it management

Der Motor für Innovation
Januar/Februar 2025

INKLUSIVE 48 SEITEN
it security

OFFICE 4.0 GEHT AUCH ON-PREM

Günstig, nachhaltig und sicher

Björn Orth, Vendosoft GmbH

PROCESS MINING FÜR UNTERNEHMEN

Anforderungen und Softwarelösungen

DIGITALE TRANSFORMATION

Mut zur Innovation jenseits der Technologie

KÜNSTLICHE INTELLIGENZ MIT SYSTEM

Datenmanagement als Schlüssel

www.it-daily.net

GITEX EUROPE Berlin | GITEX GREEN IMPACT | SMEDEX SME Digital Economy Expo | AI EVERYTHING EUROPE | NORTH STAR EUROPE

21 - 23 MAY 2025 | MESSE BERLIN GERMANY

CREATING NEW DIGITAL BUSINESS OPPORTUNITIES IN BERLIN

Europe's #1 Most Dynamic Tech & Startup Metropolis

2,500+ EXHIBITORS

1,500+ STARTUPS

1,000+ INVESTORS

100+ COUNTRIES

SCAN TO GET INVOLVED

ENDORSED BY

Senate Department for Economics, Energy and Public Enterprises | BERLIN

SUPPORTED BY

BERLIN

BERLIN PARTNER for Business and Technology

2025 – DAS JAHR DER...?

LIEBE LESERINNEN UND LESER,

Ja, ich weiß schon, was Sie denken: „Nicht schon wieder ein Jahr mit KI-Dauerbeschallung!" Künstliche Intelligenz ist wie das Koffein in unserem morgendlichen Kaffee – manchmal zu viel, aber wir kommen nicht mehr ohne aus. So sehr wir auch die Augen verdrehen, wenn wieder jemand „KI-gestützt" in seine PowerPoint-Folien schreibt, wir kommen um das Thema nicht herum.

Die große Frage lautet: Welchen speziellen Stempel drücken wir diesem Jahr auf? Sprechen wir von „Das Jahr der KI-Governance"? Schließlich werden unsere KI-Systeme allmählich erwachsen und brauchen Struktur. Allerdings konkurriert die Governance direkt mit den „KI-Agenten", die uns ohne unser Zutun assistieren sollen.

Natürlich ist 2025 auch das Jahr, in dem Ransomware „noch gefährlicher" wird, wie jedes Jahr seit 1989. Aber das ist nun mal die Realität. Denn das Katz-und-Maus-Spiel wird sicherlich erneut die Security-Schlagzeilen beherrschen und leider auch auf beiden Seiten von KI begleitet werden.

Kein Wunder, dass immer mehr Unternehmen auf Managed Service Provider setzen, sozusagen IT-Wellness mit 24/7-Rundum-Sorglos-Paket. Warum selbst graue Haare bekommen, wenn es dafür Experten gibt?

Wir könnten die Liste endlos weiterführen. Also, welchen Titel geben wir 2025? Vielleicht wird es einfach „Das Jahr des Jonglierens", denn genau das werden wir tun: All diese Bälle in der Luft halten, egal ob mit KI-Power oder ohne.

Herzlichst,

Lars Becker | Redakteur

INHALT

Farblich hervorgehobene Artikel sind von der Redaktion als besonders lesenswert empfohlen

Inklusive 48 Seiten it security

GUT ZU WISSEN

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

DRAMATISCHE SICHERHEITSLÜCKEN

FORTUNE-500-UNTERNEHMEN VERSAGEN BEI CYBERSICHERHEIT

Eine aktuelle Analyse des Cybernews Business Digital Index offenbart gravierende Sicherheitsmängel bei den größten US-Unternehmen. Besonders alarmierend: 43 Prozent fielen komplett durch und erhielten ein „F".

Die Forscher untersuchten 466 der Fortune-500-Unternehmen anhand von sieben Schlüsselkriterien, darunter Software-Patching, Webanwendungssicherheit, E-Mail-Sicherheit und SSL-Konfiguration. Dabei stießen sie auf insgesamt 671 kritische oder hochriskante Schwachstellen, die von Angreifern zur Kompromittierung von Netzwerken ausgenutzt werden könnten.

Finanzsektor besonders gefährdet

Ausgerechnet der Finanz- und Versicherungssektor, der mit 102 Unternehmen die größte Gruppe stellt, schnitt besonders schlecht ab. Nur ein Prozent der Finanzunternehmen erreichte ein „A" in der Bewertung. 63 Prozent erhielten ein „D" und weitere 24 Prozent ein „F". Der Durchschnittswert lag bei 71 von 100 möglichen Punkten.

Kritische Infrastruktur mangelhaft geschützt

Auch in kritischen Bereichen wie Energie und Rohstoffe zeigen sich massive Defizite. 61 Prozent der analysierten Unternehmen erhielten ein „F", weitere 24 Prozent schafften gerade noch ein „D". Lediglich sieben Prozent erreichten ein „A".

Der Technologie- und IT-Sektor, von dem man eigentlich bessere Ergebnisse erwarten würde, enttäuscht ebenfalls: 75 Prozent der untersuchten Unternehmen erreichten maximal ein „D".

SSL-Konfiguration als Hauptproblem

Als häufigste Schwachstelle identifizierten die Forscher Probleme bei der SSL-Konfiguration. Allein in diesem Bereich wurden über 490 Sicherheitsmängel bei den 466 analysierten Unternehmen gefunden. Darüber hinaus dokumentierten die Forscher 254 Probleme bei der E-Mail-Sicherheit und insgesamt 480 Datenpannen.

Lars Becker

SICHERHEITSRATINGS DER FORTUNE-500-UNTERNEHMEN

6 % der Unternehmen erreichten ein Score Level A

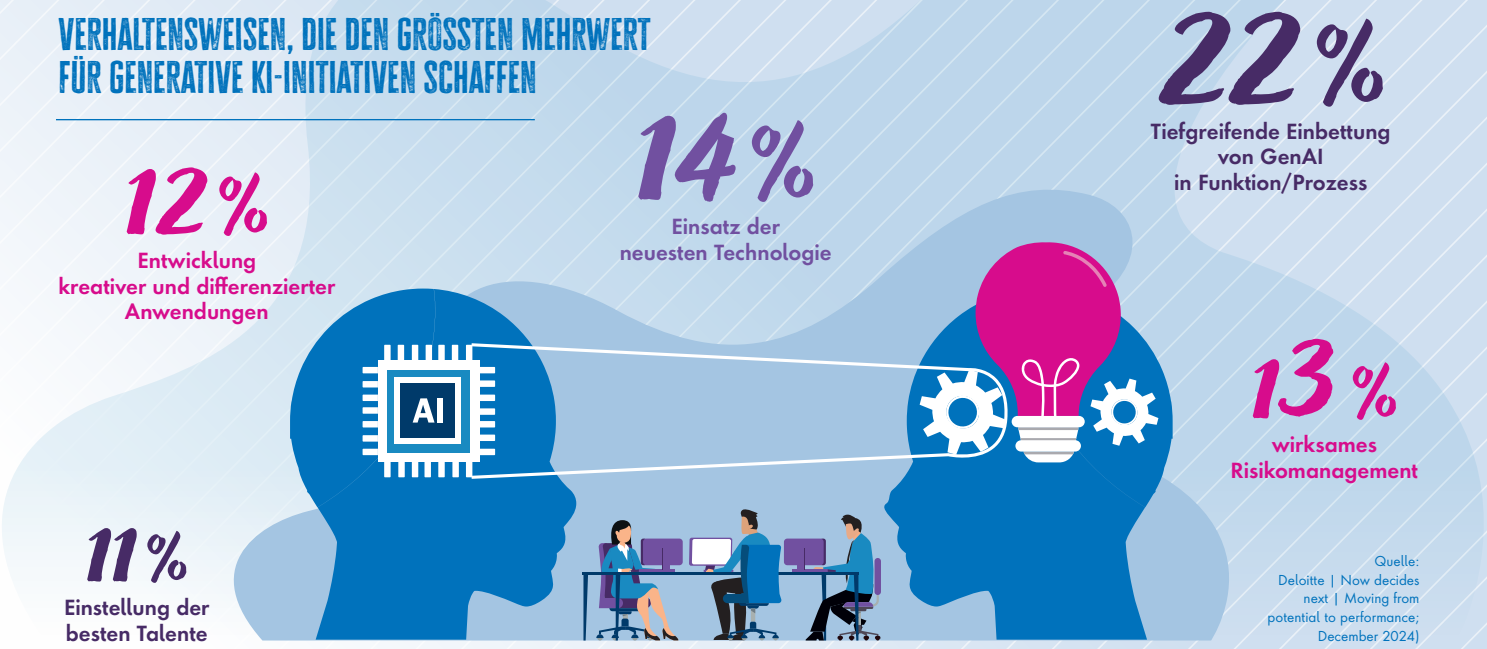
2 % erreichten Level B

8 % erreichten Level C

41 % erreichten Level D

43 % erreichten Level F

Quelle: https://cybernews.com/business-digital-index/



Künstliche Intelligenz

INNOVATION UND KUNDENBINDUNG

Die Anforderungen an Künstliche Intelligenz ändern sich messbar: Deutlich weniger Unternehmen als bisher fokussieren sich hierzulande auf reine Effizienzsteigerung durch KI. Waren es vor einem Jahr noch 67 Prozent der Befragten, sind es aktuell nur noch 45 Prozent. Auch bei den Kosteneinsparungen rechnen lediglich 29 Prozent mit signifikanten Vorteilen, vier Prozentpunkte weniger als zuvor.

Dafür soll die neue Technologie nun mehr Ideen und Erkenntnisse liefern: Für nahezu jedes dritte Unternehmen (29%) ist die Bedeutung von KI für die Förderung von Innovationen und strategischen Entscheidungen entscheidend. Das sind deutlich mehr als noch vor knapp einem Jahr (17%), und es spricht für eine Verbesserung der Innovationskultur in deutschen Unternehmen, so die jüngste Deloitte-Umfrage State of GenAI in the Enterprise (Q3), für die weltweit über 2770 (Deutschland: 150) Unternehmen befragt wurden.

Unternehmen holen bei Umsetzung stark auf

Beachtliche 23 Prozent der Unternehmen in Deutschland konnten mehr als die Hälfte ihrer Experimente mit generativer KI in die Produktion überführen, was deutlich über dem globalen Durchschnitt liegt (16%). Gleichzeitig haben 74 Prozent der Organisationen ihre Investitionen in Cloud-Lösungen erhöht, um eine solide Datenbasis für zukünftige KI-Initiativen zu schaffen. Einen Bedeutungszuwachs verzeichnete auch der Fokus auf Kundenbeziehungen, der um vier Prozentpunkte auf 23 Prozent anstieg.

Die Talentakquise gewinnt ebenfalls an Bedeutung, 35 Prozent der Befragten sehen beim Mangel an Talenten einen wesentlichen Hemmschuh für Wachstum durch KI: „Erst funktionierende Talentakquise und effektive Mitarbeiterschulung stellt sicher, dass das für den Einsatz neuer Technologien erforderliche Know-how verfügbar ist und die Fähigkeiten der KI voll ausgeschöpft werden können. Das gilt auch für die Führungskräfte: Ein umfassendes Technologieverständnis ist notwendig, um die richtigen strategischen Entscheidungen in diesem Wachstumsfeld zu treffen“, erklärt Dr. Björn Bringmann, Managing Director des Deloitte AI Institute.

Tiefe KI-Integration ist das Erfolgsrezept

Neben dem Thema Talente bleibt auch das Datenmanagement ein kritischer Bereich, hier belegen hiesige Unternehmen den vorletzten Platz unter allen Ländern: Nur 33 Prozent der Befragten halten sich hierzulande für sehr gut vorbereitet – deutlich weniger als im globalen Durchschnitt (41%).

Als Schlüsselfaktor für die Wertschöpfung gilt laut Befragung die Einbettung von Künstlicher Intelligenz in Kernprozesse, 22 Prozent der Befragten bezeichnen sie als die wichtigste Maßnahme.

www.deloitte.com/de

LICHTBLICK

DIGITALBRANCHE WÄCHST

Deutschland steuert auf das dritte Rezessionsjahr zu – die digitale Wirtschaft bleibt aber auf Wachstumskurs. Trotz des aktuell schwierigen konjunkturellen Umfelds erwartet der Digitalverband Bitkom im deutschen Markt für IT und Telekommunikation (ITK) 2025 ein Umsatzplus von 4,6 Prozent auf 232,8 Milliarden Euro. Im vergangenen Jahr hatten die ITK-Umsätze um 3,3 Prozent auf 222,6 Milliarden Euro zugelegt. Parallel entstehen in der Branche neue Arbeitsplätze. Die Zahl der Beschäftigten im ITK-Sektor soll laut Bitkom im Jahresverlauf 2025 um rund 20.000 auf 1,371 Millionen wachsen. Im Jahr 2024 sind 9.000 neue Arbeitsplätze entstanden.

KI mit rasantem Wachstum von 43 Prozent

Die Informationstechnik ist weiterhin wichtigste Wachstumstreiber. Nach der aktuellen Prognose werden in Deutschland in diesem Jahr 158,5 Milliarden Euro mit IT umgesetzt, das entspricht einem Plus von 5,9 Prozent. Vor allem das Geschäft mit Software legt nochmals stark zu (plus 9,8 Prozent auf 51,1 Milliarden Euro). Insbesondere der anhaltende Boom bei Künstlicher Intelligenz sticht hier hervor: Das Geschäft mit KI-Plattformen, auf denen KI-Anwendungen entwickelt, trainiert und betrieben werden können, wächst rasant um 43 Prozent auf 2,3 Milliarden Euro. Kollaborationstools zur Zusammenarbeit und zum mobilen Arbeiten in Unternehmen wachsen ebenfalls stark: um 12 Prozent auf 1,4 Milliarden Euro. Sicherheitssoftware steigt um 11 Prozent auf 5,1 Milliarden Euro an.

Zweistellige Wachstumsraten werden außerdem bei Cloud-Services erwartet, die um 17 Prozent auf 20 Milliarden Euro zulegen. Die Umsätze mit IT-Dienstleistungen insgesamt steigen laut Bitkom 2025 um 5,0 Prozent auf 53,8 Milliarden Euro.

Telekommunikation

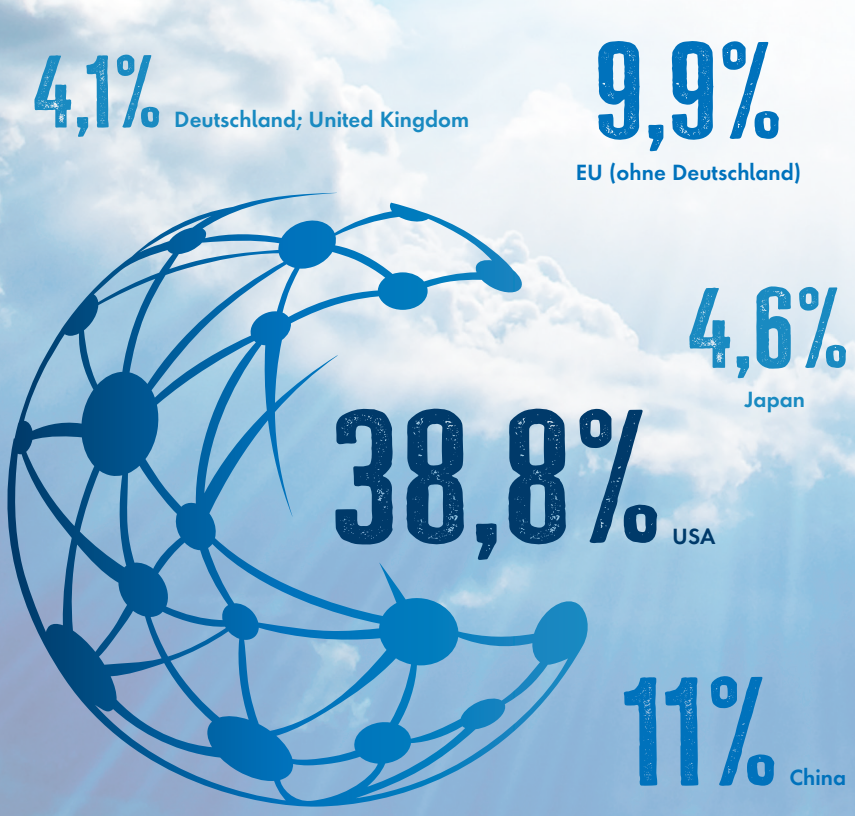
Im Markt für Telekommunikation erwartet Bitkom für 2025 ein Wachstum um 1,8 Prozent auf 74,3 Milliarden Euro. Den größten Anteil daran hat das Geschäft mit Telekommunikationsdiensten, die 53,5 Milliarden Euro ausmachen, das entspricht einem Plus von 1,4 Prozent. Die Investitionen in Telekommunikations-Infrastruktur steigen um 3,5 Prozent auf 8,0 Milliarden Euro an, die Umsätze mit Endgeräten legen mit 2,7 Prozent auf 12,8 Milliarden Euro ebenfalls zu.

Insgesamt bleiben die Investitionen der ITK-Unternehmen hoch. So wollen 17 Prozent ihre Investitionen 2025 anheben, 59 Prozent wollen sie konstant halten. 23 Prozent wollen oder müssen ihre Investitionen allerdings drosseln. Dabei fließen die Gelder vor allem in Software sowie Forschung und Entwicklung. Trotz der guten Geschäftsaussichten in diesem Jahr zeigt sich jedoch, dass nicht alle Unternehmen vom prognostizierten Marktwachstum profitieren können. Insbesondere kleinere und mittelständische Unternehmen können von dem allgemeinen Wachstum nur teilweise profitieren.

www.bitkom.org

UMSATZ MIT ITK 2025 WELTWEIT – MARKTANTEILE 2025

Deutschlands Digitalmarkt belegt im weltweiten Vergleich Rang 4



WAS TECH-ABSOLVENTEN VON ARBEITGEBERN ERWARTEN

AKTUELLE STUDIE

Sopra Steria stellt in einer aktuellen Studie die Wünsche von Hochschulabsolventen aus den Bereichen Ingenieurwesen, IT und MINT in Europa und Indien vor. Die Untersuchung zeigt: Es besteht beim IT-Nachwuchs ein großes Interesse an neuesten Technologien.

www.soprasteria.de

WAS SIND DIE DREI WICHTIGSTEN KRITERIEN BEI DER WAHL EINES ARBEITSPLATZES?

52% Vergütung

47% Work-Life-Balance

36% Arbeitsumfeld

WAS SIND DIE SPANNENDSTEN TECHNOLOGIEN FÜR DEUTSCHE ABSOLVENTEN?

58% Quantencomputing

58% Green IT

51% Cloud Computing

Office 4.0 geht auch on-prem

GÜNSTIG, NACHHALTIG UND SICHER

Office 4.0 steht für die Digitalisierung und Modernisierung der Büroarbeit in einer vernetzten, cloudbasierten und oft ortsunabhängigen Umgebung. Auch die Microsoft-Lizenzberatung von VENDOSOFT steht für ein modernes Office 4.0 – nur muss das laut Geschäftsführer Björn Orth nicht teuer sein. Im Gespräch mit Ulrich Parthier, Herausgeber it management, erzählt er, wie Unternehmen auch ohne Microsoft Online-Dienste effizient arbeiten, viel Geld sparen und sogar „ein bisschen die Welt retten" können.

? **Ulrich Parthier:** *Mögen Sie kurz erklären, worauf sich VENDOSOFT spezialisiert hat?*

Björn Orth: Natürlich gern. Unternehmen erleben seit geraumer Zeit, dass sie in eine Cloud gedrängt werden, die Jahr um Jahr teurer wird. Das muss nicht sein und das beweisen wir mit unserer Herangehensweise. Wir lizenzieren Unternehmen mit Microsoft-Produkten. Auch mit M365, vor allem aber in hybriden Cloud-Modellen mit gebrauchter Software. Oder ausschließlich mit gebrauchter Software. Damit sparen unsere Kunden enorme Beträge bei der IT-Beschaffung.

? **Ulrich Parthier:** *Im Zuge der Digitalisierung wechseln Unternehmen eher auf reine Cloud-Lösungen.Wie passt da gebrauchte Software ins Bild?*

Björn Orth: Sehr gut sogar. Wir verfolgen den Ansatz, dass nicht alle Anwendungen in die Cloud müssen und nicht alle Daten in die Cloud gehören. Denn die schafft zunächst einmal Abhängigkeiten. Das haben 25 Prozent Preissteigerung in den letzten beiden Jahren gezeigt. Gleichzeitig offenbaren Security Reports, dass die Microsoft Cloud nicht die Datensicherheit bietet, die man ihr zuschreibt. Wenn ich mir das als Unternehmen anschaue, stelle ich also fest: M365 wird immer teurer und ist das Einfallstor Nr. 1 für Cyberattacken. Wenn man sich dann noch die Flexibilität der Cloud-Dienste ansieht, zeigt sich: Die wurde durch teure Monatsverträge immer weiter beschnitten. Und seit TEAMS nicht mehr in jedem Plan enthalten ist, leistet eine gebrauchte Office-Version dasselbe wie O365, kostet aber nur die Hälfte oder weniger! Unsere Beratung zielt deshalb auf diese Formel ab: So wenig Cloud wie nötig und so viel Gebrauchtsoftware wie möglich. Damit bekommen Unternehmen die perfekte Lizenzierung zum günstigsten Preis. Mit Kauf statt Miete schaffen sie gleichzeitig Vermögenswerte, die sich zu einem späteren Zeitpunkt durch Verkauf an uns wieder monetarisieren lassen.

? **Ulrich Parthier:** *Wie alt sind die von Ihnen gehandelten Lizenzen und wie günstig ist ‚günstig'?*

Björn Orth: Wir kaufen gerade die ersten Office 2024 und Windows Server 2025 an. Im Wiederverkauf – also als gebrauchte Software – können wir beide etwa 20 bis 30 Prozent unter Neupreis anbieten. Mit älteren Versionen wie Office 2021, für die der Support im nächsten Jahr endet, sparen Unternehmen derzeit 70 bis 80 Prozent an Kosten ein.

> OFFICE 4.0 MUSS KEINE HOHEN IT-BUDGETS VERSCHLINGEN. JEDENFALLS NICHT FÜR MICROSOFT-LIZENZEN.
>
> **Björn Orth, Geschäftsführer, VENDOSOFT GmbH, www.vendosoft.de**

Ulrich Parthier: *Mich würde interessieren: Wer geht in die Cloud und wer bevorzugt on-premises?*

Björn Orth: Es gibt kein archetypisches Unternehmen, für das nur das eine oder nur das andere passt. Manche Anwender arbeiten remote und müssen auf dem neuesten Stand der Microsoft-Technik sein. Die profitieren von Tools wie TEAMS oder Copilot. Der meist größere Teil einer Belegschaft ist mit gebrauchten Lizenzen bestens ausgestattet. Ist das der Fall, empfehlen wir einen ‚hybriden Mix'. Damit spart ein Unternehmen im Vergleich zur reinen Cloud schnell 30 bis 40 Prozent. Jährlich. Darüber sollte jeder CIO nachdenken!

Aber natürlich gibt es Unternehmen, die zieht es komplett in die Cloud (wie den John-Deere-Fachhändler LVA Landtechnik). Andere nicht: etwa im Gesundheitswesen, bei Behörden oder produzierenden Betrieben (wie dem Anlagenbauer KIESELMANN). Ob cloud-only, cloudless oder hybrides Lizenzmodell – die Entscheidung hängt in der Regel von den Faktoren Kosten, Datenhoheit und Nachhaltigkeit ab.

Ulrich Parthier: *Inwiefern spielt denn Nachhaltigkeit bei der Software-Auswahl eine Rolle?*

Björn Orth: Bei der Entscheidung Cloud versus On-Premises (und dann gebraucht) spielen im Wesentlichen drei Nachhaltigkeitsaspekte eine Rolle: Wer nicht mehr benötigte Lizenzen an uns verkauft, stellt sie dem Gebrauchtsoftware-Markt zur Verfügung. Dort ist hochwertige Technologie günstig erhältlich und keine Frage von Kapital. Das dient dem UN-Nachhaltigkeitsziel „Weniger Ungleichheiten." Zweitens setzen Einsparungen durch günstige Software-Beschaffung Mittel für nachhaltige Projekte frei.

Und bei dem UN-Ziel „Nachhaltiger Konsum und Produktion" macht sich gebrauchte Software indirekt bemerkbar: Wer auf die neuesten Upgrades verzichtet und Lizenzen bis zu ihrem Support-Ende einsetzt, verlängert die Nutzungsdauer der Hardware, auf der sie laufen. Softwarebedingte Obsoleszenz heißt das im Fachjargon. Dieser Impact ist gewaltig! In einem Computer werden hunderte Rohstoffe verbaut. Produziert wird, wo Menschenrechte, soziale und ökologische Standards am niedrigsten sind. Da kann man sich die Schäden ausmalen, die jeder neue PC, Laptop oder Server verursacht. Dafür möchten wir IT-Verantwortliche sensibilisieren und haben der neuen VENDOSOFT-Broschüre auch deshalb den Titel gegeben: „Wie man Software ein zweites Leben schenkt und nebenbei ein bisschen die Welt rettet."

Ulrich Parthier: *Großartig! Herr Orth, ich danke Ihnen für dieses Gespräch.*

CLOUD-ONLY-LIZENZIERUNG MIT VENDOSOFT – ABER GÜNSTIG

Beim John-Deere-Händler LVA Landtechnik kommt die gesamte Palette der Microsoft-Cloud-Dienste zum Einsatz, um Werkshallen, Logistik- und Schulungszentrum, Verkaufs- und Service Points optimal anzubinden. Bis Februar 2022 bezog das Unternehmen noch M365-Abos von unterschiedlichen Dienstleistern. Das wollte man ändern und schrieb ein Komplettangebot aus. VENDOSOFT punktete mit den besten Konditionen, Online-Bestell-Portal und der Möglichkeit zur monatlichen Abrechnung trotz Jahresverträgen. Vor allem aber damit, dass der zuständige Microsoft Licensing Consultant unterschiedliche Szenarien und Kostenmodelle durchrechnete. Damit konnte jeder einzelne Mitarbeitende mit dem exakt passenden Online-Plan lizenziert werden – zum jeweils günstigsten Preis.

Mehr dazu über den QR-Code.

CLOUDLESS-LIZENZIERUNG MIT VENDOSOFT – 245.000 EURO GESPART

Der deutsche Anlagenbauer KIESELMANN zählt zu den führenden Herstellern von Fluidtechnik mit weltweitem Export. Rund 350 PCs stattete VENDOSOFT hier mit Gebrauchtsoftware aus: Mit Office, Project und Visio 2016 und 2019, die noch bis Oktober 2025 supported werden. Mit Windows Servern und Core CAL sowie SQL und Exchange Servern, die gebraucht besonders hohe Einsparungen bringen. Bei jeder Umstellung auf neuere Versionen wird darauf geachtet, die Software möglichst lange nutzen zu können. Die aktuellste Version kommt nie in Frage, ebenso wenig die Microsoft Cloud. Eine Strategie, mit der KIESELMANN bereits über 245.000 Euro an Lizenzkosten einsparte.

Mehr dazu über den QR-Code.

Business Kommunikation

FÜNF TRENDS, DIE DAS JAHR 2025 PRÄGEN WERDEN

2025 dürfen Unternehmen sich in Sachen Business-Kommunikation auf große Herausforderungen einstellen. Der Fachkräftemangel hält unvermindert an, der Kostendruck steigt, Compliance-Anforderungen werden mehr und komplizierter und Cyberangriffe gehen mit immer raffinierteren Methoden vonstatten, sodass die Bedrohungslage weiterwächst. Unternehmen müssen daher klug in ihre IT-Strategie investieren. Die digitale Transformation eröffnet immense Chancen, die Herausforderungen zu meistern und die geschäftskritische Kommunikation sicher und effektiv zu gestalten.

Fünf zentrale Trends werden im kommenden Jahr die Business-Kommunikation maßgeblich prägen: von der verstärkten Automatisierung und einem gezielten Einsatz künstlicher Intelligenz bis hin zu Lösungen für hybride Cloud-Welten, umfassenden Sicherheitsstrategien und der Umsetzung komplexer regulatorischer Vorgaben. Retarus beleuchtet diese Schlüsseltrends und zeigt praxisnahe Ansätze, wie Unternehmen nicht nur Effizienz und Sicherheit steigern, sondern auch die Grundlage für langfristige Wettbewerbsfähigkeit schaffen können.

#1 Automatisierung

In der aktuellen wirtschaftlichen Lage stehen Unternehmen unter immensem Kosten- und damit einhergehenden Effizienzdruck. Gleichzeitig verschärft der Fachkräftemangel die Situation: Allein 2024 verlor die deutsche Wirtschaft Produktionskapazitäten im Wert von 49 Milliarden Euro, wie das Institut der deutschen Wirtschaft ermittelte. Eine Automatisierung von Arbeitsabläufen ist daher unverzichtbar.

Innovative Produkte fördern gezielt die Digitalisierung und Automatisierung, um schlankere und effizientere Prozesse zu ermöglichen. Dazu zählen Lösungen, die sämtliche Integrationsszenarien entlang der Supply Chain – dem Kern jedes Unternehmens – umsetzen. Darüber hinaus ermöglicht ein ungebrochener Trend zu Cloud-Technologien und standardisierten Schnittstellen (APIs) einen effizienteren Betrieb moderner Kommunikationslösungen. Dazu gehört die Migration zu Cloud-basierten Kommunikationslösungen ebenso wie die automatisierte Erfassung unstrukturierter Daten und ihre Umwandlung in strukturierte Daten unabhängig davon, ob sie per E-Mail, Fax, oder PDF eingehen. Diese Ansätze senken Kosten nachhaltig und stärken die Wettbewerbsfähigkeit.

MODERNE LÖSUNGEN FÜR DIE DIGITALE GESCHÄFTSKOMMUNIKATION BIETEN TRANSPARENZ, KONTROLLE UND COMPLIANCE AUF HÖCHSTEM NIVEAU.

Yvonne Kaupp, Analyst Relations, Retarus, www.retarus.com

#2 Künstliche Intelligenz

Künstliche Intelligenz (KI) spielt eine zentrale Rolle in der digitalen Transformation. Doch angesichts der Vielzahl verfügbarer KI-Lösungen herrscht oft Unsicherheit darüber, ob und in welchen Bereichen der Einsatz tatsächlich sinnvoll ist. Unternehmen sollten bei der Auswahl einer KI-Lösung für die Geschäftskommunikation daher stets den konkreten Anwendungsfall im Blick behalten. Der Einsatz von KI ist nur dort sinnvoll, wo sie messbaren Mehrwert schafft.

Ein Beispiel ist die Dokumentenverarbeitung: Multimodale KI-Lösungen für Intelligent Document Processing ermöglichen eine effiziente Bearbeitung geschäftskritischer Dokumente wie Bestellungen, Auftragsbestätigungen, Rechnungen und Lieferscheine. Technologien wie Deep Learning, Natural Language Processing (NLP) und Computer Vision sorgen dabei für eine präzise und leistungsstarke Automatisierung mit überdurchschnittlichen Ergebnissen.

#3 Sicherheitsrisiken

Der BSI-Lagebericht 2024 zeigt, dass die Bedrohungslage im Cyberraum weiterhin angespannt bleibt. Cyberangriffe nehmen nicht nur zu, sondern werden durch den Einsatz künstlicher Intelligenz zunehmend raffinierter. Zusätzlich stellen die Professionalisierung von Cyberkriminellen und neue regulatorische Vorgaben wie der Cybersecurity Act und der Cyber Resilience Act Unternehmen zunehmend vor Herausforderungen. Unternehmen sollten daher 2025 ihr Risiko- und IT-Sicherheitsmanagement überprüfen und gegebenenfalls ausbauen – insbesondere im Bereich der geschäftskritischen Kommunikation. Sichere, transparente und Compliance-konforme Lösungen sind unverzichtbar.

Moderne Komplettlösungen für die E-Mail-Kommunikation können den beson-

deren rechtlichen und sicherheitstechnischen Anforderungen von Unternehmen gerecht werden und bieten umfassenden Schutz vor ausgefeilten Cyber-Angriffen. Gleichzeitig entlasten die so genannten Enterprise-E-Mail-Lösungen die IT-Abteilung. Leistungsstarke Analyse- und Reporting-Tools ermöglichen Administratoren einen Echtzeit-Überblick über verarbeitete Dokumente. Idealerweise kombinieren solche Lösungen umfassende E-Mail-Security mit flexiblen Verschlüsselungs- und Archivierungsoptionen. Für den Ernstfall sollte zudem eine E-Mail-Continuity-Lösung integriert sein, die eine unterbrechungsfreie Kommunikation auch bei Security-Vorfällen oder IT-Ausfällen sicherstellt.

#4 Hybride Cloud-Welten

Viele Unternehmen nutzen mittlerweile Microsoft 365 oder andere Cloud-Dienste für ihre E-Mail-Kommunikation. Die Migration global verteilter, heterogener oder teils veralteter On-Premises-Systemlandschaften in die Cloud ist jedoch oft komplex. Insbesondere hybride E-Mail-Infrastrukturen im Enterprise-Umfeld erfordern zusätzliche Add-on-Dienste, um eine sichere und zuverlässige Kommunikation sowie einen unterbrechungsfreien Geschäftsbetrieb sicherzustellen. Dadurch steigt auch der Verwaltungsaufwand für solche Systeme.

Eine leistungsstarke Lösung, die in komplexen, hybriden Infrastrukturen nahtlos funktioniert, ist daher unverzichtbar. Sie sollte alle wichtigen Mail-Kategorien wie User Traffic, transaktionale E-Mails und Marketing-Automatisierung abdecken. Gleichzeitig müssen fortschrittliche Sicherheitsfunktionen sowie effiziente Tools für Routing, Reporting und Traffic Management integriert sein. Ergänzend bieten Enterprise-Services wie Verschlüsselung und E-Mail-Archivierung einen umfassenden Schutz. Mit einer ganzheitlichen Lösung aus einer Hand profitieren Unternehmen von höchster Zuverlässigkeit, Transparenz und einer reibungslosen E-Mail-Zustellung – und garantieren so einen sicheren und effizienten E-Mail-Verkehr.

#5 Compliance-Anforderungen

Unternehmen müssen neue Technologien bewusst und verantwortungsvoll einsetzen – sowohl bei der Anwendung als auch bei strategischen Investitionen. Dies schließt die Einhaltung neuer gesetzlicher Vorgaben wie E-Invoicing, NIS2, DORA und dem Digital Services Act (DSA) ein. Diese Regularien verpflichten Unternehmen, höchste Standards in den Bereichen Sicherheit und Datenschutz zu erfüllen.

Moderne Lösungen für die digitale Geschäftskommunikation bieten Transparenz, Kontrolle und Compliance auf höchstem Niveau. Mit klar definierten Service Level Agreements (SLAs) gewährleisten sie die Einhaltung strenger Vorgaben und schaffen gleichzeitig eine stabile Grundlage für Datenschutz und Governance. Durch den Einsatz solcher Lösungen können Unternehmen nicht nur den wachsenden regulatorischen Anforderungen gerecht werden, sondern auch Vertrauen und Sicherheit im Umgang mit neuen Technologien fördern.

Yvonne Kaupp

ERP-SECURITY-TRENDS 2025

DIESE ENTWICKLUNGEN SOLLTEN SIE AUF DEM SCHIRM HABEN

ERP-Systeme sind das Rückgrat moderner Unternehmen – und zugleich ein immer beliebteres Ziel für Cyberangriffe. Auf was sollten Sie achten, um Cyberkriminellen einen Schritt voraus zu sein?

Künstliche Intelligenz

Der gigantische Hype um maschinelles Lernen (ML) und künstliche Intelligenz (KI) flaut langsam ab. Es gibt zwar echte und durchaus berechtigte Bedenken gegenüber der neuen Technologie, etwa in Bezug auf den Missbrauch durch Deepfakes, aber geschäftskritische Anwendungen sollten davon nicht betroffen sein. Solange Unternehmen in der Lage sind, Patches schnell zu implementieren, besteht kein erhöhtes Cyberrisiko für die SAP-Sicherheit aufgrund von Fortschritten in der KI-Entwicklung.

Künstliche Intelligenz spielte in diesem Jahr keine wesentliche Rolle bei den Aktivitäten von Angreifern – selbst bei hochspezialisierten Akteuren, die genau wissen, worauf sie aus sind, wie etwa Nationalstaaten. Ein Beispiel liefert der aktuelle CISA-Bericht über die am häufigsten ausgenutzten Schwachstellen. Im Jahr 2022 standen SAP und Oracle ganz oben auf der Liste. Seitdem ist jedoch die Zahl der Schwachstellen zurückgegangen. Obwohl die Bedrohungen weiter bestehen, spiegelt dieser Rückgang die Fortschritte bei der Bewältigung bekannter Risiken wider und keine erhöhte Aktivität aufgrund von KI.

Besorgniserregend bleiben SAP-Installationen mit Schwachstellen, die nicht gepatcht werden. Wenn die Sicherheit geschäftskritischer Anwendungen nicht priorisiert wird, werden Angreifer weiterhin in diese Umgebungen eindringen können, allerdings nicht durch den Einsatz von KI. Es ist unwahrscheinlich, dass sich diese Situation im Jahr 2025 ändern wird.

Verzögerungen bei der Cloud-Migration

Viele Unternehmen stehen unter dem Druck, ihre geschäftskritischen Daten in die Cloud zu migrieren, zögern dies jedoch hinaus. Sobald die Migration dringlich wird – vor allem, wenn wir uns Fristen wie der von SAP für die Umstellung auf S/4HANA in 2027 nähern – wird die Eile und Hektik bei der Umstellung zu Fehlern führen. Das können Schwachstellen sein, die im zu übertragenden Code oder in den Daten verbleiben. Diese Versäumnisse können zu kostspieligen Verzögerungen oder Nachbesserungen führen. Unternehmen, die noch mit Altsystemen arbeiten, sollten ihre Anwendungen frühzeitig modernisieren, um wettbewerbsfähig zu bleiben und sich an die Anforderungen einer zunehmend digitalen Welt anzupassen. 2025 sollte der Fokus auf Migration liegen – und zwar auf einer adäquaten, funktionsübergreifenden Planung und Umsetzung.

Neues Jahr, gleiche Schwachstellen

Während die Bedrohungslandschaft immer größer wird, bleiben die Schwachstellen, mit denen die Sicherheitsteams jedes Jahr zu kämpfen haben, mehr oder weniger dieselben. Die Absicherung von geschäftskritischen Anwendungen hat bei vielen Unternehmen noch immer keine hohe Priorität. Das führt dazu, dass alte und neue Schwachstellen ständig ausgenutzt werden, um IoT-Geräte, Firewalls und VPNs zu überwinden. Sobald Bedrohungsakteure dann in die Systeme eines Unternehmens eingedrungen sind, haben sie es auf die wertvollsten Informationen abgesehen, die in geschäftskritischen Anwendungen wie dem SAP gespeichert sind.

Bei der Erarbeitung der Geschäftsziele für 2025 müssen Führungskräfte daher prüfen, welchen Stellenwert sie der Cybersicherheit auf ihrer Prioritätenliste einräumen und wie sie Bedrohungen am besten bekämpfen können.

https://onapsis.com/de/

Der VoIP-Markt

HERAUSFORDERUNGEN UND CHANCEN FÜR PROVIDER UND SYSTEMINTEGRATOREN

Vor rund 15 Jahren dominierte die Deutsche Telekom den deutschen Festnetzmarkt, während der Voice over IP-Markt (VoIP) noch in den Kinderschuhen steckte. Traditionelle Telefonanlagen wurden um IP-Funktionen erweitert, oder moderne IP-Telefone wurden an bestehende PSTN-Anlagen angeschlossen. Etwa 95 Prozent der ersten VoIP-Migrationen wurden von Systemintegratoren durchgeführt. Mit der fortschreitenden Digitalisierung verzeichnete der IP-Telefonie-Markt ein beeindruckendes Wachstum. Treiber waren Breitbandtechnologien, Investitionen in All-IP-Infrastrukturen und der wachsende Bedarf an flexiblen Kommunikationslösungen, die Unternehmen nicht nur Kosten sparen, sondern auch die betriebliche Effizienz steigern.

Heute wird der VoIP-Markt von großen Anbietern geprägt, die meistens standardisierte Lösungen direkt an Unternehmen oder über Wiederverkäufer anbieten und unzähligen regionalen Providern.

Neue Potenziale nutzen

Das Erfolgsrezept der großen Telekommunikationsunternehmen ist die Standardisierung. „All-inclusive"-Standard-Angebote, kombiniert mit wenigen Modellen von IP-Tischtelefonen und schnurlosen IP-DECT-Lösungen, schaffen Effizienz und attraktive Margen, wozu auch die Hardware beiträgt: sie wird nicht verkauft, sondern wird – als Teil der monatlichen Gebühr – zu einer zusätzlichen Margenquelle. In dieser Konstellation sind die von Snom angebotene dreijährige Garantie und die bekannte Widerstandsfähigkeit der Telefone auch unter härtesten Einsatzbedingungen sehr willkommen. Ein solches Vertriebsmodell weist jedoch Grenzen auf: Der zunehmende Preiskampf führte zu Konsolidierungen, die die Vielfalt der Angebote einschränken könnten.

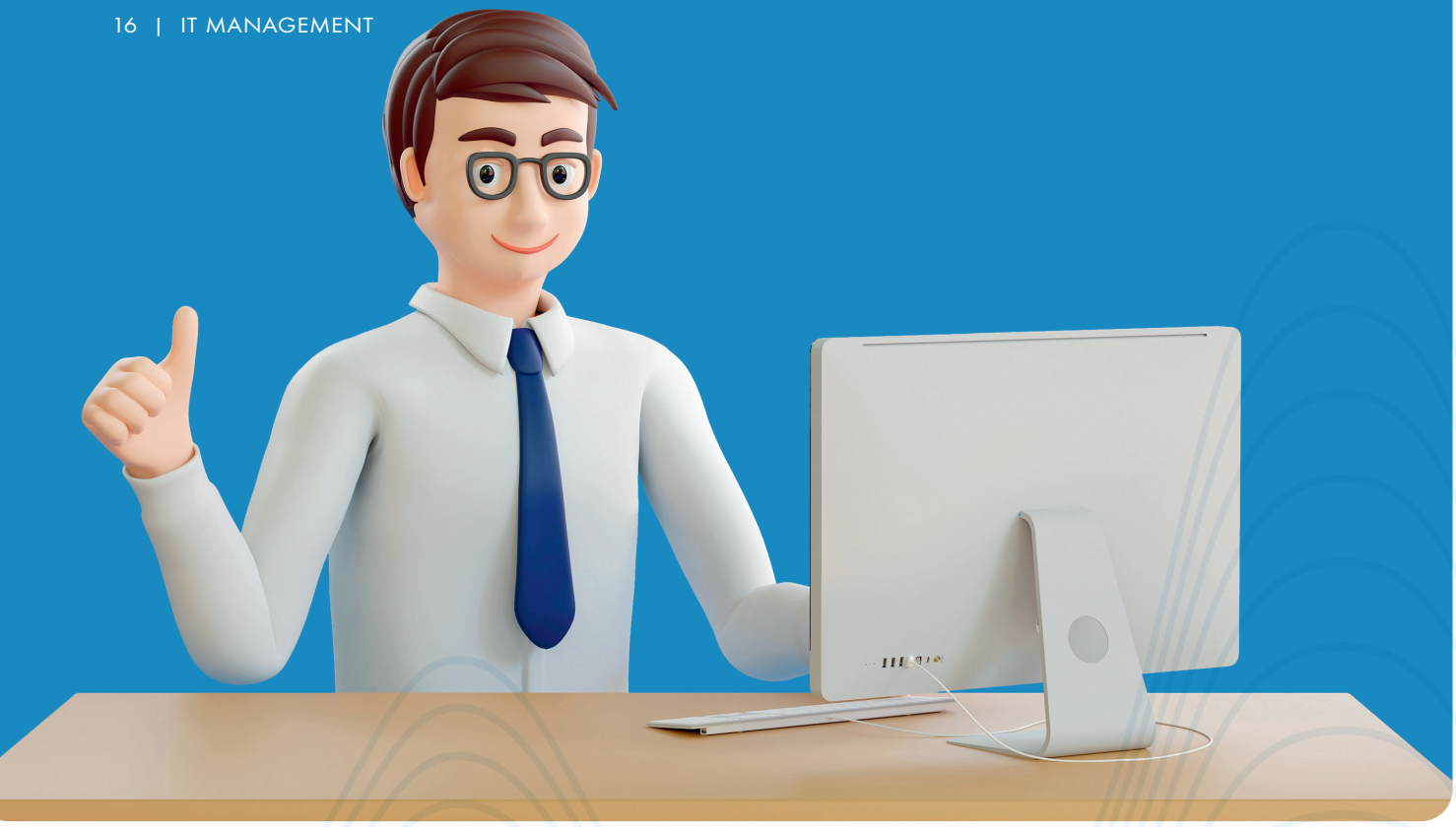
Kleinere Anbieter von VoIP-Lösungen und Systemintegratoren stehen andererseits vor der Herausforderung, sich gegen die Marktdominanz großer Anbieter zu behaupten. Ihr Erfolg hängt davon ab, neue Technologien zu integrieren, geografische Grenzen durch Partnerschaften zu überwinden und ihre Angebote auf monatliche Abrechnungsmodelle umzustellen. Innovation ist dabei der Schlüssel: Die Nutzung von Cloud-Plattformen, KI-gestützte Anrufanalysen und die Integration von Gebäudeautomation eröffnen neue Geschäftsmöglichkeiten. Durch spezialisierte Endgeräte, die in Branchen wie Industrie oder Gesundheitswesen unverzichtbar sind, können sie ein einzigartiges Portfolio mit maßgeschneiderten Lösungen wie gehosteten IP-PBX-Diensten, Cloud-Kontaktzentren und einheitlichen Kommunikationsplattformen aufbauen. Doch nicht nur: Die Zusammenarbeit mit Internet Service Providern (ISPs) könnte ebenfalls neue Potenziale eröffnen. Kombinierte Pakete aus Konnektivität und VoIP-Diensten bieten Synergien, von denen beide Seiten profitieren würden. ISPs können ihre Kundenbasis ausbauen, während VoIP-Anbieter durch Cross-Selling eine erhöhte Sichtbarkeit und den Zugang zu neuen Zielgruppen gewinnen – besonders im öffentlichen Sektor, der oft an große Betreiber gebunden ist.

Indem kleinere Anbieter auf Qualität, Vielseitigkeit und Innovation setzen, sichern sie sich also ihre Position im wachsenden VoIP-Markt und erschließen neue Geschäftsfelder.

Mark Wiegleb

INDEM KLEINERE ANBIETER AUF QUALITÄT, VIELSEITIGKEIT UND INNOVATION SETZEN, SICHERN SIE SICH ALSO IHRE POSITION IM WACHSENDEN VOIP-MARKT UND ERSCHLIESSEN NEUE GESCHÄFTSFELDER.

Mark Wiegleb, Head of Customer Success, Snom Technology GmbH, www.snom.com



Der perfekte Digital Workplace

AUTOMATION, KI, VIRTUALISIERUNG, KOSTENTRANSPARENZ UND CLOUD PERFEKT VEREINT

Was KMU aktuell an IT- und TK-Technik einsetzen, kann schnell unübersichtlich werden: Telefonie-Lösungen, Desktop-Geräte, eigene Server und Netzwerke, Cloud-Anwendungen und klassische Business-Software. Eine Vielzahl an Lizenzen, knappe Budgets und der Wunsch nach mehr Automatisierung und KI führen zu einer enormen Komplexität. Oft ist die Verwaltung dieses Digital Workplace über viele Systeme verteilt und die Abhängigkeiten untereinander gar nicht klar. Das führt immer wieder zu Fehlern, Funktionsstörungen und Sicherheitslücken. Ein Lösungsansatz: Einführung eines zentralen Management-Overlays, um die darunterliegenden Systeme zu koordinieren.

Mitarbeitende erwarten von ihren Arbeitgebern eine moderne und performante Ausstattung an IT- und Kommunikationslösungen – etwa Notebook, Smartphone, Cloudsysteme, Kollaborationsplattformen und Videotelefonie. Unternehmen haben für die Bereitstellung der Anwendungen peu à peu immer neue Systeme eingeführt. Sind es nur zwei oder drei, nehmen die Verantwortlichen die Einarbeitung noch hin. Bei zehn oder 20 Systemen ist das mehr als nur lästig: Sie verhindern Automatisierungsbestrebungen, weil die Schnittstellen das nicht erlauben. Das führt zu enorm aufwendigen On- und Off-Boarding-Prozessen, weil viele Einzelaktionen nötig sind. Gerne wird auch vergessen, Accounts ausgeschiedener Mitarbeitender abzuschalten. Die vielen Systeme machen bei Fehlern die Ursachensuche komplex und langwierig. Und sie verhindern Innovationen, weil Verantwortliche sich davor scheuen, bestehende Systeme auszutauschen. Auch der Einkauf und Support erfordern viele Ressourcen.

Die Gesamtheit aller digitalen Systeme, der Digitale Workspace, ist aber das Rückgrat aller Firmen und KMU. Wird er zu starr und unflexibel, verhindert er die notwendige Weiterentwicklung und Kostenoptimierungen. Eine digitale Transformation wie die Einführung von neuen Funktionen und Systemen wird dadurch zu einem enormen Kraftakt. In Anbetracht des wachsenden Fachkräftemangels kann das für Unternehmen sogar gefährlich werden, weil schlicht die Manpower und das Wissen fehlen, um alle Anwendungen und Systeme zukünftig zu betreuen.

Häufig kommen noch lästige Abhängigkeiten hinzu: Hat man Anwendungen in eine bestimmte Cloud ausgegliedert, ist der Wechsel zu einem anderen Cloud-Provider schwierig. Ähnlich verhält es sich mit Lizenzen für proprietäre Anbieter von Business-, Virtualisierungs- oder Datenbanklösungen. Diese bilden nicht selten einen großen Kostenblock bei den IT-Kosten.

Lösungsansätze für einen schlanken digitalen Workplace

Dieser scheinbar gordische Knoten lässt sich lösen. Ansatzpunkt ist eine Verwaltungsplattform, die sowohl Technik als auch Kosten- und Budget-Aspekte unter einer einfach zu bedienenden Oberfläche verwaltet. Dieses Frontend lässt sich flexibel erweitern und besitzt konfigurierbare Dashboards, die den jeweiligen Anwendenden die Informationen zeigen, die sie benötigen.

Das Backend sorgt für die Anbindung der verschiedenen technischen Systeme. Dazu gehören sowohl Kommunikationslösungen für Telefonie, Video-Calls, E-Mail und Chat als auch IT-Infrastruktur wie Netzwerk-Strukturen, Server, Cloud-Systeme und -Anwendungen. Aber hier sollte das Management nicht enden.

Zum IT-Management gehören auch Service & Support, Beschaffung und Life-Cycle-Management sowie die intelligente Verknüpfung von Geschäftsprozessen. Wenn das System die komplette IT im Blick hat, ist die Einhaltung von Compliance-Anforderungen und das gesetzlich vorgegebene Reporting wesentlich einfacher durchzuführen.

Wesentliche Faktoren bei der Implementierung

Bei der Wahl der richtigen „Middleware" sollten KMU auf mehrere Faktoren achten, um sich nicht in eine Lock-in-Situation zu begeben. Das System sollte über eine flexible, offene Architektur verfügen, um verschiedene Cloud-Anbieter, TK-Anlagen und Dienste anbinden zu können. Mit Hilfe der Management-Plattform lassen sich in der Folge schnell und einfach Provider wechseln, wenn sich Konditionen verändern oder der Markt neue Möglichkeiten eröffnet.

Es gilt eine Architektur zu wählen, die höchste Sicherheitsstandards einhält und die Daten auf Servern speichert, die den europäischen, deutschen oder Schweizer Vorgaben (DSGVO) entsprechen und die sich in der EU oder der Schweiz befinden.

MITARBEITENDE ERWARTEN VON IHREN ARBEITGEBERN EINE MODERNE UND PERFORMANTE AUSSTATTUNG AN IT- UND KOMMUNIKATIONSLÖSUNGEN, KOLLABORATIONSPLATTFORMEN UND VIDEOTELEFONIE.

Thierry Kramis,
Head of Seabix ICT Services,
www.seabix.com

Diese Form der Datensouveränität ist mit den großen amerikanischen Cloud-Providern häufig schwierig umzusetzen.

Vorteile einer offenen, hochintegrierten Plattform

Eine hochintegrierte Plattform vereinfacht beispielsweise das On- und Off-Boarding von Mitarbeitenden enorm. Statt die Person in diversen Systemen nacheinander manuell anlegen zu müssen, erfolgt dies auf Knopfdruck über einen Dialog im System. Schon stehen alle Lizenzen bereit, sind alle Accounts angelegt, das persönliche Notebook und Telefon eingerichtet. Das senkt den Arbeitsaufwand um viele Stunden.

Das Management aller Lizenzen erfolgt automatisiert bei der Anschaffung von neuer Hard- und Software. Die IT-Leitung kann jederzeit einsehen, welche Budgets dafür aktuell abgerufen werden.

Erst die Integration des gesamten ITK-Managements erlaubt eine hochgradige Automatisierung und damit die Nutzung von Synergieeffekten. So können KI-Agenten auch komplexe Aufgaben autonom übernehmen und Tätigkeiten ausführen. Dies war vorher Spezialisten vorbehalten, weil nur sie sich mit den einzelnen IT-Systemen auskannten. Die Automatisierung entlastet die gesuchten Fachkräfte und bindet sie besser ans Unternehmen.

