Beschleunigung von Entwicklungszyklen
- Verbesserung der Anwendungsqualität bei reduziertem Testaufwand
- Substanzielle Verbesserung des Kundenerlebnisses
- Proaktive Problembewältigung statt reaktiver Problembehandlung

Der Kern der Selbstheilungsstrategie liegt aber zunächst einmal in einer intelligenten Datennutzung. Unternehmen müssen hochwertige Daten aus allen Unternehmensbereichen sammeln - von Infrastruktur und Netzwerken bis zu Anwendungen und Protokollen. Diese Daten bilden die Grundlage für präzise Machine-Learning-Modelle, die Anomalien früh erkennen können.

Ein weiterer Vorteil liegt darin, es Unternehmen zu ermöglichen, technische Herausforderungen proaktiv zu bewältigen, indem sie ungeplante Ausfälle reduziert, Leistungsprobleme in der Nutzererfahrung beseitigt und das Kundenerlebnis substanziell verbessert.

> IN ZEITEN DER DIGITALEN TRANSFORMATION ENTWICKELN SICH IT-SELBSTHEILUNGSPROZESSE VON EINER TECHNISCHEN MÖGLICHKEIT ZU EINER STRATEGISCHEN NOTWENDIGKEIT.
>
> **Ulrich Parthier,**
> **Publisher it management,**
> **it Verlag GmbH, www.it-daily.net**

Darüber hinaus unterstützt das Self-Healing Unternehmen bei komplexen Herausforderungen wie Ressourcenoptimierung und Abbau von Software- und Infrastrukturüberkapazitäten. Ein weiterer entscheidender Aspekt ist die Beschleunigung der Anwendungsentwicklung: Durch geringeren Testaufwand und höhere Anwendungsqualität können Unternehmen Produkte schneller auf den Markt bringen.

Der Weg zur erfolgreichen Implementierung ist aber lang. Unternehmen müssen zunächst die grundlegenden Mechanismen des Automatisierungsprozesses verstehen und schrittweise einen Reifegrad erreichen, der die Verwirklichung ihrer strategischen Ziele ermöglicht.

Vorgehensweise

Die Baseline-Erstellung ist dabei entscheidend. Ähnlich wie ein Arzt Patientenakten analysiert, um individuelle Gesundheitszustände zu verstehen, müssen Unternehmen mathematische Modelle erstellen, die Normalzustände ihrer IT-Systeme definieren. Dabei werden Anwendungs-, Netzwerk-, Endbenutzer- und Infrastrukturdaten individuell betrachtet und verfolgt.

Der Automatisierungsprozess durchläuft mehrere kritische Phasen. Zunächst geht es um die Implementierung von Warnskripten, die Probleme frühzeitig erkennen und ihre Herkunft identifizieren. Diese Skripte reduzieren Fehlalarme und minimieren menschliche Fehlerquellen. Gleichzeitig verkürzen sie die Entwicklungs- und Erkennungszeiten (MTTD, MTTK), was die Reaktionsfähigkeit der IT-Systeme dramatisch verbessert.

Die eigentliche Selbstheilung beginnt, wenn Automatisierungsskripte nicht nur Probleme erkennen, sondern auch eigenständig Lösungen implementieren. Sie verkürzen Ausfallzeiten (MTTF, MTTR) und beheben Störungen, noch bevor Benutzer sie wahrnehmen. Dies führt zu einer signifikanten Verbesserung des Kundenservices und der Systemstabilität.

Entscheidend für den Erfolg ist ein ganzheitlicher Ansatz: Kontinuierliches Systemfeedback, umfassendes Problemmanagement und ständige Prozessoptimierung sind keine einmaligen Aufgaben, sondern permanente Entwicklungsarbeit. Die Technologie lernt kontinuierlich aus Erfahrungen und passt sich verändernden Systemanforderungen an.

Herausforderungen und Ausblick

Trotz der vielversprechenden Perspektiven stehen besonders kleinere und mittlere Unternehmen vor erheblichen Herausforderungen. Die erforderlichen personellen und finanziellen Ressourcen übersteigen oft ihre Möglichkeiten. Die Hoffnung liegt auf Hyperscalern, die Plattformen als Open-Source-Lösungen bereitstellen könnten.

In Zeiten der digitalen Transformation entwickeln sich IT-Selbstheilungsprozesse von einer technischen Möglichkeit zu einer strategischen Notwendigkeit. Sie sind mehr als eine Effizienzsteigerung - sie sind ein Wettbewerbsvorteil, der Unternehmen befähigt, agil, robust und zukunftsorientiert zu agieren.

Ulrich Parthier

Projektifizierung und die Renaissance des Corporate L&D

WARUM DIE INDUSTRIE DEN RAHMEN JETZT NEU SETZEN MUSS!

In der Renaissance veränderten sich Weltansichten und der Glaube an die eigene Freiheit und Wirksamkeit. Erfindungen prägten den Wandel. Es war eine Zeit der Erneuerung und des Aufbruchs. Ähnliches erleben wir gerade: Zwischen Digitalisierung und Agilität versucht der Mensch Schritt zu halten mit technologischen Entwicklungen, sozialen Ereignissen und wirtschaftlichen Umbrüchen. Dies kann nur gelingen, wenn Organisationen es schaffen, das Lernen der Mitarbeitenden zu revitalisieren und die Lernkultur zu transformieren.

Wie damals gewinnen heute Inspiration und Innovation immer mehr an Bedeutung. Um sich den Herausforderungen der sich wandelnden Märkte und der globalen Wirtschaft zu stellen, strebt die Industrie nach Transformation. Dies gilt nicht nur für Produkte, Prozesse und Abläufe, sondern für jeden Mitarbeitenden. Um den Bedürfnissen der schnelllebigen Geschäftswelt gerecht zu werden, bedarf es eines dynamischeren, relevanteren und wirkungsvolleren Ansatzes für die persönliche Entwicklung – über den fachlichen Bereich hinaus.

Die Projektifizierung der Industrie

Nie war die strategische Bedeutung des Projektmanagements größer. Die Industrie muss den Bedarf an qualifizierten Projektmanagerinnen/-managern jedoch zunächst erkennen, um ins Handeln zu kommen. Wichtiges Bindeglied ist die HR-Abteilung; doch sind die Learning and Development (L&D)-Manager gefangen im Fachkräftemangel, bleibt oft wenig Verständnis und Engagement für eine wirklich individuelle und strategische Personalentwicklung. Wie also schafft man ein Bewusstsein für die zunehmende Notwendigkeit qualifizierter PM-Professionals? Und welche überzeugenden Gründe gibt es, damit die Industrie diese Entwicklung endlich priorisiert? Eine Antwort lautet: Die unvermeidbare „Projektifizierung" wird durch drei Schlüsselfaktoren vorangetrieben:

1. **Globaler Wettbewerb und Marktdynamik:** Von digitalen Transformationsinitiativen über die Entwicklung neuer Produkte bis hin zur internationalen Expansion verlässt sich die Industrie zunehmend auf Projekte, um Wachstum zu fördern und sich an veränderte Marktbedingungen anzupassen.

2. **Technologische Fortschritte:** Die Integration fortschrittlicher Technologien wie KI, Datenanalyse und Automatisierung erfordert spezialisierte Projektmanagementfähigkeiten. Die Leitung dieser Projekte umfasst die Bewältigung von Komplexitäten und die Sicherstellung, dass technologiegetriebene Investitionen greifbaren geschäftlichen Nutzen bringen.

LEBENSLANGES LERNEN IST UNERLÄSSLICH FÜR DIE ENTWICKLUNG DES EINZELNEN, ABER EBENSO ENG VERBUNDEN MIT DER ENTWICKLUNG DES UNTERNEHMENS.

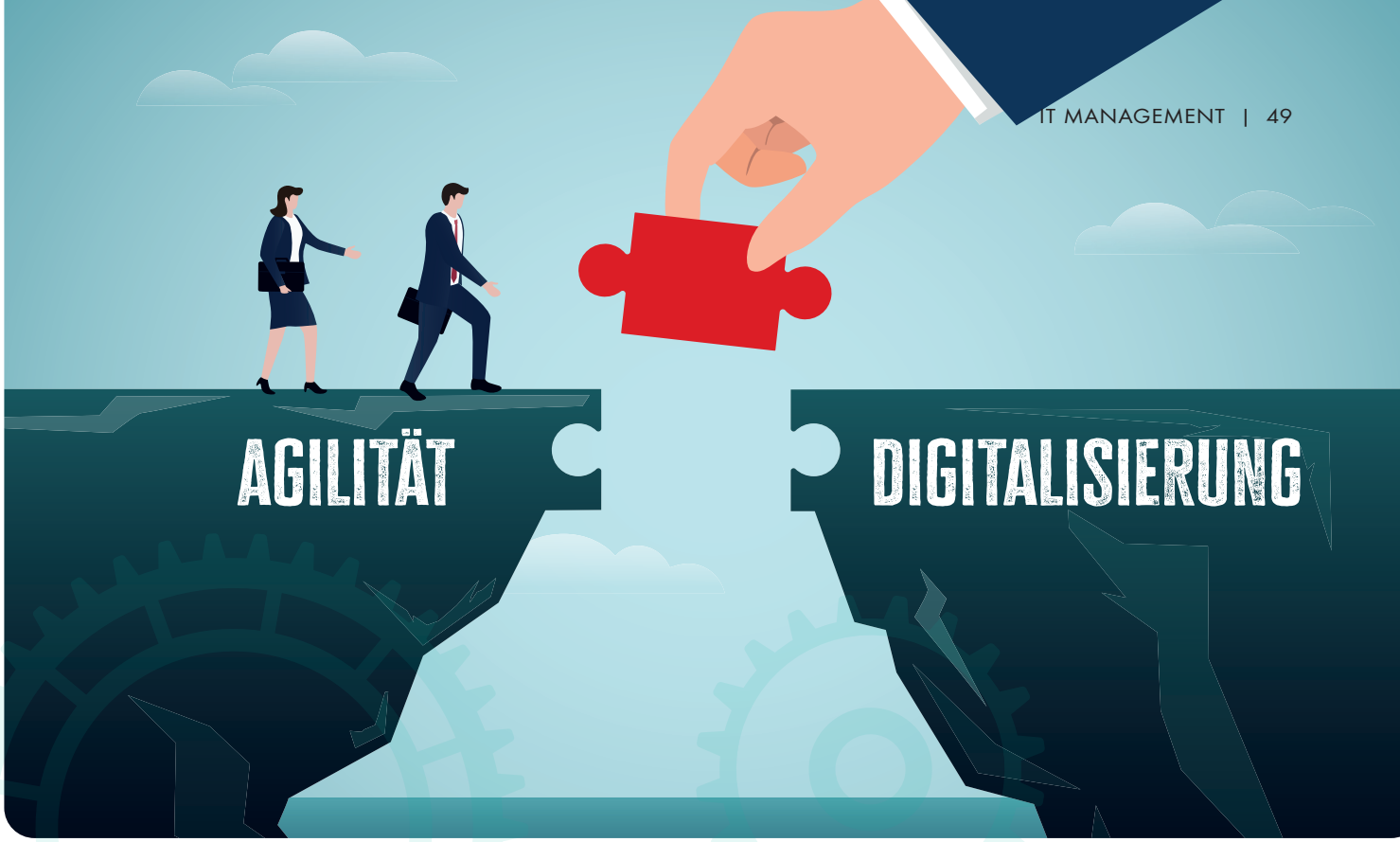
Sidra Sammi, Geschäftsentwicklung DACH, ILX Group, www.ilxgroup.com/eur

3. **Erhöhte Fokussierung auf Innovation:** Um der Konkurrenz voraus zu bleiben, investiert die Industrie in Forschungs- und Entwicklung (F&E). Diese Innovationsprojekte erfordern kompetente Projektmanager, die funktionsübergreifende Teams effektiv führen und Ressourcen verwalten können, um neue Produkte schnell auf den Markt zu bringen.

Die wachsende „Projektifizierung" der Wirtschaft hat ohne Zweifel weitreichende Auswirkungen auf die Industrie. In Verbindung mit dem Fachkräftemangel besteht ein dringender Bedarf, die Fähigkeiten der Mitarbeitenden kontinuierlich auszubauen. Technische Kompetenzen alleine reichen nicht aus, es braucht vor allem Fähigkeiten hinsichtlich Projektmanagement sowie Soft Skills, um den anstehenden Aufgaben gerecht zu werden und eine erfolgreiche Umsetzung im Team zu ermöglichen.

Die Wirkung von L&D-Initiativen maximieren

Die letzten Jahre haben es gezeigt: Digitale Transformation ist die neue Norm und zugleich ein fortlaufender Prozess. Bleiben wir hinsichtlich unserer digitalen wie methodischen Fähigkeiten nicht auf dem Laufenden, erschweren uns die Wissens- und Erfahrungslücken sowohl die Freude am Tun (individuell und im Team) als auch die Aussicht auf Erfolg. Nachfolgend sieben Schlüsselstrategien, um die Wirkung von L&D-Initiativen zu maximieren und sicherzustellen, dass Unternehmen die vollen Vorteile jeglicher Schulungsbemühungen ernten, also im Idealfall die Rendite der L&D-Investition steigern:



#1 Abstimmung von L&D mit den Unternehmenszielen

Diese Ausrichtung gewährleistet, dass jede Schulungsinitiative direkt dazu beiträgt, breitere organisatorische Meilensteine zu erreichen, sei es die Verbesserung der Kundenzufriedenheit, die Steigerung der operativen Effizienz oder die Förderung von Innovationen.

#2 Durchführung einer Kompetenzanalyse, um Wissenslücken zu identifizieren

Dies beinhaltet die Bewertung der aktuellen Kompetenzen der Mitarbeitenden, das Verständnis der Anforderungen ihrer Rollen und die Vorhersage zukünftiger Branchentrends, die sich auf das Unternehmen auswirken können. Durch die Anpassung der L&D-Strategie an diese identifizierten Bedürfnisse gewährleistet eine Organisation die Relevanz und den Wert ihrer Schulungsprogramme.

#3 Verwendung von Technologie

Online-Schulungen ermöglichen es den Lernenden, jederzeit und überall auf Kursmaterial zuzugreifen, was den unterschiedlichen Lernstilen und Zeitplänen gerecht wird. Die Integration dieser Technologien in die L&D-Strategie kann die Teilnahme- und Abschlussraten dramatisch erhöhen.

#4 Nutzen von Daten

Die Integration von Datenanalytik ermöglicht eine kontinuierliche Verbesserung der Schulungsprogramme, um sicherzustellen, dass sie effektiv sind und den Bedürfnissen der Lernenden und der Organisation gerecht werden. Datenanalytik kann auch dazu beitragen, das Lernerlebnis zu personalisieren und dessen Wirksamkeit zu steigern.

#5 Etablieren einer Kultur, die kontinuierliches Lernen wertschätzt

Die Befähigung der Mitarbeitenden, ihre eigene Lernreise in die Hand zu nehmen, ist entscheidend für die Förderung einer Kultur der kontinuierlichen Verbesserung. Unternehmen müssen vermehrt Ressourcen und Tools bereitstellen, die selbstgesteuertes Lernen unterstützen. Es kann auch hilfreich sein, Initiativen der Mitarbeitenden zur Weiterentwicklung ihrer Fähigkeiten anzuerkennen und zu belohnen.

#6 Förderung des Wissensaustausches

Unternehmen sollten Möglichkeiten für Mitarbeitende schaffen, ihre Erkenntnisse und Erfahrungen mit ihren Kollegen durch Mentoring-Programme, Workshops und Diskussionsforen zu teilen. Dies festigt das Wissen und fördert eine kooperative und unterstützende Lernumgebung innerhalb der Organisation.

#7 Erfassen von Auswirkungen und Ergebnissen

Um den Erfolg einer L&D-Strategie zu bestimmen, ist es entscheidend, ihre Auswirkungen sowohl auf die Leistung der Lernenden als auch auf die Geschäftsergebnisse zu messen. Ideal dafür ist eine Kombination aus quantitativen (z. B. Abschlussraten von Kursen, Testergebnisse) und qualitativen (z. B. Rückmeldungen der Lernenden, Verhaltensänderungen) Kennzahlen, um die Wirksamkeit von Schulungsprogrammen zu bewerten.

Fazit

Lebenslanges Lernen ist unerlässlich für die Entwicklung des Einzelnen, aber ebenso eng verbunden mit der Entwicklung des Unternehmens – das zeigt sich vor allem im Bereich Corporate L&D. Bleibt zu hoffen, dass die Industrie die Chance dieser modernen Renaissance erkennt. Dann steht der „Wiedergeburt" unserer innovativen deutschen Wirtschaft nichts mehr im Wege.

Sidra Sammi

UNSERE THEMEN

it management

Fokusthema: Cloud & Edge Computing

Schwerpunktthemen: Unified Communications, 5G, ITSM, Storage, Software Testing, Data Center & Data Management

Die Ausgabe 05/06 2025 erscheint am 14. Mai 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

IMPRESSUM

Herausgeber: Ulrich Parthier (08104-6494-14)

Geschäftsführer: Ulrich Parthier, Vasiliki Miridakis

Chefredaktion: Silvia Parthier (-26)

Redaktion: Carina Mitzschke (nur per Mail erreichbar)

Redaktionsassistenz und Sonderdrucke: Eva Neff (-15)

Autoren: Lars Becker, Lisa Burr, Marco Heid, Tobias Knieper, Carina Mitzschke, Angelika Mühleck, Naeem Nazari, Silvia Parthier, Ulrich Parthier, Prof. Dr. Peter Preuss, Sidra Sammi, Linda Schmittner, Sebastian Weber, Constantin Wehmschulte, Tendü Yogurtçu

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

Online Campaign Manager:
Roxana Grabenhofer, 08104-6494-21, grabenhofer@it-verlag.de
Head of Marketing:
Vicky Miridakis, 08104-6494-15, miridakis@it-verlag.de

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

Erscheinungsweise: 6 x pro Jahr

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

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

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

e3mag.com

SUMMIT DER SAP-COMMUNITY

COMPETENCE CENTER

Salzburg
21. und 22. Mai 2025

CC-Summit Themen 2025

Als SAP-Bestandskunde brauchen Sie ein Customer Center of Expertise, nur so erreichen Sie das volle S/4-Potenzial.

- ✓ Customer CoE: Single Source of Truth
- ✓ Support Desk für SAP S/4 Hana
- ✓ SolMan, Cloud ALM und SAP-Monitoring
- ✓ Basissupport: Rise und Grow with SAP
- ✓ SAP Security und Compliance
- ✓ Process Mining und ERP-Architektur
- ✓ S/4-Conversion und Hana

Teil-nahmegebühr **590,–** Euro (netto)

Wird gesponsert von:

CONSILIO

e3mag.com/de/cc-summit

#DeinMeinBusiness

Teamwork? Aber sicher!

Schützen dein Team vor Gefahren im Netz: unsere Sicherheitslösungen. Jetzt kostenfrei in allen T Business Mobilfunktarifen.*

Die T Business Mobilfunk-Deals

Connecting your world.

Hier mehr erfahren:

it security

Detect. Protect. Respond.
März/April 2025

SCHUTZ SENSIBLER UNTERNEHMENSDATEN

Datensicherheit mit AI Mesh

Frank Limberger, Forcepoint

CYBER-VERSICHERUNG

Cybercrime: Im Fadenkreuz der Hacker

SPEZIAL: IAM, PAM, CIAM

Die digitale Verteidigungslinie ist unverzichtbar

KI UND 24/7-SERVICE

Ransomware-Angriffe abwehren

www.it-daily.net

6. – 9. Mai, **bcc Berlin Congress Center / online**

eic european identity and cloud conference 2025

Pionierarbeit für digitale Identitätsökosysteme

EIC 2025: Seien Sie dabei!

Die European Identity and Cloud Conference (EIC) 2025 ist das führende Event für digitale Identität, Sicherheit, Datenschutz und Governance in einer KI-gesteuerten Welt.

Warum an der EIC 2025 teilnehmen?

Expertenwissen

- **Lernen Sie von über 300 Branchenführern und Vordenkern.**
- **Umfassende Agenda:** Nehmen Sie an mehr als 230 Sessions teil, die die neuesten Trends und Herausforderungen im Bereich digitale Identität, Sicherheit und Datenschutz in einer KI-gesteuerten Welt behandeln.
- **Networking Möglichkeiten:** Knüpfen Sie Kontakte mit über 1.500 Fachleuten aus der ganzen Welt.
- **Innovative Lösungen:** Entdecke die neuesten Technologien und Strategien zur Verbesserung der Sicherheitslage deines Unternehmens.

Key Topics:

- Decentralized Identity
- Enterprise Identity und Access Management
- eIDAS2, ID Wallets, Travel credentials
- B2B Identity Management und Onboarding
- Identität in einer KI-Welt (AI Tech Stack, Retrieval-Augmented Generation, AI Act)
- Datenschutz und Datensicherheit
- Moderne Authentifizierungsansätze (AuthZ)
- ... und vieles mehr!

Sichern Sie sich Ihren Platz!

Early-Bird-Rabatt bis 14. März

Besuchen Sie **kuppingercole.com/events/eic2025** um sich zu registrieren und mehr über das Konferenzprogramm und die Speaker zu erfahren.

kuppingercole ANALYSTS

Inhalt

COVERSTORY

SPEZIAL: IAM, PAM, CIAM

IT SECURITY

Datensicherheit mit AI Mesh

SCHUTZ SENSIBLER UNTERNEHMENSDATEN

Frank Limberger ist Data & Insider Threat Security Specialist bei Forcepoint in München. Im Interview erläutert er, warum an datenzentrierter IT-Sicherheit kein Weg mehr vorbeiführt und weshalb sich Unternehmen vor der Klassifizierung ihrer Daten nicht mehr fürchten müssen.

it security: *Die IT-Security entwickelt sich zunehmend von netzwerkbasierter Sicherheit hin zu einem datenzentrierten Ansatz. Was steckt hinter diesem Trend?*

Frank Limberger: Die herkömmlichen Sicherheitsansätze, die sich auf den Schutz des Netzwerks und des Perimeters konzentrieren, reichen in Zeiten von Cloud, SaaS, GenAI und Remote Work nicht mehr aus. Früher verließen beispielsweise die Entwicklungsdaten von Unternehmen nie die interne Datenbank. Da genügte es, die Zugänge zu dieser Datenbank abzusichern. Heute kopiert ein Mitarbeiter Daten heraus, fügt sie in eine Präsentation ein und legt diese in SharePoint Online ab, um sie in einem Meeting mit Kollegen oder Kunden zu teilen. In der Cloud haben diese sensiblen Informationen aber ein niedrigeres Schutzniveau und sind dadurch einem erhöhten Risiko ausgesetzt.