Durch die einfach zu bedienende Management-Oberfläche können KMU außerdem flexibel das Service-Management der IT-Infrastruktur an einen Dienstleister delegieren oder Stück für Stück selbst übernehmen. Das wirkt einem Fachkräftemangel entgegen und kann fehlendes Fachwissen kompensieren.

Beispiel Seabix IO

Ein Beispiel für diesen hochintegrierten, aber offenen Ansatz bildet Seabix IO. Die Plattform lässt sich tief in die jeweiligen Business-Prozesse eines Unternehmens integrieren und automatisiert das Gerätemanagement inklusive der Beschaffung, Lieferung und Betrieb, also dem kompletten Lifecycle. Das System kann den digitalen Arbeitsplatz eines neuen Mitarbeitenden auf Knopfdruck bestellen und einrichten. In Seabix IO können KMU ihre ITK-Landschaft inklusive Cloud und Filesharing managen und über Server in einem Schweizer Rechenzentrum bereitstellen. Die Plattform unterstützt die IT-Verantwortlichen durch ein einfaches, effizientes und transparentes Management aller technischen Assets und Prozesse. Auch Green-IT-Strategien lassen sich damit zentral und automatisiert verfolgen.

Thierry Kramis

Von Hushed zu Real Hybrid

STRATEGIE AUF DATENBASIS

Beim „Hushed Hybrid"-Trend umgehen Teams in stiller Absprache starre Präsenzregeln fürs Büro. Doch mit der richtigen Balance aus Flexibilität und datenbasierten Insights können Unternehmen heimliche Homeoffice-Arbeit reduzieren, Ressourcen effizienter nutzen und Mitarbeitende stärker einbeziehen.

Wie strenge Regeln Hushed Hybrid fördern

In Deutschland verlangen viele Unternehmen derzeit wieder mehr Präsenzarbeit von ihren Mitarbeitenden. Teilweise wird sogar eine komplette Rückkehr ins Büro gefordert. Laut JLL Research erwarten 87 Prozent der Unternehmen zumindest eine zeitweise Büropräsenz. Ein Drittel hat sogar eine Anwesenheitspflicht eingeführt. Das gefällt nicht allen - und ist Motor für die Entwicklung neuer Strategien zum Umgang mit den unliebsamen Regeln.

Der Trend „Hushed Hybrid" ist eine davon. Dabei arbeiten Mitarbeitende mit stiller Zustimmung ihrer Führungskräfte oft mehr im Homeoffice, als die offiziellen Vorgaben erlauben. Die direkten Leader sehen diese Freiheit oft als wichtige Maßnahme, um Talenten genug Flexibilität zu bieten, damit diese nicht den Arbeitgeber wechseln. Das Problem: Unternehmen stehen vor Herausforderungen wie einem ineffizienten Ressourceneinsatz, wenn nicht klar ist, wer wann im Büro arbeitet. Büroflächen sind mitunter zu groß oder Teams arbeiten ineffizienter zusammen, wenn sie einander nicht antreffen. Hushed Hybrid birgt auf Mitarbeitendenseite zudem die Gefahr von Unzufriedenheiten, wenn herauskommt, dass einige Teams mehr Privilegien genießen als andere.

Individualität trifft Planbarkeit

Um diese komplexen Anforderungen zu bewältigen, spielt die IT eine zentrale Rolle. Denn sie bietet mit der richtigen Strategie die Basis für eine offene, transparente Kommunikation im Unternehmen über die Passgenauigkeit der Hybrid-Regeln. Das ist essenziell, damit die Bedürfnisse der Mitarbeitenden berücksichtigt werden und sie dadurch weniger geneigt sind, sich über die Vorgaben hinwegzusetzen. Wichtig dabei: Der Fokus sollte stets darauf liegen, wie die besten Ergebnisse erzielt werden können. Präsenzarbeit nur um der Präsenzarbeit willen ist keine Lösung. Eine gewisse Planbarkeit ist jedoch wichtig, damit das Management die Übersicht über die Ressourcenanforderungen behält und Mitarbeitende ihren Arbeitsort sinnvoll koordinieren können. Hier die richtige Strategie zwischen Präsenzwunsch der Führungsebene und individuellen Anforderungen der Teams zu wählen, ist eine Herausforderung, die nicht alle Unternehmen meistern.

Datenbasiert zum Win-Win

Die IT-Abteilung kann bei dieser Aufgabe unterstützen und Treiberin des passenden Arbeitsmodells sein. Mit den richtigen Technologien ermöglicht sie den Spagat zwischen Flexibilität und Planbarkeit.

Laut Konstanzer Homeoffice Studie befürchten etwa 43 Prozent der Führungskräfte und 31 Prozent der Beschäftigten ohne Führungsverantwortung schlechtere Kommunikation durch Remotearbeit.

Tools für Arbeitsmanagement, digitale Zusammenarbeit und Projektmanagement können Teams dabei helfen, ihre Arbeitsweise besser abzustimmen. Wer jedoch denkt, „viel hilft viel", liegt leider falsch. Gewählte Tools müssen stets die Unternehmensstrategie unterstützen und aktiv genutzt sowie gefördert werden, damit sie auch wirklich die Basis für mehr Flexibilität bieten. Holen die Verantwortlichen aber alles aus den Lösungen heraus, schaffen sie damit die Grundlage für zukunftsfähige Hybridstrategien.

Ein zentraler Ansatzpunkt für IT-Abteilungen im Umgang mit Hushed Hybrid ist daher die Analyse der Daten aus den eingesetzten Tools. Dazu zählen Informationen über die Auslastung von Büroflächen und die Präferenzen der Mitarbeitenden. Zudem lässt sich über die Tools feststellen, ob bestehende Hybrid-Regeln eingehalten werden. Abweichungen können digital kommuniziert und auf Wunsch bewilligt werden. Solche Auswertungen helfen dabei, hybride Arbeitsmodelle besser an die tatsächlichen Bedürfnisse anzupassen: Sind in einem Unternehmen zum Beispiel die Meetingräume stets überbelegt, zeigt dies den Bedarf nach mehr Platz für Zusammenarbeit. Bleiben viele Schreibtische ungenutzt, lassen sich Flächen reduzieren oder umgestalten.

Solche Änderungen sollten jedoch immer mit den Betroffenen abgestimmt werden, damit die Strategie nicht zu mehr Unzufriedenheit führt. Spiegelt das Büro andererseits die eigenen Bedürfnisse wider, wird es zum attraktiven Arbeitsort - ein natürliches Mittel gegen Hushed Hybrid.

Erfolgsfaktoren sichern

Damit diese Analysen zum Erfolg für beide Seiten führen, gilt es, einige Faktoren zu beachten. Denn die Nutzung von Tools und Daten kann helfen, hybride Arbeitsmodelle effizient zu gestalten, doch birgt bei falscher Umsetzung auch Risiken.

- **Systemintegration:** Damit Daten überhaupt sinnvoll erfasst werden können, müssen neue Tools nahtlos in bestehende Systeme integriert werden. IT-Abteilungen sind gefordert, Systeme zu konsolidieren und eine intuitive Benutzererfahrung zu schaffen. Lösungen sollten flexibel erweiterbar sein und sich an veränderte Anforderungen anpassen lassen. Ziel ist es, eine digitale Infrastruktur zu schaffen, die die Zusammenarbeit erleichtert und die Produktivität steigert, anstatt sie zu behindern.

- **Transparenz statt Kontrolle:** Unternehmen müssen sicherstellen, dass die Datenanalysen Transparenz fördern und nicht als Kontrollinstrument wahrgenommen werden. Dies erfordert klare Kommunikationsstrategien, die den Nutzen der Daten für alle Beteiligten nachvollziehbar machen.

ES BRAUCHT EINE KLUGE MISCHUNG AUS TECHNOLOGISCHEN TOOLS, FLEXIBILITÄT UND EINEM KLAREN FOKUS AUF DIE BEDÜRFNISSE DER MITARBEITENDEN, UM HUSHED HYBRID ERFOLGREICH ZU BEWÄLTIGEN.

Ivan Cossu, CEO & Co-Founder, deskbird, https://de.deskbird.com/

- **Offene Kommunikation:** Beim Einsatz digitaler Tools ist daher die menschliche Komponente nicht zu vernachlässigen. Führungskräfte müssen ihren Teams aktiv zuhören, um z. B. Bedenken adressieren zu können. Schulungen, sowohl zu Kommunikation und Feedback als auch dem richtigen Umgang mit digitalen Lösungen, helfen Führungskräften, Missverständnisse zu vermeiden und Vertrauen für den Umgang mit den Daten zu schaffen. Der Austausch im Team kann aber auch eine Möglichkeit sein, Wünsche anzusprechen. So lernen die Teamleads, wie die Mitarbeitenden produktiv bleiben und können Erwartungen abstimmen.

- **Datenschutz:** Mitarbeitende müssen darauf vertrauen können, dass ihre Daten anonymisiert und ausschließlich zur Verbesserung der Arbeitsbedingungen genutzt werden. IT-Abteilungen sollten hier als Vermittler agieren, die gleichsam technologische Möglichkeiten ausschöpfen und die Privatsphäre der Mitarbeitenden schützen. Transparente Richtlinien zur Datennutzung und regelmäßige Feedbackschleifen sind essenziell, um das Vertrauen in datengetriebene Ansätze zu stärken.

Hushed Hybrid datenbasiert meistern

Es zeigt sich: Starre Präsenzregeln sind in der modernen Arbeitswelt oft nicht die ideale Lösung. Stattdessen braucht es eine kluge Mischung aus technologischen Tools, Flexibilität und einem klaren Fokus auf die Bedürfnisse der Mitarbeitenden, um Hushed Hybrid erfolgreich zu bewältigen. Durch den Einsatz digitaler Lösungen können Unternehmen wertvolle Einblicke in Präferenzen und Ressourcenbedarf erhalten. Diese Informationen ermöglichen es, hybride Arbeitsmodelle passgenau zu gestalten. So wird Hushed Hybrid vom einstigen Problem zum Katalysator für zukunftsfähige Unternehmen.

Ivan Cossu

Was bleibt, was kommt!

REMOTE MANAGEMENT DER IT-INFRASTRUKTUR

Immer mehr Teams arbeiten dezentral, deshalb ist es für Unternehmen essenziell zu verstehen, wie sie am besten ihre IT-Infrastruktur remote verwalten können. Mit der richtigen Auswahl an Tools und Strategien können IT-Abteilungen Unternehmenssysteme von jedem Ort aus effektiv überwachen, Fehler beheben und so einen reibungslosen Betrieb sowie minimale Ausfallzeiten gewährleisten.

Die Fernverwaltung einer IT-Infrastruktur kann ein erhöhtes Risiko von Cyberangriffen bedeuten, insbesondere beim Zugriff auf Systeme über ungesicherte Netzwerke. Der Schutz von Verbindungen, Endpunkten und Daten vor Sicherheitsverletzungen sollte immer höchste Priorität haben. Dennoch kann es eine Herausforderung sein, eine konsistente

DAS REMOTE-MANAGEMENT EINER IT-INFRASTRUKTUR BIRGT SICHERHEITSRISIKEN, DENNOCH SIND DIE VERÄNDERTEN ARBEITSSTRUKTUREN NICHT MEHR WEGZUDENKEN.

André Schindler, General Manager EMEA/SVP Global Sales, NinjaOne, www.ninjaone.com/de

Sicherheit über alle Geräte und Standorte hinweg zu gewährleisten.

Wichtige Tools und Technologien für das IT-Remote-Management

Erfreulicherweise existieren Lösungen, die das Remote-Management erleichtern und die IT-Systeme stabil und sicher halten:

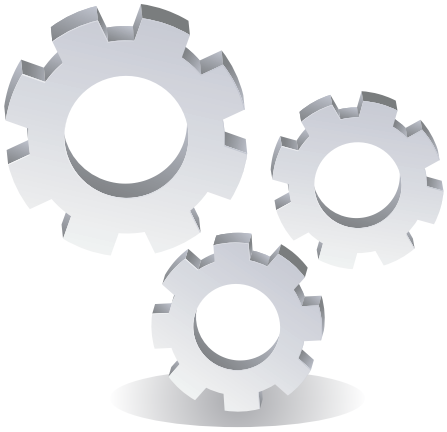
➤ **Softwarelösungen für Remote Monitoring und Management (RMM):** RMM-Tools bilden das Rückgrat der IT-Fernverwaltung. Eine RMM-Software kann Tausende von Geräten gleichzeitig überwachen, Teams über Probleme wie Systemausfälle oder Sicherheitsbedrohungen informieren sowie eine zügige Fernlösung ermöglichen. IT-Teams sollten darauf achten RMM-Tools mit integrierten Sicherheitsfunktionen wie Endpunktschutz, Netzwerküberwachung und Systemen zum Erkennen von Eindringlingen einzusetzen.

➤ **Automatisierungs-Tools:** Automatisierung erhöht die Effizienz der Fernverwaltung der IT-Infrastruktur. Die Automatisierung sich wiederholender Aufgaben wie Patching, Software-Installierung und Back-up ermöglicht es IT-Experten, sich auf übergeordnete Aktivitäten zu konzentrieren. Dies führt zu einer höheren Gesamtproduktivität durch Zeitersparnis und Standardisierung der Arbeitsabläufe, wodurch letztlich das Risiko menschlicher Fehler minimiert wird. Automatisierte Workflows können Software-Updates initiieren, Warnmeldungen bei Sicherheitsverletzungen auslösen oder Konfigurationen auf mehreren Geräten verteilen und dadurch eine konsistente und effiziente Verwaltung in remote- Umgebungen garantieren.

➤ **Plattformen zum Cloud-Management:** Da immer mehr Unternehmen ihren Betrieb auf Cloud-Server verlagern, ist das Cloud-Management ein entscheidender Faktor. Cloud-Management-Plattformen bieten eine zentrale Möglichkeit zur Überwachung von Cloud-Anwendungen und -Daten. IT-Abteilungen können die Infrastruktur über mehrere Cloud-Anbieter hinweg verwalten, die Skalierung von Ressourcen automatisieren und die Cloud-Nutzung überwachen - alles über eine einzige Schnittstelle. Cloud-native Plattformen sind noch bessere Lösungen – sie skalieren mit Unternehmen, unabhängig von Größe, Ort oder wie viele Endpunkte gemanagt werden sollen.

Welche Prozesse und Abläufe sind notwendig?

Man sollte sich nicht ausschließlich auf die genannten Tools verlassen, wenn es um Verwaltung einer IT-Infrastruktur geht.



So gilt es, regelmäßiges Patchen und Aktualisieren der IT-Systeme durchzuführen. Es ist von enormer Bedeutung, die Systeme immer auf dem neuesten Stand zu halten, um Schwachstellen sofort zu beheben, die von Hackern ausgenutzt werden können. IT-Teams sollten beim Remote-Management über automatisierte Patch-Management-Systeme verfügen, um Updates einzuspielen, sobald sie veröffentlicht werden.

Weitere wichtige Maßnahmen sind:

- **Etablierung von strengen Zugangskontrollen:** Multi-Faktor-Authentifizierung (MFA), rollenbasierte Berechtigungen und strenge Passwortrichtlinien erschweren Cyberkriminellen den Zugriff auf wichtige Systeme.

- **Regelmäßige Sicherheitsprüfungen** zur Identifikation potenzieller Schwachstellen.

- **Wirksame Überwachungs- und Benachrichtigungssysteme:** Proaktives Monitoring ist ein Muss für das Remote-Management einer IT-Infrastruktur. IT-Abteilungen müssen immer die komplette Übersicht über die Leistung und den Zustand ihres Systems haben und Echtzeit-Warnmeldungen nutzen, um Probleme wie Ausfälle, Systemüberlastungen oder Sicherheitsbedrohungen schnell anzugehen.

- **Dokumentation und Standardprozesse:** Die eindeutige IT-Dokumentation von bestimmten Abläufen ermöglicht es in verschiedenen Szenarien zügig und richtig zu reagieren. Standardprozesse sollten regelmäßig überprüft und aktualisiert werden, um neue Tools, Technologien oder Sicherheitsprotokolle zu berücksichtigen.

Trends für das Remote-Management von IT-Systemen

Das Remote Management von IT-Systemen wird in Zukunft durch viele technologische Innovationen einen beträchtlichen Wandel durchlaufen. Die Art und Weise, wie IT-Teams ihre Infrastruktur überwachen, verwalten und sichern, wird sich weiterentwickeln.

Folgende Trends zeichnen sich bereits ab:

#1 KI-basierende Patch-Management-Lösungen: Immer mehr Endpunkte bedeuten ein immer höheres Sicherheitsrisiko – das Patchen ist für die Sicherheit und Resilienz eines Unternehmens essenziell. Auf KI-basierende Lösungen reduzieren nicht nur die Risiken, sondern sie vereinfachen auch die Patch-Management-Prozesse und steigern so die Effizienz der IT-Abteilungen.

#2 Mobile Verwaltung der IT-Infrastruktur: Eine RMM-Plattform zu besitzen, auf die von unterwegs zugegriffen werden kann, wird immer wichtiger. Diese Art von RMM-Plattform gewährleistet eine bessere Unterstützung von IT-Teams, weil sie nicht an ihrem Computer sitzen müssen, um wichtige Warnmeldungen zu erhalten oder Probleme zu lösen.

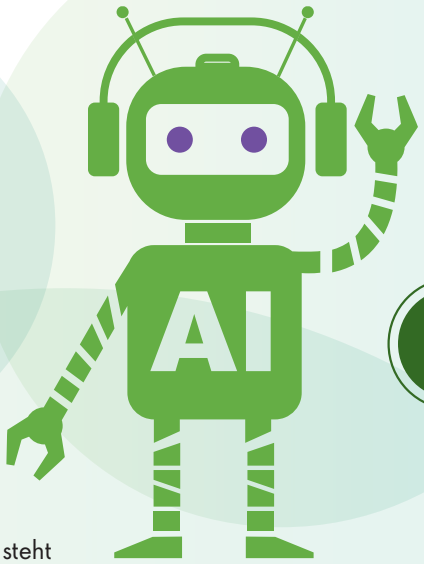
#3 Edge-Computing: Mit dem Aufstieg von Edge Computing wird mehr Verarbeitung näher an der Datenquelle durchgeführt, zum Beispiel bei IoT-Geräten, Sensoren oder in Unternehmensniederlassungen. IT-Mitarbeiter müssen sich auf die Verwaltung einer stärker dezentralisierten Infrastruktur einstellen und auf Tools verteilen, die mit Edge-Geräten umgehen können.

Das Remote-Management einer IT-Infrastruktur birgt Sicherheitsrisiken, dennoch sind die veränderten Arbeitsstrukturen nicht mehr wegzudenken. Es gibt allerdings schon jetzt sehr gute Lösungen und bewährte Prozesse, die IT-Experten in Unternehmen nutzen sollten, um ihre IT-Infrastruktur so gut wie möglich zu verwalten. Da die gesellschaftliche und technologische Entwicklung nicht stillsteht, ist es nicht nur wichtig, diese zu nutzen, sondern sich auch ständig hinsichtlich künftiger Trends auf dem Laufenden zu halten. IT-Abteilungen werden so effizienter und Unternehmen können reibungsloser agieren und dies als Wettbewerbsvorteil nutzen.

André Schindler

RECHENZENTRUMS-TRENDS 2025

INNOVATIONEN ZWISCHEN KI-POWER UND GRÜNER ENERGIE



Der Markt für den Bau und Betrieb von Rechenzentren steht unter enormem Innovationsdruck: Die wachsende Verbreitung von KI-Anwendungen treibt die Anforderungen an Rechenleistung und Effizienz rasant in die Höhe. Gleichzeitig fordert der Gesetzgeber mit neuen Vorgaben wie dem Energieeffizienzgesetz (EnEfG) eine klare Reduktion des Energieverbrauchs und eine nachhaltige Ausrichtung der Infrastruktur.

TREND 1: Steigende Rechenleistung

Die explosionsartige Zunahme von KI-Anwendungen treibt die IT-Infrastrukturen in Rechenzentren an ihre Leistungsgrenzen. Um diese Herausforderung zu meistern, wird sich zukünftig Direct Liquid Cooling (DLC) immer weiter etablieren. Durch den direkten Einsatz von Wasser oder speziellen Kühlflüssigkeiten gelingt es, die entstehende Wärme von CPUs und GPUs effizient abzuführen und die Performance der Systeme dauerhaft sicherzustellen.

TREND 2: Nachhaltigkeit und Energieeffizienz

Der Wandel zu einer nachhaltigen Energieversorgung in Rechenzentren vollzieht sich auf zwei wesentlichen Ebenen. Während der Umstieg auf erneuerbare Energiequellen wie Solar, Wind und Wasser zur Priorität wird und durch moderne Speichertechnologien für Netzstabilität ergänzt wird, gewinnt auch die effiziente Nutzung der entstehenden Abwärme an Bedeutung. Diese bisher oft ungenutzte Wärme aus Rechenzentren soll künftig systematisch für die Gebäudeheizung, industrielle Prozesse oder städtische Wärmenetze eingesetzt werden.

TREND 3: Energieverfügbarkeit

Die begrenzte Verfügbarkeit von Netzkapazitäten entwickelt sich zu einem zentralen Faktor bei der Standortwahl von Rechenzentren. Große Anbieter bevorzugen dabei Regionen, die nicht nur eine stabile Energieversorgung und ausreichende Leistungsreserven bieten, sondern auch über eine moderne Netzinfrastruktur und verlässlichen Zugang zu grünem Strom aus erneuerbaren Quellen verfügen. Parallel dazu zeichnet sich ein Trend zur dezentralen Energieversorgung ab, bei dem Rechenzentrumsbetreiber verstärkt auf eigene Energiequellen wie Solaranlagen oder lokale Partnerschaften mit Anbietern erneuerbarer Energien setzen.

TREND 4: Modulares Bauen

Steigende Baukosten und begrenzte Flächen erfordern innovative Bauweisen, die sowohl wirtschaftlich als auch zukunftssicher sind. Aus Sicht der Nachhaltigkeit punktet das modulare Bauen. Der präzise Einsatz von Materialien reduziert Verschnitt und Abfall, während vorgefertigte Bauteile häufig ressourcenschonender hergestellt werden. Gleichzeitig ermöglichen modulare Konzepte den Einsatz nachhaltiger Baustoffe wie Holz oder recycelter Stahl, die zur Reduktion der CO_2-Bilanz beitragen.

TREND 5: Edge- und On-Premises-Rechenzentren

Die zunehmende Bedeutung von Edge-Rechenzentren zeigt sich in ihrer standardisierten, oft modularen Bauweise in Containerform. Diese dezentralen Einheiten ermöglichen die Verarbeitung kritischer Daten und Anwendungen in unmittelbarer Nähe zum Endnutzer, was die Latenzzeiten deutlich reduziert. In ihrer Funktion als Bindeglied zwischen großen Cloud-Rechenzentren und Endanwendungen gewährleisten sie eine schnelle und effiziente lokale Datenverarbeitung, ohne dass Daten über weite Strecken zu zentralen Infrastrukturen transportiert werden müssen.

Fazit

Rechenzentren werden nicht nur leistungsfähiger und effizienter, sondern leisten auch einen wichtigen Beitrag zur Erreichung von Klimazielen und zur technologischen Weiterentwicklung. Die Kombination aus innovativer Kühlung, der Nutzung erneuerbarer Energien und der intelligenten Integration von Edge- und Cloud-Lösungen schafft eine resiliente, zukunftsfähige Infrastruktur, die den Anforderungen einer immer digitaleren Welt gerecht wird.

https://prior1.com/

IT-Asset-Management und IT-Servicemanagement

EFFIZIENTE ERFASSUNG UND ORGANISATION VON IT-RESSOURCEN

Durch die Kombination aus IT-Asset-Management und IT-Service-Management profitieren Unternehmen von transparenten und automatisierten Prozessen, die Kosten senken, Compliance gewährleisten und IT-Teams entlasten können.

Grundlage für effiziente IT-Prozesse

Ein systematisches IT-Asset-Management (ITAM) ist essenziell, um IT-Ressourcen effizient zu verwalten und optimal zu nutzen. Dabei umfasst ITAM den gesamten Lebenszyklus von IT-Assets – von der Beschaffung über die Nutzung bis zur Stilllegung der Geräte bzw. des Zubehörs. Zudem werden neben Hardware, Software und Cloud-Diensten auch die finanziellen und rechtlichen Aspekte erfasst und berücksichtigt. Ein sauber implementiertes und verwaltetes ITAM-System bietet Unternehmen dann klare Vorteile: Es optimiert zum Beispiel die Ressourcennutzung, minimiert Risiken durch veraltete oder nicht lizenzierte Software und unterstützt die Einhaltung von Compliance-Vorgaben. Gleichzeitig ermöglicht ITAM datenbasierte Entscheidungen, indem es präzise Einblicke in Ressourcennutzung und Kosten liefert.

Synergien für smarte Arbeitsprozesse

Die Kombination von IT-Asset-Management und IT-Service-Management (ITSM) schafft eine solide Grundlage für flexible und effiziente IT-Prozesse. Während sich ITSM auf die Bereitstellung und Steuerung von IT-Diensten konzentriert, verwaltet ITAM die dafür notwendigen Ressourcen. Zusammen bilden sie die Basis für eine IT-Strategie, die sich auf die Vorbeugung und die Priorisierung von IT-Problemen konzentriert. So kann ein Support-Team Vorfälle erkennen und beheben, bevor sie sich ausbreiten und negative Auswirkungen haben. Beispielsweise liefert ITAM im Incident Management präzise Informationen zu betroffenen Assets, was die Diagnosezeit verkürzt und konkrete Lösungen beschleunigt. Etwa: Muss ein Gerät ausgetauscht werden oder reicht eine Reparatur aus? Auch im Change Management kann ITAM unterstützen, um potenzielle Auswirkungen von Änderungen zu analysieren und Risiken zu minimieren. Die präzise Ressourcenverwaltung bzw. -nutzung sorgt somit nicht nur für reibungslose Prozesse, sondern auch für höhere Servicequalität.

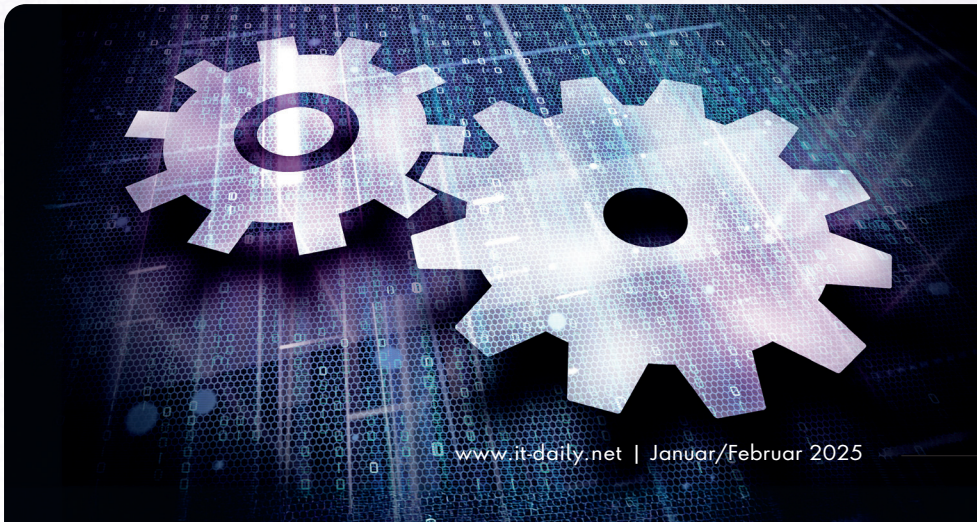
Automatisiertes ITAM mit Jira Service Management

Um ein optimiertes bzw. automatisiertes IT-Asset-Management zu realisieren, braucht es ein entsprechendes Tool. Atlassian Jira Service Management (JSM) bietet hier eine umfassende Plattform, um ITAM nahtlos in ITSM zu integrieren. Es ermöglicht das zentrale und transparente Erfassen, Verwalten und Verknüpfen von IT-Assets mit Serviceanfragen, Vorfällen und Änderungen. Funktionen wie die automatische Erkennung von IP-basierten Assets (Discovery) und ihre Attribut- sowie Abhängigkeitsüberwachung helfen dabei, IT-Infrastrukturen mit JSM effizient zu steuern – vorausgesetzt die Workflows sind entsprechend hinterlegt. Darüber hinaus ermöglichen flexible Datenimportoptionen – von CSV, JSON bis zu REST-API – und integrierte Berichtsfunktionen eine präzise Planung und Überwachung der IT-Assets.

Spezialist für ITSM und ITAM

„Die Stärke eines IT-Asset-Management-Systems liegt nicht nur in der Automatisierung, sondern auch in seiner Anpassungsfähigkeit", fügt Jan Szczepanski, CMO bei Eficode, hinzu. Als Atlassian Platinum Solution Partner und Spezialist für IT-Service-Management entwickelt Eficode unter anderem Prozesse zur nahtlosen Verknüpfung von ITAM und ITSM – mit klarem Fokus auf die Cloud-basierte Integration. Von der Prozessstruktur bis zur Lizenzberatung geht es darum, sowohl Kosten zu reduzieren als auch die Effizienz durch die intelligente Verbindung von ITSM und ITAM stetig zu steigern.

Christopher Mohr | www.eficode.com



IT-Servicemanagement

FÜNF ITSM-TRENDS, DIE SIE 2025 KENNEN MÜSSEN

Welche Entwicklungen werden dieses Jahr im IT-Servicemanagement (ITSM) auf uns zukommen und werden sie unseren Arbeitsalltag verändern? In unserer aktuellen Übersicht präsentieren wir Ihnen fünf Trends, die unserer Meinung nach 2025 das ITSM maßgeblich beeinflussen werden.

#1 Künstliche Intelligenz (KI) und Automatisierung

„KI und Automatisierung spielen schon heute eine bedeutende Rolle im IT-Servicemanagement", greift Alexander Baldauf, Technical Consultant beim Softwarehersteller TOPdesk, einen anhaltenden Trend auf. Der KI-Experte ist auch als Redner aktiv, unter anderem bei der Service Desk & Service Management World des Handelsblatts. „2025 wird das Thema weiter an Bedeutung gewinnen.", ist sich Baldauf sicher.

Der erfolgreiche Einsatz von KI erfordert allerdings geschulte Mitarbeiter. Aktuellen Studien zufolge, bemängelt jedoch rund die Hälfte der deutschen Arbeitnehmer das Fehlen entsprechender Schulungsangebote. 2025 werden also vor allem Organisationen profitieren, die KI richtig integrieren und auch ihre Teams entsprechend ausbilden.

Trotz voranschreitender Technik bleibt aber weiterhin der Mensch im Fokus: Kreativität, Empathie und Innovation können dank der KI-unterstützten Entlastung gezielt gefördert werden. Die ausgewogene Kombination aus KI, Automation und menschlicher Interaktion wird im kommenden Jahr sowohl die Effizienz als auch das Serviceerlebnis vieler IT-Abteilungen verbessern.

LETZTLICH WIRD ES 2025 VOR ALLEM DARUM GEHEN, IT-SERVICES NICHT NUR EFFIZIENT, SONDERN AUCH NACHHALTIG UND SICHER ZU GESTALTEN.

Dominik Hagen, Business Development Manager, TOPdesk, www.Topdesk.com

#2 Service Integration and Management (SIAM)

Der Trend, dass IT-Organisationen immer mehr Services an externe Serviceprovider vergeben, wird auch 2025 anhalten. Daher wird auch SIAM immer wichtiger: Es ermöglicht es, die Koordination zwischen verschiedenen Dienstleistern effizient zu gestalten und gleichzeitig eine hohe Servicequalität zu gewährleisten. Dabei wird zwischen drei wesentliche Rollen unterschieden: die strategische Kundenorganisation, die operativen Serviceprovider und der taktische Service Integrator. Letztgenannter ist für die Bereitstellung von Services sowie für die gegenseitige Zusammenarbeit der verschiedenen Serviceprovider verantwortlich.

Der Einstieg in SIAM muss nicht groß angelegt sein: Es empfiehlt sich, zunächst mit strategischen Lieferanten zu arbeiten und diese Zusammenarbeit zu optimieren. Mit einer durchdachten SIAM-Strategie können Organisationen ihre Servicebereitstellung nicht nur effizienter gestalten, sondern auch Kosten senken und die Zusammenarbeit stärken.

Viele weitere Informationen rund um Implementierung, Vorteile und Best Practices verrät Ihnen TOPdesk im Blogartikel „Was ist SIAM in der IT?".

#3 DevOps

DevOps wird 2025 besonders wichtig im ITSM-Umfeld werden, weil es in vielen Organisationen für Wettbewerbsvorteile sorgen kann. Eine enge Zusammenarbeit zwischen Entwicklungs- und IT-Teams ermöglicht es, Produkte schneller zu entwickeln und gleichzeitig den operativen Betrieb kontinuierlich zu unterstützen. Dadurch kann Benutzern eine immer bessere (Service-)Erfahrung geboten werden.

Von der starken Vernetzung beider Abteilungen profitieren aber auch die Teams selbst. Durch den engen Austausch erhält die Entwicklung regelmäßig Feedback aus Benutzerrückmeldungen und der Servicedesk wird frühzeitig über geplante

MEHR WERT
ITSM: Use Cases

MEHR WERT
Was ist SIAM in der IT?

Releases informiert. Beide Teams können somit effektiver agieren und den Benutzern konsistente und hochwertige Unterstützung bieten.

Dieser Trend wird 2025 mit klaren Prozessen und kontinuierlichem Feedback die Servicequalität verbessern und für eine effiziente, zukunftssichere IT-Organisation sorgen.

Mehr zum Thema finden Sie im Artikel „ITSM und DevOps: Freunde oder Feinde?" für Sie zusammengefasst.

#4 Nachhaltigkeit und „Green IT"

Mit dem steigenden Fokus auf Nachhaltigkeit werden Organisationen zunehmend gefordert, umweltbewusster zu agieren – auch in Hinblick auf bestehende IT-Prozesse. ITSM spielt hierbei eine zentrale Rolle, da es hilft, den Energieverbrauch und die Ressourcennutzung in der IT-Infrastruktur zu optimieren. Durch die Implementierung von Prozessen, die den ökologischen Fußabdruck verringern, können Organisationen nicht nur Kosten senken, sondern auch zur Erreichung ihrer Umweltziele beitragen. In den kommenden Jahren wird diese Praxis zunehmend an Bedeutung gewinnen.

Auch außerhalb des ITSM nehmen immer mehr Organisationen ihre Corporate Social Responsibility (CSR) ernst. Strategien umfassen nachhaltige Softwareentwicklung, klimaneutrales Hosting aber auch Barrierefreiheit vor Ort, im Web und in Anwendungen. Mit Maßnahmen wie gasfreier Büroheizung, der Förderung umweltfreundlicher Arbeitswege oder der Reduktion von Dienstreisen arbeiten alle gemeinsam an einer grüneren Zukunft.

#5 Security

Die zunehmende Digitalisierung und vernetzte Systeme machen Organisationen immer anfälliger für Cyberangriffe. Daher wird Cybersecurity unserer Meinung nach eines der wichtigsten Themen im kommenden Jahr. Organisationen jeder Art und Größe müssen Sicherheitslücken frühzeitig erkennen, Risiken minimieren und schnell auf neue Bedrohungslagen reagieren können. ITSM spielt dabei eine Schlüsselrolle: strukturierte Prozesse und klare Verantwortlichkeiten helfen dabei, Sicherheitsvorfälle schneller zu erkennen und zu beheben. Zudem stärken direkt in Workflows integrierte Sicherheitsvorkehrungen die Widerstandsfähigkeit gegenüber Cyberbedrohungen.

„Und falls es doch einmal zu einem erfolgreichen Angriff kommt", so Martin Stephan, Informationssicherheitsbeauftragter bei TOPdesk, „hilft ein gut definierter Incident Response Plan (IRP) dabei, klar strukturiert, ohne Panik und auf die bestmögliche Art und Weise darauf zu reagieren."

Fazit

Letztlich wird es 2025 vor allem darum gehen, IT-Services nicht nur effizient, sondern auch nachhaltig und sicher zu gestalten. Wem dies gelingt, wird sich dadurch Wettbewerbsvorteile sichern.

Dominik Hagen

MEHR WERT
ITSM und DevOps

Die NIS2 Pflicht meistern

AAGON ZEIGT, WIE'S GEHT

Mit der Richtlinie NIS2 – oder ausgeschrieben „Network and Information Security Directive 2" – will die Europäische Union die Cybersicherheit im EU-Raum weiter erhöhen. Unternehmen und Bundesbehörden, die kritische Dienstleistungen erbringen oder zur kritischen Infrastruktur gehören, werden verpflichtet, ihre Widerstandsfähigkeit gegen Cyberangriffe noch auszubauen.

Bis letzten Herbst sollten die Mitgliedstaaten die Richtlinie eigentlich in Gesetzesform gegossen haben, nun wird Frühjahr 2025 angepeilt. Es ändert nichts daran: Jede betroffene Organisation (EU-weit 30.000) muss jetzt prüfen, ob sie die gestiegenen Anforderungen erfüllt. Viele Kommunen sind ausgenommen, hier greift der IT-Grundschutz. Betroffene Unternehmen müssen sich selbst bei den entsprechenden Behörden registrieren. Für Zulieferer NIS2-pflichtiger Unternehmen gelten die Vorschriften aufgrund des Lieferkettensorgfaltspflichtengesetzes gegebenenfalls auch, sozusagen subsidiär.

Wer nach ISO 27001 zertifiziert ist, ist schon einmal sehr gut aufgestellt, es gehört jedoch noch mehr dazu. Daneben gibt es eine Reihe von Hebeln, über die Organisationen NIS2-ready werden können. Das Gute: Wer mit einem Unified-Endpoint-Management (UEM)-System arbeitet, verfügt damit bereits über die wesentlichen Bestandteile. UEM-Hersteller Aagon hat das Thema NIS2 seit längerem im Blick. In der aktuellen Version 6.7 seiner ACMP Suite finden sich folglich zahlreiche Funktionen, die speziell auf die erforderliche Cyberresilienz einzahlen.

Was NIS2 im Einzelnen verlangt

Unternehmen und Organisationen, die unter die Richtlinie fallen, müssen strenge Cybersicherheitsmaßnahmen implementieren und kontinuierlich überwachen. Bei Sicherheitsvorfällen müssen sie diese schnell und detailliert melden, um eine koordinierte Reaktion zu ermöglichen. Wer die Anforderungen nicht erfüllt, hat mit strengeren Strafen zu rechnen. Um die kollektive Cybersicherheitslage zu verbessern, fördert NIS2 außerdem die Zusammenarbeit und den Informationsaustausch zwischen den EU-Mitgliedstaaten. Nationale Aufsichtsbehörden erhalten ferner mehr Befugnisse und Ressourcen, um die Einhaltung der neuen Bestimmungen zu überwachen und durchzusetzen.

ACMP Suite unterstützt wesentliche Anforderungen

Mit welchen Maßnahmen – technischer wie organisatorischer Natur – lassen sich die Anforderungen nun erfüllen, und wo kann ein UEM-System hier unterstützen? NIS2 fordert grundsätzlich die Entwicklung und Implementierung einer umfassenden Cybersicherheitsstrategie, die Maßnahmen zur Risikominderung enthält. Das klingt komplizierter als es ist. Denn wenn eine UEM-Plattform wie die ACMP Suite zusätzlich zum Client Management auch verschiedene Sicherheits-Tools und -systeme integriert, liefert sie damit schon alles, was zur Umsetzung eines SOAR-Konzepts benötigt wird. Security Orchestration, Automation and Response heißt dieses Schlagwort in der Cybersicherheit – eine Allzweckwaffe zum gebündelten Abarbeiten von Security-Aufgaben. Und damit nichts anderes als eine Konkretisierung der geforderten Sicherheitsstrategie!

Im Bereich „Risikomanagement und Sicherheitsstrategien" gehört zu den Maßnahmen eine enge Risikobewertung, das heißt die Durchführung regelmäßiger Risikoanalysen, um potenzielle Bedrohungen und Schwachstellen zu identifizieren. Mit ihrem Schwachstellenmanagement hilft die ACMP Suite Administrationsabteilungen dabei, kritische Sicherheitslücken in der IT aufzuspüren, automatische Reaktionsroutinen festzulegen und Risiken mithilfe von CVSS- und CVE-zertifizierten Handlungsempfehlungen zu beseitigen. Das rechtzeitige Einspielen von Sicherheits-Updates läuft über eine automatisierte Patch-Management-Funktion. Sie stellt sicher, dass alle Endpunkte regelmäßig auf den neuesten Stand gebracht werden.

Organisationen müssen des weiteren dafür sorgen, dass alle Netzwerk- und Informationssysteme robuste Sicherheitsstandards erfüllen. Ihre Infrastruktur diesbezüglich absichern können Unternehmen mit dem Modul ACMP Defender Management. Es wurde entwickelt, um Microsoft Defender über nur eine Oberfläche auf allen Clients und Servern zu verwalten. Das Modul zeigt den Defender-Status, Scan-Historien, neueste Bedrohungen sowie Infos zum nächsten anstehenden Scan an und erlaubt Abfragen der genutzten / nicht genutzten Konfigurationsprofile. Und es steckt Geräte bei Befund in eine zentrale Quarantäne – ein großer Vorteil im Vergleich zur Einzelverwaltung des Defenders.

Verschlüsselung und Zugriffsmanagement sind weitere zentrale Themen von NIS2. Zum Schutz sensibler Daten müssen Verschlüsselungs- und Authentifizierungsmechanismen implementiert werden. Das Verschlüsselungs-Tool von Microsoft, der BitLocker, ist bereits tief in Windows integriert. Indem Aagon ihn in sein Management-Konzept einbettet, ergänzt sie den BitLocker um zusätzliche Funktionen: zentrale Verwaltung der Festplattenverschlüsselungen, Statusabfragen von Schlüsselschutzvorrichtungen, Überblick über BitLocker-fähige Clients sowie Monitoring- und Reporting-Funktionen für aussagekräftige Analysen. Das zentrale Zuweisen individueller Konfigurationsprofile ermöglicht eine einfache und strukturierte Konfiguration der Festplattenverschlüsselung.

Durch die Implementierung von Multi-Faktor-Authentifizierung (MFA) an der ACMP Console sind die wichtigen Daten der IT-Infrastruktur gesichert und damit die Anforderungen der NIS2-Richtlinie entsprechend umgesetzt. Deshalb hat Aagon die MFA in das neue ACMP Release 6.7 aufgenommen. Sie arbeitet mit einem Time-based Onetime-Passwort-Verfahren (TOTP), welches klassisch über den Google- oder Microsoft-Authenticator verbunden wird.

Einhaltung gesetzlicher Vorschriften und Audits

Von der NIS2 betroffene Organisationen müssen außerdem regelmäßige Audits ihrer Cybersicherheitsmaßnahmen durchlaufen. Mithilfe detaillierter Berichte des UEM-Systems zum Status aller Endpunkte können sie nachweisen, dass sie alle Anforderungen erfüllen und kontinuierlich an der Verbesserung ihrer Cybersicherheit arbeiten.

Die Reports lassen sich automatisch versenden und können als unterstützende Dokumentation bei der Zusammenarbeit hausintern, mit anderen Unternehmen, Sektoren sowie Behörden genutzt werden. Das dient nicht zuletzt dem von der NIS2 geforderten Informationsaustausch.

Mit Lizenzaudits haben Unternehmen es in regelmäßigen Abständen zu tun, weshalb Aagon ein Lizenzmanagement in seine Managementkonsole integriert hat. Damit lässt sich die genaue Anzahl von Softwarelizenzen im Unternehmen und deren detaillierte Nutzung analysieren. Eine Fingerprint-Datenbank zur Identifizierung lizenzpflichtiger Software erkennt neue und alte Versionen installierter Software automatisch und bietet umfangreiche Möglichkeiten zur Kategorisierung. So lässt sich zum Beispiel auch eine Kategorie für Software einrichten, die im Unternehmen allgemein nicht erwünscht ist – ein in Sachen Security wichtiges Feature, um Kontrolle und Überblick zu behalten.

Und wenn doch einmal ein Angriff geglückt ist? Business Continuity Management im Sinne von NIS2 umfasst alle Maßnahmen zur Aufrechterhaltung des Geschäftsbetriebs im Falle eines Sicherheitsvorfalls. OS Deployment für den automatischen Rollout von Betriebssystemen und ACMP CAWUM (Complete Aagon Windows Update Management) zum automatischen Patchen von Microsoft Updates ohne WSUS Server sind die Antworten von Aagon darauf, um in diesem Bereich zu unterstützen. Im Zweifel lässt sich so eine Infrastruktur schnell wiederherstellen, und das Unternehmen ist wieder startklar. Diese und weitere Möglichkeiten bietet das Unternehmen bei der Umsetzung von NIS2 als Unterstützung an. Alle genannten Aspekte reichen noch nicht zu 100 Prozent für die NIS2 Compliance, sind jedoch ein wichtiger Faktor bei der Zielerreichung. Themen wie die Festlegung und Dokumentation von Ansprechpartnern und getroffenen Maßnahmen müssen zum Teil individuell auf die eigene Organisation angepasst und durchgeführt werden.

Sebastian Weber

NIS2 FORDERT GRUNDSÄTZLICH DIE ENTWICKLUNG UND IMPLEMENTIERUNG EINER UMFASSENDEN CYBERSICHERHEITSSTRATEGIE, DIE MASSNAHMEN ZUR RISIKOMINDERUNG ENTHÄLT.

Sebastian Weber,
Head of Product Management,
Aagon GmbH,
www.aagon.com

CUSTOMER EXPERIENCE DESIGN

ERLEBNISSE FÜR ERFOLGREICHE KUNDENPROJEKTE GESTALTEN

In einer Welt austauschbarer Produkte ist es das Kundenerlebnis, das den entscheidenden Unterschied macht. Dieses Buch ist Ihr Wegweiser zu einem durchdachten Customer-Experience-Design.

Customer Experience Design:

Erlebnisse für erfolgreiche Kundenprojekte gestalten; Ingrid Gerstbach; Carl Hanser Verlag GmbH & Co.KG; 01-2025

Ob Führungskraft oder Change-Treiber: Entdecken Sie praxiserprobte Methoden, um die Bedürfnisse Ihrer Kunden wirklich zu verstehen. Lernen Sie, wie Sie durch gezielte Designforschung wertvolle Erkenntnisse gewinnen und in schlagkräftige Strategien umsetzen.

Erfahren Sie, wie Sie durch kontinuierliches Testen und Optimieren nicht nur die Zufriedenheit, sondern auch die Loyalität Ihrer Kunden nachhaltig steigern. Anhand inspirierender Fallstudien und sofort umsetzbarer Ansätze zeigt Ihnen Ingrid Gerstbach, wie Sie Kundenerlebnisse auf ein neues Level heben.

Sind Sie bereit, Ihre Kunden nicht nur zufriedenzustellen, sondern zu begeistern? Dann ist dieses Buch Ihr Schlüssel zum Erfolg. Tauchen Sie ein in die Welt des Customer Experience Design und revolutionieren Sie die Beziehung zu Ihren Kunden!

CYBERATTACKEN

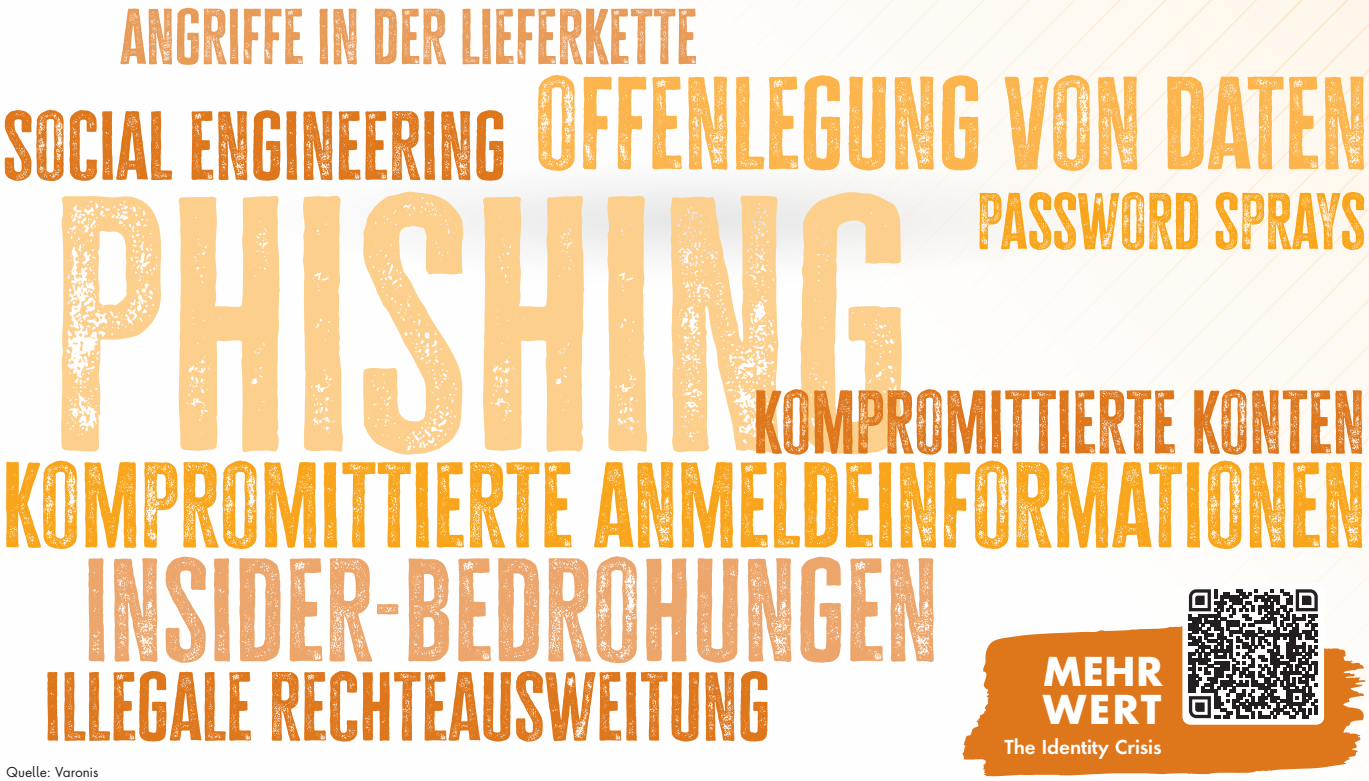
CYBERKRIMINELLE BRECHEN NICHT EIN, SIE LOGGEN SICH EIN

Bei 57 Prozent der erfolgreichen Angriffe nutzten Cyberkriminelle ein kompromittiertes Nutzerkonto, um Zugang auf die Systeme zu erhalten. Dies ergibt die Analyse von 35 der US-amerikanischen Börsenaufsicht gemeldeten Cybervorfällen zwischen Januar und August 2024, die von Varonis im Report „The Identity Crisis: An in-depth report of cyberattacks in 2024" vorgelegt wurde. Das Ziel der meisten Vorfälle waren dabei die wertvollen Unternehmensdaten, allen voran personenbezogene Daten (54 %) gefolgt von Gesundheitsinformationen (23 %). Die Analyse ergab zudem, dass auch Wochen und Monate nach dem Vorfall 85 Prozent der Angriffe noch untersucht werden. Dies deutet zum einen auf die Komplexität der Untersuchungen gepaart mit mangelnden Forensik-Möglichkeiten hin, zum anderen bedeutet dies auch, dass weitaus mehr als jeder zweite Angriff über ein kompromittiertes Konto erfolgt sein könnte. „Die Zahlen unterstrichen einen Trend, den unser Incident Response Team schon seit geraumer Zeit beobachtet: Cyberkriminelle brechen immer seltener ein, stattdessen nutzen sie ergaunerte Anmeldeinformationen, um sich in die Systeme ihrer Opfer einzuloggen", erklärt Volker Sommer, Regional Sales Director DACH von Varonis. „Dies macht ihre Entdeckung prinzipiell schwieriger, da es sich ja um scheinbar legitime Insider handelt, die sich mit gewissen Rechten ausgestattet in der Infrastruktur bewegen. Ohne eine intelligente Analyse des Nutzerverhaltens hat man kaum eine Chance, diesen Kriminellen schnell auf die Schliche zu kommen."

www.varonis.de

WIE KOMMT ES ZU CYBERANGRIFFEN?

Bei mehr als der Hälfte (57 %) der untersuchten Cyberangriffe kompromittierten die Angreifer eine Identität, um sich Zugang zur Umgebung zu verschaffen, wobei sie unter anderem folgende Techniken einsetzten:



Quelle: Varonis

MEHR WERT
The Identity Crisis

Hybrid-Cloud vs. Cloud Repatriation

WIE SIE DIE KONTROLLE ÜBER IHRE INFRASTRUKTUR BEHALTEN

In den letzten Jahren hat das Hybrid-Cloud-Modell in der IT-Infrastruktur von Unternehmen an Bedeutung gewonnen. Durch die Kombination diverser Computing Environments profitieren Organisationen von einer Reihe von Vorteilen in Bezug auf Effizienz, Zugang, Flexibilität, Skalierbarkeit, Kostenreduktion, Sicherheit und Leistung ihrer digitalen Netzwerke. Laut einer im Jahr 2022 von 451 Research und Cisco durchgeführten Studie, die 2.500 IT-Leiter in 13 Ländern befragte, hatten 82 Prozent der IT-Teams bereits Hybrid-Cloud-Modelle in ihren Organisationen implementiert, und fast die Hälfte (47%) nutzte zwischen zwei und drei öffentliche Infrastructure-as-a-Service (IaaS)-Dienste.