Im modernen, verteilten IT-Umgebungen ist ein anderer Ansatz erforderlich. Unternehmen müssen Daten unabhängig von ihrem Speicherort schützen. Das geht nur, indem sie die Daten selbst schützen. Sie müssen ihnen eine Vertraulichkeitsstufe zuweisen und daraus ableiten, was mit ihnen getan werden darf und was nicht. Nur so können sie dem Verlust von geistigem Eigentum vorbeugen und die immer zahlreicheren Compliance-Anforderungen erfüllen.

it security: *Cloud-Plattformen, SaaS-Anwendungen oder GenAI-Tools einfach zu verbieten, ist nicht wirklich eine Alternative, oder? Sie werden ja schließlich aus guten Gründen genutzt.*

Frank Limberger: Genau. Unternehmen treiben den Einsatz dieser Technologien ja selbst voran, weil sie von Vorteilen wie Flexibilität, Produktivität, Skalierbarkeit und ortsunabhängigem Zugriff profitieren. Außerdem würde das auch gar nicht funktionieren. Unternehmen können solche Dienste zwar mit URL- oder DNS-Filtern sperren, aber nur innerhalb des Unternehmensnetzwerks. Mitarbeiter können diese Sperren leicht umgehen, indem sie mobil oder im Homeoffice darauf zugreifen. Dadurch würde eine gefährliche Schatten-IT entstehen, die sich der Kontrolle der Unternehmen vollständig entzieht. Deshalb ist es besser, dafür zu sorgen, dass die Mitarbeiter diese Dienste ohne erhöhte Risiken nutzen können.

> SENSIBLE DATEN LASSEN SICH HEUTE AUTOMATISIERT AUFSPÜREN UND KLASSIFIZIEREN.
>
> **Frank Limberger, Data & Insider Threat Security Specialist, Forcepoint, www.forcepoint.com**

it security: *Wie sieht das konkret aus? Wie können Unternehmen datenzentrierte IT-Sicherheit in der Praxis umsetzen?*

Frank Limberger: Im Wesentlichen durch die Kombination von Data Loss Prevention (DLP) mit Data Security Posture Management (DSPM). Eine DLP-Software kann Datenflüsse überwachen und Verstöße gegen Datensicherheits-Richtlinien verhindern. Spezielle Agenten auf den Endgeräten gewährleisten dabei, dass diese Richtlinien auch außerhalb des Unternehmensnetzwerks durchgesetzt werden. Eine enge Integration des DLP mit anderen Sicherheitstools stellt zudem sicher, dass den Richtlinien auch über sämtliche Kanäle hinweg Geltung verschafft wird. Zu diesen Tools zählt beispielsweise ein Cloud Access Security Broker, der den Zugriff auf Cloud-Dienste überwacht und steuert. Wenn bestimmte Daten als streng vertraulich eingestuft sind, können sie dann beispielsweise weder in eine Cloud hochgeladen, noch per E-Mail verschickt noch im Homeoffice ausgedruckt werden.

Ein DLP-System ist aber auf korrekt klassifizierte Daten angewiesen. Das war früher ein großes Problem, weil die Klassifizierung manuell durchgeführt werden musste. Dieses Vorgehen ist aber ungenau und meist ein Fass ohne Boden. Viele Unternehmen haben Klassifizierungsprojekte abgebrochen, weil sie feststellen mussten, dass sie ihrem ständig anwachsenden Datenbestand nicht mehr hinterherkommen. Einmal ganz davon abgesehen, dass Unternehmen in den heutigen verteilten IT-Umgebungen oft gar keinen Überblick mehr darüber haben, wo sich ihre Daten überhaupt befinden. Moderne DSPM-Lösungen räumen dieses Hindernis jetzt aus dem Weg. Sie ermöglichen es, Daten automatisiert aufzuspüren und auch automatisiert exakt und fortlaufend zu klassifizieren.

it security: *Wie funktionieren die DSPM-Lösungen genau?*

Frank Limberger: Eine DSPM-Software ist im Grunde genommen ein intelligentes Tool für die Analyse von Content. Besonders Lösungen, die auf der AI-Mesh-Technologie basieren, erhöhen die Genauigkeit bei der Datenerkennung entscheidend. Unternehmen stellen dem Tool zunächst Beispiele für schützenswerte Daten wie Kundenlisten, Konstruktionszeichnungen, Code-Stücke oder Präsentationen zur Verfügung. Die Software analysiert dann diese Beispiele und ist von da an in der Lage, ähnliche Daten aufzuspüren und entsprechend zu klassifizieren. Und zwar unabhängig davon, ob sie auf firmeneigenen Servern, in Clouds oder auf den Endgeräten der Mitarbeiter liegen. Diese Scans können in regelmäßigen Abständen immer wieder durchgeführt werden, so dass auch neu hinzukommende Daten kontinuierlich erfasst und klassifiziert werden.

it security: *Was ist unter einem AI Mesh zu verstehen?*

Frank Limberger: Ein AI Mesh ist ein vernetztes System aus mehreren KI-Komponenten, das dezentral arbeitet und sich selbstständig optimiert. Beim AI Mesh von Forcepoint steht dabei ein GenAI Small Language Model im Zentrum. Es bietet im Vergleich mit Large Language Models, wie man sie etwa von ChatGPT kennt, mehrere Vorteile. Es ist wesentlich effizienter, wodurch das System bis zu 300 Files pro Sekunde analysieren und klassifizieren kann. Außerdem ist das Modell überschaubar, so dass Unternehmen nachvollziehen können, wie es zu den jeweiligen Klassifizierungen kommt. Die Scan-Prozesse unseres AI Mesh werden von On-Premises-Servern aus gesteuert. Dadurch fließen keine Informationen über die sensiblen Inhalte der Unternehmen an einen Cloud-Dienst. Sonst würden sich die Unternehmen in Sachen Datensicherheit ein größeres Problem ins Haus holen, als das, was sie lösen möchten.

it security: *Sie haben bereits die GenAI-Tools erwähnt, die ja inzwischen von immer mehr Mitarbeitern genutzt werden. Welche Datenrisiken gehen von diesen Tools aus?*

Frank Limberger: Wenn sensible oder kundenbezogene Informationen in solche Tools eingegeben werden, kann das geistiges Eigentum gefährden und Verstöße gegen Datenschutzgesetze bedeuten. Viele GenAI-Anbieter verarbeiten die Daten auf Systemen in Ländern, deren Datenschutzniveau nicht dem Niveau der Europäischen Union und damit auch nicht den Anforderungen der DSGVO entspricht. Außerdem nutzen die Anbieter die eingegebenen Informationen zur laufenden Optimierung ihrer Modelle. Wenn beispielsweise jemand einen Quellcode für eine kritische IT-Komponente schreibt, und diesen Code zur Optimierung in ein GenAI-Tool kopiert, riskiert er, dass Andere diesen Code aus dem Tool herausbekommen können. Ein DLP kann das verhindern, indem es das Kopieren dieses kritischen Codes blockiert. Harmlosen Code dagegen können sich die Mitarbeiter auch weiterhin von GenAI optimieren lassen.

it security: *Herr Limberger, vielen Dank für das Gespräch.*

Datensicherheit neu gedacht

RISIKO-ADAPTIVER SCHUTZ STATT SCHWARZ-WEISS-REGELN

Klassische Lösungen für Datensicherheit setzen auf Regeln, die nur Schwarz und Weiß kennen: Aktivitäten werden entweder geblockt oder gestattet. Dieser Ansatz hat Schwächen, weil er meist sehr restriktiv umgesetzt wird und die Mitarbeiter im Arbeitsalltag behindert. Besser geeignet sind Lösungen, die Sicherheitsmaßnahmen in Echtzeit an das jeweilige Risiko anpassen.

Die neue Arbeitswelt mit Remote Work und Cloud-Services birgt aus Security-Sicht viele Herausforderungen, weil sich nur noch schwer bestimmen lässt, welche Aktivitäten die Datensicherheit gefährden und welche nicht. Handelt es sich beim Download einer Datei vom zentralen Server auf einen Rechner außerhalb des Unternehmensnetzwerks um eine normale geschäftliche Aktivität oder einen Datendiebstahl? Welche Dokumente dürfen Mitarbeiter auf USB-Sticks kopieren, per E-Mail verschicken oder von einem KI-Service in der Cloud auswerten lassen? Und ist es okay, im Online-Meeting einen Screenshot der dort gezeigten Präsentation mit Finanzdaten zu machen?

All diese Vorgänge lassen sich mit starren Richtlinien kaum beherrschen, denn diese stellen Security-Teams mangels Flexibilität vor ein Dilemma. Entweder sorgen sie mit sehr restriktiven Richtlinien für Frust bei den Mitarbeitern, weil viele Aktivitäten schlicht nicht gestattet sind und blockiert werden. Dadurch sinken Produktivität und Motivation – und es steigt die Gefahr, dass Mitarbeiter versuchen, die Sicherheitsmaßnahmen zu umgehen. Oder sie gestalten die Richtlinien weniger restriktiv, um Mitarbeiter im Arbeitsalltag nicht zu behindern, und lassen damit womöglich Lücken im Schutz. In der Regel entscheiden sich Security-Teams für die erste Variante, da Datenabflüsse einfach ein zu großes geschäftliches Risiko darstellen.

Zwar können Unternehmen mit Awareness-Schulungen das Bewusstsein ihrer Mitarbeiter für den verantwortungsvollen Umgang mit sensiblen Daten schärfen. Einen wirklich zuverlässigen Schutz garantiert das allerdings nicht, denn Mitarbeiter können – gerade in hektischen Arbeitssituationen – unaufmerksam sein oder Fehleinschätzungen unterliegen. Und auch gegen Insider-Bedrohungen und den Missbrauch kompromittierter Benutzer-Accounts helfen Schulungen nicht, sodass bei klassischen Lösungen für Datensicherheit üblicherweise kein Weg an restriktiven Richtlinien vorbeiführt.

Schärfere Sicherheitsmaßnahmen für riskante Aktivitäten

Eine Alternative stellen moderne Lösungen dar, die einen Risiko-adaptiven Ansatz verfolgen. Sie berücksichtigen Anwenderaktivitäten und deren Kontext, um das Risiko zu ermitteln und geeignete Sicherheitsmaßnahmen einzuleiten. So kann beispielsweise das Kopieren von Daten auf einen USB-Stick ohne Einschränkungen erlaubt sein, einen kurzen Warnhinweis hervorrufen, eine Verschlüsselung auslösen oder sogar komplett blockiert werden – je nachdem, welchen „Risk Score" ein Anwender hat. Dahinter steht eine einzige Richtlinie, die durch den Risk Score dynamisch und in Echtzeit angepasst wird – in diesem Fall die Richtlinie für das Kopieren von Daten auf USB-Medien.

Den Risk Score berechnet die Sicherheitslösung anhand der Aktivitäten des Anwenders beziehungsweise sogenannter Verhaltensindikatoren. Das sind Aktionen wie das Erstellen, Speichern, Bearbeiten, Herunterladen, Löschen und Versenden von Dokumenten, das Installieren von Anwendungen, das automatische Weiterleiten von E-Mails und das Komprimieren von Dateien in verschlüsselten Archiven.

Die einzelnen Verhaltensindikatoren beeinflussen den Risk Score unterschiedlich stark: Der Upload eines unverfänglichen Dokuments mit technischen Informationen in die Cloud etwa erhöht ihn kaum, das Speichern von Vertragsdokumenten auf einem USB-Stick hingegen deutlich. Bei bestimmten Schwellenwerten werden die Sicherheitsmaßnahmen verschärft, sodass Aktivitäten, die ursprünglich möglich gewesen wären, einigen Restriktionen unterliegen. Die Kundenliste kann zum Beispiel nur noch verschlüsselt auf dem Speicherstick abgelegt werden. Besonders kritische Aktivitäten wie der Versand von Kundenlisten, Konstruktionsdaten oder Finanzinformationen per E-Mail an Empfänger außerhalb des Unternehmens heben den Risk Score auf einen Schlag so stark an, dass die Aktivitäten sofort blockiert werden.

Optimale Risikobewertung mit KI und Machine Learning

Um einen schnellen Schutz zu bieten, nutzen gute Datensicherheitslösungen smarte Funktionen für Data Discovery und Datenklassifizierung. Diese spüren Daten über alle Speicherorte des Unternehmens hinweg auf und nehmen mit Hilfe von KI und Machine Learning eine automatische Einstufung in verschiedene Kategorien vor. Darüber hinaus nutzen sie ein Fingerprinting der Dateiinhalte anstatt einen Hashwert der gesamten Datei zu erstellen. So können schützenswerte Daten, die von Fachbereichen bereitgestellt werden, wie zum Beispiel Code-Fragmente, Auszüge aus vertraulichen Dokumenten oder personenbezogene Daten, zuverlässig identifiziert werden – unabhängig davon, auf welchem Weg sie das Unternehmen zu verlassen drohen. Der Risk Score erhöht sich also auch dann, wenn Anwender statt der gesamten Datei nur einen Teil des Inhalts in eine Mail, einen Chat oder das Eingabefeld eines Online-Übersetzungsdienstes kopieren. Selbst in Screenshots versteckt Inhalte werden dank OCR-Funktionen (Optical Character Recognition) aufgespürt und erkannt.

Darüber hinaus nutzen die Sicherheitslösungen maschinelles Lernen, um zu verstehen, wie normales Benutzerverhalten aussieht, sodass sie abweichende Aktivitäten identifizieren und den Risk Score entsprechend anpassen können. Eine Anomalie wäre beispielsweise der Download großer Datenmengen, wenn der betreffende Anwender sonst eigentlich nur einzelne Dokumente aus der Cloud oder vom File-Server abruft.

Security ohne Einschränkungen im Arbeitsalltag

Wenn keine neuen Verhaltensindikatoren erkannt werden, sinkt der Risk Score im Laufe der Zeit wieder, sodass Anwender nicht dauerhaft durch die zusätzlichen Sicherheitsmaßnahmen eingeschränkt werden. Dann können sie Dokumente zum Beispiel wieder unverschlüsselt auf USB-Sticks kopieren und bekommen nur einen kurzen Warnhinweis angezeigt, dass das gegen Richtlinien verstoßen könnte.

Auf diese Weise verhindern Datensicherheitslösungen mit Risiko-adaptivem Schutz nicht nur, dass Anwender sensible Daten versehentlich oder absichtlich gefährden, sondern auch dass Cyberkriminelle kompromittierte Accounts nutzen, um sensible Daten zu entwenden. Die Sicherheitsmaßnahmen schränken die Anwender im Normalfall nicht ein und werden erst verschärft, wenn mehrere Aktivitäten in der Gesamtbetrachtung auf ein erhöhtes Risiko hindeuten oder einzelne Aktivitäten besonders sensible Daten betreffen.

Fabian Glöser

> UM EINEN SCHNELLEN SCHUTZ ZU BIETEN, NUTZEN GUTE DATENSICHERHEITSLÖSUNGEN SMARTE FUNKTIONEN FÜR DATA DISCOVERY UND DATENKLASSIFIZIERUNG.
>
> **Fabian Glöser, Team Lead Sales Engineering, Nordics, Central- & Eastern-Europe, Forcepoint, www.forcepoint.com**

PRAXISBUCH ISO/IEC 27001

MANAGEMENT DER INFORMATIONSSICHERHEIT UND VORBEREITUNG AUF DIE ZERTIFIZIERUNG

Praxisbuch ISO/IEC 27001

- Management der Informationssicherheit und Vorbereitung auf die Zertifizierung; Michael Brenner, Nils gentschen Felde, Wolfgang Hommel, Stefan Metzger, Helmut Reiser, Thomas Schaaf; Carl Hanser Verlag GmbH & Co.KG; 07-2024

Informationen sind das wertvollste Kapital vieler Organisationen. Geraten sie in falsche Hände, kann sogar das Überleben eines Unternehmens gefährdet sein.

Zur Informationssicherheit müssen alle ihren Beitrag leisten, von der Arbeitsebene bis zum Topmanagement. Die ISO/IEC 27001 stellt dabei die wichtigste internationale Norm dar, an der man praktisch in keiner Branche vorbeikommt. Ein dieser Norm entsprechendes Informationssicherheitsmanagementsystem (ISMS) ist zunehmend Voraussetzung für die Erfüllung von Kunden-Anforderungen sowie von gesetzlichen und behördlichen Vorgaben, unter anderem im Rahmen des IT-Sicherheitsgesetzes.

In diesem Buch erhalten Sie die optimale Unterstützung für den Aufbau eines wirksamen ISMS. Die Autoren vermitteln zunächst das notwendige Basiswissen zur ISO/IEC 27001 sowie zur übergeordneten Normenreihe und erklären anschaulich die Grundlagen. Im Hauptteil finden Sie alle wesentlichen Teile der deutschen Fassung der Norm, DIN EN ISO/IEC 27001, im Wortlaut. Hilfreiche Erläuterungen, wertvolle Praxistipps für Maßnahmen und Auditnachweise helfen Ihnen bei der Umsetzung der Norm. Ebenfalls enthalten sind Prüfungsfragen und -antworten, mit deren Hilfe Sie sich optimal auf Ihre persönliche Foundation-Zertifizierung vorbereiten können.

AUS DEM INHALT (Auszug)

- Einführung und Basiswissen
- Die Standardfamilie ISO/IEC 27000 im Überblick
- Grundlagen von Informationssicherheitsmanagementsystemen
- Spezifikationen und Mindestanforderungen
- Maßnahmen im Rahmen des ISMS
- Verwandte Standards und Rahmenwerke
- Zertifizierungsmöglichkeiten und Begriffsbildung nach ISO/IEC 27000

IAM, PAM, CIAM – SICHERES FUNDAMENT FÜR DIGITALE INFRASTRUKTUREN

Die Unternehmens-IT steht vor unterschiedlichsten Herausforderungen, sei es die digitale Transformation, komplexe Compliance-Anforderungen, zunehmende Ransomware-Angriffe oder wachsende Kosten in allen Bereichen.

Vor ganz besondere Herausforderungen stellt IT-Entscheider aber die Identitätsverwaltung. Zwar ergeben sich bei Identity and Access Management (IAM), Privileged Access Management (PAM) und Customer Identity Access Management (CIAM) Überschneidungen, sie haben aber unterschiedliche Funktionen. Während das IAM die grundlegende Verwaltung von Mitarbeiterzugängen übernimmt, schützt das PAM besonders kritische Administrative-Zugänge. Das Customer Identity and Access Management wiederum optimiert die Verwaltung externer Nutzer wie Kunden und Partner.

Diese drei Säulen unterscheiden sich in ihren Anforderungen, bilden aber gemeinsam das Fundament einer sicheren digitalen Infrastruktur.

Die digitale Verteidigungslinie

CIAM ALS STRATEGISCHES ELEMENT MODERNER FINANZINSTITUTE

Die Digitalisierung des Bankwesens schreitet unaufhaltsam voran, doch mit ihr wachsen auch die Risiken. Finanzinstitute sehen sich zunehmend komplexen Cyberbedrohungen wie Account Takeover, Phishing und Credential-Stuffing ausgesetzt. Allein 2023 wurden mehr als 40 Prozent der Cyberangriffe auf die Finanzbranche verzeichnet – ein alarmierender Trend, der umfassende Sicherheitsmaßnahmen erfordert. Gleichzeitig steigen die Erwartungen der Kunden an nahtlose und sichere digitale Interaktionen. In dieser anspruchsvollen Gemengelage hat sich Customer Identity and Access Management (CIAM) als essenzieller Baustein etabliert, der Sicherheit, Compliance und Nutzerfreundlichkeit in Einklang bringt.

Herausforderungen in der Cybersicherheit: Banken im Visier

Banken sind seit jeher ein beliebtes Ziel für Cyberkriminelle. Mit der zunehmenden Digitalisierung des Sektors steigt die Angriffsfläche jedoch exponentiell. Besonders kritisch sind Angriffe auf Authentifizierungsprozesse, die direkten Zugang zu Konten und sensiblen Daten ermöglichen. Veraltete Sicherheitsmethoden wie statische Passwörter oder One-Time Passwords (OTP) sind den ausgeklügelten Angriffsmethoden nicht mehr gewachsen.

Hinzu kommt der regulatorische Druck: Vorgaben wie die EU-Datenschutz-Grundverordnung (DSGVO), die Zweite Zahlungsdiensterichtlinie (PSD2), die neue NIS2-Richtlinie und die Digital Operational Resilience Act (DORA) verlangen von Banken und Finanzdienstleistern eine kontinuierliche Anpassung ihrer Sicherheitsmaßnahmen. Diese Regularien fordern nicht nur den Schutz personenbezogener Daten, sondern auch umfassende Audit-Fähigkeiten und dokumentierte Prozesse zur Einhaltung von Compliance.

Darüber hinaus stehen viele Banken vor der Herausforderung, historisch gewachsene IT-Architekturen mit modernen Anforderungen zu vereinen. Heterogene Systeme, fragmentierte Datenstrukturen und isolierte Anwendungen erschweren die Einführung konsistenter und zukunftssicherer Sicherheitslösungen.

DIE FORTSCHREITENDE DIGITALISIERUNG DES BANKENSEKTORS MACHT CIAM-LÖSUNGEN ZU EINER UNVERZICHTBAREN GRUNDLAGE FÜR SICHERHEIT UND BENUTZERFREUNDLICHKEIT.

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

Wie CIAM Banken zukunftssicher macht

Moderne CIAM-Lösungen bieten Banken die Möglichkeit, Sicherheitsrisiken proaktiv zu bewältigen und gleichzeitig eine benutzerfreundliche Erfahrung zu gewährleisten. Kernfunktionen sind unter anderem:

➤ **Dynamische Sicherheitsmaßnahmen für präzise Bedrohungserkennung:** Moderne CIAM-Systeme setzen auf adaptive Sicherheitsmaßnahmen, die sich in Echtzeit an das Verhalten der Nutzer anpassen. Mithilfe von Risk-Based Authentication (RBA) analysiert die Lösung die verschiedenen Parameter Standort, Gerätetyp, Login-Zeiten und Nutzerhistorie. Erkennt das System eine Anomalie, kann es automatisch zusätzliche Verifikationsstufen wie biometrische Authentifizierung oder Multi-Faktor-Authentifizierung (MFA) aktivieren. Diese proaktive Sicherheitsstrategie minimiert das Risiko von Kontoübernahmen und unbefugtem Zugriff.

➤ **Mehr Sicherheit, weniger Angriffsfläche durch Passwortlose Authentifizierung:** Passwörter gehören zu den größten Sicherheitsrisiken im Finanzsektor. Phishing, Credential-Stuffing und Datenlecks machen statische Passwörter zunehmend unsicher. CIAM ermöglicht die Einführung passwortloser Authentifizierungsmethoden wie FIDO2-basierte Lösungen, biometrische Verfahren (Gesichtserkennung, Fingerabdruck) oder Public-Key-Kryptografie. Diese Methoden reduzieren nicht nur das Risiko kompromittierter Zugangs-

daten, sondern verbessern auch die Nutzerfreundlichkeit, indem sie Login-Prozesse vereinfachen.

➤ **Plattformübergreifende Integration und Identity Federation:** Finanzinstitute betreiben oft historisch gewachsene IT-Infrastrukturen mit isolierten Systemen und fragmentierten Datenbanken. CIAM löst dieses Problem durch eine zentralisierte Identitätsverwaltung, die sich über verschiedene Plattformen und Anwendungen hinweg erstreckt. Technologien wie Identity Federation und Single Sign-On (SSO) ermöglichen es Kunden, mit nur einer Anmeldung auf verschiedene Services zuzugreifen – unabhängig davon, ob es sich um Online-Banking, mobile Apps oder Drittanbieter-Dienste handelt.

➤ **Erfüllung regulatorischer Vorgaben durch Compliance-by-Design:** Regulierungsrahmen wie DSGVO, PSD2, DORA und NIS2 erfordern von Banken detaillierte Nachweise über Sicherheitsmaßnahmen und Zugriffskontrollen. CIAM-Systeme bieten Audit-Trails, automatisierte Protokollierung und fein abgestufte Berechtigungsverwaltung, um regulatorische Anforderungen effizient umzusetzen. Zusätzlich stellen Privacy-by-Design- und Zero-Trust-Modelle sicher, dass personenbezogene Daten geschützt und nur minimal verarbeitet werden.

CIAM als Wettbewerbsvorteil

Die fortschreitende Digitalisierung des Bankensektors macht CIAM-Lösungen zu einer unverzichtbaren Grundlage für Sicherheit und Benutzerfreundlichkeit. Sie verbinden höchste Sicherheitsstandards mit einer positiven Benutzererfahrung und ermöglichen es Finanzinstituten, auf die wachsenden Anforderungen durch Cyberangriffe und regulatorische Vorgaben zu reagieren. Die erfolgreiche Umsetzung bei SIX (siehe Box) zeigt, wie eine strategische CIAM-Integration nicht nur bestehende Herausforderungen adressiert, sondern auch die Basis für zukünftige Innovationen schafft.

Angesichts der sich stetig wandelnden Bedrohungslandschaft ist CIAM für Banken weit mehr als eine technologische Lösung – es ist ein zentraler Baustein für ihre Wettbewerbsfähigkeit und Zukunftssicherheit.

Stephan Schweizer

PRAXISBEISPIEL: SIX UND NEVIS

SIX, Betreiberin der Finanzinfrastruktur für 120 Banken in der Schweiz und Spanien, zeigt eindrucksvoll, wie CIAM-Technologien in der Praxis funktionieren können. Die Einführung einer modernen CIAM-Plattform ermöglichte es SIX, ihre IT-Infrastruktur umfassend zu modernisieren und die höchsten Sicherheitsstandards zu erfüllen.
Mit täglich bis zu 80.000 Authentifizierungsanfragen in Spitzenzeiten hat SIX eine Plattform etabliert, die sowohl skalierbar als auch hochperformant ist, was für eine kontinuierliche Verfügbarkeit sorgt – 24 Stunden am Tag, 365 Tage im Jahr.
Ein zentraler Meilenstein war die Konsolidierung von mehreren separaten Plattformen in eine einheitliche Architektur. Dies harmonisierte nicht nur die Sicherheitsprozesse, sondern reduzierte auch den Wartungsaufwand.
Durch den Einsatz moderner CIAM-Technologien konnte SIX die strengen regulatorischen Anforderungen der Finanzbranche problemlos erfüllen. Identity Federation, Multi-Faktor-Authentifizierung und Datenschutz-by-Design-Ansätze bieten den Nutzern eine komfortable und gleichzeitig sichere Zugriffssteuerung. Dies stärkte nicht nur die Kundenbindung, sondern reduzierte auch Risiken wie Session-Hijacking oder Credential-Stuffing.

Fortschrittliches PAM

PROAKTIVE STRATEGIEN FÜR LANGFRISTIGE SICHERHEIT

Kompromittierte Zugangsdaten gehören zu den Hauptauslösern vieler Sicherheitsverletzungen. Mit einem fortschrittlichen PAM-Programm können Unternehmen gezielt privilegierte Zugriffe sichern und Bedrohungen frühzeitig erkennen. So gelingt die erfolgreiche Umsetzung.

Kompromittierte Zugangsdaten sind heute die Hauptursache für die meisten Sicherheitsverletzungen. Gleichzeitig macht die immer komplexer werdende IT-Landschaft es für Unternehmen schwerer, privilegierte Zugriffe abzusichern. Standardmaßnahmen wie einfache Zugriffskontrollen und Passwortverwaltung reichen längst nicht mehr aus, um diesen Herausforderungen zu begegnen. Stattdessen müssen Unternehmen auf ein „Fortschrittliches Private Access Management (PAM)" setzen, das über grundlegende Schutzmaßnahmen hinausgeht und einen proaktiven Sicherheitsansatz verfolgt. Damit können sie Zugriffsrichtlinien dynamisch anpassen und Risiken frühzeitig erkennen, um sensible Zugangsdaten und Endpunkte effektiv zu schützen. Doch wie setzen Unternehmen das Konzept erfolgreich um?

UM SICHERHEITSVERLETZUNGEN VORZUBEUGEN UND PRIVILEGIERTE ZUGRIFFE ZU SICHERN, SOLLTEN UNTERNEHMEN EINEN PROAKTIVEN ANSATZ MIT FORTSCHRITTLICHEM PAM VERFOLGEN.

Andreas Müller,
Vice President Enterprise Sales Central & Eastern Europe, Delinea, www.delinea.com

Schlüsselrollen und Zuständigkeiten klar definieren

Ein erfolgreiches PAM-Programm lebt vom Zusammenspiel zwischen Mensch und Technologie – daher ist es entscheidend, zunächst alle Zuständigkeiten zu definieren. In der Regel liegt die Verantwortung beim Identity Access Management (IAM)-Team, das als Schnittstelle zwischen Sicherheitsexperten und Risikomanagern agiert. In größeren Unternehmen verteilen sich die Aufgaben auf mehrere Abteilungen wie IT-Sicherheit, IAM, Betrieb und Entwicklung, wobei alle Teams unter der Leitung des CISO oder CIO zusammenarbeiten sollten. Besonders wichtig ist die Abstimmung mit dem IT-Support, wenn Sicherheitsmaßnahmen wie das Entfernen lokaler Administratorenrechte die Arbeitsabläufe beeinflussen.

Der PAM-Lebenszyklus

Ein umfassendes PAM-Programm erfordert eine ganzheitliche, langfristige Strategie, die den gesamten PAM-Lebenszyklus abdeckt. Es sollte daher als kontinuierlicher Prozess verstanden werden, der regelmäßig überprüft, optimiert und durch geeignete Technologien unterstützt werden muss. Der PAM-Lebenszyklus beinhaltet sieben Phasen:

#1 Definieren

In der Definitionsphase setzen Unternehmen Prioritäten, indem sie die kritischsten Zugriffspunkte identifizieren und festlegen, wer diese wann und zu welchem Zweck nutzen darf. Sie sollten dabei ermitteln, welche Funktionen im Unternehmen Zugriff auf sensible Daten und Systeme benötigen. Eine kontinuierliche, integrierte und automatisierte Risikoanalyse unterstützt dabei, potenzielle Bedrohungen frühzeitig zu erkennen, während klare Governance-Richtlinien helfen, den Umgang mit privilegierten Konten zu regeln. Diese Schritte bilden die Basis, um Umfang und Struktur des PAM-Programms festzulegen.

#2 Ermitteln

In der Ermittlungsphase analysieren Unternehmen die Sicherheitsaspekte privilegierter Konten wie Dienstkonten, Anwendungspools und AWS-Berechtigungen. Ein automatisierter Ermittlungsprozess – idealerweise einmal pro Woche – erfasst Veränderungen wie Neueinstellungen oder Systemupdates. So lässt sich die Angriffsfläche genau bestimmen und ungenutzte Berechtigungen, etwa in Domänenadministratorgruppen, identifizieren. Auf dieser Basis können Unternehmen gemeinsam genutzte Konten einrichten, überflüssige Rechte entfernen und temporäre Privilegien automatisiert zuweisen, um das Risiko zu senken und die Kontrolle über privilegierte Zugriffe zu verbessern.

#3 Verwalten und Schützen

In dieser Phase geht es darum, den Zugriff auf Systeme, Anwendungen und Cloud-Dienste konsequent zu kontrollieren. Automatisierte Kontrollen wie die regelmäßige Rotation von Passwörtern, Multi-Faktor-Authentifizierung

(MFA) und Least-Privilege-Richtlinien sind hier entscheidend. Privilege Elevation and Delegation Management (PEDM) sorgt beispielsweise dafür, dass Berechtigungen nur bei Bedarf erhöht werden und Angreifer zusätzliche Hürden überwinden müssen. Zudem sollten Unternehmen Dienstkonten proaktiv verwalten und temporäre Berechtigungen für spezifische Zugriffe gewähren, um Missbrauch zu vermeiden.

#4 Aktivitäten überwachen

Die Überwachung privilegierter Konten ist entscheidend, um Missbrauch frühzeitig zu erkennen. Protokolle helfen, Sicherheitsverletzungen zu analysieren und Gegenmaßnahmen zu ergreifen. Sitzungsaufzeichnungen auf Vault- oder Host-Ebene sowie die Integration in Session Launcher, die Administratoren für Remote-Verbindungen nutzen, unterstützen die Sicherheit – besonders in Cloud-Umgebungen wie AWS, indem nur vertrauenswürdige IP-Adressen zugelassen werden. Durch Echtzeit-Analyse und Sitzungsüberwachung können Unternehmen Berechtigungen anpassen und Verbindungen bei Bedarf sofort trennen – alles unter der Kontrolle einer „Vier-Augen"-Funktion, die zusätzliche Sicherheit bietet.

#5 Erkennen

Durch geeignete Überwachungsmaßnahmen können Unternehmen Missbrauch on privilegierten Konten frühzeitig erkennen. Verhaltensanalyselösungen hinterlegen typische Normalwerte für privilegierte Aktivitäten und erkennen Abweichungen wie ungewöhnliche Zugriffszeiten oder untypisches Nutzerverhalten. Bei Verdacht auf Missbrauch sendet das System eine Warnmeldung, um gezielte Maßnahmen zu ergreifen.

#6 Reagieren

Die Reaktionsmaßnahmen auf eine Sicherheitsverletzung hängen vom Ausmaß des Vorfalls und betroffenen Konto ab. Bei einem kompromittierten Dienstkonto genügt oft eine Passwortrotation, während bei einem Domänenadministrator-Konto das gesamte Active Directory neu aufgebaut werden muss, um weiteren Zugriff zu verhindern. Fortschrittliche PAM-Systeme ermöglichen schnelle Reaktionen, indem sie automatisch Warnmeldungen auslösen und sofort handeln – etwa indem sie Passwörter ändern oder Sitzungen beenden. Redundante Systeme und Geo-Redundanz sorgen für eine schnelle Wiederherstellung des Normalbetriebs.

#7 Prüfen und auditieren

KI-gestützte Warnmeldungen und klare Berichte sind essenziell, um Sicherheitsvorfälle zu analysieren und die Einhaltung von Richtlinien zu gewährleisten. Bei der Prüfung privilegierter Konten helfen die erfassten Metriken, fundierte Entscheidungen zu treffen. Unternehmen profitieren auch von bewährten Sicherheitsframeworks wie NIST oder CIS, die als Orientierung für eine solide Sicherheitsstrategie dienen. Compliance sollte dabei als ein kontinuierlicher Prozess verstanden werden, der fortlaufend zur Verbesserung der Sicherheitspraktiken beiträgt.

Fazit

Um Sicherheitsverletzungen vorzubeugen und privilegierte Zugriffe zu sichern, sollten Unternehmen einen proaktiven Ansatz mit fortschrittlichem PAM verfolgen. Das erfordert klare Zuständigkeiten und enge Zusammenarbeit der Teams. Entscheidend ist, dass das PAM-Programm als ein kontinuierlicher Prozess – im Rahmen des PAM-Lebenszyklus – verstanden wird, der regelmäßig optimiert werden muss, um Sicherheitslücken zu schließen und langfristig Risiken zu minimieren.

Andreas Müller

Privilege Access Management

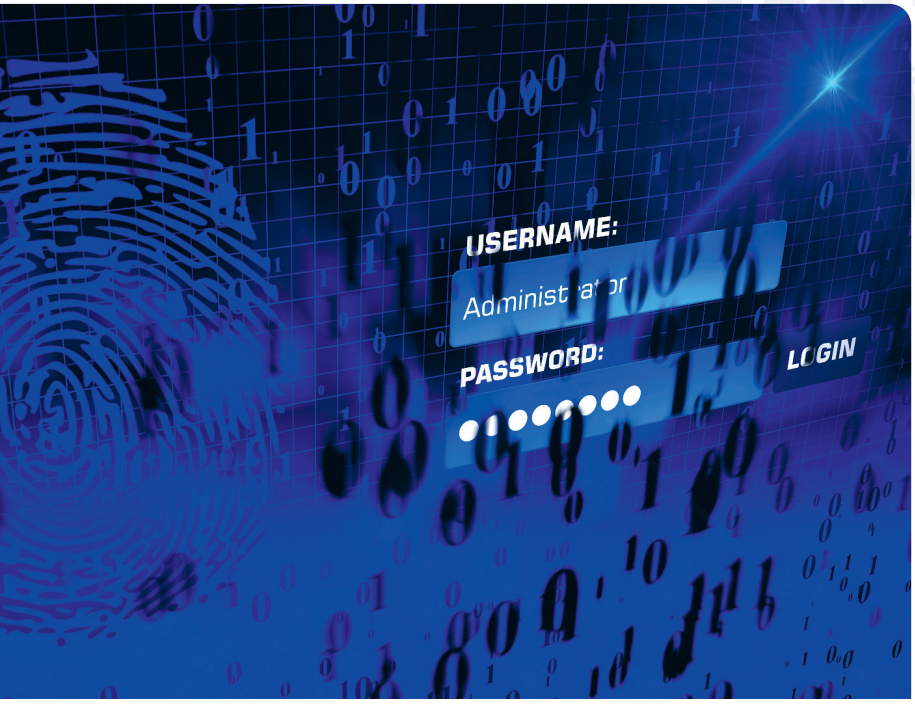
WORAUF ES WIRKLICH ANKOMMT

Ein Privilege Access Management (PAM) schützt die kritischsten Systeme von Unternehmen vor unberechtigten Zugriffen. Doch was muss eine PAM-Lösungen können und auf welche Aspekte, die über Features hinausgehen, sollten Unternehmen bei der Auswahl achten?

Viele Unternehmen stehen vor großen Security-Herausforderungen beim Schutz ihrer kritischen Daten und Systeme. Das liegt nicht nur an den wachsenden Cybergefahren, sondern auch an der immer strengeren Regulierung von Sicherheit und Datenschutz sowie zunehmend heterogenen IT-Landschaften mit mehr und mehr Cloud-Services, Remote Workern und automatisierten Abläufen. Zero Trust hat sich als Sicherheitskonzept in solchen Umgebungen bewährt, weil es die Angriffsfläche unter anderem durch eine minimale Rechtevergabe und eine konsequente Verifizierung aller Zugriffe deutlich verkleinert.

Ein entscheidender Baustein von Zero Trust ist ein Privilege Access Management (PAM), das sich auf die Accounts konzentriert, von denen ob der erweiterten Berechtigungen das größte Risiko ausgeht und die ganz besonders im Visier von Cyberkriminellen stehen. Viele Aufsichtsbehörden, Cyberversicherer und Security-Frameworks verlangen inzwischen explizit nach einem Credential Management, einem Session Monitoring und der Umsetzung von Least-Privilege-Prinzipen – und damit nach Dingen, die zu einem Privilege Access Management gehören.

Wollen Unternehmen wirksame PAM-Kontrollen einführen, um ihre Sicherheit zu verbessern, müssen sie zunächst verstehen, dass PAM kein einmaliger Aufwand, sondern ein fortwährender Prozess ist. Schließlich geht es darum, privilegierte Zugriffe kontinuierlich zu erkennen und zu schützen – und das in sich stetig verändernden IT-Umgebungen. Moderne PAM-Lösungen können dabei helfen, indem sie Abläufe zuverlässig automatisieren, was den Verwaltungsaufwand reduziert und den Schutz verbessert.



Quelle: Thomas Breher – Pixabay

Augen auf bei der Anbieter-Auswahl

Doch zu welchen Lösungen sollten Unternehmen greifen – welchem Anbieter den Schutz genau der Accounts anvertrauen, die Zugriff auf ihre kritischsten Assets haben? Klar ist, dass sie höchste Sicherheitsanforderungen erfüllen müssen, also über sicherheitsrelevante Zertifizierungen wie AICPA SOC 2 und ISO 27001 verfügen sollten. Details zu den Zertifizierungen und zu internen Security-Praktiken veröffentlichen die meisten Anbieter auf ihren Websites.

Darüber hinaus ist ein Blick auf ihren Track Record sinnvoll – immerhin hatten einige Anbieter in der Vergangenheit mit Sicherheitslücken und Datenlecks zu kämpfen. Teilweise war es ihnen nicht einmal gelungen, ihre eigenen privilegierten Accounts zu schützen. Eine Recherche nach entsprechenden CVEs, aber auch schon eine einfache Google-Suche fördern hier viele Informationen zu Tage. Und schließlich können Unternehmen auch ihren Wirtschaftsprüfer, Cyberversicherer oder IT-Dienstleister nach Erfahrungen mit PAM-Anbietern fragen und um eine Empfehlung bitten.

Hat ein Anbieter zudem Referenzkunden in der Branche des Unternehmens, zeigt das, dass er die jeweiligen Herausforderungen und gesetzlichen Anforderungen kennt. Dies verringert das Risiko, dass es Probleme bei der Implementierung der Lösung oder mit branchenspezifischen Technologien wie SCADA in der Fertigung gibt.

Die PAM-Basics müssen sitzen

Da in eigentlich jedem Unternehmen die digitalen Infrastrukturen wachsen, muss eine PAM-Lösung gut skalieren. Denn mit jedem neuen Mitarbeiter, jeder neuen Anwendung und jedem neuen Rechner oder Server kommen neue Accounts und Identitäten hinzu, die es zu schützen gilt. Ein PAM sollte diese automatisiert erkennen und ihre privilegierten Zugriffe verwalten. Dazu zählt auch, die Credentials sicher zu speichern, zu managen und regelmäßig zu rotieren – unabhängig davon, ob es sich um lokale Admin-Passwörter, Domänen-Passwörter, SSH- und API-Keys, Passwörter von Mitarbeitern oder die Secrets von Anwendungen handelt.

Weitere wichtige PAM-Funktionen sind die Umsetzung von Least Privilege und rollenbasierte Zugriffskontrollen (RBAC), die sich für Multi-Cloud-Umgebungen eignen. Viele Cloud-Anbieter empfehlen mittlerweile, menschliche und nicht-menschliche Identitäten standardmäßig ohne Privilegien auszustatten (Zero Standing Privileges, ZSP) und nur bei Bedarf session-basiert Berechtigungen zuzuweisen. Allerdings gelingt es bislang nur wenigen PAM-Lösungen, die Rollen und Berechtigungen tatsächlich dynamisch zur Laufzeit zu generieren und am Ende der Session automatisch zu löschen.

Eine Isolierung der Sessions verhindert, dass sich Angreifer oder Malware ungehindert innerhalb der Infrastruktur ausbreiten können, während ein Session-Monitoring die Untersuchung von Sicherheitsvorfällen und Audits erleichtert. Und zu guter Letzt muss ein PAM auch die privilegierten Zugriffe von Externen wie Kunden, Partnern und Dienstleistern schützen, unter anderem durch die Zuweisung von Berechtigungen just in time (JIT), RBAC und zentralisierte Audits.

Zentralisierte Audits helfen Unternehmen, die Einhaltung von Compliance-Vorgaben und Sicherheitsstandards nachzuweisen. Interne und externe Prüfer erhalten ohne langes Suchen detaillierte Einblicke in alle privilegierten Sessions – von Zugriffen auf IT-Systeme on-premises über Zugriffe auf OT-Systeme bis hin zu Zugriffen auf Cloud- und Web-Ressourcen. In einigen PAM-Lösungen unterstützen zudem KI-Funktionen bei den Audits, aber auch bei der Identity Threat Detection and Response (ITDR). Sie nutzen Bedrohungsinformationen und Verhaltensanalysen, um mögliche Sicherheitsverletzungen zu erkennen und frühzeitig einzudämmen.

Die Anwender nicht vergessen

PAM-Lösungen, die sich einfach und nahtlos in bestehende Infrastrukturen einfügen, machen nicht nur den Security-Teams das Leben leichter, sondern auch den Anwendern. Mehr noch: Sie verhindern, dass Anwender nach Wegen suchen, die Sicherheitsmaßnahmen zu umgehen, weil sie sich in ihren gewohnten Arbeitsabläufen behindert fühlen. Daher sollten PAM-Lösungen die Tools unterstützen, mit denen sich IT-Spezialisten, Entwickler und andere Techniker bevorzugt mit Windows- und Linux-Systemen, Cloud-Services, VMs, Kubernetes-Umgebungen und Datenbanken verbinden.

Darüber hinaus müssen sich PAM-Lösungen in die bestehende Security-Landschaft integrieren, und das out of the box und ohne Zusatzkosten. Das betrifft vor allem die Zusammenarbeit mit dem Identity and Access Management (IAM), dem Security Information and Event Management (SIEM) und dem IT Service Management (ITSM). Vorsicht ist bei Anbietern geboten, die umfangreiche kostenpflichtige Professional Services für Integrationen bieten, denn das kann ein Zeichen dafür sein, dass die PAM-Lösung sehr komplex ist – und die Kosten erhöhen, wenn später neue Technologien eingeführt werden und weitere Integrationen notwendig sind.

Mit einem Privilege Access Management legen Unternehmen den Grundstein für die Einführung eines umfassenden Programms für Identitätssicherheit. Ein solches dehnt den Schutz von privilegierten Accounts auf alle menschlichen und maschinellen Identitäten aus, die auf kritische Ressourcen zugreifen. Es stellt sicher, dass sämtliche Identitäten zur richtigen Zeit die richtigen Berechtigungen erhalten, und führt zu einer weiteren Minimierung des Risikos, das von kompromittierten Accounts und dem Missbrauch von Berechtigungen ausgeht.

Sam Flaster

MIT EINEM PAM LEGEN UNTERNEHMEN DEN GRUNDSTEIN FÜR DIE EINFÜHRUNG EINES UMFASSENDEN PROGRAMMS FÜR IDENTITÄTSSICHERHEIT.