Ein großer Treiber für die Einführung von Hybrid-Clouds ist die künstliche Intelligenz (KI). Die Verbreitung und Entwicklung generativer KI-Dienste erfordern das Management großer Datenmengen, die nur eine flexible und effiziente Architektur bewältigen kann. Das Ausbalancieren von Workloads zwischen verschiedenen Clouds, wie einer in-house Infrastruktur in Kombination mit einem Hyperscale Provider, wird zunehmend zur Notwendigkeit.

Darüber hinaus wird erwartet, dass KI einen starken Einfluss auf Unified Communications as a Service (UCaaS) Dienste haben wird, da sie die Automatisierung von Prozessen, Antworten und Tasks ermöglicht, was die Produktivität steigert und die Kommunikation innerhalb von Unternehmen verändert.

Ähnlich ist die Integration hybrider Modelle mit 5G Networks und dezentralen Edge-Computing-Systemen ein Schlüssel zur Optimierung von Geschwindigkeit und zur Reduzierung der Latenz, was neue und innovative Wege der Cloud-Nutzungen ermöglichen wird. Denn in bestimmten Branchen und Anwendungsbereichen, wie etwa bei autonomen Fahrzeugen, Drohnen oder Krankenhausgerätschaften, ist der Unterschied zwischen einer Millisekunde und einer Sekunde entscheidend. In diesem Zusammenhang wird erwartet, dass die globalen Ausgaben für Edge Computing im Jahr 2024 232 Milliarden US-Dollar erreichen werden, was einem Anstieg von 15,4 Prozent gegenüber 2023 entspricht, so die Daten der Beratungsfirma IDC.

MIT DEM TECHNOLOGISCHEN FORTSCHRITT UND DEN STEIGENDEN ANFORDERUNGEN AN LEISTUNG, GESCHWINDIGKEIT UND SICHERHEIT FESTIGEN HYBRIDE (CLOUD-) INFRASTRUKTUREN IHRE POSITION IN DEN HEUTIGEN IT-INFRASTRUKTURMODELLEN.

Matthias Gromann,
VP Product Architecture & Strategy,
FNT Software GmbH,
www.fntsoftware.com

Cloud Repatriation

Dennoch erlebt die allgemeine Hybridisierung der IT-Infrastrukturen einen Aufschwung durch einen gleichzeitig auftretenden Gegentrend: die Cloud Repatriation. Eine kürzlich von der Citrix Cloud Software Group durchgeführte Studie ergab, dass 25 Prozent der befragten Organisationen im Vereinigten Königreich bereits die Hälfte oder mehr ihrer cloudbasierten Workloads auf On-Premises-Infrastrukturen zurückverlagert haben.

93 Prozent der an der Umfrage beteiligten IT-Leiter, die zu ihren aktuellen Cloud-Computing-Ansätzen befragt wurden, gaben an, in den letzten drei Jahren an einem Cloud-Rückführungsprojekt teilgenommen zu haben. Als häufigste Gründe für die Rückführung gelten Kosteneffektivität und unerfüllte Erwartungen.

Auch die Sicherheit ist ein zentraler Aspekt bei der Wahl virtueller oder On-Prem-Ressourcen. Laut einem IBM Report betrug der durchschnittliche globale Kostenfaktor für Datenpannen im Jahr 2023 4,45 Millionen US-Dollar, was einem Anstieg von 15 Prozent in drei Jahren entspricht. Zudem würden 51 Prozent der Unternehmen planen, ihre Sicherheitsinvestitionen aufgrund einer Datenschutzverletzung oder Datenpanne zu erhöhen. Präventiv haben bestimmte Branchen strenge Vorschriften zur Datenspeicherung, die erfordern, dass Daten an bestimmten geografischen Standorten oder unter strengen Sicherheitsmaßnahmen gespeichert werden. Ein weiterer Grund, warum Unternehmen heutzutage auf On-Premises-Ressourcen zurückgreifen.

Infolgedessen änderten diese Unternehmen ihren Ansatz von „Cloud-Only" oder

„Cloud-First" hin zur Einführung eines hybriden Infrastrukturmodells, bei dem jeder Workload in einer Umgebung platziert wird, die die entsprechenden Anforderungen optimal unterstützt.

Wie behält man die Kontrolle?

Vor dem Hintergrund der zunehmenden Nutzung von Hybrid-Cloud Umgebungen und dem gleichzeitigen Wechsel von On-Premises in die Cloud und zurück, wird die Dokumentation und Verwaltung dieser dynamischen Infrastrukturen immer wichtiger. Dies umfasst Administration, Monitoring und Kontrolle von On-Premises- und virtuellen Ressourcen, öffentliche und private Clouds, um deren Integration und effizienten Betrieb sicherzustellen.

Effizientes Management hybrider Umgebungen erfordert gründliche Dokumentation. Detaillierte Aufzeichnungen zu Konfigurationen, Abhängigkeiten und Arbeitsabläufen ermöglichen es IT-Teams, den Überblick zu behalten, potenzielle Probleme schnell zu erkennen Service-Verfügbarkeit zu sichern. Es erleichtert die Erfassung und Umverteilung ungenutzter Ressourcen und deren Neuverteilung nach Bedarf. Dies optimiert nicht nur Ressourcennutzung und Betrieb, sondern reduziert auch Kosten und steigert die Produktivität.

Einer der Hauptvorteile hybrider Infrastrukturen und Hybrid Cloud Solutions ist ihre Skalierbarkeit. Eine ordnungsgemäße Dokumentation bietet ein klares Verständnis der vorhandenen Architektur, was eine effiziente Planung und Durchführung von Erweiterungsmaßnahmen erleichtert.

Dokumentation ist auch entscheidend für die Systemsicherheit. In hybriden Infrastrukturen, wo jede Umgebung eigene Sicherheitsprotokolle und Compliance-Anforderungen hat, ist es wichtig, einheitliche Sicherheitsrichtlinien umzusetzen, um Schwachstellen zu minimieren. Zudem belegt präzise Dokumentation die Einhaltung branchenspezifischer Standards, schützt vor Strafen und wahrt den Ruf der Organisation.

Im Falle eines Systemausfalls oder eines Cyberangriffs, erlauben gut dokumentierte Systeme eine schnellere Wiederherstellung und gewährleisten die Geschäftskontinuität durch gesicherte Daten und festgelegte Notfallprotokolle.

Kurz gesagt, mit dem technologischen Fortschritt und den steigenden Anforderungen an Leistung, Geschwindigkeit und Sicherheit festigen hybride (Cloud-) Infrastrukturen ihre Position in den heutigen IT-Infrastrukturmodellen. Gleichzeitig müssen Infrastrukturen dynamisch bleiben, um Kosteneffizienz und Zuverlässigkeit zu gewährleisten. Flexible Kombinationen von On-Premises- und Cloud-Ressourcen werden immer häufiger, und IT-Manager müssen sich darauf einstellen.

Diese Entwicklungen machen es umso wichtiger, detaillierte Management- und Dokumentationslösungen zu implementieren. Nicht nur, um die betriebliche Effizienz, Sicherheit und Compliance mit den Geschäftsanforderungen zu gewährleisten, sondern auch, um eine robuste Plattform für kontinuierliche Weiterentwicklung und Innovation zu schaffen.

Matthias Gromann

Die unsichtbare Gefahr für Ihr IT-Budget

VERSTECKTE KOSTEN BEI OBSERVABILITY-TOOLS

Die Anforderungen an moderne IT-Infrastrukturen wachsen rasant: Dynamik und Komplexität nehmen zu, insbesondere durch den Wandel hin zu hybriden und Cloud-nativen IT-Umgebungen. Die Überwachung und Optimierung dieser Systeme ist heute eine Kernaufgabe jeder IT-Abteilung.

Mit der zunehmenden Verlagerung in die Cloud gewinnen Observability-Tools immer mehr an Bedeutung. Sie bieten Unternehmen leistungsstarke Möglichkeiten, um kritische Infrastrukturen zu überwachen, Engpässe frühzeitig zu erkennen und einen stabilen Betrieb sicherzustellen.

Doch Vorsicht: Hinter diesen Vorteilen lauern oft unvorhergesehene und versteckte Kosten, die Ihr IT-Budget erheblich belasten können. Eine klare Strategie ist daher entscheidend, um die Vorteile der Technologie voll auszuschöpfen und gleichzeitig die Kosten im Griff zu behalten.

Observability: Oft ein unverzichtbarer Baustein moderner IT-Strategien

Observability Tools sind mehr als ein Monitoring. Sie erweitern die klassische Überwachung von IT-Systemen, indem sie mit Hilfe von KI nicht nur Zustände, sondern auch Anomalien erkennen und die Ursachen von Problemen analysierbar machen. Besonders im Application Performance Management (APM) sind diese Tools essenziell, da sie Metriken, Logs und Traces in Echtzeit auswerten und so Störungen frühzeitig identifizieren. In einer zunehmend digitalen Welt ist der Ausfall gerade von systemkritischer Infrastruktur keine Option.

Für Cloud-Migrationen, Kubernetes-Cluster und serverlose Architekturen ist Observability eine zentrale Technologie, um Stabilität und Leistung sicherzustellen. Doch gerade diese modernen Umgebungen treiben auch die Datenmengen nach oben und damit die verbrauchsabhängigen Kosten, die sich meist anhand des monatlichen Datenvolumens berechnen. Viele Observability-Anbieter setzen hierzu auf schwer durchschaubare Preismodelle, bei denen eine verlässliche Planung, trotz scheinbar transparenter Kosten, kaum möglich ist. Besonders kritisch wird es, wenn der Datenverbrauch plötzlich Spitzenwerte erreicht: In solchen Fällen können die Log-Management-Kosten rapide ansteigen.

Daten- und Kostenexplosionen: Die unsichtbare Dimension

Der Übergang von On-Premises-Systemen zu Cloud-basierten Infrastrukturen, die auf Microservices und Containern beruhen, revolutioniert IT-Architekturen – bringt jedoch auch erhebliche Herausforderungen mit sich. Anstelle weniger großer Anwendungen entsteht nun eine fragmentierte Landschaft aus Hunderten oder sogar Tausenden kleinerer Microservices.

Die IT-Monitoring Lösung der USU

Diese Entwicklung führt zu einer dramatischen Zunahme der Telemetrie-Datenmengen, die IT-Abteilungen bewältigen müssen. Diese Umstellung auf moderne Architekturen führt in Unternehmen häufig zu einer zwei- bis zehnfachen Steigerung der Daten für Logs, Metriken und Traces. Die Prognosen von Experten sind eindeutig: Man erwartet eine Verdopplung der Datenlast alle zwei bis drei Jahre.

Ein Beispiel verdeutlicht das Szenario: Ein einmaliges Ereignis, wie ein plötzlicher Anstieg der Benutzeraktivität oder eine Störung in einem Service, kann eine sprunghafte Zunahme der Datenmenge auslösen, zum Beispiel durch eine stark anwachsende Auslastung der CPU-, Netzwerk- und Speicherkapazitäten. Dies führt auch in Observability-Tools zu einer regelrechten Datenexplosion bei Logs, Metriken und Traces und treibt dadurch die Kosten erheblich in die Höhe. Gleichzeitig stellt die langfristige Zunahme der Datenmengen Unternehmen vor erhebliche Herausforderungen, die Observability-Kosten zuverlässig zu prognostizieren. Obwohl die Kosten klar ersichtlich sind, bleibt eine präzise Planung aufgrund der schwer kalkulierbaren Datenmengen nahezu unmöglich. Dadurch besteht die Gefahr, dass Unternehmen ihr Budget aufgrund dieser schwer vorhersehbaren Variablen erheblich überschreiten.

OBSERVABILITY-LÖSUNGEN SIND UNVERZICHTBAR, UM DIE KOMPLEXITÄT MODERNER IT-INFRASTRUKTUREN ZU BEWÄLTIGEN.

Frank Laschet, Global Produkt Marketing Manager, USU GmbH, www.usu.com

Die Tücken flexibler Preisgestaltung: Günstiger Einstieg, teure Folgen

Viele Anbieter von Observability-Tools locken mit niedrigen Einstiegspreisen, verstecken essenzielle Funktionen jedoch hinter kostspieligen Add-ons. Besonders bei langfristigen Verträgen wird dies kritisch: Anfangs attraktive Rabatte entpuppen sich oft als trügerisch, wenn nicht kalkulierte Zusatzkosten das Budget sprengen.

Ein weiteres Problem liegt in den Preismodellen vieler Anbieter. Statt auf die durchschnittliche Nutzung zu setzen, orientieren sie sich an den höchsten gemessenen Traffic-Niveaus (Peaks). Selbst kurzzeitige Spitzen treiben dadurch die Kosten unverhältnismäßig in die Höhe, obwohl sie nicht die tatsächliche, langfristige Auslastung widerspiegeln. Unternehmen zahlen so oft für Ressourcen, die nur für wenige Stunden benötigt wurden, während in der übrigen Zeit ungenutzte Kapazitäten verfallen.

Zudem kombinieren viele Preismodelle verschiedene Abrechnungseinheiten wie Hosts, Agents, Nodes oder CPU-Kerne. Diese Vielfalt erfordert präzise Prognosen, um Zusatzkosten zu vermeiden. Doch in dynamischen IT-Umgebungen sind solche Vorhersagen nahezu unmöglich. Häufig basieren Lizenzen auf festen Monatsvolumina: Nicht genutzte Kapazitäten verfallen, während Überschreitungen zu erheblichen Mehrkosten führen. Bereits wenige Stunden mit erhöhtem Traffic können ausreichen, um die monatlichen Kosten drastisch zu steigern – in extremen Fällen sogar zu verdoppeln.

Strategien zur Kostenkontrolle: Der richtige Toolmix

- **Legen Sie den Fokus auf kritische Bereiche:** Observability-Tools sollten dort eingesetzt werden, wo sie den größten Mehrwert bieten – in unternehmenskritischen Bereichen wie dem Application Performance Management oder bei sicherheitsrelevanten Systemen. Hier können KI-gestützte Anomalieerkennungen und umfassende Analysen ihre Stärken ausspielen.

- **Klassisches Monitoring für weniger kritische Systeme:** Für weniger kritische Anwendungen reicht oft ein klassisches IT-Monitoring aus. Diese Lösungen sind nicht nur kosteneffizienter, sondern auch einfacher zu implementieren und zu verwalten. Indem Unternehmen ihre Überwachungsstrategie aufteilen, reduzieren sie die Menge an Daten, die durch teure Observability-Tools verarbeitet werden.

Vorteile eines Toolmixes

- **Kostenersparnis:** Kritische Systeme profitieren von Observability, während weniger wichtige Systeme kostengünstig überwacht werden.

- **Effizienzsteigerung:** Der gezielte Einsatz von Tools verhindert eine Überdimensionierung und erhöht die Wirtschaftlichkeit.

- **Flexibilität:** Unternehmen können ihre Überwachungsstrategie dynamisch anpassen, ohne sich langfristig an teure Preismodelle zu binden.

Fazit: Der Schlüssel liegt im gezielten Toolmix

Observability-Lösungen sind unverzichtbar, um die Komplexität moderner IT-Infrastrukturen zu bewältigen. Sie bieten nicht nur eine umfassende Überwachung, sondern ermöglichen durch KI-gestützte Anomalieerkennung und präzise Analysen, Probleme frühzeitig zu identifizieren und zu lösen. Besonders in systemkritischen Bereichen, wie dem Application Performance Management (APM), sicherheitsrelevanten Infrastrukturen oder geschäftskritischen Services, entfalten diese Tools ihren vollen Mehrwert. Hier können sie sicherstellen, dass Ausfälle vermieden und der Betrieb störungsfrei aufrechterhalten wird.

KLASSISCHES IT-MONITORING EIGNET SICH FÜR DIE KOSTENGÜNSTIGE ÜBERWACHUNG DER IT-INFRASTRUKTUR, WÄHREND OBSERVABILITY TOOLS GEEIGNET SIND FÜR DIE TIEFGREIFENDE ANALYSE EIGENS ENTWICKELTER SOFTWARE, DIE AUF HYPERSCALERN BETRIEBEN WIRD.

Alexander Wiedenbruch, Director R&D & Domain Representative, USU GmbH, www.usu.com

Doch nicht jedes System erfordert Observability. Weniger kritische Bereiche, deren Ausfälle keine gravierenden Auswirkungen haben, profitieren von klassischem Monitoring, das kosteneffizienter arbeitet und die Komplexität reduziert. Ein flächendeckender Einsatz von Observability-Tools würde die Datenmengen und Kosten unnötig erhöhen, ohne einen entsprechenden Nutzen zu bieten.

Der strategische Einsatz eines ausgewogenen Toolmixes – Observability für kritische Bereiche und klassisches Monitoring für weniger wichtige Systeme – ist der Schlüssel, um eine stabile IT-Infrastruktur zu gewährleisten und gleichzeitig das Budget zu schonen – ein entscheidender Wettbewerbsvorteil in einer zunehmend digitalen Welt.

Frank Laschet

DATA GOVERNANCE

DER LEITFADEN FÜR DIE PRAXIS

Data Governance:
Der Leitfaden für die Praxis;
Christiana Klingenberg, Kristin Weber,
Carl Hanser Verlag GmbH & Co.KG;
03-2025

Das Buch bietet einen kompakten, praxisorientierten Einblick in das Thema Data Governance. Dabei geht es um die Rahmenbedingungen und Standards für die Verwaltung und Zugriffssteuerung großer Datenmengen. Der Begriff wird in den Kontext der digitalen Transformation gestellt und nimmt Bezug auf die aktuellen Herausforderungen im Datenmanagement der heutigen Zeit. Dabei unterscheiden die Autorinnen nicht zwischen unterschiedlichen Datendomänen wie Geschäftspartnerdaten oder Produktstammdaten, sondern betrachten das Thema Data Governance aus einer übergeordneten Perspektive. Profitieren Sie von den Ergebnissen intensiver, praxisnaher Forschung und von jahrelanger Projekterfahrung in Unternehmen unterschiedlicher Größenordnung und Branchen. Erfahren Sie, welche Vorgehensweisen wirklich funktionieren. Das Buch enthält praktische Handlungsempfehlungen, mit denen Sie schnell die ersten Data-Governance-Aktivitäten in Ihrem Unternehmen vorbereiten, umsetzen und so einen ersten Mehrwert schaffen können.

„NUR WER IT VERSTEHT UND LIEBT, KANN AUCH IT KOMMUNIZIEREN“

Wieso IT-Unternehmen PR-Experten brauchen, die sich auch mit KI und Quantencomputing auskennen

Viele Unternehmen mit erklärungsbedürftigen Lösungen verkaufen sich unter Wert, wenn sie mit dem Markt kommunizieren. Um ihre Kernthemen verständlich und konsequent zu vermitteln, benötigen sie PR- und Kommunikationsexperten wie PR-COM, die sich vollständig der IT verschrieben haben.

Interview mit Alain Blaes, CEO von PR-COM, und Dominik Mohilo, Redakteur und IT-Experte bei PR-COM

PR-COM ist seit 35 Jahren erfolgreich darin, IT-Unternehmen aus verschiedensten Bereichen bei der Unternehmenskommunikation zu helfen. Wieso ist PR-Arbeit gerade in der IT so wichtig?
Alain Blaes: Es gibt zahlreiche Technologien, Lösungen und Konzepte, die nicht einfach unter die Leute zu bringen sind. SASE, AIOps, SOAP, SDN, MXDR ... die Liste lässt sich beliebig fortsetzen. Viele Unternehmen setzen auf faktengeladene Datenblätter, doch das überzeugt vor allem Tech-Heads. Effizienzsteigerungen, Budgetersparnisse oder kreative IT-Verfahren sind ebenfalls wichtige Kriterien und Alleinstellungsmerkmale vieler Lösungen und bleiben auf der Strecke. Das führt zwangsläufig dazu, dass sich viele Unternehmen der IT-Branche unter Wert verkaufen. Schließlich beinhaltet gute Kommunikation nicht nur, Produkte und Services zu beschreiben, sondern auch den Nutzen für die Zielgruppe zu skizzieren – und am Ende vor allem die Bekanntheit zu erhöhen und das Image zu verbessern.

Wie hilft PR-COM in diesem Zusammenhang?
Alain Blaes: Wir sind die Schnittstelle zwischen IT-Unternehmen und den Medien, die ihre Kunden konsumieren. Wir bereiten den richtigen Content auf, finden die richtigen Argumente, treffen, je nach Medium, den richtigen Ton und erreichen so exakt die richtigen Zielgruppen. Wir sind der festen Überzeugung: nur wer IT versteht und liebt, kann sie

auch erfolgreich kommunizieren – genau dafür stehen wir als Agentur. Und um dies auch personell abzubilden, beschäftigen wir nicht nur die erfahrensten Beraterinnen, die mit den Influencern und Journalistinnen der Branche per Du sind, sondern haben auch eine der größten IT-Fachredaktionen im deutschsprachigen Raum.

„VIELE UNTERNEHMEN DER IT-BRANCHE VERKAUFEN SICH UNTER WERT“

Dominik Mohilo: Dafür ist es gerade für mich als Redakteur und meine Kollegen aus der Redaktion wichtig, nicht nur die Produkte unserer Kunden zu kennen, sondern auch aktuelle Themen und Trends im Blick zu haben. Nur so können wir sicherstellen, dass wir einerseits verstehen, was unsere Kunden anbieten, und andererseits sicherstellen, ihre Alleinstellungsmerkmale und Botschaften im exakt richtigen Kontext, Umfeld und Zeitpunkt zu präsentieren.

Welche Themen und Trends werden in der IT-Branche aktuell am heißesten diskutiert?

Dominik Mohilo: Insbesondere generative KI ist natürlich allgegenwärtig. Tools wie ChatGPT sind im Alltag angekommen, DeepL hilft bei Übersetzungen und Midjourney kreiert Bilder. Das ist für den normalen User bereits ein Quantensprung. Besonders spannend wird allerdings zu beobachten sein, wie generative KI hochprofessionelle Tools wie Entwicklungsumgebungen oder Bereiche wie die Cybersecurity verändert.

Welches Potenzial schlummert in KI und GenAI noch?

Dominik Mohilo: Nun, Experten versprechen sich von KI gerade in Verbindung mit neuartigen Quantenrechnern große Durchbrüche. Die Wirkung ist in dem Zusammenhang wechselseitig. Einerseits wird generative KI dabei helfen, die Zukunftstechnologie Quantencomputing nahbar zu machen und die Programmierung der entsprechenden Hardware maßgeblich zu vereinfachen. Andererseits wird künstliche Intelligenz selbst durch die große Leistungsstärke von Quantencomputern profitieren. Bislang stoßen herkömmliche Rechnersysteme, die auf Bits und Bytes basieren, nämlich bei komplexen Anwendungen wie LLMs oder Machine-Learning-Prozessen, immer häufiger und schneller an Kapazitätsgrenzen. Das liegt an der binären Natur von Bits, die eben nur zwei Zustände kennt. Qubits, also deren Äquivalent aus dem Quantencomputing, können wegen der Superposition in der Quantenwelt praktisch unendlich viele Zustände haben – das sorgt für ganz neue Möglichkeiten und eine unvergleichliche Performanz.

Was bedeutet der Fortschritt von Quantencomputing für die Cybersicherheit?

Dominik Mohilo: Vor kurzem gelang es Wissenschaftlern aus China angeblich aktuelle, mit traditionellen Mitteln unknackbare kryptografische Standardverfahren anzugreifen und zu entschlüsseln. Sollte diese Meldung sich bewahrheiten, wäre das ein Beweis für die unglaubliche Performanz von Quantencomputing – und ein Warnsignal. Spätestens jetzt ist es an der Zeit, neue Sicherheitsverfahren zu entwickeln, die auch in der Ära der Quantencomputer wirksam sind. Auch dabei kann generative KI helfen. Die Kombination der beiden Schlüsseltechnologien könnte allerdings auch, so der positive Aspekt, die Hoffnungen erfüllen, die wir uns als Menschheit bereits von generativer KI allein versprochen hatten: Die Heilung bislang nicht heilbarer Krankheiten wie Krebs oder Alzheimer oder die Entwicklung ultrapräziser Klimamodelle, die der Politik und Wissenschaft die nötigen Stellschrauben aufzeigen, um den Klimawandel effektiv zu bekämpfen. Zunächst jedoch wird Quantencomputing erst einmal die IT-Branche und die Sicherheitsbehörden beschäftigen.

Alain Blaes: Am Beispiel KI und Quantencomputing sieht man, mit welcher Leidenschaft PR-COM die Themenvielfalt verinnerlicht hat, die die IT ausmacht. Und diese Expertise bekommen sowohl Kunden als auch die Medienlandschaft in Form von präzisen und pointierten journalistischen Beiträgen, Events, Interviews, Networking und unserer exzeptionellen Beratung zu spüren. Kein Wunder also, dass einige Großkaliber der Branche seit Jahrzehnten auf unsere Fachkenntnis in der IT vertrauen.

PRCOM

PR-COM ist eine PR- und Kommunikationsagentur, die IT liebt, sich deshalb auf IT-Unternehmen spezialisiert und deren Technologien und Zielmärkte aus dem Effeff kennt. Mit der vermutlich größten IT-Redaktion im gesamten DACH-Raum stellt sie sich seit 35 Jahren exklusiv den komplexen IT-Themen für die unterschiedlichen Zielbranchen wie Healthcare, Finance, Automotive oder Behörden und bereitet sie punktgenau, verständlich und überzeugend auf. Die Beraterinnen ergänzen die Arbeit der Redaktion in Perfektion: Sie sind per Du mit den wichtigsten Influencerinnen und Journalisten aller Mediengattungen, von Social Media über IT- und Branchenmedien bis hin zu den großen Wirtschaftsmedien. PR-COMs uneingeschränktes Commitment für Excellence, die Spezialisierung auf B2B-IT und die sehr umfangreiche Erfahrung mit der Vermarktung von komplexen Themen sind die Garantie für diesen Erfolg.

www.pr-com.de
Kontakt: excellence@pr-com.de

Industry Clouds

INTELLIGENT VERNETZT, AGILER UND KONFORM

Industry Clouds bringen immer mehr Firmen in die Datenwolken. Egal, ob in der Medizin, der Industrie oder im Handel, Branchen-Clouds gehört die Zukunft, weil sie Unternehmen agiler und Geschäftsmodelle intelligenter machen. Wie vertikale Plattformen die Adaption antreiben, welche Rolle sie für KI spielen und worauf es in puncto Konnektivität ankommt, lesen Sie im folgenden Beitrag.

Industry Clouds bieten mehr

Medizinische Daten mit KI analysieren, um Erkrankungen früher zu erkennen und Gesundheitsausgaben einzusparen – bis dato ist das im Healthcare-Bereich und vielen weiteren Branchen kein Regelfall. Industry Clouds sollen das ändern. Zum einen, indem sie passgenaue Softwares, Infrastrukturen und Plattformen als Managed Service aus dem Rechenzentrum bedarfsgerecht bereitstellen. Und zum anderen, indem sie dafür sorgen, dass Anwender spezifische Vorgaben im Hinblick auf Compliance, Governance und Datenschutz einhalten – eine Kernvoraussetzung, nicht nur, wenn Ärzte Schlaganfälle über personenbezogene Bilddaten erkennen möchten. Sondern überall dort, wo bestimmte Branchen ebenso bestimmte Anforderungen haben, geben dedizierte Clouds für dedizierte Nutzerkreise den notwendigen technologischen und rechtlichen Rahmen vor.

Kosten senken und Aufwand reduzieren – Industry Clouds bieten aber mehr als das. Gewissermaßen von der Stange weg liefern sie wie eine Branchensoftware Lösungsbausteine entlang der jeweiligen Geschäftsprozesse und Use Cases. Der modulare Ansatz macht es dabei besonders einfach, Dienste, Services und Angebote auf den eigenen Bedarf zuzuschneiden. Über die Public Cloud lassen sich zudem Dienstleister, Partner und Lieferanten ebenso einfach integrieren.

> WORKLOADS AGIL MANAGEN, DATENBASIERTE GESCHÄFTSSERVICES AUCH ÜBERGREIFEND REALISIEREN UND GESETZE EINHALTEN – INDUSTRY CLOUDS VERNETZEN KOMPLETTE ÖKOSYSTEME VERTIKAL.
>
> **Dr. Thomas King, CTO, DE-CIX, www.de-cix.net/de**

Trend zu Industry Cloud-Lösungen steigt

Workloads agil managen, datenbasierte Geschäftsservices auch übergreifend realisieren und Gesetze einhalten – Industry Clouds vernetzen komplette Ökosysteme vertikal. Ökosysteme, die Chancen für alle Akteure bieten und laut Gartner dafür sorgen, dass mehr und mehr Branchen häufiger auf öffentliche Dienste aus fremden Rechenzentren setzen werden. Von Behörden über Banken bis hin zu Versorgern – eine Umfrage der Marktforscher aus dem Jahr 2023 zeigt, dass sich weltweit 39 Prozent aller Unternehmen auf Industry Clouds zubewegen. 14 Prozent der Befragten realisieren bereits erste Pilotprojekte.

Smarte Applikationen

Was den Erfolg der Branchen-Datenwolken weiter antreiben wird, sind etwa Software-as-a-Service-Lösungen, kurz SaaS. Jede App setzt sich dabei in der Public Cloud aus vielen einzelnen Open-Source-Modulen zusammen. Der Vorteil: Wer SaaS-Dienste verwendet, der profitiert von stets aktuellen Anwendungen. Die Provider spielen Innovationen laufend in die Apps ein, passen sie so nicht nur im Hinblick auf neue Regularien und Vorgaben, sondern auch Technologien wie KI an. Industry Clouds weisen den Weg, um KI transparent, verantwortungsvoll und nachvollziehbar zu implementieren.

Maschinen vorausschauend warten und Anlagen verfügbar halten, saisonale Lastspitzen im Online-Handel prognostizieren und abfangen oder Kontobewegungen überwachen und Betrügern das Handwerk legen – KI verändert die Arbeit und erschließt neue Potenziale, um digitale Werte zu schöpfen. Über Industry Clouds ziehen smarte Applikationen in die Geschäftsmodelle kompletter Branchen ein. Dabei steckt KI zum einen nativ im Kern vieler Anwendungen selbst. Zum anderen bieten die Plattformen aber auch intelligente Bausteine, die sich je nach Applikation kombinieren und verbinden lassen – vom digitalen Sprachassistenten über den automatisierten Kunden-Service bis hin zur smarten Logik für Geschäftsvorgänge.

Sorge um Latenz

Gerade dann, wenn Cloud und KI zusammenfinden und Daten über unterschiedliche Ökosysteme hinweg fließen sollen, kommen weitere Anforderungen auf Industry Clouds zu. Beispiel Datendurchlaufzeiten: Mit Blick auf Latenz und KI aus der Cloud sorgen sich laut aktueller

Analyse von IDC 22 Prozent der europäischen Unternehmen um die Leistungsfähigkeit ihrer Netzwerke. 14 Prozent erwarten sogar, dass KI-Anwendungen die Cloud-Nutzung beeinträchtigen, weil sie die Anforderungen an Konnektivität verändern. Denn wer Apps und Daten in Industry Clouds über das öffentliche Internet oder Dritte per IP-Transit nutzt und austauscht, kann weder den Pfad kontrollieren, auf dem Informationen fließen, noch die Qualität und Performanz der Anbindung steuern. Die Folge: Hohe Latenzzeiten, stockende Datenflüsse und stotternde KI-Applikationen.

Die Lösung liefern Cloud Exchanges: Sie tauschen Daten dediziert und privat am öffentlichen Internet vorbei aus, was Informationsflüsse optimiert und Durchlaufzeiten minimiert. Wer Netze und Clouds so zusammenschaltet, sichert sich nicht nur eine leistungsstarke, reaktionsschnelle und interoperable, sondern auch Compliance- und Governance-konforme Umgebung: Datenströme lassen sich geografisch kontrollieren und lenken. Darüber hinaus ist der Austausch am Cloud Exchange besonders sicher. Beispiel Distributed-Denial-of-Service-Angriffe (DDoS): Beim so genannten Blackholing lässt sich der DDoS-Traffic erkennen und gezielt rausfiltern.

Auf dem Weg in das Cloud- und KI-Zeitalter

Industry Clouds bieten mehr als nur Rechen- und Speicherressourcen. Die Anbieter liefern ein ausgereiftes Stack aus Applikationen, Algorithmen und Technologien, der sich sofort und flexibel einsetzen lässt, um Geschäftsmodelle und Organisationen in das Cloud- und KI-Zeitalter zu bewegen. Was Innovationen treibt und agiler macht, ist zudem nötig, weil viele Firmen in puncto Cloud noch nicht da sind, wo sie stehen wollen. Schlaganfälle früher erkennen, Menschenleben retten und Gesundheitsausgaben in Milliardenhöhe einsparen – dass branchenspezifische Lösungen nicht nur Medizinern häufiger helfen sollen, steht auch für Gartner außer Frage. Im Zeitraum von 2023 bis 2027 soll die Anzahl an Unternehmen insgesamt, die Industry Clouds nutzen, von 15 auf 70 Prozent zulegen – Tendenz weiter steigend.

Dr. Thomas King

INDUSTRIE-CLOUD-PLATTFORMEN

Inwieweit spielen branchenspezifische Cloud-Plattformen eine Rolle für Ihr Unternehmen?

17 %
planen eine Implementierung bis 2026

14 %
befinden sich in der Pilotphase

39 %
haben mit der Einführung begonnen

Gartner prognostiziert, dass bis 2027 mehr als 70 Prozent der Unternehmen Industry Cloud Platforms zur Beschleunigung ihrer Geschäftsinitiativen nutzen werden.

(Quelle: Gartner: "What are Industry Cloud Platforms?" November 2023)

Datenbankadministration

DAS GOLDENE ZEITALTER BEGINNT

Unternehmen, die ihre Daten nicht effektiv nutzen, haben keine Chance, konkurrenzfähig zu bleiben. Unser hochtechnologisches Informationszeitalter macht DBAs zu heiß begehrten und dringend benötigten Mitarbeitern. Sie bereiten das Fundament jeder datengetriebenen Business-Initiative und verwalten, schützen und überwachen die kostbare Datenbankinfrastruktur. Das einzige Problem: Es gibt viel zu wenige von ihnen und die Aufgaben werden immer umfangreicher.

In den meisten Unternehmen wird das vertikale Wachstum des „Data Estates" – also die steigenden Datenmengen – von einem horizontalen Wachstum der Datenbanken, Plattformen, Technologien sowie Hosting-Szenarien begleitet. Das ist auf Geschäftsebene insofern problematisch, als sie durch die immer weiter steigende Komplexität auf ein Datenbankteam angewiesen sind, das immer auf dem neuesten Stand der Technik operieren kann und dem massiven Workload gewachsen ist. Für Database Engineers und andere Experten aus diesem Umfeld ist daher spätestens seit dem zunehmenden Einsatz von KI und dessen enormen Datenhunger ein goldenes Zeitalter angebrochen: Nie zuvor war die Nachfrage nach Datenbankspezialisten größer als heute.

Doch kein Licht ohne Schatten. Die Kehrseite der Medaille ist der immer anspruchsvollere Berufsalltag mit einer kaum noch zu stemmenden Palette an Aufgaben. Der Fachkräftemangel steigert die Last noch zusätzlich, die auf den Schultern der Datenbankadministratoren ruht. Ohne passende Maßnahmen entwickelt sich die eigentlich für alle Beteiligten positive Ausgangslage – mehr gewinnbringend nutzbare Daten für Unternehmen und eine vorteilhafte Beschäftigungslage für Datenbankadministratoren – zu einer Lose-Lose-Situation geprägt von brachliegenden Datenschätzen und überarbeiteten IT-Teams.

Das richtige Werkzeug für das richtige Problem

Monitoring-Tools, die die Überwachung der Datenbankinfrastruktur erleichtern beziehungsweise überhaupt erst ermöglichen, sind inzwischen obligatorisch. Natürlich unterscheidet sich jede Datenbankinfrastruktur und in einer idealen Welt hätte jedes IT-Team die Zeit und die Fähigkeit, seine eigene Software zu programmieren. Da sie jedoch mit ihrem Aufgabenspektrum ohnehin bereits ausgelastet oder gar überlastet sind, ist das unrealistisch. Es bedarf daher einer sehr feingranularen Evaluierung, bevor Unternehmen sich für ihr Tool der Wahl entscheiden. Sie sollten es beispielsweise via APIs mit allen genutzten Hosting-Plattformen und Datenbanksystemen verbinden können. Um die Datenbankexperten zu entlasten, sollte das passende Monitoring-Tool zudem alle relevanten Informationen in einer intuitiv zu bedienenden Weboberfläche darstellen und ein frei konfigurierbares und standardisiertes Alerting-System bieten.

Um Einblicke konsistent über alle Plattformen hinweg zu allokieren, ist es überdies unabdingbar, dass Metriken und die Art und Weise, wie die Daten konsumiert werden, ebenfalls Standards folgen. Gute Monitoring Tools überwachen jedoch nicht nur, ob alles „läuft", sondern jede Änderung eines Objekts in einer Datenbank. Falls dann etwas nicht stimmt, gibt es einen Alert aus. Das ist wichtig, da es ohne entsprechende Überwachungsinstanzen bei einem Performance-Drop schwer ist, die Ursache zu finden. Daher ist ein Monitoring umso wichtiger, das Korrelationen erlaubt.

Automatisiertes Datenbankmanagement und KI

Eine weitreichende Standardisierung und holistisches Monitoring sorgen für mehr Effizienz und erlauben proaktivere Herangehensweisen. Zusätzlich bilden sie auch die Grundlage für die Automatisierung und den Einsatz von maschinellem Lernen

UNTERNEHMEN, DIE IHRE DATEN NICHT EFFEKTIV NUTZEN, HABEN KEINE CHANCE, KONKURRENZFÄHIG ZU BLEIBEN.

Oliver Stein, Geschäftsführer DACH, Redgate Software, www.red-gate.com/de

oder künstlicher Intelligenz. Im Bereich Datenbankmanagement ist Automatisierung heutzutage praktisch unabdingbar. Gerade bei repetitiven Aufgaben wie dem Installieren großer Mengen von Servern und Datenbanken spielt sie ihre großen Vorteile aus und sorgt für deutlichen Zeitgewinn. Diese Ressourcen können Mitarbeitende für wertschöpfende Aufgaben verwenden.

Künstliche Intelligenz sorgt für noch mehr Effizienz, denn basierend auf dem Monitoring-Fundament können Datenbankexperten KIs trainieren, die ohne menschliche Intervention auf bestimmte Vorgänge reagieren. Läuft beispielsweise ein Datenspeicher voll, kann eine KI – sofern das Monitoring-Tool den ausgehenden Storage identifiziert hat – den Datenfluss umleiten oder mehr Speicherressourcen zuweisen. Digitale Helfer aus dem Bereich generative KI (GenAI) können Datenbankentwickler und -administratoren zudem bei ihrer täglichen Arbeit unterstützen, indem sie Lösungswege proaktiv vorschlagen oder die Informationsrecherche deutlich erleichtern. Jedoch ist Vorsicht geboten, denn KI-Tools sind keineswegs über jeden Zweifel erhaben. Halluzinationen zum Beispiel, also logisch klingende Resultate, die nicht auf Trainingsdaten basieren, sind aktuell noch eine große Gefahr.

Datenbanksicherheit: Strategien und Taktik

In Sachen Sicherheit ist Monitoring – neben dem Einsatz spezieller Maßnahmen wie Firewalls, Backupstrategien oder Verschlüsselungsmechanismen – das A und O. Datenbankadministratoren sollten nicht nur überwachen wo Daten und Sicherungskopien liegen, sondern auch wer darauf Zugriff hat und ob irgendwelche Veränderungen vorgenommen werden – und von wem. Stellt das Monitoring-Tool fest, dass jemand Anpassungen durchführen will, die nicht durch einen Approval-Prozess oder die gewohnte CI/CD-Pipeline gegangen sind, muss es genauso Alarm schlagen, wie wenn die Nutzerberechtigungen verändert, Änderungen am Server vorgenommen oder SQL Injections versucht werden: All das sind Hinweise auf Hacker-Attacken.

In Sachen Security muss für Unternehmen die Maxime gelten: Ein Cyberangriff ist unvermeidlich. Es gilt daher, sich doppelt abzusichern. Einerseits mit klassischen Sicherheitsmaßnahmen wie Firewall, Monitoring der IT-Infrastruktur und des Datenverkehrs im Netzwerk. Und andererseits durch das Monitoring der Datenbankumgebung. Hacker nutzen heute gerade Datenbankabfragen, um Schwachstellen und potenzielle Einfallstore in die IT-Infrastruktur von Unternehmen zu finden. Gute Datenbank-Monitoring-Tools erkennen diese Vorgehensweise und warnen die Administratoren vor entsprechenden Aktivitäten.

Neben dem Datenbankmanagement wird KI auch beim Thema Security und in praktisch allen anderen Unternehmensbereichen zukünftig eine gewichtige Rolle spielen: Sie entlastet bereits heute das Fachpersonal und gibt tiefe Einblicke in die Geschäftsprozesse inklusive Vorschläge für deren Optimierung. Da dafür Unmengen von Daten erhoben, sicher gespeichert und für die Anwendungen bereitgestellt werden müssen, sind Datenbankexperten so gefragt wie nie – Tendenz rapide steigend.

Oliver Stein

Process Mining

ANFORDERUNGEN UND SOFTWARELÖSUNGEN

Als Methode zur datengetriebenen Prozessanalyse hilft Process Mining, Erkenntnisse aus Prozessen abzuleiten, um diese effektiver und effizienter zu gestalten. Unternehmen stehen jedoch häufig vor dem Problem, aus einer Vielzahl unterschiedlicher Softwarelösungen die richtige Option auszuwählen, die den spezifischen Anforderungen gerecht wird. In diesem Beitrag wird daher untersucht, welche Anforderungen an eine Process Mining Software gestellt werden und für drei Softwarelösungen geprüft, inwieweit diese Anforderungen erfüllt werden.

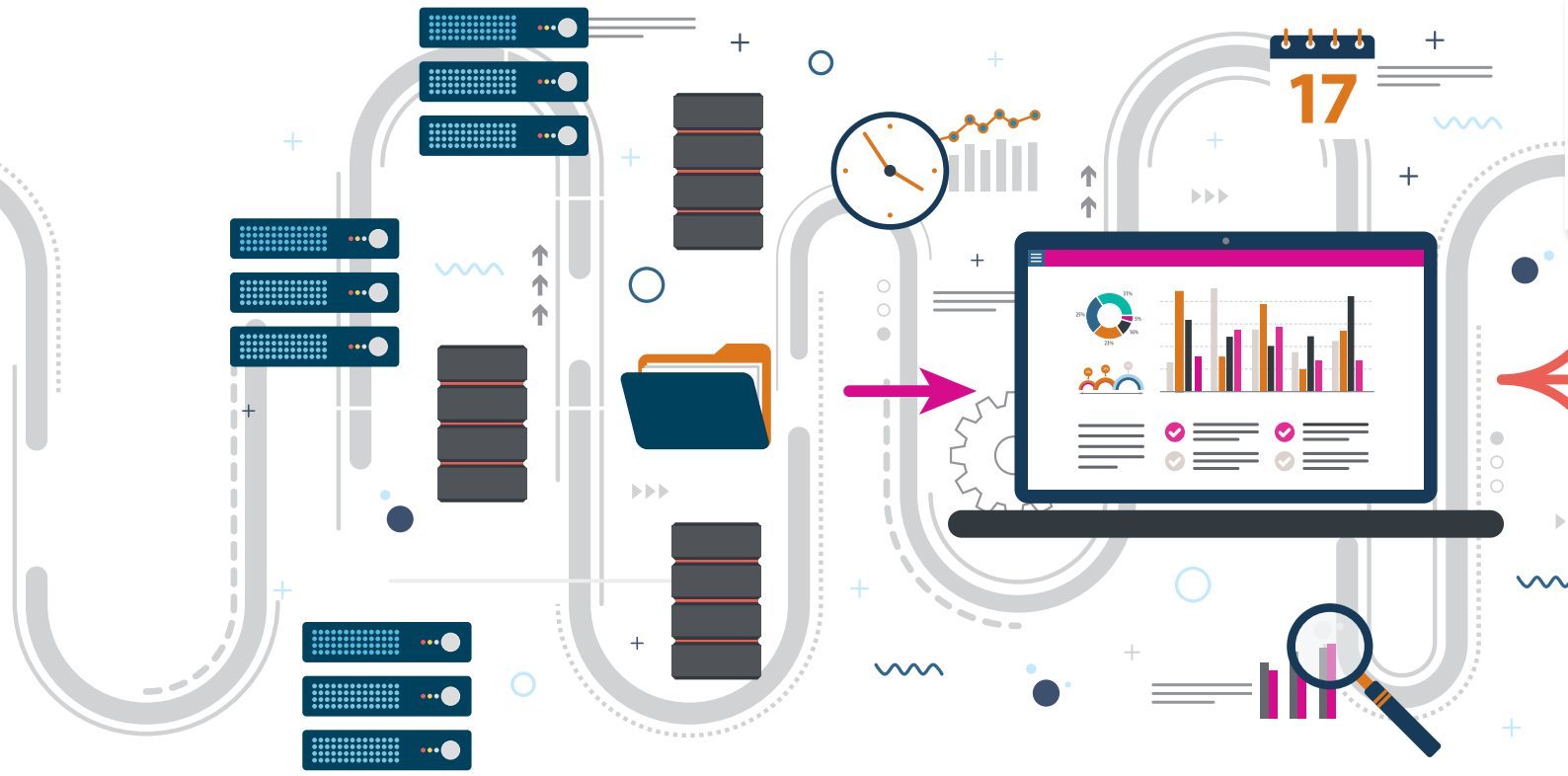
Grundlagen zu Process Mining

Process Mining ist eine Analysemethode, die digitale Spuren von Geschäftsprozessen aus IT-Systemen nutzt, um diese Prozesse zu rekonstruieren und zu optimieren. Dabei werden Data Mining und Geschäftsprozessmanagement kombiniert, um Transparenz über die tatsächlichen Prozessabläufe in Unternehmen zu schaffen. Erreicht wird dies durch die Auswertung von Transaktionsdaten aus IT-Systemen. Diese Daten enthalten Informationen über die ausgeführten Aktivitäten, die zugehörigen Zeitstempel und die beteiligten Ressourcen. Mit Process Mining lassen sich dann Abweichungen zwischen geplanten und tatsächlichen Abläufen erkennen, so dass Unternehmen Ineffizienzen und Engpässe aufdecken können.

Die Methode umfasst die drei Hauptanwendungen Discovery, um Prozesse aus Daten zu rekonstruieren, Conformance, um Abweichungen zu analysieren, und Enhancement, um bestehende Prozesse zu verbessern. Moderne Process Mining Werkzeuge visualisieren diese komplexen Daten, so dass Prozesse verständlich dargestellt werden können. Dies ermöglicht eine datengetriebene Optimierung von Prozessen.

Softwarelösungen für das Process Mining

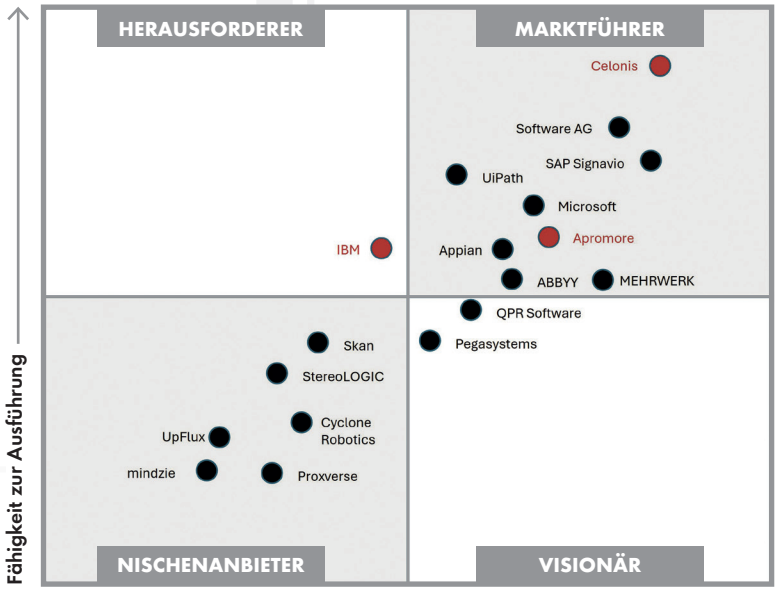
Auf dem Softwaremarkt werden zahlreiche Process Mining Lösungen angeboten. Im Gartner Magic Quadrant for Process Mining Tools 2024 wurden 18 relevante Anbieter identifiziert und deren Lösungen hinsichtlich ihrer Stärken und Schwächen bewertet. Die Bewertung zeigt, wie gut die Anbieter ihre Visionen umsetzen können und ordnet sie einem der vier Quadranten zu: Marktführer, Herausforderer, Nischenanbieter und Visionäre. Neun



Process Mining Produkte befinden sich aktuell im Quadranten der Marktführer und ein Produkt im Quadranten der Herausforderer (siehe Bild 1).

Im Folgenden werden die drei rot markierten Produkte von Celonis, Apromore und IBM kurz vorgestellt und verglichen.

Bild 1: Gartner Magic Quadrant for Process Mining April 2024



➤ **Apromore** ist eine Open Source Process Mining Software zur Visualisierung und Analyse von Geschäftsprozessen. Sie bietet Funktionen zur Prozesserkennung (Discovery), zur Abweichungsanalyse (Conformance) und zur Prozessverbesserung (Enhancement). Die Plattform ermöglicht die Visualisierung von Prozessen auf Basis von Event-Logs, die aus unterschiedlichen IT-Systemen stammen können. Anwender können mit der Software Engpässe und Abweichungen identifizieren und die Effizienz und Konformität von Prozessen bewerten. Unterstützt werden unter anderem Prozesssimulationen, Engpassanalysen und die Untersuchung von Automatisierungsmöglichkeiten. Die Software bietet eine grafische Oberfläche zur Darstellung und Bearbeitung der Daten. Als Open-Source-Tool kann Apromore an spezifische Anforderungen angepasst und in bestehende IT-Systeme integriert werden.

➤ **Celonis** bietet auch Discovery, Conformance und Enhancement Funktionen, um Prozesse zu analysieren, zu bewerten und zu optimieren. Geschäftsprozesse werden auch auf Basis von Event-Logs aus IT-Systemen analysiert. Celonis unterstützt die Integration von Daten aus verschiedenen Systemen wie ERP, CRM und anderen Unternehmensanwendungen. Weitere Funktionen sind die Identifizierung von Engpässen, die Analyse von Prozesskennzahlen und die Simulation von Verbesserungen. Die Plattform umfasst außerdem Dashboards und Visualisierungen, die einen detaillierten Einblick in die Prozesse ermöglichen. Celonis wird von Unternehmen verschiedener Branchen eingesetzt, um datenbasierte Entscheidungen über ihre Prozesse zu treffen. Die Software kann sowohl on-premise als auch in der Cloud betrieben werden und bietet eine Vielzahl von Konnektoren für unterschiedliche Quellsysteme. Celonis ist vor allem bei Großunternehmen etabliert. Die Software wird weltweit eingesetzt und hat durch ihre breite Funktionalität und Integration in bestehende Systeme eine starke Marktpräsenz. Durch strategische Partnerschaften und die Fokussierung auf Process Mining und Execution Management hat sich Celonis als Marktführer in diesem Technologiebereich positioniert.

PROCESS MINING LÖSUNGEN GEWINNEN ZUNEHMEND AN BEDEUTUNG, DA DIE PRODUKTE TIEFERE EINBLICKE IN GESCHÄFTSPROZESSE ERMÖGLICHEN.

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

➤ Als dritte Softwarelösung wird **IBM Process Mining** näher betrachtet. Wie bei den vorherigen Produkten wird die Software für alle drei Hauptanwendungen von Process Mining eingesetzt und verwendet Algorithmen, um Engpässe, Ineffizienzen oder Abweichungen von Standardprozessen zu identifizieren. Darüber hinaus bietet IBM Process Mining Funktionen zur Prozessmodellierung und -simulation, mit denen mögliche Verbesserungen getestet werden können. Ziel ist es, datenbasierte Entscheidungen zu fördern und Unternehmen bei der digitalen Transformation zu unterstützen. Die Software lässt sich gut mit anderen IBM Produkten und Software von Drittanbietern integrieren, um eine umfassende Prozessanalyse zu ermöglichen. Neben der Analyse ermöglicht IBM Process Mining auch die Echtzeit-Überwachung von Prozessen, um kontinuierliche Verbesserungen zu gewährleisten.

Bewertung ausgewählter Process Mining-Produkte

In einer unternehmensinternen Studie wurden die Anforderungen an eine Process Mining Software ermittelt und die drei vorgestellten Produkte anhand dieser Bewertungskriterien bewertet. Die Bewertungskriterien lassen sich in folgende acht Themenbereiche gruppieren:

IN ZUKUNFT WIRD DIE INTEGRATION VON KI IN PROCESS MINING LÖSUNGEN EINE WICHTIGE ROLLE SPIELEN.