Sam Flaster, Director of Product Marketing, CyberArk, www.cyberark.com

Passwortlose Authentifizierung

REIFEGRADMODELL FÜR MEHR SICHERHEIT UND EFFIZIENZ

Mit Angriffen auf die kritische Infrastruktur, wie Gesundheitsversorger, erhalten Cyberkriminelle hohe Aufmerksamkeit in der Bevölkerung und Zugriff auf wertvolle Daten. Das macht Organisationen im Gesundheitswesen zu bevorzugten Zielen für Cyber-Attacken. Phishing, Ransomware und Insider-Bedrohungen gehören zu den größten Cyber-Gefahren, denen sich Krankenhäuser und Kliniken gegenübersehen. Die zunehmende Digitalisierung macht es notwendig, Sicherheitsstrategien neu zu denken – insbesondere im Bereich des Identity and Access Management (IAM).

PASSWORTLOSE AUTHENTIFIZIERUNG IST KEIN FERNER ZUKUNFTSTRAUM, SONDERN MUSS DAS ZIEL SEIN, UM CYBERANGRIFFE ZU VERHINDERN UND DIE EFFIZIENZ IM GESUNDHEITSWESEN ZU STEIGERN.

Dirk Wahlefeld,
Manager Technical Services, Imprivata,
www.imprivata.com

Besonders kritisch ist die Authentifizierung von Mitarbeitenden im Gesundheitswesen. Traditionelle Passwörter sind nicht nur ein Sicherheitsrisiko, sondern beeinträchtigen auch die Arbeitsabläufe. Ärzte sowie Pflegekräfte haben keine Zeit, komplexe Passwörter einzugeben oder sich mit vergessenen Zugangsdaten auseinanderzusetzen. Hier setzt die passwortlose Authentifizierung an: Sie verbessert nicht nur die Benutzererfahrung, sondern reduziert auch die Angriffsfläche für Cyberattacken.

Passwörter sind nicht die Lösung

Passwörter sind in vielen Bereichen nach wie vor Standard, doch sie bringen erhebliche Nachteile mit sich:

- **Sicherheitsrisiken:** Passwörter sind anfällig für Phishing, Brute-Force-Angriffe und Credential Stuffing.
- **Gemeinsam genutzte Geräte:** Medizinisches Personal arbeitet oft an gemeinsam genutzten Workstations oder mobilen Endgeräten, was die sichere Authentifizierung erschwert.
- **Schlechte Benutzerfreundlichkeit:** Lange und komplexe Passwörter sind schwer zu merken und führen zu ineffizienten Workflows.
- **Hoher Verwaltungsaufwand:** IT-Abteilungen sind mit zahlreichen Passwortzurücksetzungen und Supportanfragen konfrontiert.

Ein vielversprechender Ansatz ist daher der schrittweise Übergang zu passwortlosen Lösungen, die sowohl die Sicherheit als auch die Effizienz verbessern. Dabei ist der Weg das Ziel:

Reifegradmodell für passwortlose Authentifizierung

Die vollständige Abschaffung von Passwörtern kann nicht von heute auf morgen erfolgen. Imprivata hat daher ein Reifegradmodell entwickelt, das Organisationen im Gesundheitswesen hilft, den Umstieg strukturiert zu gestalten.

STUFE 1 Reduzierung der Passworteingaben

In dieser Phase wird die Zahl der manuellen Passworteingaben drastisch gesenkt. Hier kommen Enterprise Single Sign-On (E-SSO) und „tap-and-go"-Lösungen zum Einsatz. Mitarbeitende im Gesundheitswesen nutzen dabei eine Chipkarte oder ein anderes sicheres Authentifizierungsmedium, um sich mit einer einzigen Berührung bei mehreren Systemen anzumelden.

Sofern das Applikationsdesign es zulässt sollte auch der Einsatz von integriertem Single Sign-on erwogen werden, auf Basis von „OpenID Connect" (OIDC) oder „Open Authentication" (OAuth), da diese mit verfügbaren Authentisierungsmethoden kombiniert werden können und einzelne Applikationen direkt auf Stufe 4 des Reifegradmodells heben.

Diese Technologie reduziert nicht nur den Zeitaufwand pro Anmeldung, sondern verringert auch die Versuchung, Passwörter aufzuschreiben oder mit Kollegen zu teilen – ein Problem, das im stressigen Klinikalltag oft vorkommt.

STUFE 2 Eliminierung von Passwörtern in kritischen Workflows

Sobald SSO implementiert ist, werden passwortlose Methoden gezielt für sicherheitskritische Anwendungen einge-

führt. Dafür wird „tap-and-go" mit Multifaktor-Authentifizierung (MFA) kombiniert. Für hohe Sicherheit sorgen Methoden wie FIDO-Sicherheitsschlüssel (Fast IDentity Online) oder biometrische Authentifizierung, die gegen Phishing resistent sind. Besonders im Bereich des privilegierten Zugriffs (z. B. bei Verwaltungs- oder Cloud-Anwendungen) ist dies entscheidend.

Bei diesem hybriden Ansatz verwenden Mitarbeitende ihre Dienstausweise, die bei Bedarf mit biometrischen Verfahren kombiniert werden.

STUFE 3 Maskierung von Passwörtern für Endnutzer

Ab diesem Punkt werden Passwörter für die Anwender unsichtbar. IT-Systeme übernehmen das Management der Passwörter und rotieren sie regelmäßig. Nutzer müssen sich nicht mehr aktiv Passwörter merken oder eingeben, da Authentifizierungsprozesse vollständig im Hintergrund ablaufen.

Dies verbessert die Sicherheit erheblich, da Nutzer nicht durch Phishing oder Social Engineering getäuscht werden können. Ein weiterer Vorteil: Längere, komplexere Passwörter können automatisch generiert und eingesetzt werden, ohne dass die Usability darunter leidet.

STUFE 4 Vollständige Abschaffung von Passwörtern

Die höchste Stufe besteht darin, Passwörter aus allen Systemen durch integriertes Single Sign-On zu eliminieren. Dies setzt voraus, dass alle Anwendungen die Protokolle der modernen Authentifizierungsstandards wie „OpenID Connect" (OIDC) oder „Open Authentication" (OAuth) unterstützen. In der Praxis wird es noch Jahre dauern, bis Organisationen diesen Punkt erreichen, aber bereits die Umsetzung der ersten drei Stufen bringt erhebliche Vorteile.

Sicherheit ohne Passwort

Bis zu fünf Lösungen sind für die vollständige passwortlose Authentifizierung notwendig:

#1 **Tap-and-go:** Nutzer melden sich per Badge/NFC-Token an und wechseln nahtlos zwischen Geräten.

#2 **FIDO-Badges und Passkeys:** Sicherheitsschlüssel basierend auf dem FIDO2-Standard ermöglichen Phishing-resistente Authentifizierung.

#3 **Biometrische Authentifizierung:** Gesichtserkennung oder Fingerabdruckscanner sorgen für eine intuitive und sichere Anmeldung.

#4 **Secure Walk Away:** Mithilfe von Bluetooth Low Energy (BLE) erkennt das System, ob sich der Nutzer in der Nähe befindet, und sperrt den Bildschirm automatisch bei Verlassen.

#5 **Automatische Passwortrotation:** Für nicht-passwortlose Legacy-Systeme werden komplexe Passwörter regelmäßig aktualisiert und per SSO verwaltet.

Diese Technologien lassen sich flexibel kombinieren und in bestehende IT-Infrastrukturen sowie medizinische Geräte integrieren. Damit können Krankenhäuser individuell entscheiden, welche Methode für welchen Workflow am besten geeignet ist.

Zudem sollte immer der Einsatz von standardisierter Technologie und Protokollen gegenüber proprietären Lösungen bevorzugt werden, um die Anpassungen der nächsten Jahre komplikationslos unterstützen zu können.

Die Zukunft des Gesundheitswesens ist passwortlos

Der Weg zu einem vollständig passwortlosen Gesundheitswesen ist ein schrittweiser Prozess, der nicht nur Technologie, sondern auch Change Management erfordert. Kliniken sollten mit den Bereichen beginnen, in denen Passwörter die größten Sicherheitsrisiken oder Usability-Probleme verursachen. Gemäß dem strukturierten Reifegradmodell können Organisationen den Übergang sicher und effizient gestalten.

Passwortlose Authentifizierung bietet zahlreiche Vorteile: Sie schützt vor Cyberangriffen, verbessert den klinischen Workflow und ermöglicht es medizinischem Personal, sich auf das Wesentliche zu konzentrieren: die Patientenversorgung.

Dirk Wahlefeld

MEHR WERT
Enterprise Access Management

Startklar für NIS2 mit Open Source Software

QUICK WINS DURCH MFA UND MEHR

Cyber-Sicherheit ist in aller Munde und nicht mehr wegzudenken aus dem Verantwortungsbereich aller CIOs und CISOs. Da sich diese Sicherheit nicht mehr nur noch aus der richtigen Auswahl an Tools speist, sondern ein allumfassendes Thema ist, muss ein IT-Verantwortlicher sich nicht nur in der Endpunkt-Sicherheit auskennen, sondern auch die Awareness aller Mitarbeiter im Blick haben. Ein schwieriges Unterfangen, zumal sich die Gefahr nach innen durch Cloud- und Webdienste und mit dem digitalen Fußabdruck externer Nutzer wesentlich vergrößert. Die intrinsische Sicht reicht so nicht mehr aus.

IT-Sicherheit ist ein Bestandteil von Cyber-Sicherheit

Häufig wird Cyber-Sicherheit falsch verstanden. Zum einen besteht sie nicht aus einzelnen Maßnahmen und Programmen, die man durchführt oder installiert. Zum anderen sind weit mehr Verantwortliche betroffen als vermeintlich angenommen.

Die IT beispielsweise führt Identity & Access Management zwar zumeist ein, IAM betrifft jedoch das gesamte Unternehmen und die Stakeholder – externe Verbindungen in der Lieferkette, ob Partner, Kunden oder Lieferanten. IAM spielt bei den Vorgaben der neuen Cyber-Regularien eine tragende Rolle, auch wenn NIS2 diese Komponente nicht explizit nennt.

IAM ist ein präventiver Teil von Cyber-Abwehr

IAM-Systeme entstanden aus Compliance-getriebenen Gründen und um intern Daten und Systeme vor unbefugtem Zugriff zu schützen. Die IT-Abteilung ist dafür zuständig, in großen Unternehmen sogar ein eigenständiges IAM-Team. Aber auch HR-Bereiche können federführend sein.

Die identitätsrelevante Komponente, wie der Datenschutz und die Prozesse für On- und Offboarding, auch als User-Life-Cycle bekannt, komplettierten später die Aufgaben interner IAM-Systeme. Cyber-Sicherheit für Identitäten entstand durch die Ausweitung der identitätsbezogenen Informationssicherheit um mobile oder Cloud-Dienste und mit der Digitalisierung der Lieferkette wie etwa Services für Externe. Ein Dreh- und Angelpunkt hierbei ist die Verantwortlichkeit für die Sicherheit externer Identitäten, die nicht bei der IT-Abteilung liegt. Häufig tun sich Unternehmen schwer das richtige Maß zu finden, auch diese Nutzer entsprechend zu schützen.

CYBER-SICHERHEIT ALLER IDENTITÄTEN, DIE EIN UNTERNEHMEN VERWALTET, IST NICHT MIT HILFE EINES INTERNEN IAM-SYSTEMS ZU LÖSEN.

Stephanie Ta, IAM Business Development Consultant, Syntlogo GmbH, www.syntlogo.de

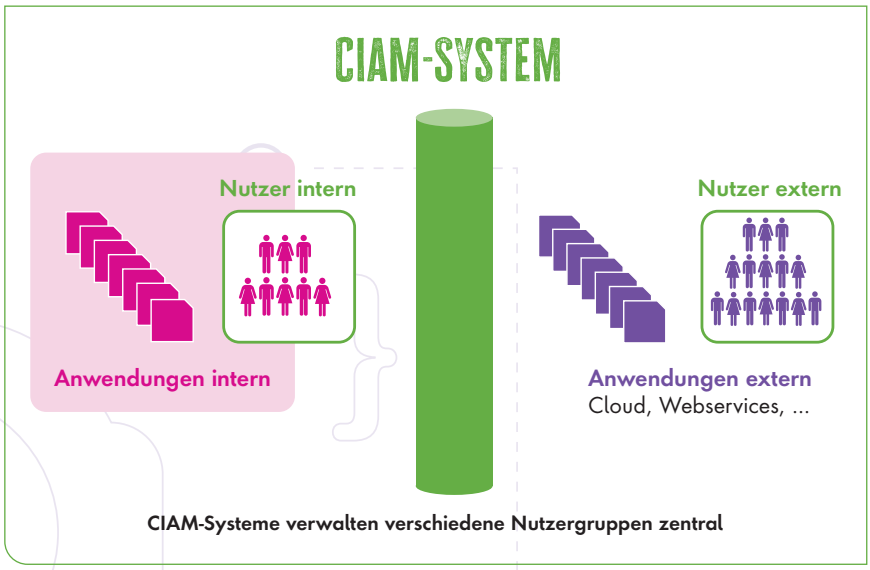
Führungskräfte vernachlässigen externe Nutzer-Sicherheit

Meist haben Geschäftsleiter diesen Aspekt gar nicht auf dem Schirm, denn das Marketing, der Einkauf oder ein Product Owner einer Anwendungssoftware ist gleichzeitig der Sicherheitschef externer Identitäten. Nur Datenschützer bilden dabei eine Querschnittsfunktion. Es ist nun an der Geschäftsführung sich dieser Verantwortung anzunehmen und wichtige Aufgaben, Maßnahmen und technische Anforderungen an die richtigen Verantwortlichen zu delegieren.

Um echte Cyber-Resilienz gemäß NIS2 zu erreichen, resultieren neue Anforderungen an die Identitätsverwaltung:

- Zero Trust-Prinzip
- Ende-zu-Ende-Sicherheit
- DSGVO-Umsetzung und Cyber-Sicherheit für alle mit dem Unternehmen vernetzten Nutzer
- Mehrstufige Strategien und Technologien, um eine erfolgreiche Cyber-Abwehr für diese Identitäten bereit zu stellen
- Interne IT-Sicherheit mit identitätsbezogenen Prozessen zu einer allumfassenden Cyber-Sicherheit verknüpfen

Durch die Verschmelzung identitätsbezogener, interner Prozesse mit der Außenwelt, wird es umso wichtiger eine zentrale „Single Source of Truth“ zu ha-



CIAM-Systeme verwalten verschiedene Nutzergruppen zentral

ben, die die Kontrolle und die Steuerung von Identitäten und ihren Berechtigungen ganzheitlich erledigt. Das kann bedeuten, dass interne und externe Quellen mit einem zentralen Customer Identity & Access Management-System verknüpft sind, welches insbesondere für die Cyber-Sicherheit und die effiziente Verwaltung der Nutzer verantwortlich ist.

Sicheres Berechtigungsmanagement als Wettbewerbsfaktor

Letztendlich darf die Geschäftsleitung diesen Aspekt nicht vernachlässigen, da die richtigen IAM-Funktionen das Unternehmen nicht nur cyber-resilient machen, sondern auch einen enormen Wettbewerbsvorteil bringen.

Zum Beispiel ist die Einführung von Single-Sign-On (SSO) – ein einziger Login für alle angeschlossenen Anwendungen – ein fruchtbarer Boden, der nicht nur die Sicherheit erhöht. Ein kleiner Exkurs dazu: Sicherheit durch Open Source Software.

In einem größeren Projekt im Jahr 2015 führte Syntlogo beispielsweise die IAM-Lösung Keycloak ein. Ursprünglich sollte der Einsatz der Open Source Software das Problem der vielen Logins in verschiedene Kundenportale lösen. Durch die hiermit wesentlich verbesserte User Experience erhöhte sich neben der Cyber-Sicherheit auch die Nutzungsrate des Online-Angebotes um 240 Prozent. Ein Effekt, von dem manche Unternehmen nur träumen können.

Open Source für SSO und MFA

Die Einführung von SSO bereitet sogar die Grundlage zur Einführung von Multi-Faktor-Authentifizierung (MFA), die mit Keycloak out-of-the-box für verschiedene Technologien bereitsteht.

Die Open Source-Lösung beinhaltet die, auf den neuesten Standards basierende Technik zur sicheren Authentifizierung. Durch die lebendige Community sind alle Login- und Registrierungsprozesse sicherheitstechnisch up-to-date.

Mit seiner Flexibilität verschiedene Verzeichnisdienste und Identity Provider anzubinden, dient Keycloak als zentrale Nutzerverwaltung zwischen internen und externen Diensten und Anwendungen. Das Self-Hosting oder ein Keycloak as a Service bietet vergleichsweise günstige und schnelle Wege, um die Cyber-Sicherheit stark zu erhöhen. Und zwar aller Identitäten, die ein Unternehmen zu verwalten hat.

Die Lösung besitzt eine moderne REST-Schnittstelle, unterstützt perfekt die Standardprotokolle OIDC und SAML2 und lässt sich einfach um eigene Erweiterungen ergänzen. So kann diese Software auch den heutigen Enterprise-Anforderungen gerecht werden.

Erweiterung als CIAM-System

Möchte man Keycloak als CIAM-System einsetzen, dann ist ein zentraler Aspekt die User Experience. Durch die Adaptier- und Erweiterbarkeit der Oberflächen kann eine nahtlose Integration erfolgen. Damit die Lösung als zusätzliche Sicherheit nicht zur Hürde für den Nutzer wird, lassen sich Registrierungs- und Anmeldeprozesse optimal anpassen.

Gerade für NIS2 spielen Berechtigungen eine tragende Rolle. Oft bedarf es einer ausgefeilten Berechtigungsverwaltung in Form dezentraler Berechtigungsstrukturen. Die manuelle Verwaltung von Identitäten kann zu einer mühseligen Aufgabe für einen zentralen IT-Support mutieren. Nur durch Automatisierung und Dezentralisierung lässt sich eine moderne Vergabe und Kontrolle von Rechten und Rollen effizient und sicher umsetzen.

Interessante Funktionen können die sogenannte Delegierte Administration sein, die im B2B-Bereich mit einer dezentralen Organisationsverwaltung durch Business Administratoren oder Projektleiter möglich ist. Im Consumer-Bereich ist die Abbildung von Familien-Accounts enorm praktisch, wenn Kinder oder Jugendliche noch nicht die gleichen Rechte besitzen, wie die erwachsenen Eltern.

Auch hier ist der Einsatz einer durch Keycloak-gestützten MFA-Technologie realisierbar. Sogar die neuesten Entwicklungen mit Passkeys sind damit problemlos umsetzbar.

Stephanie Ta

MEHR WERT

Cyberversicherung: Mehr als ein Backup

WESHALB IT-SICHERHEIT ALLEIN NICHT AUSREICHT

Deutsche Unternehmen werden fast wöchentlich Ziel eines Cyberangriffs und trotz steigender IT-Ausgaben sind viele Firmen nicht auf den Ernstfall vorbereitet. Um Schäden vorzubeugen, die durchaus die Existenz eines Unternehmens bedrohen können, sollten Unternehmen ihre Cybersicherheit stärken und in präventive Maßnahmen investieren. Das Restrisiko kann mit einer guten Cyberversicherung abgedeckt werden, die das Unternehmen im Ernstfall unterstützt.

Die Cyber-Bedrohungslage in Deutschland spitzt sich für Unternehmen weiter zu: 2024 verzeichneten 60 Prozent der deutschen Unternehmen mehr Angriffe als im Vorjahr. Im Durchschnitt wurden sie fast wöchentlich von Cyber-Kriminellen attackiert. Das ergab eine repräsentative internationale Befragung des Spezialversicherers Hiscox im Rahmen des aktuellen Cyber Readiness Reports. Angriffe, die Unternehmen nicht abwehren konnten, haben einschneidende wirtschaftliche Folgen: Während 52 Prozent der angegriffenen Unternehmen Kosten von unter 100.000 Euro angaben, erlitt ein Viertel Schäden von über 500.000 Euro. Zudem litten Unternehmen unter der Dauer der Betriebsunterbrechungen: Während diese bei 26 Prozent der Befragten zwei bis vier Wochen anhielten, brauchten 30 Prozent ein bis drei Monate und 7 Prozent sogar noch länger, bis der Betrieb wiederhergestellt war.

FÜR UNTERNEHMEN IST WICHTIG ZU WISSEN: OHNE GRUNDLEGENDE CYBERSICHERHEITS-MASSNAHMEN SIND SIE NICHT VERSICHERBAR.

Gisa Kimmerle, Head of Cyber, Hiscox, www.hiscox.de

Auch über die ersten finanziellen Schäden hinaus spüren viele Unternehmen die Folgen eines Cyberangriffs langfristig, sodass sie existenzbedrohende Ausmaße annehmen können: Der Hälfte der befragten Unternehmen fiel es schwerer, neue Kundschaft zu gewinnen, wenn der Angriff öffentlich bekannt wurde. 46 Prozent verloren als Folge der Cyberattacke sogar Kundinnen und Kunden. Der Cybervorfall hat in diesen Fällen das Vertrauen der Stakeholder nachhaltig geschädigt. Sie zweifeln etwa die Kompetenz des Unternehmens an, ihre personenbezogenen Daten zu schützen. Für Geschäftspartner und Kunden ist Digital Trust ein wichtiger Faktor für die Zusammenarbeit und damit für deutsche Unternehmen eine Voraussetzung, um wettbewerbsfähig zu bleiben und die digitale Transformation gut zu meistern.

Cybersicherheit deutscher Unternehmen reicht nicht aus

Die meisten deutschen Unternehmen begreifen durchaus den Ernst der Lage und investieren in ihre IT-Sicherheit. 45 Prozent der Befragten geben 6 Prozent bis 10 Prozent des gesamten IT-Budgets für IT-Sicherheitsmaßnahmen aus, bei 42 Prozent sind es sogar 15 Prozent. Die Befragung zeigt, an welchen Stellen Unternehmen trotzdem nicht gut genug aufgestellt sind, sodass Cyberkriminelle diese Schwachstellen nutzen können: Unternehmens-Server in der Cloud sind das häufigste Einfallstor für Cyberkriminelle (55 %). Auch der Mensch bleibt eine der größten Schwachstellen in Unternehmen: 47 Prozent der Angriffe erfolgten durch Phishing oder Social-Engineering. Darüber hinaus blieb auch Ransomware eine häufig genutzte Methode.

5 Tipps für mehr Cyber-Resilienz

Diese besorgniserregenden Zahlen zeigen, dass die Bemühungen von Unternehmen bisher noch nicht ausreichen. Die Maßnahmen zur Verbesserung der Cybersicherheit müssen stark ausgeweitet werden. Die Umsetzung der folgenden Maßnahmen steigert die Cyber-Resilienz von Unternehmen deutlich:

#1 Sicherheitslücken überprüfen und regelmäßige Software-Updates

Unternehmen sollten ihre internen Systeme sehr genau im Blick behalten. Durch regelmäßige Updates lassen sich Sicherheitslücken in der Software vermeiden und Cyberangriffen über diese Schwachstellen vorbeugen.