Christian Dirr, Fachreferent, Deutsche Telekom Technik GmbH, www.telekom.com/

#1 Allgemeine Anforderungen: Ein Process Mining Tool sollte benutzerfreundlich und übersichtlich gestaltet sein, damit Anwender auch ohne Expertenwissen Prozesse erkennen können. Schulungsmöglichkeiten und Support erleichtern die Einarbeitung und Problemlösung. Eine performante und skalierbare Architektur sowie regelmäßige Updates und Dokumentationen gewährleisten Stabilität und Fehlerbehebung. Kostentransparenz und eine Community zum Austausch fördern den erfolgreichen Einsatz.

#2 Die Anforderungen an das Datenmanagement umfassen flexible Schnittstellen zur Integration neuer und bestehender Systeme sowie zur individuellen Datenaufbereitung. Importmöglichkeiten wie CSV-Dateien oder ETL-Prozesse sollten zur Verfügung stehen, um Daten effizient zu integrieren und deren Qualität durch Prüflogiken sicherzustellen. Big-Data-Technologien gewährleisten Performance und Skalierbarkeit. Das Tool sollte eine wirtschaftliche Verwaltung der Datenhistorie ermöglichen, aktuelle Daten priorisieren und die Verfügbarkeit durch regelmäßige Backups sicherstellen.

#3 Die Anforderungen an die Prozessaufdeckung umfassen die klare Visualisierung des Ist-Prozesses einschließlich aller Prozessschritte, um Automatisierungsmöglichkeiten und deren Potenzial zu identifizieren. Das Tool sollte auch die automatische Erkennung von Prozessen anhand von Logfiles oder Transaktionsdaten ermöglichen, um Überschneidungen zu erkennen und manuelle Vorarbeiten wie zum Beispiel Labeling zu minimieren. Schließlich ist die Definition von Use Cases notwendig, um gezielt Automatisierungspotenziale innerhalb der Prozesse zu identifizieren und umzusetzen.

#4 Anforderungen an die Konformitätsprüfung: Soll-Prozesse sollen beispielsweise durch den Import von BPMN-Dateien übersichtlich dargestellt und automatisch mit Ist-Prozessen verglichen werden. Das Tool sollte Abweichungen flexibel aufzeigen und deren Nutzen unter bestimmten Bedingungen bewerten.

#5 Die Integrationsanforderungen erfordern eine nahtlose Integration von KI und maschinellem Lernen für Vorhersagen, Fehlerbehebung und Automatisierung. Darüber hinaus sollte das Tool in der Lage sein, RPA zu nutzen, um Automatisierungen direkt anzustoßen. Eine Rückmeldung der Ergebnisse ist erforderlich, um die Auswirkungen zu visualisieren und weiter zu analysieren.

#6 Die Anforderungen an Visualisierung, Monitoring und Reporting beinhalten flexible Dashboards, die im laufenden Betrieb angepasst und erweitert werden können, mit KPIs wie Durchlaufzeiten, Prozessfällen oder Automatisierungsgrad. Automatische Hervorhebungen wie Ampeldarstellungen und Warnmeldungen sollen kritische Abweichungen aufzeigen. Filter- und Sortierfunktionen ermöglichen spezifische Sichten und unterstützen ein effizientes Monitoring priorisierter Themen.

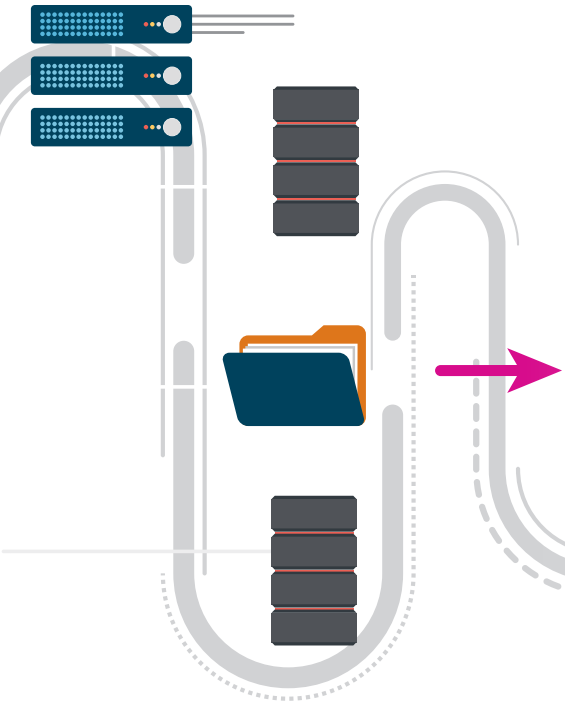
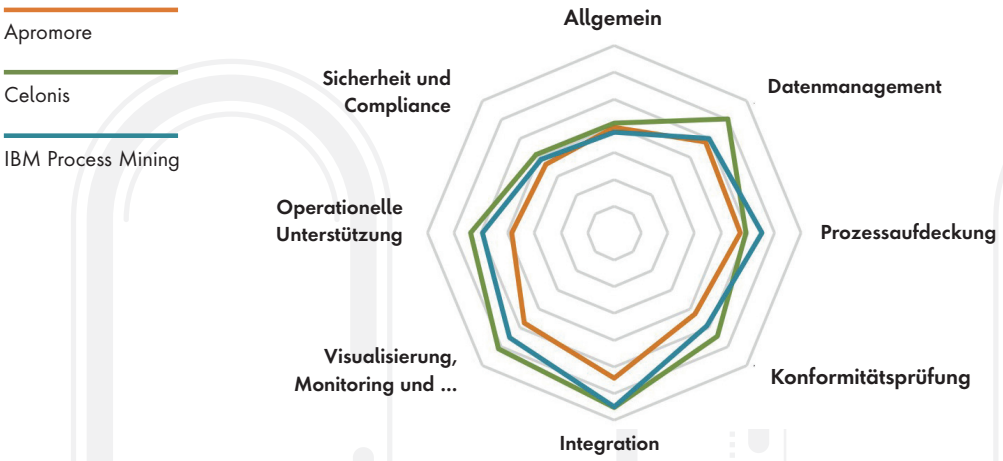


Bild 2: Ergebnisse der unternehmensinternen Process Mining Studie

Kategorie	∅ Gewichtung	Apromore Bewertung	Apromore Score	Celonis Bewertung	Celonis Score	IBM Bewertung	IBM Score
Allgemein	10,50%	52	0,792	54	0,819	50	0,752
Datenmanagement	13,33%	58	0,964	72	1,204	60	0,999
Prozessaufdeckung	12,33%	23	0,944	24	0,986	27	1,105
Konformitätsprüfung	12,33%	35	0,855	44	1,088	40	0,98
Integration	15,50%	21	1,085	25	1,303	25	1,3
Visualisierung, Monitoring und Reporting	13,83%	48	0,953	62	1,225	56	1,106
Operationelle Unterstützung	11,83%	20	0,771	27	1,078	25	0,988
Sicherheit und Compliance	10,33%	28	0,725	32	0,828	30	0,777
Summe	**100%**		**7,089**		**8,531**		**8,007**
Ranking			**3**		**1**		**2**



#7 Anforderungen an die operationelle Unterstützung: Ein Process Mining Tool sollte automatisch generierte Handlungsempfehlungen durch KI liefern, um Optimierungspotenziale und Maßnahmen aufzuzeigen. Eine an den Anwendungsfall angepasste Datenaktualität von monatlich bis echtzeitnah ist essentiell. Fallback-Optionen ermöglichen bei Datenlücken den Zugriff auf historisierte Daten, um weiterhin Informationen bereitzustellen.

#8 Anforderungen an Sicherheit und Compliance: Ein Process Mining Tool benötigt ein Berechtigungskonzept wie Role Based Access Control (RBAC) für differenzierte Zugriffsrechte. Die Einhaltung gesetzlicher Vorgaben wie der DSGVO muss durch Anonymisierung, Verschlüsselung und Datenlöschung sichergestellt werden. Zudem sollte das Tool Compliance-Verstöße automatisch erkennen, etwa bei Abweichungen von Standardprozessen.

Die unternehmensinterne Studie zeigt, dass die erweiterten Verbesserungsmöglichkeiten, insbesondere durch fortschrittliche Technologien wie KI und RPA, mit der höchsten Gewichtung als zentral angesehen werden, währen die allgemeinen Anforderungen sowie Sicherheit und Compliance in diesem Fall die geringste Relevanz haben. Siehe Spalte „Gewichtung" in Bild 2.

In der unternehmensinternen Studie erhält Celonis die beste Gesamtnote, da die Software durch vielfältige Datenmanagement- und Echtzeitanalysemöglichkeiten, den Process Adherence Manager und eine gute Integration von KI und RPA überzeugt. Apromore punktet mit Stärken bei allgemeinen, nicht-funktionalen Anforderungen und IBM Process Mining mit detaillierten Simulationsfunktionen zur Prozess-Erkennung, während beide in spezifischen Bereichen hinter Celonis zurückbleiben.

Schlussbetrachtung

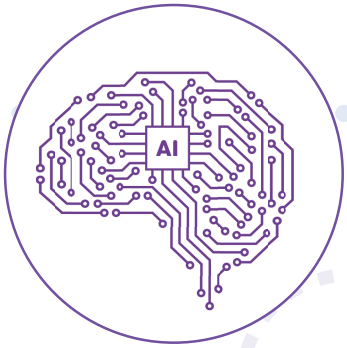
Process Mining Lösungen gewinnen zunehmend an Bedeutung, da die Produkte tiefere Einblicke in Geschäftsprozesse ermöglichen. Zukünftig wird die Integration von KI sicherlich noch umfassendere Analysen und die Identifikation von Optimierungspotenzialen ermöglichen, wodurch Unternehmen ihre Prozesse effizienter gestalten können. Anbieter wie Celonis beschreiten diesen Weg bereits. Sie entwickeln innovative Lösungen wie NLP-basierte Abfragen, die komplexe Analysen ohne tiefes Expertenwissen ermöglichen.

Prof. Dr. Peter Preuss, Christian Dirr

Hype oder Impact?

DAS POTENZIAL DER GENERATIVEN KI ERSCHLIESSEN

Ende 2022 erreichte OpenAI mit der Veröffentlichung von ChatGPT einen Meilenstein für die Anwendung künstlicher Intelligenz (KI): Generative KI (GenAI) wurde plötzlich für den Massenmarkt kostenlos zugänglich. Mit rasender Geschwindigkeit steigt die Zahl der Nutzer seitdem und übertraf nach nur zwei Monaten die Marke von 100 Millionen Usern. Der Oberbegriff „KI" steht nun bei allen Unternehmen weltweit auf der Agenda. Von personalisierten Produktempfehlungen bis zur Ableitung strategischer Entscheidungen – die Versprechen sind groß. Doch eine entscheidende Frage bleibt: Warum gelingt es vielen Unternehmen nicht, den Hype in messbare Ergebnisse umzuwandeln?



Die Antwort liegt in der Schwierigkeit, KI strategisch zu implementieren.

Gefahr der Oberflächlichkeit: Interface-Trugschluss

Die Nutzung von KI ist oft komplex, da sie spezialisierte Modelle und anspruchsvolle Datenverarbeitung erfordert. GenAI bietet hingegen einen benutzerfreundlichen Ansatz für kreative Lösungen und Content-Generierung, erleichtert die Implementierung, birgt jedoch das Risiko, dass Unternehmen GenAI nur opportunistisch nutzen. Der Trugschluss liegt darin, GenAI primär als Tool zur Inhaltsproduktion zu sehen. Tatsächlich besteht ein signifikantes Potenzial in der Fähigkeit, Daten zu analysieren, zu verknüpfen und Entscheidungen auf Basis von Mustern vorzubereiten beziehungsweise zu treffen. Unternehmen, die nicht über die Oberfläche hinaus blicken, riskieren einen Verlust an Effizienz und Effektivität. Ein Blick auf den aktuellen Einsatz von GenAI zeigt wiederkehrende Muster: Bislang werden primär operative, repetitive Aufgaben an GenAI-Anwendungen übergeben. Die entscheidende Frage ist, wie GenAI auf die strategische Ebene gehoben werden kann, um skalierbaren Nutzen zu schaffen.

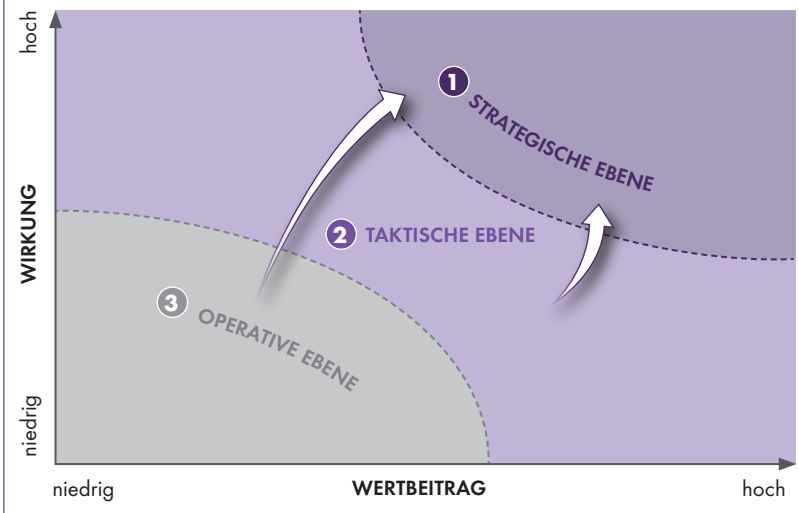
Vom Konsum zur professionellen Anwendung

Der Schlüssel liegt darin, GenAI als strategisches Instrument verfügbar zu machen – ein Beispiel bieten Large Language Models für strategische Fragestellungen. Diese werden so trainiert, dass KI-Agenten zur Identifikation relevanter Trends oder zur Diskussion von Problemlösungen verschiedene Perspektiven, zum Beispiel von Politikern, Top-Managern oder Wissenschaftlern, beisteuern. So werden etablierte Innovationsmethoden mit GenAI für die Findung und Entwicklung strategischer und innovativer Lösungen genutzt.

GenAI-Anwendungsszenario in der Beratung

Eine Möglichkeit zur Entwicklung einer prototypischen IT- und Digitalstrategie bildet der Strategiesprint. In fünf Tagen

AKTUELLE MUSTER IM UMGANG MIT GenAI



Strategische Ebene: GenAI spielt eine eher untergeordnete Rolle und bleibt ein Experimentierfeld, das in Innovationslaboren getestet, aber selten strategisch genutzt wird.

Taktische Ebene: Teams nutzen KI opportunistisch für die Erstellung von Konzepten, um Datenanalysen zu beschleunigen oder Ideen zu generieren.

Operative Ebene: Hier ist GenAI weitverbreitet. E-Mails verfassen oder repetitive Aufgaben automatisieren _ all das geschieht mit beeindruckender Effizienz.

wird gemeinsam mit einem Expertenteam des Kunden eine Strategie samt Transformationsroadmap konzeptioniert. Dabei können Strategietools wie qbs.ai unterstützen, indem es kundenspezifische Business Capability Maps erzeugt. Mit diesen und mithilfe des Know-hows der Strategieberater können dann relevante Business Capabilities identifiziert und passende Maßnahmen abgeleitet werden, um die strategischen Ziele zu erreichen.

Fazit: Das volle Potenzial von GenAI realisieren

Um das volle Potenzial von GenAI auszuschöpfen, müssen Unternehmen über operative Vorteile hinaus denken. Entscheidend ist ein ganzheitlicher Ansatz, der strategische, taktische und operative Anwendungen von GenAI integriert. Dabei sollten Unternehmen langfristige Investitionen in die Fähigkeiten ihrer Mitarbeitenden, in Infrastruktur und Governance berücksichtigen, um nachhaltige Wettbewerbsvorteile zu sichern.

Dr. Andreas Reuschl, Juri Rybicki, Sebastian Frost | www.kobaltblau.com

STRATEGIESPRINT

	Umfeld & Ambition	Design-Prinzipien & Prototyp	Verprobung & Adaption	Maßnahmen & Priorisierung	Transformation & Roadmap
Sprint-Tag	**Tag 1**	**Tag 2**	**Tag 3**	**Tag 4**	**Tag 5**
Beschreibung	Entwicklung eines gemeinsamen Verständnisses des Unternehmensumfeldes mit Definition der strategischen Ambition	Entwicklung von Design-Prinzipien als Rahmen für die Strategieentwicklung mit anschließender Definition eines ersten Strategieprototyps zur initialen Verprobung	Test und Aktualisierung des Strategieprototyps mit Feedback der relevanten Stakeholder aus Business und IT sowie spezifischen KI-Agenten	Identifizierung von Maßnahmen zur Umsetzung der Strategie anhand der Capability Map sowie Priorisierung der Maßnahmen	Erarbeitung eines effektiven Transformationsansatzes sowie Entwicklung der Roadmap unter Berücksichtigung von Prioritäten und Abhängigkeiten
GenAI-Impact	qbs.ai liefert relevante Trends und Herausforderungen zur Umfeldanalyse und Gestaltung der Ambition sowie eine kundenspezifische Business Capability Map für den Sprint	Business Capability basierte Erzeugung von Design-Prinzipien mit strategischen Impulsen für die Entwicklung des Strategieprototyps	Entwicklung von Lösungsszenarien durch Betrachtung von Trends und Business Capabilities verschiedener Branchen mit qbs.ai	Basierend auf den Ergebnissen der Verprobung wird die Business Capability Map adaptiert und relevante Maßnahmen zur Umsetzung der Strategie durch qbs.ai vorgeschlagen und priorisiert	Transformationsansätze werden mit KI-Agenten entwickelt und initial verprobt, um eine effektive Entscheidungsfindung zu gewährleisten

KI mit System

DATENMANAGEMENT ALS SCHLÜSSEL ZUR DIGITALEN INNOVATIONSKRAFT

Anwendungsfälle für Künstliche Intelligenz gibt es viele – die Herausforderung liegt vor allem darin, sie effizient umzusetzen. Neben einem einheitlichen und strukturierten Vorgehen kommt es dabei auf flexible und skalierbare IT-Architekturen mit optimal aufeinander abgestimmten Komponenten an. Diese ermöglichen es, Daten zügig und risikoarm in Erkenntnisse verwandeln lassen, und das in immer neuen Anwendungsfällen.

Wollen Unternehmen das enorme Potenzial von Künstlicher Intelligenz erschließen, stehen sie oft vor der Frage, wo sie anfangen sollen. Denn die Technologie ist so unglaublich vielseitig, dass die gezielte Suche nach Einsatzmöglichkeiten eher zu viele als zu wenige Anwendungsfälle zutage fördert. Welche davon als erste umgesetzt werden, sollte dann nicht allein vom erwarteten Nutzen abhängen, den sie für das Geschäft generieren, obwohl das natürlich der zentrale Faktor ist. Unternehmen müssen aber auch die Machbarkeit und den Aufwand berücksichtigen: Fehlen die benötigten Daten oder erschweren komplexe Regularien, mangelndes Know-how oder technische Beschränkungen die Umsetzung, drohen langwierige Projekte, die viel Geld verschlingen und womöglich nie die gewünschten Ergebnisse bringen.

Die Dell AI Factory umfasst ein breites Angebot an Infrastrukturlösungen, KI-Software und Services, die die Einführung von KI beschleunigen und Risiken reduzieren

(Quelle: Dell Technologies)

Daher sollten sich Unternehmen zum Einstieg in das Thema KI auf Anwendungsfälle konzentrieren, die mit überschaubarem Aufwand umgesetzt werden können. Diese liefern nicht nur wertvolle Erfahrungen, die in Folgeprojekte einfließen, sondern auch Erfolgserlebnisse, die wichtig für die Akzeptanz der neuen KI-Anwendungen, die Motivation der Mitarbeiter und die Bewilligung weiterer Budgets sind. Idealerweise entwickeln Unternehmen zudem Prozesse, um kontinuierlich Anwendungsfälle zu sammeln und nach einheitlichen Kriterien zu bewerten, damit die Suche und Evaluierung von KI-Einsatzmöglichkeiten keine einmalige Sache bleiben. Das Ziel sollte sein, die KI-Nutzung immer weiter voranzutreiben, um mehr und mehr Abläufe zu verbessern.

Neue Ansätze beim Datenmanagement

Gut für den KI-Einstieg eignen sich erfahrungsgemäß Chatbots und KI-Assistenten auf GenAI-Basis, die internes Wissen leicht zugänglich machen und Fachbereichen wie IT, HR, Vertrieb oder Kundenservice eine schnellere und bessere Beantwortung von Anfragen erlauben. Alternativ dazu sind auf klassischer KI aufbauende Tools für Planungs- und Optimierungsaufgaben beispielsweise in der Produktion, der Logistik oder im Vertrieb erfolgsversprechende Einstiegspro-

Quelle: AdobeStock

jekte. Für alle diese Anwendungsfälle haben Unternehmen in der Regel bereits eine umfangreiche Datenbasis – die Herausforderung liegt vor allem darin, sie nutzbar zu machen.

Häufig lagert das vorhandene Unternehmenswissen nämlich weit verteilt über verschiedene Clouds und Speichersysteme an mehreren Standorten und steckt in unterschiedlichen Datenbanken, Anwendungen und Fileshares mit Dokumenten fest. Teilweise werden die Informationen zwar in Data Warehouses und Data Lakes zusammengeführt, doch das geht mit einem komplexen Geflecht aus Daten-Pipelines einher. Damit dieses nicht noch komplizierter wird und Mitarbeiter nicht unnötig Zeit mit der Suche, Prüfung und Bereinigung von Daten verschwenden, benötigen Unternehmen neue Ansätze beim Datenmanagement – sowohl technisch als auch organisatorisch.

Auf technischer Seite liefern moderne Management-Plattformen wie Dell Data Lakehouse mit einer flexiblen Analytics-Engine eine einheitliche Sicht auf alle Daten – unabhängig davon, wo sie gespeichert sind. Sie müssen nicht mehr in monolithischen Strukturen gesammelt werden, sondern können für Analysen direkt am ursprünglichen Speicherort abgerufen werden. Dabei kümmern sich die Plattformen um ein intelligentes Zwischenspeichern der Daten oder der Ergebnisse von Abfragen, um hohe Lasten auf den Bestandssystemen zu vermeiden. Deren teure und aufwendige Modernisierung ist daher in den meisten Fällen nicht notwendig, und auch die Pflege unzähliger ETL-Prozesse (Extract, Transform, Load) für das Zusammenführen von Daten entfällt.

Mit einer solchen Management-Plattform schaffen Unternehmen zugleich die Grundlage für organisatorische Veränderungen, die die Bereitstellung von Daten für das Training von KI-Modellen oder für Auswertungen durch KI-Anwendungen erleichtern. Dabei geht es vor allem um die Betrachtung von Daten als Produkt und dezentrale Verantwortlichkeiten, sprich: Statt des IT-Teams kümmern sich ausgewählte Datenproduzenten in den Fachbereichen um die Pflege ihrer Daten und stellen sie als einfach nutzbares Datenprodukt bereit. Auf diese Weise erhalten Nutzer saubere und qualitativ hoch-

wertige Datensätze und nicht einfach nur Rohdaten oder einen Datenbankzugriff. Den Verantwortlichen für das jeweilige Datenprodukt obliegt es sicherzustellen, dass ihr Produkt optimal zu den Anwendungsfällen passt und gegebenenfalls weiterentwickelt wird, wenn sich die Anforderungen an die Daten ändern.

Größer ist nicht immer besser

Passgenaue Datenprodukte ermöglichen ein effizientes Training oder Fine-Tuning von KI-Modellen und helfen, Hardware-Anforderungen zu reduzieren – und damit auch die Anschaffungs- und Betriebskosten. Viele Unternehmen haben dies mangels Erfahrung mit KI-Projekten nicht im Blick und wollen insbesondere Modelle für generative KI mit möglichst allen verfügbaren Informationen füttern, auch wenn das für die gewünschten Anwendungsfälle gar nicht notwendig ist. Sie glauben, Highend-Systeme, große Modelle und viele Daten seien wichtig, um keine Chancen zu verpassen, wodurch die Kosten erheblich steigen und sich die Projektlaufzeiten deutlich verlängern.

UNTERNEHMEN BENÖTIGEN EINE EINHEITLICHE SICHT AUF ALLE DATEN, UM SIE FÜR ANALYSEN DIREKT AM SPEICHERORT ABRUFEN ZU KÖNNEN. EINE ZENTRALE SAMMLUNG IN MONOLITHISCHEN STRUKTUREN IST DANN ÜBERFLÜSSIG.

Roland Kunz, Principal Systems Engineer for Emerging Technologies EMEA, Dell Technologies, www.delltechnologies.com

Für einen internen Chatbot oder KI-Assistenten zum Beispiel wird aber meist kein Large Language Model mit der größtmöglichen Anzahl von Parametern benötigt. Ein solches eignet sich zwar für ein breites Einsatzspektrum, weil es über unglaublich viel öffentlich zugängliches Wissen verfügt, doch beim Einsatz in den Fachbereichen eines Unternehmens kommt es vor allem auf domänenspezifisches Know-how an. Besser geeignet sind daher kleinere, möglichst schon mit Spezialwissen vortrainierte Modelle, die dann noch mit internem Wissen angereichert werden.

Dieses interne Wissen kann dem Modell mittels Fine-Tuning antrainiert oder mittels Retrieval Augmented Generation (RAG) zur Verfügung gestellt werden. Ein Fine-Tuning ist aufwendiger und erfordert mehr Rechenressourcen. Dafür sind die unternehmensspezifischen Informationen fest in das Modell integriert, das sich auch gut auf die fachspezifische Terminologie versteht. Ändert sich das Wissen oder kommt neues Wissen hinzu, ist ein erneutes Training notwendig. Daher lohnt es sich, die Datenbasis sorgfältig auszuwählen, um der KI nicht immer wieder Unnötiges beizubringen und Ressourcen zu verschwenden.

Bei RAG hingegen fließt das interne Wissen aus Datenbanken und Dokumenten – etwa Handbüchern oder technischen Dokumentationen – in eine Vektordatenbank ein, auf die das Modell zugreifen kann. Bei Anfragen sucht es dort nach Informationen und nutzt dann seine bestehenden generativen Fähigkeiten, um diese aufzubereiten. Dadurch ist seine Wissensbasis stets aktuell. Möglicherweise hat das Modell aber Schwierigkeiten mit bestimmten fach- oder unternehmensspezifischen Begriffen und Formulierungen oder dem kontextuellen Verständnis. In solchen Fällen können Fine-Tuning und RAG kombiniert werden: Das Fine-Tuning sorgt dafür, dass das Modell die Anfragen besser versteht und fachgerecht formulierte Antworten liefert, während RAG sicherstellt, dass das Modell jederzeit auf relevante und aktuelle Daten zugreifen kann.

Beratung verhindert Fehlinvestitionen

Um die Anschaffung neuer Hardware zu vermeiden, nutzen Unternehmen für KI-Experimente gerne die Cloud. Diese birgt allerdings Herausforderungen im Bereich der Data Governance und eignet sich aufgrund hoher Latenzen nicht für jeden Anwendungsfall. Zudem unterschätzen Unternehmen leicht die Kosten, die durch Datentransfers, Datenspeicherung und die Nutzung von Compute-Ressourcen entstehen – gerade, wenn die Experimente später ausgeweitet werden. Dann ist es aber oft schon zu spät und der Umzug zurück ins eigene Rechenzentrum nur noch mit großem Aufwand und hohen Kosten möglich. Infrastrukturen on-premises sind für KI daher meist von Anfang an die bessere Wahl – es gilt das Motto: Nicht die Daten zur KI bringen, sondern die KI zu den Daten, und die befinden sich weiterhin vor allem in zentralen Rechenzentren und am Edge, wo etwa die Hälfte aller neuen Daten generiert wird.

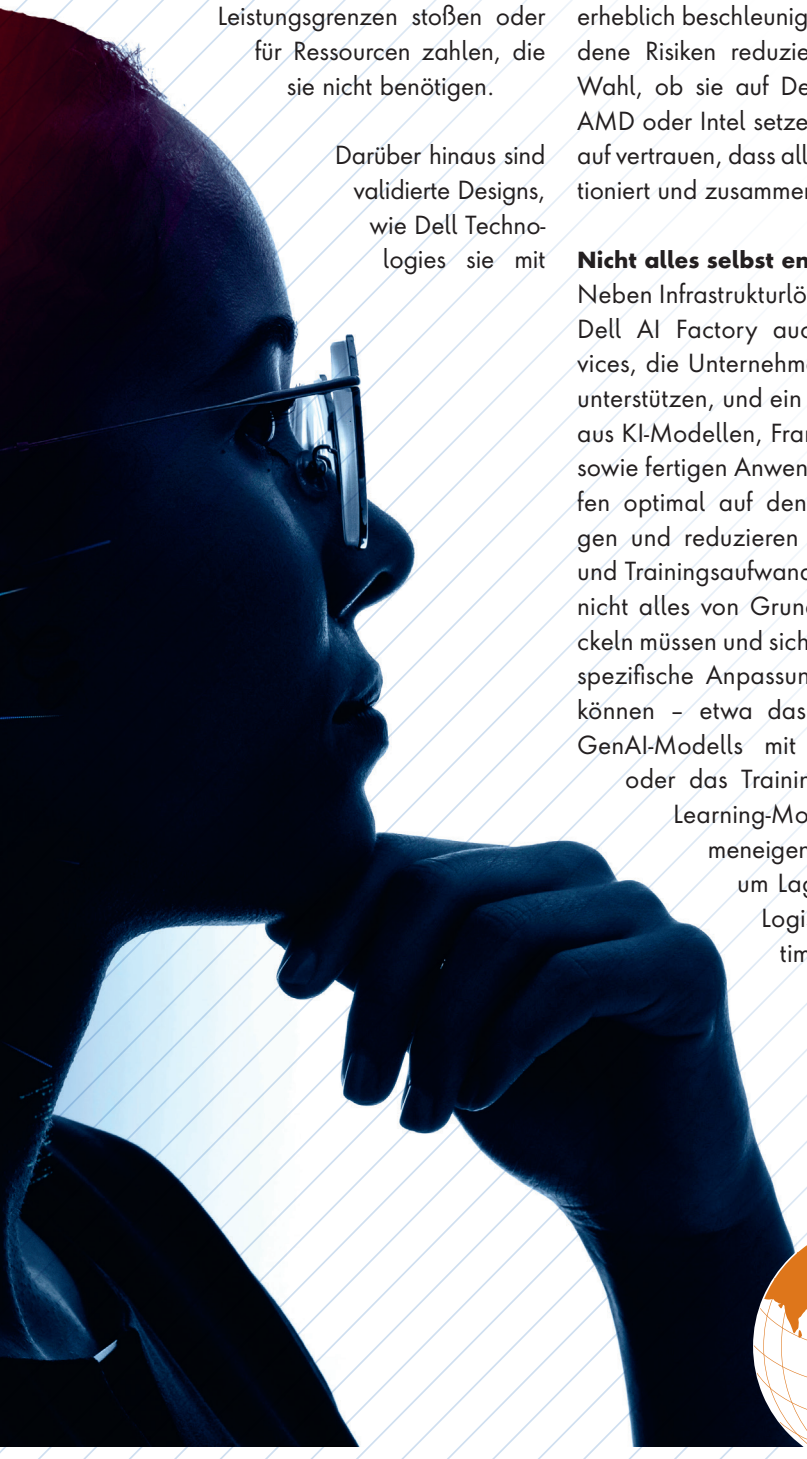
Um Fehlinvestitionen zu vermeiden, sollten Unternehmen zunächst in eine gute Beratung investieren. Erfahrene Systemhäuser und IT-Dienstleister unterstützen bei der Auswahl geeigneter Anwendungsfälle für den KI-Einstieg, der Modernisierung des Datenmanagements sowie der Auswahl und Anpassung von KI-Modellen und der benötigten Infrastrukturlösungen. Bei Bedarf können sie auch deren Betrieb übernehmen.

Wichtig ist, dass die ausgewählten IT-Systeme optimal zum jeweiligen Anwendungsfall passen – unter Umständen

DELL AI FACTORY

reicht schon eine leistungsstarke Workstation für das lokale Training eines Modells aus – und gut skalieren, damit sie sich später problemlos erweitern lassen. Mit Pay-per-Use- und As-a-Service-Modellen vermeiden Unternehmen zudem hohe Anfangsinvestitionen und eine teure Überprovisionierung von Storage- und Compute-Ressourcen. Diese wachsen dynamisch mit, sodass Unternehmen nicht irgendwann an Kapazitäts- oder Leistungsgrenzen stoßen oder für Ressourcen zahlen, die sie nicht benötigen.

Darüber hinaus sind validierte Designs, wie Dell Technologies sie mit der Dell AI Factory bereitstellt, ausgesprochen hilfreich. Dabei handelt es sich um Systemarchitekturen, die bewährte und getestete Komponenten in der optimalen Konfiguration zusammenführen und sich genau an die Anforderungen bestimmter Anwendungsfälle wie Chatbots oder KI-Assistenten anpassen lassen. Unternehmen sparen sich somit umfangreiche Planungen, Integrationen und Tests, was die Infrastrukturbereitstellung erheblich beschleunigt und damit verbundene Risiken reduziert. Sie haben die Wahl, ob sie auf Designs mit NVIDIA, AMD oder Intel setzen, und können darauf vertrauen, dass alles reibungslos funktioniert und zusammenspielt.



Nicht alles selbst entwickeln

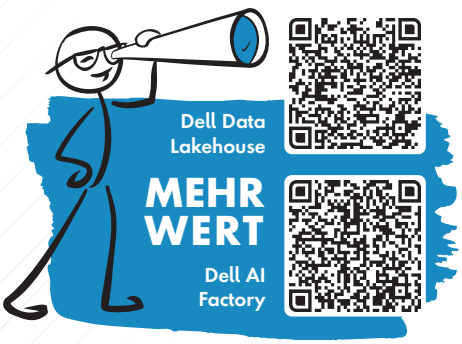
Neben Infrastrukturlösungen umfasst die Dell AI Factory auch zahlreiche Services, die Unternehmen bei KI-Projekten unterstützen, und ein großes Ökosystem aus KI-Modellen, Frameworks und Tools sowie fertigen Anwendungen. Diese laufen optimal auf den Infrastrukturlösungen und reduzieren den Entwicklungs- und Trainingsaufwand, da Unternehmen nicht alles von Grund auf selbst entwickeln müssen und sich auf unternehmensspezifische Anpassungen konzentrieren können – etwa das Fine-Tuning eines GenAI-Modells mit internem Wissen oder das Training eines Machine-Learning-Modells mit den firmeneigenen Bestandsdaten, um Lagerverwaltung und Logistikprozesse zu optimieren.

VALIDIERTE DESIGNS, DIE BEWÄHRTE KOMPONENTEN IN DER OPTIMALEN KONFIGURATION ZUSAMMENFÜHREN, BESCHLEUNIGEN DIE BEREITSTELLUNG VON INFRASTRUKTUREN FÜR KI UND REDUZIEREN DIE RISIKEN.

Peter Dümig, Senior Server Product Manager, Dell Technologies, www.delltechnologies.com

Mit einem modernen Datenmanagement und KI-optimierten Infrastrukturen, die nahtlos mitwachsen, gelingt Unternehmen die Bereitstellung von KI in jeder Größenordnung und an jedem Standort. Braucht es die ersten Projekte noch, um Erfahrung zu sammeln und effiziente Prozesse aufzubauen, entsteht bald eine gut geölte Maschinerie, mit der sich neue Anwendungsfälle zügig und risikoarm umsetzen lassen – um quasi industriell immer neue Erkenntnisse aus Daten zu gewinnen, die die Innovationskraft und Wettbewerbsfähigkeit stärken.

Peter Dümig, Roland Kunz



Steampunk, Clean Core und BTP

SAP-WERKZEUGKASTEN FÜR DIE CLOUD

Die BTP ist eine zentrale Komponente für Unternehmen, die ihre SAP-Systemlandschaft modernisieren und digitalisieren möchten. Sie ermöglicht es Unternehmen, flexibler und agiler zu werden, Innovationen voranzutreiben und die Vorteile der Cloud zu nutzen.

Trotz einiger Herausforderungen bietet die BTP eine Vielzahl von Möglichkeiten, die SAP-Systemlandschaft zu verbessern und zu erweitern. Sie kann als Brücke zwischen der On-prem- und der Cloud-Welt fungieren. Die Einrichtung und der Betrieb der BTP-Komponenten können allerdings kostspielig und wartungsintensiv sein.

Clean Core, ABAP, BTP und Steampunk bilden ein wichtiges Zusammenspiel, das es SAP-Bestandskunden ermöglicht, ihre SAP-Systeme zu modernisieren, flexibler zu werden, Innovationen voranzutreiben und die Vorteile der Cloud zu nutzen. Die BTP wird zum zentralen Element der SAP-Strategie positioniert und bietet die Möglichkeit zur Individualisierung von SAP-Systemen, während der ERP-Kern standardisiert und sauber bleibt. Die BTP ist eine komplexe Plattform, die ein tiefes Verständnis für ihre Funktionalitäten erfordert. Daher gibt es noch viele Fragezeichen bezüglich des Billing-Systems, der technischen Basis und der zu verwendenden Programmiersprache.

Komplexität reduzieren

Nicht alle SAP-Bestandskunden haben sich bisher ausreichend mit der BTP auseinandergesetzt. Es gibt Bedenken hinsichtlich der fehlenden Customizing-Möglichkeiten, insbesondere in der Public Cloud. Die Einarbeitung in die BTP erfordert Zeit und Mühe, da neue Architekturen und Technologien erlernt werden müssen. Clean Core ist eine Strategie, die darauf abzielt, den Standard-ERP-Kern so wenig wie möglich durch kundenspezifische Anpassungen zu verändern. Der ERP-Kern soll „sauber" und standardisiert bleiben. Durch die Trennung von Standardprozessen und Individualentwicklungen sollen zukünftige Upgrades und Release-Wechsel einfacher, schneller und kostengünstiger durchgeführt werden. Die Komplexität des ERP-Systems soll reduziert und die Wartbarkeit erhöht werden. Um die Clean Core-Strategie umzusetzen, werden Anpassungen und Erweiterungen auf der SAP Business Technology Platform (BTP) vorgenommen.

ABAP (Advanced Business Application Programming) ist eine von SAP entwickelte Programmiersprache, die hauptsächlich für die Entwicklung von Anwendungen im SAP-Umfeld verwendet wird. ABAP ist seit Jahrzehnten ein wichtiges Werkzeug für SAP-Bestandskunden, um individuelle Anpassungen und Erweiterungen im ERP-System vorzunehmen. Mit der Einführung der BTP und der Clean Core-Strategie erfährt ABAP eine Modernisierung. SAP bietet nun das ABAP-Cloud-Entwicklungsmodell an, das es ermöglicht, upgradestabile und cloudfähige Lösungen und Erweiterungen zu bauen. Embedded ABAP (Steampunk) ist eine Möglichkeit, ABAP im Kontext der BTP zu nutzen.

https://e3mag.com/de/steampunk-summit/

STEAMPUNK & BTP SUMMIT 2025

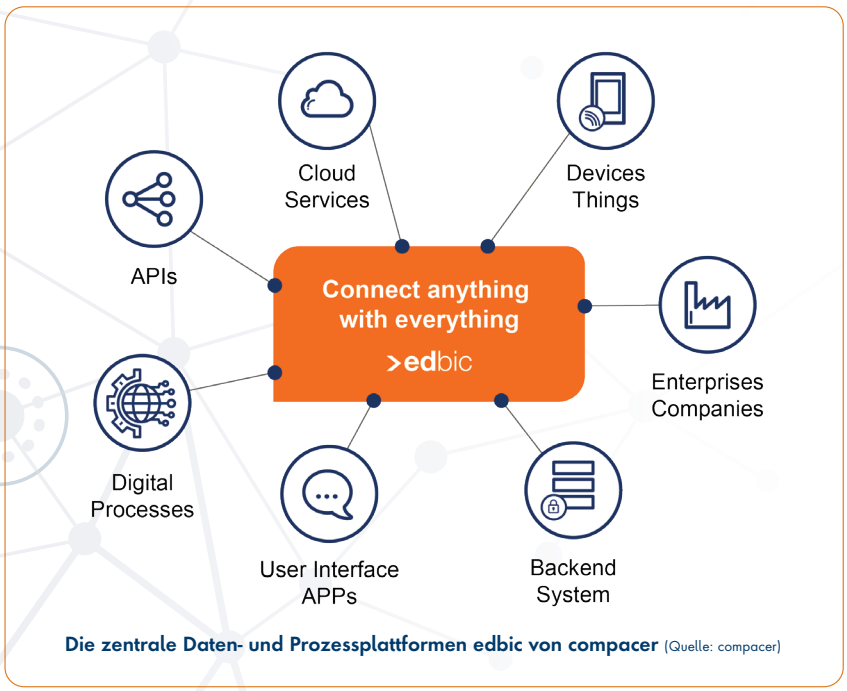
Alle diese Themen und Herausforderungen werden auf dem Steampunk und BTP Summit der SAP-Community am 5. und 6. März 2025 in Heidelberg präsentiert und diskutiert. Exklusiv für die Leser des IT-Verlag bieten wir den Promocode: stpITV2025. Damit können sie einen reduzierten Ticketpreis beziehen. Mit einem Rabatt von 25 Prozent jetzt anmelden!

Digitale Transformation in der Logistik

ZENTRALE DATEN- UND PROZESSPLATTFORMEN STELLEN WEICHEN FÜR DIE ZUKUNFT

Laut einer Prognose von Statista betrug der Umsatz in der Logistikbranche in Deutschland 2024 rund 331 Milliarden Euro. Das sind etwa 19 Prozent mehr als 2019. Den Umsatz generieren Unternehmen wie beispielsweise Kühne+Nagel, DHL und DB Schenker in den Bereichen Transport, Umschlag, Lager, Spedition und Verpackung. Damit ist die Logistikbranche in Deutschland der zweitwichtigste Wirtschaftszweig – noch vor dem Maschinenbau und dem Chemie-Sektor.

Von jeher ist in der Logistik ein Maximum an Flexibilität gefragt - und das nicht nur, um im Fall von Lieferengpässen schnell und angemessen reagieren zu können. Auch die Veränderungen in der Weltwirtschaft werden stetig dynamischer. Da sich Unternehmen mit hohem Digitalisierungsreifegrad leichter tun, diesem Wandel erfolgreich zu begegnen, sollten die Logistikunternehmen ihre Digitalisierungsprojekte unbedingt vorantreiben. Schließlich entscheiden das Sammeln, Verarbeiten und Auswerten von Daten immer mehr über Erfolg oder Misserfolg eines Unternehmens.



Die zentrale Daten- und Prozessplattformen edbic von compacer (Quelle: compacer)

Warum also nicht auf moderne Technologien und Plattformen setzen, die Daten aus unterschiedlichen Systemen einsammeln, konsolidieren und nutzbar machen?

Zentrale Daten- und Prozessplattformen in der Praxis

Seit einigen Jahren sind zentrale Daten- und Prozessplattformen auf dem Markt, wie beispielsweise edbic von compacer, die den Austausch von Informationen zwischen verschiedenen Systemen und Prozessbeteiligten erleichtern. Die Integration der Daten sowie die Vernetzung von Geschäftspartnern, Systemen und Geräten innerhalb der gesamten Wertschöpfungskette ist ein erster wichtiger

Schritt hin zu intelligenten Geschäftsprozessen.

Damit eine solche Daten- und Prozessplattform möglichst wirkungsvoll ist, sollte sie sich unkompliziert in die bestehende IT-Umgebung integrieren – idealerweise über standardisierte Schnittstellen und die Nutzung gängiger Datenformate, etwa EDIFACT oder moderne RESTful APIs. Wer im eigenen Unternehmen zudem auf die Skalierbarkeit der Cloud-basierten Infrastruktur setzt, muss diese auch durch einen leistungsstarken Data-Hub unterstützen können. Eine Plattform wie edbic bietet darüber hinaus den Einsatz von Microservice-basierten Architekturen an, was zahlreiche Vorteile mit sich bringt – etwa, dass komplexe Anwendungen in kleine, unabhängige Dienste aufgesplittert werden können, die jeweils eine spezifische Funktion erfüllen und unabhängig voneinander entwickelt, bereitgestellt und skaliert werden können.

Die Einführung einer Daten- und Prozessplattform lohnt sich schon allein deshalb, weil sie einen reibungslosen Datenaustausch und automatisierte Workflows bietet, die helfen Kosten und Zeit zu sparen sowie Risiken zu minimieren. So entstehen nicht nur mehr Agilität, Sicherheit und validere Prozesse, sondern auch Quick Wins entlang der gesamten Wertschöpfungskette.

So lassen sich Daten- und Prozessplattformen optimal nutzen

#1 Integration von IoT-Technologien

Die Integration von IoT-Technologien, zum Beispiel über die Einbindung von Sensoren, ermöglicht die Echtzeitüberwachung von physischen Assets, wie beispielsweise Containern, Fahrzeugen, Ausrüstungen etc.

#2 Berücksichtigung von Big Data und Analytics

Die Nutzung von Big-Data-Technologien und Analytics kann dazu beitragen, wertvolle Erkenntnisse aus den umfangrei-

DIESE IT-TRENDS PRÄGEN DIE LOGISTIK 2025

Integration von Künstlicher Intelligenz (KI) und Maschinellem Lernen (ML)

Künstliche Intelligenz und Maschinelles Lernen werden zur Analyse großer Datenmengen eingesetzt, um Muster zu erkennen, Vorhersagen zu treffen und automatisierte Entscheidungen zu ermöglichen. Dies kann zur Optimierung von Logistikprozessen und zur effizienteren Ressourcennutzung beitragen.

Mehr Vertrauen durch Blockchain-Technologie und digitale Identitäten

Die Integration von Blockchain trägt zur Verbesserung der Transparenz, Integrität und Sicherheit von Transaktionsdaten bei. Die Blockchain-Technologie kann dabei helfen, Vertrauen zwischen den Parteien zu schaffen und den Austausch von Informationen zu vereinfachen. Die Implementierung digitaler Identitäten sowie sicherer Authentifizierungsmethoden sorgt dafür, dass nur autorisierte Benutzer auf die Daten zugreifen können.

Automatisierung und Robotik

Der Einsatz von Automatisierungstechnologien und Robotik kann die Effizienz von Be- und Entladevorgängen verbessern und damit den Gesamtprozess beschleunigen.

Interoperabilität IoT, Sensornetzwerke

Fortgesetzte Bemühungen um die Verbesserung der Interoperabilität zwischen verschiedenen Logistiksystemen sowie die Einhaltung offener Standards, unterstützt die nahtlose Integration zentraler Steuerungsplattformen in die globale Lieferkette. Die erweiterte Nutzung des IoT und von Sensornetzwerken hilft bei Echtzeitüberwachung physischer Assets und ermöglicht eine präzisere Nachverfolgung sowie eine verbesserte, operative Effizienz.

Predictive Analytics für bessere Planung

Predictive Analytics wird verstärkt angewendet, um zukünftige Entwicklungen vorherzusagen und eine proaktive Planung und Wartung zu ermöglichen. Dies kann dazu beitragen, Engpässe zu vermeiden und die Effizienz zu steigern.

5G & Edge für mehr Schnelligkeit

Die Nutzung von 5G-Technologie gewährleistet eine schnellere und zuverlässigere Konnektivität. Dies ist besonders wichtig für die Echtzeitübertragung großer Datenmengen. Der Einsatz von Edge Computing in der Datenverarbeitung führt zu schnelleren Reaktionszeiten und einer effizienteren Nutzung von Netzwerkressourcen.

chen Datenmengen zu gewinnen, die im Laufe eines Logistikprozesses generiert werden.

#3 Mobile Anwendungen

Die Entwicklung mobiler Anwendungen für verschiedene Benutzergruppen ermöglicht einen flexiblen und standortunabhängigen Zugriff auf die Managementsysteme. Das bietet insbesondere Logistikfachkräften, Inspektoren und anderen mobilen Nutzern zahlreiche Vorteile.

#4 Sicherheits- und Datenschutzmaßnahmen

Die Implementierung umfassender Sicherheits- und Datenschutzmaßnahmen schützt sensitive Informationen und umfasst die Verschlüsselung, Zugangskontrollen, Überwachung und Audits.

DAS SAMMELN, VERARBEITEN UND AUSWERTEN VON DATEN ENTSCHEIDET IMMER MEHR ÜBER ERFOLG ODER MISSERFOLG EINES UNTERNEHMENS.

Volker Hettich, Chief Strategy Officer, compacer GmbH, www.compacer.com

#5 Robuste Ausfallsicherheit und Redundanz

Die Plattform sollte über Mechanismen für die Ausfallsicherheit und Redundanz verfügen, um sicherzustellen, dass auch bei technischen Problemen oder Ausfällen zuverlässig gearbeitet werden kann.

Unternehmen, die eine solche Plattform einführen, werden schnell feststellen, dass sie von zahlreichen Mehrwerten profitieren, wie etwa einer Vereinfachung der Geschäftsprozesse. Vor allem aber sorgt eine solche Neuausrichtung dafür, dass ihre Prozesse wesentlich unkomplizierter an veränderte Rahmenbedingungen, beispielsweise Änderungen im Lieferkettengesetz oder bei Zöllen, angepasst werden können. Diese Agilität kann im harten Wettbewerb der Logistik ein entscheidender Vorteil sein.

Volker Hettich

CHATGPT POWER-PROMPTING

PROFI-STRATEGIEN FÜR DEN ERFOLGREICHEN EINSATZ VON KI

Mit diesem Praxisbuch lernen Sie alle Techniken, um das Potenzial von ChatGPT und ähnlicher KIs voll auszuschöpfen. Sie erfahren, wie Sie zielgerichtete Prompts schreiben und mit der KI interagieren, um qualitativ hochwertige Ergebnisse zu erhalten, die genau Ihren Anforderungen entsprechen. Ganz gleich, ob Sie ChatGPT im Berufsalltag oder privat einsetzen – dieses Buch führt Sie Schritt für Schritt zum Erfolg.

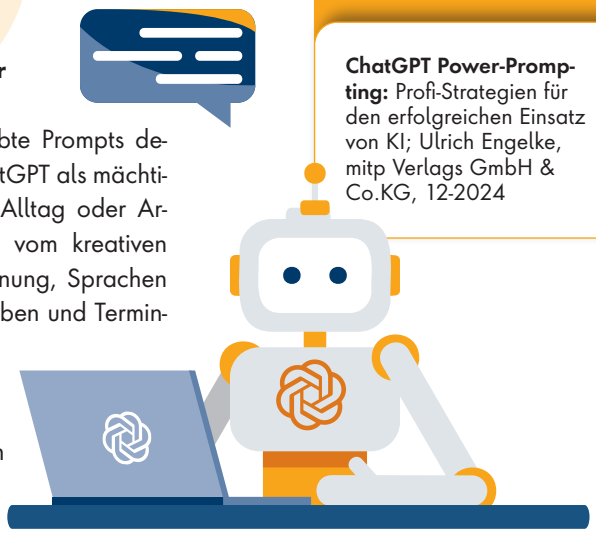
Systematischer Leitfaden für Einsteiger und Profis

Dieses Buch bietet eine umfassende Einführung in das professionelle Prompt Engineering. Erfahren Sie, wie Sie ChatGPT bestimmte Rollen zuweisen, Kontext und Zielgruppe genau festlegen und differenzierte Antworten erzielen. Diese grundlegenden Techniken sowie das Erstellen von Custom GTPs ermöglichen es Ihnen, die KI gezielt zu steuern und für jeden Anwendungsfall optimale Ergebnisse zu erhalten.

ChatGPT effektiv in der Praxis einsetzen

Über 1.000 praxiserprobte Prompts demonstrieren, wie Sie ChatGPT als mächtiges Werkzeug in Ihren Alltag oder Arbeitsprozess integrieren: vom kreativen Schreiben über Reiseplanung, Sprachen lernen Bewerbungsschreiben und Terminplanung bis hin zu Marketing und Serien-Mails. So sind sie perfekt auf den Einsatz von ChatGPT in der Praxis vorbereitet.

ChatGPT Power-Prompting: Profi-Strategien für den erfolgreichen Einsatz von KI; Ulrich Engelke, mitp Verlags GmbH & Co.KG, 12-2024



IT-Fachkräftemangel

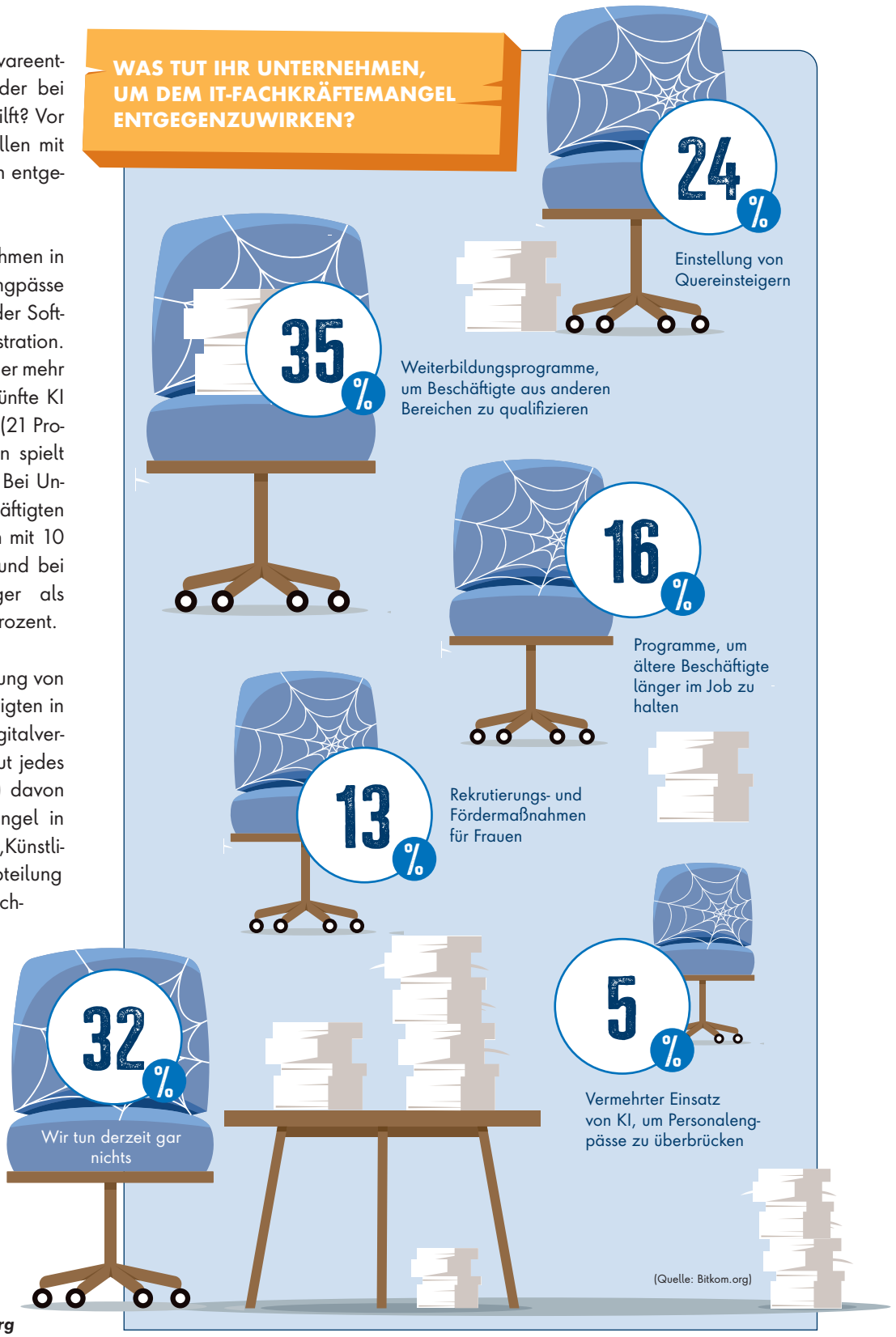
GROSSE UNTERNEHMEN SETZEN AUF KÜNSTLICHE INTELLIGENZ

Künstliche Intelligenz in der Softwareentwicklung oder ein KI-Chatbot, der bei PC-Problemen im Unternehmen hilft? Vor allem größere Unternehmen wollen mit KI dem Mangel an IT-Fachkräften entgegenwirken.

So geben 5 Prozent der Unternehmen in Deutschland an, mit KI Personalengpässe überbrücken zu wollen, etwa in der Softwareentwicklung oder IT-Administration. Von den Unternehmen mit 250 oder mehr Beschäftigten setzt sogar jedes fünfte KI gegen den Fachkräftemangel ein (21 Prozent). Bei kleineren Unternehmen spielt KI eine deutlich geringere Rolle: Bei Unternehmen mit 50 bis 249 Beschäftigten sind es nur 12 Prozent, bei jenen mit 10 bis 49 Beschäftigten 7 Prozent und bei Kleinst-Unternehmen mit weniger als zehn Beschäftigten sogar nur 2 Prozent.

Das sind Ergebnisse einer Befragung von 852 Unternehmen ab 3 Beschäftigten in Deutschland im Auftrag des Digitalverbands Bitkom. Insgesamt geht gut jedes dritte Unternehmen (35 Prozent) davon aus, dass KI den Fachkräftemangel in Deutschland abmildern kann. „Künstliche Intelligenz kann eine IT-Abteilung nicht ersetzen. KI kann aber IT-Fachkräfte bei den unterschiedlichsten Aufgaben unterstützten und zum Beispiel bei Problemen und Fragen aus dem Team oft ebenso gute Unterstützung bieten wie ein menschlicher Support“, sagt Bitkom-Hauptgeschäftsführer Dr. Bernhard Rohleder. „KI kann zudem bei eher langweiligen Aufgaben oder solchen, die eine langanhaltend hohe Konzentration erfordern, helfen.“

www.bitkom.org



Zu viele Chiefs, zu wenig Mensch

AUF DIE PRIORITÄTEN KOMMT ES AN

CTO, CIO, CDO, CAIO – mit jeder technischen Welle ein neuer Chief. Kurz: C-irgendwas-mit-Tech-O, der "CIMTO". Wo bleibt da der Mensch im Strudel technologischen Wandels? Ein Plädoyer für die richtige Priorität.

Gebt mir ein C, gebt mir ein T...

Jede Welle technologischer Entwicklungen zieht offenbar auch unweigerlich eine neue Rolle im C-Level nach sich. Erst waren es der Chief Technology Officer und Chief Information Officer. CTO vor allem für Technologie im Außenverhältnis, zweitgenannter für den Fokus auf das Innere der Organisation. Danach der Chief Digital Officer, denn die Welt war plötzlich digital beziehungsweise sollte es schnellstmöglich werden. Und jetzt, auf der aktuellen Stufe der Digitalisierung: der Chief Artificial Intelligence Officer. Der CAIO also.

Offenbar leistet man sich im Hype um die neue General Purpose Technology sogar einen Buchstaben mehr und bricht aus dem gewohnten Buchstaben-Dreiklang aus. Warum auch nicht. Es scheint ja wirklich wichtig zu sein, denn schließlich spricht alle Welt über KI und selbst Nobelpreise gibt es inzwischen dafür. CTO, CIO, CDO, CAIO - und als nächstes dann CQCO für Chief Quantum Computing Officer? Klingt dann doch alles irgendwie beliebig. Warum also nicht gleich noch einen fünften Buchstaben oben drauf und „CIMTO" für „C-irgendwas-mit-Tech-O"?

Mensch, wo hakt es denn?

Wie auch immer man die Position nennen mag. Zunächst ist es natürlich wichtig, dass Technologie als Thema auf Board-Level verortet ist. Es braucht im neuen Maschinenzeitalter eine Rolle mit Entscheidungsgewalt und Überblick. Ohne wird heute und morgen kein größeres Unternehmen überleben können.

Was aber fehlt, ist der Fokus auf diejenigen, die von Technologie betroffen sind - und das sind zuallererst die Mitarbeitenden. Mit Fokus sind hier keine Lippenbekenntnisse in Sonntagsreden gemeint, sondern echte Priorität. Was einer glaubwürdigen und wirksamen Priorisierung des Faktor Mensch im Wege steht - eine kurze Vorstellung in drei Akten:

#1 Die Person:

Glaubwürdig wird Priorität zunächst über die Person, die die C-Rolle ausfüllt. Was ist der „CIMTO" für ein Fabelwesen? Es geht ja schließlich um fundamentale Transformationen mit Implikationen für das, was uns allen schon aus naturgemäßem Egoismus am wichtigsten ist: den Menschen. Sind CTO, CIO, CDO und CAIO also Menschen mit einem Background in HR, Psychologie, Soziologie oder Philosophie? Natürlich nicht - der Hintergrund ist, zunächst logisch, IT und/oder General Management. Idealerweise also der Techie mit Blick fürs Business. So werden und sind die meisten dieser Positionen besetzt. Häufige Headline: „300.000 Dollar Jahresgehalt für den CAIO" statt „Tech-affine Sozialwissenschaftler kapern C-Level".

#2 Die Integration:

Selbstredend kann auch eine Person ohne fachlichen Hintergrund mit Fokus Mensch für die Belange von Beschäftigten eintreten, kann in der Mission Digital den Menschen in den Mittelpunkt rücken. Dafür braucht ein „CIMTO" aber den Auftrag. Den hat aber schon jemand anderes: der Personaler. Entweder CHRO oder Personalleiterin unter C-Level. Wer bekommt nun also den Auftrag für die humanzentrierte Begleitung technologischer Themen? Meistens HR, und falls beide, muss sich auf Augenhöhe und mit Respekt begegnet werden, muss echte Zusammenarbeit über sehr lange Zeit stattfinden. Einen derartigen Schulterschluss sieht man selten. Stattdessen viele Silos: HR für Faktor Mensch versus „CIMTO" für Tech. So wird das dann doch eher nichts.

#3 Der Blickwinkel:

Wirkliche Priorität hat der Mensch nur dann, wenn man nicht auf die Technologie, sondern die Technologiefolgen blickt. Interessant ist also weniger, welche Architektur eine Software hat, sondern was diese Software mit der Architektur des Menschen macht. Und für diesen Blickwinkel ist Fachwissen aus der Psychologie, speziell zur Anwendung dieser Disziplin auf das Change Management gefragt. Fünf Fragen, die ein „CIMTO" beantworten können muss, aber meist von ChatGPT beantworten lässt:

(a) Was motiviert Beschäftigte, eine Technologie zu nutzen?

(b) Welche Hürden zur Nutzung gibt es in der Belegschaft und wodurch sind diese bedingt?

(c) Welche positiven und negativen Erwartungen haben Mitarbeitende hinsichtlich der Implikationen von Technologie für ihren Job?

(d) Was macht Technologie mit Leistung, Engagement, Gesundheit und Zufriedenheit von Beschäftigten?

(e) Wodurch zeichnen sich Befürworter versus Gegner technologischen Wandels in Erleben und Verhalten aus?

Hat ein „CIMTO" fundierte Antworten auf diese Fragen? Ohne Fundament in der eigenen Person und ohne Rückendeckung durch die Integration mit HR ist das sehr unwahrscheinlich.

Namen sind Schall und Rauch

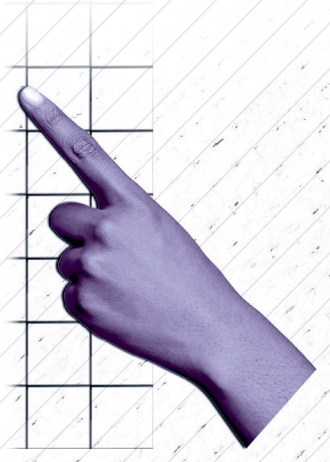
Bevor wir also den nächsten Buchstaben zwischen C und O pressen, sollten wir endlich eine Rolle jenseits von Silos definieren, die die Transformation wirklich humanzentriert begleiten will, kann und darf. Menschen auf dieser Position wandeln zwischen den Welten, zwischen Technologie (in) der Organisation und Psychologie der Belegschaft. Um diesen Weg zu beschreiten, braucht es Rückendeckung, muss sich das Top-Management insgesamt zum Faktor Mensch bekennen und den Wertbeitrag von HR auch in technologischen Fragen erkennen.

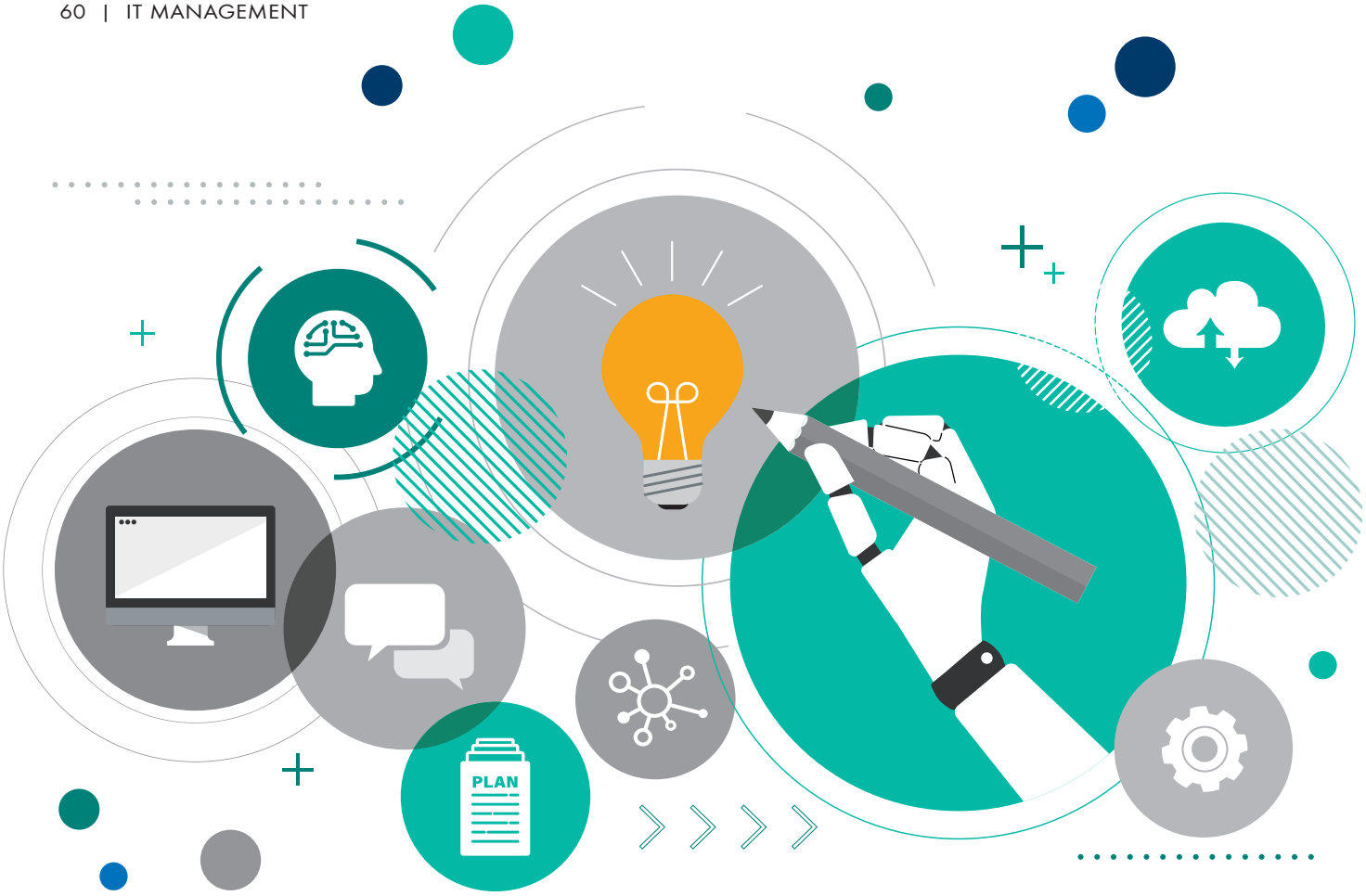
Vielleicht ist die Verwirrung um das neue C im Board ja aber auch ein guter Impuls, den Blick neu zu justieren, weg vom exponierten Individuum hin zum orchestrierten Kollektiv. Denn solange Menschen mit den richtigen Prioritäten und einer geteilten Mission gemeinsam agieren, ist eine Transformation jeder Art weit weniger steinig. Und falls es dann doch beim alten pyramidalen System mit personenzentriertem Heldenkult bleiben soll: Wie wäre es beispielsweise mit dem Chief Human Nature Digital Transformation Integration Officer? Etwas sperrig? Auf den Namen kommt es nicht an. Was zählt, sind Prioritäten - richtig ausgerichtet und richtig ernstgemeint.

Dr. Jens Nachtwei

SOLANGE MENSCHEN MIT DEN RICHTIGEN PRIORITÄTEN UND EINER GETEILTEN MISSION GEMEINSAM AGIEREN, IST EINE TRANSFORMATION JEDER ART WEIT WENIGER STEINIG.

Dr. Jens Nachtwei forscht und lehrt zur Ingenieurpsychologie an der HU Berlin und Hochschule für angewandtes Management.





Welche Kompetenzen verlangt die digitale Transformation?

MUT ZUR INNOVATION JENSEITS DER TECHNOLOGIE

Menschen, Innovationen und moderne Technologien sind die wichtigsten Zutaten für die Entwicklung digitaler Strategien. Eine neue Forschungsarbeit zeigt auf, welche Akteure für die Exploration neuer Möglichkeiten entscheidend sind.

Die Entwicklung einer „echten" digitalen Strategie verlangt nach Mut, Ausdauer und drei wichtigen Ressourcen. Nach dem initialen Impuls braucht es Mut, der neuen Idee zu folgen, und es erfordert Ausdauer, um sie zum Erfolg zu führen. Die drei Ressourcen sind das Budget, die Akteure und natürlich Zeit.

Die Digitalisierung des Geschäftsmodells ist ein reines Innovationsthema. Unternehmen erlangen neue Ideen meist durch Explorationen, die ergebnisoffene Erkundung neuer Möglichkeiten. Es ist immer eine Investition in eine unbekannte Zukunft, welche im disruptiven Internetzeitalter den Fortbestand des Unternehmens sichern soll.

Die Digitalisierung verändert die Kosten, die Produktivität und den Customer Value. So besitzen digitale Plattformen neun Attribute, die eine analoge Organisation niemals alle abdecken kann. Diese Attribute sind: direkt, erreichbar, präzise, transparent, einheitlich, dynamisch, allumfassend, unermüdlich und individuell. Sie können einzeln oder in Kombination wirken. Deshalb sollten alle Unternehmen diese neuen Möglichkeiten kennen und angehen, bevor sie zu einer Bedrohung werden.

Um diese Vorteile auf das eigene Unternehmen zu übertragen, braucht es besondere interne und externe Akteure, die für den Erfolg zusammenarbeiten sollten. Vier Personengruppen sind essenziell für den geschützten Rahmen, die Konzeption, die Koordination und die Umsetzung. Also nach wem verlangt die digitale Transformation?

Menschen vor Technologie

Die Digitalisierung der eigenen Geschäftsmodelle wird oftmals mit moderner Technologie (Web, App und Cloud) gleichgesetzt. Die Studie zeigt jedoch klar, dass die Technologie nur der Auslöser für neue Möglichkeiten ist.

Zur Erklärung: Die Digitalisierung entspringt der Verschmelzung zweier Basistechnologien, dem Computer und dem Internet. Öffnen sich Unternehmen dem Internet, verbinden sie sich über ihre Plattform systemisch mit Kunden, Lieferanten, Partnern und anderen Plattformen.

Mithilfe von Algorithmen werden digitale Angebote – in Form eines selbst handelnden Agenten – entwickelt, die dem Kunden einen Mehrwert liefern. Diese Intelligenz beruht auf neuen Geschäftsmodellen und unterscheidet sich von den traditionellen Geschäftsmodellen analoger Organisationen. Zwei elementare Neuerungen zeichnen die Digitalisierung aus: die Öffnung zum Internet und die digitale Intelligenz. Die Handlungsempfehlung für Unternehmer, angehende Projektleiter und Interessierte lautet sehr prägnant:

„Vergessen Sie die Technologie! Für das Internetzeitalter braucht es neue Ideen, und diese kommen von den Menschen."

Die Studie zeigt auf, dass der Ursprung für den angestrebten wirtschaftlichen Erfolg nicht in der Wahl einer Technologie oder den Versprechen der Technologieanbieter zu finden ist. Digitale Strategien basieren auf einem neuartigen Geschäftsmodell, das den Bauplan für das neue digitale Angebot darstellt. Geschäftsmodelle werden von den Menschen im Unternehmen entwickelt und den Experten, die sie dabei anleiten. Der Aufbau und die Motivation des richtigen Teams sind mit Abstand die schwierigsten Aufgaben für das Vorhaben.

Vorteile digitaler Geschäftsmodelle

Steve Jobs, Gründer von Apple Inc., hat nie über einen traditionellen Schallplattenladen nachgedacht, als er die erste digitale Musikplattform iTunes entwarf. Seine Idee war es, sich dem Internet zu öffnen und die gesamte Musik der Welt den Menschen jederzeit, von überall und besonders einfach zum Download anzubieten.

Die Immanenz von digitalen Geschäftsmodellen beruht auf drei Eigenschaften: Ubiquität, Vernetzung und Intelligenz. Das Geschäftsmodell von iTunes besitzt diese drei Merkmale. Es ist jederzeit und von überall erreichbar (Ubiquität) und es ist vernetzt mit Endkunden, Musikern sowie Produzenten (Vernetzung). Zudem nutzt Apple durchdachte Algorithmen, welche die Musik verwalten, vermarkten und abrechnen (Intelligenz).

Apple sprengt mit seinem digitalen Angebot die physischen Begrenzungen des Schallplattenladens. Es zeigt sich, dass bereits zwei der neun Attribute digitaler Plattformen die Produktivität steigern. Die Plattform arbeitet rund um die Uhr und ist „unermüdlich", denn es gibt keine Begrenzung in den Downloads. Sie bietet mit über 100 Millionen Songs ein „allumfassendes" Angebot. Der Customer Value ist exponentiell gestiegen, die Produktivität ist nahezu unbegrenzt und die Kosten sind auf dem geringstmöglichen Level. Der Schallplattenladen hat keine Chance zu überleben, denn die digitale Welt folgt anderen Gesetzen.

Die Pseudo-Digitalisierung!

Viele Unternehmen starten IT-Projekte und betiteln sie plakativ als den Schritt in die digitale Transformation. Es bleiben aber klassische IT-Projekte, deren Ziel es ist, den Arbeitsaufwand und die Kosten zu senken. Die Projekte sind oftmals isolierte Verbesserungen innerhalb einer Abteilung oder für einen Teilprozess. Es fehlen klare Ziele, eine Strategie und der ganzheitliche Ansatz. Trotz allem sind diese Projekte wichtig, denn in der Summe aller Einzelinitiativen stärken Unternehmen sukzessive ihre Wettbewerbsfähigkeit.

Die Investition in Prozesse und Systeme ist die „leichte" Entscheidung, denn Unternehmen erzielen in der Regel eine spürbare Verbesserung. Die Vorhaben sind übersichtlich, kalkulierbar, beherrschbar, risikoarm und sichern den Status quo. Das Problem ist aber der Status quo, denn das alte analoge Geschäftsmodell wird gefestigt und die Möglichkeiten digitaler Geschäftsmodelle werden ignoriert.

Falsch sind die plakativen Überschriften, denn sie gaukeln eine Digitalisierung vor und liefern am Ende eine Pseudo-Digitalisierung. Unternehmer, Manager und Projektleiter

zeigen sich immer neugierig, doch schnell kommen in den Gesprächen Zweifel und Unbehagen auf. Es fehlt ihnen an Wissen, an den Fähigkeiten und dem Bewusstsein für Veränderungen. Letztlich lehnen sie die Digitalisierung der eigenen Geschäftsmodelle als unvorstellbar ab. Das Resultat ist, dass die Pseudo-Digitalisierung floriert, denn sie ist immer die sichere Entscheidung. Alle Akteure kennen das Prozedere, fühlen sich wohl und sind zufrieden.

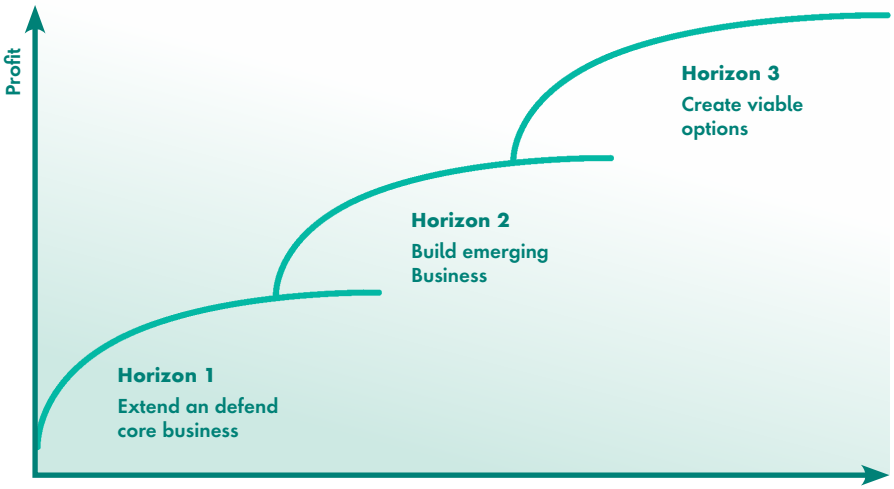
Horizonte bringen Transparenz

Das McKinsey 3 Horizon Framework beschreibt, wie Unternehmen die analoge Organisation stärken und die digitale Zukunft erkunden können. Dieses Modell ist ein strategisches Framework, das Unternehmen dabei hilft, ihre Ziele und Initiativen über einen Zeitraum von drei Horizon zu organisieren.

Horizon 1 Projekte sichern den Status quo. Sie besitzen aber den Nimbus einer Pseudo-Digitalisierung, denn das Level der Geschäftsmodellentwicklung wird nie tangiert. Die Möglichkeiten der digitalen Transformation werden nicht aktiviert.

Der Horizon 2 Ansatz sagt, dass bestehende Geschäftsmodelle um digitale Komponenten erweitert werden. Eine Möglichkeit ist die digitale Entwicklung der Außenbeziehungen. Das heißt, die Interaktion mit Kunden, Lieferanten und Partnern erfolgt durch den systemischen Austausch von Informationen.

MCKINSEY 3 HORIZON FRAMEWORK



Quelle: Baghai, Cloey und White

Für eine Horizon 3 Innovation analysieren Unternehmen ihre Kunden. Es gilt, die Motivation des Endkunden zu hinterfragen, einen höheren Nutzen (Preis, Zeit, Komfort, Ubiquität) zu stiften oder ein Problem des Kunden besser zu lösen.

Der Unternehmer entscheidet, welche Zielsetzung er bei der Entwicklung seiner digitalen Strategie wählt. Möchte er eine Verbesserung des operativen Geschäfts, bewegt er sich im Horizon 1. Wählt er die ergebnisoffene Exploration neuer Opportunitäten zur Sicherung der Zukunft seines Unternehmens, bewegt er sich in Horizon 2 oder 3.

Innovationen mit Experten

Vier Akteure wurden identifiziert, die für den Erfolg der digitalen Transformation dringend gebraucht werden. Im Zusammenspiel der Personen oder Personengruppen ermöglichen sie es, das Wissen, die Methoden und die klare Zielsetzung sowie den Rahmen für die Exploration zu erschaffen.

#1 Top-Management

Jedes Projekt braucht einen Impuls. Sind die bevorstehenden Veränderungen weitgreifend, benötigt es eine starke Persönlichkeit. Die Digitalisierung der Geschäftsmodelle startet auf der Ebene des Middle-Managements oder im Top-Management. Beide Ebenen werden für den initialen Impuls gebraucht und bedingen einander.

Das Umfeld und der Charakter der Initiatoren sind weitere wichtige Komponenten. Unternehmen mit einem hohen Innovationsgrad (Early Adopter) sind eher bereit für Explorationen als andere. Es verlangt den ambitionierten Entscheider (First Mover), der das Potenzial erkennt und mit Mut und Ausdauer vorangeht. Und es braucht einen oder mehrere Promoter, die die Exploration anführen, kommunizieren und schützen. Alle Initiatoren werden als Kosmopolit beschrieben. Sie gelten als weltoffen, informiert, gebildet, multikulturell und IT-affin.

Die Aufgabe des Managements ist es, einen langfristigen Rahmen für die Exploration zu schaffen und die nötigen Ressourcen zu sichern. Mit dem Projektteam werden die Fortschritte diskutiert, neue Schritte

eingeleitet und Erfolge bewertet.

#2 Strategieberatung für die Exploration

Die Studie hat belegt, dass das digitale Geschäftsmodell den wichtigsten Planungsschritt darstellt. Wird dieser Schritt übersprungen, beginnen Unternehmen die Digitalisierung als ein reines Technologieprojekt und investieren ohne Vision, Ziele oder einen Bauplan.

Die Strategieberater – von denen es nur wenige am Markt gibt – starten mit einem Wissenstransfer. In einer spielerischen Vorgehensweise wird versucht, dem Kunden ein besseres digitales Angebot zu unterbreiten. Hierfür hinterfragen sie den Kunden, seine Motivation und Erwartungen. Ideen werden geboren, geprüft, verbessert und verworfen. Ist eine Idee tragfähig, wird sie skaliert, getestet und wieder verbessert. Ist es eine reife Idee, wird das Geschäftsmodell realisiert. Genutzt werden hierfür Business Canvas Modelle, die es erlauben, Geschäftsmodelle mithilfe von sieben Elementen zu beschreiben.

Die Strategieberater sind ausschließlich auf die Erkundung neuer Möglichkeiten fokussiert. In einem explorativen Vorgehen führen sie Teams zusammen, kreieren Ideen, erkunden die Wirkung und verändern nachhaltig das Mindset. Die Berater haben berichtet, dass die Unternehmen nicht nur den ersten Entwurf realisieren, sondern weiter daran arbeiten, die Motivation ihrer Kunden tiefer und tiefer zu analysieren.

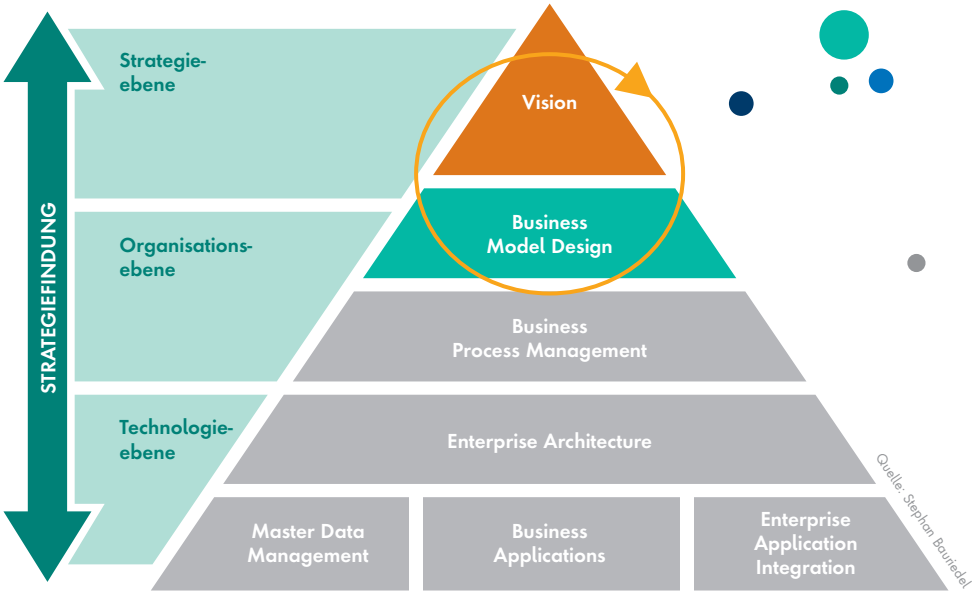
#3 Technologiepartner für die Realisierung

Ist das Geschäftsmodell gereift, geht es um die technische Realisierung. Das Unternehmen wählt eine Technologie und die dazugehörigen Partner aus. Es mag sein, dass es mehrere Technologien und Partner benötigt, um das Vorhaben umzusetzen.

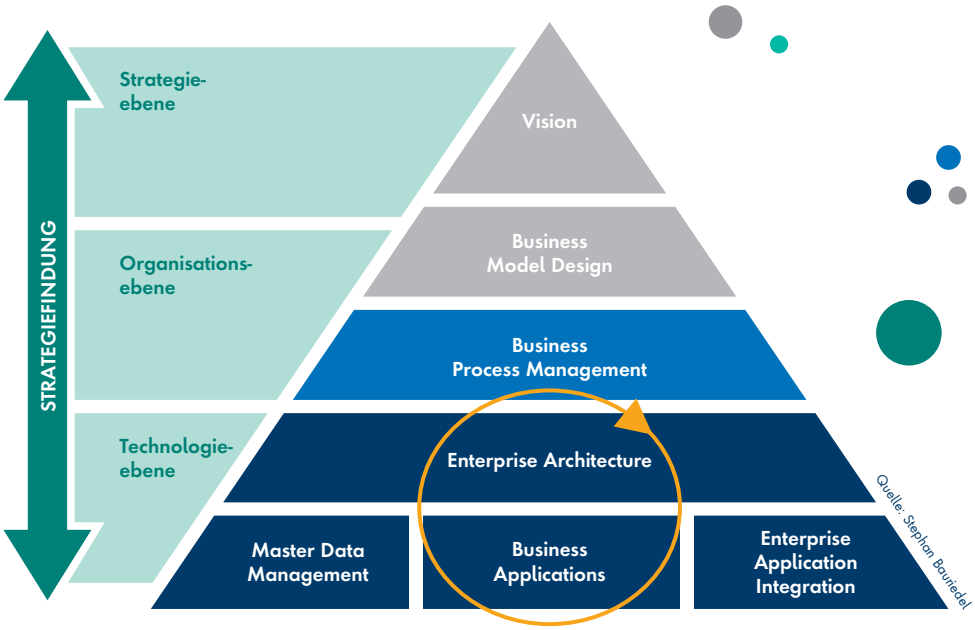
Die Technologiepartner kommen mehrfach ins Spiel und agieren agil. So kann es sein, dass sie aufgefordert werden, ein unreifes Testobjekt zu kreieren, welches erste Teile des Geschäftsmodells abbildet. Sicher ist, dass ein oder mehrere Prototypen erforderlich sind, die zumindest das Kernangebot des Geschäftsmodells umfassen. Anhand der Prototypen kann das Projektteam die Conversion (Nutzung) messen. Dieser Indikator sagt aus, inwieweit Kunden das Angebot annehmen, wieder kommen oder verweilen.

Wichtig ist, dass die Technologiepartner die Intention des Geschäftsmodells kennen und verstehen. Es ist kein technologi-

DIGITAL ACTION MODELL – STRATEGIEBERATER



DIGITAL ACTION MODELL – TECHNOLOGIEPARTNER



sches Konstrukt aus Daten und Funktionen, sondern ein ubiquitäres, vernetztes und intelligentes Angebot für Kunden.

#4 Projektleiter(in) und das interne Projektteam

Der Projektleiter oder die Projektleiterin hat den schwierigsten und spannendsten Job von allen Akteuren. Die Aufgaben sind, die vielfältigen internen und externen Kompetenzen zu koordinieren und natürlich die Gesamtverantwortung zu übernehmen.

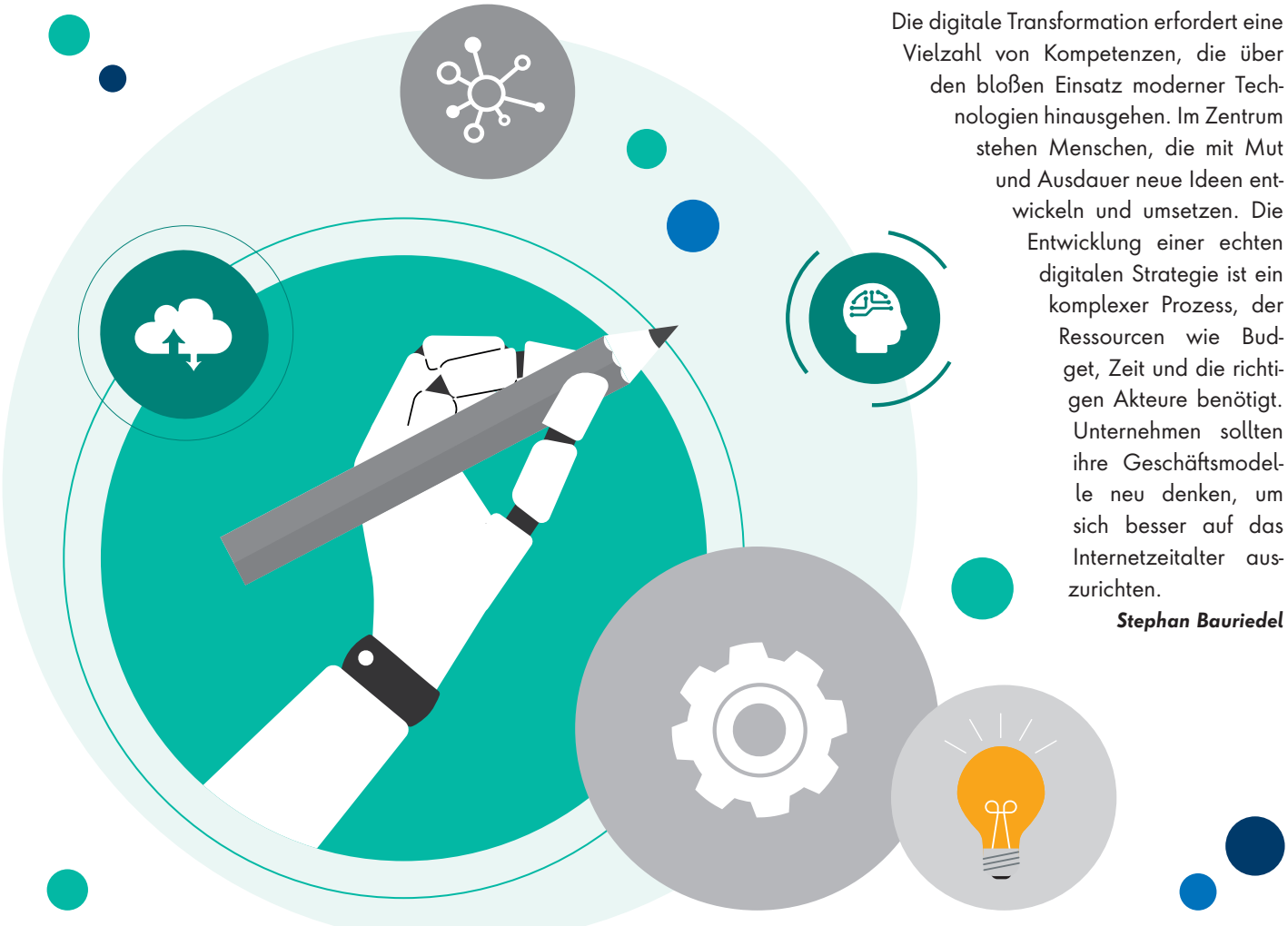
In der Strategiephase geht es um den Wissenstransfer, das Teambuilding, die Ideen und die Erkundung neuer Möglichkeiten. Ist das Geschäftsmodell gefunden, braucht es zunehmend den Koordinator, der die externen Akteure führt, und den Promoter, der das Vorhaben intern verkauft. Und zum Schluss den Macher, der die alte analoge Organisation verdrängt und die Transformation abschließt.

Das Anforderungsprofil an die Projektleitung und das Team ist weitreichend. Die fachlichen Kompetenzen erstrecken sich vom Innovationsmanagement, der Geschäftsmodellentwicklung, der erforderlichen Projekterfahrung bis zu den digitalen Technologien. Es verlangt nach einer gestandenen Persönlichkeit mit Führungsstärke, Skills in Moderation, Kommunikation, Teambuilding und der angesprochenen kosmopolitischen Prägung.

Anders als bei einem Start-up sollte das Projektteam in einem langfristig geschützten Rahmen agieren können, welcher über ein gesichertes Commitment und das erforderliche Budget verfügt.

VERGESSEN SIE DIE TECHNOLOGIE. FÜR DAS INTERNETZEITALTER BRAUCHT ES NEUE IDEEN, UND DIESE KOMMEN VON DEN MENSCHEN.

Stephan Bauriedel, Spezialist für CRM und die Digitalisierung, www.erfolg-mit-crm.de



Fazit

Die digitale Transformation erfordert eine Vielzahl von Kompetenzen, die über den bloßen Einsatz moderner Technologien hinausgehen. Im Zentrum stehen Menschen, die mit Mut und Ausdauer neue Ideen entwickeln und umsetzen. Die Entwicklung einer echten digitalen Strategie ist ein komplexer Prozess, der Ressourcen wie Budget, Zeit und die richtigen Akteure benötigt. Unternehmen sollten ihre Geschäftsmodelle neu denken, um sich besser auf das Internetzeitalter auszurichten.

Stephan Bauriedel

VISIBILITY

ESSENZIELLER BEITRAG ZU MEHR SICHERHEIT

Unternehmen investieren mehr und mehr in verschiedene Wege, um sich gegen das steigende Cyber-Risiko zu wappnen. Dafür greifen sie unter anderem auch zu Network-Detection-and-Response-Lösungen (NDR). Allerdings reicht es nicht, diese einfach zu installieren und sich selbst zu überlassen. Stattdessen gehen mit der Implementierung drei wesentliche Herausforderungen einher, die Security- und IT-Teams nicht unterschätzen dürfen:

#1 Für eine effiziente NDR-Ausstattung müssen Unternehmen zunächst in Vorkasse gehen. Danach sind durchgängig weitere Ausgaben notwendig, um die stetig wachsende Menge an Daten zu speichern und zu analysieren. Nicht selten müssen Entscheider dafür tiefer in die Tasche greifen als erwartet – vor allem, wenn sie vorher nicht den gesamten Netzwerk-Traffic transparent einsehen können und somit die potenziellen Risiken und Schwachstellen nicht kennen.

#2 Der laufende Betrieb von NDR-Tools – einschließlich ihrer Sensoren – ist oftmals mit operativem Aufwand verbunden. Die sich verändernde und ausbreitende IT-Infrastruktur macht eine eingehende Instandhaltung notwendig, im Zuge dessen auch die Sensoren umverlegt werden müssen. Dies nimmt den Experten nicht nur wertvolle Zeit, in der sie sich eigentlich um die Beseitigung von Schwachstellen und anderen Bedrohungen kümmern sollten. In all der Komplexität könnte den Security- und IT-Teams möglicherweise auch der Gesamtüberblick verloren gehen.

#3 Netzwerkumgebungen werden immer komplexer, wodurch sie zum Nährboden für Blind Spots werden. So kommt Traffic mit großen Datenmengen aus verschiedenen Richtungen ins Netzwerk, da dieses mittlerweile zahlreiche Anwendungen, Geräte und Nutzer auch außerhalb der Unternehmensgrenzen umfasst. Die Tatsache, dass Cyber-Angreifer ihre Malware zunehmend in verschlüsseltem Datenverkehr verstecken, macht Security- und IT-Teams das Leben schwer. Umso wichtiger ist es, dass die Teams den IT-Stack in seiner Gesamtheit einsehen können.

Keine Transparenz = keine Benefits mit NDR-Tools

Aufgrund der Komplexität eignen sich traditionelle Sicherheitslösungen immer weniger, um moderne Infrastrukturen effizient zu schützen. NDR-Tools gewährleisten nur partielle Sichtbarkeit des Netzwerk-Traffics. Es geht aber darum, Einsicht in den gesamten IT-Stack – also einschließlich aller Daten und Anwendungen, bis hinunter auf Netzwerkebene – zu gewinnen (Deep Observability). Schließlich können NDR-Lösungen nur auf Bedrohungen reagieren, die sie sehen können.

Eine Deep-Observability-Lösung wird direkt zwischen Infrastruktur und Performance-, Monitoring- und Sicherheits-Tools platziert. Dort fließt der gesamte Traffic zusammen, der sich durch die physischen, virtuellen und Cloud-Umgebungen bewegt. Nachdem sie die Daten analysiert, optimiert und eventuell entschlüsselt hat, sendet sie sie weiter zu den entsprechenden Performance-, Monitoring- und Security-Lösungen – einschließlich der NDR-Tools. Dank dieser netzwerkbasierten Insights profitieren Security- und IT-Teams von vollständiger Visibility über das gesamte Netzwerk hinweg und folglich von maximaler Monitoring-Leistung. Dadurch sind sie in der Lage, Bedrohungen, Schwachstellen, Blind Spots und verschlüsselten Datenverkehr schnell zu identifizieren und auszumerzen. Gleichzeitig lassen sich Security-relevante Ausgaben optimieren, sodass Sicherheit nicht zur Kostenfalle wird.

www.gigamon.com

UNSERE THEMEN

it management

Fokusthema: Industrial Transformation

Schwerpunktthemen: Internet of Things, ERP, AI/KI, Digital Twins, Digitalisierung, Nachhaltigkeit, Managed Services, Lizenzmanagement, SAP-Partnerlösungen, RPA

UNSERE THEMEN

it security

Special: IAM, PAM und CIAM

Fokusthema: Cyberversicherungen

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.

Die Ausgabe 03/04 2025 erscheint am 14. März 2025

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: Stephan Bauriedel, Lars Becker, Ivan Cossu, Christian Dir, Peter Dümig, Peter M. Färbinger, Sebastian Frost, Matthias Gromann, Dominik Hagen, Volker Hettich, Yvonne Kaupp, Dr. Thomas King, Thierry Kramis, Roland Kunz, Frank Laschet, Carina Mitzschke, Christopher Mohr, Dr. Jens Nachtwei, Silvia Parthier, Ulrich Parthier, Prof. Dr. Peter Preuss, Dr. Andreas Reuschl, Juri Rybicki, André Schindler, Oliver Stein, Sebastian Weber, Mark Wiegleb

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.


Steampunk
und BTP Summit 2025
5. und 6.
März 2025
Heidelberg
SAP Business Technology Platform, BTP,
wird nach Meinung der SAP-Community
die bestimmende ERP-Strategie.
Der Summit 2025 präsentiert Abap, CAP,
RAP und Steampunk sowie SAP BTP als
Basisplattform und S/4-Hana-Nachfolger.
Wird gesponsert von:
boomi
ifm
snap consulting
e3mag.com/de/steampunk-summit
Eine Veranstaltung des E3-Magazins:
e3mag.com

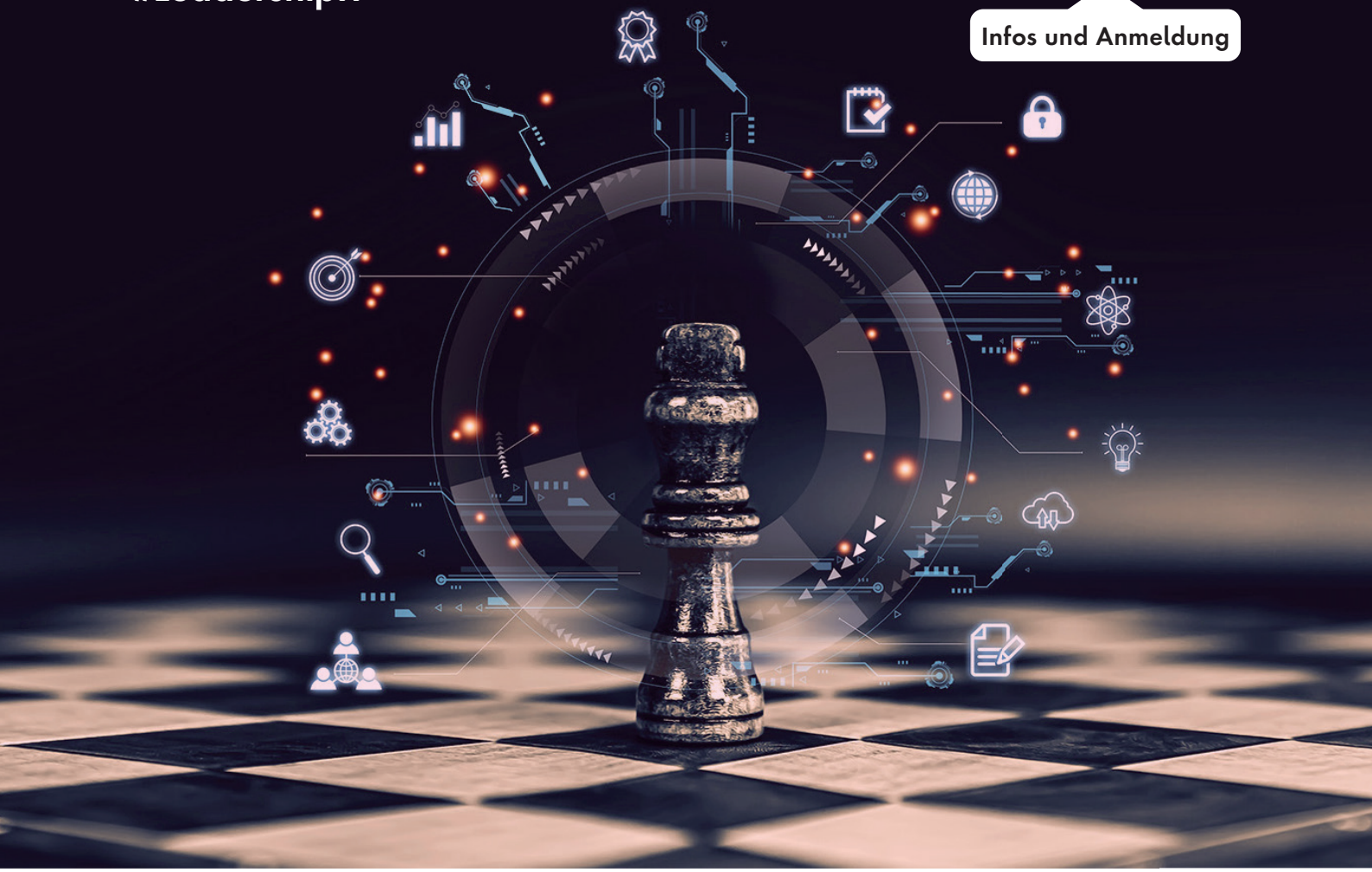
IT MANAGEMENT DIGITALEVENT

THOUGHT LEADERSHIP IN DER IT

MITTWOCH, 12.02.2025 | AB 9UHR

#LeadershipIT

Infos und Anmeldung



Eine Veranstaltung von itmanagement, itsecurity & it-daily.net

it security

Detect. Protect. Respond.
Januar/Februar 2025

VOM PFLICHTPROGRAMM ZUR GELEBTEN SICHERHEITSKULTUR

Information Security Management System

Jens Bothe, OTRS Group

PRIVILEGED ACCESS MANAGEMENT

PAM ist das neue IAM und PIM

CYBER-VERSICHERUNG

Warum sie unverzichtbar ist

DATA LOSS PREVENTION

Hemmschuh für Nachhaltigkeit

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

Inhalt

Information Security Management System

VOM PFLICHTPROGRAMM ZUR GELEBTEN SICHERHEITSKULTUR

In unserem Interview spricht Ulrich Parthier, Publisher it security, mit Jens Bothe, Vice President Information Security der OTRS Group. Thematisch geht es um das ISMS, warum es mehr als nur ein Tool ist und wie der Weg hin zu einer lebendigen Prozesslandschaft aussieht.

? **Ulrich Parthier:** *Herr Bothe, warum benötigen Unternehmen ein ISMS?*

Jens Bothe: Ein Information Security Management System (ISMS) ist für Firmen essenziell, um geschäftskritische Daten zu schützen, das Vertrauen von Kunden und Partnern zu stärken und gesetzliche Vorgaben wie die DSGVO zu erfüllen. In Zeiten zunehmender Cyberbedrohungen und regulatorischer Anforderungen, wie etwa die neuen NIS2- oder DORA-Richtlinien, bietet es den Rahmen, um Risiken zu identifizieren, zu bewerten und geeignete Schutzmaßnahmen zu ergreifen. Ohne ein solches System sind Organisationen anfällig für Sicherheitsvorfälle, die finanzielle und reputative Verluste nach sich ziehen können.

? **Ulrich Parthier:** *Wie würden Sie die Ziele eines ISMS und seine Bestandteile definieren?*

Jens Bothe: Das übergeordnete Ziel eines ISMS ist es, die Vertraulichkeit, Integrität und Verfügbarkeit von Informationen in Organisationen sicherzustellen. Es soll gewährleisten, dass Informationen nur von befugten Personen, Systemen oder Prozessen eingesehen oder verwendet werden; dass sie korrekt bleiben und nicht unautorisiert geändert oder manipuliert werden; und dass sie jederzeit verfügbar sind. Um dies zu erreichen, ist als erster Baustein ein Risikomanagement erforderlich.

Das heißt es reicht nicht aus, einfach ein ISMS-Tool zu installieren oder eine ISO/IEC 27001 Zertifizierung zu erlangen. Es braucht eine systematische Kombination von Richtlinien, Prozessen und Technologien, um festzulegen und zu steuern, wie Informationen geschützt werden sollen. Ein weiterer wichtiger Bestandteil sind Trainings, um Mitarbeitende für die Bedeutung von Informationssicherheit zu sensibilisieren und im Umgang mit Informationen unterschiedlicher Art zu schulen. Zu guter Letzt gehört auch die kontinuierliche Verbesserung zu jedem guten ISMS, um den sich schnell verändernden Bedrohungen gerecht zu werden.

? **Ulrich Parthier:** *Die IT ist ja keine grüne Wiese. Welche vorhandenen Applikationen erleichtern die Einführung eines ISMS?*

Jens Bothe: Dass die IT keine grüne Wiese ist, ist in diesem Fall tatsächlich vorteilhaft. Viele Unternehmen haben zum Beispiel bereits ein etabliertes IT Service Management (ITSM) mitsamt zugehörigen Tools und Anwendungen wie einer Service Management Software. Eine bestehende ITSM-Landschaft mit Prozessen wie Incident-, Change- und Problem-Management sowie eine

Configuration Management Database (CMDB) bieten eine solide Basis, um ein ISMS aufzubauen und damit Informationssicherheitsrisiken zu bewältigen.

Ulrich Parthier: *Der IST-Zustand, also eine Analyse des bestehenden Zustandes ist die Ausgangslage für jedes Projekt. Wie sehen die folgenden Schritte aus?*

Jens Bothe: Nach der IST-Analyse folgt die Risikobewertung. Dafür müssen Unternehmen wissen, welche Assets und Informationen mit welcher Priorität geschützt werden müssen. Denn nicht alle Informationen haben den gleichen Schutzbedarf und nicht alle Assets sind gleich wichtig. Kundendatenbankserver oder sensible Geschäftsgeheimnisse sind beispielsweise kritischer als allgemeine Bürodokumente.

Unternehmen müssen also für alle Assets und Informationen den Schutzbedarf ermitteln, in normalen, erhöhten und hohen Schutzbedarf einstufen und entsprechend priorisieren.