#2 Kontinuierliche Schulungen

Mitarbeitende müssen kontinuierlich weitergebildet werden, damit sie Angriffe besser erkennen und ihnen mit den passenden Gegenmaßnahmen begegnen können.

#3 Ransomeware-sichere Back-ups

Regelmäßige und ransomware-sichere Back-ups sind essenziell, um die Systeme im Ernstfall zügig wiederherstellen zu können. Außerdem machen sich Unternehmen damit im Fall einer Lösegeldforderung weniger erpressbar. Für Cyberangriffe gilt: Prävention ist die beste Verteidigung.

#4 Vorbereitung auf den Ernstfall mit einem Krisenplan

Ein solcher Plan definiert und klärt unter anderem die wichtigsten Handlungsanweisungen und die zuständigen Personen für den Fall eines Cyberangriffs.

#5 Passgenaue Cyberversicherung abschließen

Kein Unternehmen ist so resilient gegen Cyber-Kriminalität aufgestellt, dass es „unangreifbar" ist – daher ist eine Cyber-Police für die Absicherung des Restrisikos sowie die schnelle Unterstützung durch Experten im Ernstfall.

Unverzichtbarer Teil jeder Strategie: Die Cyberversicherung

Gute Cyber-Versicherungen übernehmen nicht nur die Schäden des Cyberangriffs, sondern auch die Kosten der dadurch entstandenen Betriebsunterbrechung sowie Schadenersatzforderungen, die ein Dritter im Zusammenhang eines Cybervorfalls von dem Unternehmen verlangt. Letzteres kann beispielsweise vorkommen, wenn ein Mitarbeiter bei einem Datentransfer unwissentlich einen Virus an einen Kunden des Unternehmens überträgt. Darüber hinaus können unbegründete Ansprüche in diesem Fall durch einen inkludierten passiven Rechtsschutz abgewehrt werden.

Im Fall eines erfolgreichen Angriffs sind bei guten Versicherungen auch verschiedene Assistance-Leistungen enthalten, sodass betroffene Unternehmen schnelle Unterstützung von Experten wie IT-Forensikern, Datenrechtsanwälten und Krisen-PR-Beratern bekommen. So können nicht nur die Systeme möglichst schnell wiederhergestellt werden, sondern auch die Reputation des Unternehmens geschützt werden, um die Schäden für das Unternehmen möglichst klein zu halten.

Von der Hilfe des Versicherers profitieren Unternehmen aber nicht nur nach einem Schaden, sondern auch bereits davor, etwa bei der Erstellung eines Krisenplans. Manche Versicherer bieten auch Cyber-Trainings für Mitarbeitende an, sodass versicherte Unternehmen einen Teil der Präventionsarbeit auslagern können.

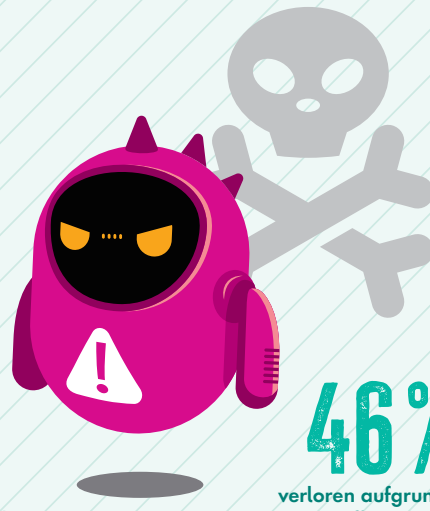
Ein häufiger Irrtum ist übrigens, dass nur große Unternehmen das Opfer von Cyberangriffen werden und ausschließlich diese sich dagegen versichern müssen. Dabei geraten zunehmend auch kleine und mittelgroße Unternehmen in das Visier von Cyberkriminellen, die wegen fehlender oder kleiner IT-Abteilungen nicht auf einen Cyberangriff vorbereitet sind und die Unterstützung eines Versicherers dringend benötigen.

Für Unternehmen ist wichtig zu wissen: Ohne grundlegende Cybersicherheitsmaßnahmen sind sie nicht versicherbar. Aber wenn diese Maßnahmen implementiert sind, ist für die Absicherung des Restrisikos eine Cyberversicherung essentieller Bestandteil einer umfassenden Sicherheitsstrategie.

Gisa Kimmerle

ERKENNTNISSE AUS DEM CYBER READINESS REPORT 2024

60 %
der befragten Unternehmen wurden häufiger Opfer von Cyberangriffen



79 %
sehen Cyberresilienz als ein sehr wichtiges Unternehmensziel

46 %
verloren aufgrund von Angriffen Kunden

Cybercrime: Im Fadenkreuz der Hacker

CYBERVERSICHERUNG: SCHUTZSCHILD FÜR DEN MITTELSTAND

Die zunehmende Bedrohung durch Hackerangriffe, Ransomware und Datendiebstahl ist seit Jahren spürbar. Sie sind die Kehrseite einer fortschreitenden Digitalisierung, die mit effizienten Geschäftsprozessen und neuen Geschäftsmodellen einhergeht. Und sie ist ein gesamtgesellschaftliches Problem, das Unternehmen in Deutschland und Europa unabhängig von ihrer Größe hart trifft. Allerdings sind besonders kleine und mittelständische Unternehmen (KMU) überproportional häufig betroffen, da ihnen robuste IT-Sicherheitsmaßnahmen fehlen. Für diese Betriebe können Cyberattacken existenzbedrohend sein – sei es durch Produktionsausfälle, Reputationsverluste oder hohe Lösegeldforderungen bei Ransomware-Angriffen.

Hinzukommt die rasante technologische Entwicklung – etwa durch den Einsatz von Künstlicher Intelligenz (KI). Sie verändern sowohl die Häufigkeit als auch die Intensität von Cyberattacken. 67 Prozent der entstandenen Schäden, die deutschen Unternehmen 2024 durch Diebstahl, Industriespionage oder Sabotage entstanden sind, sind auf Cyberattacken zurückzuführen.

Blickt man auf die kommenden Monate, zeichnen sich bei Cybercrime insbesondere folgende Entwicklungen ab:

➤ Automatisierung und KI treiben neue Angriffswellen: Die Qualität der Bedrohungslage verändert sich, weil Cyberkriminelle vermehrt auf automatisierte Angriffsmethoden und KI-gestützte Tools setzen: Wurden Attacken früher manuell durchgeführt, ermöglicht KI automatisierte, zielgerichtete und hochpräzise Attacken. So zeigt sich beispielsweise im Bereich des Phishings, dass KI nicht mehr nur massenhaft generische E-Mails versendet, sondern individuelle, täuschend echte Nachrichten erstellt. Mit Hilfe von Deepfake-Technologien werden zudem Stimmen und Videos nachgeahmt, um Führungskräfte zu imitieren und sogenannte CEO-Fraud-Angriffe durchzuführen. Zudem prognostiziert das FBI in seinem aktuellen IC Report, dass Business E-Mail Compromise (BEC) auch 2025 eine bedeutende Rolle spielen wird.

➤ Auch Distributed-Denial-of-Service (DDoS)-Angriffe entwickeln sich weiter:

Laut Cloudflare stiegen diese im vierten Quartal 2023 um 80 Prozent und legten im darauffolgenden Jahr nochmals um 50 Prozent zu. Moderne DDoS-Attacken nutzen mittlerweile KI, um in Echtzeit Sicherheitsmechanismen auszuwerten und Angriffsmuster dynamisch anzupassen. Solche intelligenten Angriffe können kritische Infrastrukturen wie Stromnetze, Verkehrsleitsysteme oder Gesundheitsdienste ins Visier nehmen und massive gesellschaftliche Schäden verursachen.

➤ Gezielte Angriffe auf kritische Infrastruktur und sensible Lieferketten: Energieversorger, Gesundheitsdienste und Verkehrssysteme stehen zunehmend im Visier, da deren Ausfall weitreichende gesellschaftliche und wirtschaftliche Folgen haben kann. Angriffe sind oft gut geplant und erfolgen in mehreren Stufen, um erste Abwehrmechanismen zu überwinden und letztlich den Betrieb zu stören. Der Ransomware-Angriff auf die Deutsche Energie-Agentur DENA Ende 2023 illustriert dies deutlich.

Da Unternehmen immer stärker auf digitale Netzwerke und Cloud-Dienste setzen, richten sich Angriffe vermehrt gegen die gesamte Lieferkette. Dies zeigt etwa das Beispiel des Cyberangriffs auf den Technologie-Zulieferer Kendrion aus dem Jahr 2023. Hier drohten Hacker damit, Unternehmensdaten zu veröffentlichen, sollte das Unternehmen kein Lösegeld zahlen.

Ziel kann es beispielsweise auch sein, über kleinere Zulieferer in größere Unternehmen einzudringen. Dabei werden Schwachstellen in weniger gut geschützten IT-Systemen genutzt, um sich so Zugang zu den Netzwerken von Großunternehmen zu verschaffen.

Proaktive IT-Sicherheitsstrategien als Schlüssel

Vor diesem Hintergrund müssen Unternehmen Cybercrime als strategische Herausforderung begreifen und proaktiv in ihre IT-Sicherheit investieren. Denn der Schaden, der durch die analogen und digitalen Angriffe entsteht, nimmt zu: Im Vergleich zum Vorjahr sind sie laut Bundesamt für Verfassungsschutz im Jahr 2024 um 29 Prozent angestiegen. Damit haben sie den bisherigen Höchststand von 223,5 Mrd. Euro aus dem Jahr 2021 übertroffen.

DURCH EINEN REGELMÄSSIGEN KI-BASIERTEN RISIKOSCAN VERHINDERN WIR SCHÄDEN, DIE EXISTENZBEDROHEND FÜR FIRMEN SEIN KÖNNEN.

Vincenz Klemm, Mitbegründer und CEO, Baobab Insurance, www.baobab.io

Technologische Maßnahmen wie regelmäßige Back-ups an extern gesicherten Standorten, strenge Passwort-Policies, Zwei-Faktor-Authentifizierung und ein durchdachtes Zugriffsmanagement sind dabei essenzieller Bestandteil einer proaktiven IT-Sicherheitsstrategie. Ebenso wichtig:

➤ Alle digitalen Vermögenswerte im Unternehmen, einschließlich Hardware, Software, Daten und Mitarbeiter, sollten regelmäßig auf mögliche Risiken bewertet werden. Durch diese kontinuierliche Analyse können potenzielle Schwachstellen frühzeitig erkannt und entsprechende Gegenmaßnahmen ergriffen werden.

➤ Einbindung der Mitarbeitenden in Form von Awareness-Trainings und regelmäßigen Schulungen helfen, damit sie Phishing-Mails und verdächtige Aktivitäten frühzeitig erkennen. Denn eine gut geschulte Belegschaft kann die Erfolgsquote von Cyberangriffen signifikant senken.

➤ Aussetzen eines soliden Incident-Response-Plan und regelmäßige Simulationen von Cyberangriffen bereiten das Team darauf vor, im Ernstfall schnell und koordiniert zu handeln. Ein solcher Notfallplan definiert zentrale Kommunikationsschritte und Verantwortlichkeiten, sodass im Falle eines Sicherheitsvorfalls keine wertvolle Zeit verloren geht.

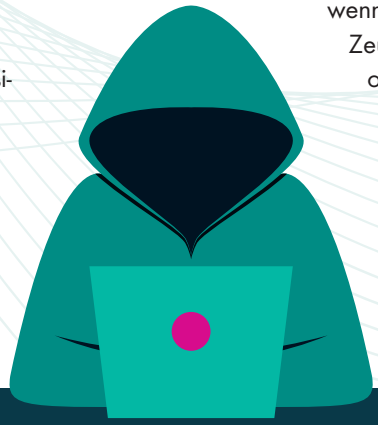
Cyberversicherungen und IT-Haftpflicht

Neben präventiven Maßnahmen spielt der Versicherungsschutz eine zunehmend wichtige Rolle. Hier sollten Unternehmen darauf achten, welche Leistungen die Anbieter abdecken: Moderne Cyberversicherungen wie Baobab helfen Unternehmen mit einem ganzheitlichen Serviceangebot nicht nur, finanzielle Schäden im Zuge eines Angriffs zu kompensieren. Sie bieten auch proaktive Hilfestellungen – von Checklisten für Sicherheits-Patches über Vorlagen für Incident-Response-Pläne bis hin zu regelmäßigen, KI-gestützten Risikoscans.

Letzterer hilft Schwachstellen in der IT frühzeitig zu identifizieren und zu beheben, bevor es zu einem Angriff kommt.

Für IT-, Software-, Technologie- und Telekommunikationsunternehmen macht außerdem eine IT-Haftpflichtversicherung Sinn, die finanzielle Sach- und Personenschäden abdeckt.

Sie hilft dem Versicherungsnehmer nicht nur dabei die Schuldfrage zu klären, sondern auch unberechtigte Forderungen abzuwehren. So greift diese Produkthaftpflichtversicherung beispielsweise, wenn eine fehlerhafte Software-Installation bei einem Kunden Schaden anrichtet und der Versicherungsnehmer verklagt wird. Aber sie deckt auch Datenverluste infolge eines Serverausfalls oder einen Verstoß gegen die Datenschutzbestimmungen ab und trägt die Ausfallkosten, wenn eine versicherte Person als Zeuge oder in anderer Funktion an einem Gerichtsverfahren teilnehmen muss.



Sicher in die digitale Zukunft

Die Bedrohung durch Cybercrime wird sich auch in den kommenden Monaten weiterentwickeln. Für IT-Verantwortliche und Entscheider bedeutet das: IT-Sicherheit ist ein kontinuierlicher Lernprozess und muss strategische Priorität erhalten. Unabhängig von ihrer Größe sind Unternehmen gefordert, ihre IT-Sicherheitsstrukturen ständig zu überprüfen und anzupassen – von der Sensibilisierung der Mitarbeitenden über den Einsatz modernster Technologien bis hin zu einem Versicherungsschutz mit ganzheitlichem Serviceangebot. Nur wer bereit ist, sich den dynamischen Herausforderungen der digitalen Welt zu stellen, kann langfristig erfolgreich agieren und den digitalen Wandel sicher gestalten.

Vincenz Klemm

CYBER-RESILIENZ

UNVERZICHTBAR FÜR DEN GESCHÄFTSERFOLG

In der digital vernetzten Welt von heute sind Unternehmen ausgeklügelten Cyberbedrohungen beispielsweise durch Ransomware, Datenschutzverletzungen und insiderbedingte Risiken ausgesetzt. Diese Angriffe richten sich gegen das Herzstück des Geschäftsbetriebs – Daten – und verursachen Betriebsausfälle, finanzielle Verluste, Rufschädigung und Nichteinhaltung von Vorschriften. Als Unternehmen auf diese Herausforderungen vorbereitet zu sein, ist unverzichtbar.

Angesichts dieser Herausforderungen ist CyberResilienz die Grundlage für Stabilität, Schutz der Daten und Geschäftsbetrieb. Durch umfassende Sicherheitsmaßnahmen, nahtlosen Geschäftsbetrieb und schnelle Wiederherstellung im Notfall können Unternehmen kritische Funktionen schützen und sich gegen die sich stetig weiterentwickelnden Bedrohungen wappnen.

In diesem Whitepaper gehen wir auf die Notwendigkeit und die Grundsätze der Cyber-Resilienz ein und stellen ein Rahmenwerk für die Integration von Präventions-, Erkennungs- und Wiederherstellungsmaßnahmen im Unternehmen vor. Gut gerüstete Unternehmen können so nicht nur ihre Daten und ihren Geschäftsbetrieb schützen, sondern auch ihre Glaubwürdigkeit gegenüber ihren Kunden wahren.

WHITEPAPER DOWNLOAD

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

www.it-daily.net/download

Cybervorfälle: Die größte Bedrohung für Unternehmen

SICHERHEITSÜBERPRÜFUNG ALS STRATEGISCHE NOTWENDIGKEIT

Cyberkriminalität ist die zentrale Geschäftsbedrohung unserer Zeit. Zum vierten Mal in Folge stehen im Allianz Risk Barometer 2025 Cyberangriffe unangefochten an der Spitze der Unternehmensrisiken – noch vor Betriebsunterbrechungen und geopolitischen Spannungen. In Deutschland beliefen sich 2024 die jährlichen Schäden durch Cyberangriffe laut Statista auf über 260 Milliarden Euro.

Trotz dieser Risiken gibt es in vielen Unternehmen keine systematische Überprüfung der Cybersicherheit. Während in regulierten Branchen Audits längst Standard sind, wird IT-Sicherheit oft nur punktuell betrachtet. Dabei zeigt sich in anderen Bereichen der Wirtschaft deutlich, dass regelmäßige Sicherheitsüberprüfungen unerlässlich sind: In der Automobilindustrie sind technische Inspektionen Voraussetzung für den Betrieb, in der Finanzbranche verhindern kontinuierliche Risikoanalysen schwerwiegende Fehlentscheidungen und im Gesundheitswesen reduziert Prävention das Risiko unerwarteter Krisen.

DIE ERWEITERTE VERANTWORTUNG DER GESCHÄFTSFÜHRUNG DURCH NIS2 MACHT D&O-VERSICHERUNGEN ODER VERGLEICHBARE ABSICHERUNGSLÖSUNGEN UNVERZICHTBAR.

Andrea Michalczyk-Schröder, Leiterin Specialty und Mitglied der Geschäftsleitung, Ecclesia Gruppe, www.ecclesia-gruppe.de

Als wesentlicher Baustein eines angemessenen Risikomanagements wird vermehrt auf eine Cyberversicherung gesetzt, die auch als Risikoevaluierung fungiert, regelmäßig Sicherheitslücken identifiziert und eine kontinuierliche Verbesserung der Schutzmaßnahmen ermöglicht. Allerdings erweist sich der Zugang zu einer Cyberversicherung aufgrund der großen Hürden zur Versicherbarkeit nicht immer als selbstverständlich.

Risikoevaluierung als Grundlage

Die Versicherbarkeit eines Unternehmens ist ein direktes Spiegelbild seines IT-Sicherheitsniveaus. Die entscheidende Frage ist nicht, ob ein Unternehmen Ziel eines Cyberangriffs wird, sondern ob es darauf vorbereitet ist. Eine fundierte Risikoevaluierung schafft Transparenz über bestehende Sicherheitsmaßnahmen, Schwachstellen und die Wirksamkeit aktueller Schutzkonzepte.

Für die Geschäftsführung bedeutet dies eine belastbare Einschätzung des aktuellen Risikoniveaus sowie der regulatorischen und haftungsrechtlichen Anforderungen. IT-Leitungen profitieren von einer datenbasierten Grundlage, um Investitionen in Cybersicherheitsmaßnahmen strategisch zu priorisieren und Budgetentscheidungen fundiert zu begründen.

Unternehmen, die ihre Cybersicherheit nicht regelmäßig prüfen, riskieren nicht nur finanzielle Schäden, sondern auch erhebliche Reputationsverluste, regulatorische Sanktionen und operative Einschränkungen.

Cyberversicherung als strategischer Faktor für Resilienz

Effektives Risikomanagement setzt eine nachvollziehbare Dokumentation der IT-Sicherheitslage voraus. Versicherer stellen heute zunehmend hohe Anforderungen an Schutzmaßnahmen und Re-

aktionsprozesse, um Risiken wirtschaftlich tragfähig abzusichern.

Unternehmen, die sich systematisch mit ihrer Cybersicherheit auseinandersetzen, profitieren von einem besseren Marktzugang sowie attraktiveren Versicherungsprämien.

Ähnlich wie eine Krankenversicherung nicht vor einem Unfall schützt, kann eine Cyberversicherung keine Hackerattacken verhindern. Jedoch haben Versicherer großes Interesse daran, den Kunden bestmöglich in der Cybersicherheit zu unterstützen. Oftmals sind Schwachstellenanalysen oder Awarenessmaßnahmen integraler Bestandteil von Cyberversicherungen. Und im Falle eines Angriffs bietet sie wichtigen Schutz: Zum einen dient diese als Vermögensschadendeckung dazu, die finanziellen Folgen abzudecken. Darüber hinaus stehen spezialisierte Dienstleister bereit, um die Krise zu bewältigen. Dies umfasst beispielsweise forensische Schadenfeststellung, die Verhandlung von Lösegeldern mit Erpressern oder die Datenwiederherstellung. Ebenfalls gedeckt sind Haftpflichtansprüche, wenn der Versicherungsnehmer aufgrund eines Cyberangriffs in Anspruch genommen wird.

UNSERE RISIKOEVALUIERUNG ERMÖGLICHT EINE UNABHÄNGIGE UND FUNDIERTE BEWERTUNG DER IT-SICHERHEITSLAGE EINES UNTERNEHMENS.

Ben Schmidt, Teamleiter Cyberversicherung, Produktmanagement und Komposit, Ecclesia Gruppe, www.ecclesia-gruppe.de

ECCYBER - STRATEGISCHER PARTNER FÜR NACHHALTIGE CYBERSICHERHEIT

Die Ecclesia Gruppe ist einer der führenden Versicherungsmakler Deutschlands und berät Kunden in sämtlichen Marktsegmenten. Als etablierter Akteur auf der it-sa geht die Expertise von eccyber weit über das Vermitteln von Versicherungslösungen hinaus. Ein zentrales Element des Ansatzes von eccyber ist die kontinuierliche Sicherheitsüberprüfung.

Unternehmen, die ihre Schutzmaßnahmen regelmäßig evaluieren und anpassen, minimieren Risiken, verbessern ihre Versicherbarkeit und stärken ihre langfristige Widerstandsfähigkeit gegenüber Cyberbedrohungen. Darüber hinaus verfügt eccyber über ein starkes Netzwerk aus führenden IT-Sicherheitsanbietern, Forensik- und Rechtsexperten sowie führenden Cyberversicherern.

D&O-Versicherung

Die D&O Versicherung hat bereits seit langem aufgrund der persönlichen Haftung für Managementfehler eine existenzielle Bedeutung für jeden Manager ein. Mit der rasant wachsenden Bedrohung durch Cyberkriminalität sowie der zuletzt mehrfach verschärften Gesetzgebung zur Cybersicherheit (insbesondere die NIS2 Richtlinie, DORA, sowie die DSGVO) wachsen die Haftungsrisiken der Geschäftsleitung noch einmal erheblich. Führungskräfte stehen zunehmend in der Pflicht, nachzuweisen, dass angemessene Schutzmaßnahmen etabliert wurden und kontinuierlich überprüft werden.

Vermehrt diskutiert wird in diesem Zusammenhang die Möglichkeit einer persönlichen Inanspruchnahme der Geschäftsführung. Eine solche Möglichkeit könnte sich auch durch den Regress einer Cyberversicherung ergeben. Insofern macht die steigende Verantwortung der Geschäftsleitung D&O-Versicherungen (Directors & Officers) unverzichtbar, um persönliche Haftungsrisiken im Zusammenhang mit Cybervorfällen abzusichern. Eine dezidierte Beratung bezüglich des Versicherungsumfangs sowie des Verhältnisses der einzelnen Versicherungszweige kann nur durch ein spezialisiertes Maklerhaus erfolgen.

Fazit

Cyberbedrohungen erfordern eine proaktive und strategische Herangehensweise an IT-Sicherheit. Regelmäßige Überprüfung und Optimierung der Cyberabwehr sind heute eine betriebswirtschaftliche Notwendigkeit.

Unternehmen, die frühzeitig auf ein strukturiertes Risikomanagement setzen, sichern sich nicht nur gegen finanzielle Schäden ab, sondern positionieren sich langfristig als widerstandsfähige und vertrauenswürdige Akteure im Markt.

Andrea Michalczyk-Schröder, Ben Schmidt

Souveräne IT-Sicherheit in der Praxis

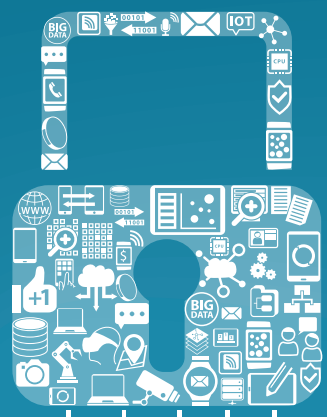
INTEGRALER BESTANDTEIL EINER MODERNEN CYBERSICHERHEITSSTRATEGIE

„Ohne digitale Souveränität wird es auch mit der europäischen Souveränität nichts," sagte Claudia Plattner – jetzt Präsidentin des BSI - im Jahr 2022, als sie noch IT-Leiterin der Europäischen Zentralbank war. Mit dieser Aussage unterstreicht sie die Relevanz der digitalen Souveränität für den europäischen Raum.

Doch was heißt „Souveränität" im Kontext der IT-Sicherheit und wie kann diese in der Praxis erreicht werden? Dieser Frage gingen wir im Februar auf der „Thought Leadership in der IT" nach und vertiefen diese im Rahmen des folgenden Artikels.

Der Begriff der digitalen Souveränität

Zunächst geht es um die Begriffsklärung, denn „digitale Souveränität" ist eine facettenreiche Vokabel. Verortet wird „Souveränität" zunächst auf der staatlichen Ebene, wenn es darum geht, die Handlungsfähigkeit von Staaten zu beschreiben insbesondere die Fähigkeit des Staates, digitale Vorgänge zu kontrollieren, die einen Einfluss auf sein Territorium haben und bei denen der Staat selbst oder staatliche Institutionen betroffen sind. Der Begriff beschränkt sich aber nicht nur auf die Kontrolle über digitale Prozesse und Technologien. Er umfasst darüber hinaus zusätzlich folgende Aspekte:



#1 Digitale Selbstbestimmung:
Individuen und Organisationen sollen die Kontrolle über ihre eigenen Daten und Informationen haben. Dies bedeutet Kontrolle darüber, wer auf die Daten zugreifen darf und die Möglichkeit, datengetriebene Prozesse (Wie kontrolliere ich Daten, den Zugriff auf diese und wer/was nutzt sie?) aktiv zu gestalten.

#2 Unabhängigkeit von externen Technologien und Diensten:
Die Abhängigkeit von Technologiekonzernen birgt Risiken, etwa durch den sogenannten Hersteller-Lock-In. Dieser erschwert Kunden aufgrund technischer oder wirtschaftlicher Barrieren den

Wechsel von Produkten oder Dienstleistungen eines bestimmten Herstellers. Die Reduzierung von Wahlmöglichkeiten durch Hersteller-Monopole hat unmittelbaren Einfluss auf die digitale Selbstbestimmung.

#3 Datenkontrolle und -schutz:
Daten haben einen Bedeutungsgehalt, der weit über den Ort ihrer Speicherung hinausgeht. Kontrolle über die Daten beinhaltet daher nicht nur deren physischen Schutz, sondern auch die Sicherstellung ihrer Integrität und die Kontrolle über die Verwendung der Daten.

Resilienz: Anpassungsfähigkeit an Herausforderungen
Im Kontext „digitaler Souveränität" spielt der Begriff der „Resilienz" eine wichtige Rolle. Er bezeichnet die Fähigkeit, auf unerwartete Herausforderungen zu reagieren und trotzdem funktionsfähig zu bleiben. Konkret bedeutet dies:

- **Anpassungsfähigkeit:** Flexibilität im Umgang mit (gesetzlichen) Änderungen, die erhebliche Auswirkungen auf die Datensicherheit und -integrität haben können, zum Beispiel dem US-Cloud-Act. In diesem Zusammenhang bedeutet Resilienz, dass ein IT-System und die dahinterstehenden Prozesse sich schnell an neue Rahmenbedingungen anpassen können, ohne die eigenen Schutzstandards zu gefährden.
- **Sicherheitsstrategien:** Robuste Sicherheitsmaßnahmen, die u.a. bei verstärkten Cyberangriffen wirksam bleiben. Eine resiliente IT-Infrastruktur ist nicht nur gegen Angriffe gehärtet, sondern kann schnell wiedergestellt werden, sollte ein Angriff erfolgreich sein.
- **Kontinuität:** Sicherstellung der Verfügbarkeit und Integrität der IT-Dienste – auch bei Störungen, um die Handlungsfähigkeit von Staaten und Unternehmen zu gewährleisten.
- **Transparenz:** Kommunikation und Aufklärung gegenüber der Bevölkerung, um Vertrauen zu stärken und Unsicherheiten zu minimieren.

IN EINER GLOBAL VERNETZTEN WELT IST ES ENTSCHEIDEND, FLEXIBEL UND HANDLUNGSFÄHIG ZU BLEIBEN, UM DIE DIGITALE SOUVERÄNITÄT IN EUROPA ZU GEWÄHRLEISTEN.

Martin Mangold, Senior Vice President Platform & Operations, DriveLock SE, www.driveLock.com

Digitale Souveränität in der Praxis

Sicherheit und Souveränität: Zwei Seiten derselben Medaille
Um digitale Souveränität in der Praxis zu gewährleisten, müssen Sicherheit und digitale Souveränität zusammen gedacht und umgesetzt werden. Diese strategische Herangehensweise ermöglicht es, resiliente Strukturen aufzubauen und Sicherheitsrisiken zu reduzieren.

Security Controls: Maßnahmen gegen Cyberangriffe
Ein zentrales Element dieser Strategie sind die Security Controls - Maßnahmen gegen Cyberangriffe, die entlang der gesamten Kill Chain positioniert werden. Diese umfassen mehrere Bereiche:

- **Mitarbeitende:** Schulung und Sensibilisierung für Cybergefahren, um menschliche Fehler zu minimieren und ein hohes Sicherheitsbewusstsein zu fördern. Es geht darum eine Sicherheitskultur zu etablieren.
- **Endgeräte:** Schutz vor unbefugtem Zugriff und Malware, um die Integrität und Vertraulichkeit der Daten auf den Geräten sicherzustellen.
- **Applikationen:** Sicherstellung der Integrität und Authentizität von Software. Nur vertrauenswürdige Anwendungen dürfen ausgeführt und eingesetzt werden. Darüberhinaus geht es um die Kontrolle was Applikation tun dürfen bzw. auf welche Daten sie zugreifen dürfen.
- **Daten:** Verschlüsselung und Zugangskontrollen, um die Vertraulichkeit und Sicherheit sensibler Informationen zu gewährleisten.

Digitale Souveränität geht jedoch über reine Sicherheitsmaßnahmen hinaus und umfasst auch die Kontrolle über digitale Prozesse, Daten und Technologien.

- Digitale Prozesse: Die Integration und transparente Steuerung der IT-Prozesse zur Sicherstellung einer nahtlosen und sicheren Zusammenarbeit der Systeme.
- Daten: Der Schutz sensibler Daten vor unbefugtem Zugriff und die sichere Verwaltung nach den gesetzlichen Datenschutzrichtlinien.
- **Technologien:** Der Einsatz souveräner IT-Lösungen, die nicht von externen Anbietern abhängig sind, um die Kontrolle und Flexibilität über die eingesetzten Technologien zu gewährleisten.

Wenn Sicherheit und digitale Souveränität Hand in Hand gehen, erhöht dies die Widerstandsfähigkeit (Resilienz) der IT-Infrastrukturen von Staaten und Unternehmen und stellt ihre Unabhängigkeit und Selbstbestimmung in der digitalen Welt sicher.

Das Shared Responsibility Model

In diesem Kontext sollte das Shared Responsibility Model neu gedacht und erweitert werden, um den umfassenderen Anforderungen moderner IT-Infrastrukturen gerecht zu werden. Bisher lag der Fokus primär auf der Verteilung von Verantwortlichkeiten zwischen Cloud-Anwendern und -Providern, hauptsächlich in Bezug auf Cloud Services. Für das Zusammenspiel von Souveränität und Sicherheit müssen Endgeräte, Applikationen, Daten und Menschen berücksichtigt werden. Die Verantwortung für Sicherheit und Souveränität darf nicht nur auf die Cloud-Infrastruktur beschränkt sein, sondern muss alle Elemente der IT-Landschaft umfassen. Unternehmen wie Staaten müssen sicherstellen, dass ihre Endgeräte vor unbefugtem Zugriff geschützt sind, Applikationen ihre Integrität und Authentizität bewahren, Daten verschlüsselt und kontrolliert werden und dass Mitarbeitende durch Schulungen und Sensibilisierungen auf die Bedeutung und Maßnahmen der Cybersicherheit vorbereitet sind. Nur durch eine ganzheitliche Betrachtung aller Komponenten können Souveränität und umfassende Sicherheit erreicht werden. Der wichtige Aspekt ist hier, dass Hersteller wie Anwender ganzheitlich ihre Verantwortung wahrnehmen. Dazu gehört die bewusste Entscheidung digitale Prozesse aktiv zu gestalten.

Quellen:
https://www.cio.bund.de/Webs/CIO/DE/digitale-loesungen/digitale-souveraenitaet/digitale-souveraenitaet-node.html
https://www.cio.bund.de/SharedDocs/downloads/Webs/CIO/DE/digitale-loesungen/eckpunktpapier-digitale-souveraenitaet.pdf?__blob=publicationFile&v=4
https://www.inside-it.ch/lex-laux-was-ist-digitale-souveraenitaet
https://de.wikipedia.org/wiki/Digitale_Souver%C3%A4nit%C3%A4t

Fazit

Digitale Souveränität ist keine isolierte Herausforderung, sondern ein integraler Bestandteil einer modernen Cybersicherheitsstrategie. Staat und Unternehmen müssen gemeinsam die Verantwortung für Sicherheit, digitale Selbstbestimmung und Resilienz übernehmen. Dies erfordert nicht nur den Aufbau souveräner IT-Infrastrukturen, sondern auch die Entwicklung ganzheitlicher Sicherheitskonzepte.

Souveränität wird schnell als „Abschottung" verstanden. Das ist sie ausdrücklich nicht. Vielmehr geht es um die Fähigkeit, Kontrolle und Selbstbestimmung auszuüben. In einer global vernetzten Welt ist es entscheidend, flexibel und handlungsfähig zu bleiben, um die digitale Souveränität in Europa zu gewährleisten. Nur so kann die digitale Souveränität, wie von Claudia Plattner betont, ein Grundpfeiler der europäischen Souveränität werden.

Martin Mangold

Hannover Messe 2025

NEUE ANTWORTEN AUF DYNAMISCHE RISIKEN IN DER INDUSTRIE

Weltweit nimmt in allen Bereichen der Industrie die Integration der Information Technology (IT) und Operational Technology (OT) zu. Doch in dem Maße, wie das Industrial Internet of Things (IIoT) wächst, wachsen auch die Cyber-Risiken. Somit gewinnt der Ausstellungsbereich IT-/OT-Security der Hannover Messe 2025 zentrale Bedeutung für die industrielle Transformation.

Die auf der Hannover Messe 2025 allgegenwärtigen neuen Technologien wie KI, Cloud Computing, Data Analytics, 5G oder Blockchain sind nicht nur Enabler der industriellen Transformation, sondern auch – oft kaum geschützte – Angriffsziele krimineller Energie. Die jährlichen weltweiten Kosten von Cyber-Verbrechen könnten laut einer von Statista veröffentlichten aktuellen Prognose zwischen 2024 und 2029 kontinuierlich um insgesamt 6,4 Billionen US-Dollar (+69,41 Prozent) steigen und im Jahr 2029 voraussichtlich 15,63 Billionen US-Dollar und damit einen neuen Höchststand erreichen.

Geschäftskritische Cyber-Sicherheit

„Cyber-Sicherheit ist geschäftskritisch", betont auch Marcel van Asperdt, der als Chief Information Security Officer von Eye Security auf der Industrial Security Circus Stage über die steigenden Bedrohungen sprechen wird, die durch Fachkräftemangel und Kostendruck noch verschärft werden. „Besonders für den Mittelstand sind bezahlbare Lösungen essenziell – ein kontinuierliches Sicherheitsmonitoring kombiniert mit einer Cyber-Versicherung bietet den besten Schutz", so van Asperdt weiter.

Cyber-Sicherheitsgesetze als Wettbewerbsfaktor

Mit der Entwicklung eines netzwerkbasierten Angriffserkennungssystems für die OT hat die Rhebo GmbH die Cyber-Sicherheit industrieller Netze bereits vor gut zehn Jahren neu gedacht. Heute beschreibt Uwe Dietzmann, Sales Manager des Unternehmens, die Cyber-Sicherheit vor dem Hintergrund neuer Cyber-Sicherheitsgesetze wie NIS2 und dem Cyber Resilience Act als wichtigen Wettbewerbsfaktor in der EU. „Besuchende des Industrial Security Circus auf der Hannover Messe 2025 erwartet mit Rhebo das ausgefeilteste und leistungsstärkste Portfolio für OT Security Made in Germany – vom OT-Kern bis zur IIoT Edge, von der initialen Risikobewertung bis zum Betrieb eines Systems zur Angriffserkennung", so Dietzmann.

Die Stars der Manege des Industrial Security Circus

Die Stars der Manege des Industrial Security Circus sind also keineswegs so ratlos wie die Artisten in der Zirkuskuppel im legendären Spielfilm von Alexander Kluge. Mit Netz und doppeltem Boden sorgen sie für den Schutz von Menschen, Anlagen, Umwelt und Unternehmensreputation. Die DCSO beispielsweise liefert die passenden Antworten auf die asymmetrische Bedrohung durch global agierende, organisierte Cyber-Kriminalität und staatlich gelenkte Wirtschaftsspionage und das BSI informiert, wie mit einer gesamtstaatlichen Anstrengung unsere Resilienz weiter erhöht werden kann. Das Airbus Tochterunternehmen Infodas stellt mit der SDoT Secure Network Card einen wirksamen Schutz gegen Supply-Chain-Angriffe vor und Secunet präsentiert mit der SINA Cloud die erste Cloud-Infrastrukturlösung in Deutschland, deren Sicherheitsarchitektur für Verschlusssachen (VS) zugelassen wird – und zwar bis einschließlich der Einstufung GEHEIM.

www.hannovermesse.de

Managed Security Operations Center

DER SCHLÜSSEL ZU EINER EFFEKTIVEN IT-SICHERHEIT

Die aktuelle Bedrohungslage erfordert in Unternehmen eine zeitgemäße IT-Sicherheitsstrategie. Gefragt sind Konzepte, die in der Lage sind, Cyberangriffe umgehend zu stoppen oder gar zu verhindern. Möglich ist das mit einem Managed Security Operations Center (kurz Managed SOC).

Der klassische Virenschutz war lange Zeit das Maß aller Dinge bei der IT-Sicherheit in Firmen. Bis heute ist er eine bewährte Sicherheitslösung. Sie stößt allerdings an Grenzen. Früher waren Schadprogramme die Basis von Cyberangriffen. Diese wurden durch die umfangreichen Technologien im Virenschutz zuverlässig entdeckt und unschädlich gemacht. Die Kriminellen haben mittlerweile aber ihre Strategie geändert und setzen heute auf dateilose Angriffsverfahren: Häufig nutzen sie Windows-Funktionen oder ungeschlossene Sicherheitslücken in Anwendungen oder dem Betriebssystem aus, um in die IT-Infrastruktur einzudringen. Eine weitere Möglichkeit ist ein individualisierter, genau auf das betroffene Unternehmen zugeschnittener Angriff. Hier kommen Phishing oder Social Engineering zum Einsatz, um zum Beispiel Zugangsdaten zu den Systemen zu erhalten. Diese Angriffsarten sind nur zu entdecken, indem etwa Fachleute Logs aus Analysesystemen auswerten und schädliche Aktionen erkennen.

Cyberangriffe sofort stoppen

Ein Managed SOC ermöglicht das Sammeln und die Analyse von Logs und damit das Stoppen von dateilosen Angriffen. Die gemanagte SOC-Lösung ist mit einer breit gefächerten Sensorik ausgestattet, um zentral alle fragwürdigen und schädlichen Aktivitäten in den IT-Systemen eines Unternehmens aufzudecken. Hierzu überwacht ein erfahrenes, externes Analystenteam die IT-Systeme rund um die Uhr und analysiert Vorgänge. Verdächtige Aktivitäten, zum Beispiel die plötzliche Vergabe von Administrationsrechten, werden überprüft. So lässt sich verifizieren, ob es sich um eine Cyberattacke handelt oder nicht. Liegt ein Angriff vor, reagiert das Analystenteam umgehend und leitet Gegenmaßnahmen ein. Der Vorteil: So lassen sich Cyberattacken schon in den Anfängen erkennen und beenden, bevor es zu größeren Schäden kommt. Hier zeigt sich ein weiterer großer Vorteil von Managed SOC gegenüber einer Virenschutzlösung: Die Response auf schadhafte Vorgänge im Netzwerk.

24/7-Security

Die Gewährleistung von IT-Sicherheit ist eine Rund-um-die-Uhr-Aufgabe, denn Cyberkriminelle greifen auch nachts

und an Wochenenden an. Daher ist das Analystenteam einer Managed-SOC-Lösung 24 Stunden und an sieben Tagen in der Woche im Einsatz. So ist sichergestellt, dass keine wertvolle Zeit vergeht, bis ein Angriff gestoppt wird. IT-Teams in Unternehmen können eine Rund-um-die-Uhr-Schichtabdeckung oft nicht leisten, da diese Aufgabe viel Personal und Aufwand in Anspruch nimmt. Im Regelfall sind die Mitarbeitenden durch das Tagesgeschäft bereits voll ausgelastet, sodass keine Zeit für IT-Sicherheit bleibt. Der Mangel von Fachkräften ist generell ein großes Problem, insbesondere im Bereich IT-Sicherheit. Im Jahr 2023 fehlten in Deutschland fast 105.000 IT-Fachkräfte (Quelle: Cybersicherheit in Zahlen von G DATA CyberDefense, Statista und brand eins) und die Lage hat sich bis heute nicht geändert.

IT-Mitarbeitende in Unternehmen verfügen oft nicht über das tiefgreifende Security-Spezialwissen, um schädliche Vorgänge zu entdecken und detailliert zu analysieren, damit die richtige Reaktion darauf erfolgt. Wird ein Angriff in seinen Anfängen nicht entdeckt und beendet, hat dies weitreichende und fatale Folgen für das Unternehmen, die von teuren Ausfällen bis hin zu wirtschaftlichen Schwierigkeiten führen. Daher ist es sinnvoll, auf externe Expertise zu setzen und damit auf eine gemanagte SOC-Lösung. Das Analystenteam ist fachlich immer auf dem neuesten Stand und im ständigen Austausch über neue Angriffsvektoren und Cybercrime-Trends mit einem internationalen Netzwerk. Von dem Wissen und der Erfahrung profitieren Unternehmen, gerade wenn es um Handlungsempfehlungen abseits der reinen Überwachung geht. Diese häufige Komponente eines Managed SOC sorgt für weitere IT-Sicherheit.

Compliance-gerecht sein

Ein Managed SOC ist insbesondere für Unternehmen gut geeignet, die hohen Regulatorik-Anforderungen gerecht werden müssen. Ein Beispiel hierfür ist die Network-and-Information-Richtline – kurz NIS oder der Cyber Resilience Act. Je nachdem, welche Regulatorik zu befolgen ist, sind Firmen hierdurch verpflichtet, weitgehende Sicherheitsmaßnahmen zu ergreifen und auch Meldepflichten einzuhalten. Bei NIS-2 sind die Erkennung, Analyse, Eindämmung und Reaktion auf schädliche Vorfälle vorgeschrieben. Diese Aufgaben gehören auch zu den Tätigkeiten der Expertinnen und Experten von Managed SOC. Generell ist dieses Konzept eine gute Lösung für Firmen, die einem hohen Cyberrisiko ausgesetzt sind – unabhängig von der Unternehmensgröße und der Branche. Anzudenken ist ein Einsatz aber auch, wenn die IT-Infrastruktur sehr komplex und hierdurch nur schwer zu überblicken ist. Das kann schon bei einem kleinen Mittelständler der Fall sein.

Managed SOC und die Rolle von KI

In einem Managed SOC werden jeden Tag eine Vielzahl von Daten analysiert und diese Menge wächst immer weiter an. Schon heute ist Künstliche Intelligenz (KI) an dieser Stelle im Einsatz und nicht mehr wegzudenken. Die Analystinnen und Analysten wären ansonsten nicht in der Lage, mit der Vielzahl an Informationen zu arbeiten, diese zu bewerten und bei Bedarf einzugreifen. KI ist ein Teil der Analysesysteme und clustert und sortiert die Daten vor, sodass sich die Expertinnen und Experten auf die wichtigen Fälle konzentrieren. Künstliche Intelligenz ist schon jetzt sehr leistungsfähig und dies wird in Zukunft weiter zunehmen und auch die Rolle wird immer wichtiger: KI kann viel schneller als ein Mensch einschätzen, wo Unregelmäßigkeiten bestehen. Hierdurch beschleunigen sich die Prozesse enorm.

Trotz aller Vorteile durch Künstliche Intelligenz wird sie den Menschen bei einem Managed SOC nicht ersetzen, sondern Hand in Hand mit dem Analystenteam arbeiten. Weiterhin macht es Sinn, manuelle Analysen durchzuführen und sich nicht vollständig auf KI zu verlassen. Der Grund: Eine KI arbeitet auch nicht immer fehlerfrei. Daher ist die Kombination aus Künstlicher Intelligenz und einem Analystenteam ideal bei einem Managed SOC. Unternehmen profitieren von leistungsfähiger IT-Sicherheit.