> EIN ISMS STEIGERT DURCH KLARE PROZESSE UND AUTOMATISIERUNG DIE EFFIZIENZ UND STÄRKT DEN RUF DES UNTERNEHMENS.
>
> **Jens Bothe, Vice President Information Security, OTRS Group, www.otrs.com**

Eine CMDB unterstützt bei der Risikobewertung. Die zentrale Sicht auf IT Assets und deren Beziehungen hilft, Bedrohungen, Schwachstellen und damit verbundene Risiken zu identifizieren und zu bewerten. Zudem kann der Schutzbedarf dokumentiert und Maßnahmen zur Risikominderung definiert werden.

Ulrich Parthier: *Sind die Schwachstellen erkannt und priorisiert, geht es um die Zuordnung von Verantwortlichkeiten. Also sowohl eine organisatorische als auch eine technische Umsetzung. Wie gestalte ich eine solche Maßnahme und wie kontrolliere ich deren Umsetzung?*

Jens Bothe: Wenn ein Risiko erkannt wird, muss klar sein, wer für den Schutz und die Verwaltung zuständig ist, um im Ernstfall schnell reagieren und Schäden verhindern oder zumindest mindern zu können. Für jedes identifizierte Risiko oder jede Schwachstelle sollte es einen Applikationsverantwortlichen, einen technischen Ansprechpartner und genehmigende Instanzen geben. Diese sollten ebenfalls in der CMDB am jeweiligen Asset dokumentiert sein, damit Zuständigkeiten und Prozesse zu jeder Zeit für alle transparent und klar sind.

Aufbauend darauf ist ein konkreter Maßnahmenplan unerlässlich, der spezifische Ziele, einen Zeitrahmen und messbare Erfolgsindikatoren beinhaltet. In der technischen Umsetzung kommen geeignete Sicherheitslösungen wie Verschlüsselung oder Zugriffssteuerungen zum Einsatz.

Sämtliche Kommunikation und Aktionen, die im Zusammenhang mit einer Maßnahme stattfinden, sollten in einem integrierten Projektmanagement- und/oder ISMS-Tool abgebildet werden, um den Status kontinuierlich zu verfolgen

und zu dokumentieren. Regelmäßige Berichte, KPIs und interne Audits unterstützen zusätzlich dabei, die Umsetzung zu kontrollieren.

? **Ulrich Parthier:** *Bei ISMS-Tools gibt es ja eine Vielzahl von Lösungen mit den unterschiedlichsten Leistungsspektren. Was sollte sie in puncto User Experience, kontinuierliche Risikoanalyse, Compliance und Standards bieten?*

Jens Bothe: Ein ISMS-Tool muss benutzerfreundlich sein, sodass es auch Personen ohne technische Vorkenntnisse leicht bedienen können. Darüber hinaus spielt Automatisierung eine zentrale Rolle: Risikoanalysen und Compliance-Überprüfungen sollten regelmäßig automatisch durchgeführt werden, um den manuellen Aufwand zu minimieren. Zudem muss das Tool mit gängigen Standards und Frameworks wie ISO 27001 oder NIST kompatibel sein, um die Einhaltung rechtlicher und organisatorischer Vorgaben zu unterstützen. Schließlich sollte eine nahtlose Integration in bestehende Systeme wie ITSM, CMDB und Monitoring-Tools gewährleistet sein, um Datenflüsse und Effizienz zu optimieren.

? **Ulrich Parthier:** *Kommen wir noch einmal zurück zu dem Herzstück eines ISMS, der CMDB. Diese ist ja eine Datei, die die Beziehungen zwischen der Hardware, der Software und den Netzwerken verdeutlicht, die eine IT-Organisation verwendet. Beim Aufbau einer CMDB stellt sich die Frage, wie im jeweiligen Unternehmen das Asset Management in die ISMS-Prozesslandschaft integriert ist oder werden soll. Wie sind hier ihre Erfahrungen?*

Jens Bothe: Richtig, das Asset Management bildet die Grundlage für ein ISMS. Für die Integration in die ISMS-Prozesslandschaft sollte daher zunächst sichergestellt sein, dass die Daten in der CMDB vollständig und aktuell sind. Nur so lassen sich die richtigen technischen und organisatorischen Maßnahmen für bestimmte Informationswerte festlegen.

In der Praxis sehen sich Security-Teams bei der Integration allerdings oft mit Herausforderungen konfrontiert. In unserer Umfrage „OTRS Spotlight: Corporate Security 2024" beklagen 61 Prozent der Befragten die Komplexität der Integration als größtes Hindernis. Existiert bereits eine bestehende Lösung, kann für den Aufbau einer CMDB ein einfacher CSV-Import genutzt werden. Das birgt jedoch die Gefahr, veraltete, fehlerhafte oder doppelte Daten aus Legacy-Lösungen zu übernehmen und erfordert einen hohen manuellen Aufwand. Dateninkonsistenz und verzögerte Datensynchronisation geben mit 42 und 40 Prozent auch viele Befragte als größte Hindernisse bei der Integration an.

Um sicherzustellen, dass die Daten aktuell, korrekt und vollständig sind und um den Aufwand so gering wie möglich zu halten, sollten Lösungen genutzt werden, die den Prozess vereinfachen.

Das können zum Beispiel dedizierte Asset Management Softwarelösungen, spezielle Integrationstools oder Schnittstellen zu Inventory-Lösungen sein, die einen Datenaustausch in beide Richtungen sowie Datenmapping erlauben.

Ulrich Parthier: *Oftmals werden Applikationen aus einem Silodenken heraus projektiert. Wie erreiche ich einen ganzheitlichen Blick auf das ISMS und wie können Sicherheitsverantwortliche ein solches etablieren und seine kontinuierliche Durchführung gewährleisten?*

Jens Bothe: Ein ganzheitlicher Ansatz erfordert die Einbindung aller relevanten Abteilungen, einschließlich IT, Compliance und HR, um eine unternehmensweite Zusammenarbeit zu fördern. Prozessübergreifendes Denken und der Abbau von Silos sind essenziell, um effektive Sicherheitsprozesse zu etablieren. Kontinuierliche Schulungen stärken zudem das Sicherheitsbewusstsein aller Mitarbeitenden. Zentralisierte Plattformen, die eine umfassende 360°-Sicht bieten, unterstützen die Steuerung der Prozesse. Regelmäßige Audits sorgen dafür, dass Maßnahmen fortlaufend überprüft und gegebenenfalls angepasst werden können.

Ulrich Parthier: *Wie kann ich Stakeholdern wie Usern den Nutzen und Mehrwerte aufzeigen, mögliche Stolpersteine überwinden und die generellen Vorteile für das Unternehmen aufzeigen?*

Jens Bothe: Typische Stolpersteine sind die hohe Komplexität der Anforderungen, fehlende Akzeptanz der Mitarbeitenden und mangelnde Ressourcen. Der Schlüssel, um diese zu überwinden, ist vor allem Kommunikation. Dabei sollte immer darauf geachtet werden, welche Interessen die jeweiligen Stakeholder haben und die entsprechenden Mehrwerte eines ISMS herausgestellt werden.

Das Management mag bei der Einführung eines ISMS beispielsweise Bedenken hinsichtlich des Kosten-Nutzen-Verhältnisses haben. Hier sollte verdeutlicht werden, dass ein ISMS nicht nur vor Sicherheitsvorfällen, sondern damit auch vor wirtschaftlichen Schäden und rechtlichen Konsequenzen bei Nichteinhaltung von Compliance-Anforderungen schützt. ISMS-Tools mit klar strukturierten Berichtsfunktionen, übersichtlichen Dashboards und Reports helfen dabei, Sicherheitsstatus und Fortschritte verständlich zu kommunizieren.

Welcher Vorteil in der Regel außerdem allen Stakeholdern zusagt: Ein ISMS steigert durch klare Prozesse und Automatisierung die Effizienz. Zuletzt stärkt es zudem den Ruf des Unternehmens und baut Vertrauen bei Kunden und Partnern auf.

Ulrich Parthier: *Gibt es ein generisches Vorgehensmodell zur Einführung eines ISMS und können Sie anhand ihrer langjährigen Erfahrungen eine Empfehlung geben?*

Jens Bothe: Nein, ein Standardmodell, das für alle Unternehmen gleichermaßen passt, gibt es nicht. Die Einführung eines ISMS muss stets auf die spezifischen Gegebenheiten, Anforderungen und die bestehende Tool- und Prozesslandschaft des Unternehmens abgestimmt werden.

Aus meiner Erfahrung empfehle ich jedoch allen, der Projektinitiierung und der kontinuierlichen Verbesserung besondere Aufmerksamkeit zu widmen. Zu Beginn müssen Ziele, Verantwortlichkeiten und Ressourcen klar definiert werden, um die folgenden Bestandteile effektiv und effizient aufzubauen. Und ein ISMS sollte nie als abgeschlossenes Projekt betrachtet, sondern aktiv gelebt, regelmäßig überprüft und an neue Anforderungen angepasst werden. Nur so erfüllt es seinen Zweck, Informationen im Unternehmen fortlaufend und nachhaltig zu schützen.

Ulrich Parthier: *Herr Bothe, wir danken wir das Gespräch!*

WAS IST EIN ISMS?

Ein ISMS (Information Security Management System) ist ein systematischer Ansatz, um Informationen in einer Organisation zu schützen. Es umfasst Richtlinien, Prozesse und Technologien, die entwickelt wurden, um Risiken in Bezug auf Informationssicherheit zu identifizieren, zu bewerten und zu steuern.
Ziel eines ISMS ist es, die Vertraulichkeit, Integrität und Verfügbarkeit von Informationen sicherzustellen.

HACKS & BUGS

DIE GRÖSSTEN SECURITY-EREIGNISSE 2024

Das Jahr 2024 hat uns einmal mehr gezeigt, dass die Cybersecurity-Welt voller Überraschungen steckt – manchmal bedrohlich, manchmal kurios, aber immer lehrreich. Von kritischen Infrastrukturschwachstellen bis hin zu tragikomischen Vorfällen präsentieren wir Ihnen die bemerkenswertesten Security-Ereignisse des Jahres.

Der CrowdStrike-GAU: Wenn ein Update die Welt stillstehen lässt

Der 19. Juli 2024 wird als der Tag in Erinnerung bleiben, an dem ein fehlerhaftes Software-Update die (digitale) Welt ins Chaos stürzte. Der „Falcon Sensor" des Cybersecurity-Anbieters CrowdStrike löste einen der größten IT-Ausfälle der Geschichte aus. Ein simpler Konfigurationsfehler in der Channel File 291 führte zu weltweiten Systemabstürzen bei Windows-Computern.

Die Folgen waren dramatisch: Über 2.000 Flüge wurden gestrichen, Krankenhäuser mussten Operationen absagen, Banken kämpften mit Handelsverzögerungen. Etwa 8,5 Millionen Windows-Geräte waren betroffen. Der Vorfall unterstreicht eindrucksvoll die Abhängigkeit moderner Infrastrukturen von einzelnen Software-Anbietern.

Die XZ-Utils-Backdoor

Die Linux-Community erlebte Anfang des Jahres einen ihrer größten Sicherheitsvorfälle, als Red Hat eine kritische Warnung bezüglich einer Backdoor in XZ Utils herausgab. Die kompromittierten Versionen 5.6.0 und 5.6.1 enthielten bösartigen Code, der es Angreifern ermöglichte, über den SSH-Daemon unauthorisierten Systemzugriff zu erlangen.

Die Entdeckung gelang dem PostgreSQL-Entwickler Andres Freund bei Microsoft, der ungewöhnliche Verzögerungen bei SSH-Logins und Valgrind-Fehler bemerkte. Die Bedrohung wurde unter der Kennung CVE-2024-3094 als kritisch eingestuft. Besonders gravierend war die Situation für Nutzer von Fedora 41 und Fedora Rawhide, aber auch andere Distributionen wie Debian-unstable waren betroffen.

DDoS-Rekord: Cloudflare stemmt sich gegen 5.6 Terabit-Tsunami

Cloudflare gelang es, den bisher größten öffentlich dokumentierten DDoS-Angriff erfolgreich abzuwehren. Mit einer beeindruckenden Spitzenleistung von 5,6 Terabit pro Sekunde (Tbps) übertraf dieser Angriff sogar den bisherigen Rekord von Microsoft (3,47 Tbps).

Die massive Attacke war Teil einer monatelangen Kampagne gegen Organisationen aus den Bereichen Finanzdienstleistungen, Internet und Telekommunikation. Bemerkenswert war nicht nur die schiere Größe des Angriffs, sondern auch die Häufigkeit: Mehr als 100 hochvolumige DDoS-Attacken wurden registriert, viele davon mit über zwei Milliarden Paketen pro Sekunde.

Operation LockBit: Der Fall eines Cybercrime-Imperiums

Ein bedeutender Erfolg im Kampf gegen organisierte Cyberkriminalität gelang den Strafverfolgungsbehörden mit der Zerschlagung der berüchtigten LockBit-Gruppierung. Die Verhaftung von zwei Schlüsselfiguren und die laufenden Ermittlungen gegen Entwickler und Partner der Gruppe markieren einen Wendepunkt in der Geschichte der Ransomware-Bekämpfung.

LockBit, bekannt für seine skrupellosen Angriffe selbst auf Krankenhäuser und kritische Infrastrukturen, ist nur einer von mehreren großen Erfolgen der Behörden. Im Dezember gelang dem FBI gemeinsam mit internationalen Partnern die Beschlagnahmung der Server und Leak-Site von BlackCat. Kurz darauf konnte die von Fancy Bear eingesetzte Mooboot-Malware auf Ubiquiti-Routern neutralisiert werden.

Die Ausschaltung der beiden größten Ransomware-Banden hat das Potenzial, die Bedrohungslandschaft nachhaltig zu verändern. Experten erwarten eine zunehmende Fragmentierung und Dezentralisierung von Cybercrime-Gruppen.

Lars Becker

PLUS

Lesen Sie den kompletten Beitrag hier

Kleines Leck, große Wirkung

WARUM IM JAHR 2024 NIEMAND VOR DATENABFLUSS SICHER WAR

In den vergangenen zwölf Monaten erreichten die Folgen von ungewolltem Datenabfluss abermals neue Rekordhöhen. Finanzielle Verluste sind dabei nur ein Aspekt: Grundrechtsverletzungen, massive Reputationsschäden für Unternehmen und ein erschüttertes Vertrauen in staatliche Institutionen zählten zu den schwerwiegenden Konsequenzen. Besonders das Superwahljahr 2024 zeigte, wie Datendiebstahl demokratische Prozesse destabilisieren kann. Der Schutz sensibler Daten ist daher von entscheidender Bedeutung. Diese und weitere Erkenntnisse liefert der aktuelle Cybersecurity-Report von infodas, der sich dediziert mit Data-Leakage auseinandersetzt.

MASSGESCHNEIDERTE LÖSUNGEN VON INFODAS

Seit über 50 Jahren steht infodas, ein Airbus Tochterunternehmen spezialisiert auf Cyber und IT, für verlässliche Cyber- und IT-Sicherheit. infodas bietet mit der SDoT Produktfamilie Hochsicherheitsprodukte gegen den ungewollten Datenabfluss aus Unternehmen, der öffentlichen Verwaltung, Kritischen Infrastrukturen und militärischen Sicherheitsdomänen. Darüber hinaus bietet das Systemhaus umfangreiche Beratungsleistungen in den Bereichen IT-Security und IT. Datengetriebene und maßgeschneiderte Lösungen mittels KI gehören auch zum Portfolio der infodas.

Daten als Goldmine für Bedrohungsakteure

In der digitalen Gesellschaft sind Daten zur unverzichtbaren Ressource geworden. Sie bieten allerdings auch Anreize für illegale Machenschaften. Hier überrascht kaum, dass finanzielle Motive die primäre Triebfeder für Data-Leakage darstellen. Der Schlüssel zu maximalem Profit liegt dabei in der Jagd auf Informationen wie geistigem Eigentum, Kunden-, Lieferanten-, Finanz- oder Gesundheitsdaten. Für Opfer sind diese Informationen von besonderer Bedeutung, was sie zu idealen Druckmitteln oder begehrten Handelsgütern in Untergrundforen machen. Abseits der opportunistischen Cyberkriminalität sind auch staatlich-finanzierte oder rein staatliche Akteure am Werk. Sie nehmen behördliche Institutionen oder staatsnahe Unternehmen ins Visier - mit dem Ziel, hochsensible Informationen wie Verschlusssachen zu erbeuten.

Hack-and-Leak – Die Besinnung auf das Wesentliche

Ransomware stellt weiterhin den Modus Operandi für Erpressung dar. Im vergangenen Jahr lässt sich jedoch eine Masche beobachten, welche sich rein auf den Datendiebstahl fokussiert und simpler nicht sein könnte. Die Rede ist von Hack-and-Leak, oder auch Data-Extortion. Hierbei werden die sensiblen Daten nicht aufwendig verschlüsselt, um Geld zu erpressen. Stattdessen exfiltrieren Angreifer sie und drohen mit der Veröffentlichung auf sogenannten Dedicated-Leak-Sites sollte keine Löse- oder Schweigegeldzahlung erfolgen. Aber Hack-and-Leak etablierte sich nicht nur als lukrativer Monetisierungsvektor. Im Superwahljahr sorgte diese Taktik auch für Aufsehen, um politische Einrichtungen oder das Europäische Parlament zu diskreditieren.

Der Fluch und Segen von LLMs

Spätestens mit der Veröffentlichung von ChatGPT wurde das Potenzial von Künstlicher Intelligenz (KI) und insbesondere von LLMs (Large-Language-Models) offenkundig. Doch nutzen unlängst auch Bedrohungsakteure diese Technologie, um ihre Operationen effizienter zu planen und durchzuführen. KI-gestützte Phishing- oder Vishing-Kampagnen sind hier nur der Anfang. Darüber hinaus sind LLMs enorme Wissensspeicher und besonders exponierte Ziele, sensible Daten zu entlocken. Mehrere Vorfälle sind bereits bekannt, mit einem erwarteten Anstieg für das Jahr 2025.

www.infodas.com

MEHR WERT
Download Report „Data Leakage 2024+“

Erfolgsfaktor Data Loss Prevention

DATENVERLUST: HEMMSCHUH FÜR NACHHALTIGKEIT

Daten bilden das Fundament der heutigen Wirtschaftswelt. Gehen sie verloren, hat dies Folgen für den Geschäftsbetrieb und die langfristige Stabilität eines Unternehmens. Besonders gravierend ist der Verlust sensibler Informationen: Er zieht nicht nur finanzielle Einbußen und rechtliche Konsequenzen nach sich, sondern erfordert auch immense Ressourcen für Wiederherstellung und Schadensbegrenzung. Zudem schadet er der wirtschaftlichen, ökologischen und gesellschaftlichen Nachhaltigkeit. Spätestens hier wird deutlich: Eine effektive Strategie zur Vermeidung von Datenverlusten (Data Loss Prevention) ist unabdingbar. Was genau hinter dem Begriff Data Loss Prevention steckt und wie sie sich erfolgreich umsetzen lässt, verrät dieser Beitrag.

Data Loss Prevention: Sicherheit trifft Nachhaltigkeit

Unter Data Loss Prevention (DLP) versteht man den Schutz sensibler Informationen, wie personenbezogener Daten, Finanzdaten oder geistigem Eigentum, vor Verlust, unerlaubter Weitergabe und unbefugtem Zugriff durch den Einsatz von Sicherheitsstrategien, -prozessen und -technologien. Doch DLP ist weit mehr als nur eine Sicherheitsmaßnahme. Es trägt entscheidend dazu bei, ein Unternehmen aus wirtschaftlicher, ökonomischer und gesellschaftlicher Sicht zukunftssicher aufzustellen:

#1 Nachhaltigkeit aus ökonomischer Sicht

Der Verlust vertraulicher Daten hat oft weitreichende finanzielle Folgen: Entgangene Geschäfte, erhöhte IT-Kosten und drakonische Bußgelder bei Verstößen gegen die DSGVO, die NIS2-Richtlinie, das KRITIS-Dachgesetz oder andere gesetzliche Vorschriften belasten den Liquiditätsbestand bisweilen erheblich. Im Extremfall ist er sogar existenzbedrohend.

Eine starke DLP-Strategie wirkt präventiv gegen Datenverluste und minimiert so wirtschaftliche Risiken. Moderne Technologien wie virtuelle Datenräume auf Basis der Sealed-Cloud-Technologie helfen Unternehmen, ihre vertraulichen Informationen zu schützen, perspektivisch Kosten zu senken sowie die Effizienz zu steigern. Vor allem aber stärken sie die Resilienz und Wettbewerbsfähigkeit eines Betriebs und sichern so dessen langfristiges Überleben.

#2 Nachhaltigkeit aus ökologischer Sicht

Verlorene Daten verursachen auch ökologische Schäden. Denn bei ihrer Wiederherstellung gilt es, Backup-Systeme zu aktivieren. Wird die Software durch den Verlust von System- oder Konfigurationsdateien beschädigt – oder im Falle von Cyberattacken verschlüsselt –, ist es mitunter erforderlich, sie nochmals zu installieren. Schlimmstenfalls heißt es, das System komplett neu aufzusetzen. All diese Maßnahmen erfordern enorme Rechenleistung und somit einen erhöhten Energieverbrauch. Unternehmen mit einer umfassenden DLP-Strategie und energieeffizienten Rechenzentren können ihren ökologischen Fußabdruck erheblich reduzieren.

#3 Nachhaltigkeit aus gesellschaftlicher Sicht

Nachhaltigkeit spiegelt sich auch im Vertrauen von Kunden, Partnern und der Öffentlichkeit in den verantwortungsbewussten Umgang mit sensiblen Daten wider. Betriebe mit umfassenden DLP-Vorkehrungen zeigen, dass sie höchsten Sicherheitsstandards gerecht werden. Zertifizierungen wie ISO/IEC 27001 oder TCDP wiederum beweisen, dass diese Unternehmen den Datenschutz und die Informationssicherheit ernst nehmen und gesetzliche Anforderungen einhalten. Zudem minimiert ein Betrieb, der auf starke DLP-Strategien setzt, das Risiko existenzbedrohender Folgen eines Datenverlusts. Dadurch bleibt er langfristig wirtschaftlich stabil, kann so der Belegschaft dauerhaft sichere Arbeitsplätze bieten und sich als verlässlicher Geschäftspartner profilieren.

Die Top-10-Verfahren für Data Loss Prevention

Eine erfolgreiche DLP-Strategie erfordert den Einsatz moderner Verfahren, die sensible Daten vor unerlaubtem Zugriff schützen. Insbesondere diese zehn Ansätze haben sich dabei bewährt:

DLP-Verfahren	Beschreibung	Vorteile	Nachteile
Datenklassifizierung	Systematisches Kategorisieren von Daten nach ihrer Vertraulichkeit	– effektiver Schutz sensibler Daten – verbesserte Compliance	– Komplexität – hoher Zeitaufwand – klare Regeln zur Vermeidung subjektiver Einschätzungen der Vertraulichkeit der Daten erforderlich
Endpoint-DLP	Überwachen und Steuern von Datenbewegungen auf Endgeräten wie PCs oder Smartphones	– Verhindern unsicherer und unautorisierter Datenweitergabe – Schutz der Endgeräte vor Insider- und Cyberbedrohungen	– Ressourcenaufwand – benötigt regelmäßige Updates – erfordert Einhaltung einheitlicher Sicherheitsrichtlinien auf allen Endgeräten
Netzwerk-DLP	Überprüfen des Datenverkehrs auf verdächtige Aktivitäten und automatisches Blockieren von Richtlinienverstößen	– Überblick über Datenflüsse – Verhindern von Datenabflüssen – erhöhte Netzwerksicherheit	– Beschränkung auf den Netzwerkbereich – Komplexität – hohe Kosten – unter Umständen Auswirkungen auf die Systemleistung
Verschlüsselungstechnologien	Verschlüsselung der Daten sowohl im Ruhezustand als auch während der Übertragung	– DSGVO-Compliance – sicheres standortübergreifendes Arbeiten	– komplexe und teils ressourcenintensive Implementierung – kein Schutz vor Hackerangriffen/Systemausfällen beim Cloud-Dienst-Anbieter – kein Schutz vor Ransomware-Attacken
Cloud-DLP	Kontinuierliches Überwachen der Datenbewegungen in der Cloud	– sichere Cloud-Nutzung und Schutz von Daten – Echtzeitüberwachung und Verschlüsselung – Schutz der Daten vor unbefugtem Zugriff	– Abhängigkeit vom Betreiber und von korrekter Einrichtung – Kompatibilitätsprobleme möglich
Data Masking/Tokenisierung	Ersatz realer Daten durch Platzhalter	– Schutz der Daten bei der Verarbeitung oder Nutzung in Testumgebungen – minimierte Datenexposition – Unbrauchbarkeit sensibler Daten für Unbefugte im Fall einer Datenpanne – Einhaltung von Datenschutz- und Compliance-Vorgaben	– aufwendig in der Planung – Rückverfolgbarkeit der Daten nicht vollständig ausgeschlossen
Zugriffskontrollsysteme	Kontrollierter Zugriff auf sensible Daten durch präzise Berechtigungs- und Rollenzuweisung	– reduziert Risiken durch Zugriffe Unbefugter – granulare Regelung von Zugriffsrechten	– kontinuierliche Pflege von Rollen und Berechtigungen erforderlich – begrenzter Schutz vor Insiderbedrohungen
Überwachung und Auditierung	Echtzeitüberwachung und Protokollierung von Datenbewegungen	– Erkennung und Protokollierung verdächtiger Aktivitäten in Echtzeit – schnelle Problemlösung	– robuste Analysetools und Ressourcen erforderlich
Incident-Response- und IT-Forensik	Automatisiertes Erkennen und Beheben von Datenschutzverletzungen, Durchführen IT-forensischer Analysen	– schnelle Identifikation von und Reaktion auf Datenschutzverletzungen – schnelle Reaktion auf Sicherheitsvorfälle	– reaktiv statt präventiv – kann bei häufigen Vorfällen teuer werden
Secure Collaboration Tools wie: – virtuelle Datenräume – Versiegelungstechnologien (Sealed Cloud)	Sicherer Austausch vertraulicher Daten in geschützter Umgebung, transparente Dokumentation aller Aktivitäten	– sicherer Datenaustausch – Compliance und Datenintegrität	– abhängig von korrekter Einrichtung und Verwaltung – erfordert präzise definierte Berechtigungen

Virtuelle Datenräume als Baustein moderner DLP-Strategien

Gerade, wenn es darum geht, streng vertrauliche Daten zu verwalten oder auszutauschen, spielen virtuelle Datenräume (VDRs) eine wichtige Rolle. Vor allem durch folgende Aspekte werden sie zu einem unverzichtbaren Bestandteil einer gut durchdachten DLP-Strategie:

#1 Individuelle Zugriffsrechte und revisionssichere Protokollierung

Virtuelle Datenräume gestatten es, individuelle Zugriffsrechte pro Anwender zu erteilen. So lässt sich exakt definieren, wer welche Art Zugriff auf welche Daten erhalten soll. Dies minimiert das Risiko von Insider-Bedrohungen und stellt sicher, dass sensible Informationen geschützt bleiben. VDRs protokollieren jede Aktivität lückenlos (und somit revisionssicher), was langfristig die Datensicherheit und Nachhaltigkeit eines Unternehmens gewährleistet.

Für zusätzliche Transparenz sorgt die sogenannte Auditor-Rolle, die manche VDRs bieten. Mit dieser Funktion ist es möglich, detaillierte Aktivitätsberichte einzusehen sowie zu exportieren und stets einen Überblick über alle Datenraum- und Administratoraktivitäten zu gewährleisten – und das unter Einhaltung sämtlicher Unternehmensrichtlinien sowie regulatorischer Standards. Sollte es doch einmal zu einem Datenverlust oder einer Datenschutzverletzung kommen, kann der Auditor mit wenig Aufwand eine umfassende Berichterstattung erstellen und Schwachstellen auf diese Weise schnell und treffsicher identifizieren.

#2 Maximale Sicherheit durch zukunftsweisende Technologien

Ebenfalls punkten kann ein VDR, wenn ihm hochmoderne Technologien zugrunde liegen, die allerhöchsten Si-

UNTERNEHMEN, DIE AUF EIN ZIELGERICHTETES DLP-KONZEPT SETZEN, STÄRKEN DAS VERTRAUEN IHRER KUNDEN, PARTNER UND MITARBEITER UND FÖRDERN DIE STABILITÄT IHRER ARBEITSPLÄTZE.

Siegfried Kirschner, Chief Information Security Officer (CISO), idgard |uniscon GmbH, www.idgard.com/de

cherheitsstandards entsprechen. Basiert er zum Beispiel auf einem Confidential-Computing-Ansatz wie der Sealed-Cloud-Technologie, kann selbst der Betreiber des Cloud-Dienstes zu keiner Zeit auf die gespeicherten Daten seiner Kunden zugreifen.

Diese zusätzliche Sicherheitsebene geht weit über herkömmliche Cloud-Schutzmaßnahmen hinaus und ist besonders für Branchen mit strengen regulatorischen Anforderungen unverzichtbar. VDRs tragen somit sowohl zum Datenschutz als auch zur Einhaltung von Compliance-Vorgaben bei, was die Nachhaltigkeit des Unternehmens auf lange Sicht stärkt.

#3 Zertifikate: Nachweis geprüfter Sicherheit

Ein nach TCDP zertifizierter VDR erfüllt nachweislich höchste Sicherheits- und Datenschutzanforderungen – ein wichtiger Aspekt in Bezug auf die Nachhaltigkeit. Denn ein zuverlässiger Partner mit entsprechenden Zertifizierungen trägt dazu bei, das Vertrauen der Öffentlichkeit zu stärken und langfristige Geschäftsbeziehungen zu sichern.

#4 Nachhaltigkeit durch energieeffiziente Rechenzentren

Das Rechenzentrum, in dem der VDR gehostet wird, spielt ebenfalls eine wichtige Rolle in der Zukunftssicherheit einer DLP-Strategie. Moderne, hochsichere Rechenzentren, die strenge regulatorische Anforderungen erfüllen und mehrfach zertifiziert sind, gewährleisten nicht nur den physischen Schutz sensibler Daten, sondern setzen auch auf Nachhaltigkeit. Energieeffiziente Technologien, erneuerbare Energiequellen, wassersparende Maßnahmen und Wärmerückgewinnungssysteme tragen wiederum dazu bei, den ökologischen Fußabdruck zu minimieren.

Diese Aspekte machen moderne Rechenzentren zu einem zentralen Baustein einer zukunftsorientierten IT-Infrastruktur und einer effektiven DLP-Strategie. Zusätzlich können so die von der EU-Kommission geforderten Vorgaben zur Reduzierung der Nachhaltigkeitsrisiken erfüllt werden.

Fazit: DLP als Schlüssel zur Nachhaltigkeit

Data Loss Prevention ist weit mehr als eine reine Sicherheitsmaßnahme – sie ist Teil einer ganzheitlichen Nachhaltigkeitsstrategie. Unternehmen mit einem gut durchdachten und umgesetzten DLP-Fahrplan reduzieren nicht nur ihre finanziellen Risiken und schützen sich vor Datenverlusten, sondern leisten auch einen wichtigen Beitrag zur Reduzierung ihres ökologischen Fußabdrucks.

Moderne Technologien wie die Sealed Cloud, virtuelle Datenräume und energieeffiziente Rechenzentren bieten Betrieben die Möglichkeit, ihre IT-Infrastruktur sicher und nachhaltig zukunftsorientiert aufzustellen. Ganz nebenbei stärken Unternehmen, die auf ein zielgerichtetes DLP-Konzept setzen, das Vertrauen ihrer Kunden, Partner und Mitarbeiter, fördern die Stabilität ihrer Arbeitsplätze und sichern sich damit langfristig einen Wettbewerbsvorteil.

Siegfried Kirschner

Weckruf für Unternehmen

ALARMIERENDE SICHERHEITSLÜCKEN BEI ICS-/OT-FACHKRÄFTEN

Eine aktuelle Studie zur Sicherheit industrieller Steuerungssysteme (ICS) und Betriebstechnologie (OT) enthüllt gravierende Mängel in der Ausbildung und Erfahrung von Fachkräften. Obwohl zwei Drittel der Unternehmen ihre Mitarbeiter als größte Sicherheitsrisiken einstufen, wird lediglich ein Viertel des Budgets für Schulungen bereitgestellt. Diese Schieflage birgt immense Risiken für kritische Infrastrukturen.

Erfahrene Mitarbeiter als Schlüssel zur Cybersicherheit

Der SANS 2024 State of ICS/OT Cybersecurity Report zeigt, dass mehr als 50 Prozent der ICS-/OT-Fachkräfte weniger als fünf Jahre Berufserfahrung besitzen. Dieser Mangel an Expertise schwächt die Verteidigungsfähigkeit gegen immer komplexere Cyberbedrohungen. „Der Mangel an gut ausgebildeten, erfahrenen ICS/OT-Fachkräften ist heute eine der größten Herausforderungen", erklärt Holger Fischer, Sales Director EMEA Central bei OPSWAT. „Es braucht gezielte Investitionen in Menschen, um kritische Infrastrukturen widerstandsfähiger zu machen."

Wichtige Erkenntnisse aus der Studie:

- **Erfahrungslücken:** Die Mehrheit der ICS-Fachkräfte verfügt über weniger als fünf Jahre Erfahrung. Dies verdeutlicht den Bedarf an besserem Mentoring und Wissenstransfer.
- **Mangel an Zertifizierungen:** 51 Prozent der Fachkräfte arbeiten ohne branchenspezifische Zertifizierungen, was ihre Fähigkeit, ICS/OT-spezifische Bedrohungen zu bewältigen, einschränkt.
- **Budgetprioritäten:** Während 66 Prozent der Unternehmen „Menschen" als das größte Risiko ansehen, fließen nur 25 Prozent der Cybersicherheitsbudgets in Personalentwicklung. Im Gegensatz dazu werden 52 Prozent für Technologien ausgegeben.

Technologische Lösungen sind nicht genug

Die Studie unterstreicht, dass technologische Investitionen allein nicht ausreichen. Die zunehmende Komplexität von ICS-/OT-Umgebungen erfordert hochqualifizierte und zertifizierte Mitarbeiter, um Risiken effektiv zu managen. Unternehmen mit erfahrenem Personal sind besser aufgestellt, um Sicherheitspläne umzusetzen und widerstandsfähige Architekturen zu entwickeln – beides Schlüsselkomponenten der SANS Five ICS Cybersecurity Controls.

MEHR WERT

SANS 2024 State of ICS/OT Cybersecurity Report

„Ohne das richtige Humankapital können selbst die besten Technologien scheitern", so Fischer. Unternehmen müssen daher verstärkt in Schulungen und die Bindung von Talenten investieren.

ES BRAUCHT GEZIELTE INVESTITIONEN IN MENSCHEN, UM KRITISCHE INFRASTRUKTUREN WIDERSTANDSFÄHIGER ZU MACHEN.

Holger Fischer, Sales Director EMEA Central, OPSWAT, www.opswat.com

Die Rolle der Führungsebene

Eine zentrale Rolle bei der Stärkung der ICS-/OT-Sicherheit spielt die Führung durch Chief Information Security Officers (CISOs). Die Studie zeigt, dass Programme unter CISO-Leitung eine 82-prozentige Konformitätsrate mit Branchenstandards erreichen, während dezentral geführte Ansätze nur 42 Prozent erreichen. Dies unterstreicht, wie entscheidend eine starke Governance für die Cybersicherheitsstrategie und die Personalentwicklung ist.

Fazit: Mensch und Technologie vereinen

Der SANS 2024 ICS/OT Cybersecurity Report macht deutlich, dass die Stärkung der Belegschaft oberste Priorität haben muss. Unternehmen müssen ihre Sicherheitsbudgets neu ausrichten und in Schulungsprogramme investieren, um die wachsenden Herausforderungen in ICS-/OT-Umgebungen zu bewältigen. Nur durch die Kombination von technologischem Fortschritt und menschlicher Expertise können kritische Infrastrukturen wirksam geschützt werden.

Holger Fischer

Identitätsbetrug & Deepfakes

WIE SICH UNTERNEHMEN SCHÜTZEN KÖNNEN

Das Entrust Cybersecurity Institute veröffentlichte kürzlich die Ergebnisse seines 2025 Identity Fraud Report. Die weltweite Untersuchung belegt, dass künstliche Intelligenz die Häufigkeit und Raffinesse von Betrugsversuchen deutlich erhöht – Cyberkriminelle passen ihre Techniken immer weiter an, um existierende Abwehrmechanismen zu umgehen. 2024 fand alle fünf Minuten ein Deepfake-Angriff statt, die Fälschungen digitaler Dokumente nahmen im Vergleich zum Vorjahr um 244 Prozent zu.

Bild: Entrust

Die Bedrohungen haben weitreichende Auswirkungen auf alle Branchen, Behörden und Privatpersonen. Um Betrügern zuvorzukommen, sollten Sicherheitsteams ihre Strategien daher proaktiv anpassen und ihre Unternehmen auf die neue Realität vorbereiten. Dazu gehört insbesondere der Aufbau einer funktionierenden Zero-Trust-Architektur – für die wiederum identitätszentrierte Sicherheit die wesentliche Voraussetzung ist.

Maßgeschneiderte Lösungen für eine starke Abwehr

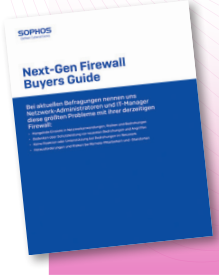
Für regulierte Branchen ist die digitale Verifizierung von Identitäten als Teil der Know-Your-Customer oder Anti-Geldwäsche-Vorschriften ohnehin nicht verhandelbar. Aber auch für nicht oder weniger regulierte Unternehmen bietet sie wesentliche Vorteile – einer davon ist die Betrugsprävention. Identitätsbetrug kann durch die Implementierung eines mehrschichtigen Ansatzes verhindert werden, der die Verifizierung von Dokumenten und biometrischen Merkmalen, die Erkennung wiederholter Betrugsversuche und die Validierung von Daten kombiniert. Eine Zero-Trust-Umgebung zur Verifizierung und Autorisierung von Kunden bildet eine starke Abwehr gegen sich weiterentwickelnde Betrugstechniken und hilft Unternehmen, ihren Kunden sichere, vernetzte Erfahrungen zu ermöglichen. Breit aufgestellte Sicherheitsexperten wie die von Entrust helfen dabei, für jedes Unternehmen eine maßgeschneiderte Lösung zu finden.

www.entrust.com

MEHR WERT
Identity Fraud Report

NEXT-GEN FIREWALL

WIE FINDEN SIE DIE RICHTIGE FIREWALL FÜR IHR UNTERNEHMEN?



WHITEPAPER DOWNLOAD

Das Whitepaper umfasst 11 Seiten und steht kostenlos zum Downloadbereit.

www.it-daily.net/download

Aktuelle Umfragen unter IT-Fachleuten decken kritische Schwachstellen gängiger Firewalls auf. Hauptprobleme sind mangelnde Einsicht in Netzwerkaktivitäten, Zweifel an der Schutzleistung gegen neueste Bedrohungen, fehlende Unterstützung bei erkannten Gefahren und Sicherheitsrisiken durch Remote-Arbeit.

Dieser Buyers Guide soll Ihnen dabei helfen, die richtige Firewall für Ihr Unternehmen zu finden, damit Sie Ihre Kaufentscheidung später nicht wie die von uns befragten IT-Netzwerk-Manager bereuen. Wir besprechen alle Funktionen, auf die Sie beim Kauf Ihrer nächsten Firewall achten sollten. Außerdem haben wir wichtige Fragen für Sie zusammengestellt, die Sie Ihrem IT-Partner oder -Anbieter stellen sollten, um sicherzustellen, dass das jeweilige Produkt auch wirklich Ihre Anforderungen erfüllt. Auf den letzten Seiten finden Sie zudem eine praktische Übersicht, die Ihnen dabei hilft, geeignete Firewall-Anbieter in die engere Auswahl zu ziehen.

Zero Trust

WARUM DIE MISSION WICHTIGER IST, ALS DIE PRODUKTE

KLASSISCHES RISK MANAGEMENT IN CYBER-SECURITY VERSAGT. STATT ENDLOSER RISIKO-ANALYSEN BRAUCHT ES PROAKTIVE SCHUTZMASS-NAHMEN WIE ZERO-TRUST-ARCHITEKTUREN.

John Kindervag, Chief Evangelist von Illumio, www.illumio.com

Zero Trust gilt als Schlüsselstrategie moderner Cybersicherheit. Im Gespräch mit it security-Publisher Ulrich Parthier erläutert John Kindervag, Chief Evangelist von Illumio und Architekt des Zero-Trust-Konzepts, warum dieser Ansatz wichtiger ist denn je.

Ulrich Parthier: *Herr Kindervag, wie hat sich Zero Trust aus Ihrer Sicht entwickelt?*

John Kindervag: Im Laufe meines Berufslebens habe ich verschiedene Positionen bekleidet, etwa als Netzwerkingenieur, Sicherheitsingenieur oder Sicherheitsarchitekt, und ich wurde oft gefragt: „Was sind die grundlegenden Probleme in der IT?" Meine Antwort war folgende: „Man definiert für jede Schnittstelle eine Vertrauensstufe, die in Richtlinien umgesetzt wird. Das interne Netz wird als vertrauenswürdig bezeichnet und hat die Vertrauensstufe Hundert, das externe Netz ist nicht vertrauenswürdig und hat die Vertrauensstufe Null. Daher brauchen Sie keine Richtlinie, um von einem Netzwerk mit hohem Vertrauensniveau zu einem Netzwerk mit niedrigem Vertrauensniveau zu wechseln. Jeder Datenverkehr kann also ohne Kontrolle von innen nach außen fließen." Das ist dumm. Denn alle Schnittstellen müssen die gleiche Vertrauensstufe haben, und zwar Null. Dies war im Jahr 2010 der Ursprung von Zero Trust. Ich habe das in zwei Papieren dokumentiert.

Ulrich Parthier: *Sie bezeichnen Segmentierung als das Fundament von Zero Trust. Wie kann Mikrosegmentierung zur Stärkung der Cyberresilienz und somit letztlich zur Minimierung von Risiken beitragen?*

John Kindervag: Normale Netzwerke sind leicht zu kompromittieren. Ich sage immer, wenn du ein flaches Netzwerk

ohne Segmentierung hast, bezahlst du vielleicht die Rechnungen, aber es gehört den Angreifern. Denn so ein Netzwerk bietet kaum Hindernisse oder Kontrollpunkte, um sich lateral zu bewegen. Aus diesem Grunde benötigen wir die Segmentierung. Es ist die Schlüsselkomponente in einer Security-Architektur, um Assets zu schützen. Das Verständnis für die Protect Surface – also was wie zu schützen ist – ist fundamental für das Verständnis von Zero Trust.

? **Ulrich Parthier:** *Würden Sie sagen, Zero Trust ist die Antwort auf moderne Cyberbedrohungen und die immer neuen Angriffsvektoren, die für die IT entstehen? Und warum reichen herkömmliche Sicherheitsmodelle nicht mehr aus?*

John Kindervag: Wenn ein erfolgreicher Angriff auf die IT-Infrastruktur erfolgt, dann liegt die Ursache in einer fehlerhaften Policy, die den Angriff nicht verhindert hat. Das bedeutet, wir sind nicht Opfer ein Cyberattacke, sondern eines Vorfalls, den eine Policy erlaubt hat. Alle schlechten Dinge geschehen, weil wir das zulassen – in Zero Trust-Umgebungen passiert das nicht. Solche Bedrohungen können wir ignorieren, denn wenn Policies diese nicht zulassen, sind sie schlicht obsolet.

? **Ulrich Parthier:** *Heutzutage spielt sich vieles in hybriden Cloud-Umgebungen ab. Wie verändert Zero Trust die Sicherheitsstrategien in Cloud- und On-Premises-Infrastrukturen?*

John Kindervag: Zero Trust ist es egal, wo die Protect Surfaces liegen. In der technischen Umsetzung kann es kleine Unterschiede geben, aber konzeptionell sind die Services gleich und basieren auf dem gleichen Framework.

? **Ulrich Parthier:** *Zero Trust ist ja kein fertiges Produkt, sondern eine Kombination aus Technologien, Prozessen, Schulungen und ja, letztendlich kommen auch Produkte zum Einsatz.*

John Kindervag: Zero Trust ist eine Strategie, die Produkte zur Umsetzung nutzt.

? **Ulrich Parthier:** *Aktuell gehören unter anderem Aspekte wie IAM, Mikrosegmentierung, mehrstufige Authentifizierung und Bedrohungs- und Anomalieerkennung zum Themenkreis von Zero Trust. Wenn wir über die Zukunft der Cybersicherheit und die Weiterentwicklung von Zero Trust und seine Rolle bei der Anpassung an neue Bedrohungen und Technologien kommen, wie sieht Ihr Szenario aus?*

John Kindervag: Bei Zero Trust geht es um die Mission, nicht um Produkte. Ziel ist es, die Folgen von Sicherheitsverletzungen zu minimieren. Das Implementierungsmodell wird sich nicht ändern, wohl aber mit der Zeit die Technologien und Kontrollmechanismen.

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

ZERO TRUST: WER HAT'S ERFUNDEN?

Zero Trust ist heute ein prägender Begriff in der IT-Sicherheit und vielfach ein Marketing Buzzword. Über die Herkunft gibt es unterschiedliche Ansichten. Und, nicht immer ist alles korrekt, was in Wikipedia steht.

Dort findet man die Aussage, der Begriff sei schon April 1994 erstmals von Stephen Paul Marsh in seiner Doktorarbeit zur Computersicherheit an der University of Stirling geprägt worden. Im Jahr 2010 benutzt schließlich der Analyst John Kindervag in einem Forschungsbeitrag für Forrester Research den Begriff des Zero-Trust-Modells. Dies stellte einen Paradigmenwechsel dar, von der Strategie „Vertrauen, aber überprüfen" hin zu „Nie vertrauen, immer überprüfen".

Das Modell von Kindervag sah die Verlagerung der Authentifizierung und Cybersicherheit in den Datenpfad sowie eine Segmentierung zwischen einzelnen Sitzungen vor. Es bleibt zwar weiterhin dem Paradigma des Netzwerkzugangs verhaftet, verschiebt den Sicherheitsperimeter jedoch ins Netzwerk.

Für sein Forschungspapier wurden laut Kindervag damals alle zugänglichen Quellen gescannt – zum Thema Zero Trust habe man jedoch nichts gefunden. Marsh schrieb allerdings bereits früher über die Vertrauenswürdigkeit digitaler Systeme – also das genaue Gegenteil von Zero Trust. Dessen Ziel ist es, besagtes Vertrauen in digitale Systeme komplett zu beseitigen, denn Vertrauen ist in der IT per se schlecht und eine Schwachstelle, die es zu vermeiden gilt.

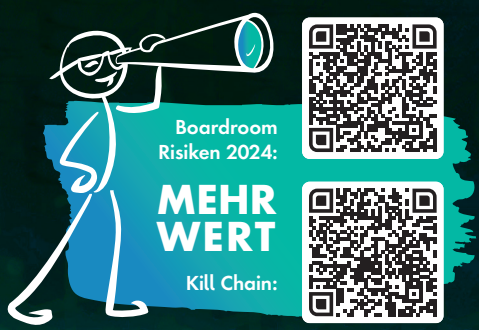
Cyberversicherung in der IT-Sicherheit

WARUM CYBERVERSICHERUNGEN HEUTE UNVERZICHTBAR SIND

Die Risikolandschaft für Unternehmen nimmt stetig zu – so auch Cyber-Risiken: Die fortschreitende Vernetzung und Digitalisierung von Geschäftsprozessen eröffnet nicht nur neue Chancen, sondern birgt auch erhebliche Risiken. Unternehmen jeder Größe müssen sich dieser Gefahr bewusst sein und entsprechend vorbeugende Maßnahmen ergreifen, um ihre IT-Infrastrukturen zu schützen. Eine Cyberversicherung bietet hierbei nicht nur finanzielle Absicherung, sondern auch Zugang zu wertvollen Ressourcen und Expertise, die im Ernstfall schnell und effizient zur Schadenbewältigung beitragen kann. In einer Zeit, in der Cyberangriffe immer häufiger und raffinierter werden, ist die Sinnhaftigkeit einer Cyberversicherung unumstritten.

Ein Katz-und-Maus-Spiel

Der Kampf zwischen Sicherheitsexperten und Cyberkriminellen gleicht einem ewigen Katz-und-Maus-Spiel. Jede neue Sicherheitsmaßnahme wird von Hackern auf Schwachstellen überprüft und – wenn entdeckt – ausgenutzt, um Zugriff auf ihr nächstes Opfer zu erlangen.



Daher reicht es nicht nur vereinzelt Sicherheitsmaßnahmen einzuführen. Eine mehrschichtige Sicherheitsstrategie ist notwendig, bei der nicht nur technische Maßnahmen, sondern auch organisatorische und personelle Aspekte berücksichtigt werden müssen. Die Cyberversicherung ist hierbei nicht nur ein Teil des rein finanziellen Risikotransfers: Optimal eingesetzt, kann sie die Resilienz eines Unternehmens gegenüber potenzieller Bedrohungen erhöhen und bei einer erfolgreichen Attacke dabei unterstützen, den Betrieb schnell wieder ins Laufen zu bringen.

Krisenmanagement als zentraler Baustein

Ein gut durchdachtes Krisenmanagement ist nicht nur reaktiv, sondern auch proaktiv, um Unternehmen auf den Ernstfall vorzubereiten. Ein wesentlicher Bestandteil einer Cyber-Police ist das Krisenmanagement. Unternehmensentscheider sollten auf Lösungen setzen, die umfassende Dienstleistungen anbieten, welche über die rein finanzielle Absicherung hinausgehen. Dazu gehören unter anderem Awarenessmaßnahmen, um Mitarbeitende für potenziell bösartige Szenarien zu sensibilisieren und die allgemeine Sicherheitskultur innerhalb einer Organisation zu erhöhen, die Überprüfung oder Erstellung von Notfallplänen, um sicherzustellen, dass ein Unternehmen im Fall eines Incidents schnell und effektiv reagieren kann, oder die Bereitstellung von IT-Forensikern, die innerhalb kürzester Zeit die Ursache und den Umfang eines Sicherheitsvorfalls analysieren können, um betroffene Systeme zu isolieren und weiteren Schaden zu verhindern (Incident-Response-Retainer).

Cyberversicherungen bieten auch Zugang zu spezialisierten Rechtsberatern, die Unternehmen durch die komplexen regulatorischen Anforderungen und Meldepflichten navigieren. Dies ist wichtig, um die Datenschutzgesetzte einzuhalten und so juristische Konsequenzen zu vermeiden, die sich aus Datenschutzverletzungen ergeben können. Besonders Bußgelder aufgrund der DSGVO sind ein viel diskutiertes Thema. Neben dem Zugriff auf Datenschutzexperten bietet die Cyberversicherung auch den schnellen Zugang zu PR-Beratern, die das sich in der Cyber-Krise befindliche Unternehmen im Rahmen von Öffentlichkeitsarbeit unterstützen, um einen möglichen Reputationsschaden zu minimieren.

Ob groß oder klein – jedes Unternehmen steht im Visier

Größere Unternehmen und Konzerne sind sich der möglichen Cyber-Risiken oft bewusster und verfügen über mehr Ressourcen, um sich gegen Cyberangriffe zu verteidigen. Dennoch sind sie aufgrund ihrer komplexen IT-Infrastrukturen und vielfältigen Technologien angreifbar. Das etablierte Cyber-Risikomanagement kann es Hacker-Gruppen, die häufig den Weg des geringsten Widerstands bevorzugen, erschweren, erfolgreiche Attacken auszuführen. Dies führt dazu, dass auch kleine und mittelständische Unternehmen ein attraktives Ziel von Kriminellen sind. Sie zeichnet häu-

fig eine geringere Resilienz gegenüber Cyber-Bedrohungen aus und somit größere Erfolgschancen für die Angreifer.

Hinzukommend sind kleinere Unternehmen in der digitalen Supply Chain oft mit zahlreichen weiteren Organisationen vernetzt und können somit als Einfallstor zur Attacke auf größere Unternehmen ausgenutzt werden. Ein Beispiel dafür ist die Kill-Chain eines Hacks aus 2013, wobei Target, einer der größten US-Einzelhändler, Opfer eines erfolgreichen Cyberangriffs war.

Digitale Ökosysteme - weitreichendes Schadenpotenzial

Viele IT-Abteilungen weltweit beschäftigte im Sommer 2024 die Eindämmung der Folgen eines fehlerhaften Sicherheitspatches: Das von Cybersecurity-Dienstleister CrowdStrike zur Verfügung gestellte und fehlerhafte Update für seine Software Falcon verursachte bedeutende IT-Ausfälle und in Folge dessen Betriebsbeeinträchtigungen (zum Beispiel im Flugverkehr, der Industrie und Kommunikationsunternehmen) und erreichte circa 8,5 Millionen Windows-Geräte weltweit.

Es ist wichtig darauf hinzuweisen, dass dieser Incident nicht etwa aus böswilliger Motivation entstanden ist und ein Patch bereits in kürzester Zeit bereit stand, um die IT-Infrastruktur schnell wieder ins Laufen zu bringen. Dennoch hatten vor allem Fluggesellschaften weitreichende Betriebsstörungen und mussten zahlreiche Flüge verschieben oder gar stornieren, wodurch Millionenschäden entstanden. Auch Krankenhäuser waren betroffen, die Eingriffe, wenn möglich, verschieben oder ihre Notaufnahme schließen mussten.

Sicherheitsexperten sind überzeugt, dass ein ähnlicher böswilliger Angriff dieser Art auf in vielen Unternehmen genutzte Sicherheitsarchitektur einen weitreichenderen und dramatischeren Verlauf gezeigt hätte.

Der Fall Crowdstrike hat veranschaulicht wie fragil globale Technologienetzwerke sind und welche Konsequenzen im Ökosystem folgen können, wenn ein Glied in der digitalen Lieferkette von einer Informationssicherheitsverletzung betroffen ist.

Cyberversicherungen mit weitem Deckungsumfang, wie des Spezialversicherers Beazley, tragen nicht nur Schäden aufgrund von zielgerichteten Angriffen auf den Versicherungsnehmer, sondern auch solche Schäden, die aufgrund von Informationssicherheitsverletzungen (böswillig oder zufällig) im abhängigen Computersystem entstehen.

> CYBERVERSICHERUNGEN BIETEN NICHT NUR FINANZIELLEN SCHUTZ IM FALLE EINES ANGRIFFS, SONDERN AUCH DEN MEHRWERT DES ZUGANGS ZU EXPERTEN UND DIENSTLEISTUNGEN.
>
> **Gesine Froese,**
> **Regional Manager Cyber Risks DACH,**
> **Beazley, www.beazley.com**

Fazit:
Schutz auf verschiedenen Ebenen

Cyberversicherungen bieten nicht nur finanziellen Schutz im Falle eines Angriffs, sondern auch den Mehrwert des Zugangs zu Experten und Dienstleistungen, die Unternehmen bei der Schadenbewältigung und -eindämmung unterstützen. Ob durch die schnelle Unterstützung durch IT-Forensiker bis hin zur rechtlichen Beratung – der Assistance-Aspekt der Police trägt dazu bei, dass Unternehmen nach einem Angriff schnell wieder operativ tätig werden können.

Gesine Froese

Cybersicherheit im Mittelstand

WARUM EIN ISMS DEN ENTSCHEIDENDEN UNTERSCHIED MACHT

Die Bedrohung durch Cyberangriffe nimmt stetig zu. Laut Bitkom e.V. verursachten Cyberangriffe allein in Deutschland im Jahr 2023 einen Gesamtschaden von über 205 Milliarden Euro – das entspricht rund 500.000 Euro Schaden pro betroffene Unternehmen. Trotz des technischen Fortschritts sind viele Unternehmen nicht ausreichend auf die neuen Bedrohungen vorbereitet. Der Grund? Häufig mangelt es nicht an technischen Lösungen, sondern an organisatorischer Resilienz.

Hier setzt ein Informationssicherheitsmanagementsystem (ISMS) an. Es schafft eine systematische Grundlage zur Identifikation, Bewertung und Behandlung von Risiken, die nicht nur den Schutz der Infrastruktur verbessern, sondern auch die strategische Entscheidungsfindung unterstützen.

Organisation versus Technik

Moderne IT-Infrastrukturen sind meist auf einem hohen technischen Niveau. Unternehmen investieren in Firewalls, Antivirus-Software und Überwachungssysteme. Doch Technik allein reicht nicht aus: Rund 70 Prozent der Cybervorfälle lassen sich auf organisatorische Mängel und Fehlverhalten von Mitarbeitenden zurückführen.

Ein ISMS wie die VdS 10000 (angelehnt an ISO 27001) greift genau hier ein. Es hilft, Risiken klar zu benennen, Prozesse zu analysieren und Verantwortlichkeiten festzulegen. Vor allem aber fördert es einen kontinuierlichen Verbesserungsprozess (KVP), der auf langfristige Sicherheit abzielt.

Vorteile für Kunden und Versicherungen

Für Unternehmen bietet eine Zertifizierung nicht nur Sicherheit nach innen, sondern auch Transparenz nach außen. Kunden verlangen zunehmend Nachweise über Informationssicherheit – vor allem im B2B-Bereich. Eine Zertifizierung signalisiert, dass das Unternehmen proaktiv Risiken adressiert und Schutzmaßnahmen implementiert hat.

Darüber hinaus eröffnet ein ISMS die Möglichkeit, Cyberrisiken präzise zu quantifizieren. In der Zusammenarbeit mit Cyberversicherern ermöglicht dies die gezielte Gestaltung der Versicherungspolice. Unternehmen können konkret benennen, welche Risiken abgedeckt werden sollen, und profitieren so von einer optimierten Kostenstruktur.

Beispiel aus der Praxis

Ein mittelständisches Unternehmen der Automobilzuliefererbranche führte ein

ISMS ein, um die Anforderungen seiner internationalen Kunden zu erfüllen. Bereits im ersten Jahr nach der Zertifizierung wurden signifikante Verbesserungen erzielt: Risiken in der Lieferkette wurden frühzeitig erkannt und durch gezielte Maßnahmen minimiert. Darüber hinaus konnte das Unternehmen bei seiner Cyberversicherung eine Prämienreduzierung von 15 Prozent erreichen – ein klarer Wettbewerbsvorteil.

Rechtliche Anforderungen und NIS2

Mit der NIS2-Richtlinie, die aufgrund der aktuellen Spannungen in der Bundesregierung voraussichtlich nicht vor März 2025 in nationales Recht überführt wird, steigen die regulatorischen Anforderungen an Unternehmen. Ein ISMS erleichtert die Erfüllung dieser gesetzlichen Vorgaben, indem es die notwendigen Maßnahmen zur Risikobewertung und Dokumentation systematisch abdeckt. Besonders in Sektoren, die als kritische Infrastruktur gelten, wird dies zu einer unverzichtbaren Pflicht.

Fazit

Cybersicherheit ist nicht länger ein optionales IT-Thema, sondern ein zentraler Bestandteil der Unternehmensstrategie. Ein ISMS hilft, Risiken zu verstehen, organisatorische Schwachstellen zu schließen und kontinuierlich zu verbessern. Für Kunden schafft dies Vertrauen, für Versicherer Transparenz und für das Unternehmen selbst eine resiliente, zukunftsfähige Basis.

Ein starkes ISMS ist mehr als ein technischer Schutzwall – es ist das Fundament für die sichere und erfolgreiche Zukunft des Mittelstands.

Thomas Adenauer

CYBERSICHERHEIT IST NICHT LÄNGER EIN OPTIONALES IT-THEMA, SONDERN MUSS ZU EINEM ZENTRALEN BESTANDTEIL DER DIGITALEN UNTERNEHMENSSTRATEGIE WERDEN.

Thomas Adenauer,
Abteilungsleiter VdS Cyber-Security,
VdS Schadenverhütung GmbH,
www.cyber.vds.de

ISO/IEC 27001: Sinnvolle Grundlage für NIS2?

PRAKTISCHE HILFESTELLUNGEN FÜR GESETZESKONFORMITÄT

NIS2 ist gekommen, um zu bleiben. Auch im neuen Jahr beschäftigt die EU-Richtlinie zahlreiche IT-Verantwortliche. Kann ISO/IEC 27001 als solide Grundlage für NIS2 Compliance dienen? Wo gibt es Überschneidungen, wo Diskrepanzen? Und was können Unternehmen ganz praktisch machen, um NIS2-compliant zu werden?

Überblick ISO/IEC 27001

ISO/IEC 27001 ist die international führende Norm für Informationssicherheits-Managementsysteme (ISMS). Sie ermöglicht Unternehmen, ein effektives Information Security Management System zu etablieren und zu pflegen. Damit wird die Informationssicherheit für Organisationen transparenter und ihre Cyberresilienz gesteigert. Eine Zertifizierung nach ISO/IEC 27001 ist grundsätzlich freiwillig. Jedoch sind Betreiber Kritischer Infrastrukturen (KRITIS) seit 2018 gemäß IT-Sicherheitsgesetz dazu verpflichtet, alle zwei Jahre die Umsetzung eines Informationssicherheits-Managementsystems nachzuweisen. Nicht wenige liefern diesen Nachweis in Verbindung mit einer erfolgreichen Zertifizierung nach ISO/IEC 27001.

ISO/IEC 27001 und NIS2

Die Norm umfasst in ihren 10 Kapiteln und ihrem Anhang detaillierte Ansätze, Methoden und Schritte, die dazu beitragen, die umfassenden Anforderungen von NIS2 zu erfüllen, und ist für alle in der EU tätigen Unternehmen relevant, die mit sensiblen Informationen umgehen. Die NIS2-Richtlinie bezieht sich in Abschnitt 79 direkt auf die ISO/IEC 27000-Reihe. Insgesamt deckt die Norm bereits viele Anforderungen von NIS2 ab. Jedoch gibt es spezifische zusätzliche Anforderungen, die berücksichtigt werden müssen.

Wo passen ISO/IEC 27001 und NIS2 (nicht) zusammen?

Ganz konkret deckt die ISO/IEC 27001 NIS2-Anforderungen in zahlreichen Bereichen ab – von der Risikoanalyse, über das Krisenmanagement bis hin zur Bewertung der Wirksamkeit von Maßnahmen – und wird am Stand der Technik (in der jeweiligen Branche) gemessen. Jedoch gibt es auch gewisse Unterschiede in der Zertifizierung, so dass Unternehmen in diesen Bereichen zusätzliche Maßnahmen ergreifen müssen, um ihre NIS2-Compliance zu erreichen. Die Details dazu liefert die Tabelle auf der rechten Seite.

NIS2 Compliance nachweisen – Zertifikat notwendig?

NIS2 unterscheidet zwischen wesentlichen und wichtigen Einrichtungen, die unterschiedliche Vorgaben zu erfüllen haben. Auf dem Weg zu NIS2-Compliance empfiehlt sich für alle betroffenen Organisationen als erster Schritt ein Risiko-Assessment und eine Gap Analyse. Sie helfen Schwachstellen in bereits etablierten Cybersecurity-Maßnahmen aufzudecken. Auf dieser Basis können die Unternehmen dann Verbesserungen vornehmen. Entweder lassen sie sich dann nach ISO 27001 zertifizieren und erfüllen zusätzlich die obengenannten NIS2 spezifischen Vorgaben. Alternativ können sie nachweislich Konformität auf der Grundlage der Schließung der im NIS2-Risikobewertungsbericht festgestellten Lücken sowie der Aufrechterhaltung und kontinuierlichen Verbesserung des ISMS erlangen. Als kleinere oder mittelgroße Organisation ist es wichtig, sich zuerst auf die ISMS-Implementierung zu konzentrieren, da eine ISO 27001 Zertifizierung für wichtige Einrichtungen zweitrangig – und nicht immer unbedingt notwendig – ist.

Anforderung	NIS 2	ISO 27001
Incident Reporting	Verpflichtung zur externen Meldung von erheblichen Vorfällen, die die Sicherheit von Netzwerken und Informationssystemen betreffen, an die zuständigen Behörden oder CSIRTs erforderlich.	Schwerpunkt auf internem Incident Reporting, ohne ausdrückliche Verpflichtung zur externen Berichterstattung.
Zusammenarbeit mit Behörden	Eine aktive Zusammenarbeit mit den nationalen Behörden und CSIRTs bei erheblichen Sicherheitsvorfällen oder Inspektionen ist erforderlich. Dazu gehört, wenn notwendig, auch die Kommunikation mit der Öffentlichkeit.	Die Organisation muss mit den zuständigen Behörden Kontakt aufnehmen und halten.
Einhaltung von Verhaltenskodizes	Die Angleichung an EU- oder nationale Code of Conducts und sektorspezifische Standards ist vorgeschrieben.	Im Rahmen des Geltungsbereiches des ISMS sind entsprechende Gesetze und Vorgaben (bspw. spezifische Standards) einzuhalten.
Governance-Anforderungen	Die Geschäftsleitung muss das Risikomanagement genehmigen und beaufsichtigen. Außerdem muss das Management regelmäßige Schulungen zur Cybersicherheit absolvieren und ist für die Überwachung der Cybersicherheit verantwortlich.	Das Management trägt die Verantwortung für das Managementsystem, angemessene Sensibilisierung muss vorhanden sein und regelmäßig aufgefrischt werden.
Sicherheit der Lieferkette	Erfordert umfassende Sicherheitsbewertungen und -kontrollen in der gesamten Lieferkette, die das Risiko Dritter und Lieferantenbeziehungen abdecken.	Enthält Kontrollen für (einzelne, relevante) Lieferantenbeziehungen, aber keine detaillierten Anforderungen an die Lieferkettensicherheit.
Einsatz von Kryptographie und Verschlüsselung	Bestimmt formalisierte Kryptografierichtlinien, die Einhaltung bestimmter Verschlüsselungsprotokolle und regelmäßige Aktualisierungen der Kryptografiestandards.	Es müssen Regeln für den wirksamen Einsatz von Kryptographie inklusive der verwendeten Schlüssel geschaffen werden.
Security im Bereich Personal	Legt explizite Richtlinien für die Zugangskontrolle, die Verwaltung von Vermögenswerten und andere personalbezogene Sicherheitspraktiken fest.	Befasst sich weniger detailliert mit HR-Sicherheitskontrollen, sondern primär mit allgemeinen Sicherheitsüberprüfungen ohne spezifische rollenbasierte Anforderungen. Diese kann ggf. durch die Organisation erfolgen.
Verwendung von Multi-Faktor-Authentifizierung (MFA) und sicherer Kommunikation	Verpflichtung zur Nutzung von MFA, sicherer Kommunikationsprotokolle und Notfallkommunikationssysteme.	Enthält allgemeine Kontrollen zur Authentifizierung und Kommunikationssicherheit, insbesondere zur Implementierung von sicheren Authentisierungstechnologien und -verfahren ohne spezifische Verpflichtung zu MFA oder Notfallprotokollen.

Praktische Tipps für die Umsetzung von NIS2

Schenken Sie besonders den Abschnitten Aufmerksamkeit, die sowohl in ISO/IEC 27001 als auch in NIS2 am häufigsten vorkommen, wie zum Beispiel dem ISMS-Anwendungsbereich und dem Verzeichnis der Vermögenswerte, der Risikoidentifizierung und -bewertung, Incident Response und Schwachstellenmanagement, Zugriffskontrolle, Endpoint- und Netzwerksicherheit sowie der Schaffung eines Bewusstseins für Informationssicherheit und Cyberhygiene. Orientieren Sie sich dafür gerne an dem von ENISA veröffentlichten Konsultationsentwurf zur Umsetzung von Sicherheitsmaßnahmen gemäß NIS2.

Erstellen Sie eine erweiterte Anwendbarkeitserklärung (Statement of Applicability, SoA), die über das geforderte SoA der ISO/IEC 27001 hinausgeht und NIS2-spezifische Anforderungen und Kontrollen enthält.

Dokumentieren Sie Ihre Konformitätsbemühungen, und legen Sie klare Rollen und Verantwortlichkeiten fest. Führen Sie außerdem regelmäßige Überprüfungen durch, um die Konformität kontinuierlich zu gewährleisten.

Denken Sie daran: NIS2 existiert nicht isoliert. Prüfen Sie, welche anderen EU-, nationalen und branchenspezifischen Sicherheitsanforderungen und -standards in Verbindung mit NIS2 berücksichtigt werden müssen. Stellen Sie sicher, dass alle anderen relevanten Anforderungen und Standards (DORA, CER, GDPR, EU-RCE-Richtlinie, IEC 62443) identifiziert und in eine Liste von Anforderungen aufgenommen werden.

Auch wenn IT-Verantwortliche NIS2 mittlerweile nicht mehr hören können – das Gesetz wird auch in Deutschland kommen. Daher ist es spätestens jetzt an der Zeit mit Risk-Assessments und Gap Analysen zu beginnen und ein ISMS aufzubauen.

Thomas Janz, Richard Skalt
www.tuvsud.com

Der FIDO-Standard als Investitionssicherheit

PASSWORTLOS IN DIE ZUKUNFT

Die FIDO-Alliance ist mit dem Ziel angetreten, die Verwundbarkeit durch Cyberangriffe zu reduzieren, indem die Authentifizierungsstandards verbessert werden sollen. Der Authentifizierungsstandard FIDO2, verspricht eine passwortlose Zukunft, die mit der Einführung von Passkeys den Nutzern mehr Sicherheit schenken soll. Doch längst noch nicht alle setzen diese Technologie aktuell ein – dabei rechnet sich die Investition, denn sie ist vor allem eines: zukunftssicher.

Mit der Entwicklung hin zu hybriden Arbeitsmodellen kommen neue Herausforderungen auf die Unternehmen zu. Denn um alle in der Cloud gespeicherten Daten abzusichern, braucht es zuverlässige Lösungen. Hinzu kommt, dass die Anforderungen der NIS2-Richtlinie erfüllt werden müssen. Unternehmen, die unter die NIS2-Regelung fallen, sind angehalten, alle Nutzer mit einer Multi-Faktor-Authentifizierung abzusichern und Kryptographie zu nutzen. Ansonsten drohen Unterbrechungen des Geschäftsbetriebs und die Kompromittierung von Netzwerken und Systemen durch Cyberkriminelle. Die aktuelle Bedrohungslage fordert hohe Sicherheitsstandards und eine Null-Toleranz-Strategie. So müssen die Identitäten der Mitarbeiter mit einer effizienten Authentifizierungslösung geschützt werden. Weitere wichtige Aspekte sind die Absicherung aller Endgeräte, die auf das Unternehmensnetzwerk zugreifen sowie die Datensicherheit.

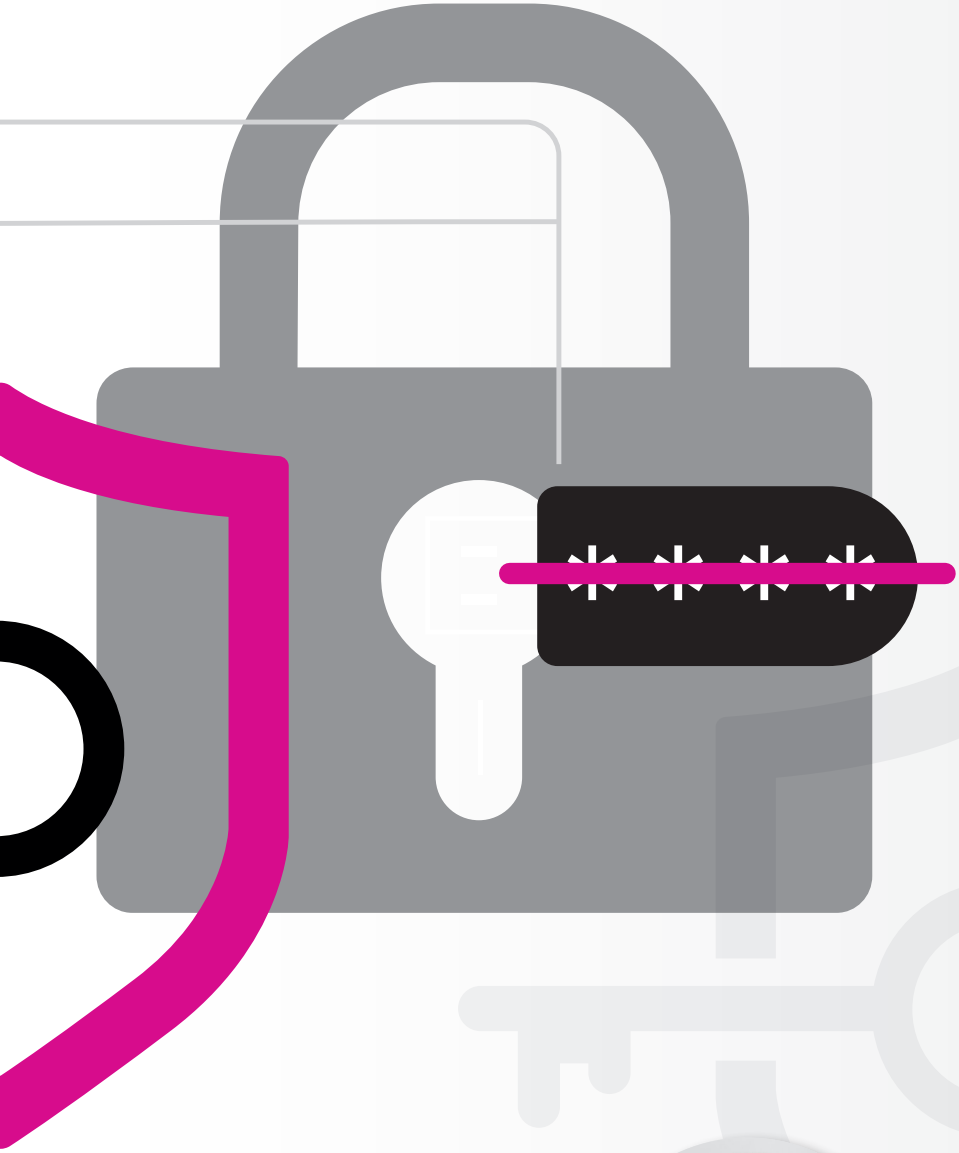
Eine starke Authentifizierung als Basis

Der Schutz der Identität ist die Basis einer effektiven Null-Toleranz-Strategie. Hier ist es einerseits entscheidend, dass die eingesetzte Authentifizierungslösung nicht umgangen werden kann. Andererseits sollen alle Beteiligte vor Phishing und anderen Angriffsmethoden zuverlässig geschützt werden. Gerade dann, wenn auch private Endgeräte für das mobile Arbeiten hinzugezogen werden, werden Sicherheitsmaßnahmen gerne umgangen. Alternative Multi-Faktor-Authentifizierungslösungen (MFA) wie SMS, mobile Push-Benachrichtigungen und Einmal-Passwörter (OTP) reichen nicht aus, um Angriffe zu verhindern und öffnen gerade Man-in-the-Middle-Attacken Tür und Tor.

Eine Lösung stellen Sicherheitsschlüssel dar, die auf dem FIDO2-Standard basieren, zusätzlich auch noch andere Protokolle unterstützen und eine Phishing-resistente MFA bieten, die Kontoübernahmen einen Riegel vorschieben.

FIDO2 – für eine Zukunft ohne Passwörter

Der offene und lizenzfreie Industriestandard FIDO2 ermöglicht eine sichere, schnelle und einfache Authentifizierung. Bei den FIDO-konformen Passkeys handelt es sich um Paare aus privaten und öffentlichen Schlüsseln, die auf dem Branchenstandard WebAuthn basieren. Produkte, die auf diesem Standard basieren, wie der Sicherheitsschlüssel YubiKey von Yubico, nutzen zur hardwaregestützten Authentifizierung Fingerabdruck oder PIN. Da sie nicht kopiert oder synchronisiert werden können, handelt es sich bei den hardwaregebundenen YubiKeys um die sicherste Form der Passkeys. Nutzer können sich so problemlos bei beispielsweise Online-Services anmelden – ganz ohne die Notwenigkeit von Passwörtern. Das Client to Authenticator Protocol (CTAP) schafft einen sicheren Datenaustausch zwischen der im Webbrowser laufenden WebAuthn-Anwendung und dem damit verbundenen



Hardware-Token, welches über USB, NFC oder BLE verbunden ist. Diese Hardware-Token unterstützen in der Regel neben FIDO auch andere Sicherheitsprotokolle, wie OTP oder CCID, die auch zusammen eingesetzt werden können.

Der Vorteil: Weder werden die verschlüsselten FIDO2-Zugangsdaten auf einem Server gespeichert, noch verlassen sie das vom Nutzer zur Authentifizierung eingesetzte Gerät, noch werden sie über das Internet versendet. Phishing, Datendiebstahl oder Man-in-the-Middle-Angriffe werden so effektiv verhindert. Zusätzlich schützt FIDO2 vor geklonten Authentifikatoren. Kommen gefälschte Tokens zum Einsatz, wird der Zugriff unterbunden. Die gewünschte Sicherheitsstufe – 2FA oder MFA – lässt sich für jede Anwendung und Nutzer konfigurieren, sodass ein dynamischer Umstieg möglich ist.

Nicht nur zukunftssicher, auch investitionssicher

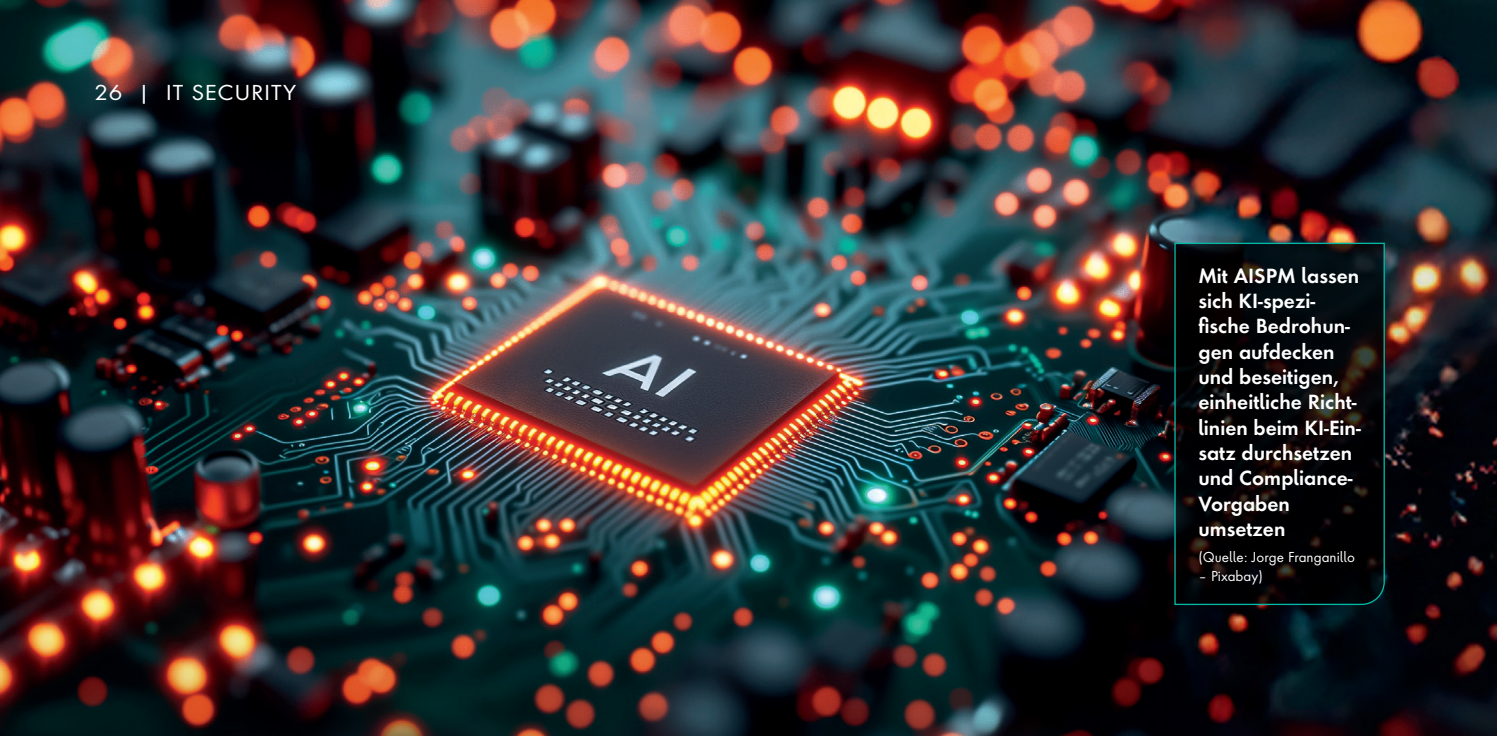
Offene Standards wie FIDO2 bieten Unternehmen absolute Entscheidungsfreiheit bei der Endgeräteauswahl, sodass die Mitarbeiter stets vor identitätsbasierten Cyberangriffen wie Phishing geschützt sind, unabhängig davon, auf welchen Geräten sie arbeiten. Hardware-basierte, phishing-resistente Multifaktor-Authentifizierungslösungen, die auf offenen Standards wie FIDO2 basieren, unterstützen außerdem eine Vielzahl an Authentifizierungsprotokollen und sind in diversen Formfaktoren und mit mehreren Anschlüssen, wie USB-A, USB-C, Lightning und NFC, erhältlich. So ist sichergestellt, dass sie von nahezu jeder Organisation und jedem Nutzer verwendet werden können.

Ein weiterer Faktor, der auf die Investitionssicherheit einzahlt, ist die Auslastung der Helpdesk-Mitarbeiter. Unternehmen verwenden viel Zeit und Personalressourcen für die Einrichtung und Verwaltung von Passwortrichtlinien, während die Nutzer mit nervigen Passwort-Richtlinien und -zurücksetzungen zu kämpfen haben. Organisationen, die veraltete MFA-Lösungen verwenden, haben außerdem Probleme mit schlechten Nutzererfahrungen, veralteten Protokollen und minderwertiger Hardware. Hardware-Tokens auf Basis von FIDO2 eliminieren praktisch das Risiko von Phishing und Diebstahl von Anmeldeinformationen, fördern das Geschäftswachstum aufgrund des hohen Sicherheitsniveaus sowie der gestiegenen Reputation und verbessern die Produktivität und Benutzererfahrung.

Alexander Koch

DER OFFENE UND LIZENZFREIE INDUSTRIE-STANDARD FIDO2 ERMÖGLICHT EINE SICHERE, SCHNELLE UND EINFACHE AUTHENTIFIZIERUNG.

Alexander Koch, VP Sales EMEA, Yubico, www.yubico.com



Mit AISPM lassen sich KI-spezifische Bedrohungen aufdecken und beseitigen, einheitliche Richtlinien beim KI-Einsatz durchsetzen und Compliance-Vorgaben umsetzen

(Quelle: Jorge Franganillo – Pixabay)

AI Security Posture Management (AISPM)

SICHERHEIT FÜRS KI-ZEITALTER

Künstliche Intelligenz ist aus den meisten Unternehmen nicht mehr wegzudenken, birgt aber Risiken – vom Abfluss sensibler Daten bis hin zu falschen Ausgaben und Entscheidungen durch manipulierte Trainingsdaten und Modelle. Ein AI Security Posture Management (AISPM) hilft, die Entwicklung und Nutzung von KI abzusichern.

Künstliche Intelligenz ist eine transformative Technologie, die nicht nur einzelne Unternehmen, sondern ganze Branchen verändert. Sie hilft, Abläufe zu automatisieren, Mitarbeiter zu entlasten, bessere Entscheidungen zu treffen und Kosten zu senken – weshalb viele Unternehmen den KI-Einsatz schnell vorantreiben, um möglichst keine Chancen zu verpassen. Dass damit erhebliche Sicherheitsrisiken einhergehen, ist ihnen allerdings nicht immer bewusst.

Eine unterschätzte Gefahr ist der Abfluss sensibler Daten, wenn Mitarbeiter interne Dokumente beispielsweise von externen KI-Services optimieren oder zusammenfassen lassen. Enthalten die Dokumente personenbezogene Daten, kann das einen Verstoß gegen die DSGVO darstellen, so es sich um Dienste außerhalb der EU handelt. Schließlich landen alle Eingaben und Uploads auf den Servern der Anbieter und werden dort gespeichert und verarbeitet.

Das gilt auch für vertrauliche Informationen wie Finanzdaten oder geistiges Eigentum, die etwa durch einen Angriff auf den KI-Service an die Öffentlichkeit gelangen können. Verwendet der Anbieter die Nutzereingaben zur Verbesserung seiner KI-Modelle, können die internen Daten sogar in den Antworten für andere Nutzer des Services auftauchen.

KI ist nur so gut wie die Trainingsdaten

Auch bei selbstentwickelten KI-Anwendungen besteht das Risiko von Datenabflüssen, schließlich lebt KI von großen Datenmengen – je mehr Informationen zum Training oder Fine-Tuning eingesetzt werden, desto besser sind die Prognosen, Entscheidungen und generierten Inhalte. Befinden sich sensible Daten im Trainingsmaterial, tauchen diese möglicherweise in den Ausgaben für Mitarbeiter auf, die eigentlich keinen Zugriff auf diese Daten haben sollten – oder schlimmer: in den Ausgaben für externe Nutzer.

Darüber hinaus stehen die Trainingsdaten zunehmend im Visier von Cyberkriminellen, die durch Manipulationen versuchen, KI-Modelle gezielt zu schwächen oder zu infiltrieren. Das heißt, auf den Modellen basierende Anwendungen liefern dann allgemein oder in einzelnen Bereichen schlechtere Ergebnisse oder generieren bei einem bestimmten Input einen ganz spezifischen, vom Angreifer erwünschten Output. Neben manipulierten Trainingsdaten sorgen allerdings auch schlechte oder schlecht ausgewählte Trainingsdaten für proble-

matische Ergebnisse – etwa ungenaue Prognosen oder unfaire, vorurteilsbehaftete Entscheidungen und Inhalte.

Und nicht zuletzt existieren operative Risiken beim KI-Einsatz – beispielsweise unvorhergesehene Reaktionen des Modells, die wichtige Geschäftsprozesse unterbrechen, oder eine schleichende Verschlechterung der Ergebnisse, wenn sich Datenquellen verändern oder wegfallen.

Mit der KI-Discovery fängt alles an

Ein Ansatz, um die mit dem KI-Einsatz verbundenen Risiken in den Griff zu bekommen, ist AI Security Posture Management (AISPM). Anders als ein Cloud Security Posture Management (CSPM), das sich auf Cloud-Risiken konzentriert, oder ein Data Security Posture Management (DSPM), das den gesamten Lebenszyklus von Daten abdeckt, fokussiert es sich auf die Sicherheit von KI – unabhängig davon, ob es sich um klassische oder generative KI, externe Services oder intern entwickelte Anwendungen handelt. Allerdings gibt es durchaus Überschneidungen zwischen den Ansätzen und den eingesetzten Security-Lösungen.

Eine wichtige Komponente von AISPM ist die KI-Discovery – das Erkennen der im Unternehmen eingesetzten KI-Tools und -Services, darunter auch Schatten-KI, die einzelne Fachbereiche oder Mitarbeiter ohne Wissen der IT-Abteilung nutzen. Mithilfe der so gewonnenen Aufstellung können Unternehmen Risikobewertungen vornehmen, unter anderem in Bezug auf Datensicherheit, Modellintegrität und operative Auswirkungen des KI-Einsatzes. Und sie können unautorisierte Services sperren beziehungsweise legalisieren, indem sie die Services ins Sicherheitskonzept integrieren.

Natürlich ist die Discovery und Evaluierung von KI-Anwendungen keine einmalige Angelegenheit, sondern eine regelmäßig durchzuführende Tätigkeit, da sich KI schnell weiterentwickelt, immer mehr Tools und Services verfügbar sind und auch die Bedrohungslandschaft sich kontinuierlich verändert.

Einheitliche Regeln durchsetzen

AISPM unterstützt Unternehmen dabei, Fehlkonfigurationen aufzuspüren, die beispielsweise den Abfluss von Daten oder den unautorisierten Zugriff auf KI ermöglichen. Unternehmen können so in die Lage versetzt werden Konfigurationsregeln zentral zu definieren und über alle KI-Tools und -Services hinweg durchzusetzen. Ebenso können sie dazu befähigt werden, dass der KI-Einsatz regulatorischen Vorgaben entspricht und konform zu internen Compliance-Richtlinien erfolgt. Dazu zählt auch die Umsetzung einer robusten Data Governance, die für sichere, korrekte und ausgewogene Trainingsdaten sorgt und diese durch Verschlüsselung und strenge Zugriffskontrollen schützt.

Ein kontinuierliches Monitoring der KI-Tools und -Services deckt Schwachstellen und mögliche Bedrohungen auf und erlaubt es, Sicherheitsmaßnahmen anzupassen und Angriffspfade zu eliminieren.

UNTERNEHMEN SOLLTEN DAS THEMA AISPM NICHT AUF DIE LANGE BANK SCHIEBEN, SONDERN PROAKTIV HANDELN, UM DATENSICHERHEITSRISIKEN ZU MINIMIEREN.

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

Datensicherheit als Einstieg ins AISPM

Da es sich bei AISPM um einen recht neuen Ansatz handelt, hat sich noch kein festes Features-Set für AISPM-Lösungen etabliert. Mit dem wachsenden Bewusstsein für das Thema und der damit verbundenen Nachfrage wird sich das aber voraussichtlich bald ändern.

Einstweilen sind die CASB- (Cloud Security Access Broker) und Secure-Web-Gateway-Funktionen (SWG) sowie die Fähigkeiten zur Data Discovery und Datenklassifizierung, die DSPM-Lösungen mitbringen, ein guter Einstieg. Mit ihrer Hilfe können Unternehmen externe KI-Services aufspüren und die Nutzung reglementieren. Ebenso können sie sensible Daten identifizieren und vor unbefugten Zugriffen schützen. Risikobasierte Mechanismen passen den Schutz dabei kontextabhängig und in Echtzeit an. Ergänzend dazu verhindert eine DLP-Lösung, dass sensible Informationen bei KI-Tools und -Services eingegeben werden.

Bei der Datenklassifizierung, die früher sehr aufwendig war, setzen DSPM-Lösungen selbst auf KI, um den Prozess weitgehend zu automatisieren. Mit verschiedenen Small Language Models, die sehr schnell und ressourcenschonend sind, können Unternehmensdaten zuverlässig klassifiziert werden und die Genauigkeit steigt dank Machine-Learning kontinuierlich.

Letztlich sollten Unternehmen das Thema AISPM nicht auf die lange Bank schieben, sondern proaktiv handeln, um Datensicherheitsrisiken zu minimieren. Als goldene Regel gilt hier - das Fundament bildet eine flächendeckende Datenklassifizierung.

Fabian Glöser

Unternehmens IT und geopolitische Krisen

WIE DIE GEOPOLITISCHE LAGE IT IN UNTERNEHMEN FORDERT

Die geopolitische Lage ist äußerst angespannt und politische Gegebenheiten, die für die Weltgemeinschaft bisher selbstverständlich waren, werden in Frage gestellt. Dies hat mittlerweile nicht nur politische, sondern gleichermaßen auch wirtschaftliche Auswirkungen auf Unternehmen und ihre IT.

Die hybriden Bedrohungen und daraus resultierenden Risiken, die von diesen Konflikten ausgehen, sind real, was zahlreiche Vorfälle wie das Kappen von Unterseekabeln, Cyberangriffe und Wahlbeeinflussung zeigen. Nicht umsonst diskutiert die NATO neue Strategien zur Abwehr hybrider Angriffe. Dabei spielt auch die Destabilisierung von Lieferketten eine wichtige Rolle.

Mangelhaftes Krisenmanagement

Unternehmen müssen für ihre IT, insbesondere wenn es sich um kritische Unternehmenzprozesse handelt, ein entsprechendes Krisenmanagement betreiben und ihre IT-Resistenz entscheidend erhöhen. Obwohl 90 Prozent der in der Kyndryl-Studie „IT Readiness Report 2024" befragten deutschen Führungskräfte ihre IT-Infrastruktur für erstklassig halten, ist nur ein Drittel der Meinung, dass ihre IT-Infrastruktur für zukünftige Risiken und Störfaktoren gewappnet ist. Diese Diskrepanz sollten Unternehmen auflösen, um ihre Geschäftsfähigkeit auch in Krisenzeiten sicherzustellen.

Ein dezidiertes, konsequentes und präzises IT-Sicherheitsmanagement, wie es von allen relevanten, internationalen Sicherheitsstandards (zum Beispiel ISO/IEC 27001 / 27005, NIST SP 800x) gefordert wird, ist für ein effektives Krisenmanagement unerlässlich. Dabei hat beispielsweise das Büro für Technikfolgenabschätzung des Deutschen Bundestages (TAB) die Auswirkungen von Stromausfällen auf andere Sektoren und die Zivilgesellschaft untersucht. Besonders Unternehmen im Bereich der kritischen Infrastruktur, wie Energieversorger und Telekommunikation aber auch Finanzdienstleister, Regierung, Gesundheit sind immer häufiger potenzielle Angriffsziele.

Parallele Schadensereignisse zu bewältigen fällt in den Aufgabenbereich des Krisenmanagements. Eine Umfrage des ASW-Bundesverbandes zeigt jedoch, dass nur 32 Prozent der befragten Unternehmen Werkzeuge für das Lage- und Führungsmanagement einsetzen, während 56 Prozent keine spezifischen Verfahren dafür haben.

Schutz vor hybriden Angriffen

IT-Unternehmen können nur dann ein effektives Krisenmanagement betreiben, wenn auch ihre Cybersicherheit lückenlos funktioniert. Dies ist heute jedoch nicht mehr so einfach, da Hacker mit Hilfe von KI-gestützten Bots sehr schnell große Mengen an Systemdaten auf Schwachstellen untersuchen. Zudem können sie mit generativen KIs sehr einfach und nahezu ohne Programmierkenntnisse Codebausteine generieren. Mit sogenannten Prompt Injections können Angreifer das System, das normalerweise bösartige Eingabeaufforderungen blockiert, schnell überlisten.

Daher ist der Einsatz von KI für ein effektives Krisenmanagement und bei der Verteidigung gegen KI-gestützte Angriffe zwingend notwendig.

Einige Beispiele, die verdeutlichen, warum der Einsatz von KI in der Verteidigung unverzichtbar ist, sind etwa:

➜ **Automatisierte Schwachstellenanalyse:** Angreifer nutzen KI für sekundenschnelle System-Scans. Als Gegenmaßnahme überwachen KI-gestützte

Vulnerability Management Systeme die IT-Umgebung kontinuierlich und priorisieren Schwachstellen nach Risiko.

➜ **Anomalie-Erkennung in Echtzeit:** Gegen KI-gesteuerte Phishing-Angriffe helfen intelligente Überwachungssysteme. Sie erkennen verdächtiges Benutzerverhalten in Echtzeit und können automatisch Gegenmaßnahmen einleiten.

➜ **Bedrohungsanalyse:** Angreifer nutzen KI-Tools, um Zero-Day-Schwachstellen zu identifizieren. Defensive KI-Systeme könne dafür genutzt werden, kontinuierlich das Netzwerk zu analysieren und automatisch Schutzmaßnahmen wie Patching oder Isolierung durchführen.

➜ **KI gesteuerte Malware-Erkennung:** Gegen polymorphe Malware, die sich ständig verändert, können Unternehmen auf KI-basierte Endpoint-Security mit Verhaltensanalyse statt klassischer Signaturen setzen.

➜ **Automatische Reaktion und Isolation:** Angreifer automatisieren die Verbreitung von Ransomware in Unternehmensnetzwerken mit Hilfe von KI. KI-Systeme erkennen dann diese verdächtige Verschlüsselungsaktivitäten und können betroffene Systeme automatisch isolieren, bevor sich die Schadsoftware ausbreitet.

Diese Beispiele sind nur eine Auswahl, die belegen, dass KI-unterstützte Gegenmaßnahmen entscheidend sind, um mit der Geschwindigkeit und Komplexität KI-basierter Angriffe Schritt zu halten. Nicht nur können Angriffe mit ihr erkannt und abgewehrt, sondern auch die IT-Umgebung proaktiv abgesichert werden. Der Schlüssel liegt in der Kombination aus Automatisierung, kontinuierlicher Überwachung und adaptiven Modellen, die Angriffe frühzeitig erkennen und abwehren können.

IT-UNTERNEHMEN KÖNNEN NUR DANN EIN EFFEKTIVES KRISENMANAGEMENT BETREIBEN, WENN AUCH IHRE CYBERSICHERHEIT LÜCKENLOS FUNKTIONIERT.

Robert Christian, CTO – Security and Resiliency, Kyndryl Consult, Kyndryl Deutschland GmbH, www.kyndryl.com/de/de

Eine erweiterte Resilienzstrategie als Pflicht

Doch eine effektive Cybersicherheit ist noch lange nicht das Ende der Fahnenstange, damit Unternehmen krisenfest werden. Um sich auf mögliche Krisen vorzubereiten, sollten sie eine umfassende Resilienzstrategie entwickeln. Diese sollte zahlreiche Aspekte umfassen: Für das Krisenmanagement sind technische Lösungen wie Apps, mobile Leitstände und GPS-gestützte Tools unerlässlich. Dezentrale Strukturen, alternative Rechenzentrumsstandorte und eine gesicherte Notstromversorgung sind zudem für die eigenen Standorte entscheidend. Außerdem profitieren Kommunikation und Netzwerke von Redundanz durch Satellitennetze, Richtfunk und automatisierte Failover-Systeme.

In der IT-Infrastruktur sind Geo-Redundanz, Ersatzteillagerung und Geräteportabilität von zentraler Bedeutung, während Unternehmen bei ihren Anwendungen und Diensten auf Automatisierung und regionale Reservekapazitäten setzen sollten. Darüber hinaus sollten sie ihr Schlüsselpersonal identifizieren und auf Weiterbildung und Fernübungen setzen. Schließlich verbessern integrierte Prozesse und Tools die Effizienz und Sicherheit durch Standardisierung, Echtzeit-Asset-Management und einheitliches Patch-Management.

Ganzheitliche Strategien

Der Einsatz von KI kann dabei helfen, Bedrohungen schneller zu erkennen und Sicherheitsprozesse effizienter zu gestalten.

Gleichzeitig ist eine erweiterte Resilienzstrategie nötig, die Aspekte wie dezentrale IT-Infrastruktur, redundante Kommunikationsnetze, Notstromversorgung und gut ausgebildetes Schlüsselpersonal umfasst. Nur eine Kombination aus technischer Innovation, organisatorischer Vorbereitung und strategischer Planung kann IT-Unternehmen krisenfest machen. Plattformen wie Kyndryl Bridge unterstützen Unternehmen dabei, indem sie durch Nutzung faktischer, betrieblicher und eingebetteter Daten KI-Transparenz über die gesamte IT-Landschaft eines Unternehmens schaffen. So liefert sie einen Status dieser IT-Landschaft über die Bereiche Best Practice, Reaktions- und Wettbewerbsfähigkeit. Unternehmen verfügen so über ein solides Werkzeug für das Krisenmanagement und die Implementierung ihrer Resilienzstrategie.

Fazit

Nur durch die Kombination aus technischer Innovation, organisatorischer Vorbereitung und strategischer Planung können Unternehmen die Herausforderungen der heutigen geopolitischen Lage meistern und langfristig krisenresistent bleiben.

Robert Christian

Privileged Access Management

PAM IST DAS NEUE IAM UND PIM

Fast so alt wie die IT sind auch die Diskussionen über das Zugangs-, Berechtigungs- oder Zugriffsmanagement. Ursprünglich zum einfachen Schutz von Daten vor unbefugtem Zugriff konzipiert, ist das Zugriffs- und Identitätsmanagement heute ein unverzichtbarer Bestandteil der IT-Sicherheit. In einer hochgradig vernetzten Welt, in der Daten zu den wertvollsten Gütern von Unternehmen gehören, ist das Privileged Access Management (PAM) eines der wichtigsten Instrumente für den Schutz sensibler Informationen und die Gewährleistung der Privatsphäre.

Der lange Weg zur modernen Kontrolle

Ein kurzer historischer Abriss zeigt, dass schon immer die Notwendigkeit bestand, den Zugang zu IT-Systemen und deren Daten zu begrenzen.

Die ersten Systeme, die ein Zugriffsmanagement implementierten, tauchten in den 1960er Jahren auf, als die Computertechnik in wenigen Unternehmen und Universitäten Einzug hielt. Das damalige Zugriffsmanagement war eine einfache Identifikation der Benutzer über ein Passwort. Mit der Zunahme der Nutzung von Computern in verschiedenen Bereichen wuchs die Notwendigkeit einer besseren Organisation und Kontrolle des Zugriffs. Access-Control-Listen (ACLs) ermöglichten es, Rechte für einzelne Benutzer oder Benutzergruppen festzulegen, was ein erster Schritt in Richtung differenziertes Zugriffsmanagement war.

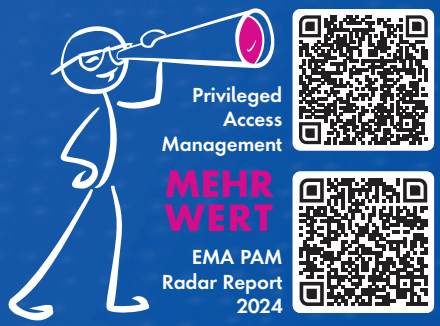
In den 1980er Jahren nahm der Einsatz von Mehrbenutzerbetriebssystemen wie UNIX - später Microsoft Windows - an Bedeutung zu. Insbesondere UNIX führte komplexere Mechanismen zur Authentifizierung und Rechtevergabe ein, darunter die Möglichkeit, verschiedene Benutzergruppen zu erstellen und ihnen unterschiedliche Berechtigungen zuzuweisen. Spätere, zentralisierte Authentifizierungssysteme markierten einen bedeutenden Schritt in Richtung einer sicheren Zugriffsverwaltung in verteilten Systemen.

PAM STELLT SICHER, DASS AUTORISIERTE BENUTZER MIT ZUGRIFF AUF DIE WICHTIGSTEN UND SENSIBLEN INFORMATIONEN GENAU ÜBERWACHT WERDEN.

Darren Guccione, CEO und Mitbegründer, Keeper Security, www.keepersecurity.com

Ab den 1990er Jahren stand die IT-Industrie vor einer neuen Herausforderung: dem Internet. Unternehmen mussten ihre IT-Infrastruktur so gestalten, dass sie nicht nur lokalen, sondern auch entfernten Benutzern sicheren Zugriff auf Daten und Anwendungen ermöglichen konnten. In dieser Zeit rückten Konzepte wie beispielsweise das Single Sign-On (SSO) oder das Lightweight Directory Access Protocol (LDAP) in den Fokus.

Der Paukenschlag, der bis heute nachhallt, war die Entwicklung eines umfassenden Zugriffsmanagements in den 2000er Jahren. Identity and Access Management (IAM) wurde zum wichtigen Bestandteil von IT-Sicherheitsstrategien. IAM-Systeme ermöglichten eine zentrale Verwaltung von Identitäten, Authentifizierung, Autorisierung und Audit-Protokollen. Sie bildeten die Grundlage für eine systematische Kontrolle darüber, wer auf welche Ressourcen wann zugreifen durfte – allerdings nicht ohne erheblichen Aufwand bei der Implementierung und im Betrieb.



Die heutige Rolle des IAM

Ein modernes IAM-System ist heute mehr als das Zugriffsmanagement der 2000er Jahre. Es ist ein Sicherheitswerkzeug und ein Mittel zur Effizienzsteigerung, Risikominimierung und zur Einhaltung gesetzlicher Vorgaben. Und es bildet den Rahmen für viele weitere Sicherheitssysteme, darunter Privileged Identity Management (PIM) und PAM. IAM ermöglicht es Organisationen, Identitäten sicher zu verwalten, Zugriff auf Ressourcen zu steuern und Compliance-Anforderungen zu erfüllen. Es zeichnet sich durch folgende Komponenten aus:

➤ **Identitätsmanagement (Identity Management):**

- Verwaltung von Identitätsdaten (Benutzerprofile, Rollen, Berechtigungen).
- Zentralisierte Benutzerverzeichnisse (zum Beispiel Active Directory, LDAP).

➤ **Authentifizierung (Authentification):**

- Sicherstellung, dass der Benutzer derjenige ist, der er vorgibt zu sein.
- Methoden: Single Sign-On (SSO), Passwortlose Authentifizierung, Biometrie, MFA.

➤ **Autorisierung (Authorization):**

- Regelbasierte Entscheidung, welche Ressourcen ein Benutzer nutzen darf.
- Implementierung von Rollenbasierter Zugriffskontrolle (Role-Based Access Control, RBAC) oder Attributbasierter Zugriffskontrolle (Attribute-Based Access Control, ABAC).

➤ **Zugriffsverwaltung (Access Management):**

- Durchsetzung von Zugriffskontrollrichtlinien in Echtzeit.
- Adaptive Zugriffskontrollen basierend auf Kontextfaktoren wie Standort, Gerät oder Verhalten.

➤ **Self-Service-Portal:**

- Ermöglicht Benutzern, ihre Profile zu aktualisieren, Anfragen zu stellen oder Zugriffe zu verwalten.
- Reduziert den Verwaltungsaufwand für IT-Teams.

➤ **Provisionierung und Deprovisionierung:**

- Automatisierung der Benutzerzugriffsbereitstellung bei Neueinstellungen und deren Entzug bei Austritt.
- Integration mit HR-Systemen zur Synchronisierung von Lebenszyklusereignissen.

➤ **Überwachung und Reporting:**

- Überwachung von Benutzeraktivitäten und Sicherheitsvorfällen.
- Bereitstellung von Berichten für Audits und Compliance.

➤ **Privileged Identity Management (PIM):**
- Verwaltung und Sicherung von privilegierten Identitäten und Zugriffen

➤ **Privileged Access Management (PAM):**
- Verwaltung und Schutz privilegierter Benutzerkonten (Admins, Superuser).
- Reduziert das Risiko durch Missbrauch hochsensibler Zugriffe.

IAM-Systeme stellen Unternehmen aufgrund ihrer Vielfalt und Komplexität vor große Herausforderungen bei der Implementierung und der fortlaufenden Verwaltung. Für IAM in seiner gesamten Bandbreite sind meist hohe Budgets und personelle Ressource nötig, so dass IAM eher großen Konzernen vorbehalten ist.

Glücklicherweise haben sich einzelne Elemente des IAM stark weiterentwickelt und avancieren für alle Unternehmensgrößen, von großen Konzernen über den Mittelstand bis hin zu kleineren Unternehmen, zu effizienten Alternativen. Zu diesen Security-Lösungen gehören beispielsweise Privileged Identity Management und allen voran das Privileged Access Management.