EIN MANAGED SOC ERMÖGLICHT DAS SAMMELN UND DIE ANALYSE VON LOGS UND DAMIT DAS STOPPEN VON DATEILOSEN ANGRIFFEN.

Kathrin Beckert-Plewka, Public Relations Managerin, G DATA CyberDefense AG, www.gdata.de

Fazit: Managed SOC als große Chance für Unternehmen

Unternehmen sind auch zukünftig einem hohen Risiko durch Cyberattacken ausgesetzt. Ein Managed SOC ist für IT-Verantwortliche daher eine gute Möglichkeit, für mehr und effektive IT-Sicherheit zu sorgen, ohne dass dies an fehlendem Personal oder mangelndem Know-how scheitert. Am Ende erreichen IT-Verantwortliche schnell einen Return of Invest (ROI), da teure Systemausfälle und andere Schäden verhindert werden.

Kathrin Beckert-Plewka

KI und 24/7-Service: Die neue Security-Strategie

WIE UNTERNEHMEN TROTZ FACHKRÄFTEMANGEL RANSOMWARE-ANGRIFFE ABWEHREN

Mangel führt bekanntlich zu Kreativität, insbesondere wenn dieser Mangel lange anhält und elementar wichtige Bereiche betrifft. Genau das ist seit Jahren in der IT-Sicherheit der Fall. IT-Administratoren, IT-Ingenieure oder IT-Leiter zu finden gleicht einem harten Rennen, bei dem viele Supersportler um den Sieg kämpfen – insbesondere die kleineren Unternehmen und der Mittelstand. Unternehmen, die sich besonders engagieren, haben mit herausragenden Angeboten zumindest eine Chance, den Stich um die wenigen verfügbaren Spezialisten zu machen. Die Alternative: Das Unternehmen geht ganz einfach andere Wege und lagert Teile der IT-Security an die KI und externe Spezialisten aus. Klingt einfach, ist es auch.

Zu den Fakten

Um für eine effektive Cybersecurity zu sorgen, ist umfassende Expertise erforderlich, wobei die Anforderungen stetig steigen. Cyberangriffe werden immer komplexer, weshalb ein hohes Maß an Erfahrung und Fachwissen vorhanden sein muss, um sie zu erkennen und zu stoppen. Ein Ende des Fachkräftemangels im Bereich Cybersecurity ist jedoch nicht abzusehen. Dies trifft KMUs überproportional stark. Laut einer weltweiten Umfrage von Sophos bewerten Unternehmen mit weniger als 500 Mitarbeitern fehlendes Fachwissen/ Fachpersonal im Bereich Cybersecurity als zweitgrößtes Cybersecurity-Risiko. Nur Zero-Day-Bedrohungen werden als noch größere Gefahr betrachtet.

Gleichzeitig ist es für KMUs besonders schwierig, intern ausreichend Cybersecurity-Expertise aufzubauen. Wenn das IT-/Sicherheitsteam nur wenige Mitarbeiter umfasst, können diese nur höchst selten aus dem Alltagsbetrieb herausgenommen werden, um an Weiterbildungen teilzunehmen. Zudem haben weniger Kollegen auch weniger Möglichkeiten, gegenseitig voneinander zu lernen.

Gleichzeitig folgen Angreifer keinem geregelten Arbeitsalltag, sodass Cyberschutz rund um die Uhr vorhanden sein muss. Tatsächlich beginnen 91 Prozent der Ransomware-Angriffe außerhalb der normalen Geschäftszeiten, da Angreifer die Abwehr unerkannt überlisten möchten. Aus der Sophos Umfrage geht auch hervor, dass in KMUs während eines Drittels der Zeit niemand Warnungen aktiv überwacht, analysiert oder darauf reagiert. Ohne genügend Mitarbeiter, die aktiv auf Bedrohungen reagieren, sind demnach kleinere Organisationen den Angriffen weitestgehend schutzlos ausgesetzt.

Somit sind mindestens vier oder fünf Vollzeitmitarbeiter erforderlich, um 24/7 für Cybersecurity zu sorgen und Urlaub, Krankheitstage und Wochenenden abzudecken. In den meisten KMUs kann dies jedoch weder personell noch budgetär geleistet werden.

Folglich werden die Cybersecurity-Aufgaben unter weniger Mitarbeitern aufgeteilt, was das Burnout-Risiko steigert. In separaten, von Sophos beauftragten Studien gaben 85 Prozent der Unternehmen an, dass ihre Cybersecurity- und IT-Experten sich müde und erschöpft fühlen, wobei beinahe ein Viertel (23 %) „häufig" und 62 Prozent „gelegentlich" davon betroffen ist. Ebenfalls beunruhigend: 90 Prozent der Unternehmen geben an, dass Fälle von Burnout und Erschöpfung in den letzten 12 Monaten angestiegen sind. 30 Prozent berichten sogar, dass diese Fälle „deutlich" angestiegen sind.

MIT EINEM MEHRSCHICHTIGEN CYBERSECURITY-ANSATZ MIT 24/7 DETECTION AND RESPONSE SERVICES SIND UNTERNEHMEN BESTENS AUFGESTELLT.

Michael Veit, Security-Experte, Sophos, www.sophos.com

Ein Teufelskreis, den es zu unterbrechen gilt.

Auf den richtigen Partner kommt es an

Eine Möglichkeit, den Mangel an Fachpersonal, Kapazitäten und Expertise abzufedern, ist die Zusammenarbeit mit externen Sicherheitsexperten. Der Zugriff auf externe Cybersecurity-Experten ist für die meisten Unternehmen die einfachste und kosteneffizienteste Methode, die internen Schwächen in der Cybersecurity zu kompensieren.

Dabei wird am häufigsten auf Managed Detection and Response (MDR) Services und Managed Service Provider (MSP) gesetzt. Bei MDR-Services übernimmt ein Expertenteam rund um die Uhr die Aufgaben des Threat Hunting sowie der Erkennung und Reaktion. Spezialisierte Analysten halten 24/7 proaktiv Ausschau nach Bedrohungen, reagieren auf verdächtige Aktivitäten und beseitigen Angriffe, bevor Schaden für das Unternehmen entsteht.

Dabei ist es wichtig, einen Anbieter von Security-Dienstleistungen an Bord zu nehmen, der sich an die Anforderungen und die gewünschte Arbeitsweise anpasst: Vielleicht möchte ein Unternehmen die Bedrohungserkennung und -reaktion komplett auslagern, oder aber nur bei Alarmen und Vorfällen mit den Analysten des Anbieters zusammenarbeiten. Da Budgets in der Regel knapp sind, sollten sich Unternehmen zudem für einen Service-Anbieter entscheiden, der die vorhandenen Sicherheitstechnologien nutzen kann und keine zusätzlichen Kosten und Unterbrechungen für einen Austausch verursacht.

Nicht nur geschützt, sondern sicher

Es ist die Kombination aus Security-Lösung und Security-Service-Partner, die bei der Cybersicherheit die Spreu vom Weizen trennt. Viele Cybersecurity-Lösungen wurden für größere Unternehmen mit großen Teams entwickelt, die diese Lösungen bereitstellen und verwalten. Es mag im ersten Moment zwar nach einer guten Idee klingen, umfassende Unternehmenslösungen einzusetzen. Allerdings bemerken kleinere Unternehmen dabei oft keine Vorteile in puncto Sicherheit und Rendite, da sie diese Lösungen nicht optimal nutzen können. Für kleinere Unternehmen und KMUs sind stattdessen Sicherheitstools relevant, die ebenso wie die Enterprise-Lösungen technisch fortgeschritten sind, aber so konzipiert wurden, dass kleine und überlastete IT-Teams sie in der Praxis einfach nutzen können. Wichtig in diesem Zusammenhang sind zwei As-

pekte: Die Integration aller Sicherheits-Tools in eine skalierbare Plattform und die Integration von KI für den bestmöglichen Cyberschutz.

Wenn Cybersecurity-Lösungen in einer zentralen Plattform konsolidiert sind, reduziert sich der tägliche Verwaltungsaufwand deutlich. Weder interne noch externe Administratoren müssen von Konsole zu Konsole wechseln, um die Security-Infrastruktur und die Meldungen in Blick zu behalten. Zudem können in einer leistungsstarken Plattform die unterschiedlichen Sicherheitslösungen nahtlos zusammenarbeiten und beispielsweise Telemetriedaten, Erkenntnisse und nutzerbasierte Richtlinien gemeinsam nutzen, um Ihre Cyberabwehr zu stärken.

In diesem Zusammenhang kommt der Künstlichen Intelligenz (KI) eine ganz besondere Rolle bei der Cyberabwehr zu. Um einen wichtigen Aspekt an dieser Stelle klarzustellen, die KI kann bis heute nicht die Kreativität und Intuition eines Menschen ersetzen und ist daher immer noch eine Technologie und kein Ersatz für menschliches Handeln. Allerdings sind KI-Modelle so weit fortgeschritten, dass sie eine Datenfülle in ungeheurem Ausmaß korrelieren und aus den Schlüssen Aktionen ableiten können.

Wirkungsvolle Plattformen für die Cybersicherheit integrieren modernste KI-Technologien und erkennen beziehungsweise stoppen Ransomware-Angriffe, bevor sie ins Netzwerk eindringen. Mit einer Kombination aus fortschrittlicher KI und Machine Learning, die auf Millionen von Samples trainiert wurde, sowie Echtzeit-Sandboxing, erkennen Security-Lösungen mit integrierter KI auch bisher unbekannte Bedrohungen.

Folglich ...

Die Cyberkriminalität und darin insbesondere Ransomware entwickelt sich ständig weiter. Nach wie vor sehen sich viele Unternehmen so zur Zahlung von Lösegeld gezwungen. Das Ziel ist es, Angreifer daran zu hindern, in das Unternehmen einzudringen. Falls es den Cyberkriminellen doch gelingen sollte, müssen diese von der KI und den Cybersecurity-Serviceteam schnell erkannt und gestoppt werden. Mit einem mehrschichtigen Cybersecurity-Ansatz mit 24/7 Detection and Response Services sind Unternehmen bestens aufgestellt.

Michael Veit

live
WEBINAR
AM 27.03.2025
10:00 BIS
11:00 UHR

HERAUSFORDERUNG NIS2

SO MACHEN SIE UNTERNEHMEN FIT FÜR DIE ANFORDERUNGEN

NIS2 – Was kommt auf Unternehmen zu und wie können sie sich optimal vorbereiten? Das Webinar mit Sebastian Weber, findet live am Donnerstag, den 27.03.2025, von 10:00 bis 11:00 Uhr statt. Die Teilnahme ist gebührenfrei.

Die neue NIS2-Richtlinie stellt Unternehmen vor große Herausforderungen – doch was genau steckt dahinter, wer ist betroffen und welche Maßnahmen sind jetzt erforderlich? In diesem Webinar erhalten Sie einen kompakten Überblick über die wichtigsten Anforderungen und erfahren, warum frühzeitiges Handeln entscheidend ist.

Besonders spannend: In einer Live-Demo zeigen wir Ihnen, wie Sie mit der Aagon Client Management Platform (ACMP) gezielt Sicherheitsanforderungen umsetzen und Ihr Unternehmen optimal auf NIS2 ausrichten. Erleben Sie praxisnahe Lösungen, konkrete Handlungsempfehlungen und wertvolle Insights für eine effektive Umsetzung.

Nutzen Sie diese Gelegenheit, um sich bestens auf die neuen Vorgaben vorzubereiten!

Warum Sie unbedingt dabei sein sollen? Sie erfahren:

#1 Eine Praxisnahe und verständliche Erklärung der NIS2-Richtlinie inklusive der wichtigsten Anforderungen und betroffenen Unternehmen.

#2 Eine frühzeitige Vorbereitung auf NIS2, um Risiken zu minimieren und den neuen Vorgaben gerecht zu werden.

#3 Einen direkten Mehrwert durch konkrete Lösungen und einer ACMP Live-Demo, die zeigen, wie sich NIS2 effizient umsetzen lässt.

SPRECHER:
SEBASTIAN WEBER

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.

HIER ANMELDEN FÜR DAS KOSTENLOSE LIVE-WEBINAR

Mobile Security

WARUM KMU AUF MOBILFUNKTARIFE MIT INTEGRIERTER SICHERHEIT SETZEN SOLLTEN

Maßgeschneiderte Mobilfunktarife bieten KMU nicht nur Kosteneffizienz und Flexibilität, sondern auch integrierte Sicherheitsfunktionen – unerlässlich, um Mitarbeitende vor Cyberbedrohungen zu schützen.

Der Einsatz von Smartphones, Tablets und anderen mobilen Geräten ist in vielen Branchen unverzichtbar geworden – ob im Außendienst oder bei Kundenbesuchen. Nicht nur in großen Unternehmen: Auch ein kleiner Handwerksbetrieb etwa, dessen Mitarbeitende täglich auf Baustellen unterwegs sind, benötigt eine zuverlässige und flexible mobile Kommunikation, um effizient zu arbeiten. Die Bereitstellung von Firmenhandys mit passenden Mobilfunktarifen geht jedoch oft mit hohen Kosten einher. Hier setzen maßgeschneiderte Mobilfunktarife an, die speziell auf die Bedürfnisse von kleinen und mittleren Unternehmen (KMU) zugeschnitten sind.

Kosten sparen durch Teamkarten

KMU, die besonders auf die Kosteneffizienz achten müssen, sollten die Möglichkeit haben, Verträge flexibel und bedarfsgerecht zu gestalten. Dies hilft, unnötige Ausgaben zu vermeiden. Ein effektiver Weg ist zum Beispiel die Nutzung von hinzubuchbaren SIM-Karten, mit denen sich effizient ein komplettes Team ausstatten lässt. Dies bietet volle Kostenkontrolle und stellt sicher, dass nur für tatsächlich genutzte Leistungen bezahlt wird. Indem sie Mobilfunkverträge bündeln, können Betriebe von Mengenrabatten profitieren und die Mobilfunkkosten erheblich einfacher verwalten.

> MASSGESCHNEIDERTE MOBILFUNKTARIFE SIND FÜR KLEINERE BETRIEBE UNERLÄSSLICH, UM IN EINER ZUNEHMEND MOBILEN UND DIGITALEN ARBEITSWELT WETTBEWERBSFÄHIG ZU BLEIBEN.
>
> **Lukas Lebahn, Vice President Commercial Management für den Geschäftskundenbereich T Business, Deutschen Telekom, www.telekom.de**

Die mobile Sicherheit im Blick behalten

Ein noch weitaus wichtigerer Aspekt: Mit der zunehmenden Nutzung von Mobilfunkgeräten im Arbeitsalltag nehmen auch die Sicherheitsrisiken zu. Viele KMU verfügen nicht über ausreichende mobile Sicherheitsmaßnahmen. Eine Untersuchung des Technologiekonzerns Sharp zeigt, dass 55 Prozent der KMU keine mobile Sicherheitslösung nutzen und 57 Prozent auch noch keine Multi-Faktor-Authentifizierung implementiert haben. Diese Lücke wird zum Beispiel relevant, wenn Mitarbeitende mit ihren Smartphones sensible Kundendaten verwalten. Die IT-Sicherheitsinfrastrukturen vieler KMU haben also Potenzial für Verbesserungen.

Vielfältige Bedrohungen für dienstliche Mobilgeräte

Ein häufiges Sicherheitsproblem ist etwa das Abfangen sensibler Daten. Hierbei versuchen Angreifer, den mobilen Datenverkehr der Endgeräte mitzulesen oder zu manipulieren. Eine weitere ernstzunehmende Bedrohung sind Phishing-Angriffe, bei denen Angreifer täuschend echt aussehende Nachrichten oder E-Mails versenden, um Mitarbeitende dazu zu bringen, vertrauliche Informationen preiszugeben oder schädliche Links zu öffnen. Meist verwenden die Angreifer Logistik- und Zahlungsdienstleister als Absender ihrer gefälschten Nachrichten. Den Security-Experten von Barracuda zufolge gingen 71 Prozent aller gezielten E-Mail-Angriffe, denen kleine Unternehmen 2024 ausgesetzt waren, auf das Konto von Phishing.

Diese Angriffe sind besonders effektiv, wenn Mitarbeitende unterwegs sind und weniger aufmerksam auf Sicherheitswarnungen reagieren. Darüber hinaus kann das mobile Endgerät durch den Download von Apps aus unbekannten Quellen zum Teil eines Bot-Netzes werden. Hierbei handelt es sich um Netzwerke, die aus kompromittierten Geräten bestehen und von Cyberkriminellen ferngesteuert werden können, um DDoS-Angriffe durchzuführen oder Schadsoftware zu verbreiten.

Kosten und Aufwand sparen durch integrierte Security

Ein maßgeschneiderter Mobilfunktarif für kleinere Betriebe kann dabei helfen, diesen Attacken vorzubeugen. Der Tarif

sollte eingebaute Sicherheitsfunktionen bieten – und zwar ohne zusätzliche Kosten oder die Notwendigkeit einer speziellen App. Die integrierte Sicherheitsleistung in einem solchen Tarif blockiert den Zugriff auf betrügerische Webseiten und verhindert, dass sensible Daten preisgegeben werden. Sie erkennt schädliche Links, bevor sie Schaden anrichten können. Zudem schützt sie mobile Geräte vor unerwünschten Zugriffen und Fernsteuerung durch Cyberkriminelle.

Sind die Sicherheitsleistungen bereits im Mobilfunknetz integriert – und damit automatisch aktiv –, bieten sie effektiven Schutz vor Cyberbedrohungen. Regelmäßige Sicherheitsreports, über ein zentrales Portal abrufbar, ermöglichen es Unternehmen zudem, einen Überblick über potenzielle Angriffe und deren Abwehr zu behalten und ihre Mitarbeitenden gezielt vor Risiken zu warnen.

Ein weiterer Vorteil integrierter Sicherheitsfunktionen ist, dass sie im Vergleich zu Sicherheits-Apps von Drittanbietern nahtlos in den Mobilfunktarif integriert sind. Unternehmen müssen so keine zusätzlichen Apps oder Clients installieren oder verwalten, der administrative Aufwand sinkt erheblich. KMU sparen nicht nur Kosten, etwa für die Buchung einer Sicherheitsapp, sondern auch Zeit und Ressourcen, denn Updates werden direkt aus dem Mobilfunknetz heraus durchgeführt. Ein weiterer großer Vorteil: Kunden profitieren davon, dass sich Sicherheits-Expertinnen und -Experten mit langjähriger Erfahrung im Schutz von Geschäftskunden-Infrastrukturen um die mobile Sicherheit kümmern. Sie analysieren kontinuierlich die Bedrohungslage und passen die Schutzmaßnahmen entsprechend an.

Empfehlungen für KMU

Gerade kleinere Betriebe sollten sich deshalb mit dem Thema Mobile Security beschäftigen und darauf achten, dass Mobilfunktarife integrierte Sicherheitsfunktionen bieten. Diese sollten einen guten Basis-Schutz vor Cyberbedrohungen bieten und ohne zusätzliche Kosten oder Verwaltungsaufwand genutzt werden können. Außerdem sollten KMU ihre Mitarbeitenden regelmäßig für die potenziellen Gefahren sensibilisieren und die richtigen Verhaltensweisen im Umgang mit IT-Sicherheit schulen.

Denn eines ist klar: Auch kleine Unternehmen sind auf mobiles Arbeiten angewiesen. Mitarbeitende können auch außerhalb des Büros auf wichtige Informationen und Kommunikationskanäle zugreifen, was zu einer schnelleren und effizienteren Kommunikation führt. Beschäftigte ohne Computerarbeitsplatz, zum Beispiel in Produktion, Handel, Logistik oder Vertrieb, lassen sich in die interne Kommunikation einbinden und bleiben mit Kollegen in Kontakt.

Zudem erwarten vor allem jüngere Bewerber und Bewerberinnen von ihrem potenziellen Arbeitgeber, dass er ihnen eine entsprechende technische Ausstattung bietet. Das sollte nicht an den Kosten scheitern – schon gar nicht, wenn es um die mobile Sicherheit geht. Deshalb sind maßgeschneiderte Mobilfunktarife für kleinere Betriebe unerlässlich, um in einer zunehmend mobilen und digitalen Arbeitswelt wettbewerbsfähig zu bleiben.

Lukas Lebahn

CYBERSICHERHEITSRISIKEN

der europäischen KMU wurden schon Opfer von Phishing- oder Malware-Angriffen.

haben ihre internen Cybersicherheitsschulungen nicht an hybrides Arbeiten angepasst.

(Quellen: Sharp, Barracuda)

sehen mangelnde Kenntnisse ihrer Mitarbeitenden über Cybersicherheitsrisiken.

aller E-Mail-Angriffe auf KMU sind Phishing-Mails.

Datenschutzberatung mit innovativer Technologie

STEIGERN SIE DIE EFFIZIENZ MITHILFE VON KÜNSTLICHER INTELLIGENZ

Die fortschreitende Digitalisierung stellt Unternehmen und Organisationen vor immer größere Herausforderungen, ihre sensiblen Daten zu schützen. Statistiken zeigen dies deutlich: Nach einer Umfrage aus dem Jahr 2024 waren rund neun von zehn der deutschen Unternehmen u.a. von Datendiebstahl und Industriespionage mit hoher Wahrscheinlichkeit betroffen. Dies macht einen Anstieg von über zehn Prozent im Vergleich zum Vorjahr aus. Am häufigsten wurden Kommunikationsdaten wie E-Mails (63 Prozent), Kundendaten (62 Prozent), Zugangsdaten (35 Prozent) oder geistiges Eigentum (26 Prozent) gestohlen [1].

Neben massiven unternehmerischen Risiken, etwa durch Verlust oder ungewollte Offenlegung sensitiver Daten, sowie der Verantwortung gegenüber Beschäftigten und Kunden, fallen auch regulatorische Risiken zum Schutz von Personendaten auf Basis des Artikels 83 der Datenschutz-Grundverordnung (DSGVO) ins Gewicht. Letzterer in besonderem Maße, da hierin ein empfindlicher Bußgeldrahmen festgesetzt wird [2]. So belaufen sich nach Berichten die durchschnittlichen Kosten für eine Datenschutzverletzung im Jahr 2024 in Deutschland auf 5,15 Millionen Euro. Damit belegt das Land nach wie vor einen der Top-Ränge für anfallende Kosten im internationalen Vergleich [3].