Ein Buchstabe macht den großen Unterschied

Beleuchtet man PIM und PAM wird schnell klar, welche Rolle sie in der Security spielen und wie unterschiedlich die beiden Konzepte sind. Beim Privileged Identity Management geht es um die Identitäten in einem Unternehmen und um die Verwaltung der Personen, die auf die Daten oder das Netzwerk eines Unternehmens zuzugreifen. Im Gegensatz dazu konzentriert sich Privileged Access Management auf die Überwachung des Zugriffs auf sensible Informationen und Daten eines Unternehmens. Konten, die regelmäßig auf sensible Systeme zugreifen, wie die IT-Abteilung oder die Personalabteilung, müssen vor unbefugten Benutzern geschützt werden. Ist diese Kontrolle lückenhaft, entstehen Sicherheitslücken, die zu einer Datenschutzverletzung führen können. Mit PAM behält ein Unternehmen die Kontrolle über Konten und den Zugriff auf die wichtigsten Unternehmensdaten und es stellt sicher, dass die Aktivitäten der privilegierten Benutzer granular überwacht werden.

PAM wird erwachsen

Den großen Unterschied zwischen PIM und PAM sehen nicht nur Hersteller von Lösungen, sondern auch diejenigen, die die Märkte und die Entwicklungen dieser zunehmend wichtigen Technologie für die Cybersicherheit regelmäßig beleuchten. Trend- und Marktforscher beschäftigen sich seit einigen Jahren mit PAM – mutmaßlich, weil sie darin großes Marktpotenzial sehen.

In der Betrachtung von EMA Radar werden die Hauptakteure am Markt nach Stärke der Lösung im Verhältnis zur Kosteneffizient eingestuft. Keeper Security ist eines der Unternehmen, das mit wenigen anderen an der Spitze dieser Bewertung stehen. Neben der Kosteneffizienz unterstreicht der 2024 EMA PAM Radar Report Stärken in mehreren Schlüsselbereichen. Dazu gehört, dass eine Installation schnell und mit minimalen Unterbrechungen durchgeführt werden kann sowie die Anpassungsfähigkeit über unterschiedliche Geräte und Betriebssysteme hinweg. Zudem baut das Sicherheits-Framework auf den Prinzipien von Zero-Trust und Zero-Knowledge auf und bietet umfassenden Schutz für alle Benutzerkonten und sensiblen Daten.

Eine weitere Einschätzung des Marktes für Identitätsschutz bietet GigaOm mit seinem GigaOm Radar Report for Enterprise Password Management. Der Bericht bewertet dreizehn Passwortverwaltungslösungen und konzentriert sich auf Schlüsselmerkmale, Geschäftskriterien und neue Technologien. Auch bei dieser Einschätzung erzielt Keeper hohe Bewertungen und zeichnet sich durch Innovation sowie seine Zero-Trust-Lösung für privilegiertes Zugriffsmanagement (PAM), KeeperPAM, aus.

Die Qual der Wahl

IAM, PIM, PAM: Was sollten Unternehmen in Betracht ziehen und für welchen Zweck? Jedes Unternehmen weiß, dass es den bestmöglichen Schutz seiner digitalen Assets gewährleisten sollte und dass die Resilienz der Sicherheit ein wichtiges Kriterium bezüglich der sicherheitstechnischen Zukunftsfähigkeit ist.

Um die Szenerie von PIM, PAM und IAM zu verdeutlichen, eignet sich eine einfache Analogie: Das IAM kann man sich als Sicherheitspersonal bei einem Konzert vorstellen. IAM stellt sicher, dass nur Personen mit einem gültigen Ausweis und einer gültigen Eintrittskarte Zutritt haben. PIM hingegen funktioniert wie das System, das die Konzertkarten erstellt, verwaltet und festlegt, wer näher an der Bühne sitzen darf. PAM ist in diesem Zusammenspiel die VIP-Konzertkarte, die es nur besonderen Zuschauern erlaubt, bestimmte, sensible Bereich zu betreten – beispielsweise hinter die Bühne zu gehen und die Künstler zu treffen.

PAM stellt sicher, dass autorisierte Benutzer mit Zugriff auf die wichtigsten und sensiblen Informationen genau überwacht werden. Zudem enthalten moderne PAM-Lösungen viele PIM-Funktionen, um die Gesamtsicherheit eines Unternehmens zu verbessern.

Fortschrittliche Lösungen wie KeeperPAM konsolidieren wichtige PAM-Funktionen in einem Cloud-Tresor, der den sicheren Zugriff auf jede geschützte Ressource wie Datenbanken, Webanwendungen, Server und Workloads ermöglicht. Innerhalb eines einheitlichen Interface bietet die Cloud-native Plattform die Verwaltung von Geheimnissen, Verbindungsmanagement, Zero-Trust-Zugriff und Remote-Browser-Isolation.

Sicherheits-, Compliance- und Technik-Teams können KeeperPAM für ihre spezifischen Anwendungsfälle nutzen. Sicherheitsteams können den Zugriff auf Systeme und Daten zentralisieren, MFA für alle Ressourcen durchsetzen und jeden Benutzer im Unternehmen durch automatische SCIM-Bereitstellung schützen. Audits werden für Compliance-Teams durch detaillierte Protokolle, Sitzungsaufzeichnungen und automatisierte Berichte mühelos möglich. Engineering-Teams können moderne Tools für den Zugriff auf Infrastruktur und Workloads verwenden, zum Beispiel ihr bevorzugtes Datenbankverbindungstool oder die Integration mit Terraform, um die Ausbreitung von Geheimnissen zu verhindern.

Letztendlich kann KeeperPAM jeden Benutzer im Unternehmen schützen und unbefugten Zugriff und Sicherheitsverstöße verhindern.

Darren Guccione

Wallet-basierte Identitäten

ZUM ENTWICKLUNGSSTAND VERIFIZIERBARER DIGITALER IDENTITÄTSAUSWEISE

Seit mehreren Jahren schon arbeiten Staaten weltweit an der Möglichkeit, die physischen Identitätsausweise ihrer Bürger zu digitalisieren und mit ihren digitalen Verwaltungsangeboten zu verknüpfen. Ihr Ziel: eine effektivere und effizientere Verwaltung – sowie zufriedenere Bürger. In Europa wurde in diesem Zusammenhang zu Beginn des Jahres 2024 die Regulierung eIDAS 2.0 verabschiedet. Sie sieht vor, dass alle europäischen Staaten bis 2026 ihren Bürgern ein europaweit gültiges Wallet-basiertes System zur Identifizierung und Authentifizierung ihrer digitalen Identitäten zur Verfügung stellen. In Deutschland hinkt man diesem Ziel – zumindest derzeit – noch weit hinterher. In anderen Staaten ist man schon wesentlich weiter – mancherorts nicht zuletzt, da man dort die Hilfe erfahrener externer Anbieter in Anspruch genommen hat.

Staatliche Verwaltungsprozesse können unter Zuhilfenahme Wallet-basierter Identitätsausweise deutlich effektiver und effizienter als unter Zuhilfenahme eines physischen Identitätsausweises gestaltet werden. Im Frühjahr 2024 hat das Europäische Parlament die Regulierung Electronic Identification, Authentication and Trust 2.0 (eIDAS 2.0) verabschiedet. Sie gibt den EU-Mitgliedsstaaten bis 2026 Zeit, ihren Bürgern ein Wallet-basiertes System zur Identifizierung und Authentifizierung ihrer digitalen Identitäten als EU-Bürger bereit zu stellen.

Eine zentrale Forderung: die jeweiligen nationalen Lösungen sollen mit einer noch zu schaffenden europäischen digitalen Identitäts-Wallet (EUDIW) kompatibel sein. Identitäts- und Authentifizierungsdokumente sollen auf ihr sicher gespeichert und verwaltet und dann in allen europäischen Mitgliedsstaaten bequem und nahtlos genutzt werden können. Auch Deutschland unterstützt diese Bemühungen, ist in mehrere Pilotprojekte der Wallet-Initiative stark eingebunden. Allerdings: viele EU-Mitgliedsstaaten sind mittlerweile schon einen Schritt weiter als Deutschland. Bereits heute bieten sie ihren Bürgern EUDIW-kompatible Wallets an und demonstrieren, welches Anwendungspotential in verifizierbaren digitalen Identitätsausweisen steckt.

BEI EINER UMFASSENDEN IDENTITY WALLET-NUTZUNG DER BEVÖLKERUNG IST EIN WIRTSCHAFTLICHER MEHRWERT VON RUND 3 PROZENT DES BIP ZU ERWARTEN.

Detlev Riecke, RVP DACH, Ping Identity, www.pingidentity.com

EU-Staaten zeigen, wie es geht

Viele europäische Staaten haben schon vor geraumer Zeit mit der Entwicklung nationaler EUDIW-kompatibler Apps begonnen. In Frankreich beispielsweise, ließ die französische Regierung über das Programm France Identité Numérique (FIN) die France Identité App erstellen. Bei Google Play verzeichnet sie bereits über eine Milli-

on Downloads. Über 1.400 Online-Dienste der französischen Verwaltung können ihre Nutzer, dank Wallet-basiertem Identitätsausweis, digital in Anspruch nehmen. Bürger Griechenlands können seit Juli 2022 auf die Gov.gr Wallet zugreifen. Auch hier sind bereits über eine Million Downloads zu verzeichnen. Mehr als 1.765 Online-Dienstleistungen der öffentlichen Verwaltung stehen ihren Anwendern zur Verfügung. In Belgien wurde vor Kurzem die App mygov.be freigegeben. Bereits nach einem Monat war sie mehrere 10.000 mal gedownloadet worden. Auf den ersten Blick werden die Apps also gut frequentiert. Doch haben viele – wenn nicht die meisten von ihnen – ein großes Manko: ihre Bewertungen im Netz fallen – zumindest bislang – eher dürftig aus. So kommt die France Identité App im Apple App Store zwar auf 4,0 von 5 Sternen, bei Google Play aber nur auf 2,2 von 5 Sternen. Die Gov.gr-Wallet schaffte im Apple App Store sogar nur 2,6 von 5 Sternen und bei Google Play lediglich 3 von 5 Sternen. Wie das Urteil über die noch junge belgische Wallet-App ausfallen wird, bleibt abzuwarten.

Deutschlands Behörden hinken hinterher

Es ist zu hoffen, dass sich die deutschen App-Entwickler die Erfahrungen ihrer europäischen Kollegen – und diese Kritik ihrer Nutzer – zu Herzen nehmen werden. Zeit genug sollten sie eigentlich haben. Denn in Deutschland hat die Entwicklung des Wallet-basierten Identitätsausweises eben erst begonnen. Vor wenigen Monaten hat das BMI die Bundesagentur für Sprunginnovationen (SPRIND) einen Innovationswettbewerb zur Entwicklung deutscher EUDIW-kompatibler App-Prototypen eröffnen lassen. Zwei Jahre verbleiben der Bundesrepublik nun noch, eine sichere und nutzerfreundliche deutsche App-Variante zu entwickeln und öffentlich zugänglich zu machen.

Expertise steigert den Erfolg

Dass man bei der App-Entwicklung größere Erfolge einfahren kann, wenn man bereit ist, Expertise und Erfahrungen von außen mit einzubeziehen, dass man dabei auch nicht auf Open Source verzichten muss, das haben der US-Bundesstaat Colorado und das DMV des Bundesstaats Kalifornien in den vergangenen Jahren anschaulich demonstriert. Beide haben – um ihr Sicherheitsbedürfnis und die Anforderungen ihrer Anwender an die Nutzerfreundlichkeit ihrer Wallet-basierten Identitätsnachweise in Einklang zu bringen – auf externe Anbieter gesetzt; mit Erfolg.

Die myColorado-App hatte 2023 1,15 Millionen registrierte Nutzer – bei 5,88 Millionen Einwohnern. Knapp jeder fünfte Einwohner Colorados besitzt die App also bereits – bei einem jährlichen Nutzeranstieg von 25 Prozent. Mit der App lassen sich zahlreiche staatliche Verwaltungsleistungen – auch Sozialleistungen – in Anspruch nehmen. Außerdem kann sie genutzt werden, um Identität, Alter und Wohnsitz zu bestätigen.

Die California DMV Wallet steckt zwar schon seit geraumer Zeit in der Pilot-Phase fest, doch auch ihr Ergebnis kann sich sehen lassen: über eine Million hochzufriedene Pilotphasen-Nutzer. Die Wallet lässt sich als mobiler Führerschein einsetzen.

In Punkto Kundenzufriedenheit können diese Wallets – nicht zuletzt da hier die Expertise externer Anbieter mit eingeflossen ist – mehr überzeugen als ihre europäischen Pendants. In Apples App Store erreicht die MyColorado-App 4,8 von 5 Sternen, bei Google Play 4 von 5 Sternen. Die DMV-Wallet kommt

in Apples App Store sogar auf 4,6 von 5 Sternen und bei Google Play auf 4,8 von 5 Sternen.

Fazit

Auf den zweiten Blick ist es vielleicht gar nicht so schlecht, dass sich die Bundesrepublik mit der Entwicklung ihrer Identity Wallet-App Zeit gelassen hat. So haben ihre Entwickler nun zahlreiche Vorlagen, können analysieren, was bei ihren europäischen (und außereuropäischen) Kollegen funktioniert hat – und was nicht. Ein Blick über den deutschen Tellerrand hinaus zeigt: eine Identity Wallet-App ‚from the scratch' zu entwickeln ist kein leichtes Unterfangen. Wie überall im Bereich der App-Entwicklung geht es auch hier darum, Sicherheit und Nutzerfreundlichkeit in Einklang zu bringen. Doch der Einsatz lohnt sich. Bereits 2019 hielt eine Studie des McKinsey Global Institute fest, dass selbst für eine gut entwickelte Volkswirtschaft – bei einer umfassenden Identity Wallet-Nutzung der Bevölkerung – ein wirtschaftlicher Mehrwert von rund 3 Prozent des BIP zu erwarten ist.

Detlev Riecke

MEHR WERT
EUDIW

Cybersicherheit in Bereitschaft

EIN LEITFADEN ZUR INCIDENT RESPONSE

Ransomware und Malware sind seit Jahren für massive Schäden und Sabotage-Akte in Unternehmen verantwortlich: Verschlüsselung von Daten, Erpressung, Lösegeldforderungen, Hochstapelei, Betrug, Server-Ausfälle, Maschinenstopps, Zerstörung von Datensätzen – all das gehört dazu. Der finanzielle Schaden geht oft in die Millionen: Für das Jahr 2024 werden durchschnittlich weltweit Kosten für ausgenutzte Schwachstellen von 4,5 Millionen Euro geschätzt, eine Zunahme von 10 Prozent gegen 2023.

Viele dieser Angriffe können jedoch mit einem Konzept der Incident Response (IR) als umgehende Antwort auf Zwischenfälle abgewehrt werden.

Die sogenannte IR-Bereitschaft ist eine Reihe regelmäßiger Prozesse, Verfahren und Technologien, die Sicherheitsvorfälle bereits im Anfangsstadium erkennen und auf diese reagieren, um eventuelle Schäden und Kosten zu minimieren. Die folgenden Schritte sind notwendig, um IR-Bereitschaft zu erreichen und das Unternehmen auf alle Arten von Cyber-Attacken vorzubereiten.

JEDES SYSTEM UND JEDE SCHUTZMASSNAHME, DIE NICHT REGELMÄSSIG AKTUALISIERT UND AUFGERÜSTET WIRD, WEIST IRGENDWANN SCHWACHSTELLEN AUF, DIE VON HACKERN AUSGENUTZT WERDEN KÖNNEN.

Marco Eggerling, Global CISO, Check Point Software Technologies, www.checkpoint.com

Asset Tracking und Asset Management

Man kann nicht schützen, was man nicht sieht. Dennoch sind sich viele Unternehmen immer noch nicht ihrer kritischen Assets bewusst, unterhalten vermeintlich inaktive, die noch Zugriff auf ihre Netzwerke haben, und setzen interne Ressourcen mangelhaft geschützt dem öffentlichen Zugriff aus. Erschwert wird dies durch schlechte Unternehmensrichtlinien, wie ungenügende Regeln zum Konzept des Bring Your Own Device (BYOD), die externen Assets Zugriff auf Unternehmensdateien gewähren, ohne die Geräte voll zu erfassen. Nur aber durch die Investments in die Erkennung, Identifizierung und Klassifizierung der Geräte lässt sich ein Asset Management aufsetzen, dass im Notfall für Klarheit sorgt. Im Falle einer Kompromittierung muss das Gerät oder der Account schnell und umfassend untersucht und gesperrt werden können. Shadow IT und neuerdings auch Shadow AI ist eines der größten Hindernisse bei der Absicherung der Angriffsfläche.

Einführung eines Frameworks

Sobald ein Unternehmen ein besseres Verständnis seiner Assets erhalten hat, lohnt es sich, ein einheitliches Framework für Cyber-Sicherheit zu diskutieren und einzuführen. Das NIST Cyber Security Framework aus den USA, allgemein als CSF bezeichnet, ist ein guter Ausgangspunkt für jedes Unternehmen, das seine Sicherheitsrichtlinien, -prozesse und -verfahren standardisieren möchte.

Schutz der Assets

Nach der Einführung eines einheitlichen Rahmenwerkes besteht der nächste wichtige Schritt darin, Prozesse, Verfahren und Technologien einzuführen, die bei der Überwachung und Erkennung von bekannten Bedrohungen helfen. Unternehmen sollten zumindest Endpoint Detection and Response (EDR) für alle kritischen Anlagen einsetzen, mit dem Ziel, die Abdeckung auf alle Geräte und Netzwerkausgangsknoten auszuweiten. Sobald alle Anlagen abgedeckt sind, muss sichergestellt werden, dass sie ordnungsgemäß konfiguriert und kontinuierlich von einem geschulten Team überwacht werden, das auf die ersten Anzeichen eines Angriffs reagieren kann. Dies kann durch interne Teams oder durch spezielle externe Managed Detection and Response (MDR) Services erfolgen.

MEHR WERT
IR-Bereitschaft

MEHR WERT
NIST Cyber Security Framework

Patch- und Schwachstellen-Management

Jedes System und jede Schutzmaßnahme, die nicht regelmäßig aktualisiert und aufgerüstet wird, weist irgendwann Schwachstellen auf, die von Hackern ausgenutzt werden können, um sich Zugang zu den Ressourcen des Unternehmens zu verschaffen. Jedes Unternehmen sollte ein Patching-System einführen, das Schwachstellen aufspürt und sie so schnell wie möglich behebt. Das Patching-System sollte ebenso den Schweregrad bekannter Schwachstellen und ihre Auswirkungen auf das Unternehmen berücksichtigen.

Planung der Reaktion auf Zwischenfälle

Die IR-Reaktion der Organisation sollte in einem dokumentierten und dynamischen Incident Response Plan (IRP) festgehalten werden. Der IRP sollte dokumentiert und von der höchsten Ebene der Organisation genehmigt werden. Im Rahmen der Erstellung und Dokumentation des IRP sollte die Organisation zudem Reaktionsgruppen einführen und die wichtigsten Interessenten ermitteln, Kontakte zu Drittanbietern und Vereinbarungen für externe IR-Unterstützung herstellen, sowie Reaktions-Toolkits und -vorlagen, Cyber-Versicherungen und andere Maßnahmen zur Risikominderung zusammenstellen. Ein gut ausgearbeiteter IRP sollte einfach und effizient sein, um nicht nur das Umfeld und die Bedürfnisse der Organisation widerzuspiegeln, sondern auch die wichtigste Richtschnur für die Reaktion auf Vorfälle zu sein.

Ausbildung

Das beste Kapital einer Organisation sind die Angestellten. Menschen, die geschult mit digitalen Technologien, Prozessen und Verfahren arbeiten, sind der Schlüssel dazu, ob ein Vorfall ein kleines Ereignis bleibt oder eine ausgewachsene Katastrophe wird. Daher müssen alle Mitarbeiter als Aktivposten der IT-Sicherheit betrachtet werden. Alle Schulungen sollten auf die Rollen und Verantwortlichkeiten der Mitarbeiter zugeschnitten werden, regelmäßig stattfinden und realistisch sein. Die Schulungen können Cyber-Awareness-Schulungen, Phishing-Schulungen und Schulungen zu anderen gängigen Bedrohungen sowie komplexen Unterricht, wie IR-Reaktionstrainings im Stile von Tabletop-Übungen, umfassen – bis hinauf zur Führungsebene.

Prüfung der Sicherheitsmaßnahmen

Sobald die genannten Maßnahmen umgesetzt wurden, ist es wichtig, dass alle Anlagen regelmäßig geprüft werden, die Schutzmaßnahmen von internen Teams bewertet, von externen Teams getestet und der Plan für die Reaktion auf Zwischenfälle steht. Außerdem muss das Playbook in simulierten Zwischenfällen innerhalb von Tabletop-Übungen trainiert worden sein. Alle daraus gezogenen Lehren und alle entdeckten Lücken sollten dann bedacht und geschlossen werden, um die Sicherheitsmaßnahmen zu verbessern.

Schlußfolgerung

Der Aufbau eines Incident Response Teams kann eine Herausforderung darstellen und kostspielig sein, vor allem für bereits überlastete IT-Sicherheitsleute. Im Vergleich zu den möglichen finanziellen Verlusten des Unternehmens, der Rufschädigung und den Kosten für die Wiederherstellung der Sicherheit bietet die Bereitschaft zur Reaktion auf Vorfälle jedoch eine gute Rendite und ist im Vergleich zu den Kosten für eine verspätete Reaktion auf tatsächliche Vorfälle ein Schnäppchen.

Für Unternehmen, die einen präventiven Ansatz für ihre Incident Response Readiness verfolgen möchten, stehen unabhängig von ihrer Größe verschiedene Ressourcen zur Verfügung. Dazu gehören lokale und staatliche Unterstützung, die sowohl technische als auch finanzielle Hilfe bietet. Desweiteren sollten Unternehmen aber auch auf Sicherheitsanbieter setzen, die über eigene IR-Teams verfügen und den Aufbau unterstützen können. Sie können wie Detektive agieren und ermöglichen nicht nur die Aufklärung, sondern auch Verhinderung weiterer Cyber-Attacken. Schaden wird abgewendet und Unternehmen erhalten die benötigte Ruhe zur Konzentration auf die Kerntätigkeiten.

Marco Eggerling

Cybersicherheit im Finanzsektor

VORBEREITUNG AUF DIE BEDROHUNGEN VON MORGEN

Der Finanzsektor steht vor beispiellosen Cybersicherheitsherausforderungen im Vorfeld des Jahres 2025. Mit 93,2 Prozent der Finanzorganisationen, die 2023 erfolgreiche Cyberangriffe bestätigten, befindet sich die Branche an einem kritischen Wendepunkt. Besonders besorgniserregend ist dabei, dass 83 Prozent der kleinen und mittleren Unternehmen finanziell nicht auf die Bewältigung eines Cyberangriffs vorbereitet sind. Die Einführung des Digital Operational Resilience Act (DORA) im Januar 2025 erhöht den regulatorischen Druck und macht es für Organisationen unerlässlich, ihre Sicherheitsposition auf mehreren Ebenen zu stärken. Die durchschnittlichen Kosten einer schwerwiegenden Datenpanne belaufen sich mittlerweile auf 4,9 Millionen Euro, was die finanzielle Dimension der Bedrohung verdeutlicht.

Aufbau einer sicherheitsbewussten Kultur

Phishing bleibt eine der hartnäckigsten Bedrohungen, der 94 Prozent der Organisationen zum Opfer fallen. Die erste Verteidigungslinie liegt im Aufbau einer sicherheitsbewussten Organisationskultur. Regelmäßige Mitarbeiterschulungen sind unverzichtbar geworden, da menschliches Versagen weiterhin eine bedeutende Schwachstelle in Sicherheitssystemen darstellt.

Ein effektives Schulungsprogramm muss dabei weit über das traditionelle Format jährlicher Compliance-Schulungen hinausgehen. Moderne Ansätze setzen auf kontinuierliches, praxisnahes Lernen

durch simulierte Phishing-Kampagnen, interaktive Workshops und regelmäßige Kurzschulungen. Mitarbeiter lernen dabei nicht nur die Erkennung ausgefeilter Phishing-Versuche, sondern entwickeln auch ein tieferes Verständnis für Social-Engineering-Taktiken und sichere Kommunikationspraktiken. Besonders wichtig ist die Etablierung einer Fehlerkultur, in der Mitarbeiter keine Scheu haben, Sicherheitsvorfälle zu melden.

Die Schulungsinhalte müssen dabei kontinuierlich an neue Bedrohungsszenarien angepasst werden. Besonders relevant sind derzeit Schulungen zur Erkennung von KI-generierten Phishing-Mails und Deep-Fake-Attacken in Videokonferenzen. Auch der sichere Umgang mit mobilen Geräten und Home-Office-Szenarien gewinnt zunehmend an Bedeutung. Die Schulungen sollten dabei auf die spezifischen Bedürfnisse und Risiken verschiedener Abteilungen und Hierarchieebenen zugeschnitten sein.

Technische Integration

Die technische Infrastruktur bildet das Rückgrat moderner Cybersicherheit. Ein mehrschichtiger Sicherheitsansatz beginnt bei grundlegenden Maßnahmen wie regelmäßigen Systemaktualisierungen und einem robusten Patch-Management. Darauf aufbauend sind fortschrittliche Endpunktsicherheit, intelligente Netzwerksegmentierung und ein ausgereiftes Security Information and Event Management (SIEM) unerlässlich.

Besondere Bedeutung kommt der Integration verschiedener Sicherheitssysteme zu. Die Verknüpfung von Endpunktschutz, Netzwerküberwachung und Threat Intelligence ermöglicht eine ganzheitliche Sicherheitsstrategie. Moderne SIEM-Systeme nutzen dabei zunehmend künstliche Intelligenz, um Anomalien frühzeitig zu erkennen und potenzielle Bedrohungen zu identifizieren.

PHISHING BLEIBT EINE DER HARTNÄCKIGSTEN BEDROHUNGEN, DER 94 PROZENT DER ORGANISATIONEN ZUM OPFER FALLEN.

Gerald Eid, Managing Director DACH, Getronics Germany GmbH, www.getronics.com

Für viele Organisationen, insbesondere kleinere Finanzinstitute, stellt die interne Wartung dieser komplexen technischen Infrastruktur erhebliche Herausforderungen dar. Die Zusammenarbeit mit spezialisierten Managed-Service-Anbietern bietet hier einen strategischen Vorteil. Diese gewährleisten nicht nur eine 24/7-Sicherheitsüberwachung und schnelle Reaktionsfähigkeit bei Vorfällen, sondern bringen auch spezialisiertes Know-how und Skalierbarkeit mit.

Best Practices der Implementierung

Die erfolgreiche Implementierung von Sicherheitsmaßnahmen erfordert einen strukturierten Ansatz. Zunächst ist eine gründliche Bestandsaufnahme der vorhandenen Systeme und Prozesse notwendig. Darauf aufbauend sollte eine Risikoanalyse durchgeführt werden, die sowohl technische als auch organisatorische Schwachstellen identifiziert.

Ein besonderer Fokus sollte auf der Integration von Sicherheitsmaßnahmen in bestehende Geschäftsprozesse liegen. Dabei gilt es, einen ausgewogenen Ansatz zu finden, der Sicherheit gewährleistet, ohne die Effizienz der Arbeitsabläufe zu beeinträchtigen. Wichtig ist auch die Etablierung klarer Verantwortlichkeiten und Kommunikationswege für den Fall von Sicherheitsvorfällen.

Die KI-Herausforderung

Mit Blick auf 2025 entwickelt sich künstliche Intelligenz zu einem Game-Changer in der Cybersicherheit. Sicherheitsexperten erwarten einen signifikanten Anstieg KI-gesteuerter Cyber-Bedrohungen im ersten Quartal 2025. Besonders besorgniserregend ist dabei die zunehmende Sophistikation von Deep-Fake-Technologien. Diese ermöglichen nicht nur die täuschend echte Nachahmung von Führungskräften in Videoanrufen, sondern auch das Klonen von Stimmen für betrügerische Autorisierungen.

Die Integration von KI in Sicherheitssysteme erfordert dabei nicht nur technische Expertise, sondern auch ein tiefes Verständnis der zugrundeliegenden Al-

ÜBER 75 % DER CYBERANGRIFFE BEGINNEN MIT EINER E-MAIL.

ES WIRD ANGENOMMEN, DASS **CYBERKRIMINELLE** IN 93% DER UNTERNEHMENSNETZWERKE **EINDRINGEN KÖNNEN.**

gorithmen und ihrer potenziellen Schwachstellen. Organisationen müssen sicherstellen, dass ihre KI-Systeme regelmäßig trainiert und aktualisiert werden, um mit der Evolution der Bedrohungen Schritt zu halten.

Die Bedrohungslandschaft wird zunehmend durch automatisierte, KI-gesteuerte Angriffssysteme geprägt. Diese können Schwachstellen automatisch identifizieren und ausnutzen, Passwörter intelligent knacken und sich durch adaptive Malware kontinuierlich an Abwehrmaßnahmen anpassen. Besonders gefährlich sind kontextbewusste Phishing-Kampagnen, die mithilfe von KI personalisierte und damit besonders überzeugende Angriffsszenarien entwickeln.

Regulatorische Compliance und Risikomanagement

Die Einführung von DORA markiert einen Wendepunkt in der europäischen Finanzregulierung. Die Verordnung verlangt von Finanzinstituten nicht nur die Implementierung umfassender ICT-Risikomanagement-Systeme, sondern auch regelmäßige Tests der operationellen Resilienz. Besondere Bedeutung kommt dabei dem Management von Drittanbieterrisiken zu, da die Lieferkette zunehmend als Einfallstor für Cyberangriffe genutzt wird.

Ein effektives Risikomanagement muss dabei die verschiedenen Bedrohungsszenarien priorisieren und entsprechende Gegenmaßnahmen entwickeln. Wichtig ist auch die Integration von Cyber-Threat-Intelligence, um proaktiv auf neue Bedrohungen reagieren zu können. Die Zusammenarbeit mit spezialisierten Intelligence-Sharing-Plattformen und die aktive Teilnahme an Branchennetzwerken sind dabei von entscheidender Bedeutung.

Lessons Learned und Zukunftsperspektiven

Die Erfahrungen der letzten Jahre zeigen, dass erfolgreiche Cybersicherheit vor allem eine Frage der Unternehmenskultur ist. Organisationen, die Sicherheit als integralen Bestandteil ihrer Geschäftsstrategie verstehen und entsprechende Ressourcen bereitstellen, sind deutlich besser gegen Cyberangriffe gewappnet.

Für die Zukunft zeichnet sich ab, dass die Grenzen zwischen physischer und digitaler Sicherheit weiter verschwimmen werden. Die zunehmende Vernetzung von Systemen und die Integration von IoT-Geräten erfordern ganzheitliche Sicherheitskonzepte, die beide Dimensionen berücksichtigen.

Womit fängt man am besten an?

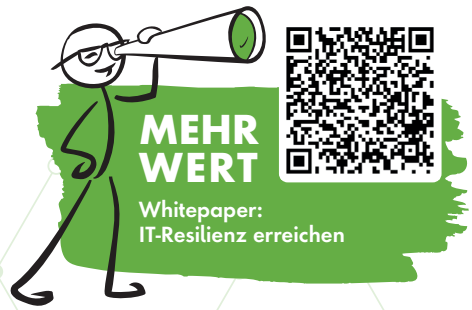
Die Cybersicherheitslandschaft im Finanzsektor wird sich in den kommenden Jahren weiter dynamisch entwickeln. Der Erfolg von Sicherheitsstrategien wird dabei zunehmend von der Fähigkeit abhängen, Menschen, Technologie und Prozesse optimal zu integrieren.

Konkrete Handlungsempfehlungen für Organisationen umfassen:

- Die Entwicklung einer ganzheitlichen Sicherheitsstrategie unter Berücksichtigung aller relevanten Stakeholder
- Kontinuierliche Investitionen in Mitarbeiterschulungen und technische Infrastruktur
- Die Etablierung starker Partnerschaften mit spezialisierten Sicherheitsdienstleistern
- Die aktive Teilnahme an Branchennetzwerken zum Informationsaustausch
- Regelmäßige Überprüfung und Anpassung der Sicherheitsmaßnahmen

Die Investition in Cybersicherheit ist dabei nicht nur eine technische, sondern vor allem eine strategische Entscheidung. Organisationen müssen sicherstellen, dass sie über die notwendigen Ressourcen und Expertise verfügen, um den Herausforderungen von morgen bereits heute zu begegnen. Nur wer sich frühzeitig auf die kommenden Bedrohungen vorbereitet und seine Sicherheitssysteme kontinuierlich weiterentwickelt, wird in der zunehmend komplexen Bedrohungslandschaft bestehen können.

Gerald Eid



PHISHING

DAS ANGELN DER ETWAS ANDEREN ART

Jeder von uns experimentiert auf die eine oder andere Weise mit dem Thema KI. Die Frage ist, wie kann ich KI sinnvoll in den täglichen Arbeitsablauf integrieren, denn für alles ist sie nicht geeignet.

Während künstliche Intelligenz Unternehmen mit innovativen Lösungen revolutioniert, nutzen Cyberkriminelle dieselbe Technologie, um ausgeklügeltere Phishing-Attacken zu entwickeln. Somit ermöglicht KI es Angreifern, täuschend echte gefälschte E-Mails zu generieren, Sprachmuster zu imitieren und personalisierte Betrugsversuche zu orchestrieren und die klassische Abwehrmechanismen zu unterlaufen.

In diesem eBook erwartet Sie Wissenswertes zu den Aspekten der unterschiedlichen Arten von Phishing, psychologische Aspekte bei Angriffen, Erkennungsmerkmale, Details zu häufigen Angriffszielen, Schutzmaßnahmen, rechtliche Aspekte, dem Thema Notfallplan, Schulung und Sensibilisierung sowie ein Ausblick zu den Zukunftsperspektiven.

Aus dem Inhalt

- Cybersicherheit im Finanzsektor
- Grundlagen zum Thema Phishing
- Notfallplan bei Phishing-Atttacken
- Zukunftsperspektiven

eBOOK DOWNLOAD

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

Willkommen in der Ära der Deepfakes

EIN SURVIVAL-GUIDE FÜR DIE PARALLELWELT

Die Nachricht erreicht Sie plötzlich und unerwartet: Ein dringender Videoanruf vom Chef, der eine sofortige Überweisung anfordert. Ein virales Video eines Prominenten mit bizarren Ausgaben oder eine täuschend echte Nachricht eines Familienmitgliedes in Not – Willkommen in der Ära der Deepfakes. Dieser Artikel soll Ihnen dabei helfen, Deepfakes im Alltag zu erkennen:

Die alarmierenden Deepfake-Fälle der letzten Jahre zeigen, wie realistisch diese Täuschungen geworden sind. Vom millionenschweren Betrug bis zum viralen Spaß-Bild: Die folgende Auswahl macht deutlich, warum wir uns dringend mit diesem Thema auseinandersetzen müssen.

Fallen Ihnen die Fehler auf? Ein Tipp: Schauen Sie auf Hände und Brille.

Bildquelle: Generiert mit Midjourney

Prominente Deepfake-Fälle

Der 25-Millionen-Dollar-Betrug bei Arup

Januar 2024: Die Täter kombinierten klassisches Phishing mit hochmodernen Deepfake-Technologien. Obwohl der Finanzangestellte des Ingenieur-Büros Arup zunächst skeptisch war, überzeugte ihn ein täuschend echter Videoanruf mit vermeintlichen Führungskräften. In 15 Einzeltransaktionen überwies er daraufhin insgesamt 25 Millionen Dollar. Besonders erschreckend: Selbst seine anfängliche Vorsicht wurde durch die Qualität der Fälschungen überwunden.

Der Papst im Streetwear-Look

Ein Bild von Papst Franziskus in einer weißen Balenciaga-Daunenjacke erobert 2023 das Internet. Millionen Menschen teilen das Foto, was viele aber nicht wissen: Es ist ein Deepfake. Die KI schafft zwar ein realistisches Bild, aber nicht ganz ohne Makel. So sind die Hände falsch dargestellt und eine Seite der Brille sieht anders aus als

die andere. Viralität ist auch noch lange kein Beweis für Echtheit.

Eine deutliche Warnung: Die Technologie wird immer besser. Aber wie können wir uns in Zukunft davor schützen, damit wir nicht darauf hereinfallen?

Schritt 1:
Die erste Prüfung
Die erste Prüfung ist entscheidend – hier werden die meisten Deepfakes entlarvt. Gerade in emotionalen Situationen und unter Zeitdruck passieren die schlimmsten Fehler. Sowohl im privaten als auch im geschäftlichen Kontext nutzen Betrüger genau diese menschliche Schwäche aus. Ein fingierter Notfall, eine angeblich dringende Überweisung – die Täter wollen, dass Sie schnell und ohne nachzudenken handeln. Nehmen Sie sich daher bewusst Zeit für diese ersten, wichtigen Prüfschritte:

- Ruhe bewahren, mehrfach ansehen/anhören
- Quelle kritisch prüfen
- bei geschäftlichen Anfragen: Etablierte Kommunikationswege nutzen
- bei privaten Nachrichten: direkten Kontakt auf bekannter Nummer suchen

Schritt 2:
Bewegungsmuster analysieren
Die menschliche Bewegung ist hochkomplex und für KI schwer nachzuahmen. Trotz beeindruckender Qualität der gefälschten Videos, verraten diese sich durch unnatürliche Bewegungsabläufe. In Geschäftsmeetings ist dies besonders relevant, da Sie die Gestik Ihrer Kollegen oft gut kennen. Achten Sie besonders auf die Harmonie der Bewegungen – echte Menschen bewegen sich fließend und natürlich:

- natürliche Bewegungen von Haaren und Kleidung
- Übergänge zwischen Kopf und Hals
- Synchronität aller Bewegungen
- Besonders bei Geschäftsmeetings: Gestik und Mimik der bekannten Person

Schritt 3:
Gesichtsdetails checken
Das menschliche Gesicht ist eine der komplexesten Bewegungsstrukturen überhaupt. Beim Arup-Betrug waren es gerade die feinen Details, die hätten stutzig machen können. Jeder Mensch hat charakteristische Mikroausdrücke und Bewegungsmuster, die eine KI nur schwer perfekt nachahmen kann. Diese Details sind sowohl im privaten als auch im geschäftlichen Kontext entscheidende Warnsignale.

- Augenglanz und natürliches Blinzeln
- Lippensynchronität bei Sprache
- Natürliche Hautstrukturen
- Mikroexpression und kleine Bewegungen

Schritt 4:
Die Stimme analysieren
Die Stimme ist unser persönlicher Fingerabdruck. Mittlerweile kann diese aber erschreckend gut gefälscht werden. Doch es gibt subtile Merkmale, die man beachten sollte – besonders, wenn Sie die echte Stimme der Person kennen:

- natürliche Sprachmelodie überprüfen
- auf Atmung und Pausen achten
- typische Sprachmuster und Redewendungen der Person suchen
- bei ungewöhnlichen Anweisungen oder emotionalen Appellen besonders skeptisch sein

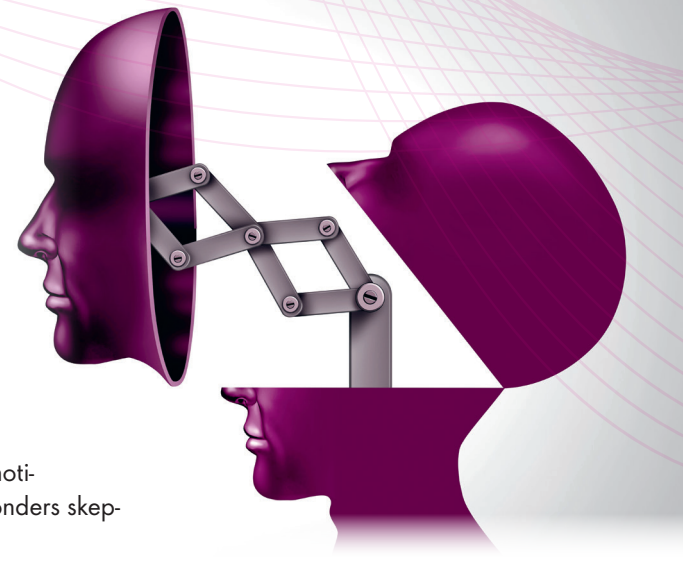
Schritt 5:
Kontext ist König
Der Kontext eines Videos oder einer Nachricht ist oft aufschlussreicher als technische Details. Der Papst im Streetwear-Look ging viral, weil viele den Kontext ignorierten. Wie wahrscheinlich ist es, dass sich das Kirchenoberhaupt in einer Balenciaga-Jacke öffentlich zeigen würde? Im Business-Bereich nutzen Betrüger oft vermeintliche Dringlichkeit, um übliche Abläufe und Prozesse zu umgehen. Prüfen Sie daher immer den größeren Zusammenhang.

Für Unternehmen:

#1 Passt die Anfrage zur Geschäftspolitik?
#2 Wurden übliche Hierarchien eingehalten?
#3 Entspricht die Kommunikation den Unternehmensrichtlinien?

Für Privatpersonen:

#1 Ist das Verhalten typisch für die Person?
#2 Passen der Zeitpunkt und die Art der Kommunikation?
#3 Gibt es ungewöhnlichen Zeitdruck?
#4 Werden Sie zu untypischen Handlungen gedrängt?



Schritt 6:

Physikalische Logik prüfen

Die physikalische Realität ist der größte Feind der Deepfakes. Bei Videocalls sind es oft unmögliche Lichtreflexionen. KI-Systeme können zwar Gesichter und Stimmen imitieren, scheitern aber häufig an den grundlegenden Gesetzen der Physik:

- Schatten und Lichtreflexionen analysieren
- auf unmögliche Objektbewegungen achten
- Größenverhältnisse überprüfen
- Bei Videocalls die Umgebung auf Stimmigkeit prüfen

Schritt 7:

Technische Absicherung

Die technischen Möglichkeiten zur Deepfake-Erkennung entwickeln sich ständig weiter. Sie können ein wichtiger Baustein der Verteidigung sein. Moderne Tools können Ihnen helfen, Fälschungen zu erkennen – nutzen Sie diese Ressourcen:

- Reverse-Image-Search für Bilder
- Zwei-Faktor-Authentifizierung für Geschäftsprozesse
- Verifizierte Kommunikationskanäle
- Bei Bedarf verwenden Sie KI-Erkennungstools

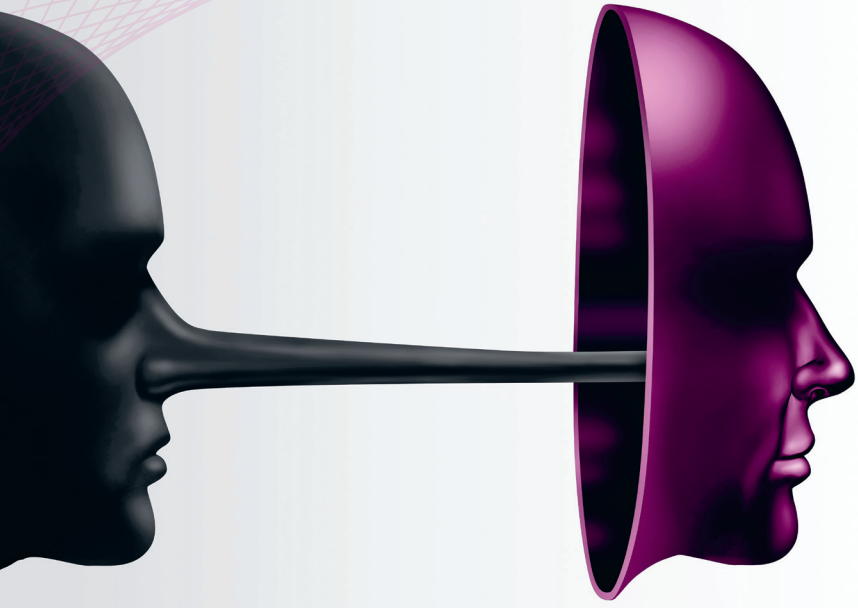
Schritt 8:

Sicherheitsprotokoll implementieren

Der Arup-Betrug hätte durch strikte Sicherheitsprotokolle verhindert werden können. In allen Bereichen sind klare Prozesse der beste Schutz gegen Deepfake-Betrug. Etablieren Sie feste Regeln und halten Sie diese konsequent ein.

Für Unternehmen:

#1 Festgelegte Verifizierungsschritte für wichtige Transaktionen
#2 regelmäßige Schulungen der Mitarbeiter
#3 Notfallpläne für Deepfake-Angriffe
#4 regelmäßige Updates der Sicherheitsprotokolle



AUCH DER ÜBERZEUGENDSTE DEEPFAKE HAT SEINE SCHWACHSTELLEN.

Lars Becker,
Redakteur, it verlag GmbH,
www.it-daily.net

Für Privatpersonen:

#1 Persönliche Codeworte mit Familie für Notfallsituationen vereinbaren
#2 bei „Notfallanrufen" immer Rückruf auf bekannter Nummer
#3 keine finanziellen Entscheidungen unter Zeitdruck

Fazit

Die Deepfake-Technologie entwickelt sich rasant weiter. Die gute Nachricht ist, dass Sie sich, Ihre Familie und Ihr Unternehmen mit einem geschulten Auge, klaren Prozessen und einem gesunden Menschenverstand schützen können. Denn auch der überzeugendste Deepfake hat seine Schwachstellen – man muss nur wissen, wonach man sucht.

Lars Becker

BUSINESS SECURITY

SIEBEN STRATEGIEN FÜR EFFEKTIVEN SCHUTZ VOR CYBERKRIMINALITÄT

Cyberangriffe nehmen stetig zu und bedrohen Unternehmen jeder Größe. Entdecken Sie in unserem Whitepaper, wie Sie Ihr Unternehmen mit sieben bewährten Strategien vor digitalen Bedrohungen schützen und nachhaltig absichern können. Von der Prävention bis zur Reaktion auf Vorfälle – starten Sie jetzt in eine sichere Zukunft.

Sind Sie bereit für die Herausforderungen der Cyberkriminalität?
Die Bedrohungslage im digitalen Raum war nie größer. Moderne Cyberangriffe treffen nicht nur große Konzerne, sondern zunehmend auch mittelständische Unternehmen und öffentliche Einrichtungen. Dabei stehen weit mehr als nur IT-Systeme auf dem Spiel: Kundendaten, Reputation und sogar die Geschäftskontinuität können gefährdet sein.

Unser Whitepaper „7 Strategien für eine proaktive Business Security" bietet Ihnen wertvolle Einblicke und praktische Lösungsansätze:

- Wie Sie eine robuste Sicherheitskultur etablieren
- Die Bedeutung eines effektiven Risikomanagements
- Modernste technische Schutzmaßnahmen und deren Implementierung
- Vorbereitung auf Sicherheitsvorfälle mit einem klaren Notfallplan

Schützen Sie Ihr Unternehmen proaktiv und bleiben Sie dem Wandel der Cyberbedrohungen stets einen Schritt voraus.

WHITEPAPER DOWNLOAD

Das Whitepaper umfasst 17 Seiten und steht kostenlos zum Downloadbereit.
www.it-daily.net/download

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:
Thomas Adenauer, Lars Becker, Robert Christian, Marco Eggerling, Gerald Eid, Holger Fischer, Gesine Froese, Fabian Glöser, Darren Guccione, Thomas Janz, Siegfried Kirschner, Alexander Koch, Carina Mitzschke, Silvia Parthier, Ulrich Parthier, Detlev Riecke, Richard Skalt

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

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.

TROTZ VERBOT WEITERHIN IM EINSATZ

WIE EFFEKTIV SIND TECHNOLOGIE-POLITISCHE MASSNAHMEN?

Wie eine neue Untersuchung des Sicherheitsunternehmens Bitsight ergab, verwenden rund 40 Prozent der US-Organisationen, die vor dem Stichtag am 29. September 2024 Kaspersky-Produkte einsetzten, diese auch nach dem Inkrafttreten des Verbotes weiterhin – darunter 19 staatliche Einrichtungen. Die Erkenntnisse basieren auf der Beobachtung von Verbindungen zwischen globalen IP-Adressen und Kaspersky-Update-Servern.

Die Analysten betonen, dass diese Ergebnisse die Notwendigkeit effektiverer Maßnahmen zur Überwachung des Technologieeinsatzes innerhalb der Landesgrenzen aufzeigen. Dies sei besonders relevant angesichts wachsender Bedenken bezüglich der Lieferkettensicherheit und der Vertrauenswürdigkeit von Technologieanbietern.

Deutlicher Rückgang weltweit

Trotz der anhaltenden Nutzung in den USA zeigt die Studie einen signifikanten Einfluss des Verbots auf die weltweite Verwendung von Kaspersky-Produkten. Während Bitsight im April 2024 noch Kommunikation von nahezu 22.000 Organisationen und über sieben Millionen einzelner IP-Adressen mit Kaspersky-Servern registrierte, sank diese Zahl bis Ende November auf etwa 8.000 Organisationen und zwei Millionen IP-Adressen – ein Rückgang um etwa zwei Drittel.

Interessanterweise war der Rückgang in Ländern ohne explizites Verbot sogar stärker ausgeprägt: Deutschland verzeichnete einen Rückgang um 69 Prozent, Großbritannien um 70 Prozent und Italien um 65 Prozent – verglichen mit 58 Prozent in den USA.

Die Ergebnisse der Analyse werfen die Frage auf, wie effektiv solche technologiepolitischen Maßnahmen in der Praxis umgesetzt werden können und welche Herausforderungen bei der Durchsetzung bestehen.

Lars Becker

The Aftermath of the Kaspersky Ban

MEHRWERT

Haben Sie etwa eine Ausgabe der itmanagement und itsecurity

verpasst?

...mit einem Abo wäre das nicht passiert.

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

ZUM ABO

it-daily.net/leser-service

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

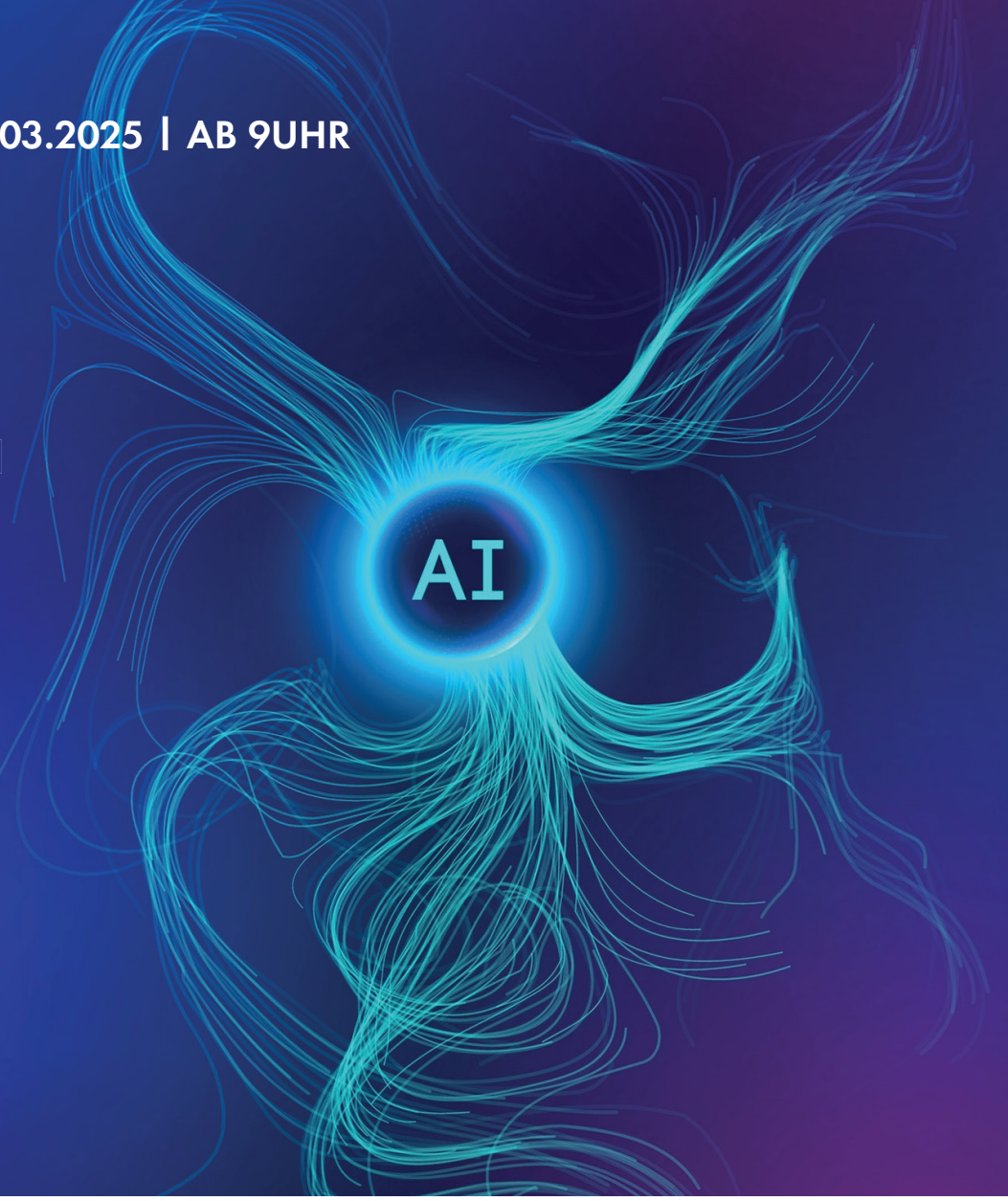
IT MANAGEMENT DIGITALEVENT

GENERATIVE AI: ZUKUNFT DER TECHNOLOGIE

MITTWOCH, 19.03.2025 | AB 9UHR

#GenAI

Infos und Anmeldung



Eine Veranstaltung von itmanagement & it-daily.net