Mangelndes Verständnis und Gefahr von Shadow-IT

Die Gründe für solche Verletzungen und etwaige Schäden sind vielfältig. Es fehlt häufig das notwendige juristische Verständnis über einzuhaltende Pflichten hinsichtlich der DSGVO. Außerdem liegt das relevante Fachwissen für da-

tenverarbeitende Systeme, deren Pipelines und Datennutzungsszenarien, bestenfalls bei unterschiedlichsten Experten innerhalb des Unternehmens. Um diese Mammutaufgabe dennoch zu bewältigen und somit die Einhaltung der Regulatorik gewährleisten zu können, betrauen Unternehmen interne oder externe qualifizierte Datenschutzbeauftragte (DSB). Als unabhängige Kontrollinstanz und Berater analysieren sie Prozesse, bewerten Risiken und sprechen Handlungsempfehlungen aus. Im Idealfall münden diese Empfehlungen in gezielten Maßnahmen, welche durch das Unternehmen umgesetzt werden. Allerdings beruht dieses kontinuierliche Vorgehen zur Wahrung der DSGVO auf der Annahme, dass Unternehmen grundsätzlich wissen, wo und wie ihre sensiblen Daten gespeichert und prozessiert werden – eine Annahme mit wenig Tragkraft in der Praxis. Ein Indiz dafür ist der steigende Trend für die sogenannte Shadow-IT, also jene IT-Systeme innerhalb oder außerhalb eines Unternehmens, über die Entscheider keinerlei Kenntnis haben. Waren es im Jahr 2022 noch rund 41 Prozent der Mitarbeiter, welche solche Technologien nutzen, liegt nach Prognosen der Anteil bei 75 Prozent für das Jahr 2027 [4].

Effizienter Datenschutz durch KI

Bedingt durch diese unvollständige Informationslage und weiteren praktischen Unzulänglichkeiten sind DSBs häufig nicht in der Lage, genau die Empfehlungen auszusprechen, welche für das Unternehmen gerade notwendig sind. An dieser Stelle ergänzt ein datengetriebener Ansatz den kontinuierlichen Prozess des Datenschutzes wertbringend. Mittels Technologie basierend auf Künstlicher Intelligenz (KI) lassen sich Modelle auf bekannten Datenquellen unternehmensspezifisch trainieren, um nicht inventarisierte sensible Daten systematisch und präzise ausfindig zu machen. Dadurch werden manuelle Aufwände seitens der Experten und interne Audits auf ein Minimum reduziert. Dies schafft nicht nur eine umfassende Transparenz über sämtliche Systeme und Datenflüsse, sondern bildet auch die Grundlage für zielgerichtete Maßnahmen und deren engmaschige Überprüfung hin zu einer effizienten Datenschutzberatung.

www.infodas.de

Verweise:
[1] R. Wintergerst, „Wirtschaftsschutz 2024," Bitkom e.V., Berlin, 2024.
[2] Europäische Union, „Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG," 2016.
[3] IBM, „Bericht über die Kosten einer Datenschutzverletzung 2024," IBM Corporation, 2024.
[4] Gartner, „Gartner Unveils Top Eight Cybersecurity Predictions for 2023-2024," 28. März 2023. [Online]. Available: https://www.gartner.com/en/newsroom/press-releases/2023-03-28-gartner-unveils-top-8-cybersecurity-predictions-for-2023-2024.

Cyberresilienz

WER RASTET, DER RISKIERT

Es gibt viele gute Gründe für Unternehmen, ihre Cyberresilienz zu erhöhen. Darauf zu warten, bis Regulierungen wie die NIS2-Richtlinie in nationales Recht umgesetzt sind und sie dazu zwingen, ist dabei nicht ratsam. Vielmehr sollte der eigene Selbsterhaltungstrieb Grund genug sein. Denn ein erfolgreicher Cyberangriff kann katastrophale Folgen haben: Produktionsausfälle, Datenverluste, Reputationsschäden und hohe Kosten.

Cyberresilienz ist geschäftskritisch

Wer nicht darauf vorbereitet ist, sein Geschäft auch im Fall von Angriffen oder Beeinträchtigungen seiner Systeme weiterführen oder schnell wiederaufnehmen zu können, riskiert im Ernstfall die eigene Existenz. Besonders KRITIS-Unternehmen stehen im Visier von (hybriden) Attacken, da sie essenzielle Versorgungsleistungen sicherstellen. Doch auch außerhalb dieser Kategorie sind Organisationen nicht sicher.

Wenn beispielsweise ein Unterseekabel für Strom oder Datenverkehr beschädigt wird, wie in den letzten Monaten mehrfach geschehen, wirkt sich dies nicht nur auf die Eigentümer und Betreiber der Kabel aus, sondern auch auf alle, die deren Dienste nutzen. Hinzu kommen Supply-Chain-Attacken, Ransomware und gezielte Phishing-Kampagnen, die jedes Unternehmen treffen.

Dynamische Bedrohungen erfordern dynamische Cyberresilienz

Unternehmen aller Branchen sind also gefordert, ihre Cyberresilienz zu steigern. BSI-Grundschutz und ISO27001 bieten dafür bereits eine wertvolle Grundlage. Doch allein reichen sie nicht aus, um sich wirklich resilient aufzustellen. Dynamische Bedrohungen erfordern ergänzende technische und organisatorische Maßnahmen, um proaktiv und flexibel agieren und wirklich widerstandsfähig zu sein.

#1 Resilienz beginnt mit Prävention

Prävention bringt in der Regel zwar weder Ruhm noch Ehre, ist aber ein zentraler Baustein der Cyberresilienz. Zu den grundlegenden Maßnahmen gehört hier ein strukturiertes Schwachstellenmanagement. Durch regelmäßige Scans, automatisierte Alerts und standardisierte Prozesse können Sicherheitslücken frühzeitig erkannt und schnellstmöglich geschlossen werden.

Ebenso kontinuierlich sollten Risikoanalysen und Bedrohungsmodellierungen durchgeführt werden. So können potenzielle Angriffsvektoren identifiziert und proaktiv Schutzmaßnahmen ergriffen werden. Auch bei der Auswahl neuer Softwarelösungen sollten bereits Notfallszenarien bedacht und Risiken evaluiert werden. Unternehmen sollten zum Beispiel erwägen, sicherheits- und geschäftskritische Funktionen auf mehrere SaaS-Anbieter zu verteilen, um nicht von einzelnen, großen Anbietern abhängig zu sein.

Um die Angriffsfläche weiter zu reduzieren, empfiehlt es sich zudem, einen Zero-Trust-Ansatz zu implementieren und IT-Systeme kontinuierlich zu härten. Konkret bedeutet das zum einen, eine durchgängige Authentifizierung und Autorisierung aller Nutzer und Geräte sicherzustellen. Zum anderen sollten alle Dienste, Zugriffsrechte und sicherheitskritischen Einstellungen immer wieder kritisch überprüft und gegebenenfalls begrenzt, deaktiviert oder angepasst werden.

Nicht zuletzt sind Schulungen und die Sensibilisierung aller Mitarbeitenden essenzielle Präventivmaßnahmen, um die Cyberresilienz zu erhöhen. Regelmäßige Security Awareness-Schulungen, Trainings, realistische Phishing-Tests und simulierte Angriffe fördern das Sicherheitsbewusstsein im gesamten Unternehmen nachhaltig. IT- und Security-Fachkräfte sollten darüber hinaus spezialisierte Schulungen erhalten, um ihr Wissen über aktuelle Bedrohungen und Sicherheitsmaßnahmen zu vertiefen.

#2 Detect. React. Repeat.

Ohne Monitoring geht in der Cybersicherheit nichts. Unternehmen setzen häufig mehrere Tools ein, um Bedrohungen, Angriffe, ungewöhnliche Aktivitäten und Schwachstellen über ihre gesamte Infrastruktur hinweg zu überwachen. Daher ist ein Security Information and Event Management (SIEM) unerlässlich, in dem die Daten und Informa-

tionen aus all diesen Quellen an einem zentralen Punkt zusammenlaufen. So behalten Security Teams den Überblick und können Vorfälle nach Faktoren wie Schweregrad, Kritikalität und Eintrittswahrscheinlichkeit priorisieren.

Tritt ein kritischer Vorfall ein, ist Schnelligkeit gefragt, um Schäden zu minimieren. Dazu sollten bereits Notfallpläne mit strukturierten Incident-Response-Prozessen vorhanden sein. Sofort muss klar sein, wer was zu tun hat. Eine integrierte Security Orchestration, Automation and Response (SOAR)-Lösung hilft dabei, Vorfälle automatisch zu eskalieren und unverzüglich Incident-Response-Prozesse zu aktivieren. Diese Prozesse sollten regelmäßig trainiert, überprüft und angepasst werden, damit Security Teams eingespielt sind und schnellstmöglich wirkungsvolle Maßnahmen ergreifen können.

Ein oft unterschätztes Mittel, um die Cyberresilienz zu erhöhen, ist das, was nach einem Vorfall geschehen sollte: Post Incident Reviews. Jeder Vorfall bietet potenziell wertvolles Lehrmaterial, um sich auf künftige Vorfälle besser vorzubereiten. Neben forensischen Analysen, um einen Vorfall technisch zu untersuchen, gehört dazu auch zu evaluieren, ob und an welchen Stellen Incident-Response-Prozesse nachgebessert werden müssen.

#3 Strg+S: Backups als Shortcut zur Cyberresilienz

Wahrscheinlich hat es jeder schon mal erlebt: Stundenlang hat man an einem Dokument gearbeitet, nicht zwischengespeichert, der Computer stürzt ab und man muss von vorne anfangen. Bei Sicherheitsvorfällen ist fehlende Datensicherung nicht nur ein kleines Ärgernis, sondern kann Schäden in ungeahnter Höhe verursachen.

Dennoch vernachlässigen viele Unternehmen diesen Bereich. Das hat beispielsweise der CrowdStrike-Vorfall im vergangenen Jahr eindrücklich offengelegt, wie unsere Umfrage „OTRS Spotlight: Corporate Security 2024" ergab. Nur 32 Prozent der betroffenen Unternehmen konnten auf robuste Rollback-Mechanismen, Disaster Recovery und Backups zurückgreifen, um ihre Systeme schnell wieder auf eine stabile Version zurückzusetzen.

Der Nachholbedarf ist also entsprechend groß. Da IT-Umgebungen immer komplexer werden, sind eine durchdachte und lückenlose Backup-Strategie und Wiederherstellungspläne notwendig. Wichtige Bestandteile sind dabei nicht nur Datensicherungen in On-Premises-, Cloud- und SaaS-Umgebungen. Unternehmen sollten darüber hinaus auch unabhängige „Schatten"-IT wie zum Beispiel isolierte Notebooks außerhalb des Netzwerks und alternative Kommunikationsmöglichkeiten vorbereiten. Notwendige Informationen wie den Notfallplan selbst sollten sie redundant, offline und extern vorhalten.

Ohne ständige Verbesserung bleibt Cyberresilienz ein Strohfeuer

Die Bedrohungslandschaft ändert und verschärft sich stetig. Um sicherzustellen, dass die Vorkehrungen alle notwendigen Bereiche abdecken und damit der Geschäftsbetrieb im Ernstfall aufrechterhalten oder wiederhergestellt werden kann, müssen sämtliche Maßnahmen regelmäßig überprüft, getestet und trainiert werden. Wer seine Cyberresilienz nicht kontinuierlich überwacht und nachbessert, spielt mit dem Feuer – und riskiert, dass ein einzelner Vorfall das gesamte Unternehmen ins Wanken bringt.

Jens Bothe | www.otrs.com

NACH DEM CROWDSTRIKE-VORFALL HABEN 93% DER BEFRAGTEN UNTERNEHMEN IHRE SICHERHEITSVORKEHRUNGEN ERHÖHT

36%

Immerhin etwas mehr als ein Drittel der Unternehmen hat den CrowdStrike-Vorfall zum Anlass genommen, sich in Sachen Backup und Disaster Recovery besser aufzustellen.

Quelle: OTRS Spotlight: Corporate Security 2024

- **45%** haben ihre IT- und Software-Landschaft diversifiziert, um weniger abhängig von einzelnen Software-Anbietern zu sein.
- **40%** haben erweiterte Echtzeit-Überwachungs-und Warnsysteme eingeführt.
- **39%** haben zusätzliche Tests für neue Patches und Updates eingeführt.
- **39%** haben einen Incident Response Plan eingeführt oder ihren bestehenden aktualisiert.
- **36%** haben Disaster Recovery und Backup-Pläne implementiert oder bestehende aktualisiert.
- **26%** sind zu stufen-/phasenweisen Rollouts von Patches und Updates übergegangen.
- **24%** haben Unified Endpoint Management (UEM) eingeführt.
- **17%** haben automatische Updates für all ihre Software deaktiviert.
- **4%** haben keine Maßnahmen ergriffen und
- **3%** wissen es nicht.

KI: Zwischen Bedrohung und Chance

GAMECHANGER IN DER IT-SICHERHEIT

Künstliche Intelligenz (KI) verändert die Bedrohungslage in der IT-Sicherheit grundlegend – Unternehmen setzen sie zur Cyberabwehr ein, Cyberkriminelle nutzen sie, um ihre Angriffe raffinierter zu gestalten. So warnt auch das Bundesamt für Sicherheit in der Informationstechnik (BSI) davor, dass KI insbesondere Phishing- und Social-Engineering-Angriffe auf ein neues Niveau hebt und Schwachstellenausnutzung automatisiert[1]. Bestätigt wird dieser Trend auch in einer aktuellen IDC-Metastudie[2] im Auftrag von IONOS: 66 Prozent der befragten Security Professionals gaben an, dass KI die größte Bedrohung für ihre Cyberabwehr darstellt – vor Ransomware oder Social Engineering.

1 http://bit.ly/41jmPmP2
2 https://bit.ly/43gsgG4

Die neue Dimension der Bedrohung

Ist diese Sorge berechtigt? KI bietet den Cyberkriminellen zwar keine völlig neuen Angriffsszenarien, potenziert aber die Wirkung bekannter Angriffe. Dabei ist besonders bedrohlich, dass die Technologie die Einstiegs- und Erfolgsschwelle für Cyberkriminelle deutlich senkt. Mussten Hacker früher über umfassende Programmierkenntnisse verfügen, können sie heute mit wenig Aufwand Malware entwickeln oder Phishing-Kampagnen in verschiedenen Sprachen erstellen.

Die Qualität der Angriffe steigt dabei kontinuierlich. Moderne KI-Systeme generieren nicht nur täuschend echte Texte, Bilder und Stimmen. Sie analysieren auch das Verhalten potenzieller Opfer und personalisieren die Attacken. Dadurch werden Desinformationskampagnen durch KI-generierte „Fake Contents" verstärkt und Botnets und Ransomware schlagen dank KI-optimiertem Code effektiver zu.

Besonders gefährlich: Die hohe Geschwindigkeit von KI-gestützten Angriffen. Was früher Wochen oder auch Monate in der Entwicklung benötigte, erstellen KI-Systeme heute in wenigen Stunden. Diese Anpassungsfähigkeit macht es den Sicherheitssystemen schwer, mit den Bedrohungen Schritt zu halten. Hinzu kommt, dass Angreifer KI dafür nutzen, Schwachstellen automatisiert zu scannen. So identifizieren sie potenzielle Angriffsziele schneller.

Deutsche Unternehmen besonders im Fokus

Auf dem deutschen Markt ist die Situation besonders komplex. Deutsche Unternehmen legen einen größeren Wert auf Datensicherheit und unterliegen strengen regulatorischen Anforderungen wie der NIS2-Richtlinie. Es fehlen jedoch entsprechende Fachkräfte.

Deutsche Unternehmen sehen vor allem darin die größten Herausforderungen, Compliance-Richtlinien einzuhalten und sensible Daten zu schützen. Erschwerend kommt hinzu, dass viele KI-Lösungen wie von OpenAI oder DeepSeek aus den USA oder China kommen. Solche Abhängigkeiten werfen auch Fragen bezüglich des Datenschutzes und der digitalen Souveränität auf.

Gerade Deutschland als Industrienation mit einem starken Mittelstand bietet eine große Angriffsfläche. Außerdem müssen die Unternehmen neben der europäischen DSGVO auch nationale Regularien erfüllen.

Eine Herausforderung: Die Konzentration von KI-Expertise außerhalb Europas. Viele Talente und Entwicklungen im KI-Bereich sitzen vor allem in den USA und China. Deutsche Unternehmen müssen daher kreative Wege finden, um ihre Sicherheitsteams gut aufzubauen und zu verstärken. Der kommende EU AI Act wird außerdem strengere Regeln für den Einsatz von KI definieren, als es sie in anderen Regionen gibt. Dies führt zu zusätzlichen Compliance-Anforderungen, welche die Entwicklung und den Einsatz von KI-Lösungen in Deutschland hemmen können.

Der zweischneidige Einsatz von KI in der Cyberabwehr

Neben all den Risiken und Herausforderungen, die der Einsatz von KI in der IT-Sicherheit mit sich bringt, bieten sich auch erhebliche Chancen. Die KI ist nicht nur ein nützliches Werkzeug für die Angreifer, sie kann auch die Verteidigung stärken. So analysieren KI-Systeme etwa in Security Operations Centers (SOCs) große Datenmengen in Echtzeit und erkennen Anomalien, die auf Angriffe hindeuten. Sie unterstützen bei der Analyse von Logfiles und helfen Spam und Desinformation zu identifizieren.

Unternehmen setzen KI bereits erfolgreich in verschiedenen Bereichen der Cyberabwehr ein. Zur Früherkennung können KI-Systeme verdächtige Muster im Netzwerkverkehr identifizieren, noch bevor ein Angriff erfolgt. In der Incident Response beschleunigen sie die Analyse von Sicherheitsvorfällen und automatisieren Routineaufgaben. In der Krisenkommunikation unterstützt KI, indem sie Anfragen effizient bearbeitet und die Teams bei der Dokumentation entlastet.

EINES IST SICHER: DER WETTLAUF ZWISCHEN ANGREIFERN UND VERTEIDIGERN WIRD SICH DURCH KI WEITER BESCHLEUNIGEN.

Dr. Jochen Haller,
Head of TechOps Information Security,
IONOS SE, www.ionos.de

Unternehmen aus dem Finanzsektor setzen zum Beispiel lieber auf individuell entwickelte KI-Modelle wie eigene Chatbots. Für sie ist wichtig, dass diese Modelle in Deutschland und der EU betrieben werden, um den rechtlichen Anforderungen zu genügen. Der Standort des Hostings spielt gerade für die Einhaltung von Compliance-Standards in der Public Cloud eine zentrale Rolle. Für eine effektive Cyberabwehr werden hier spezialisierte und integrierte KI-Lösungen benötigt, die auf etablierten Machine-Learning Netzwerken basieren und über Standardmodelle hinausgehen.

Der Einsatz von KI in der Cyberabwehr birgt aber auch Risiken. Überhöhte Erwartungen an die Technologie können ein Gefühl falscher Sicherheit hervorrufen. Dabei könnten Gefahren versehentlich unterschätzt oder gar ignoriert werden. Ein besonderes Problem besteht darin, dass KI-Systeme „halluzinieren" und dadurch falsche Ergebnisse liefern können – fatal in Bereichen, in denen scharfe Entscheidungen aufgrund exakter Informationsgrundlagen getroffen werden müssen.

Hinzu kommen die praktischen Herausforderungen, vor denen Unternehmen stehen, wenn sie KI in bestehende Sicherheitsarchitekturen integrieren. Neben der technischen Komplexität müssen auch Fragen der Verantwortlichkeit geklärt werden: Wer haftet, wenn eine KI-gestützte Entscheidung zu Schäden führt? Wie lassen sich KI-Entscheidungen nachvollziehen? Nicht zuletzt erfordert der KI-Einsatz in der Cyberabwehr auch neue Kompetenzen in den Sicherheitsteams, die oft erst erworben und aufgebaut werden müssen.

Fazit: Strategischer Ansatz erforderlich

KI wird die IT-Sicherheit weiter verändern – sowohl auf Seiten der Angreifer als auch auf Seiten der Verteidiger. Für Unternehmen bedeutet das, dass sie ihre Security-Strategien anpassen müssen. Dabei sind folgende Aspekte wichtig:

- **KI-Kompetenz im Unternehmen aufbauen:** Dies betrifft alle Mitarbeitenden, insbesondere das Security Team und gegebenenfalls spezielle KI-Funktionen.
- **Dedizierte KI-Rollen schaffen:** KI erfordert angepasste Jobprofile, beispielsweise Prompt Engineers.
- **„Have a security strategy":** Klare Sicherheitsstrategie entwickeln und gezielt um KI-Elemente erweitern.

Eine zentrale Rolle dabei können verlässliche Partner wie IONOS spielen, die nicht nur technische Lösungen mit sich bringen, sondern auch die nötige Expertise in Fragen der Compliance und digitalen Souveränität. Und eines ist sicher: Der Wettlauf zwischen Angreifern und Verteidigern wird sich durch KI weiter beschleunigen. Gewappnet sind die Unternehmen, die sich strategisch und technologisch darauf vorbereiten.

Dr. Jochen Haller

IMPRESSUM

Herausgeber: Ulrich Parthier (08104-6494-14)

Geschäftsführer: Ulrich Parthier, Vasiliki Miridakis

Chefredaktion: Silvia Parthier (-26)

Redaktion: Carina Mitzschke
(nur per Mail erreichbar)

Redaktionsassistenz und Sonderdrucke: Eva Neff (-15)

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

Autoren:
Kathrin Beckert-Plewka, Jens Bothe, Sam Flaster, Fabian Glöser, Dr. Jochen Haller, Gisa Kimmerle, Vincenz Klemm, Lukas Lebahn, Martin Mangold, Andrea Michalczyk-Schröder, Carina Mitzschke, Andreas Müller, Silvia Parthier, Ulrich Parthier, Ben Schmidt, Stephan Schweizer, Stephanie Ta, Michael Veit, Dirk Wahlefeld

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.

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

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

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

Erscheinungsweise: 6 x pro Jahr

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

Bankverbindung:
VRB München Land eG,
IBAN: DE90 7016 6486 0002 5237 52,
BIC: GENODEF10HC

Beteiligungsverhältnisse nach § 8, Absatz 3 des Gesetzes über die Presse vom 8.10.1949: 100 % des Gesellschafterkapitals hält Ulrich Parthier, Sauerlach.

Abonnementservice: Eva Neff,
Telefon: 08104-6494-15, E-Mail: neff@it-verlag.de

Das Abonnement ist beim Verlag mit einer dreimonatigen Kündigungsfrist zum Ende des Bezugszeitraumes kündbar. Sollte die Zeitschrift aus Gründen, die nicht vom Verlag zu vertreten sind, nicht geliefert werden können, besteht kein Anspruch auf Nachlieferung oder Erstattung vorausbezahlter Beträge.

CYBERATTACKEN IM KEIM ERSTICKT

In einer Welt voller Cyber-Risiken existieren keine Regeln. Mit Full Spectrum Cyber von Beazley bleiben Versicherungsnehmer im Kampf gegen Cyberkriminalität immer einen Schritt voraus - denn eines der besten Teams der Branche hält ihnen den Rücken frei.

#GameOnCyber

Erleben Sie unser
Cyber-Ökosystem auf beazley.de

beazley

Insurance. Just different.